ISSN 2713-3192
DOI 10.15622/ia.2023.22.5
http://ia.spcras.ru

ТОМ 22 № 5

ИНФОРМАТИКА И АВТОМАТИЗАЦИЯ

INFORMATICS AND AUTOMATION

СПб ФИЦ РАН

Санкт-Петербург
2023

INFORMATICS AND AUTOMATION

Volume 22 № 5, 2023

Scientific and educational journal primarily specialized in computer science, automation, robotics, applied mathematics, interdisciplinary research
Founded in 2002

Founder and Publisher
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)

Editor: A. S. Lopotova **Interpreter:** Ya. N. Berezina
Art editor: N. A. Dormidontova

Editorial office address
SPC RAS, 39 litera A , 14-th line V.O., St. Petersburg, 199178, Russia
e-mail: ia@spcras.ru, web: http://ia.spcras.ru

The journal is indexed in Scopus

The journal is published under the scientific-methodological supervision of Department for Nanotechnologies and Information Technologies of the Russian Academy of Sciences

ИНФОРМАТИКА И АВТОМАТИЗАЦИЯ

Том 22 № 5, 2023

Научный, научно-образовательный журнал с базовой специализацией
в области информатики, автоматизации, робототехники, прикладной математики
и междисциплинарных исследований.
Журнал основан в 2002 году

Учредитель и издатель

Федеральное государственное бюджетное учреждение науки
«Санкт-Петербургский Федеральный исследовательский центр Российской академии наук»
(СПб ФИЦ РАН)

Адрес редакции

14-я линия В.О., д. 39, лит. А, г. Санкт-Петербург, 199178, Россия

e-mail: ia@spcras.ru, сайт: http://ia.spcras.ru

Журнал индексируется в международной базе данных Scopus

Журнал входит в «Перечень ведущих рецензируемых научных журналов и изданий,
в которых должны быть опубликованы основные научные результаты диссертации
на соискание ученой степени доктора и кандидата наук»

Журнал выпускается при научно-методическом руководстве Отделения нанотехнологий
и информационных технологий Российской академии наук

CONTENTS

Digital Information Telecommunication Technologies

R. Yusupov, V. Ivanov
FROM THE HISTORY OF MATHEMATICAL MODELING MILITARY OPERATIONS IN RUSSIA (1900-1917) 947

B. Sokolov, D. Verzilin, T. Maksimova, M. Zhang
MUTUAL INFLUENCE OF INTELLECTUAL CAPITAL AND INFORMATION TECHNOLOGIES OF MANAGEMENT 968

M. Pelogeiko, S. Sartasov, O. Granichin
ON STOCHASTIC OPTIMIZATION FOR SMARTPHONE CPU ENERGY CONSUMPTION DECREASE 1 004

Information Security

E. Novikova, E. Fedorchenko, I. Kotenko, I. Kholod
ANALYTICAL REVIEW OF INTELLIGENT INTRUSION DETECTION SYSTEMS BASED ON FEDERATED LEARNING: ADVANTAGES AND OPEN CHALLENGES 1 034

A.E. Asfha, A. Vaish
INFORMATION SECURITY RISK ANALYSIS IN FOOD PROCESSING INDUSTRY USING A FUZZY INFERENCE SYSTEM 1 083

U. Pilania, M. Kumar, T. Rohit, N. Nandal
A WALK-THROUGH TOWARDS NETWORK STEGANOGRAPHY TECHNIQUES 1 103

Artificial Intelligence, Knowledge and Data Engineering

S.I. Abudalfa
EVALUATION OF SKELETONIZATION TECHNIQUES FOR 2D BINARY IMAGES 1 152

A. Vorobev, A. Lapin, G. Vorobeva
SOFTWARE FOR AUTOMATED RECOGNITION AND DIGITIZATION OF ARCHIVE DATA OF AURORA OPTICAL OBSERVATIONS 1 177

I. Surov
COLOR CODING OF QUBIT STATES 1 207

СОДЕРЖАНИЕ

Цифровые информационно-телекоммуникационные технологии

Р.М. Юсупов, В.П. Иванов
ИЗ ИСТОРИИ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ БОЕВЫХ ДЕЙСТВИЙ В РОССИИ (1900-1917 ГГ.) 947

Б.В. Соколов, Д.Н. Верзилин, Т.Г. Максимова, М. Чжан
ВЗАИМНОЕ ВЛИЯНИЕ ИНТЕЛЛЕКТУАЛЬНОГО КАПИТАЛА И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ УПРАВЛЕНИЯ 968

М.А. Пелогейко, С.Ю. Сартасов, О.Н. Граничин
О СТОХАСТИЧЕСКОЙ ОПТИМИЗАЦИИ ЭНЕРГОПОТРЕБЛЕНИЯ ПРОЦЕССОРА СМАРТФОНА 1 004

Информационная безопасность

Е.С. Новикова, Е.В. Федорченко, И.В. Котенко, И.И. Холод
АНАЛИТИЧЕСКИЙ ОБЗОР ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ, ОСНОВАННЫХ НА ФЕДЕРАТИВНОМ ОБУЧЕНИИ: ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ И ОТКРЫТЫЕ ЗАДАЧИ 1 034

А.Э. Асфха, А. Вайш
АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПИЩЕВОЙ ПРОМЫШЛЕННОСТИ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ НЕЧЕТКОГО ВЫВОДА 1 083

У. Пилания, М. Кумар, Т. Рохит, Н. Нандал
КРАТКИЙ ОБЗОР МЕТОДОВ СЕТЕВОЙ СТЕГАНОГРАФИИ 1 103

Искусственный интеллект, инженерия данных и знаний

Ш.И. Абудальфа
ОЦЕНКА МЕТОДОВ СКЕЛЕТИЗАЦИИ ДВУМЕРНЫХ БИНАРНЫХ ИЗОБРАЖЕНИЙ 1 152

А.В. Воробьев, А.Н. Лапин, Г.Р. Воробьева
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ АВТОМАТИЗИРОВАННОГО РАСПОЗНАВАНИЯ И ОЦИФРОВКИ АРХИВНЫХ ДАННЫХ ОПТИЧЕСКИХ НАБЛЮДЕНИЙ ПОЛЯРНЫХ СИЯНИЙ 1 177

И.А. Суров
ЦВЕТОВАЯ КОДИРОВКА КУБИТНЫХ СОСТОЯНИЙ 1 207

УДК 004.056 **DOI** 10.15622/ia.22.5.1

Р.М. Юсупов, В.П. Иванов

ИЗ ИСТОРИИ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ БОЕВЫХ ДЕЙСТВИЙ В РОССИИ (1900-1917 ГГ.)

Юсупов Р.М., Иванов В.П. **Из истории математического моделирования боевых действий в России (1900-1917 гг.).**

Аннотация. Статья посвящена оригинальным математическим моделям боевых действий, разработанным в России в начале XX века. Одной из первых работ, в которой излагались подходы к математическому моделированию боевых действий, можно считать статью Я. Карпова «Тактика крепостной артиллерии», опубликованную в 1906 году. В ней рассматривалась задача обороны крепости от атакующих пехотных цепей противника. Исходя из идеи непреодоления атакующими рубежа обороны, были получены математические соотношения, увязывающие параметры выстрела заряда шрапнели с перемещениями пехотинца. Аналогичным образом рассматривалась задача использования для обороны крепости пулемета. Проанализировав полученные соотношения, Я. Карпов пришел к выводу, что все средства обороны крепости можно соотнести через длину обороняемого этим средством участка. Идеи Я. Карпова развил П. Никитин. Им был рассмотрен широкий спектр средства поражения. Опираясь на результаты проведенных исследований, автором сделаны рекомендации по распределению сил и средств при обороне крепостей. М. Осипов в 1915 году опубликовал яркие и самобытные модели двухсторонних боевых действий, на год раньше известной теории Ланчестера. Суммируя численности сражающихся сторон на бесконечно малых интервалах времени, а затем, переходя к пределам, он получает линейный и квадратичный законы влияния соотношения численности сражающихся сторон на их потери, исследует разнородные средства поражения. Все это проверяется практикой различных сражений. М. Осипов показал, что коэффициенты в законах потерь зависят от выучки личного состава, рельефа местности, наличия укреплений, морально-психологического состояния войск и т.д. Опираясь на результаты математического моделирования, М. Осипов впервые обосновал ряд положений военного искусства. Он показал, что ни линейный, ни квадратичный законы потерь в общем случае не соответствуют практике проведенных сражений. Для удобства использования при том уровне развития вычислительной техники и для получения более достоверного результата М. Осипов предлагал использовать в законах потерь степень «три вторых», хотя сам понимал ее приближенный характер. Много внимания уделено проблеме авторства, поискам прототипа создателя первой двухсторонней модели боевых действий, применению теории для решения современных прикладных задач.

Ключевые слова: математическое моделирование, боевые действия, алгебраические и дифференциальные модели.

1. Введение. Математическое моделирование сегодня широко применяется для решения разнообразных задач в различных сферах человеческой деятельности и тесно смыкается с компьютерным моделированием. Не является исключением и такая специфическая сфера, как вооруженная борьба. Первое использование математических методов для ее исследования относится к середине

XIX века. В начале XX века, когда вооруженная борьба впервые приобрела глобальный характер, интерес к ним усилился.

Оснащение армии новым, более совершенным оружием (магазинные винтовки, пулеметы, скорострельные пушки, авиация и т.д.) привело к коренным изменениям в формах и способах ведения боевых действий. Внедрение методов массового производства для выпуска образцов вооружений способствовало появлению многомиллионных армий. Кратковременные сражения сменились огромными по размаху в пространстве и времени операциями.

В известном смысле война стала «дорогим удовольствием», как, впрочем, и крупномасштабные учения, позволяющие комплексно оценить те или иные аспекты грядущих сражений.

Математическое моделирование позволяло получать оценки результатов операций и проводить их анализ более дешевым способом по сравнению с учениями. Поэтому начался поиск рациональных методов математического моделирования боевых действий.

Вероятностные методы, которые хотя ограниченно и применялись для различных оценок, были слишком абстрактны. Развернулась разработка более наглядных методов, которые, в эпоху, когда основным вычислительным средством являлась логарифмическая линейка, позволяли бы проще анализировать и интерпретировать получаемые результаты, отвечая на текущие запросы войск. Такой процесс с конца XIX века начался во многих ведущих военных державах мира.

Не была исключением и Россия.

2. Ранние математические модели и методы. Одной из первых отечественных работ, в которой излагались подходы к математическому моделированию боевых действий, можно считать статью Я. Карпова «Тактика крепостной артиллерии», опубликованную в 1906 году [1].

В ней рассматривалась задача обороны крепости от атакующих пехотных цепей противника. Первоначально в качестве основного средства защиты крепости автор рассматривал пушку, стреляющую шрапнелью. Общая идея его подхода заключалась в следующем.

При разрыве шрапнели пули накрывают часть поверхности земли. Для срыва атаки достаточно выпустить такое количество пуль, чтобы на участок, занимаемый человеком, за время, необходимое ему для преодоления поверхности разрыва шрапнели, пришлось не менее одной пули.

Отсюда следует, что длина участка L_i, обороняемого от атакующих цепей пехотинцев одной i-той пушкой, стреляющей шрапнелью, находится из выражения:

$$L_i = \frac{c_{sk}\, n_s\, S_p}{V_p}, \quad (1)$$

где c_{sk} – скорострельность пушки (число выстрелов в единицу времени), n_s – число пуль в шрапнельном снаряде, S_p – площадь участка, занимаемого человеком, V_p – средняя скорость движения пехотинца при атаке.

Использовав аналогичный подход, Я. Карпов получил формулу для оценки длины участка L_{ip}, обороняемого i-тым пулеметом:

$$L_{ip} = \frac{c_{sk}\, a_p\, b_p}{V_p}, \quad (2)$$

где a_p – ширина участка фронта, занимаемого человеком, b_p – глубина поражаемого пространства.

Зависимость (2) можно использовать и для оценки длины участка фронта, обороняемого пехотинцем, если под c_{sk} понимать скорострельность магазинной винтовки.

Проанализировав формулы (1) и (2), Я. Карпов пришел к мысли, что все средства обороны крепости можно соотнести через длину обороняемого этим средством участка. Он получил, что в обороне один пулемет равноценен, примерно, 40 пехотинцам. Он сделал вывод о том, что для отражения штурма крепости наиболее эффективными средствами являются скорострельная пушка и пулемет.

Несмотря на простоту, зависимости (1) и (2) позволяли решать различные тактические задачи. Например, если подразделение насчитывает m пехотинцев, вооруженных винтовками, n скорострельных пушек, k пулеметов, то можно рассчитать длину обороняемого им участка фронта. Если учесть норму потерь, то при заданном численном составе можно определить, сколько времени можно удерживать данный участок обороны.

Исследования Я. Карпова продолжил и развил П. Никитин [2]. Опираясь на созданные Я. Карповым модели, он проанализировал широкий спектр средств поражения. Результаты выполненных им расчетов представлены в таблице 1.

Подтвердив вывод Я. Карпова о том, что пулемет, примерно, в 40 раз эффективнее винтовки, П. Никитин приводит экспериментальные данные Опытовой комиссии Офицерской стрелковой школы, согласно которым при стрельбе на 2000 шагов пулемет равноценен 45 стрелкам.

Отметим, что для подтверждения теоретических положений Опытовой комиссией был сооружен специальный стенд, имитирующий продвижение атакующих цепей. Анализ результатов показал хорошее согласование теоретических и экспериментальных результатов.

Автором сделаны рекомендации по распределению сил и средств при обороне крепостей.

Таблица 1. Ширина участка обороны по фронту на одно средство поражения

Средства поражения	**Ширина участка обороны, м**
3-дм скорострельная пушка	17,1
57-мм противоштурмовая пушка – картечь – шрапнель	10,7
Пулемет	6,4
Конная или легкая пушка образца 1895 года, шрапнель	4,3
Конная или легкая пушка образца 1877 года, шрапнель	2,1
9-дм пушка, шрапнель	2,1
4-фн пушка, картечь	1,1

3. Математическая модель двухсторонних боевых действий М. Осипова. Как известно, в августе 1914 года началась Первая мировая война. На фронтах лилась кровь, а в тылу воюющих стран развернулись работы по производству новых образцов вооружений. Военные медики занялись созданием новых методик проведения хирургических операций, новых методов лечения ран. Военные ученые тоже исследовали операции, но не хирургические, а вооруженных сил, искали пути достижения победы на фронтах, в армиях, корпусах.

В июне 1915 года в России журнал «Военный сборник» опубликовал большую статью М. Осипова под названием «Влияние численности сражающихся сторон на их потери» и дополнение к ней [3 – 7].

Первая часть статьи поступила в редакцию не позже апреля 1915 г., а это значит, что основное содержание достаточно объемной статьи было написано автором к середине 1914 г., методология разработана в середине 1912 г.

В своей работе Осипов выдвигает гипотезы о том, что отношение потерь сражающихся сторон обратно пропорционально отношению их численности (первая гипотеза) или квадрату отношений (вторая гипотеза). Он приводит таблицу 38 сражений, в которой указывает численность войск до начала сражения, потери сторон и показывает, что сильнейшая сторона несет потери меньшие, чем слабейшая.

Далее он занимается разработкой методического аппарата.

Обозначив за α – число поражений, нанесенных одним стрелком в единицу времени (полагаем этот коэффициент одинаковым для сторон), Осипов вводит бесконечно малый интервал времени Δt и рассматривает оставшиеся численности сторон спустя этот интервал. Суммируя их на конечном интервале времени и переходя к пределу, т.е. осуществляя интегрирование уравнений, получает экспоненциальные выражения, увязывающие начальную и конечную численности сторон за время t. Если A – начальная численность одной стороны, а B – другой, и, соответственно, A_k, B_k – конечные численности, то:

$$A_k = A\,\frac{e^{\alpha t} + e^{-\alpha t}}{2} - B\,\frac{e^{\alpha t} - e^{-\alpha t}}{2},$$

$$B_{\text{k}} = B\,\frac{e^{\alpha t} + e^{-\alpha t}}{2} - A\,\frac{e^{\alpha t} - e^{-\alpha t}}{2}.$$

После преобразования этих выражений для удаления экспонент, Осипов в итоге получает:

$$A_k^{\,2} - B_{\text{k}}^{\,2} = A^2 - B^2. \qquad (3)$$

Это квадратичный закон численности сторон в сражении. Его суть состоит в том, что разность квадратов численностей сражающихся сторон во всех фазах сражения остается постоянной.

Напомним, что квадратичный закон вывели из предположения, что число поражений, нанесенных одним стрелком противной стороне в единицу времени (коэффициент потерь), одинаковы для сражающихся сторон. Но М. Осипов хорошо понимает, что в общем случае это не так. Коэффициент потерь зависит не только от качества вооружения, но и от выучки личного состава, компетентности командования, тактики, рельефа местности, маскировки, наличия укреплений, морально-психологического состояния войск и т.д. Поэтому он рассмотрел случай, когда каждая сражающаяся сторона имеет свой коэффициент потерь. Если α – коэффициент потерь первой стороны, а η – второй, то, повторив все выкладки и преобразования, получим:

$$A^2 - A_k^{\,2} = \frac{\eta}{\alpha}\left(B^2 - B_k^{\,2} \right), \tag{4}$$

что соответствует решению следующей системы дифференциальных уравнений:

$$\begin{aligned} \frac{dA}{dt} &= -\eta B, \\ \frac{dB}{dt} &= -\alpha A \end{aligned} . \tag{5}$$

Конечное значение численностей сторон за время t найдем после интегрирования системы уравнений (5):

$$\begin{aligned} \sqrt{\alpha}\, A_{\text{k}} &= \sqrt{\alpha}\, A\, ch(t\sqrt{\alpha\eta}) - \sqrt{\eta}\, B\, sh(t\sqrt{\alpha\eta}) , \\ \sqrt{\alpha}\, B_{\text{k}} &= \sqrt{\alpha}\, B\, ch(t\sqrt{\alpha\eta}) - \sqrt{\eta}\, A\, sh(t\sqrt{\alpha\eta}) . \end{aligned} \tag{6}$$

Соотношение коэффициентов потерь позволяет оценить качественное отличие одной стороны от другой, например, оценить влияние выучки личного состава или морально-психологического состояния войск на численность потерь сторон.

Развивая свой научный подход, Осипов вводит в него разнородные средства поражения – винтовки, пушки, пулеметы. Если, например, первая сторона имеет A пехотинцев, вооруженных винтовками, M пушек, P пулеметов с интенсивностью поражения, соответственно, α, γ, ε, а вторая сторона B пехотинцев с винтовками, N пушек, Q пулеметов с интенсивностями β, δ, ζ, то число потерь противной стороны в единицу времени составит $\alpha A + \gamma M + \varepsilon P$ и $\beta B + \delta N + \zeta Q$. Подставив эти выражения в (6), мы получим изменение численности сторон под воздействием разнородных средств поражения.

Если, например, из первого выражения вынести за скобки α, тогда:

$$\alpha A + \gamma M + \varepsilon P = \alpha \left(A + \frac{\gamma}{\alpha} M + \frac{\varepsilon}{\alpha} P \right) = \alpha A_p .$$

Выражение в скобках означает приведение к условному числу пехотинцев A_p других поражающих факторов в виде пушек и пулеметов. Соответственно, $k_p = \frac{\gamma}{\alpha}$, $k_{mg} = \frac{\varepsilon}{\alpha}$ – коэффициенты приведения.

Аналог выражения (5) для этого случая имеет вид:

$$\left(A + \frac{\gamma}{\alpha} M + \frac{\varepsilon}{\alpha} P \right)^2 - \left(A_k + \frac{\gamma}{\alpha} M + \frac{\varepsilon}{\alpha} P \right)^2 = \\ = \frac{\eta}{\alpha} \left[\left(B + \frac{\delta}{\eta} N + \frac{\zeta}{\eta} Q \right)^2 - \left(B_k + \frac{\delta}{\eta} N + \frac{\zeta}{\eta} Q \right)^2 \right].$$

Далее Осипов рассматривает ряд практических задач, в том числе, когда часть сил A не поражается B. Он выделяет из общей численности войск активные силы, от деятельности которых напрямую зависит результат поведения той или иной операции.

М. Осипов также отмечает, что вооруженная борьба редко ведется до полного уничтожения сил противника, а в основном до того момента, когда будет достигнут определенный процент потерь.

Оценку достоверности своей теории Осипов проводит, сравнивая результаты реальных сражений с вычисленными,

идеализированными. Например, квадратичный закон справедлив, если войска известной выучки с определенной интенсивностью поражения сражаются на плоской открытой ровной местности без укреплений в идеальных погодных условиях. В реальных условиях эти оговорки не выполняются. Осипов это понимал. И поэтому считал, что вместо квадратичного закона, когда за бесконечно короткий промежуток времени потери сторон обратно пропорциональны их численности, надо применять другой. Одним из простых и приемлемых для того уровня используемой вычислительной техники являлось предположение о том, что потери обратно пропорциональны квадратному корню из их численности. Что в итоге эквивалентно не квадрату в формулах (3), (4), а степени $\frac{3}{2}$. Такое приближение ближе к истинному, хотя в общем случае тоже не идеально. Методология М. Осипова позволяла получать и иные законы потерь.

Анализ результатов проведенных вычислений позволили Осипову обосновать ряд положений военного искусства. Процитируем их словами автора.

1. «*Усиливая свою численность, мы наносим неприятелю большие потери и в то же время сами несем даже намного меньшие потери*».

2. «*При превосходстве сил высылать людей в бой в наибольшем числе не значит жертвовать ими бесполезно, а, наоборот, это значит сохранить их и выиграть время при решении поставленной задачи*».

3. «*Растерявшиеся в бою становятся союзниками врага. Вот почему трусость всегда приравнивается к подлости*».

4. «*С точки зрения потерь укрепления имеют огромное значение для обороняющихся. Атаковать даже полевые укрепления открытой силой можно только при значительном превосходстве в силах и особенно в артиллерии*».

5. «*И сильнейшему, и слабейшему выгодно выставлять наибольшие активные силы. Это вполне согласуется с известным правилом военного искусства начинать и вести военные операции с полным напряжением всех сил*».

6. «*Постепенное усиление цепи вместо высылки сразу сильной цепи выгодно не себе, а противнику, выславшему сразу сильную цепь*».

7. «*Правило – бить противника по частям служит несомненным подтверждением данной теории, что потери сильнейшего числом должны быть меньше, чем у слабейшего*». «*Силы*

свои не дробить, а быть сильным в одном месте и, конечно, в важнейшем при данных условиях».

Осипов понимал, что математические методы не подменяют собой основные положения теории военного искусства, а создают предпосылки для более умелого и грамотного их обоснования и применения. Он писал: «*Единственная практическая цель теории потерь – это более сознательное управление численностью войск для уменьшения своих потерь и увеличения потерь противника*».

Достаточно глубокая по тем временам теория Осипова ориентирована на исследование боевых действий разнородных подразделений сухопутных сил. К сожалению, Первая мировая война, революции, затем Гражданская война не позволили должным образом завершить начатые исследования.

4. К вопросу о научном приоритете. Согласно научной традиции приоритет устанавливается по дате публикации законченного научного исследования, которое продолжалось в течение длительного периода времени и имело публикованные предварительные результаты [8 – 16]. Отметим, что работа Осипова вышла из печати на год раньше известной работы Ланчестера «Самолет в боевых действиях» (1916 г.) [17]. Эта достаточно объемная книга насчитывает 19 глав. Математические выкладки содержит одна глава – пятая. В ней Ланчестер также приходит к дифференциальным уравнениям вида (3). Шестая глава посвящена приложениям – действиям флота и авиации. Результаты исследований Ланчестера затем изучались в работах его последователей [18 – 28]. По сравнению со статьей Осипова работа Ланчестера носит упрощенный характер. В ней не рассматриваются разнородные силы, нет сравнения применения результатов теории с практикой с оценками достоверности. И причин тому несколько.

Перед Первой мировой войной военные теоретики и практики видели в только что зародившейся авиации лишь средство для ведения разведки, бортовое вооружение самолетов отсутствовало. В возможность ведения войны в воздухе никто не верил. Ведь, прежде чем воевать, самолет в воздухе надо найти в просторах воздушного океана, а это казалось трудноразрешимой проблемой. Но уже первые месяцы войны показали, что необходимо противодействие воздушной разведке, эффективность которой росла от полета к полету. Русский штабс-капитан П.Н. Нестеров был вынужден таранить австрийский «Альбатрос», чтобы ценой своей жизни не допустить получение австро-венгерской армии важной развединформации о русских силах. Первоначально экипажи самолетов воюющих сторон вооружались

карабинами и маузерами [29]. Но очень быстро на самолетах появились пулеметы [30]. Началась война в воздухе. Надо было создавать основы авиационной тактики, стратегии. Работа Ланчестера и касалась осмыслению этих вопросов с учетом того, что летные характеристики и вооружение самолетов 1915 года всех воюющих стран были близки.

Похоже, что теории Осипова и Ланчестера создавались независимо друг от друга и отражали специфику исследуемых задач.

На Западе, ссылаясь на то, что разрозненные материалы пятой главы публиковались Ланчестером в конце 1914 года, отдают ему научный приоритет.

Однако работа Осипова как результат законченного научного исследования была опубликована раньше, созданная им теория более целостная и глубокая по сравнению с теорией Ланчестера, поэтому именно Осипова следует считать первооткрывателем нового научного направления. На наш взгляд, уравнения двухсторонних боевых действий правильнее называть уравнениями Осипова-Ланчестера.

5. К вопросу об идентификации личности автора. Опубликованная в пяти номерах журнала «Военный сборник» за 1915 год объемная статья с дополнением подписана: «М. Осипов». Но кем он был, мы сегодня вряд ли выясним. В различных частях его статьи содержатся лишь крупицы личностной информации. Что можно почерпнуть из текста о самом авторе замечательной для своего времени теории? Когда разрабатывались основные материалы статьи?

Основной текст, не менее 80 рукописных страниц, был написан во второй половине 1914 года. На проведение достаточно глубоких математических исследований вместе с расчетами, составление многочисленных таблиц, примеров должно уйти около полутора лет. Таким образом, начало написания статьи относится к концу 1912 г. Стоит обратить внимание на то, что в 1912 году в России широко отмечалось столетие Бородинского сражения, что вызвало повышенный интерес и ко всей эпохе Наполеоновских войн и, возможно, послужило толчком к проведению военно-исторических исследований.

Осипов демонстрирует знакомство с различными русскими Уставами полевой службы, показывает глубокие знания военной истории, в том числе русской военной истории. Используемый им для исследований методологический аппарат говорит о его хорошем знакомстве с математическим и статистическим анализом и со специальными функциями. Текст статьи написан грамотно с использованием большого словарного запаса. С другой стороны,

в статье Осипов упоминает, что не участвовал в боевых действиях, жалуется на нехватку времени для разработки темы.

По-видимому, Осипов был офицером, преподавателем военно-учебных заведений, а на момент написания статьи, возможно, преподавателем Николаевской военной академии. Примерный возраст сорок пять-пятьдесят лет. С небольшой долей вероятности можно заключить, что он мог быть и военным чиновником. Преподавателей военно-учебных заведений обычно не задействовали на фронте, а единственной крупной войной перед мировой была Русско-японская.

Теперь, казалось бы, чего проще, в архивах надо найти послужной список офицера, и мы о нем знаем все! Но, – увы! – в нашем случае кажущаяся простота лишь только подчеркивает сложность решения проблемы.

Да, действительно, в Российском государственном Военно-историческом архиве хранятся послужные списки офицеров с фамилией Осипов с соответствующим инициалом, включая генерал-майора М.П. Осипова из Военно-топографической службы Императорской армии. Именно его зарубежные (J.W. Knipp) и некоторые отечественные (Н.В. Митюков [31]) исследователи объявляют создателем новой теории.

Оценим возможность написания им статьи «Влияние численности сражающихся сторон на их потери».

М.П. Осипов родился в 1859 г., с 1899 г. служил в топогеодезических подразделениях русской армии, почти непрерывно участвовал в военно-топографических экспедициях в Туркестане, Енисейской губернии, в Семипалатинской области, в Читинском крае. Уточнял географические координаты населенных пунктов и географических точек Средней Азии и Сибири. Опубликовал шесть научных работ по прикладной астрономии, топогеодезии. В 1910 году издал основополагающий труд своей жизни «Влияние рефракции на геометрическую нивелировку». По семейным обстоятельствам в 1913 г. вышел в отставку. По-видимому, до конца 1913 г. занимался решением семейных проблем.

Сфера служебных и научных интересов М.П. Осипова – прикладная астрономия, геодезия и топография. Поэтому, даже выйдя в отставку, к середине 1914 г., он вряд ли бы приобрел глубокие знания по военной истории, в том числе по истории тактики и стратегии наполеоновских войн, и не менее глубокий опыт в разработке дифференциальных и дискретных моделей боевых действий. Выше показано, что основные идеи статьи «Влияние численности сражающихся сторон на их потери» разработаны к концу

1912 года. Поэтому вряд ли бы генерал-майор М.П. Осипов успел написать глубокую и объемную статью к середине 1914 г. спустя год после выхода в отставку. Стоит отметить, что стилистика статьи «Влияние численности сражающихся сторон на их потери» и стилистика работ генерал-майора М.П. Осипова по топогеодезии и прикладной астрономии различаются друг от друга. По этим причинам М.П. Осипов не может считаться автором статьи.

Следует обратить внимание вот на какое обстоятельство.

После Русско-японской войны, анализируя причины поражения, Генеральный Штаб Русской армии сделал вывод о том, что японцы умело использовали в бою психологический портрет нашего офицера. Этот, например, будет очертя голову кидаться вперед, а этот, не проявляя никакой инициативы, будет ждать приказа и т.д.

Поэтому, с 1906 года действовал указ, предписывающий штаб- и обер- офицерам армии и флота, занимающихся планированием и проведением операций, публиковать любые научные и литературные произведения только под псевдонимом. Исключение делалось для узкопоименованного списка военных преподавателей и военных журналистов. По этой причине, скорее всего, М. Осипов – это псевдоним автора основополагающей статьи. При разгоне военного министерства в 1918 году один из офицеров-контрразведчиков уничтожил картотеку дешифровки псевдонимов.

Трагичны судьбы русских офицеров в годы революций и Гражданской войны. Кого-то расстреляли как заложника в годы красного террора, кто-то погиб на фронтах, кто-то оказался в эмиграции. Творческий потенциал тех, кто остался в России, оказался не востребован в полной мере. Давлел ограниченный опыт Гражданской войны. Зачем изучать достижения военной мысли свергнутых классов? Ведь, как пелось в песне двадцатых годов двадцатого века, «*от тайги до Британских морей Красная Армия всех сильней!*».

В Париже в двадцатых годах генерал-лейтенант профессор Николай Николаевич Головин собрал на организованных им Высших военно-научных курсах практически всех русских военных ученых-эмигрантов. Но среди них не оказалось ни одного, кто занимался бы проблематикой «Осипова».

По-видимому, он погиб в годы революции и гражданской войны. Потребуются дальнейшие историко-архивные исследования, чтобы восстановить имя автора замечательной теории.

6. Теория Осипова в наше время. Прошли годы. Появились новые научные теории, инфотелекоммуникационные технологии.

Статья оказалась забытой. В семидесятых годах двадцатого века научный труд Осипова нашел, оценил значение и глубоко проанализировал Р.М. Юсупов. В результате его подвижнической деятельности была написана статья «Математическое моделирование в военном деле» [32], в которой работе Осипова было уделено должное внимание, оценен его вклад в развитие исследования операций и математического моделирования боевых действий. К сожалению, ограниченные издательские возможности редакции «Военно-исторического журнала», в котором печаталась эта статья, не позволили отразить в полной мере все замыслы Осипова.

На Западе материалы статьи Р.М. Юсупова изучил Р.Л. Хелмболд (США). Он разыскал и статью М. Осипова. По просьбе Хелмболда был выполнен ее точный перевод. Теория Осипова произвела на Хелмболда неизгладимое впечатление. Когда в 1993 году из печати в «Европейском журнале исследования операций» вышла его статья под названием «Осипов. «Русский Ланчестер»» [33] он написал следующие строчки: «*Я очарован методологическим подходом Осипова к проверке или подтверждению этих теоретических соображений. Он довольно подробно говорит о том, какие методы он использует, и делает все возможное, чтобы объяснить их*».

Хелмболд детально разбирает статью Осипова и сравнивает ее с работой Ланчестера: «…*Уникальный вклад Осипова, возможно, более существенен и важен, чем вклад Ланчестера. Осипов более глубоко вникал в суть дела и имел более здравый, более научный подход и мировоззрение, что ставит его в авангарде тех, кто интересуется теорией боевых операций… Осипов фактически записывает общее математическое решение квадратичного уравнения потерь. Хотя я уверен, что Ланчестер знал это решение, он не представил его в своих трудах, а вместо этого ограничился графическими примерами. По общему впечатлению можно сказать, что Осипов придерживался научного подхода, а Ланчестер — политического, полемического или пропагандистского. Самым ярким примером этого, с моей точки зрения, является то особое внимание, которое Осипов уделяет проверке или подтверждению теории, сравнивая ее предсказания с результатами исторических сражений. Таким образом, он обнаруживает важный факт, что боевая мощь не пропорциональна квадрату численности сторон. Он, по-видимому, первый известный в истории человек, констатировавший этот факт, который я назвал «законом Осипова* »».

Хотя прошел уже почти век, работой Осипова продолжают интересоваться исследователи.

В.А. Короткий [34] в статье с характерным названием «Математическое моделирование военных операций по Осипову-Ланчестеру: новые перспективы практического применения» воздает должное создателю самобытной теории, хотя считает ее автором военного топографа генерал-майора М.П. Осипова. В статье он анализирует вклад Осипова в моделирование военных действий, сравнивает его с Ланчестером. В.А. Короткий полагает, что главной причиной исторического забвения теории явились не годы революций и Гражданский войны, а отсутствие генерируемых ей практических рекомендаций по ведению боя. Он утверждает, что есть только два круга задач, где модели Осипова-Ланчестера сразу могут дать практические рекомендации – предварительный расчет сценариев военных действий на основе неполной оценочной информации и планирование «войны без победы», т.е. длительных «истощающих» конфликтов в интересах третьих стран. Приводит примеры.

В 2009 г. в журнале «Историческая психология и социология истории» [35] Н.В. Митюков опубликовал статью, посвященную определению жертв войн через ланчестерские модели. В ней он излагает методологию определения численности жертв войн как через классические ланчестерские модели, так и использует их модификации. К их числу он относит модели Осипова. Что само по себе достаточно удивительно, так как автор хорошо знает, что М.П. Осипов создал свои модели раньше ланчестерских, о чем свидетельствует публикация самого Н.В. Митюкова [31].

В 2020 году в десятом номере журнала «Военная мысль» была опубликована статья В.В. Шумова «Учет морального фактора и технологических характеристик в моделях боя» [36]. Само название говорит о том, что один из основных акцентов автор ставит на учете морального фактора. Он анализирует вклад Осипова в развитие принципов моделирования боевых действий, отмечает, что им заложены основы теории боевых потенциалов, показывает, что Осиповым определены основные факторы, подлежащие учету в моделях боя, включая искусство полководца, моральное состояние войск.

Далее автор рассматривает различные модели боя.

В вероятностной модели с использованием метода наибольшего правдоподобия Шумов получил неявное выражение для статистической оценки параметра боевого превосходства, тесно увязанного с морально-психологическим состоянием нападающих.

В модели потенциалов Шумов отмечает, что победа в войнах не всегда определяется соотношением военных потенциалов. Большую роль играет психологический фактор. И, используя подход Осипова, получает нижние оценки потерь. Такую же методологию можно применить для учета технологических факторов. Показана возможность масштабирования вероятностной модели боя.

Далее он рассматривает результаты решения теоретико-игровой модели «наступление-оборона» в преломлении к управлению боем.

В известной степени продолжением указанной статьи является статья «Математические модели боевых и военных действий» [37], написанная с участием того же автора.

К настоящему времени опубликовано достаточно много научных работ, использующих «уравнения Ланчестера» [38 – 43]. Их авторы зачастую не знают о вкладе Осипова в создание и развитие данного научного направления, они не предполагают, что разработанная М. Осиповым теория глубже и многограннее теории Ланчестера.

Из ряда методов, используемых для моделирования и исследования сложных явления нашей жизни, достаточно часто используется полимодельные технологии, в которых для разработки тех или иных «кирпичиков» всегда есть место для различных теорий, включая теоретические проработки М. Осипова.

Анализируя многочисленные публикации, хочется отметить, что до сих пор полностью не исследованы достаточно разнообразные направления возможного применения теории. А ведь это, помимо разнообразных сфер практической деятельности (методология математического моделирования задач тактики, психологии, оценок эффективности систем вооружений и др.) еще и оценки достоверности самой теории.

Иными словами, теория М. Осипова еще ждет своих исследователей.

7. Заключение. Статья посвящена оригинальным математическим моделям боевых действий, разработанным в России в начале XX века – математическим моделям Я. Карпова, П. Никитина. Особое внимание уделено моделям М. Осипова, опубликованным за год до Ланчестера. Показано, что по своей глубине, широте и значимости применения модели М. Осипова представляют собой более значимый научный вклад по сравнению с моделями Ланчестера. Рассмотрены исторические аспекты создания первых моделей боевых действий и проблемы авторства.

Анализ научных направлений прошедших эпох – это не только установление приоритетов, это анализ перспектив их дальнейшего развития, выделение ценного методологического и методического аппарата. Это к тому же еще одна из форм идеологической борьбы, особенно в условиях объявленной странами Запада попытки «устранить Россию».

Литература

1. Карпов Я. Тактика крепостной артиллерии. Военный сборник. 1906. Т. 11. С. 81–92.
2. Никитин П. Организация и боевая деятельность артиллерии при атаке и обороне современных крепостей. Артиллерийский журнал. 1911. Т. 9. С. 957–995.
3. Осипов М. Влияние численности сражающихся сторон на их потери. Часть 1. Военный сборник. 1915. № 6. С. 59–74.
4. Осипов М. Влияние численности сражающихся сторон на их потери. Часть 2. Военный сборник. 1915. № 7. С. 25–36.
5. Осипов М. Влияние численности сражающихся сторон на их потери. Часть 3. Военный сборник. 1915. № 8. С. 31–41.
6. Осипов М. Влияние численности сражающихся сторон на их потери. Часть 4. Военный сборник. 1915. № 9. С. 25–37.
7. Осипов М. Влияние численности сражающихся сторон на их потери. Дополнение. Военный сборник. 1915. № 10. С. 93–96.
8. Lanchester F.W. The Principle of Concentration. Engineering. 1914. vol. 98. pp. 422–433.
9. Lanchester F.W. Aerodynamics: constituting the first volume of a complete work on aerial flight. Constable. 1907. 488 p.
10. Lanchester F.W. Aerial flight. RSA Journal. 1908. vol. 57. pp. 997.
11. Lanchester F.W. The flying machine: the aerofoil in the light of theory and experiment. Proceedings of the Institution of Automobile Engineers. 1915. vol. 9. no. 2. pp. 171–259.
12. Lanchester F.W. The horse-power of the petrol motor in its relation to bore, stroke and weight. Proceedings of the Institution of Automobile Engineers. 1906. vol. 1. no. 2. pp. 153–220.
13. Lanchester F.W. Some problems peculiar to the design of the automobile. Proceedings of the Institution of Automobile Engineers. 1907. vol. 2. no. 1. pp. 185–257.
14. Lanchester F.W. Engine balancing. Proceedings of the Institution of Automobile Engineers. 1914. vol. 8. no. 2. pp. 195–271.
15. Lanchester F.W. Balancing means for reciprocating engines. U.S. Patent no. 1,163,832. Washington, DC: U.S. Patent and Trademark Office, 1915.
16. Bashaw J.N. Automobile shaft-coupling. U.S. Patent no. 1,022,999. Washington, DC: U.S. Patent and Trademark Office, 1912.
17. Lanchester W.F. Aircraft in Warfare. The Daun of the Fourth Arm. London: Constable and Company Limited, 1916. 222 p.
18. Jaiswal N.K. Homogeneous Combat Models. Military Operations Research: Quantitative Decision Making. 1997. vol. 5. pp. 233–282. DOI: 10.1007/978-1-4615-6275-7_9.
19. Clink R. Balancing of high-speed four-stroke engines. Proceedings of the Institution of Mechanical Engineers: Automobile Division. 1958. vol. 12. no. 1. pp. 73–110.

20. Goldsbrough G.R. The properties of torsional vibrations reciprocating engine shafts. Part I. Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character. 1926. vol. 113. no. 764. pp. 259–271.
21. Goldsbrough G.R. Torsional vibrations in reciprocating engine shafts. Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character. 1925. vol. 109. no. 749. pp. 99–119.
22. Johnson W.E. A method of balancing reciprocating machines. Journal of Applied Mechanics. 1935. vol. 2(3). pp. A81-A86.
23. Guest J.J. The main free vibrations of an autocar. Proceedings of the Institution of Automobile Engineers. 1926. vol. 20. no. 2. pp. 505–548.
24. Anvoner S. Solution of problems in mechanics of machines. Pitman Paperbacks, 1970. 525 p.
25. Dawtrey L.H. Automobile brakes. Proceedings of the Institution of Automobile Engineers. 1930. vol. 24. no. 2. pp. 564–623.
26. Horovitz M. Suspension of internal-combustion engines in vehicles. Proceedings of the Institution of Mechanical Engineers: Automobile Division. 1957. vol. 11. no. 1. pp. 17–51.
27. Appendino G. The phytochemistry of the yew tree. Natural Product Reports. 1995. vol. 12. no. 4. pp. 349–360.
28. Chang J.J. Nonvolatile semiconductor memory devices. Proceedings of the IEEE. 1976. vol. 64. no. 7. pp. 1039–1059.
29. Иванов В. Первый воздушный бой авиации Военно-морского флота России. Самолеты мира. 2001. № 1. С. 22–23.
30. Groehler O. History of the Air War 1910 to 1980. Berlin: Military publishing house of the German Democratic Republic, 1990. 743 p.
31. Митюков Н.В. М.П. Осипов: к идентификации личности автора первой модели глобальных процессов. Историческая психология и социология истории. 2011. Т. 4. № 2. С. 203–207.
32. Юсупов Р.М., Иванов В.П. Математическое моделирование в военном деле. Военно-исторический журнал. 1988. № 9. С. 79–83.
33. Helmbold R.L. Osipov: The ‘Russian Lanchester’. European Journal of Operational Research. 1993. vol. 65. no. 2. pp. 278–288.
34. Короткий В.А. Математическое моделирование военных операций по Осипову-Ланчестеру: новые перспективы практического применения. Прикладные задачи математики. Материалы XXVI международной научно-технической конференции. 2018. С. 21–26.
35. Митюков Н.В. Определение жертв войн через ланчестерские модели. Историческая психология и социология истории. 2009. Т. 2. № 2. С. 122–140.
36. Шумов В.В. Учет морального фактора и технологических характеристик в моделях боя. Военная мысль. 2020. № 10. С. 82–99.
37. Шумов В.В., Корепанов В.О. Математические модели боевых и военных действий. Компьютерные исследования и моделирование. 2020. Т. 12. № 1. С. 217–242
38. Новиков Д.А. Иерархические модели военных действий. Управление большими системами. 2012. Т. 37. С. 25–62.
39. Ганичева А.В. Модифицированная модель Ланчестера боевых действий. Автоматизация управляемых процессов. 2019. № 4(58). С. 72–81.
40. Жезлов А.В., Митюков Н.В., Бусыгина Е.Л. Моделирование движения участка фронта на основе ланчестерской модели. Современные наукоемкие технологии. 2012. № 9. С. 43–45.

41. Дульнев П.А., Котов А.В., Педенко Н.П. Прогнозирование хода и исхода общевойскового боя как метод теории общей тактики. Военная мысль. 2023. № 2. С. 28–37.
42. Плужников А.А. Развитие системы моделирования боевых действий Сухопутных войск. Военная мысль. 2020. № 10. С. 37–44.
43. Гончаров С.В. Методика оценки эффективности системы морально-психологического обеспечения соединений и воинских частей. Инноватика и экспертиза. 2018. Т. 3(24). С. 177–183.

Юсупов Рафаэль Мидхатович — д-р техн. наук, профессор, член-корреспондент РАН, заслуженный деятель науки и техники РФ, руководитель научного направления, Федеральное государственное бюджетное учреждение науки "Санкт-Петербургский Федеральный исследовательский центр Российской академии наук" (СПб ФИЦ РАН). Область научных интересов: теория чувствительности, идентификация, техническая диагностика, геофизическая кибернетика, проблемы национальной безопасности, проблемы информатизации общества. Число научных публикаций — 500. yusupov@iias.spb.su; 14-я линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)323-0366.

Иванов Владимир Петрович — канд. техн. наук, старший научный сотрудник, лаборатория прикладной информатики и проблем информатизации общества, Федеральное государственное бюджетное учреждение науки "Санкт-Петербургский Федеральный исследовательский центр Российской академии наук" (СПб ФИЦ РАН). Область научных интересов: математическое моделирование, динамические системы, методы оптимизация, системный анализ, динамика полета история науки и техники. Число научных публикаций — 153. vpivanov.spb.ru@gmail.com; 14-я линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)328-1919.

DOI 10.15622/ia.22.5.1

R. YUSUPOV, V. IVANOV

FROM THE HISTORY OF MATHEMATICAL MODELING MILITARY OPERATIONS IN RUSSIA (1900-1917)

Yusupov R., Ivanov V. **From the History of Mathematical Modeling Military Operations in Russia (1900-1917).**

Abstract. The article is devoted to the original mathematical models of combat operations developed in Russia at the beginning of the XX century. One of the first works in which approaches to mathematical modeling of military operations were outlined can be considered an article by Y. Karpov «Tactics of fortress artillery», published in 1906. It considered the task of defending the fortress from attacking enemy infantry chains. Based on the idea of the attackers overcoming the line of defense, mathematical relations were obtained linking the parameters of the shot of the shrapnel charge with the movements of the infantryman. Similarly, the task of using a machine gun for the defense of the fortress was considered. After analyzing the obtained ratios, Y. Karpov came to the conclusion that all means of defense of the fortress can be correlated through the length of the area defended by this means. P. Nikitin developed Y. Karpov's ideas. He considered a wide range of means of destruction. Based on the results of the research, the author made recommendations on the distribution of forces and means in the defense of fortresses. M. Osipov in 1915 published vivid and original models of two-way combat operations, a year earlier than the well-known Lanchester theory. Summing up the numbers of the fighting sides at infinitesimal intervals of time, and then moving to the limits, he obtains linear and quadratic laws of the influence of the ratio of the number of the fighting sides on their losses, and explores heterogeneous means of destruction. All this is verified by the practice of various battles. M. Osipov showed that the coefficients in the laws of losses depend on the training of personnel, terrain, the presence of fortifications, the moral and psychological state of the troops, etc. Based on the results of mathematical modeling, M. Osipov for the first time substantiated a number of provisions of the art of war. He showed that neither linear nor quadratic laws of losses in general do not correspond to the practice of the battles conducted. For ease of use at that level of computer technology development and to obtain a more reliable result, M. Osipov proposed using the degree of "three second" in the laws of losses, although he himself understood its approximate nature. Much attention is paid to the problem of authorship, the search for a prototype of the creator of the first two-sided model of combat operations, and the application of theory to solve modern applied problems.

Keywords: mathematical modeling, combat operations, algebraic and differential models.

References

1. Karpov Ya. [Tactics of fortress artillery]. Vojennyi sbornik – Military Compilation. 1906. vol. 11. pp. 81–92.
2. Nikitin P. [Organization and combat activity of artillery in the attack and defense of modern fortresses]. Artillerijskij zhurnal – Artillery journal. 1911. vol. 9. pp. 957–995.
3. Osipov M. [The influence of the number of the fighting sides on their losses. Part 1]. Vojennyi sbornik – Military Compilation. 1915. no 6. pp. 59–74.
4. Osipov M. [The influence of the number of the fighting sides on their losses. Part 2]. Vojennyi sbornik – Military Compilation.1915. no 7. pp. 25–36.
5. Osipov M. [The influence of the number of the fighting sides on their losses. Part 3]. Vojennyi sbornik – Military Compilation. 1915. no 8. pp. 31–41.
6. Osipov M. [The influence of the number of the fighting sides on their losses. Part 4]. Vojennyi sbornik – Military Compilation. 1915. no 9. pp. 25–37.

7. Osipov M. [The influence of the number of the fighting sides on their losses. Addition]. Vojennyi sbornik – Military Compilation. 1915. no 10. pp. 93–96.
8. Lanchester F.W. The Principle of Concentration. Engineering. 1914. vol. 98. pp. 422–433.
9. Lanchester F.W. Aerodynamics: constituting the first volume of a complete work on aerial flight. Constable. 1907. 488 p.
10. Lanchester F.W. Aerial flight. RSA Journal. 1908. vol. 57. pp. 997.
11. Lanchester F.W. The flying machine: the aerofoil in the light of theory and experiment. Proceedings of the Institution of Automobile Engineers. 1915. vol. 9. no. 2. pp. 171–259.
12. Lanchester F.W. The horse-power of the petrol motor in its relation to bore, stroke and weight. Proceedings of the Institution of Automobile Engineers. 1906. vol. 1. no. 2. pp. 153–220.
13. Lanchester F.W. Some problems peculiar to the design of the automobile. Proceedings of the Institution of Automobile Engineers. 1907. vol. 2. no. 1. pp. 185–257.
14. Lanchester F.W. Engine balancing. Proceedings of the Institution of Automobile Engineers. 1914. vol. 8. no. 2. pp. 195–271.
15. Lanchester F.W. Balancing means for reciprocating engines. U.S. Patent no. 1,163,832. Washington, DC: U.S. Patent and Trademark Office, 1915.
16. Bashaw J.N. Automobile shaft-coupling. U.S. Patent no. 1,022,999. Washington, DC: U.S. Patent and Trademark Office, 1912.
17. Lanchester W.F. Aircraft in Warfare. The Daun of the Fourth Arm. London: Constable and Company Limited, 1916. 222 p.
18. Jaiswal N.K. Homogeneous Combat Models. Military Operations Research: Quantitative Decision Making. 1997. vol. 5. pp. 233–282. DOI: 10.1007/978-1-4615-6275-7_9.
19. Clink R. Balancing of high-speed four-stroke engines. Proceedings of the Institution of Mechanical Engineers: Automobile Division. 1958. vol. 12. no. 1. pp. 73–110.
20. Goldsbrough G.R. The properties of torsional vibrations reciprocating engine shafts. Part I. Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character. 1926. vol. 113. no. 764. pp. 259–271.
21. Goldsbrough G.R. Torsional vibrations in reciprocating engine shafts. Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character. 1925. vol. 109. no. 749. pp. 99–119.
22. Johnson W.E. A method of balancing reciprocating machines. Journal of Applied Mechanics. 1935. vol. 2(3). pp. A81-A86.
23. Guest J.J. The main free vibrations of an autocar. Proceedings of the Institution of Automobile Engineers. 1926. vol. 20. no. 2. pp. 505–548.
24. Anvoner S. Solution of problems in mechanics of machines. Pitman Paperbacks, 1970. 525 p.
25. Dawtrey L.H. Automobile brakes. Proceedings of the Institution of Automobile Engineers. 1930. vol. 24. no. 2. pp. 564–623.
26. Horovitz M. Suspension of internal-combustion engines in vehicles. Proceedings of the Institution of Mechanical Engineers: Automobile Division. 1957. vol. 11. no. 1. pp. 17–51.
27. Appendino G. The phytochemistry of the yew tree. Natural Product Reports. 1995. vol. 12. no. 4. pp. 349–360.
28. Chang J.J. Nonvolatile semiconductor memory devices. Proceedings of the IEEE. 1976. vol. 64. no. 7. pp. 1039–1059.
29. Ivanov V. [The first air battle of the aviation of the Russian Navy]. Samolioty mira – Planes of the world. 2001. no. 1. pp. 22–23.

30. Groehler O. History of the Air War 1910 to 1980. Berlin: Military publishing house of the German Democratic Republic, 1990. 743 p.
31. Mityukov N.V. M.P. Osipov: towards the identification of the author of the first model of global processes. Istoricheskaja psychologija i sociologya istorii – Historical psychology and sociology of history. 2011. vol. 4. no. 2. pp. 203–207.
32. Yusupov R.M., Ivanov V.P. [Mathematical modeling in military affairs]. Voienno-istoricheskij zhural – Military History Magazine. 1988. no. 9. pp. 79–83.
33. Helmbold R.L. Osipov: The 'Russian Lanchester'. European Journal of Operational Research. 1993. vol. 65. no. 2. pp. 278–288.
34. Korotkiy V.A. [Mathematical modeling of military operations by Osipov-Lanchester: new perspectives of practical application]. Prikladnye zadachi matematiki. Materialy XXVI mezhdunarodnoj nauchno-tekhnicheskoj konferencii [Applied problems of mathematics. Materials of the XXVI International Scientific and Technical Conference]. 2018. pp. 21–26.
35. Mityukov N.V. [Definition of victims of wars through Lanchester models]. Istoricheskaya psihologiya i sociologiya istorii – Historical psychology and sociology of history. 2009. vol. 2. no. 2. pp. 122–140.
36. Shumov V.V. [Taking into account the moral factor and technological characteristics in combat models]. Voiennaia mysl – Military thought. 2020. no. 10. pp. 82–99.
37. Shumov V.V., Korepanov V.O. [Mathematical models of combat and military operations]. Komp'yuternye issledovaniya i modelirovanie – Computer research and modeling. 2020. vol. 12. no. 1. pp. 217–242
38. Novikov D.A. [Hierarchical models of military operations]. Upravlenie bol'shimi sistemami – Managing large systems. 2012. vol. 37. pp. 25–62.
39. Ganicheva A.V. [Modified model of the Lanchester combat operations]. Avtomatizaciya upravlyaemyh processov – Automation of managed processes. 2019. no. 4(58). pp. 72–81.
40. Zhezlov A.V., Mityukov N.V., Busygina E.L. [Modeling of the movement of the front section based on the Lanchester model]. Sovremennye naukoemkie tekhnologii – Modern high-tech technologies. 2012. no. 9. pp. 43–45.
41. Dul'nev P.A., Kotov A.V., Pedenko N.P. [Forecasting the course and outcome of a combined arms battle as a method of the theory of general tactics]. Voiennaia mysl – Military thought. 2023. no. 2. pp. 28–37.
42. Pluzhnikov A.A. [Development of the Ground Forces combat simulation system]. Voiennaia mysl – Military thought. 2020. no. 10. pp. 37–44.
43. Goncharov S.V. [Methodology for assessing the effectiveness of the system of moral and psychological support of formations and military units]. Innovatika i ekspertiza – Innovation and expertise. 2018. vol. 3(24). pp. 177–183.

Yusupov Rafael — Ph.D., Dr.Sci., Professor, Corresponding member of the Russian Academy of Sciences, Honored worker of science and technology of the Russian Federation, Head of scientific direction, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: sensitivity theory, identification, technical diagnostics, geophysical cybernetics, problems of national security, problems of informatization of society. The number of publications — 500. yusupov@iias.spb.su; 39, 14-th Line V.O., 199178, St. Petersburg, Russia; office phone: +7(812)323-0366.

Ivanov Vladimir — Ph.D., Senior researcher, Laboratory of applied informatics and problems of information society, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: mathematical modeling, dynamic systems, optimization methods, system analysis, flight dynamics, history of science and technology. The number of publications — 153. vpivanov.spb.ru@gmail.com; 39, 14-th Line V.O., 199178, St. Petersburg, Russia; office phone: +7(812)328-1919.

УДК 004 **DOI** 10.15622/ia.22.5.2

Б.В. Соколов, Д.Н. Верзилин, Т.Г. Максимова, М. Чжан

ВЗАИМНОЕ ВЛИЯНИЕ ИНТЕЛЛЕКТУАЛЬНОГО КАПИТАЛА И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ УПРАВЛЕНИЯ

Соколов Б.В., Верзилин Д.Н., Максимова Т.Г., Чжан М. **Взаимное влияние интеллектуального капитала и информационных технологий управления.**

Аннотация. На сегодняшний день существует общее представление об интеллектуальном капитале, разработаны различные подходы к его измерению на микро- и макроуровне. Разработаны методы патентной аналитики для анализа технологических трендов. На концептуальном уровне известно, что существует взаимовлияние интеллектуального капитала и технологических трендов, но отсутствуют методические разработки для количественного оценивания такого влияния с использованием данных из различных источников. Цель исследования заключается в количественном оценивании взаимного влияния национального интеллектуального капитала и современных информационных технологий управления на макроуровне. Рассмотрены математические основания разделения компонентов интеллектуального капитала и технологий. Подтверждена гипотеза о статистической значимости взаимовлияния интеллектуального капитала и информационных технологий управления. Определена регрессионная зависимость, которая достаточно хорошо аппроксимируется линейной регрессией индекса интеллектуального капитала от логарифма индекса патентной активности страны в области IT-методов управления, что может быть интерпретировано как замедление роста индекса интеллектуального капитала при достижении определенного уровня патентной активности. Установлено, что чем более развита экономика, тем выше в ней уровень интеллектуального капитала и выше уровень распространения IT-методов управления. Явными исключениями из этой закономерности являются Китай и Индия. Китай, который относится к странам с доходом выше среднего уровня, демонстрируют более высокие, чем страны его уровня экономического развития, взаимосвязанные значения индекса интеллектуального капитала и распространенности IT-методов управления. Индия, занимающая 3-е место среди стран с уровнем дохода ниже среднего, имеет соизмеримые показатели развития интеллектуального капитала и распространения IT-методов управления со странами с уровнем дохода выше среднего. Дальнейшие исследования могут быть связаны с проверкой гипотез о возможности выявления предложенным методом количественных зависимостей между интеллектуальным капиталом и технологическим развитием. Необходима детализация выявленных зависимостей по кодам Международной патентной классификации и составляющим интеллектуального капитала, выявление зависимостей для других технологических областей.

Ключевые слова: интеллектуальный капитал, информационные технологии управления, патентные ландшафты.

1. Введение. Экономика XXI века – это экономика знаний, новых инфокоммуникационных и цифровых технологий. Концептуальное описание деятельности компаний в экономике знаний основано на понятии интеллектуального капитала. Интеллектуальный капитал есть совокупность знаний, умений, компетенций, которыми обладают сотрудники, а также нематериальных активов, связей и взаимоотношений с поставщиками и клиентами, поддерживающих эти связи

инфраструктуры, имиджа и репутации [1, 2, 3, 4]. Исследования и измерения интеллектуального капитала в значительной степени посвящены либо концептуальным вопросам [1, 2, 3, 4, 5, 6, 7], либо проблемам измерения интеллектуального капитала на уровне предприятий [3, 8, 9, 10, 11, 12, 13]. Подход к измерению интеллектуального капитала для уровня национальных экономик предложен в работе [14]. Тем не менее, в настоящее время отсутствует как строгое определение интеллектуального капитала, так и единый подход к его измерению.

Новые информационные технологии, методы искусственного интеллекта и обработки больших данных, цифровизация управленческих и производственных процессов повышают конкурентоспособность компании [15, 16, 17]. На сегодняшний день накоплен опыт использования технологий искусственного интеллекта, дополненной реальности, больших данных в управлении сложными организационными и социально-экономическими системами, бизнес-процессами крупных предприятий и организаций. Научные исследования в этой области, как правило, сосредоточены на обсуждении специфики и возможностей использования конкретных технологий для целей управления сложными системами или процессами в одной из сфер деятельности, например, в промышленности, логистике и транспорте, торговле и маркетинге, финансовом секторе, сельском хозяйстве, медицине и здравоохранении, государственном управлении [18, 19, 20].

Широкое развитие в последние годы получил инструментарий построения патентных ландшафтов, предназначенный для анализа с использованием баз патентных данных состояния и трендов развития технологий, в том числе информационных [21, 22, 23].

Несмотря на то, что информационные технологии относят к нематериальным активам организации, и часто включают в состав интеллектуального капитала, взаимосвязь интеллектуального капитала и информационных технологий (фактически с выделением информационных технологий из состава интеллектуального капитала) также изучается многими авторами, о чем свидетельствуют результаты систематического обзора [24], выполненного по материалам 49 научных статей, посвященных этой теме.

Хотя является очевидным предположение о существовании взаимного влияния и синергии интеллектуального капитала и информационных технологий управления, в известных на сегодняшний день работах не рассматриваются математические основания разделения компонентов интеллектуального капитала и технологий, отсутствуют количественные оценки такого влияния, подходы к их построению.

2. Литературный обзор

2.1. Концепция интеллектуального капитала. Концепция интеллектуального капитала используется для оценивания нематериальных активов компании, которые основаны на знаниях. Классическими работами, дающими достаточно полное представление о концепции и измерении интеллектуального капитала являются [3, 14]. Как правило, выделяют две или три взаимосвязанных составляющих интеллектуального капитала, которые оцениваются на уровне компании по статистическим данным и экспертным опросам [3, 4, 8, 9, 10, 11, 12, 13]. При двухкомпонентном подходе выделяют человеческий капитал и структурный капитал. При трехкомпонентном подходе выделяют в составе структурного капитала организационный и клиентский капитал.

Человеческий капитал определяется как совокупность знаний и навыков работников, их лояльность и приверженность компании [3, 4, 7, 8, 14].

Организационный капитал определяется как совокупность патентов, авторских прав, товарных знаков, баз данных, программных систем, а также распределительных сетей, цепочек поставок, организационных процедур, возможностей и культуры организации [3, 4, 8]. Организационный капитал является важнейшим элементом интеллектуального капитала, который помогает улучшать и поддерживать человеческий капитал.

Клиентский капитал (капитал взаимоотношений) характеризует внешние связи организации. Это активы компании, которые возникли в процессе ее функционирования: связи с заинтересованными сторонами, каналы сбыта, взаимоотношения с клиентами, партнерами [3, 4, 8].

2.2. Измерение интеллектуального капитала. В работах [4, 8] представлены систематические обзоры подходов к определению и измерению интеллектуального капитала. При измерении интеллектуального капитала обычно используют указанный многокомпонентный подход. Каждая из компонентов оценивается с использованием статистических показателей, данных управленческой и бухгалтерской отчетности компаний, включающей сведения о нематериальных активах, данных фокусных исследований и экспертных опросов.

Выделяют несколько подходов к измерению интеллектуального капитала на уровне компании [3, 4, 7, 8, 9].

Методы прямого измерения (Direct Intellectual Capital methods – DIC) предполагают, что все компоненты ИК оцениваются в денежном эквиваленте.

Метод рыночной капитализации (Market Capitalization Methods – MCM) предполагает вычисление разности между рыночной капитализацией и акционерным капиталом.

Метод рентабельности активов (Return on Assets methods – ROA) основан на следующих вычислениях. Показатели стоимости основных средств и годовая прибыль сравниваются со средними значениями для отрасли или деятельности. Превышение удельной прибыли над средним значением используется как оценка интеллектуального капитала.

Методы, основанные на разработке системы показателей, отражающих состояние различных компонентов интеллектуального капитала (Scorecard Methods – SC). Наиболее известным является метод, предложенный финансово-страховой группой Skandia – Skandia Navigator [1, 8, 14].

Skandia Navigator [1, 8, 14] позволяет оценить пять элементов влияния интеллектуального капитала на результативность компаний: финансовые результаты компании; взаимоотношения с клиентами; технологические процессы, поддерживающие процесс создания ценности (IT – системы, базы данных, рабочие процедуры); ориентация на инновационное развитие; фокус на человеческий капитал. Индексы перечисленных элементов определяются на основе статистических данных, отчетности компании, экспертных оценок и суммируются для оценки интеллектуального капитала.

В работе [5] оценивалась роль интеллектуального капитала в установлении баланса между инновационной и приносящей доход деятельностью. Для оценивания вклада инновационного капитала в установление такого баланса использовались данные 217 малых и средних предприятий производственного сектора Пакистана. Данные были получены на основе опросников со шкалой Лайкерта. К полученным данным был применён PLS-регрессионный анализ. Подтверждена гипотеза о положительном влиянии всех компонентов интеллектуального капитала на установление баланса между инновационной и приносящей доход деятельностью.

В [6] обсуждается модель интеллектуальной пропускной способности организации, как меры производительности в переработке внешних знаний, превращении их в интеллектуальный капитал и, в итоге, генерации прикладных знаний, непосредственно используемых для создания ценности.

Пожалуй, единственной системной работой, в которой обоснован и апробирован подход к оцениванию интеллектуального капитала на макроуровне является работа Carol Yeh-Yun Lin and Leif Edvinsson [14].

Авторы [14] предложили подход к измерению национального интеллектуального капитала на основе открытых статистических и экспертных данных. Модель интеллектуального капитала основана на вычислении четырех индексов: индексов человеческого, рыночного, процессного капитала и индекса возобновления капитала (human, market, process, renewal capital indices). Эти показатели рассчитаны для 40 стран в динамике с 1995 по 2008 год. Каждый индекс вычисляется на основе 7 индикаторов, которые построены на основе статистических показателей из открытых баз данных, таких как World Bank, OECD, APEC, Commission of European Community, national Department of Commerce, Statistics etc. Дополнительно авторы использовали данные опросов фокусных групп. Финансовый капитал (GDP per capita) также включен в анализ.

Однако несмотря на множество разработок по количественному оцениванию интеллектуального капитала, тема остается открытой для дальнейших научных изысканий. Например, Leif Edvinsson, один из разработчиков Skandia Navigator и методики измерения национального интеллектуального капитала на макроуровне, считает [7], что важно анализировать не только значения интеллектуального капитала для текущего состояния, но и учитывать направление и скорость его изменения. Авторы [10] доказывают, что разработанные ранее методы и модели измерения и оценки интеллектуального капитала оказываются плохо применимыми для оценивания тенденций последнего десятилетия, отмеченного интенсивным развитием новых инфокоммуникационных и цифровых технологий.

2.3. Информационные технологии и интеллектуальный капитал. Ряд исследований последних лет посвящен изучению взаимовлияния информационных технологий и интеллектуального капитала.

В работе [24] авторы среди публикаций, представленных в ScienceDirect (http://www.sciencedirect.com/), Wiley Online Library (http://onlinelibrary.wiley.com/) Emerald Insight (http://www.emeraldinsight.com/) за период с 2009 по 2014 год, выявили 49 статей, посвященных о взаимном влиянии интеллектуального капитала и информационных технологий и представили их систематический обзор и классификацию. Приведены case-study IT компаний с точки зрения интеллектуального капитала. Информационные технологии рассмотрены как инструмент управления интеллектуальным капиталом, исследовано влияние интеллектуального капитала и информационных технологий на инновационное развитие, интеллектуальный капитал проанализирован

как ресурс разработки технологий. Сделан вывод о том, что большинство авторов исследуют человеческий капитал как наиболее важный элемент интеллектуального капитала, некоторые уделяют внимание структурному капиталу и капиталу взаимоотношений.

В работах [15, 16] сделана попытка оценить взаимосвязь между смарт-технологиями, цифровизацией и интеллектуальным капиталом, выявить потенциал технологий для улучшения интеллектуального капитала. Авторы [15] на основе анализа научных работ предлагают предварительную систематизацию положительных и отрицательных сторон процессов оцифровки информации об интеллектуальном капитале с точки зрения заинтересованных сторон. В работе [16] рассматривается как Индустрия 4.0 и связанные с ней интеллектуальные технологии могут влияют на управление интеллектуальным капиталом в целом, и как цифровизация может повлиять на его отдельные компоненты.

Исследование [17] представляет обзор публикаций, демонстрирующих трансформацию представления об интеллектуальном капитале по мере развития технологий больших данных. Авторы рассматривают концепцию интеллектуального капитала в свете зарождающейся парадигмы больших данных. Авторы анализируют: управленческие причины включения больших данных в интеллектуальный капитал; типологии больших данных, улучшающие практику развития интеллектуального капитала; заинтересованные стороны, участвующие в создании стоимости интеллектуального капитала с использованием больших данных; технологии больших данных, подходящие для управления интеллектуальным капиталом. Авторы [17] обосновывают вывод о том, что в цифровой экономике фокус исследований интеллектуального капитала должен быть смещен с уровня организаций на уровень экосистемы, то есть с микро на мезоуровень.

2.4. Подходы к измерению уровня развития технологий. Современным подходом к оценке уровня развития технологий является построение патентных ландшафтов с использованием методологии патентной аналитики.

Документ [23] представляет собой изложение подходов для детальной классификации патентных семейств в области искусственного интеллекта. В качестве источника данных использована база данных FAMPAT компании Questel. На момент проведения исследования FAMPAT содержала сведения о более чем 59 миллионов патентных семейств. При проведении исследования не устанавливались какие-либо географические или временные рамки. При отборе

патентных семейств использовались как классификационные коды, так и ключевые слова. В результате было отобрано свыше 339 тысяч патентных семейств. В качестве основных классификационных признаков использовалось 20 областей применения патентных семейств и 6 основных технологий (функциональных направлений) искусственного интеллекта. Основным признаком дополнительно сопоставлялись подчиненные поля для более детальной классификации. Результаты классификации позволяют оценить интенсивность развития технологий и приложений искусственного интеллекта.

В работе [21] изучена динамика представления заявок на патенты в области аппаратного обеспечения искусственного интеллекта. Оценены доли числа одобренных заявок и длительность их рассмотрения для различных рынков. Классам аппаратного обеспечения и высокотехнологичным компаниям сопоставлены показатели среднего возраста патентов и силы патентов. Обоснованы стратегии патентование я в области аппаратного обеспечения искусственного интеллекта для крупных и средних компаний.

Построен патентный ландшафт для глубокого обучения (Deep Learning DL) [22], рассмотрены аспекты заявок на патенты, связанные с разработкой алгоритмов DL, их применением в приложениях и промышленности, описана динамика подачи и одобрения заявок.

3. Постановка задачи исследования. На сегодняшний день существует общее представление об интеллектуальном капитале, разработаны различные подходы к его измерению на микро- и макроуровне, однако отсутствует однозначное строгое определение интеллектуального капитала и единый подход к его измерению на макроуровне. Разработаны методы патентной аналитики для анализа технологических трендов. На концептуальном уровне известно, что есть взаимовлияние интеллектуального капитала и технологических трендов, но отсутствуют методические разработки для количественного оценивания такого влияния.

Поясним, для чего нужно отделять информационные технологии от компонентов интеллектуального капитала. В более общей формулировке этот вопрос звучит следующим образом: почему нельзя смешивать технологии, как ресурсы, и другие ресурсы, в том числе используемые для технологического развития.

Существуют два общих свойства ресурсов.

Первое свойство заключается в возможности независимого использовании одного и того же ресурса различными субъектами. Будем называть его разделяемостью ресурса. В отечественной

литературе разделяемые ресурсы обычно называют конкурентными, что, по нашему мнению, плохо отражает смысл этого свойства.

Второе свойство состоит в возможности предотвращения несанкционированного использования ресурса. Его принято называть исключаемостью ресурса.

Разделяемость технологии означает, что использование технологии одним субъектом не препятствует ее использованию другими субъектами. При этом право интеллектуальной собственности обеспечивает свойство исключаемости технологии как ресурса (отметим, что правовые нормы не всегда останавливают несанкционированное копирование технологий). Нельзя говорить, что технологии являются полностью разделяемыми или полностью исключаемыми ресурсами. Копирование технологии требует дополнительных затрат. Нужно учитывать, что стоимость разработки технологии обычно существенно выше, чем копирования. Инфраструктурные и человеческие ресурсы, как элементы интеллектуального капитала, представляют собой неразделяемые ресурсы. Их использование лимитируется имеющимися материальными активами и численностью персонала компании или численностью населения страны (для национального интеллектуального капитала).

Обозначим:

A и X – соответственно стоимость разделяемых и неразделяемых ресурсов, используемых для производства;

$Y=A+X$ – суммарная стоимость ресурсов;

$F(Y)$ – объем производства (производственная функция);

a – параметр масштабирования производства.

При сделанных предположениях $F()$ является однородной функцией первой степени от X, поэтому справедливы соотношения:

$$\text{Если } a > 1, \text{то}$$
$$F(aY) = F\big(a(A+X)\big) > F(A+aX) = aF(A+X) = aF(Y). \quad (1)$$

$$\text{Если } a < 1, \text{то}$$
$$F(aY) = F\big(a(A+X)\big) < F(A+aX) = aF(A+X) = aF(Y). \quad (2)$$

Учитывая, что $F(0) = 0$, при $0 < \lambda < 1$, получаем:

$$F(0(1-\lambda) + \lambda Y) < (1-\lambda)F(0) + \lambda F(Y). \quad (3)$$

Таким образом, мы убедились, что, при сделанных предположениях о свойствах ресурсов и допущении о возможности

мгновенного масштабирования производства, производственная функция не может быть вогнутой на любых интервалах, левая граница которых совпадает с нулем. Выражение (1) показывает, что при тиражировании существующих технологий обеспечивается сверхлинейный рост производства при инвестировании в неразделяемые ресурсы. Инвестирование в развитие технологий окупается только в том случае, если создается новый продукт, на который могут быть установлены цены выше рыночных. Предполагается, что инвестор может выбирать соотношение средств. Потраченных на разделяемые и неразделяемые ресурсы. Однако, при описании процессов технологического развития на уровне стран необходимо учитывать, что соотношение ресурсов может определяться объективно существующими закономерностями технологического развития. Поэтому выявление таких закономерностей представляет собой важную научно-практическую задачу.

Если в (1) и (2) предположить, что X есть функция $G(A)$ и $Y=A+G(A)$, то производственная функция:

$$F(Y) = F(A + G(A)), \tag{4}$$

уже не будет обладать перечисленными свойствами.

Более детальные модели технологического развития, основанные на выделении ресурсов двух рассмотренных типов, представлены в [25].

В настоящее время не существует открытых данных, которые позволили бы выразить стоимость технологий как ресурсов на уровне стран и в явном виде определить функции $G(A)$ и $F(Y)$, но построение количественных оценок взаимосвязи информационных технологий управления и интеллектуального капитала будет шагом в решении такой фундаментальной задачи.

В качестве характеристик развития информационных технологий управления использованы показатели патентования для технологической области «IT-методы управления». Выбор таких показателей обусловлен несколькими причинами:

– традиционным использованием характеристик патентования как результатов результативности исследований и разработок;

– возможностью трактовки показателей как характеристик разделяемых ресурсов;

– открытостью и надежностью патентных данных;

– возможностью тонких настроек запросов к патентным базам данных.

В [26] патентование рассматривалось как деятельность, в результате которой создаются новые инновационные продукты, а не как результат исследований и разработок. Авторами построены линейные регрессии, которые связывают логарифм числа новых инновационных продуктов определенной категории, которые производят компании, с логарифмом числа патентных заявок той же категории, поданных компанией в каком-либо предыдущем году:

$$\log N = \beta \log P_i + \alpha, \quad (5)$$

или:

$$N = \gamma P_i^{\beta}, \quad (6)$$

где N – количество новых инновационных продуктов,

P_i – количество патентных заявок, поданных в год, который был на i годов раньше, чем год появления продукта.

Для всех регрессий, полученных в [26] значение $\beta < 0{,}1$. Другими словами, наблюдается ощутимое замедление роста зависимой переменной при увеличении независимой переменной.

Материалы и методы, использованные в [26] позволили авторам выявить временные лаги – интервалы времени между появлением патентов и их использованием в инновационных продуктах. Фактически установлена причинно-следственная связь между результатами исследований и разработок и выходом на рынок инновационных продуктов.

Перед нами также стоит задача определения регрессионных зависимостей, в которых в качестве независимой переменной используются показатели патентования, а в качестве зависимой переменной – индекс и субиндексы интеллектуального капитала. При этом сложно говорить о явных причинно-следственных связях между патентованием и человеческим и интеллектуальным капиталом, поэтому задача анализа временных лагов не имеет простой интерпретации. Тем не менее, такой анализ позволит дополнительно уточнить взаимное влияние развития информационных технологий управления и интеллектуального капитала.

Цель исследования заключается в количественном оценивании взаимного влияния национального интеллектуального капитала и современных информационных технологий управления на макроуровне.

Для достижения этой цели существующие подходы к измерению интеллектуального капитала нами адаптированы для измерения на макроуровне национального интеллектуального капитала стран на основе открытых данных; определены по открытым

патентным данным основные технологические тренды в области информационных технологий управления с использованием инструментария патентной аналитики; разработана методика измерения интеллектуального капитала и проверены гипотезы о статистической значимости взаимовлияния интеллектуального тала и информационных технологий управления.

4. Материалы и методы исследования

4.1. Методика измерения интеллектуального капитала. При разработке системы показателей для оценивания интеллектуального капитала и инновационной активности использована двухкомпонентная концепция интеллектуального капитала. Интеллектуальный капитал включает: человеческий капитал и структурный капитал, объединяющий организационный капитал и капитал взаимоотношений с клиентами (клиентский капитал). Выбор двухкомпонентной структуры обусловлен тем, что организационный и клиентский капитал объединяют взаимосвязанные и взаимодополняющие элементы, различающиеся в основном, по критерию отнесения к внутренней (структурный) и внешней (клиентский) для организации среде, при переходе к измерению организационного и клиентского капитала они могут быть объединены в структурный капитал на уровне характеризующих их статистических показателей.

Ключевая задача состоит в том, чтобы найти статистические показатели, отражающие интеллектуальный капитал. Прямых официальных показателей, позволяющих количественно оценить интеллектуальный капитал крайне мало. Поэтому мы следовали логике выбора статистических показателей, используемой для построения субиндексов национального интеллектуального капитала [14] и глобального инновационный индекса (ГИИ) [27], а также разработанным нами подходам к оцениванию социально-экономических явлений по гетерогенным данным [28, 29]. Следует отметить, что четких критериев включения того или иного статистического показателя в состав определенного субиндекса нет. Более того, при построении глобального индекса инноваций, состав показателей незначительно меняется из года в год [27] для того, чтобы итоговые субиндексы лучше отражали результаты и условия инновационной деятельности. При индексном подходе к оцениванию интеллектуального капитала различные авторы используют разные исходные наборы статистических показателей, достаточно полная сводка используемых систем статистических показателей приводится в работе [14].

Для обеспечения воспроизводимости оценок национального интеллектуального капитала нами предлагается использовать

нормализованные значения первичных статистических показателей и индикаторов, составляющие основу для вычисления глобального инновационного индекса. Значения этих показателей доступны для загрузки с официального сайта Всемирной организации интеллектуальной собственности по ссылке https://www.wipo.int/publications/en/details.jsp?id=4622, GII 2022 Database. Выбор этих показателей обусловлен тем, что исходные данные о значениях этих показателей уже верифицированы разработчиками отчетов о глобальном инновационном индексе [27]. Предлагаемый содержательный состав показателей, определяющих интеллектуальный капитал, приведен на рисунке 1.

IC – индекс интеллектуального капитала		
	HC – субиндекс человеческого капитала	Доля обучающихся по программам высшего образования от численности возрастной группы, которая соответствует типичному возрасту студента, %
		Доля выпускников по программам высшего образования в области науки и техники от всех выпускников программ высшего образования, %
		Доля иностранных студентов от обучающихся по программам высшего образования, %
		Количество исследователей в пересчете по занятости на полную ставку, чел. на млн. населения
		Валовые расходы на НИОКР, % ВВП
		Глобальные корпоративные инвестиции в НИОКР топ-3 мировых компаний, млн. долл. США
		Средний рейтинг топ-3 университетов по рейнигу QS, баллы
		Наукоемкая занятость (доля занятых на должностях 1–3 категории по Международной классификации занятий (ISCO) от общего числа занятых), %
		Доля фирм, предлагающих официальные программы обучения для своих постоянных сотрудников, работающих полный рабочий день, в выборке обследованных фирм, %
		Доля трудоустроенных женщин с учеными степенями от общего числа трудоустроенных женщин, %
		Доля исследователей в бизнес-секторе от всех исследователей, %
		Цитируемость документов, H-индекс по https://www.scimagojr.com
	SC – субиндекс структурного капитала	Индекс доступа к ИКТ, %
		Индекс использования ИКТ, %
		Индекс развития электронного правительства, доли ед.
		Индекс электронного участия, доли ед.
		Индекс эффективности логистики, ед.
		Венчурные инвесторы, сделок / ВВП по ППС млрд. долл. США
		Получатели венчурного капитала, сделок / ВВП по ППС млрд. долл. США
		Полученный венчурный капитал, стоимость, % ВВП
		Валовые расходы на НИОКР, выполненные коммерческими предприятиями, % ВВП
		Валовые расходы на НИОКР, финансируемые коммерческими предприятиями, % ВВП
		Сотрудничество между университетами и промышленностью в области НИОКР, баллы
		Состояние кластеров, баллы
		Валовые расходы на НИОКР, финансируемые из-за рубежа, % ВВП
		Количество совместных предприятий/стратегических альянсов / ВВП по ППС млрд. долл. США
		Платежи за использование интеллектуальной собственности (импорт), % от общего объема торговли
		Высокотехнологичный импорт, % от общего объема торговли
		Импорт услуг ИКТ, % от общего объема торговли
		Прямые иностранные инвестиции, % ВВП
		Расходы на ПО, % ВВП

Рис. 1. Индекс, субиндексы и показатели для оценки интеллектуального капитала

Из 81 показателя для 132 стран, по которым рассчитывается ГИИ [27] были отобраны те, которые являются наиболее информативными, с нашей точки зрения, для отражения всех аспектов интеллектуального капитала. Таким образом, интеллектуальный капитал на макроуровне (уровне страны) определяется нами через совокупность статистических показателей, использованных для определения его индекса, вычисленного с использованием нормализованных значений 31 статистического показателя.

Значения статистических показателей нормализованы в диапазоне [0, 100], более высокие баллы соответствуют «лучшим» результатам. Субиндексы человеческого (HC) и структурного (SC) капитала определяются как линейная свертка (среднее) нормализованных значений исходных статистических показателей. Иными словами, человеческий и структурный капитал определяется нами, как и интеллектуальный, через совокупность статистических показателей, используемых для вычисления соответствующих индексов. Такой подход широко распространен в мировой практике определения интегральных показателей, например, в методологии расчета глобального инновационного индекса [27]. Подробное описание исходных статистических показателей и источников данных представлены в [27].

В соответствии с методологией построения глобального инновационного индекса (ГИИ) [27] нормализация значений первичных показателей выполняется по следующей схеме. Все показатели нормализованы в диапазоне [0, 100], где более высокие баллы соответствуют лучшим результатам. Нормирование проводилось по методу «минимум-максимум», где значения «минимум» и «максимум» были минимальным и максимальным значениями показателей в выборке. Были применены следующие формулы [27]:

$$w_i = (v_i - v_{min(i)}) / (v_{max(i)} - v_{min(i)})\ 100, \text{ если показатель «хороший»}, \quad (7)$$

$$w_i = (v_{max(i)} - v_i) / (v_{max(i)} - v_{min(i)})\ 100, \text{ если показатель «плохой»}, \quad (8)$$

где w_i – нормализованное значение i-ого показателя;

v_i – исходное значение i-ого показателя;

$v_{min(i)}$ – минимальное значение i-ого показателя;

$v_{max(i)}$ – максимальное значение i-ого показателя.

Показатель считается «хорошим», если увеличение его значений вносит положительный вклад в значение субиндекса, в состав которого он входит. В ином случае показатель считается «плохим».

Нормализованные показатели сгруппированы по субиндексам интеллектуального капитала (рисунок 1). Значение каждого субиндекса вычислялось как среднее входящих в его состав нормализованных показателей:

$$HC = \sum_{i=1}^{12} w_i^{HC}/12, \quad (9)$$

$$SC = \sum_{i=1}^{19} w_i^{SC}/19, \quad (10)$$

HC (Human Capital) – субиндекс человеческого капитала;

w_i^{HC} – нормализованные значения показателей, составляющих субиндекс человеческого капитала;

SC (Structure Capital) – субиндекс структурного капитала;

w_i^{SC} – нормализованные значения показателей, составляющих субиндекс структурного капитала;

Индекс интеллектуального капитала (*IC – Intellectual Capital*) определяется по формуле:

$$IC = (HC + SC)/2. \quad (11)$$

Предлагаемый формальный подход к определению понятий интеллектуального, человеческого и структурного капитала через совокупность статистических показателей, используемых для построения соответствующих индекса и субиндексов (выражения (9)-(11)), апробирован нами при оценивании взаимосвязи уровня развития компонентов интеллектуального капитала и инновационной активности на макроуровне [30].

4.2. Анализ уровня развития информационных технологий управления. Для оценки уровня развития информационных технологий управления использовано одно их ведущих платформенных решений Orbit Intelligence [31], в частности, база патентов FAMPAT и программное обеспечение для патентных исследований и анализа.

Временная глубина поиска – с 2003 года по настоящее время (на 31.03.2023). В качестве единицы наблюдения рассматривается патентное семейство, то есть все патенты, описывающие одно изобретение. Проанализированы данные только о действующих патентах и заявках в стадии рассмотрения. Географические рамки патентования не устанавливались.

Для построения диаграмм использованы средства визуализации QUESTEL – ORBIT. Часть диаграмм построена авторами с

использованием аналитических данных, полученных из системы QUESTEL – ORBIT.

Мы проанализировали данные о поданных заявках и зарегистрированных патентах для технологической области «IT-методы управления» (Technology domain «IT Methods for Management») и технологической области «Компьютерные технологии» (Computer Technology). Использовано доступное в Orbit Intelligence [31, 32] выделение технологических областей, которое основано на группировке классов и подклассов Международной патентной классификации (МПК). Всего выделяют 35 технологических областей, которые объединены в группы: Химия, Электротехника, Приборы, Машиностроение и Другие. Исследованные в работе технологические области входят в группу Электротехника, в которую включены: аудиовизуальные технологии; основные коммуникационные процессы; компьютерные технологии; цифровая связь; электрические машины, аппараты, энергетика; ИТ-методы управления; полупроводники; телекоммуникации.

Перспективные направления исследования в анализируемых технологических областях определялись:

– по соотношению действующих патентов и заявок на стадии рассмотрения (Technology domain «IT Methods for Management», Status Alive, Granted / Pending);

– по приросту по годам количества заявок в стадии рассмотрения (pending).

Динамика патентной активности, также свидетельствующая об интересе к технологической области и ее перспективности, оценивалась по количеству патентных семейств на 1-й год подачи заявки.

Кроме того, проведен анализ распределения патентных семейств технологической области по основным концепциям и по смежным технологическим областям, наиболее часто встречающимся в патентах.

Мировые лидеры в анализируемой технологической области определены по количеству действующих патентных семейств, опубликованных в патентном офисе страны. Экспансия на рынки, свидетельствующая о востребованности технологии, оценивалась по количеству действующих патентных семейств у правообладателей в различных патентных офисах стран. Распространённость технологии, то есть экспансия мировых лидеров в предметные области, оценивалась по количество действующих патентных семейств у правообладателей по областям применения.

4.3. Выявление взаимовлияния уровня развития IT-методов управления и национального интеллектуального капитала. Для выявления взаимовлияния уровня развития IT-методов управления и

национального интеллектуального капитала проанализировано распределение действующих патентных семейств для технологической области «IT-методы управления» по странам защиты (странам, в которых изобретения в области «IT-методы управления» защищены патентом). Выборка стран для определения зависимости была построена следующим образом. Определен топ-30 патентных офисов стран, из него исключены Европейский патентный офис (EP), патентный офис Всемирной организации интеллектуальной собственности (WO), а также патентные офисы вошедших в топ-30 европейских стран, так как многие патентообладатели, зарегистрированные в этих странах, не регистрируют заявки, поданные в Европейский патентный офис (EP) и в патентный офис Всемирной организации интеллектуальной собственности (WO), в национальных патентных офисах. Для оставшихся 15 стран определен индекс патентной активности в области «IT-методы управления» как отношение количества действующих патентных семейств в этой области к объему ВВП, выраженному в долларах США по паритету покупательной способности. Аналогичное нормирование общего количества патентных семейств используется в методологии построения составляющих глобального инновационного индекса [27].

Далее были построены и проанализированы парные регрессии между значениями индекса интеллектуального капитала и индекса патентной активности в технологической области «IT-методы управления».

Оценка временных лагов в зависимости индекса интеллектуального капитала от уровня развития информационных технологий управления проведена по данным за 2017–2021 годы о количестве действующих патентов и заявок, для которых наблюдаемый год является первым годом подачи заявки (1st application year). Подход к построению выборки стран был аналогичен описанному выше. Использован корреляционно-регрессионный анализ.

При проведении статистического анализа оценивалась статистическая значимость параметров регрессии и коэффициентов корреляции с использованием встроенных средств открытой статистической платформы Jamovi, версия 2.3.18.0 [34].

5. Результаты

5.1. Перспективность развития технологий в области IT-методов управления. Соотношение патентных заявок, находящихся в стадии рассмотрения, и одобренных заявок характеризует интенсивность патентования. Интенсивность патентования в технологической области косвенно характеризует перспективы

развития новых технологий в этой области (таблица 1). Для понимания представленных в таблице данных нужно учитывать следующие особенности подсчета заявок. Учитываются не отдельные патентные заявки, а патентные семейства. Каждое действующее патентное семейство (Alive) может быть представлено как заявками, находящимися в стадии рассмотрения, так и уже одобренными заявками. Семейства со статусом «одобренные» обязательно включает одобренные заявки. В семействах со статусом «в стадии рассмотрения» одобренные заявки отсутствуют. Мы сравнили технологическую область «IT-методы управления» с более широкой технологической областью «компьютерные технологии», при этом существуют патентные семейства, принадлежащие обеим областям одновременно. Анализ таблицы свидетельствует о том, что развитие IT методов управления более востребовано или/и эта область настоящее время обладает большим потенциалом для развития.

Таблица 1. Соотношение поданных и одобренных патентных заявок (только действующие патенты по двум технологическим областям «IT methods for management» и «Computer technology», построено по данным [31]), количество патентных семейств

Статус	IT-методы управления	Компьютерные технологии
Всего действующих (alive) патентных семейств	619 253	2 257 838
из них		
одобренные	294 971 (48%)	1 413 155 (63%)
в стадии рассмотрения	324 282 (52%)	844 683 (37%)
Семейства, в которых есть заявки в стадии рассмотрения	369 091	1 044 484
из них семейства, в которых есть одобренные заявки	44 809 (12%)	199 801 (19%)

При анализе динамики патентной активности в технологической области «IT-методы управления» использованные данные сгруппированы по году подачи первой заявки в патентном семействе (рисунок 2). В этом отличие от данных таблицы 1, в которой учитываются все действующие патентные семейства. Анализ соотношения патентных семейств, находящихся в стадии рассмотрения и патентных семейств с одобренными заявками в динамике за 20 лет с 2003 по 2023 год показал, что в 2019 году количество патентных семейств на рассмотрении впервые превысило количество одобренных патентных семейств. Это произошло в

результате сочетания двух факторов – возрастания патентный активности и продолжительного времени рассмотрения заявок. Сокращение количества одобренных патентных семейств в 2019 году вызвано тем, что для многих заявок время их рассмотрения превышает четыре года. Сокращение патентных семейств на рассмотрении в 2022 году объясняется тем, что ещё не все заявки включены в базу.

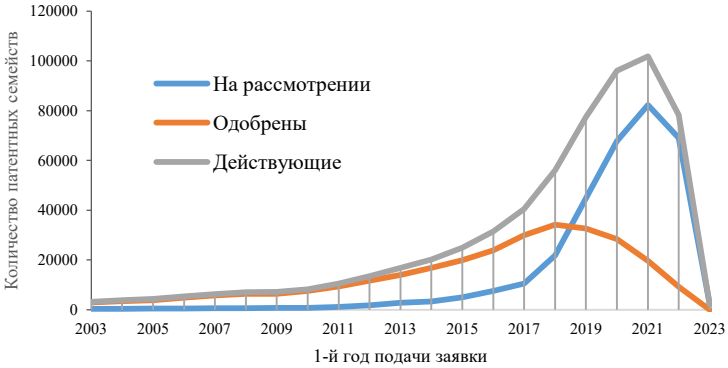


Рис. 2. Динамика патентной активности для технологической области «IT methods for management»: распределение количества патентных семейств по первому году подачи заявки, построено по данным [31]

5.2. Концепции и смежные области для технологической области IT-методы управления. Для определения основных концепций, используемых в патентных семействах технологической области «IT-методы управления», применен сервис Questel-Orbit, позволяющий построить кластеры совместно о употребляемых, взаимосвязанных по смысловой нагрузке, ключевых слов (рисунок 3). Концепция представляет тематику, характеризующую кластер. Некоторые концепции наиболее распространены, например – сбор данных (Data Acquisition), большие данные (Big Data), блокчейн (Block Chein). Еще один сервис Questel-Orbit позволил определить численность патентных семейств, одновременно принадлежащих технологической области «IT-методы управления» (619 253 патентных семейства) и остальным 34 патентным областям (рисунок 4).

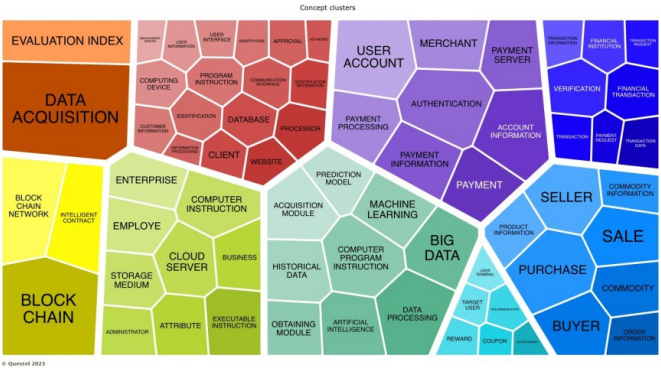


Рис. 3. Основные концепции для технологической области «IT methods for management»: распределение патентных семейств по тематическим областям, наиболее часто встречающимся в патентах, построено по данным [31]

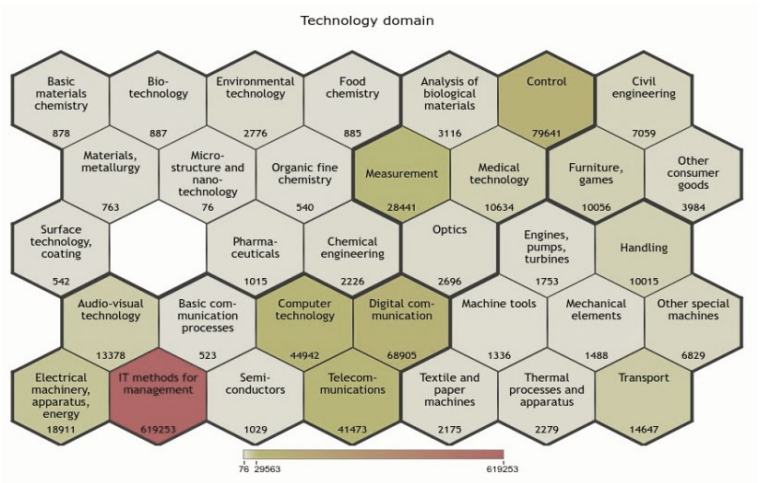


Рис. 4. Смежные технологические области для патентных семейств из технологической области «IT methods for management», построено по данным [31], количество действующих патентных семейств

С технологической областью «высокомолекулярная химия, полимеры» пересечений нет (белое поле). Рисунок позволяет оценить степень взаимосвязи IT-методов управления с технологиями и приложениями других технологических областей. Наиболее распространенным является сочетание технологической области «IT-методы управления» с областями: автоматическое управление

(control), цифровые коммуникации (digital communication), компьютерные технологии (computer technology), телекоммуникации (telecommunication) и метрология (measurement).

5.3. Страны и компании – лидеры в технологической области IT-методы управления. При определении стран-лидеров по действующим патентном семействам технологической области «IT-методы управления», мы исключили из списка европейские страны, находящиеся в юрисдикции европейского патентного офиса (EP) (рисунок 5). Также представлены данные о количестве патентных семейств, зарегистрированных в патентном офисе Всемирной организации интеллектуальной собственности (WO). Всего на дату исследования выявлено 619 253 действующих патентов в этой области. Китай является лидером как страна публикации патентов. Китайский офис аккумулирует 54% патентов, США – 24%, Япония и Корея – по 15%. В офисах WO и EP 14% и 8% соответственно. В России зарегистрировано менее 1% всех действующих патентов этой технологической области. Следует отметить, что суммарное количество патентов по всем патентным офисам больше общего числа патентов в полтора раза, так как часть патентов зарегистрированы одновременно в нескольких патентных офисах.

Рис. 5. Мировые лидеры (топ-15) по количеству действующих опубликованных в патентном офисе страны патентных семейств для технологической области «IT methods for management», построено по данным [31]

Широко известен тот факт, что и по всей совокупности патентов Китай является мировым лидером. В то же время надо учитывать, что Китай публикуют меньше патентов в других странах, чем другие страны в патентном офисе Китая (рисунок 6). Это свидетельствует о важности рынка Китая для мировой экономики знаний.

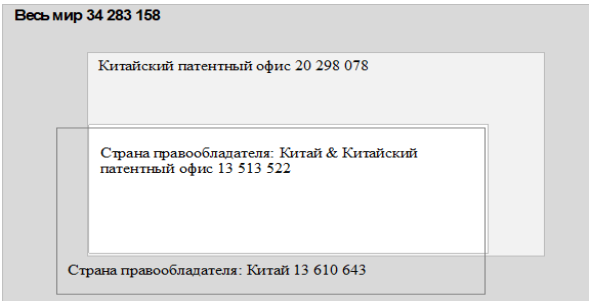


Рис. 6. Соотношение числа опубликованных патентов в мире, Китайском патентном офисе, патентов Китайских правообладателей, по данным [31]

Наблюдается экспансия топ-20 компаний-правообладателей патентных семейств в технологической области «IT-методы управления» в различные предметные области (области применения), прежде всего, средства для хранения, базы данных, транзакции (рисунок 7).

	СРЕДСТВА ДЛЯ ХРАНЕНИЯ	БАЗА ДАННЫХ	ТРАНЗАКЦИИ	СМАРТФОН	ОПЛАТА	ТЕРМИНАЛ	БЛОКЧЕЙН	ПРОДАЖИ	ИНФОРМАЦИЯ О ТРАНЗАКЦИИ	ПЛАТЕЖНАЯ ИНФОРМАЦИЯ
SGCC - STATE GRID CORPORATION OF CHINA	1696	639	259	3	53	54	147	12	56	19
BANK OF CHINA	2803	354	954	5	282	131	570	87	370	74
IBM	941	689	418	281	126	20	257	69	132	21
TENCENT TECHNOLOGY SHENZHEN	2639	319	341	95	290	256	712	204	183	105
MICROSOFT TECHNOLOGY LICENSING	835	600	207	580	132	26	21	84	47	33
ALIBABA	774	312	269	62	194	133	112	296	94	74
HITACHI	333	610	192	151	114	230	39	22	54	25
INDUSTRY & COMMERCIAL BANK CHINA	1768	245	563	9	169	56	234	71	269	63
NEC	1154	427	111	366	217	302	38	19	32	89
CHINA CONSTRUCTION BANK	1583	345	398	0	140	48	54	67	191	40
GOOGLE	743	511	227	706	153	23	1	197	42	116
ADVANCED NEW TECHNOLOGIES	1076	241	703	247	375	100	563	226	219	104
STATE GRID CORPORATION OF CHINA	337	143	78	0	12	9	55	2	14	2
YAHOO JAPAN	463	308	163	841	150	715	3	45	24	81
SAMSUNG ELECTRONICS	388	422	121	689	278	238	26	82	63	219
TOYOTA MOTOR	737	431	40	626	140	543	18	19	16	71
FUJITSU	965	530	141	241	103	215	64	13	61	33
CHINA ELECTRIC POWER RESEARCH INSTITUTE	377	107	97	1	2	2	21	4	18	0
AMAZON TECHNOLOGIES	460	278	242	222	134	3	2	313	45	126
GUANGDONG POWER GRID	893	171	30	1	3	22	20	2	9	4

Рис. 7. Экспансия правообладателей в родственные предметные области, по данным [31], количество действующих патентных семейств

Данные для топ-20 компаний-правообладателей патентных семейств в технологической области «IT-методы управления» характеризует ориентацию этих компаний на рынки Китая, Соединённых Штатов, Японии, Кореи, европейских стран, Индии и ряда других стран (рисунок 8).

	КНР	США	Япония	Корея	WO	EP	Индия	Тайвань	Канада	Австралия	Бразилия	Сингапур	Мексика	Россия
SGCC - STATE GRID CORPORATION OF CHINA	9668	43	3	4	100	4	1	0	1	8	1	0	0	0
BANK OF CHINA	4146	0	0	0	0	0	0	0	0	0	0	0	0	0
IBM	638	4085	381	127	461	120	55	157	102	70	18	11	9	2
TENCENT TECHNOLOGY SHENZHEN	3674	602	150	115	605	102	69	62	18	6	20	39	12	21
MICROSOFT TECHNOLOGY LICENSING	1770	3595	786	799	2249	1796	1055	357	407	364	440	134	318	430
ALIBABA HOLDING	2426	471	263	49	976	179	37	810	2	4	3	46	1	6
HITACHI	387	803	2662	52	774	298	124	44	13	36	14	52	3	0
INDUSTRY & COMMERCIAL BANK CHINA	2704	0	0	0	0	0	0	0	0	0	0	0	0	0
NEC	204	1144	2275	27	1611	237	57	40	5	12	10	34	4	5
CHINA CONSTRUCTION BANK	2602	0	0	0	2	0	0	1	0	0	0	0	0	0
GOOGLE	1039	2423	557	590	1526	1062	504	19	361	399	144	7	10	13
ADVANCED NEW TECHNOLOGIES	2467	921	396	377	940	633	442	730	153	170	80	716	78	80
STATE GRID CORPORATION OF CHINA	2484	11	1	1	23	0	0	0	0	4	0	0	0	0
YAHOO JAPAN	2	194	2412	2	8	2	2	10	0	0	0	0	0	0
SAMSUNG ELECTRONICS	839	1783	195	1860	1223	997	552	30	44	121	53	25	23	69
TOYOTA MOTOR	1592	1783	2170	121	51	224	90	9	17	6	77	17	4	52
FUJITSU	224	869	2228	57	251	326	3	11	5	2	0	18	2	2
CHINA ELECTRIC POWER RESEARCH INSTITUTE	2238	15	0	0	42	1	1	0	0	2	0	0	0	0
AMAZON TECHNOLOGIES	179	1926	185	35	346	217	121	0	117	35	9	30	4	6
GUANGDONG POWER GRID	1957	0	0	0	0	0	0	0	0	0	0	0	0	0

Рис. 8. Экспансия на рынки: распределение правообладателей по офисам стран подачи заявок и регистрации патентов для технологической области «IT methods for management», по данным [31], количество действующих семейств

5.4. Взаимосвязь между национальным интеллектуальным капиталом и распространением в стране IT-методов управления. Рисунок 9 иллюстрирует справедливость высказанной нами гипотезы о возможности количественного подтверждения взаимосвязи между национальным интеллектуальным капиталом, и распространением в

стране IT-методов управления. Статистически значимая регрессионная зависимость выявлена нами для группы из 15 стран, входящих в топ стран по количеству действующих опубликованных в патентном офисе страны патентных семейств в технологической области «IT-методы управления» («IT methods for management»).

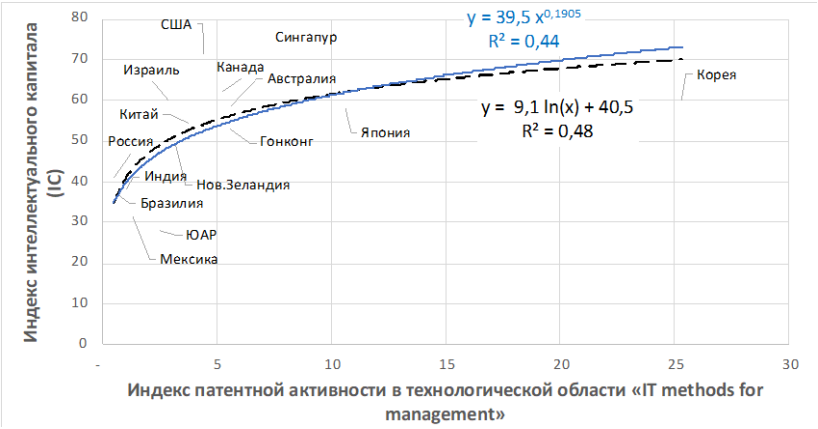


Рис. 9. Положительная взаимосвязь между интеллектуальным капиталом и патентной активностью. Размер пузырька пропорционален ВВП на душу населения в долларах США по паритету покупательной способности. Синим цветом выделены страны с высоким уровнем дохода по классификации Всемирного банка, зеленым – выше среднего, коричневым – ниже среднего

Взаимосвязи интеллектуального капитала и его элемента – человеческого капитала – от индекса патентной активности могут быть аппроксимированы зависимостями (при оценивании статистической значимости параметров регрессии и коэффициента корреляции получены p-value<0,01):

$$IC = 9{,}1\ ln(x) + 40{,}5;\ R^2 = 0{,}475, \quad (12)$$

$$IC = 39{,}5\ x^{0{,}1905};\ R^2 = 0{,}442, \quad (13)$$

где IC – индекс интеллектуального капитала, x – индекс патентной активности, R^2 – коэффициент детерминации;

$$HC = 11{,}5\ ln(x) + 36{,}8;\ R^2 = 0{,}523, \quad (14)$$

$$HC = 35{,}479x^{0{,}244};\ R^2 = 0{,}518, \quad (15)$$

где *HC* – индекс человеческого капитала, *x* – индекс патентной активности, R^2 – коэффициент детерминации.

Логарифмические регрессии (12) и (14) дают корректную интерпретацию для коэффициента детерминации как долю объясненной дисперсии зависимой переменной. Выражения (13) и (15) аналогичны полученным в [26]. Для выражений (13) и (15) значение степени при *x* может быть интерпретировано как эластичность индекса человеческого капитала по индексу патентной активности. Эластичность рассчитывается как относительное изменение зависимой переменной на единицу относительного изменения независимой переменной. Иными словами, при увеличении индекса патентной активности в 10 раз индекс человеческого капитала изменится в 10*0,244=2,44 раза.

Для рассмотренной группы стран максимальное значение *x* – индекса патентной активности в 48 раз больше минимального, а для индексов интеллектуально и человеческого капитала всего в 2,5 и 3,8 раза соответственно. Коэффициенты детерминации моделей (1) и (2) R^2 свидетельствуют, что около 50% дисперсии значений зависимых переменных объясняются зависимостью от x.

Более того, чем более развита экономика (ВВП на душу населения в долларах США по паритету покупательной способности), тем выше в ней уровень человеческого и интеллектуального капитала и выше уровень распространения IT-методов управления, и наоборот. Линия регрессии на рисунке 9 иллюстрирует эту довольно предсказуемую взаимосвязь между интеллектуальным капиталом и развитием.

Тем не менее, некоторые экономики не вписываются в эту модель. Они функционируют выше или ниже прогнозируемых моделью значений. На рисунке синим цветом выделены страны, с высоким уровнем дохода по классификации Всемирного банка. Именно эти страны, а также Китай, который относится к странам с доходом выше среднего уровня, демонстрируют более высокие взаимосвязанные значения индекса интеллектуального капитала и распространенности IT-методов управления. Страны с доходом выше среднего уровня, в которых достаточно широко распространены IT-методы управления демонстрируют более низкие значения индекса интеллектуального капитала, чем страны с высокими доходами. Интересен феномен экономики Индии, которая занимает 3-е место среди стран с уровнем дохода ниже среднего и имеет соизмеримые показатели развития интеллектуального капитала и распространения IT-методов управления со странами с уровнем дохода выше среднего.

5.5. Исследование лагов в зависимости национального интеллектуального капитала и распространения в стране IT-методов

управления. Для выявления лагов в зависимости национального интеллектуального капитала от патентной активности в области IT-методов управления проанализированы зависимости индекса интеллектуального капитала, определенного по данным за 2021 год для стран, от логарифма количества защищённых в стране действующих патентных семейств, для которых первая заявка была подана в каждый из годов 2017–2021. Выявлены значимые корреляции между логарифмами количества действующих патентных семейств для всех анализируемых годов первой подачи. Это является количественным подтверждением того факта, что страны – лидеры патентной активности сохраняют эту активность в течение достаточно долгого периода (рисунок 10). Для 2017 и 2018 годов выявлены статистически значимые корреляции между индексом интеллектуального капитала и логарифмом количества патентных семейств, а для 2019, 2020 и 2021 годов корреляции не значимы (строка 1 рисунок 10). Этот факт нельзя интерпретировать как свидетельство существования временных лагов, поскольку он может быть следствием меньшего объема выборки в 2019–2021 годах.

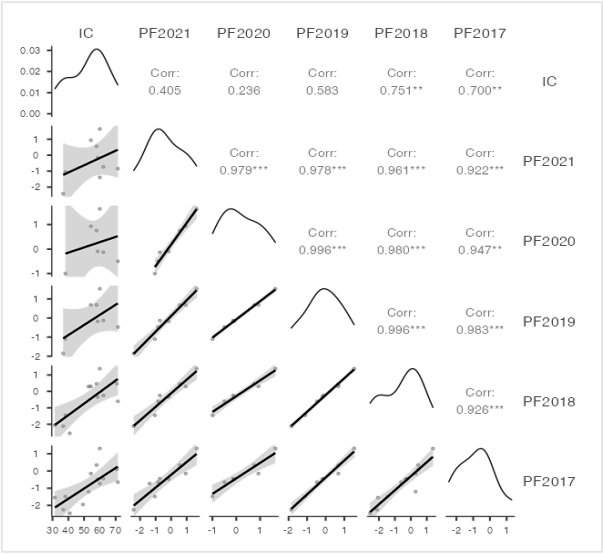


Рис. 10. Взаимосвязи между индексом интеллектуального капитала и патентной активностью: IC – индекс интеллектуального капитала за 2021 год, PF2017-PF2021 – логарифмы количества действующих патентных семейств, защищённых в стране, для которых первая заявка была подана в соответствующем году. Статистическая значимость: * p-value<0,05; ** p-value<0,01; *** p-value<0,001. Выполнено с использованием [33]

Таким образом, подтвердить или опровергнуть гипотезу о существовании временных лагов во влиянии патентной активности на интеллектуальный капитал не представляется возможным. Как было показано выше, наиболее информативным для анализа взаимовлияния является кумулятивный показатель патентной активности страны. Установлены статистически значимые регрессионные зависимости индекса интеллектуального капитала от логарифма количества действующих патентных семейств, для которых подача заявки была в 2017 и 2018 годах. Результаты регрессионного анализа представлены на рисунке 11. Соответствующие уравнения регрессии имеют вид:

$$IC = 8{,}2\ ln(x_{(2017)}) + 60;\ R^2 = 0{,}49, \quad (16)$$

$$IC = 8{,}0\ ln(x_{(2018)}) + 57;\ R^2 = 0{,}56. \quad (17)$$

Model Fit Measures

			Overall Model Test			
Model	R	R^2	F	df1	df2	p
1	0.69970	0.48957	11.510	1	12	0.00534

Model Coefficients - IC

			95% Confidence Interval				
Predictor	Estimate	SE	Lower	Upper	t	p	Stand. Estimate
Intercept	59.9911	3.1762	53.0706	66.912	18.8874	< .00001	
PF2017	8.2010	2.4173	2.9341	13.468	3.3926	0.00534	0.69970

а)

Model Fit Measures

			Overall Model Test			
Model	R	R^2	F	df1	df2	p
1	0.75060	0.56340	12.904	1	10	0.00491

Model Coefficients - IC

			95% Confidence Interval				
Predictor	Estimate	SE	Lower	Upper	t	p	Stand. Estimate
Intercept	57.2590	2.9123	50.7699	63.748	19.6609	< .00001	
PF2018	8.0200	2.2326	3.0455	12.994	3.5922	0.00491	0.75060

б)

Рис. 11. Параметры регрессионных зависимостей между индексом интеллектуального капитала и логарифмом количества действующих патентных семейств, защищённых в стране, для которых первая заявка была подана в: а) 2017; б) 2018 годах. Выполнено с использованием [33]

6. Заключение. Рассмотрены математические основания разделения компонентов интеллектуального капитала и технологий. На концептуальном уровне известно, что существует взаимовлияние интеллектуального капитала и технологических трендов. На сегодняшний день существует множество разработок по количественному оцениванию интеллектуального капитала с использованием двух-, трех-, пятикомпонентной модели его составляющих на микро- и макроуровне. Разработаны методы патентной аналитики для анализа технологических трендов. Тем не менее тема количественного оценивания взаимовлияния интеллектуального капитала и технологических трендов остается открытой для дальнейших научных изысканий, так как разработанные ранее методы и модели измерения и оценки интеллектуального капитала оказываются плохо применимыми для оценивания тенденций последнего десятилетия, отмеченного интенсивным развитием новых инфокоммуникационных и цифровых технологий.

В процессе исследования возможностей количественного оценивания взаимного влияния на макроуровне национального интеллектуального капитала и современных информационных технологий управления нами адаптированы существующие подходы к измерению интеллектуального капитала для измерения его на макроуровне с использованием открытых данных; определены по открытым патентным данным основные технологические тренды в области информационных технологий управления с использованием инструментария патентной аналитики; предложены статистические показатели, методика оценивания и проверены гипотезы о статистической значимости взаимовлияния интеллектуального капитала и информационных технологий управления.

На момент исследования в базе данных FAMPAT компании Questel, предоставляющей одно их ведущих платформенных решений Orbit Intelligence для патентной аналитики, содержалось 619 253 записей о действующих патентах и заявках в стадии рассмотрения для технологического сегмента «IT-методы управления» и 2 257 838 – для технологического сегмента «Компьютерные технологии». Сравнение этих областей по соотношению числа действующих патентов и заявок на рассмотрении позволило сделать вывод, что развитие IT-методов управления более востребовано, или/и эта область в настоящее время обладает большим потенциалом для развития.

В 2019 году количество патентных семейств на рассмотрении впервые с 2003 года превысило количество одобренных патентных семейств. Это произошло в результате сочетания двух факторов –

возрастания патентный активности и увеличения времени рассмотрения заявок.

Китай является лидером как страна публикации патентов. Из 619 253 действующих патентов в области «IT-методы управления» Китайский офис аккумулирует 54% патентов, США – 24%, Япония и Корея – по 15%. В офисах WO и EP 14% и 8% соответственно. В России зарегистрировано менее 1% всех действующих патентов этой технологической области. Суммарное количество патентов по всем патентным офисам больше общего числа патентов в полтора раза, так как часть патентов зарегистрированы одновременно в нескольких патентных офисах.

В то же время, широко известный факт, что по совокупности патентов Китай является мировым лидером, подтвержден нами и дополнен выводом о том, что Китай публикуют меньше патентов в других странах, чем другие страны в патентном офисе Китая. Это свидетельствует о важности рынка Китая для мировой экономики знаний. Установлена нацеленность топ-20 компаний-правообладателей патентных семейств в технологической области «IT-методы управления» на рынки Китая, Соединённых Штатов, Японии, Кореи, европейских стран, Индии и ряда других стран.

Для технологической области «IT-методы управления» характерна следующая содержательная структура. Наиболее распространенными концепциями, являются концепции: обработка данных (data processing), бизнес (business), идентификация (identification), товары (commodity), перспективным направлением развития технологий является построение прогнозных моделей (prediction model).

Наиболее распространенные сочетания технологической области «IT-методы управления» с другими технологическими областями: автоматическое управление (control), цифровые коммуникации (digital communication), компьютерные технологии (computer technology), телекоммуникации (telecommunication) и метрология (measurement).

В процессе исследования подтверждена справедливость высказанной нами гипотезы о возможности установления количественной взаимосвязи между национальным интеллектуальным капиталом, и распространением в стране IT-методов управления. Статистически значимая регрессионная зависимость выявлена для группы из 15 стран, входящих в топ стран по количеству действующих опубликованных в патентном офисе страны патентных семейств в технологической области «IT-методы управления» («IT methods for

management»). Регрессионная зависимость достаточно хорошо аппроксимируется линейной регрессией индекса интеллектуального капитала от логарифма индекса патентной активности страны в области IT-методов управления, что может быть интерпретировано как замедление роста индекса интеллектуального капитала при достижении определенного уровня патентной активности.

Установлено, что чем более развита экономика, тем выше в ней уровень интеллектуального капитала и выше уровень распространения IT-методов управления. Явными исключениями из этой закономерности являются Китай и Индия. Китай, который относится к странам с доходом выше среднего уровня, демонстрируют более высокие, чем страны его уровня экономического развития, взаимосвязанные значения индекса интеллектуального капитала и распространенности IT-методов управления. Индия, занимающая 3-е место среди стран с уровнем дохода ниже среднего, имеет соизмеримые показатели развития интеллектуального капитала и распространения IT-методов управления со странами с уровнем дохода выше среднего.

Дальнейшие направления исследования могут быть связаны с проверкой гипотез о возможности выявления предложенным методом количественных зависимостей между интеллектуальным капиталом и технологическим развитием. С этой целью, во-первых, необходима детализация выявленных зависимостей по кодам МПК и составляющим интеллектуального капитала, во-вторых, выявление зависимостей для других технологических областей.

Литература

1. Edvinsson L., Malone M.S. Intellectual capital: Realizing your company's true value by finding its hidden brainpower // New York: Harper Collins. 1997. 240 p.
2. Roos G., Roos J., Edvinsson L., Dragonetti N.C. Intellectual capital – Navigating in the new business landscape // New York University Press. 1997. 208 p.
3. Bontis N. Intellectual capital: An exploratory study that develops measures and models // Management Decision. 1998. vol. 36(2). pp. 63–76.
4. Petty R., Guthrie J. Intellectual capital literature review: Measurement, reporting and management // Journal of Intellectual Capital. 2000. vol. 1(2). pp. 155–176.
5. Mahmood T., Mubarik M. Balancing innovation and exploitation in the fourth industrial revolution: Role of intellectual capital and technology absorptive capacity // Technological Forecasting and Social Change. 2020. vol. 160. no. 120248.
6. Nunamaker J.F., Romano N.C., Briggs R.O. Increasing Intellectual Bandwidth: Generating Value from Intellectual Capital with Information Technology // Group Decision and Negotiation. 2002. vol. 11. pp. 69–86.
7. Edvinsson L. IC 21: reflections from 21 years of IC practice and theory // Journal of Intellectual Capital. 2013. vol. 14. no. 1. pp. 163–172.

8. Bontis N. Assessing knowledge assets: A review of the models used to measure intellectual capital // International Journal of Management Reviews. 2001. vol. 3(1). pp. 41–60.
9. Miller M., DuPont B.D., Fera V., Jeffrey R., Mahon B., Payer B.M., Starr A. Measuring and reporting intellectual capital from a diverse Canadian industry perspective: Experience, issues and prospects // International Symposium Measuring and Reporting Intellectual Capital: Experience, Issues, and Prospects, Amsterdam. 1999. pp. 9–11.
10. Bronzetti G., Sicoli G., Chiucchi M.S., Giuliani M. Intellectual Capital Measurement, Management, and Valuation (Eds.: Chiucchi M.S., Lombardi R., Mancini D.) // Intellectual Capital, Smart Technologies and Digitalization Emerging Issues and Opportunities. 2021. pp. 21–32.
11. Xu J., Shang Y., Yu W., Liu F. Intellectual Capital, Technological Innovation and Firm Performance: Evidence from China's Manufacturing Sector // Sustainability. 2019. vol. 11(19). no. 5328.
12. Xu J., Wang B. Intellectual capital, financial performance and companies' sustainable growth: Evidence from the Korean manufacturing industry // Sustainability. 2018. vol. 10(12). no. 4651.
13. Oner M., Aybars A., Cinko M., Avci E. Intellectual Capital, Technological Intensity and Firm Performance: The Case of Emerging Countries // Scientific Annals of Economics and Business. 2021. vol. 68(4). pp. 459–479.
14. Li C.Y.-Y., Edvinsson L. National Intellectual Capital: A Comparison of 40 Countries // Springer Science+Business Media. 2011. 392 p.
15. Bartolini M., Lamboglia R., Lardo A. Intellectual Capital Disclosure and Information Systems, Smart Technologies and Digitalization (Eds.: Chiucchi M.S., Lombardi R., Mancini D.) // Intellectual Capital, Smart Technologies and Digitalization: Emerging Issues and Opportunities. 2021. pp. 47–58.
16. De Santis F., Esposito P. The Impact of Smart Technologies and Digitalization on Intellectual Capital (Eds.: Chiucchi M.S., Lombardi R., Mancini D.) // Intellectual Capital, Smart Technologies and Digitalization. SIDREA Series in Accounting and Business Administration. 2021. pp. 59–71.
17. Secundo G., Del Vecchio P., Dumay J., Passiante G. Intellectual capital in the age of Big Data: establishing a research agenda // Journal of Intellectual Capital. 2017. vol. 18. pp. 242–261.
18. Sokolov B.V., Yusupov R.M. Scientific basis of management and cybernetics methodologies integration // Lecture Notes in Networks and Systems. 2022. vol. 442. pp. 52–59.
19. Gorodetsky V., Yusupov R. Artificial intelligence at present and tomorrow // Journal of Physics: Conference Series. 2021. vol. 1864. no. 012002. pp. 1–11. DOI:10.1088/1742-6596/1864/1/012002.
20. Sokolov B.V., Okhtilev M.Y., Murashov D.A., Krylov A.V., Kofnov O.V., Stepanov P.V., Styskin M.M. Methodology and Technology for Use and Development of Information-Analytic Platform for Complex Object Life Cycle Proactive Control // International Conference Cyber-Physical Systems and Control. 2023. pp. 467–474.
21. Artificial Intelligence. Technology Trends 2019 // WIPO. 2019. 158 p. Available at: https://www.wipo.int/tech_trends/en/artificial_intelligence/. (accessed 30.03.2023).
22. Deep Learning 2021. Patent Landscape // Questel. 2021. 51 p. Available at: https://www.questel.com/wp-content/uploads/2021/11/2021-Deep-Learning-Patent-Landscape-short-report-.pdf. (accessed 30.03.2023).
23. Technology Trends 2019 Artificial Intelligence. Data collection method and clustering scheme. Background paper. WIPO. 2019. 25 p. Available at:

https://www.wipo.int/export/sites/www/tech_trends/en/docs/techtrends_ai_methodology.pdf. (accessed 30.03.2023).
24. Cunha L., Cunha J.A., Matos F., Thomaz J.F. The Relationship Between Intellectual Capital and Information Technology: Findings Based on a Systematic Review // 7th European Conference on Intellectual Capital (ECIC). 2015. pp. 53–62.
25. Romer P.M. Endogenous Technological Change // Journal of Political Economy. 1990. vol. 98. no. 5. pp. 71–102.
26. Argente D., Baslandze S., Hanley D., Moreira S. Patents to Products: Product Innovation and Firm Dynamics. Working Paper 2020-4 // Federal Reserve Bank of Atlanta. 2020.
27. Global Innovation Index 2022. What is the future of innovation-driven growth? 15th Edition. Editors: Soumitra Dutta, Bruno Lanvin, Lorena Rivera León and Sacha Wunsch-Vincent // WIPO. 2022. 266 p.
28. Verzilin D., Maximova T., Antokhin Y., Sokolova I. Integration of heterogeneous data in monitoring environmental assets // Cybernetics and Algorithms in Intelligent Systems: Proceedings of 7th Computer Science On-line Conference. 2018. vol. 3. pp. 176–185. DOI: 10.1007/978-3-319-91192-2_19.
29. Verzilin D., Maximova T., Skoryk, S., Sokolova I. Linking Remote Sensing Data, Municipal Statistics and Online Population Activity for Environmental Assessments in Urban Agglomerations // Digital Transformation and Global Society: 4th International Conference (DTGS). 2019. pp. 17–28.
30. Maximova T.G., Zhang M. Regression Models of the Relationship Between Innovation Activity and Intellectual Capital. Economics. Law. Innovation. 2023. no. 1. pp. 15–26.
31. Official site QUESTEL – ORBIT. Available at: www.orbit.com. (accessed 30.03.2023).
32. Official site QUESTEL – ORBIT: Technologies. Available at: https://static.orbit.com/orbit/help/1.9.8/en/index.html#!Documents/technologies.htm. (accessed 30.03.2023).
33. The jamovi project (2022). jamovi (Version 2.3) [Computer Software]. Available at: https://www.jamovi.org. (accessed 19.06.2023).

Соколов Борис Владимирович — д-р техн. наук, профессор, заслуженный деятель науки РФ, главный научный сотрудник, руководитель лаборатории, лаборатория информационных технологий в системном анализе и моделировании, Федеральное государственное бюджетное учреждение науки "Санкт-Петербургский Федеральный исследовательский центр Российской академии наук" (СПб ФИЦ РАН). Область научных интересов: фундаментальные и прикладные исследования проблем комплексного моделирования и проактивного управления динамическими системами с перестраиваемой структурой, разработка математических моделей и методов поддержки принятия решений в сложных организационно-технических системах в условиях неопределенности и многокритериальности. Число научных публикаций — 560. sokolov_boris@inbox.ru; 14 линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)328-0103.

Верзилин Дмитрий Николаевич — д-р экон. наук, профессор, ведущий научный сотрудник, лаборатория информационных технологий в системном анализе и моделировании, Федеральное государственное бюджетное учреждение науки "Санкт-Петербургский Федеральный исследовательский центр Российской академии наук" (СПб ФИЦ РАН); заведующий кафедрой, кафедра менеджмента и экономики спорта. Область научных интересов: моделирование процессов управления в сложных организационно-технических системах, моделирование, прогнозирование

и планирование развития социально-экономических систем (с использованием математико-статистического инструментария, методов многокритериального принятия решений), технологии имитационного моделирования. Число научных публикаций — 100. verzilindn@mail.ru; 14 линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)328-0103.

Максимова Татьяна Геннадьевна — д-р экон. наук, профессор, факультет инфокоммуникационных технологий, Университет ИТМО. Область научных интересов: моделирование и прогнозирование социально-экономических процессов и систем, системный анализ, информационные технологии в экономике и социальной сфере, статистический анализ данных, статистика, управление организационными системами, экономика инноваций. Число научных публикаций — 135. maximovatg@gmail.com; Кронверкский пр., 49А, 1971018, Санкт-Петербург, Россия; р.т.: +7(921)346-7239.

Чжан Минь — аспирант, факультет технологического менеджмента и инноваций, Университет ИТМО. Область научных интересов: системный анализ, измерение и исследование человеческого капитала, оценивание инновационной активности высокотехнологичных предприятий. Число научных публикаций — 9. zhangmin.zhm@gmail.com; Кронверкский пр., 49А, 1971018, Санкт-Петербург, Россия; р.т.: +7(964)366-8068.

Поддержка исследований. Исследование выполнено при финансовой поддержке Университета ИТМО, тема НИР № 622150 «Разработка подходов к системному проектированию интеграции вузовской науки и бизнеса (пилотное исследование)». Исследования, выполненные по данной тематике, проводились в рамках бюджетной темы FFZF-2022-0004 «Методология и технологии многокритериального проактивного управления жизненным циклом существующих и перспективных интегрированных государственных и коммерческих информационно-управляющих и телекоммуникационных систем и сетей».

DOI 10.15622/ia.22.5.2

B. SOKOLOV, D. VERZILIN, T. MAXIMOVA, M. ZHANG

MUTUAL INFLUENCE OF INTELLECTUAL CAPITAL AND INFORMATION TECHNOLOGIES OF MANAGEMENT

Sokolov B., Verzilin D., Maksimova T., Zhang M. **Mutual Influence of Intellectual Capital and Information Technologies of Management.**

Abstract. To date, there is a generally accepted idea of intellectual capital, and approaches have been developed to measure it at the micro and macro levels. Methods of patent analytics for the analysis of technological trends have been developed. At the conceptual level, it is known that there is a mutual influence of intellectual capital and technological trends, but there are no methodological developments for quantifying such influence using data from various sources. The purpose of the study was to quantify the mutual influence of national intellectual capital and modern management information technologies at the macro level. The mathematical foundations for the distinction of the components of intellectual capital and technologies were considered. The hypothesis about the statistical significance of the mutual influence of intellectual capital and management information technologies was confirmed. The dependence was approximated by linear regression of the intellectual capital index on the logarithm of the country's patent activity index in the field of IT management methods, which can be interpreted as a slowdown in the growth of the intellectual capital index when a certain level of patent activity is reached. It has been established that the more developed the economy, the higher the level of intellectual capital and the higher level of dissemination of IT management methods. China and India are clear exceptions to this pattern. China, which is an upper-middle-income country, demonstrates higher than the countries of its level of economic development, interconnected values of the index of intellectual capital, and the prevalence of IT-management methods. India, ranked 3rd among lower-middle-income countries, has commensurate rates of development of intellectual capital and the spread of IT-management methods with upper-middle-income countries. Further research may be related to testing hypotheses about quantitative relationships between intellectual capital and technological development via the proposed method. It is necessary to detail the identified dependencies by IPC codes and components of intellectual capital and identify dependencies for other technological areas.

Keywords: intellectual capital, information technologies of management, patent landscapes.

References

1. Edvinsson L., Malone M.S. Intellectual capital: Realizing your company's true value by finding its hidden brainpower. New York: Harper Collins. 1997. 240 p.
2. Roos G., Roos J., Edvinsson L., Dragonetti N.C. Intellectual capital – Navigating in the new business landscape. New York University Press. 1997. 208 p.
3. Bontis N. Intellectual capital: An exploratory study that develops measures and models. Management Decision. 1998. vol. 36(2). pp. 63–76.
4. Petty R., Guthrie J. Intellectual capital literature review: Measurement, reporting and management. Journal of Intellectual Capital. 2000. vol. 1(2). pp. 155–176.
5. Mahmood T., Mubarik M. Balancing innovation and exploitation in the fourth industrial revolution: Role of intellectual capital and technology absorptive capacity. Technological Forecasting and Social Change. 2020. vol. 160. no. 120248.

6. Nunamaker J.F., Romano N.C., Briggs R.O. Increasing Intellectual Bandwidth: Generating Value from Intellectual Capital with Information Technology. Group Decision and Negotiation. 2002. vol. 11. pp. 69–86.
7. Edvinsson L. IC 21: reflections from 21 years of IC practice and theory. Journal of Intellectual Capital. 2013. vol. 14. no. 1. pp. 163–172.
8. Bontis N. Assessing knowledge assets: A review of the models used to measure intellectual capital. International Journal of Management Reviews. 2001. vol. 3(1). pp. 41–60.
9. Miller M., DuPont B.D., Fera V., Jeffrey R., Mahon B., Payer B.M., Starr A. Measuring and reporting intellectual capital from a diverse Canadian industry perspective: Experience, issues and prospects. International Symposium Measuring and Reporting Intellectual Capital: Experience, Issues, and Prospects, Amsterdam. 1999. pp. 9–11.
10. Bronzetti G., Sicoli G., Chiucchi M.S., Giuliani M. Intellectual Capital Measurement, Management, and Valuation (Eds.: Chiucchi M.S., Lombardi R., Mancini D.). Intellectual Capital, Smart Technologies and Digitalization Emerging Issues and Opportunities. 2021. pp. 21–32.
11. Xu J., Shang Y., Yu W., Liu F. Intellectual Capital, Technological Innovation and Firm Performance: Evidence from China's Manufacturing Sector. Sustainability. 2019. vol. 11(19). no. 5328.
12. Xu J., Wang B. Intellectual capital, financial performance and companies' sustainable growth: Evidence from the Korean manufacturing industry. Sustainability. 2018. vol. 10(12). no. 4651.
13. Oner M., Aybars A., Cinko M., Avci E. Intellectual Capital, Technological Intensity and Firm Performance: The Case of Emerging Countries. Scientific Annals of Economics and Business. 2021. vol. 68(4). pp. 459–479.
14. Li C.Y.-Y., Edvinsson L. National Intellectual Capital: A Comparison of 40 Countries. Springer Science+Business Media. 2011. 392 p.
15. Bartolini M., Lamboglia R., Lardo A. Intellectual Capital Disclosure and Information Systems, Smart Technologies and Digitalization (Eds.: Chiucchi M.S., Lombardi R., Mancini D.). Intellectual Capital, Smart Technologies and Digitalization: Emerging Issues and Opportunities. 2021. pp. 47–58.
16. De Santis F., Esposito P. The Impact of Smart Technologies and Digitalization on Intellectual Capital (Eds.: Chiucchi M.S., Lombardi R., Mancini D.). Intellectual Capital, Smart Technologies and Digitalization. SIDREA Series in Accounting and Business Administration. 2021. pp. 59–71.
17. Secundo G., Del Vecchio P., Dumay J., Passiante G. Intellectual capital in the age of Big Data: establishing a research agenda. Journal of Intellectual Capital. 2017. vol. 18. pp. 242–261.
18. Sokolov B.V., Yusupov R.M. Scientific basis of management and cybernetics methodologies integration. Lecture Notes in Networks and Systems. 2022. vol. 442. pp. 52–59.
19. Gorodetsky V., Yusupov R. Artificial intelligence at present and tomorrow. Journal of Physics: Conference Series. 2021. vol. 1864. no. 012002. pp. 1–11. DOI:10.1088/1742-6596/1864/1/012002.
20. Sokolov B.V., Okhtilev M.Y., Murashov D.A., Krylov A.V., Kofnov O.V., Stepanov P.V., Styskin M.M. Methodology and Technology for Use and Development of Information-Analytic Platform for Complex Object Life Cycle Proactive Control. International Conference Cyber-Physical Systems and Control. 2023. pp. 467–474.
21. Artificial Intelligence. Technology Trends 2019. WIPO. 2019. 158 p. Available at: https://www.wipo.int/tech_trends/en/artificial_intelligence/. (accessed 30.03.2023).

22. Deep Learning 2021. Patent Landscape. Questel. 2021. 51 p. Available at: https://www.questel.com/wp-content/uploads/2021/11/2021-Deep-Learning-Patent-Landscape-short-report-.pdf. (accessed 30.03.2023).
23. Technology Trends 2019 Artificial Intelligence. Data collection method and clustering scheme. Background paper. WIPO. 2019. 25 p. Available at: https://www.wipo.int/export/sites/www/tech_trends/en/docs/techtrends_ai_methodology.pdf. (accessed 30.03.2023).
24. Cunha L., Cunha J.A., Matos F., Thomaz J.F. The Relationship Between Intellectual Capital and Information Technology: Findings Based on a Systematic Review. 7th European Conference on Intellectual Capital (ECIC). 2015. pp. 53–62.
25. Romer P.M. Endogenous Technological Change. Journal of Political Economy. 1990. vol. 98. no. 5. pp. 71–102.
26. Argente D., Baslandze S., Hanley D., Moreira S. Patents to Products: Product Innovation and Firm Dynamics. Working Paper 2020-4. Federal Reserve Bank of Atlanta. 2020.
27. Global Innovation Index 2022. What is the future of innovation-driven growth? 15th Edition. Editors: Soumitra Dutta, Bruno Lanvin, Lorena Rivera León and Sacha Wunsch-Vincent. WIPO. 2022. 266 p.
28. Verzilin D., Maximova T., Antokhin Y., Sokolova I. Integration of heterogeneous data in monitoring environmental assets. Cybernetics and Algorithms in Intelligent Systems: Proceedings of 7th Computer Science On-line Conference. 2018. vol. 3. pp. 176–185. DOI: 10.1007/978-3-319-91192-2_19.
29. Verzilin D., Maximova T., Skoryk, S., Sokolova I. Linking Remote Sensing Data, Municipal Statistics and Online Population Activity for Environmental Assessments in Urban Agglomerations. Digital Transformation and Global Society: 4th International Conference (DTGS). 2019. pp. 17–28.
30. Maximova T.G., Zhang M. Regression Models of the Relationship Between Innovation Activity and Intellectual Capital. Economics. Law. Innovation. 2023. no. 1. pp. 15–26.
31. Official site QUESTEL – ORBIT. Available at: www.orbit.com. (accessed 30.03.2023).
32. Official site QUESTEL – ORBIT: Technologies. Available at: https://static.orbit.com/orbit/help/1.9.8/en/index.html#!Documents/technologies.htm. (accessed 30.03.2023).
33. The jamovi project (2022). jamovi (Version 2.3) [Computer Software]. Available at: https://www.jamovi.org. (accessed 19.06.2023).

Sokolov Boris — Ph.D., Dr.Sci., Professor, Honored scientist of the Russian Federation, Chief researcher, head of the laboratory, Laboratory of information technologies in system analysis and modeling, St Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: fundamental and applied research on complex modeling and proactive control of dynamic systems with a reconfigurable structure, development of mathematical models and decision support methods in complex organizational and technical systems under uncertainty and multicriteria. The number of publications — 560. sokolov_boris@inbox.ru; 39, 14 line V.O., 199178, St. Petersburg, Russia; office phone: +7(812)328-0103.

Verzilin Dmitry — Ph.D., Dr.Sci., Professor, Leading researcher, Laboratory of information technologies in system analysis and modeling, St Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS); Head of the department, Department of Management and Sports Economics Lesgaft University. Research interests: modeling of management processes in complex organizational and technical systems, modeling, forecasting

and planning the development of socio-economic systems (using mathematical and statistical tools, methods of multi-criteria decision making), simulation modeling technologies. The number of publications — 100. verzilindn@mail.ru; 39, 14 line V.O., 199178, St. Petersburg, Russia; office phone: +7(812)328-0103.

Maximova Tatyana — Ph.D., Dr.Sci., Professor, Faculty of infocommunication technologies, ITMO University. Research interests: modeling and forecasting of socio-economic processes and systems, system analysis, information technologies in economics and social sphere, statistical data analysis, statistics, management of organizational systems, economics of innovation. The number of publications — 135. maximovatg@gmail.com; 49A, Kronverksky Av., 1971018, St. Petersburg, Russia; office phone: +7(921)346-7239.

Zhang Min — Postgraduate student, Faculty of technology management and innovation, ITMO University. Research interests: system analysis, measurement and study of human capital, evaluation of innovative activity of high-tech enterprises. The number of publications — 9. zhangmin.zhm@gmail.com; 49A, Kronverksky Av., 1971018, St. Petersburg, Russia; office phone: +7(964)366-8068.

Acknowledgements. This research is supported by ITMO University, No. 622150 «Development of approaches to system design for the integration of university science and business (pilot study)». The research described in this paper is partially supported by state research FFZF-2022-0004 "Methodology and technologies for multi-criteria proactive life cycle management of existing and prospective integrated state and commercial information management and telecommunication systems and networks".

DOI 10.15622/ia.22.5.3

M. PELOGEIKO, S. SARTASOV, O. GRANICHIN

ON STOCHASTIC OPTIMIZATION FOR SMARTPHONE CPU ENERGY CONSUMPTION DECREASE

Pelogeiko M., Sartasov S., Granichin O. **On Stochastic Optimization for Smartphone CPU Energy Consumption Decrease.**

Abstract. Extending smartphone working time is an ongoing endeavour becoming more and more important with each passing year. It could be achieved by more advanced hardware or by introducing energy-aware practices to software, and the latter is a more accessible approach. As the CPU is one of the most power-hungry smartphone devices, Dynamic Voltage Frequency Scaling (DVFS) is a technique to adjust CPU frequency to the current computational needs, and different algorithms were already developed, both energy-aware and energy-agnostic kinds. Following our previous work on the subject, we propose a novel DVFS approach to use simultaneous perturbation stochastic approximation (SPSA) with two noisy observations for tracking the optimal frequency and implementing several algorithms based on it. Moreover, we also address an issue of hardware lag between a signal for the CPU to change frequency and its actual update. As Android OS could use a default task scheduler or an energy-aware one, which is capable of taking advantage of heterogeneous mobile CPU architectures such as ARM big.LITTLE, we also explore an integration scheme between the proposed algorithms and OS schedulers. A model-based testing methodology to compare the developed algorithms against existing ones is presented, and a test suite reflecting real-world use case scenarios is outlined. Our experiments show that the SPSA-based algorithm works well with EAS with a simplified integration scheme, showing CPU performance comparable to other energy-aware DVFS algorithms and a decreased energy consumption.

Keywords: Android OS, dynamic voltage frequency scaling, stochastic optimization, SPSA, energy consumption.

1. Introduction. Mobile devices, such as smartphones, tablets, and smartwatches, became an integral part of modern life. Digital services provided by these devices both improve quality of life and form new ways of social interactions. More than 6.3 billion smartphone subscriptions were active, and in 2024 this figure is expected to exceed 7 billion people. The most common operating system (OS) for mobile devices today is Android [1].

As the battery capacity of mobile devices is limited, power consumption optimization becomes an increasingly important task – no one wants to have an important call interrupted because of a discharged battery. This issue could be alleviated by applied software, which is capable of providing energy consumption models and eco-friendly profiles. Then, a boost of device longevity is provided by new hardware technologies like Li-Pol batteries or heterogeneous big.LITTLE CPU architecture. Finally, Android OS contains a power management subsystem which includes three components: energy-aware scheduling (EAS), dynamic voltage frequency scaling (DVFS) governors and

idle state (IS) governors, so improving underlying algorithms improves energy consumption as well.

In essence, the DVFS algorithm analyzes the current state of the smartphone and advises the CPU to switch to a particular frequency, so that the algorithm could meet some optimization criteria. Performance and energy consumption cannot be optimized at the same time, because to save energy one has to set a low frequency, and higher computational capabilities call for higher battery resources. Therefore, every energy-aware DVFS algorithm finds some form of balance by introducing combined optimization criteria. Ideally, applications run as slow as perceivable comfortable to save energy.

A significant part of research is mainly concentrated on DVFS algorithms or better energy models for task scheduling, and there is a reason behind such attention – energy-aware task allocation combined with online CPU performance control could result in considerable energy savings. Simultaneous perturbation stochastic approximation (SPSA) is one of the possible ways to track optimal CPU frequency in terms of both energy consumption and performance. On average, the algorithm will nearly follow the steepest descent direction [2]. SPSA could be considered a random search technique, and it helped in solving various computer science-related tasks [3]. In our previous work, we investigated an SPSA-based DVFS governor using a single noisy observation [4], and while working on par with commonly used algorithms, further experiments confirmed that an approach proposed there, although already usable, was not final. SPSA with two noisy observations is more stable compared to one observation version [5]. Thus, the optimal frequency tracking process converges faster on average.

The main contribution of this paper is a proof of the concept that the energy-aware DVFS algorithm could be built based on SPSA with two noisy observations. Additionally, we formulate a different average risk function which takes into account the *cost of execution* of a program at a particular frequency to save energy. Technical considerations are also investigated, for example, whether is it worth running our new DVFS governor with EAS or Completely Fair Scheduler (CFS), and how to connect it with EAS when needed. We also take into account the notable fact that the CPU frequency change cycle could be considerably longer than the DVFS cycle.

This paper is organized as follows. In Section 2, an overview of the DVFS and EAS alongside the existing algorithms for modern smartphones for those subsystems is given. It also contains a brief overview of stochastic optimization in general, a description of the SPSA approach and a review of the previous work in the field. Section 3 contains a description of the proposed DVFS algorithms. Experimental setup and methodology discussion

are presented in Section 4, while experimental results are analyzed in Section 5. Final remarks are given in Section 6 to conclude this paper.

2. Overview

2.1. DVFS and EAS. CPUs in modern smartphone systems-on-a-chip are always multicore. Generally, this architecture is homogeneous – each core has the same computational capabilities and power profile. However, there is a novel approach for mobile device CPU design reflected in the ARM bid.LITTLE architecture – a heterogeneous CPU. Cores are divided into several clusters, and each core is homogeneous only within its cluster. Therefore it is possible to run computationally non-demanding programs on weaker, but energy efficient (so-called "LITTLE") cores, while more powerful and power-hungry ("big") cores are utilized for prioritized or computationally intensive tasks. A real-world example of such a design is given in Table 1.

Table 1. Xiaomi Redmi Note 8 Pro CPU clusters frequencies

A55			A76		
F (Hz)	I (mA)	I/F (mA/GHz)	F (Hz)	I (mA)	I/F (mA/GHz)
2000000	90.04	45.02	2050000	324.33	158.21
1933000	85.8	44.39	1986000	307.98	155.08
1866000	80.27	43.02	1923000	291.52	151.60
1800000	72.77	40.43	1860000	269.61	144.95
1733000	66.61	38.44	1796000	247.53	137.82
1666000	62.05	37.24	1733000	233.56	134.77
1618000	58.95	36.43	1670000	209.73	125.59
1500000	52.33	34.89	1530000	177.39	115.94
1375000	44.83	32.60	1419000	152.46	107.44
1275000	39.69	31.13	1308000	130.33	99.64
1175000	35.5	30.21	1169000	105.19	89.98
1075000	31.24	29.06	1085000	91.11	83.97
975000	27.86	28.574	1002000	79.53	79.37
875000	25	**28.571**	919000	70.65	76.88
774000	23.5	**30.36**	835000	61.38	73.51
500000	19.55	**39.10**	774000	56.85	73.45

It is important to note for our research that core configuration is available within OS, and operating frequency is set uniformly for the entire cluster, that is, every core within a cluster always works at the same frequency. Different clusters might work at different frequencies at the same time.

DVFS as a technique is a control over CPU operating frequency and voltage at runtime to increase or decrease CPU performance at a cost of power consumption. Generally, CPU power consumption is related to the cube of its frequency, and as a side effect CPU heats. However, cooling mechanisms available to mobile devices are limited both by power usage and form factor, therefore most of the time heat could only be dissipated by surrounding air. Thus therefore, operating frequencies are limited to those producing an amount of heat that could be consistently dissipated – at the time of writing, about 2 GHz for commercially available CPUs.

Although dependency between power consumption and frequency is still vaguely close to linear at these levels, power efficiency – the relation of power to performance – is clearly exponential [6]. Power efficiency could also be interpreted as the cost of instruction execution at a selected frequency. A complimentary optimization criterion is the execution time, so in practice, the goal is to achieve a certain balance between power and performance. Android OS DVFS governors are OS modules that observe the current state of a device and send signals to the CPU to increase or decrease operating frequency. For example, `powersave` and `performance` governors set minimum and maximum frequency respectively.

Although we say that DVFS governors "set" some frequency to a cluster, it is technically a recommendation to the CPU, not a direct assignment. Frequency change does not happen immediately, and DVFS cycle length – the time between governor invocations – could be considerably lower than the frequency change time. For example, the default cycle length for the `OnDemand` governor is 10 ms, while both clusters of Xiaomi Redmi Note 8 Pro CPU take about 30 ms to change frequency. So while the first governor invocation could initiate hardware frequency update, from the CPU perspective the next two invocations are as good as non-existing.

Energy-aware scheduling (EAS) [8] is an Android OS task scheduler, which could only operate in heterogeneous CPU topologies such as ARM big.LITTLE. Power management for symmetric topologies is uniform, that is, CPU frequency is set globally for the entire CPU, therefore, the maximum occupancy and performance are the same for every core. EAS uses a normalized energy model for every core cluster, taking into account available frequencies and power usage. When a task needs to be scheduled, EAS chooses the core to run this task in such a way that CPU power consumption will increase in the least possible way. However, EAS works while the CPU load is lower than 80%, otherwise, a Completely Fair Scheduler is used until the load is decreased. In order to obtain consistent power savings, EAS should be able to

issue signals to hardware to control the CPU clusters' maximum occupancy, and `schedutil` DVFS governor is considered to be a part of EAS.

2.2. DVFS algorithms. There is a number of commonly available DVFS governors for Android OS. Some of them are Android-specific, while others were initially used in the Linux kernel [9]:

PowerSave: This governor sets the CPU to the minimal available frequency and keeps it forever. This governor saves the most energy but provides the worst performance.

Performance: This governor works exactly the opposite, it sets the maximum frequency for the best performance and highest energy consumption. `Performance` and `PowerSave` reflect two extreme optimization strategies.

OnDemand: This governor sets cluster frequency proportionally to the maximum core load – active time divided by total time – within a cluster observed between governor invocations, so the device remains responsive. When a particular CPU load threshold ($\sim 80\%$) is reached, the maximum frequency is set until the load is again below the threshold.

Conservative: An improvement over `OnDemand`, this governor gradually increases the frequency when there is activity on the CPU and decreases it is to the lowest value when there is none to little activity.

Interactive: This governor is developed specifically for Android OS with UI interaction in mind. Operating frequency is once again dependent on the activity level, but activity level evaluation is event-driven in addition to timer-driven. User interaction such as screen touch is among tracked events.

schedule: This is a governor designed to work exclusively with EAS. Its basic idea is the same as in `OnDemand`, but the definition of the load is based on the EAS energy model instead of the active time to total time ratio.

While there is a large number of DVFS algorithms created by standalone developers to enhance the characteristics of the default algorithms, additional approaches are covered in the literature.

Research is done on replacing EAS and `schedutil` with a different approach for better energy efficiency. Unlike the static energy model of EAS, AdaMD [10] implements a scheduling routine which regularly inspects various resources that are currently required by executed processes and reassigns them to a more suitable cores if needed. Compared to other thread-to-core approaches, this technique allows to save up to 28% o energy while satisfying 95% of performance constraints.

In recent years there is a research trend to evaluate neural network usage for general-purpose DVFS governors. For example, the "Long Short-term Memory" effect of the recursive network could be used, as correlations should be made only for short-term data to prevent gradient attenuation problems [11].

Such network architecture reduces CPU power consumption by a maximum of 19% in comparison to common DVFS.

DVFS could be built in mind with other criteria than performance or energy saving. Chip temperature is another important factor, and by using decisions from the relatively simple neural network in the DVFS process average chip temperature could be reduced by up to 18 deg C with a minimum execution overhead and comparable performance [12]. However, chip temperature is not mutually exclusive with energy efficiency, as using deep reinforcement learning neural network to determine the temperature of the chip and estimating environmental temperature could result in 23.9% less energy consumption while retaining the required level of performance [13].

Application-specific DVFS models could also be built. For instance, a DVFS model for augmented reality applications that takes into account the requested frame rates and response time could theoretically be decreased by up to 80%, but it was not proved in practice yet [14].

Graphical Processing Unit (GPU) is a powerful device to offload computations from the CPU, and it also could operate on different frequencies, so it is reasonable to make a joint DVFS strategy for both devices. A simple rule-based model could reduce energy consumption by 18.11%, while the smartphone frame rate drops by 3.12% [15]. Another approach is to aggregate load, energy and temperature data for CPU, GPU and RAM, and assign frequency for each component by joint priorities list. This technique saves at least 26.8% power compared to default governors and state-of-the-art approaches [16].

2.3. Idle states and idle state governors. Modern CPUs are capable to enter idle states where program execution is suspended. Multi-core processors can set one or more of their cores to idle state, while other cores remain active. While in an idle state, part of the processor hardware is switched off, so it consumes less power. The deeper the state, the more hardware is switched off, but at the cost of greater entry and exit times. In Linux and Android OS terms, the total enter latency and minimum time hardware would stay in a particular idle state is called target residency [17].

For example, without going into much detail, here is a list of idle states of dual-core ARM CortexA9 processor [18] in order of increasing idle depth:

– C0 – active state.

– C1 (WFI) – most CPU timers are deactivated. Exit latency is 4 us.

– C2 ((CPUs OFF, MPU + CORE INA) – CPU is off, memory protection unit (MPU) is activated to protect critical data, and the core is inactive. Exit latency is 1100 us.

– C3 (CPUs OFF, MPU + CORE Closed Switched with Retention) – similar to C2, but the core is in CSWR mode. Exit latency is 1200 us.

– C4 (CPUs OFF, MPU CSWR + CORE Open Switched Retention) – similar to C3, but the core is in OSWR mode. Exit latency is 1500 us.

It is important to note that ability of a CPU to enter a particular state could be or could be not utilized by mobile device system-on-chip and OS, therefore, it is possible to observe a smartphone capable of entering only C1, while its CPU could go deeper by design.

The idle state governor is a module within the Android OS kernel that can track the current system state and send a signal to the CPU to enter or exit some idle state for one or more of its cores. There are several default algorithms generally available in Android devices, and at the time of writing the default algorithm is the `menu`. It tries to predict the current idle duration, then adjusts the obtained value based on a number of factors, and then tries to find the deepest idle state given its target residency and exit latency. The prediction of the current idle duration is based on the history of the previous idle times.

2.4. Evaluating Energy Consumption. Measuring smartphone CPU energy consumption is a non-trivial task, and there are several approaches available. We classify them into direct and non-direct approaches [7].

Direct approaches involve the physical measurement of momentary CPU electrical parameters either with external or internal sensors. Energy consumed over a period of time could be estimated as:

$$E = \int_0^t U(t)I(t)\,dt,$$

where $U(t)$ is momentary voltage, $I(t)$ is momentary current. While it is technically possible to have separate circuits to power the CPU at different voltages, it is challenging, so in commercially available smartphones DVFS is in fact dynamic frequency-only scaling, while voltage changes only due to natural processes within a battery[1]. Therefore, we may rewrite the above formula as:

$$E = U \int_0^t I(t)\,dt, \tag{1}$$

[1]Battery voltage drops during discharge, but between 100% and 20% the change is technically negligible by electronic components

where U is a nominal voltage on a CPU. Equation (1) allows to simplify measurement scheme and use only an ammeter. In practice, as ammeter readings are discrete, the Riemann sum is calculated instead of the actual integral.

While this approach could provide the most reliable results, there are considerable limitations to it. First of all, while the internal sensors are rather common for smartphone peripherals such as Bluetooth and Wi-Fi modules, they are seldom used to estimate the CPU power consumption [2]. The frequency and momentary current multiple times over a single second. An external ammeter should be able to catch such high-frequency changes, so most advanced commercially advanced ammeters operate in KHz range [19], but their cost could be a prohibitive factor. Additionally, ammeters should be connected, consequentially, with the measured device. Smartphone electronics do not allow us to easily connect CPU power input with ammeter. Alternatively, one could connect an ammeter to a battery connection slot while also using an external power device at a constant voltage, but readings acquired with this approach will be inevitably skewed by other smartphone peripherals such as a screen or Wi-Fi module.

Non-direct approaches estimate energy consumption by associating statistics unrelated to energy to it by some model. For example, one could estimate how much energy is consumed by a specific CPU instruction [20]. Due to the size of instruction sets in modern CPUs, we consider this approach impractical and instead follow the model proposed by Google [21]. Under this model, a CPU operating at a specified frequency consumes a specific constant current. Therefore, equation (1) is simplified even further as:

$$E = U \sum_{i=1}^{n} I(f_i) t_{fi}, \tag{2}$$

where n – number of frequencies available to CPU, f_i – particular operating frequency, $I(f)i)$ – constant current at a specified frequency, t_{fi} – time spent by CPU at a frequency f_i.

Equation (2) is further supported by Android OS, as t_{fi} is stored in special `time-in-state` files in the `/sys` directory. Temporal data is stored in separate lines for each frequency as "`<frequency><time>`". The number of lines is equal to n. It is worth noting, that the CPU clusters under big.LITTLE architecture are treated as separate CPUs, so lines in `time-in-state` also

[2] Anecdotally, we didn't encounter them in any devices available to us.

differ from core to core depending on the cluster they belong to. Time is measured in 10 milliseconds units, and the count is started when the corresponding OS driver is installed or reset to measure processor data. Values for $I(f_i)$ are stored in a weight coefficients file called `power_profile.xml`. This file should be provided by the smartphone manufacturer, but unfortunately, it is not always the case. However, absent power constants could be extracted from other smartphones using the same CPU model with the same or similar core topology. An example of such file contents is given in Table I.

To estimate power consumption one needs to multiply timing data to corresponding weight coefficients in a device `power_profile.xml` - a file provided by a smartphone manufacturer which contains power metrics for each smartphone device or peripheral. A sample of its contents related to CPU is shown in Table I. Power constants there are reported in mA[3].

Different DVFS governors produce different time distributions over available sets of frequencies. Methodologically, when a voltage is constant, electrical charge is a main indicator of energy consumption and Equation (2) could be rewritten as:

$$q_{fi} = I(f_i)t_{fi},$$

$$q = \sum_{i=1}^{n} q_i,$$

$$E = Uq,$$

where q_{fi} is an electrical charge spent at i-th frequency, q – total electrical charge. Because of this, we report energy consumption in our experiments in mAh.

2.5. Simultaneous Perturbation Stochastic Approximation. In a significant number of control problems target system behavior could be described in the form of empirical quality functional (also known as medium risk functional). An optimal control action is taken based on the extrema of this functional. In our case, CPU operating frequency might be determined based on the list of available frequencies, current CPU workload and its history and other quality criteria such as energy consumption.

[3]It is necessary to point out, that, in general, power constants reported in mA are not enough to make conclusions on energy consumption, as voltage would also be required. However, as constant nominal voltage for mobile CPUs available to market is 1V, current constants are numerically equal to power constants.

More formally, let $F_t(x, w)$ be a function of discrete time t, some parameter x and randomised vector w. The medium risk functional is defined as:

$$f_t(x) = E_w F_t(x, w),$$

and the minimum point of $f_t(x)$ as

$$\theta_t = \arg\min_x f_t(x).$$

Then in order to find the optimal point the task is to build the sequence of estimations $\{\hat{\theta}_n\}$ such that $||\hat{\theta}_n - \theta_t|| \to \min$ based on observations of the random variables $F_t(x_n, w_n)$, n = 1, 2,..

We define a *momentary trial perturbation* as a sequence of the observed uniformly symmetrically distributed independent random vectors Δ_n with covariance matrices:

$$cov\{\Delta_n \Delta_j^T\} = \delta_{nj}\sigma_\Delta^2 I,$$

where $\delta_{nj} \in \{0, 1\}$ is the Kronecker symbol, $0 < \sigma_\Delta < \infty$. The Bernoulli random vectors are suitable and frequently used as a simultaneous trial perturbation because the vector coordinates Δ_n are independent of one another and have equiprobable values of ± 1.

It is possible to use three following algorithms when observations are noisy:

$$\hat{\theta}_n = \hat{\theta}_{n-1} - \frac{\alpha_n}{\beta_n}\Delta_n y_n,$$

$$\hat{\theta}_n = \hat{\theta}_{n-1} - \frac{\alpha_n}{2\beta_n}\Delta_n (y_n^+ - y_n^-),$$

$$\hat{\theta}_n = \hat{\theta}_{n-1} - \frac{\alpha_n}{\beta_n}\Delta_n (y_n^+ - y_n),$$

to build a minimum point estimation sequence for a functional $F(x)$ without significant loss of convergence rate [22]. We denote noisy observations in the following way:

$$y_n = F(\hat{\theta}_{n-1}, w_n^+) + v_n,$$

$$y_n^- = F(\hat{\theta}_{n-1} - \beta_n \Delta_n, w_n^+) + v_n,$$

$$y_n^+ = F(\hat{\theta}_{n-1} + \beta_n \Delta_n, w_n^+) + v_n.$$

$\{\alpha_n\}$ and $\{\beta_n\}$ here are sequences of non-negative numbers conforming to a set of conditions, w_n^+ is a stochastic perturbation vector for y_n^+ observation, v_n^+ is an arbitrary external noise during the observation. This recurrent procedure is called *simultaneous perturbation stochastic approximation* (SPSA) because it inseparably contains a randomized trial perturbation which is simultaneous in all coordinates. Overall, SPSA could be classified as a stochastic gradient descent algorithm.

The first algorithm uses only a single noisy observation, and the second and third involve two noisy observations. For the purposes of distinction between those variations of the SPSA algorithm, we will call the version with a single noisy observation as SPSA1, and the latter two variations – SPSA2.

Among the conditions for consistency of estimates we specifically set out a condition for a weak correlation between the trial perturbation $\{\Delta_n\}$ and sequences of indeterminacies $\{w_n\}$ and $\{v_n\}$ as the most important. SPSA1 has lower mean squared convergence rate compared to SPSA2 but has the advantage of using only a single noisy observation, which could be more time-efficient at the end, hence both variations could be used in practice.

Both variations of the SPSA algorithm follow the same general flow:

1. Define an empirical functional $F(x)$.
2. Make an initial optimal estimate of $\hat{\theta}_0$.
3. Perturb a current optimal estimate.
4. Obtain the required amount of the noisy observations of F and update a current optimal estimate $\hat{\theta}_n$.
5. Go to Step 3.

Previously, we developed a DVFS governor based on SPSA with a single noisy observation [4]. It was shown, that overall its energy consumption is between `OnDemand` and `Interactive` governors under the CFS scheduler with a performance drop of no more than 3.06%, but in some specific scenarios it could save up to 16% of the total CPU energy.

3. Algorithm

3.1. Defining The empirical Functional. Empirical functional is a crucial component for SPSA algorithm. Although from a theoretical perspective, its definition could vary significantly even within the same problem [2], we used the lessons learned of the SPSA1 governor and added the following considerations to the functional definition.

We start our discussion by defining a *load* L on the CPU core as the percentage of active CPU time from the total CPU time (active and idle) over some period of time. This definition is the same as the one defined for the `OnDemand` governor. Then, a *computational volume* or simply *volume* denotes a product of frequency by load. Essentially, the volume is a number of the CPU ticks dedicated to active computational processes, and it is closely related to the number of the executed instructions. The crucial observation for DVFS is that the same volume produces different loads under different frequencies: the higher the frequency, the lower the load, and vice versa.

The task of DVFS is peculiar in the sense that we can base our DVFS strategy on the history of the CPU load observations among other criteria, but still, the future load cannot be reliably determined – for example, we can't predict that smartphone would receive a phone call in the next second. Therefore, we introduce *target load* or *threshold load* L_T – a specific constant value of load over some observation time. In our experiments we used empirically determined values of L_T from 60% to 80% – such values provide additional computational capacity in a scenario where the actual load proved to be much higher than anticipated from the load history. L_T is used as a boundary between two different DVFS strategies:

– If the current load exceeds L_T, we assume that the smartphone performs a rather long computational task. Therefore, all CPU resources should be made available for it, and the optimal frequency that DVFS should set is the one that provides the closest load to L_T under the currently observed volume. In this case, performance considerations outweigh energy savings. Long-term, if a load doesn't drop below L_T, the maximum frequency will eventually be set until the load drops.

– If the load does not exceed L_T, it means there is room to optimize energy consumption by finding such a frequency that provides the best energy efficiency and the projected load still does not exceed L_T.

We now define *execution efficiency* or *cost-of-execution (CoE)* of an operating frequency f in the following way:

$$CoE = \frac{E(t)}{n_{ticks}} = \frac{\int_0^t U(t)I(t)\,dt}{ft} = \frac{I_f U}{f},$$

where CoE is cost-of-execution, $E(t)$ is energy spent over a period of time, n_{ticks} is a number of CPU ticks observed during that time, t is the observed period of time. The discussion on translation from integral to constant product is given in Subsection 2.4. In essence, CoE is the energy cost of one CPU tick under a specific operating frequency.

CoE could also be viewed as a priority for the DVFS governor for the frequency selection – the lower the value, the higher the priority. Under this point of view, some *generalized cost-of-execution GCoE* metric could be used instead of CoE to prioritize the frequency selection, as it only needs to establish order relationship between frequencies.

In our research, we defined it as:

$$GCoE = \frac{I_f}{f}.$$

As discussed, the CPU voltage is safe to be treated as constant, so by removing U term from the CoE definition we do not change the established order relationship[4].

It is important to note that, given the power constants available, with the increase of f I_f also increases, but $GCoE(f)$ is generally a non-monotonically increasing function. An example is given in Table 1, where the A55 core consumes the least amount of power at a frequency of 500MHz, but is most energy efficient at 875MHz.

In the end, when the current load is below L_T, the optimal frequency would be the one with the lowest GCoE among those who could process the same volume without the projected load exceeding L_T.

As we defined the algorithm to determine the optimal frequency in both scenarios (performance and optimization), the result of our empirical functional and the quality of the current frequency estimation is determined as the distance between the current and optimal frequency indexes in a sorted frequency list.

3.2. Theoretical Foundation. In order for empirical functional to be usable in the SPSA2 algorithm and to prove the consistency of the algorithm, some conditions should be satisfied. First, the changes of optimal frequency are bounded by a task definition:

$$\|f_n - f_{n-1}\| \leqslant \delta < \infty.$$

[4]Besides, given that in our case U=1V, CoE and GCoE are numerically equal.

Then, $F(f)$ satisfies two assumptions:

Assumption 1: $F(f)$ is strongly convex and have a minimum point f^*:

$$\langle f - f^*, \nabla F(f) \rangle \geqslant \gamma \ln 1.5 - 1, \forall \mathrm{f} \in \mathbb{R}.$$

Assumption 2:

The gradient $\nabla F(f)$ satisfies the Lipschitz condition:

$$\|\nabla F(f_1) - \nabla F(f_2)\| \leqslant \gamma 1.5^{\max(\mathrm{f}_1;\mathrm{f}_2)} \cdot \ln^2 1.5 \|\mathrm{f}_1 - \mathrm{f}_2\|, \\ \forall f_1, f_2 \in \mathbb{R}.$$

It is proved that SPSA2 converges when both assumptions for empirical functional are met [5], therefore, algorithm from 3.1 converges.

3.3. Strategies to Implement Observations. A straightforward approach to implementing SPSA2 takes 3 invocations of the DVFS routine. We note that due to the absence of floating point operations in the Android OS kernel, it is easier to manipulate with frequency indexes in a sorted array rather than with the frequencies themselves. In all cases if the index is beyond array boundaries, it is set to low or high boundary correspondingly.

1. Given the current frequency index i_i, a random number $\Delta = \pm 1$ is generated, and a frequency with the index $i_i + \Delta\beta$ is set to obtain the first noisy observation y^+ of functional.

2. Then the frequency with index $i_i - \Delta\beta$ is set to obtain the second noisy observation y^-.

3. New frequency is set by index $i_{i+1} = i_i - \frac{\alpha(y^+ - y^-)}{2\Delta\beta}$.

However, by definition of SPSA2 a faster approach is also possible which takes only two invocations:

1. The current functional value under the current frequency with index i_i is treated as the first noisy observation y^0. A random number $\Delta = \pm 1$ is generated, and a frequency with the index $i_i + \Delta\beta$ is set to obtain the second noisy observation y^+ of functional.

2. New frequency is set by index $i_{i+1} = i_i - \frac{\alpha(y^+ - y^0)}{\Delta\beta}$.

However, waiting for 2 or 3 invocations to be finished could be detrimental to governor performance and estimation accuracy. Therefore, we try out another scheme, which is not strict in terms of the SPSA2 definition, but takes only a single iteration:

1. Given the current frequency index i_i, a random number $\Delta = \pm 1$ is generated. The load for frequencies with indexes $i_i \pm \Delta\beta$ is calculated in the assumption that the volume will remain the same, and the functional value for

the modelled observations y^+ and y^- is obtained. Then the new frequency is set by index $i_{i+1} = i_i - \frac{\alpha(y^+ - y^-)}{2\Delta\beta}$.

In the last scheme, we also added an optimization for the performance mode. When the observed load is 100%, we modify the value of β and thus introduce a sequence of β_n instead of a single value to increase frequency more substantially. If, however, this decision would prove excessive, and the high load would not last long, the next iteration of the algorithm would reduce operating frequency.

In all schemes, additional precautions are taken before setting i_{i+1} to properly handle corner cases. Based on the number of observations, we will further call those schemes SPSA2$_3$, SPSA2$_2$ and SPSA2$_1$ respectively.

3.4. Accounting for Frequency Change Lag. The time CPU takes to change frequency could be considerable. For example, the `OnDemand` governor is scheduled to re-evaluate optimal frequency every 10 ms. Historically, `OnDemand` was developed for desktop computers and servers, and frequency switch could happen within 10 ms. However, in our preliminary research with Xiaomi Redmi Note 8 Pro, we found out that after the initial frequency change request by the `OnDemand`-based DVFS governor, it could take up to 3 consequent DVFS routine calls to register the updated frequency from the CPU, and the DVFS governor sends a frequency change request on every invocation.

This situation is indicative that even the most commonly available DVFS governors are based on assumptions that may not be true for the underlying hardware.

As our SPSA2 governors are also using the `OnDemand` governor timer model, and it is important for the algorithm to make noisy observations at the requested frequencies, we skip the DVFS routine invocations where the CPU cluster frequency is still different from the one requested previously. The algorithm continues when a proper frequency is set, and it is assumed that the load between two routine invocations was obtained at the requested frequency; thus, the noisy load observation is properly obtained.

3.5. EAS Integration. Energy Aware Scheduling works closely with the `schedutil` DVFS governor, and it is stated that EAS is not guaranteed to reduce energy consumption if the `schedutil` is not an active governor. In fact, `schedutil` implements the same strategy as the `OnDemand` governor, that is, it selects cluster frequency proportional to the maximum load over cluster cores with the minimum frequency corresponding to 0% load and the maximum frequency corresponding to 100% load. However, the EAS CPU load definition is significantly different from the one used in `OnDemand`. The CPU load is estimated in terms of the EAS energy model and occupancy of all

tasks assigned to a specific CPU core. Instead of a posterior evaluation, it is estimated a priori.

For our proposed schemes we used the `OnDemand` load definition even when EAS is turned on, and, as shown in the experiments, tuning α, β and L_T is enough to align our SPSA2 governors with EAS.

4. Experimental Methodology

4.1. Device Selection. For our experiments, we used Samsung Galaxy s7 SM-G930F. Its processor, Exynos 8 Octa (8890) has 2 clusters with 4 Cortex-A53 cores (LITTLE) and 4 Exynos M1 cores (big). It is notable that while originally supporting Android 8, it could be patched to run Android 10 and 11.

The smartphone was patched to run the herolte[5] Android 11 kernel, which could be run on the test device with the EAS scheduler. To test the default CFS scheduler, we used Samsung android_kernel_samsung_universal8890 for Android 10[6]. This kernel selection allows us to compare our governors' performance against commonly available Interactive, OnDemand and Schedutil governors. Our DVFS governors were added as additional modules to both of those kernels, and it was required to obtain root access for the smartphone to install custom builds. Switching to our governors was done by the default `cpufreq` system calls [9].

4.2. Test Cases. As noted in our previous work [4], it is important for the general-purpose DVFS governor to be able to handle different kinds of workloads while providing a trade-off between performance and energy consumption. However, each governor is built with a particular workload model in mind, and this model is not bound to reflect real-world scenarios.

We've considered the following list of diverse test cases to be implemented. Each test case was assigned a name for further reference.

1. **videoVLC** – playing MP4 file using VLC video player, preliminarily selected as a default video player.

2. **trialXTreme3** – imitation of playing Trial Xtreme 3.

3. **flappyBird** – imitation of playing Flappy Bird.

4. **type** – creating a note in the Notes application, writing text and deleting a note.

5. **camera** – launching a default camera application and recording a video with it. The resulting video is deleted in the end.

[5]https://github.com/pascua28/herolt

[6]https://github.com/8890q/android_kernel_samsung_universal8890/tree/lineage-17.1

6. **twitch** – watching a Twitch stream in a browser and closing the browser after a while[7].

As the `Monkeyrunner` tool we used previously was not available in the toolchain for the test device, a set of utilities that mirrors its functionality to run tests was written in Python[8].

All tests are launched 10 times for 5 minutes to average the influence of system background processes. They are implemented as Python scripts as well. To launch a test, a smartphone needs to be connected to a controlling PC, and the test execution is controlled through `adb` commands.

To test smartphone performance we selected Geekbench 5.5.1, as it has an open methodology we found valid for our purposes [23]. The performance tests were launched 3 times for each evaluated governor due to their longevity, and an average of the obtained score points was calculated.

4.3. Modified Energy Consumption Models. Overall, direct measurement approaches were not used in the research for this paper due to the difficulties outlined above. While the basic energy consumption model could already be used, it does not take into account idle state management. Moreover, the source code behind `time-in-state` files is not synchronized with the idle governors. To address this issue, we propose the following modifications to the basic model.

Equation (2) implicitly assumes that the CPU consumes a fixed amount of power by just being at a specific frequency, regardless of the fact if there is an active computational process or not. This assumption is supported by the implementation of idle task while the CPU is in C0 (Active) state. When the OS scheduler cannot schedule an active tasks for the core, it assigns a special idle task, which consists of `NOP` (No Operation) instructions. C1, however, involves stopping CPU core timers, and the computational process cannot be run.

Given than, only C0 and C1 states are available on the test device, and given the fact that there could be several clusters of cores with a single frequency for all cores within a cluster, we modify Equation (2) as:

$$E = \sum_{i=1}^{Ncl} Eidle_i(t) + \sum_{i=1}^{Ncl} U_i \cdot \sum_{j=1}^{Nf_i} I_i(f_j) \cdot \sum_{k=1}^{Ncores_i} t_{fjk}, \qquad (3)$$

[7]We would like to thank @StreamerHouse channel for their dedication to 24/7 streaming schedule as it allowed to keep test case source code without modifications regardless of the launch time.

[8]https://github.com/makar-pelogeiko/freq _gov_test

where Ncl is a number of core clusters, $Eidle_i(t)$ is energy consumed by a CPU for just being turned on, Nf_i is a number of frequencies for ith cluster, Ui is a nominal voltage of cores in ith cluster, $I_i(f)$ is a nominal current for slected frequency f in ith cluster, $Ncores_i$ is a number of cores in ith cluster, t_{fjk} is a time spent by kth core within ith cluster on jth frequency.

While this model is more elaborate than the one described in (2), it could be simplified for practical reasons. In the first term, we assume that each cluster has linear energy consumption over time for just being turned on. Intuitively, it seems that to properly calculate idle state energy footprint we should split $Eidle_i(t)$ to basic CPU energy consumption and C1 footprint for each core, but base CPU and C1 idle state power profiles are not available in `power_profile.xml`, we omit this term from further analysis.

Moreover, calculating $\sum_{k=1}^{Ncores_i} t_{fjk}$ seems excessive, because cores of the same cluster operate at the same frequency. However, this term becomes useful when we are trying to estimate the impact of deep sleep idle states impact on energy consumption.

While idle state stops CPU core timers, it does not change the nominal core operating frequency, that is, a core operating at 1 GHz before sleep will continue to work at 1 GHz after sleep. We initially assumed that the core is put to sleep when there are not enough tasks to schedule in the system overall, so the DVFS governor sets the minimum operating frequency for the cluster. Our initial idea was to deduct idle time in C1 from the time spent by the core on the lowest frequency such as in:

$$E = \sum_{i=1}^{Ncl} U_i \cdot (\sum_{k=1}^{Ncores_i} I_i(f_1)(t_{f0k} - t_k^{idle}) + \sum_{j=2}^{Nf_i} I_i(f_j) t_{fjk}),$$

where t_k^{idle} is the time spent by kth core in idle states. However, this assumption proved to be wrong, as it was shown experimentally that there were cases where $t_{f0k} < t_k^{idle}$), which means that the system put a core to sleep at a higher frequency than minimal.

While it is technically possible to modify the Android OS kernel and to track at which frequency the core was suspended, instead we assume that idle state management is independent of DVFS, but not of the OS scheduler, and a core may be put to sleep at any frequency at any time. Therefore, we propose to track idle state energy footprint by deducting idle state time from each time spent on frequency proportionally:

$$E = \sum_{i=1}^{Ncl} U_i \cdot \sum_{j=1}^{Nf_i} I_i(f_j) \cdot \sum_{k=1}^{Ncores_i} (t_{fjk} - t_k^{idle} \frac{t_{fjk}}{\sum_{m=1}^{Nf_i} t_{fmk}}).$$

As this approach is not precise but gives empirically good insights on actual energy expenditure, we use both original basic and modified models into report our results.

4.4. Device Preparation. Validity of experiments and output stability was enhanced by the following protocol we have described in the previous research [7]:

– All unnecessary applications were uninstalled, and all application activities were turned off for those that could not be uninstalled.

– Peripherals that were not used in a particular test case (i.e. Wi-Fi, 4G, GPS) were turned off.

– A cool-down period of 2 minutes was taken between the tests for background processes to finalize and decrease the device temperature.

– Before running a particular test case, it was run for a single time for warming-up purposes.

Battery charge levels were not homogenized before each test runs, as it was unnecessary by our energy consumption models. In fact, for the device to be controlled by a test run utility, it was connected to a PC via USB, so the battery was charging during the test runs.

5. Experiments. The governor implementations are available for Android 11[9] and Android 10[10].

The full experimental data is also available.[11]

The first set of the experiments was taken under Android 11 with EAS turned on. By enumerating possible parameters we found out the best-performing settings for all SPSA algorithms:

1. $\alpha = 2, \beta = 1, L_T = 70\%$;

2. Cluster 0: $\alpha = 2, \quad \beta = 1, \quad L_T = 80\%$; Cluster 1: $\alpha = 3, \quad \beta = 1, \quad L_T = 98\%$.

Tables 2 to 5 contain the median values for energy consumption under the basic and modified energy models. Here and in the subsequent tables we

[9]https://github.com/makar-pelogeiko/herolte _Eas _Idle _modification/tree/Q-stable-spsa_gov

[10]https://github.com/makar-pelogeiko/android _kernel _samsung _universal8890/tree/lineage-17.1-spsa _gov

[11]https://studentspburu-my.sharepoint.com/personal/st076963 _student _spbu _ru/ _layouts/15/onedrive.aspx?id=%2Fpersonal%2Fst076963%5Fstudent%5Fspbu%5Fru%2FDocuments%2Fdiploma%2Fresultsga=1

highlight scenarios where the SPSA governor energy consumption is higher than energy consumption of every baseline governor in *italic* and the cases where SPSA is better than some of the baseline governors in **bold**. Table 6 contains performance data. The first line for SPSA governors corresponds to the first set of parameters, and the second line – to the second set.

Table 2. Energy consumption (mAh) under Android 11 with EAS scheduler (basic energy model), videoVLC, trialXTreme3 and flappyBird tests

Algorithm	videoVLC	trialXTreme3	flappyBird
$SPSA2_3$	21.67	27.62	24.86
	21.43	24.53	24.62
$SPSA2_2$	23.40	37.44	40.64
	22.65	32.50	34.36
$SPSA2_1$	23.75	43.43	**47.04**
	22.17	30.43	31.23
Schedutil	24.56	44.30	43.56
Interactive	141.21	119.08	104.73
OnDemand	34.86	86.06	92.86

Table 3. Energy consumption (mAh) under Android 11 with EAS scheduler (basic energy model), type, camera and twitch, tests

Algorithm	type	camera	twitch
$SPSA2_3$	32.61	22.43	30.59
	30.91	22.02	24.86
$SPSA2_2$	**46.46**	25.27	38.62
	39.96	23.67	28.93
$SPSA2_1$	**52.19**	26.44	47.06
	35.66	22.86	27.32
Schedutil	47.09	27.36	51.83
Interactive	122.31	55.36	91.33
OnDemand	97.43	56.16	80.68

Overall, the energy consumption dispersion is omitted in this paper, but it is available in the full experimental report. It should be noted that the values for the SPSA and `schedutil` governors have a visibly low dispersion in all experiments, and energy consumption could be compared by the median value only. It is not true for `OnDemand` and especially `Interactive` governors. For example, `Interactive` showed in the videoVLC test the minimum and

maximum values under the basic energy model of 42.42 and 155.91 mAh respectively. However, it does not affect the validity of the analysis, as even the minimum energy consumption of both governors was higher than the maximum value for `schedutil` or SPSA governors.

Table 4. Energy consumption (mAh) under Android 11 with EAS scheduler (modified energy model), videoVLC, trialXTreme3 and flappyBird tests

Algorithm	videoVLC	trialXTreme3	flappyBird
$SPSA2_3$	5.90	14.71	10.23
	6.11	13.49	10.15
$SPSA2_2$	**6.34**	19.16	**16.27**
	6.24	16.71	14.16
$SPSA2_1$	**6.31**	19.68	**18.21**
	5.93	15.61	12.75
Schedutil	5.91	20.24	15.70
Interactive	33.74	46.78	35.46
OnDemand	8.59	34.84	32.48

Table 5. Energy consumption (mAh) under Android 11 with EAS scheduler (modified energy model), type, camera and twitch tests

Algorithm	type	camera	twitch
$SPSA2_3$	8.99	14.41	22.84
	8.67	13.71	18.98
$SPSA2_2$	7.69	**17.18**	28.18
	12.30	15.24	21.88
$SPSA2_1$	**13.02**	**17.76**	33.25
	9.36	15.43	20.70
Schedutil	10.24	15.62	34.92
Interactive	21.83	30.56	58.48
OnDemand	21.35	25.07	47.53

Performance-wise, both existing and novel algorithms perform comparably. There are no clear outliers, and for single-core test, the difference between the best and worst performance is within 15%, while it is within 18% for the multicore scenario. We note that the first set of SPSA parameters provides better performance than the second set. $SPSA2_3$ performance is worsened by the fact it needs 3 observations, but not too much.

Table 6. GeekBench 5.5.1 performance scores

Algorithm	Single core	Multicore
$SPSA2_3$	287	970
	282	913
$SPSA2_2$	302	1025
	290	962
$SPSA2_1$	331	1073
	324	966
Schedutil	319	970
Interactive	321	1112
OnDemand	296	1068

When we look at energy consumption data, it should be noted that the modified energy model significantly changes the observed values compared to the basic model, and in some cases their ratio. The modified model, in our opinion, still better reflects data reality if direct measurement is not available, and our next analysis is based on it, even though the basic model is more complimentary to the SPSA governors.

The `Interactive` and `OnDemand` governors are consistently more power-hungry than `schedutil` under EAS, and, as a general rule, we definitely suggest using `schedutil` over other governors if EAS is available in stock firmware.

As for the SPSA governors, all of them could be used in place of `schedutil`. First of all, they all handle trialXTreme3 and twitch tests better than schedutil. We assume it to be related to $\beta = 1$ in our experiments, as higher β results in a more rapid gradient descent, and in a quickly changing reality of CPU load complicated by frequency switch lags relatively smooth frequency change is good for consistent CPU usage. $SPSA2_1$ with the first set of parameters is shown to consume more energy in most of the tests (up to 27% for type test), while being only 10% better in performance compared to `schedutil`, so the second set of parameters is recommended there, as performance is at the same level, while energy consumption may be up to 31% better. $SPSA2_2$ is the most balanced governor, as it is up to 20% better in some tests and up to 10% worse in others energy-wise, but it demonstrates a 5.6% performance increase in multicore case, which is more realistic scenario. $SPSA2_3$ is the most conservative of other governors energy and performance-wise, but overall multicore performance is comparable to `schedutil`.

A special case is the videoVLC test, where the SPSA governors tend to spend more energy than `schedutil`. The difference is never significant (no

more than 7.2% for $SPSA2_2$), but our explanation is that the timings of intense computations (frame decoding) are such that the SPSA governors cannot drop frequency to lower values. The only exception is $SPSA2_3$, but the difference is within a margin of a statistical error.

Tables 7 to 10 contain the median values for energy consumption under the basic and modified energy models for the tests run under Android 10 and CFS scheduler.The situation there is drastically different. First, `schedutil` cannot be used there as a benchmark as it would be running under the conditions it was not designed for. Then, the `Interactive` governor demonstrates a remarkable improvement in energy consumption.

Table 7. Energy consumption (mAh) under Android 10 with CFS scheduler (basic energy model), videoVLC, trialXTreme3 and flappyBird tests

Algorithm	videoVLC	trialXTreme3	flappyBird
$SPSA2_3$	**23.52**	**49.49**	48.67
	23.55	43.87	44.68
$SPSA2_2$	**26.14**	**66.62**	**71.74**
	24.34	**63.82**	**62.85**
$SPSA2_1$	**26.58**	*101.24*	*116.08*
	23.65	**57.40**	**85.69**
Interactive	22.25	44.31	53.47
OnDemand	29.18	76.41	94.63

Table 8. Energy consumption (mAh) under Android 10 with CFS scheduler (basic energy model), type, camera and twitch tests

Algorithm	type	camera	twitch
$SPSA2_3$	57.73	**26.25**	38.71
	51.96	**25.08**	30.22
$SPSA2_2$	**81.87**	**36.10**	**45.66**
	70.70	**29.28**	33.41
$SPSA2_1$	*116.36*	**31.28**	**50.54**
	68.21	**25.23**	32.04
Interactive	59.52	24.32	41.73
OnDemand	101.57	41.39	66.24

However, all SPSA governors demonstrate energy behavior reminiscent of SPSA1 governor [4], where they are most of the time either between `OnDemand` and `Interactive`, and in some margin cases inconsistently demonstrate better or worse results.

Table 9. Energy consumption (mAh) under Android 10 with CFS scheduler (modified energy model), videoVLC, trialXTreme3 and flappyBird tests

Algorithm	videoVLC	trialXTreme3	flappyBird
$SPSA2_3$	**5.70**	**13.51**	12.07
	5.57	11.13	11.07
$SPSA2_2$	**6.35**	**17.53**	**17.27**
	5.66	**14.57**	**15.38**
$SPSA2_1$	**6.20**	**19.83**	*25.58*
	5.44	11.67	**20.35**
Interactive	1.31	13.28	12.30
OnDemand	7.08	21.65	24.03

Table 10. Energy consumption (mAh) under Android 10 with CFS scheduler (modified energy model), type, camera and twitch tests

Algorithm	type	camera	twitch
$SPSA2_3$	**13.22**	**4.88**	16.53
	11.33	**4.48**	13.54
$SPSA2_2$	**17.44**	**4.88**	**18.98**
	15.22	**4.18**	14.61
$SPSA2_1$	*23.59*	**3.27**	**20.50**
	14.63	2.14	13.91
Interactive	11.71	2.93	16.92
OnDemand	22.03	4.98	23.61

The reason behind such energy behavior is a change in scheduling strategy. Unlike EAS, CFS does not prioritize LITTLE cores over big ones, and in similar situations, big cores are loaded more resulting in a higher power drain.

Additionally, while overall $SPSA2_3$ demonstrates an acceptable energy consumption, its performance is worse, as at load levels of 99–100% it does not immediately recommend increase frequency. As other algorithms demonstrate higher overall energy consumption than `Interactive`, and the latter provides an acceptable performance to the end user, we did not run performance tests for the SPSA governors.

6. Conclusion. Our experiments show that all SPSA governors could be used alongside EAS to obtain better CPU energy efficiency in common use cases. In CFS-controlled environments, the SPSA governors could also be used, but they demonstrate energy efficiency comparable to existing governors.

We conclude, that like SPSA1 in our previous work [4, 7], the SPSA2 family of governors performs better than `OnDemand`, `Interactive` and `schedutil` in the scenarios where the workload is evenly distributed over time or has prolonged periods of calculations – improvement of up to 31% could be observed with the same performance under EAS. We observe that stochastic optimization provides good optimal point tracking in noisy environments in a long run without setting seemingly optimal frequencies at every step. In the spiky workloads, a conservative approach to frequency changes causes those computational spikes to be treated as constant load and therefore could result in a somewhat higher CPU energy consumption. In the end, the SPSA2 family could be used to prolong a smartphone's lifetime on a day-to-day basis.

References

1. Number of smartphone mobile network subscriptions worldwide from 2016 to 2022, with forecasts from 2023 to 2028. Available at: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/. (accessed 10.05.2023).
2. Spall J.C. Multivariate stochastic approximation using a simultaneous perturbation gradient approximation. IEEE Transactions on Automatic Control. 1992. vol. 37. no. 3. pp. 332–341.
3. Granichin O., Amelina N. Simultaneous perturbation stochastic approximation for tracking under unknown but bounded disturbances. IEEE Transactions on Automatic Control. 2015. vol. 60. no. 6. pp. 1653–1658.
4. Bogdanov E., Bozhnyuk A., Bykov D., Sartasov S., Sergeenko A., Granichin O. Dynamic Voltage-Frequency Optimization using Simultaneous Perturbation Stochastic Approximation. 60th IEEE Conference on Decision and Control (CDC). 2021. pp. 3774–3779.
5. Granichin O., Vakhitov A. Accuracy for the SPSA algorithm with two measurements. WSEAS Transactions on Systems. 2006. vol. 5.
6. Mair H.T., Gammie G., Wang A., Lagerquist R., Chung C.J., Gururajarao S., Kao P., Rajagopalan A., Saha A., Jain A., Wang E., Ouyang S., Wen H., Thippana A., Chen HsinChen, R.S., Chau M., Varma A., Flachs B., Peng M., Tsai A., Lin V., Fu U., Kuo W., Yong L.-K., Peng C., Shieh L., Wu J., Ko U. 4.3 A 20nm 2.5GHz ultra-low-power tri-cluster CPU subsystem with adaptive power allocation for optimal mobile SoC performance. 2016 IEEE International Solid-State Circuits Conference (ISSCC). 2016. pp. 76–77.
7. Bogdanov E., Bozhnyuk A., Sartasov S., Granichin O. On Application of Simultaneous Perturbation Stochastic Approximation for Dynamic Voltage-Frequency Scaling in Android OS. 7th International Conference on Event-Based Control, Communication and Signal Processing (EBCCSP'21). 2021. DOI: 10.1109/EBCCSP53293.2021.9502396.
8. The kernel development community. Energy Aware Scheduling. Available at: https://www.kernel.org/doc/html/next/scheduler/sched-energy.html. (accessed 10.05.2023).
9. CPU frequency and voltage scaling code in the Linux (TM) kernel. Linux CPUFreq. CPUFreq Governors. Available at: https://android.googlesource.com/kernel/common/+/a7827a2a60218b25f222b54f77ed38f57aebe08b/Docum freq/governors.txt. (accessed 10.05.2023).

10. Basireddy K.R., Singh A.K., Al-Hashimi B.M., Merrett G.V. AdaMD: Adaptive Mapping and DVFS for Energy-Efficient Heterogeneous Multicores. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. 2020. vol. 39. no. 10. pp. 2206–2217.
11. Lee J., Nam S., Park S. Energy-Efficient Control of Mobile Processors Based on Long Short-Term Memory. IEEE Access. 2019. vol. 7. pp. 80552–80560.
12. Rapp M., Krohmer N., Khdr H., Henkel J. NPU-accelerated imitation learning for thermal- and QoS-aware optimization of heterogeneous multi-cores. Proceedings of the 2022 Conference and Exhibition on Design, Automation and Test in Europe (DATE '22). 2021. pp. 584–587.
13. Kim S., Bin K., Ha S., Lee K., Chong S. ZTT: learning-based DVFS with zero thermal throttling for mobile devices. Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys'21). 2021. pp. 41–53.
14. Song S., Kim J., Chung J.-M. Energy Consumption Minimization Control for Augmented Reality Applications based on Multi-core Smart Devices. IEEE International Conference on Consumer Electronics (ICCE). 2019. DOI: 10.1109/ICCE.2019.8661917.
15. Ohk S.-R., Kim Y., Kim Y.-J. Phase-Based Low Power Management Combining CPU and GPU for Android Smartphones. Electronics. 2022. vol. 11. no. 16. DOI: 10.3390/electronics11162480.
16. Dey S., Isuwa S., Saha S., Singh A.K., McDonald-Maier K. CPU-GPU-Memory DVFS for Power-Efficient MPSoC in Mobile Cyber Physical Systems. Future Internet. 2022. vol. 14. no. 3. DOI: 10.3390/fi14030091.
17. CPU Idle Time Management. Available at: https://docs.kernel.org/admin-guide/pm/cpuidle.html. (accessed 10.05.2023).
18. Metri G., Agrawal A., Peri, R., Brockmeyer M., Weisong S. A simplistic way for power profiling of mobile devices. 2012 International Conference on Energy Aware Computing. 2012. DOI: 10.1109/ICEAC.2012.6471020.
19. Monsoon Power Monitor Specifications. Available at: https://www.msoon.com/specifications. (accessed 10.05.2023).
20. Chung Y., Lin C., King C. ANEPROF: Energy Profiling for Android Java Virtual Machine and Applications. 2011 IEEE 17th International Conference on Parallel and Distributed Systems. 2011. pp. 372–379. DOI: 10.1109/ICPADS.2011.28.
21. Measuring Component Power. Available at: https://source.android.com/docs/core/power/component. (accessed 10.05.2023).
22. Granichin O. Linear regression and filtering under nonstandard assumptions (arbitrary noise). IEEE Transactions on Automatic Control. 2004. vol. 49. no. 10. pp. 1830–1837.
23. Geekbench 5 CPU Workloads. Available at: https://www.geekbench.com/doc/geekbench5-cpu-workloads.pdf. (accessed 10.05.2023).

Pelogeiko Makar – Student, Software engineering department, faculty of mathematics and mechanics, St. Petersburg State University (SPbSU). Research interests: energy-efficient programming. m.pelogeiko@mail.ru; 28, Universitetsky Av., 198504, St. Petersburg, Russia; office phone: +7(812)428-4910.

Sartasov Stanislav – Assistant professor of software engineering department, Faculty of mathematics and mechanics, St. Petersburg State University (SPbSU); chief technology officer, Denominator.One. Research interests: sustainable software development, software energy efficiency, industrial software engineering, biometrics. The number of publications — 10. stanislav.sartasov@yandex.ru; 28, Universitetsky Av., 198504, St. Petersburg, Russia; office phone: +7(812)428-4910.

Granichin Oleg – Ph.D., Dr.Sci., Professor of software engineering department, Faculty of mathematics and mechanics, St. Petersburg State University (SPbSU); Laboratory "Control of complex systems", Institute for Problems in Mechanical Engineering. Research interests: randomized optimization and estimation algorithms, stochastic optimization in computer science, adaptive and optimal control, pattern recognition. The number of publications — 100. oleg_granichin@mail.ru; 28, Universitetsky Av., 198504, St. Petersburg, Russia; office phone: +7(812)428-4910.

Acknowledgements. This work was supported in part by the St. Petersburg State University (project ID 94062114).

УДК 004.451.25 **DOI** 10.15622/ia.22.5.3

М.А. Пелогейко, С.Ю. Сартасов, О.Н. Граничин

О СТОХАСТИЧЕСКОЙ ОПТИМИЗАЦИИ ЭНЕРГОПОТРЕБЛЕНИЯ ПРОЦЕССОРА СМАРТФОНА

Пелогейко М.А., Сартасов С.Ю., Граничин О.Н **О стохастической оптимизации энергопотребления процессора смартфона.**

Аннотация. Увеличение времени работы смартфона – это постоянное стремление, которое с каждым годом становится все более и более важным. Это может быть достигнуто с помощью более совершенного оборудования или путем внедрения в программное обеспечение практик с учетом энергопотребления, и последний подход является более доступным. Поскольку ЦП является одним из самых энергоемких устройств для смартфонов, динамическое масштабирование частоты напряжения (DVFS) представляет собой метод настройки частоты ЦП в соответствии с текущими вычислительными потребностями, и уже были разработаны различные алгоритмы, как энергосберегающие, так и энергонезависимые. Следуя нашей предыдущей работе по этому вопросу, мы предлагаем новый подход DVFS для использования стохастической аппроксимации одновременных возмущений (SPSA) с двумя зашумленными наблюдениями для отслеживания оптимальной частоты и реализации нескольких алгоритмов на его основе. Кроме того, мы также решаем проблему аппаратной задержки между сигналом для ЦП об изменении частоты и ее фактическим обновлением. Поскольку ОС Android может использовать планировщик задач по умолчанию или планировщик с учетом энергопотребления, который способен использовать преимущества разнородных архитектур мобильных ЦП, таких как ARM big.LITTLE, мы также исследуем схему интеграции между предлагаемыми алгоритмами и планировщиками ОС. Представлена методология тестирования на основе моделей для сравнения разработанных алгоритмов с существующими, а также описан набор тестов, отражающий реальные сценарии использования. Наши эксперименты показывают, что алгоритм на основе SPSA хорошо работает с EAS с упрощенной схемой интеграции, демонстрируя производительность ЦП, сравнимую с другими алгоритмами DVFS с учетом энергопотребления, и снижение энергопотребления.

Ключевые слова: ОС Android, динамическое масштабирование частоты напряжения, стохастическая оптимизация, SPSA, энергопотребление.

Литература

1. Number of smartphone mobile network subscriptions worldwide from 2016 to 2022, with forecasts from 2023 to 2028. Available at: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/. (accessed 10.05.2023)
2. Spall J.C. Multivariate stochastic approximation using a simultaneous perturbation gradient approximation. IEEE Transactions on Automatic Control. 1992. vol. 37. no. 3. pp. 332–341.
3. Granichin O., Amelina N. Simultaneous perturbation stochastic approximation for tracking under unknown but bounded disturbances. IEEE Transactions on Automatic Control. 2015. vol. 60. no. 6. pp. 1653–1658.
4. Bogdanov E., Bozhnyuk A., Bykov D., Sartasov S., Sergeenko A., Granichin O. Dynamic Voltage-Frequency Optimization using Simultaneous Perturbation Stochastic

Approximation. 60th IEEE Conference on Decision and Control (CDC). 2021. pp. 3774–3779.

5. Granichin O., Vakhitov A. Accuracy for the SPSA algorithm with two measurements. WSEAS Transactions on Systems. 2006. vol. 5.
6. Mair H.T., Gammie G., Wang A., Lagerquist R., Chung C.J., Gururajarao S., Kao P., Rajagopalan A., Saha A., Jain A., Wang E., Ouyang S., Wen H., Thippana A., Chen HsinChen, R.S., Chau M., Varma A., Flachs B., Peng M., Tsai A., Lin V., Fu U., Kuo W., Yong L.-K., Peng C., Shieh L., Wu J., Ko U. 4.3 A 20nm 2.5GHz ultra-low-power tri-cluster CPU subsystem with adaptive power allocation for optimal mobile SoC performance. 2016 IEEE International Solid-State Circuits Conference (ISSCC). 2016. pp. 76–77.
7. Bogdanov E., Bozhnyuk A., Sartasov S., Granichin O. On Application of Simultaneous Perturbation Stochastic Approximation for Dynamic Voltage-Frequency Scaling in Android OS. 7th International Conference on Event-Based Control, Communication and Signal Processing (EBCCSP'21). 2021. DOI: 10.1109/EBCCSP53293.2021.9502396.
8. The kernel development community. Energy Aware Scheduling. Available at: https://www.kernel.org/doc/html/next/scheduler/sched-energy.html. (accessed 10.05.2023).
9. CPU frequency and voltage scaling code in the Linux (TM) kernel. Linux CPUFreq. CPUFreq Governors. Available at: https://android.googlesource.com/kernel/common/+/a7827a2a60218b25f222b54f77ed38f57aebe08b/Docum freq/governors.txt. (accessed 10.05.2023).
10. Basireddy K.R., Singh A.K., Al-Hashimi B.M., Merrett G.V. AdaMD: Adaptive Mapping and DVFS for Energy-Efficient Heterogeneous Multicores. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. 2020. vol. 39. no. 10. pp. 2206–2217.
11. Lee J., Nam S., Park S. Energy-Efficient Control of Mobile Processors Based on Long Short-Term Memory. IEEE Access. 2019. vol. 7. pp. 80552–80560.
12. Rapp M., Krohmer N., Khdr H., Henkel J. NPU-accelerated imitation learning for thermal- and QoS-aware optimization of heterogeneous multi-cores. Proceedings of the 2022 Conference and Exhibition on Design, Automation and Test in Europe (DATE '22). 2021. pp. 584–587.
13. Kim S., Bin K., Ha S., Lee K., Chong S. ZTT: learning-based DVFS with zero thermal throttling for mobile devices. Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys'21). 2021. pp. 41–53.
14. Song S., Kim J., Chung J.-M. Energy Consumption Minimization Control for Augmented Reality Applications based on Multi-core Smart Devices. IEEE International Conference on Consumer Electronics (ICCE). 2019. DOI: 10.1109/ICCE.2019.8661917.
15. Ohk S.-R., Kim Y., Kim Y.-J. Phase-Based Low Power Management Combining CPU and GPU for Android Smartphones. Electronics. 2022. vol. 11. no. 16. DOI: 10.3390/electronics11162480.
16. Dey S., Isuwa S., Saha S., Singh A.K., McDonald-Maier K. CPU-GPU-Memory DVFS for Power-Efficient MPSoC in Mobile Cyber Physical Systems. Future Internet. 2022. vol. 14. no. 3. DOI: 10.3390/fi14030091.
17. CPU Idle Time Management. Available at: https://docs.kernel.org/admin-guide/pm/cpuidle.html. (accessed 10.05.2023).
18. Metri G., Agrawal A., Peri, R., Brockmeyer M., Weisong S. A simplistic way for power profiling of mobile devices. 2012 International Conference on Energy Aware Computing. 2012. DOI: 10.1109/ICEAC.2012.6471020.

19. Monsoon Power Monitor Specifications. Available at: https://www.msoon.com/specifications. (accessed 10.05.2023).
20. Chung Y., Lin C., King C. ANEPROF: Energy Profiling for Android Java Virtual Machine and Applications. 2011 IEEE 17th International Conference on Parallel and Distributed Systems. 2011. pp. 372–379. DOI: 10.1109/ICPADS.2011.28.
21. Measuring Component Power. Available at: https://source.android.com/docs/core/power/component. (accessed 10.05.2023).
22. Granichin O. Linear regression and filtering under nonstandard assumptions (arbitrary noise). IEEE Transactions on Automatic Control. 2004. vol. 49. no. 10. pp. 1830–1837.
23. Geekbench 5 CPU Workloads. Available at: https://www.geekbench.com/doc/geekbench5-cpu-workloads.pdf. (accessed 10.05.2023).

Пелогейко Макар Андреевич — студент, кафедра разработки программного обеспечения, факультет математики и механики, Санкт-Петербургский государственный университет (СПбГУ). Область научных интересов: энергоэффективное программирование. m.pelogeiko@mail.ru; Университетский проспект, 28, 198504, Санкт-Петербург, Россия; р.т.: +7(812)428-4910.

Сартасов Станислав Юрьевич — доцент кафедры разработки программного обеспечения, факультет математики и механики, Санкт-Петербургский государственный университет (СПбГУ); главный технический директор, Denominator.One. Область научных интересов: устойчивая разработка программного обеспечения, энергоэффективность программного обеспечения, промышленная разработка программного обеспечения, биометрия. Число научных публикаций — 10. stanislav.sartasov@yandex.ru; Университетский проспект, 28, 198504, Санкт-Петербург, Россия; р.т.: +7(812)428-4910.

Граничин Олег Николаевич — д-р физ.-мат. наук, профессор кафедры разработки программного обеспечения, факультет математики и механики, Санкт-Петербургский государственный университет (СПбГУ); лаборатория “управление сложными системами”, Институт проблем машиноведения РАН. Область научных интересов: рандомизированные алгоритмы оптимизации и оценивания, стохастическая оптимизация в информатике, адаптивное и оптимальное управление, распознавание образов. Число научных публикаций — 100. oleg_granichin@mail.ru; Университетский проспект, 28, 198504, Санкт-Петербург, Россия; р.т.: +7(812)428-4910.

Поддержка исследований. — Работа была поддержана Санкт-Петербургским государственным университетом (проект № 94062114).

УДК 006.72 **DOI** 10.15622/ia.22.5.4

Е.С. Новикова, Е.В. Федорченко, И.В. Котенко, И.И. Холод

АНАЛИТИЧЕСКИЙ ОБЗОР ПОДХОДОВ К ОБНАРУЖЕНИЮ ВТОРЖЕНИЙ, ОСНОВАННЫХ НА ФЕДЕРАТИВНОМ ОБУЧЕНИИ: ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ И ОТКРЫТЫЕ ЗАДАЧИ

Новикова Е.С., Федорченко Е.В., Котенко И.В., Холод И.И. **Аналитический обзор подходов к обнаружению вторжений, основанных на федеративном обучении: преимущества использования и открытые задачи.**

Аннотация. Для обеспечения точного и своевременного реагирования на различные типы атак, системы обнаружения вторжений собирают и анализируют большое количество данных, которые могут включать в том числе и информацию с ограниченным доступом, например, персональные данные или данные, представляющие коммерческую тайну. Следовательно, такие системы могут быть рассмотрены как источник рисков, связанных с обработкой конфиденциальной информации и нарушением ее безопасности. Применение парадигмы федеративного обучения для построения аналитических моделей обнаружения атак и аномалий может значительно снизить такие риски, поскольку данные, генерируемые локально, не передаются какой-либо третьей стороне, а обучение модели осуществляется локально – на источниках данных. Использование федеративного обучения для обнаружения вторжений позволяет решить проблему обучения на данных, которые принадлежат различным организациям, и которые в силу необходимости обеспечения защиты коммерческой или другой тайны, не могут быть выложены в открытый доступ. Таким образом, данный подход позволяет также расширить и разнообразить множество данных, на которых обучаются аналитические модели анализа, и повысить тем самым уровень детектируемости разнородных атак. Благодаря тому, что этот подход способен преодолеть вышеупомянутые проблемы, он активно используется для проектирования новых подходов к обнаружению вторжений и аномалий. Авторы исследуют существующие решения для обнаружения вторжений и аномалий на основе федеративного обучения, изучают их преимущества, а также формулируют открытые проблемы, связанные с его применением на практике. Особое внимание уделяется архитектуре предлагаемых систем, применяемым методам и моделям обнаружения вторжений, а также обсуждаются подходы к моделированию взаимодействия между множеством пользователей системы и распределению данных между ними. В заключении авторы формулируют открытые задачи, требующие решения для применения систем обнаружения вторжений, основанных на федеративном обучении, на практике.

Ключевые слова: обнаружение вторжений, аномалии, федеративное обучение, модели анализа, разделение данных.

1. Введение. Для своевременного и эффективного реагирования на различные информационные угрозы системы обнаружения вторжений (СОВ) и аномалий собирают и анализируют большие объемы данных. Большие объемы данных также требуются для обучения эффективной модели анализа, выполняющей выявление вторжений и аномалий. Зачастую такие данные могут включать различные типы конфиденциальной информации, включая персональные данные. В

Российской Федерации к персональным данным относятся данные, которые уникально определяют их владельца, а законодательства других стран расширяют это понятие, включая данные, относящиеся к устройствам, используемым человеком, такие как IP-адреса, уникальные идентификаторы устройств или приложений, а также данные о его местоположении. Таким образом, при построении систем обнаружения вторжений необходимо найти компромисс между конфиденциальностью собираемых и анализируемых данных и безопасностью субъекта персональных данных, и в большинстве случаев данная задача решается в пользу обеспечения безопасности, т.е. выполняется сбор, обработка и анализ всех данных, включая данные с ограниченным доступом. Парадигма федеративного обучения (ФО) позволяет решить эту проблему путем создания распределенных интеллектуальных систем, обеспечивающих конфиденциальность анализируемых данных [1, 2]. Суть ФО заключается в обучении аналитических моделей на наборах данных, которые находятся на разных источниках без обмена данными между ними. Более того, недавние исследования показали, что модели анализа, обученные в федеративном режиме, демонстрируют эффективность в обнаружении атак и аномалий, сравнимую с эффективностью моделей анализа, обученных классическим образом, т.е. на всем доступном наборе данных [3 – 5]. Тем не менее, ее применение связано с решением важных как практических, так и теоретических задач. К ним относятся следующие задачи [1, 6].

– Неоднородность устройств, которые генерируют анализируемые данные, что может привести к необходимости обработки различных форматов и атрибутов данных.

– Доступность устройств во время обучения модели анализа. Устройства, которые более стабильны и чаще доступны для обучения, могут оказывать более сильное влияние на результаты обучения.

– Распределение данных. Очевидно, что наборы данных, принадлежащие разным владельцам, могут иметь различные характеристики, в т.ч. иметь разное распределение меток. Такой случай распределения данных известен как случай зависимых, не идентично распределенных данных (not independent and identically distributed (non-IID) data). Он возникает в результате изменения и/или дрейфа концепций в наборах данных, а также может быть связан с разными объемами данных, хранящихся у разных владельцев.

– Настройка параметров системы ФО с учетом таких параметров как доступные вычислительные ресурсы клиентов, количество взаимодействующих клиентов, сложность обучаемой

модели анализа, которые определяют пропускную способность обучения.

Следует отметить, что, по мнению авторов, последняя задача тесно связана с проблемой доступных наборов данных, которые позволяют адекватно смоделировать как взаимодействие множества различных клиентов, так и различное распределение данных между ними, и оценить параметры системы с учетом этих факторов. В последнее время, проблема применения ФО для построения распределенных аналитических систем активно исследуется, и в научной литературе появилось множество исследований, посвященных различным теоретическим и прикладным аспектам ФО. Например, в [7 – 9] авторы исследуют задачу объединения (агрегирования) локальных моделей для формирования глобальной аналитической модели, устойчивой к неидентично распределенным данным. Проблемы построения систем ФО с учетом ограниченной пропускной способности сети клиентов обсуждаются в [10 – 12]. Например, Чжан и др. [12] решают задачу ускорения вычислений и снижения требований к вычислительным ресурсам, обусловленных использованием гомоморфного шифрования для дополнительной защиты передаваемых данных во время федеративного обучения. Другие аспекты безопасности и конфиденциальности ФО, такие как применение дифференциальной приватности, доверенных сред исполнения, изучаются в [13 – 17]. Существует также множество исследований, которые анализируют применимость ФО для решения различных практических задач. К настоящему времени исследователи предложили различные подходы на основе ФО для решения проблем цифрового здравоохранения [18, 19], безопасности [20 – 24], электронной коммерции [25 – 27], анализа текстов [28] и т.д.

Среди российских исследований следует отметить исследования, выполняемые под руководством И.И. Холода, которые посвящены разработке фреймворка федеративного обучения FL4J на языке программирования Java [29, 30].

Таким образом, несмотря на то, что ФО является относительно новой областью исследований, существует необходимость в систематизации разработанных подходов, посвященных различным аспектам ФО. В настоящей работе авторы исследуют существующие подходы к построению систем обнаружения вторжений на основе федеративного обучения, уделяя особое внимание используемым архитектурным решениям, применяемым моделям анализа, наборам данных и способам моделирования взаимодействия между множеством клиентов-владельцев данных, и схемам распределения

данных между ними. Следует отметить, что в силу того, что данное направление только начинает активно развиваться, основная мотивация данного исследования заключается в определении, какие решения для вышеупомянутых проблем уже предложены, насколько эффективно они решаются, и какие задачи предстоит еще решить. Сформулированные задачи и проблемы могут служить основой для более точной постановки целей и задач исследований, связанных с применением федеративного обучения для обнаружения вторжений и аномалий. Таким образом, основной вклад авторов заключается в:

– анализе архитектур федеративных систем обучения, включая поддерживаемые схемы распределения данных и требования к доступности клиентов и к их вычислительным ресурсам;

– анализе наборов данных, которые использовались для оценки системы, и подходов к моделированию федеративных систем;

– сравнительном анализе и систематизации предложенных подходов к обнаружению вторжений на основе федеративного обучения.

Статья организована следующим образом. В разделе 2 дано краткое описание концепции ФО и особенности систем, построенных на основе ФО. В разделе 3 обсуждаются типичные архитектурные решения СОВ. В разделе 4 представлена методология исследования и сравнительные критерии для анализа систем СОВ на основе ФО, в разделе представлена сравнительная характеристика выполненного аналитического обзора с другими обзорами по этой теме. В разделе 6 представлены результаты сравнительного анализа подходов к обнаружению вторжений на основе ФО. В конце статьи сформулированы основные преимущества использования федеративного обучения для обнаружения вторжений и задачи, которые еще предстоит решить.

2. Федеративное обучение. Ключевая идея ФО заключается в обучении локальных моделей непосредственно на клиентах, которые генерируют или владеют собственными данными, затем параметры локальных моделей объединяются для формирования глобальной модели, которая в процессе обучения рассылается всем взаимодействующим клиентам [1]. На рисунке 1 представлена схема федеративного обучения.

Таким образом, можно выделить три основных компонента систем, построенных на основе ФО: 1) клиенты, которые владеют данными и обучают локальную модель; 2) сервер, который координирует весь процесс обучения и вычисляет глобальную модель; 3) коммуникационно-вычислительная среда, которая обеспечивает

обмен параметрами модели. Исходя из этих компонент, можно выделить следующие ключевые характеристики аналитических систем, построенных с использованием ФО:

– схема взаимодействия между клиентами [18];

– вычислительные и сетевые ресурсы сотрудничающих владельцев данных;

– схема разделения данных между клиентами.

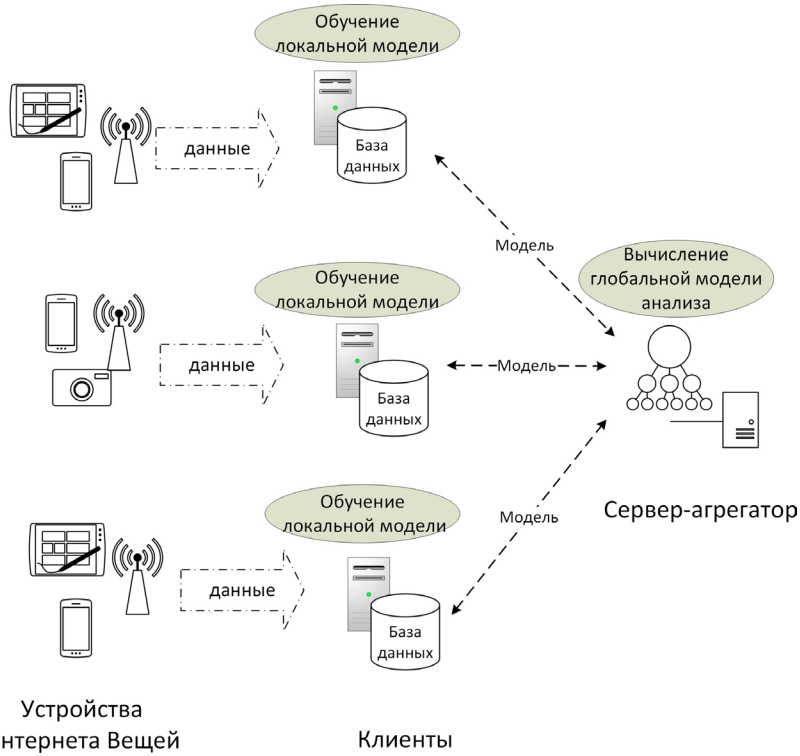


Рис. 1. Схема федеративного обучения

Схема взаимодействия между клиентами определяет, как организован процесс федеративного обучения. Различают централизованную и децентрализованную архитектуру системы ФО. В случае централизованной архитектуры один из взаимодействующих узлов выполняет роль агрегирующего сервера, который также координирует весь процесс обучения. Роль агрегирующего сервера может выполняться также некоторым доверенным лицом, который не

владеет данными. В случае децентрализованной системы ФО, функции агрегирующего сервера выполняются взаимодействующими клиентами [6]. Такая схема обучения еще известна как роевое обучение (swarm learning) [31]. На рисунке 2 показаны схемы взаимодействия во время процесса федеративного обучения.

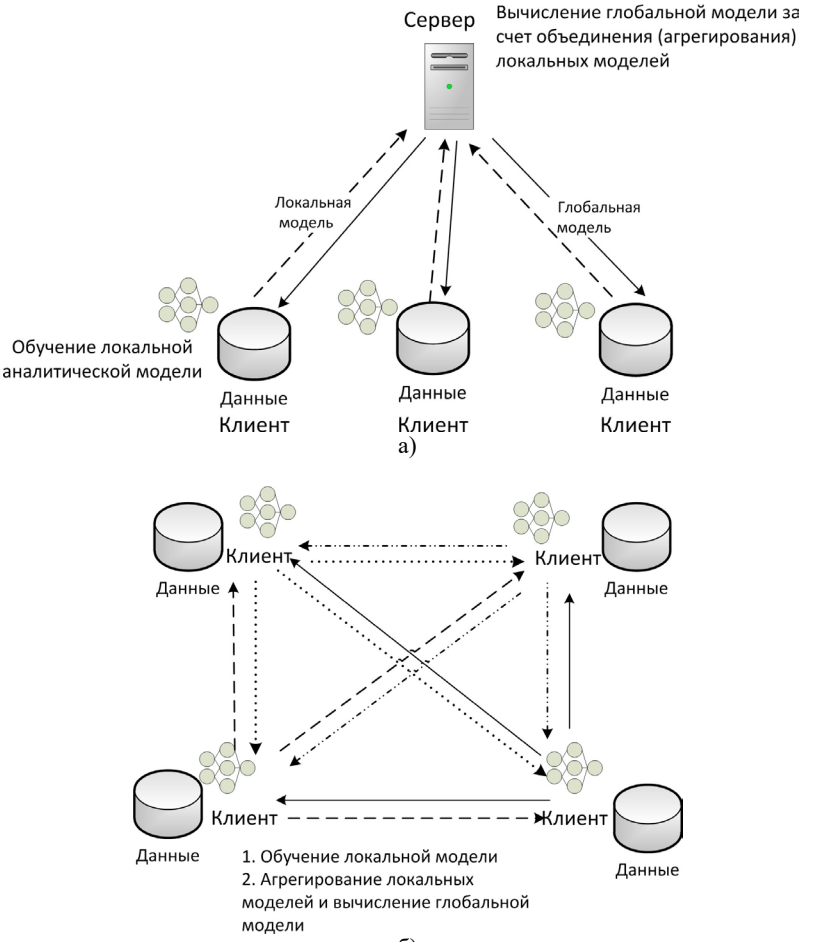


Рис. 2. Схемы взаимодействия между клиентами при ФО:
а) централизованная топология; б) децентрализованная топология

Необходимо отметить, что существуют также гибридные схемы коммуникации, которые представлены либо иерархией децентрализованных федераций, либо одноранговой сетью федераций с централизованной схемой коммуникации [18].

В зависимости от вычислительных ресурсов узлов-клиентов, их доступности во время процесса обучения, а также характеристик пропускной способности сети различают два типа объединения или федерации клиентов: федерация организаций (cross-silo) и федерация устройств (cross-device). Для федерации организаций характерно небольшое число клиентов, в роли которых обычно выступают организации и/или центры обработки данных. Для федерации устройств наоборот свойственно большое число клиентов с ограниченными вычислительными ресурсами, кроме того они могут появляться и отключаться в любой момент машинного обучения. Другой важной особенностью федеративного обучения является способ распределения данных. Семантически это понятие похоже на понятие «фрагментация данных», которое используется при организации физического хранения данных в распределенных хранилищах [32]. Обычно набор данных характеризуется двумя измерениями: 1) числом атрибутов и 2) числом записей в нем. Если клиенты имеют одинаковые наборы атрибутов, то данные разделены горизонтально. В случае вертикально распределенных данных клиенты имеют различные атрибуты данных для одного и того же набора образцов. Такой тип разбиения данных естественен для многих сценариев применения машинного обучения, например, оператор мобильной связи владеет данными о контактах человека, а финансовая организация может иметь информацию о его финансовом состоянии, и совместный анализ таких данных позволяет выявлять интересные схемы мошенничества. На рисунке 3 показаны схемы распределения данных между клиентами.

Кроме того, в реальных случаях данные могут быть разделены между клиентами частично вертикально, частично горизонтально − этот случай соответствует самому сложному типу распределения данных – гибридному. Описанные выше свойства систем ФО определяют различные сценарии использования систем ФО, включая также требования к производительности процесса обучения, выбору функции агрегирования и т.д.

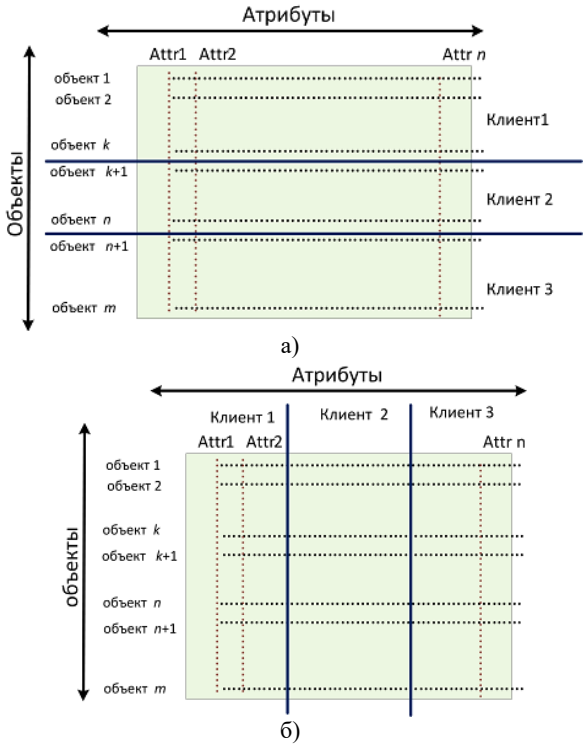


Рис. 3. Варианты распределения данных между клиентами: а) горизонтально распределённые данные; б) вертикально распределенные данные

3. Системы обнаружения вторжений. Система обнаружения вторжений (СОВ) является важной частью любой системы управления и обеспечения информационной безопасности и предназначена для обнаружения атак и аномалий в информационных системах. СОВ могут быть классифицированы в зависимости от типа анализируемых данных. В общем случае, принято выделять узловые и сетевые СОВ. Сетевая СОВ отслеживает и анализирует сетевой трафик, а узловая СОВ собирает и анализирует данные журналов операционной системы и приложений. Кроме того, существуют специализированные СОВ, разработанные для анализа данных определенных коммуникационных или других протоколов, а также гибридные решения, совмещающие анализ нескольких типов входных данных. Типичное архитектурное решение СОВ включает компоненты для сбора и обработки данных,

анализа, обнаружения атак (или аномалий) и реагирования на них (рисунок 4).

Базовые компоненты СОВ также включают репозиторий данных, в котором хранятся собранные исходные данные и сработавшие предупреждения, и базу знаний, содержащую информацию о правилах обнаружения атак, сигнатурах или шаблонах вредоносной активности. Существует два основных подхода к обнаружению атак или аномалий в информационной системе: сигнатурный и основанный на применении методов и моделей машинного обучения [33, 34]. Подходы на основе сигнатур обнаруживают атаки, используя методы сопоставления шаблонов для поиска известной атаки; поэтому база знаний об атаках должна постоянно обновляться для обеспечения высокого уровня обнаружения атак. Этот тип СОВ показывают высокую эффективность обнаружения атак известного типа; для обнаружения неизвестных атак или атак нулевого дня применяются подходы, основанные на методах и моделях машинного обучения (МО).

Рис. 4. Архитектура СОВ

В настоящее время исследователи предложили широкий спектр решений, использующих методы МО, включая адаптивную резонансную теорию [35], генетические алгоритмы [36, 37], методы кластеризации данных [38], нечеткой логики [36] и глубокие нейронные сети, такие как сверточные нейронные сети [39, 40], рекуррентные нейронные сети [41], глубокие автоэнкодеры [42] и т.д.

Дальнейшая классификация СОВ основана на том, как эти компоненты связаны и координируются в системе. Так, существуют монолитные, распределенные, иерархические и мультиагентные

системы [43, 44]. Распределенная СОВ предполагает, что каждый узел информационной системы имеет свою собственную СОВ, способную общаться с другими системами, кроме того имеется один выделенный сервер СОВ, который отвечает за окончательный анализ данных и принятие решений. В концепции иерархической СОВ локальные СОВ объединяются в кластеры, и каждый кластер имеет свой собственный головной узел, который отвечает за взаимодействие с другими кластерами [45]. Архитектура СОВ обычно выбирается исходя из типа контролируемой информационной системы и доступных вычислительных, энергетических ресурсов и пропускной способности сети. Например, типовой архитектурой СОВ для обнаружения вторжений в облаке является распределенная СОВ. Основной причиной такого выбора является необходимость анализа больших объемов сетевого трафика и ускорение вычислений на больших потоках данных. Для систем, построенных на основе технологии Интернета Вещей, примером которых служат системы «умного» дома, рекомендуемой архитектурой СОВ является распределенная иерархическая СОВ на основе агентов [39]. Это объясняется тем, что современные системы «умного» дома обычно поставляются вместе с набором облачных сервисов, предоставляемых производителем продукта. В этом случае программный агент СОВ устанавливается на домашнем маршрутизаторе с помощью специализированного программного обеспечения. Такой агент способен реализовывать различные функции, включая мониторинг потоков данных от датчиков, их предварительный анализ и пересылку результатов анализа головному компоненту СОВ, расположенному в облаке поставщика услуг. Типовая архитектура СОВ «умного» дома представлена на рисунке 5.

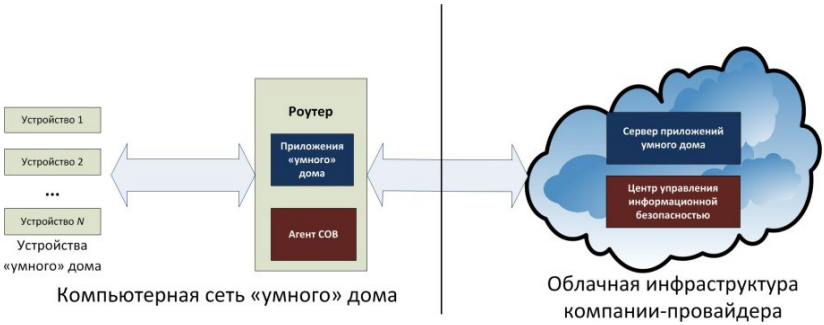


Рис. 5. Высокоуровневая архитектура иерархической распределенной СОВ для систем «умного» дома

Такая архитектура, с одной стороны, позволяет выбрать узел с более мощными ресурсами для установки СОВ, с другой стороны, поддерживает быстрый предварительный анализ локально генерируемых данных с последующим углубленным анализом, осуществляемым уже поставщиком услуг. Еще одним несомненным преимуществом такого подхода является возможность применения знаний об инцидентах безопасности в различных контролируемых системах «умного» дома. Единственным серьезным недостатком является значительный риск нарушения конфиденциальности пользователей «умного» дома из-за возможной утечки данных.

Иерархическая распределенная архитектура СОВ также предлагается для обнаружения атак и аномалий в киберфизических системах, таких как интеллектуальные энергетические сети [46 – 48]. Как правило, эти интеллектуальные сети состоят из различных взаимодействующих субъектов, включающих электростанции, конечных пользователей, представленных системами управления энергоснабжения «умного» дома, и юридических лиц, осуществляющих контроль за энергоснабжением. Иерархия локальных СОВ может быть построена либо на основе типа взаимодействующих субъектов [46, 47], либо на основе «границ вторжения», которые ограничивают распространение ущерба в случае успешной атаки [48].

Таким образом, можно выявить, что современные системы СОВ и аналитические системы, построенные на основе ФО, имеют два общих свойства, определяющих выбор архитектурного решения: это схема взаимодействия между клиентами (агентами) и требования к вычислительным ресурсам узлов с установленными интеллектуальными агентами. Архитектура децентрализованной системы ФО соотносится с распределенной СОВ с одноранговыми агентами, в то время как централизованная схема построения ФО близка к иерархической СОВ, в которой локальные агенты или кластеры одноранговых агентов связываются с главным компонентом СОВ для выработки окончательного решения. Характеристики облачной среды СОВ близки к вычислительным параметрам федерации организаций, когда взаимодействующие субъекты имеют достаточно вычислительных ресурсов и ресурсов хранения. СОВ для информационной системы на основе технологии Интернета Вещей должна учитывать те же ограничения, которые определяются характеристиками контролируемых устройств, что и система ФО для федерации устройств, т.е. энергопотребление, вычислительные ресурсы и ширину полосы пропускания. Для свойства, определяющего схему распределения данных в системах ФО, не существует

очевидного соответствия, хотя это свойство чрезвычайно важно при проектировании аналитической системы, основанной на принципах ФО. Большинство существующих систем ФО поддерживают горизонтально распределенные данные [49]. С точки зрения обнаружения вторжений и аномалий сетевые СОВ могут быть рассмотрены как клиенты с горизонтально распределенными данными, поскольку они обычно работают с определенным набором атрибутов, извлеченных из сетевого трафика, а СОВ для различных протоколов или приложений могут быть рассмотрены как случай вертикально распределенных данных, поскольку они работают с журналами различных приложений, имеющих разный формат и набор атрибутов. Аналогично, агенты СОВ в облачной среде должны иметь одинаковые наборы анализируемых атрибутов, в то время как агенты СОВ, развернутые в среде Интернета Вещей, должны быть способны обрабатывать различные признаки, характеризующие одни и те же объекты, поскольку они собирают данные с большого количества разнородных датчиков.

Основным преимуществом применения технологии ФО для построения СОВ является возможность снизить риски, связанные с обработкой конфиденциальных данных. Когда взаимодействующие субъекты представлены коммерческими организациями, критическими инфраструктурами, использование ФО позволяет повысить уровень доверия между ними и организацией, обеспечивающей информационную безопасность, поскольку в этом случае нет необходимости передавать конфиденциальные данные, и в то же время появляется возможность обмена знаниями об атаках и аномалиях с сохранением конфиденциальности. Для систем на основе Интернета Вещей применение ФО способно снизить объемы передаваемого сетевого трафика, что является важным фактором в условиях энергоэффективной сети, и обеспечивает возможность анализа большого количества разнородных устройств и датчиков.

Между тем применение федеративного обучения накладывает определенные требования к вычислительной мощности объекта, выполняющего локальное обучение модели, а также к объему памяти для хранения данных, необходимых для обучения. Поэтому при проектировании системы крайне важно оценить пропускную способность обучения системы анализа на основе ФО, характеризуемую через доступные вычислительные ресурсы клиентов, количество взаимодействующих клиентов, сложность обучаемой модели анализа. Необходимость рассмотрения этих вопросов определила основные цели данного исследования. Критерии сравнения

разработанных подходов к обнаружению вторжений на основе федеративного обучения и результаты исследования представлены в следующих разделах.

4. Методология поиска и анализа релевантных работ. Исследование и анализ СОВ на основе федеративного обучения выполнялось на основе рекомендаций по систематическому анализу научной литературы [50], которые предполагают определение 1) вопросов, решаемых в ходе исследования, 2) стратегии поиска и отбора научной литературы и 3) критериев включения и исключения работ в исследование. Ключевой задачей исследования является анализ подходов к обнаружению вторжений на основе ФО с возможной оценкой практической применимости ФО для решения задачи обнаружения вторжений, поэтому были сформулированы следующие вопросы исследования (ВИ).

ВИ1: Какая схема коммуникации для организации ФО – централизованная или децентрализованная – используется при построении СОВ?

ВИ2: Какая схема распределения данных – горизонтальная или вертикальная – учитывается при построении СОВ?

ВИ3: Какие наборы данных используются для тестирования предложенных схем распределения данных, каким образом происходит моделирование распределения данных между клиентами? Учитывается ли случай не идентично распределенных данных?

ВИ4: Какие методы и модели МО используются для обнаружения атак и/или аномалий?

ВИ5: Какие метрики используют авторы для оценки разработанных решений?

ВИ6: Какие программные библиотеки ФО используются для построения прототипов СОВ?

Эти вопросы также определили критерии оценки подходов к обнаружению вторжений, представленных в отобранных работах. Стратегия поиска научно-исследовательских работ была сформулирована как на основе исследовательских вопросов, так и в соответствии с рекомендациями [50]. Были проанализированы исследования, опубликованные в научных журналах и конференциях, не учитывались статьи в ненаучных журналах или коммерческие документы, презентации и слайды. Поиск осуществлялся как по англоязычным библиографическим системам, так и в русскоязычной научной электронной библиотеке eLibrary. Таким образом, для формирования множества исследуемых работ были выполнены следующие шаги.

Шаг 1. Формирование ключевых слов на русском и английском языках.

Шаг 2. Поиск публикаций на основе набора ключевых слов в электронных базах данных: eLibrary (поиск по ключевым словам на русском языке), IEEE Xplore, и ScienceDirect (поиск по ключевым словам на английском языке). Результатом этого шага является первоначальный набор публикаций.

Шаг 3. Проверка исходного набора публикаций на соответствие критериям включения и исключения. Эти критерии позволяют оценить, будет ли публикация включена в окончательную выборку для последующего рассмотрения. В качестве ключевых слов были определены следующие слова:

– на русском языке:

федеративное обучение AND (аномалии OR атаки OR вторжений) AND (компьютерные сети OR информационные системы),

– на английском языке:

federated learning AND (anomaly detection OR attack detection OR intrusion detection).

Были определены следующие критерии включения (КВ) и исключения (КИ):

КВ1. В работе четко описан подход к обнаружению аномалий и вторжений на основе федеративного обучения, обсуждается архитектура решения, модель анализа, описан сценарий эксперимента и используемые наборы данных, описана методика визуализации данных, т.е. даны исходные данные и способ построения графического представления.

КВ2. Публикация имеет четкую структуру. Методы представлены четко и наглядно.

КВ3. Публикация написана на русском (английском) языке с соблюдением стилистических и грамматических норм.

КИ1. В работе представлен обзор работ или сравнение методов.

КИ2. Представленный подход плохо описан, а публикация не имеет четкой структуры и/или изложена ненаучным языком. Общая схема этапа сбора исходных данных представлена на рисунке 6. На рисунке 7 представлена статистика публикаций, сгруппированных по их типу, за последние три года по базам IEEE Xplore и ScienceDirect. Следует отметить, что на русском языке работ по исследуемой тематике на момент выполнения исследования обнаружено не было. Это позволяет говорить о том, что данная тема исследований недостаточно хорошо изучена и исследована российскими учеными.

Рис. 6. Схема процесса отбора научных публикаций, посвященных проблеме применения федеративного обучения для задач обнаружения вторжений и аномалий. Все числовые значения даны на август 2022

5. Сравнение с другими обзорами. Есть несколько обзоров по федеративному обучению для обнаружения вторжений в Интернете вещей, среди которых следует отметить [51, 52], в которых рассматриваются теоретические проблемы и будущие направления исследований, связанных с применением ФО для обнаружения атак и аномалий. Аналитический обзор, представленный в статье [52], довольно обширен. Авторы проанализировали 15 исследовательских работ, связанных с СОВ на основе ФО, но авторы сосредоточены на исследовании особенностей предложенных подходов, не сравнивают их в контексте параметров, специфических для ФО, такие как архитектура ФО, модель МО, подход к разбиению набора данных для моделирования взаимодействия нескольких клиентов, функция агрегации, и т.д. В [51] авторы описали и сравнили 12 работ, связанных с применением ФО для повышения эффективности СОВ. Авторы рассмотрели не только предлагаемые подходы, но также представили используемые наборы данных, модели МО, и специфические настройки федеративного обучения, такие как число раундов агрегации, а также функция агрегирования. Однако данная информация представлена кратко, основной акцент сделан на разрабатываемый авторами подход. Таким образом, настоящий обзор является наиболее полным, в нем рассмотрено более 40 работ, кроме того, подробно исследованы вопросы, связанные с моделированием взаимодействия между устройствами (клиентами), и схемой распределения данных, рассматриваются подходы к моделированию неидентично распределенных данных.

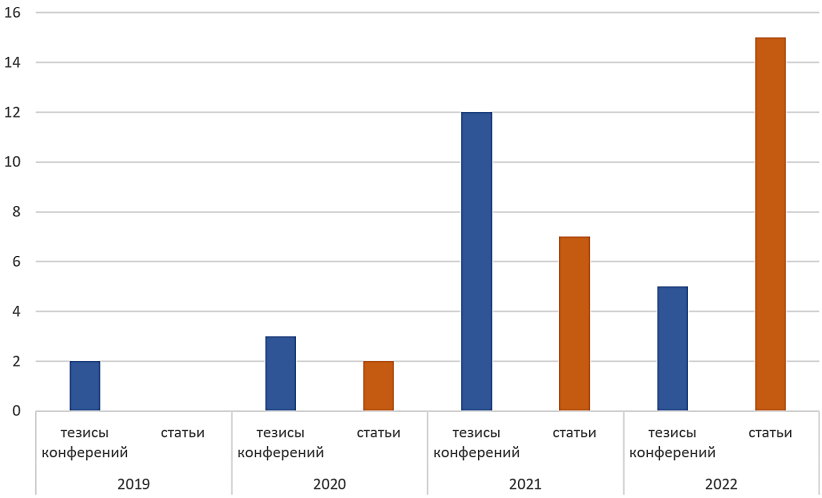


Рис. 7. Статистика публикаций, сгруппированных по их типу, за последние 3 года по базам IEEE Xplore и ScienceDirect

6. Подходы к обнаружению вторжений, построенных на принципах федеративного обучения. Обобщенные результаты выполненного анализа исследовательских работ представлены в таблицах 1–5. Результаты сгруппированы по предметным областям, для которых предложены СОВ на основе ФО: сетевая безопасность (таблица 1), безопасность IoT-устройств (таблица 2), медицинские устройства (таблица 3), промышленные киберфизические системы (таблица 4) и транспортные интеллектуальные системы (таблица 5). В таблице 6[1] представлен анализ особенностей настроек федеративного обучения, используемых для построения СОВ.

Таблица 1. Сравнительный анализ работ (сетевая безопасность)

Ref.	Модель анализа	Набор данных	Оцениваемые показатели
[53]	НС (сверточная НС)	набор данных, сгенерированный 20 участниками проекта LAN-Security Monitoring Project[2]	Точность (accuracy), полнота, точность (precision), F-мера
[54]	НС (LSTM НС)	улучшенный SEA [55] (набор команд сервера)	Точность (accuracy), полнота, точность (precision), F-мера, loss (значение функции потерь)

[1] Пустые ячейки в таблице говорят о том, что этот вопрос в работе не рассматривался.

[2] https://www.lan-security.net/

Продолжение Таблицы 1

Ref.	Модель анализа	Набор данных	Оцениваемые показатели
[56]	полносвязная НС	NSL-KDD [57]	Точность (accuracy), loss (значение функции потерь)
[58]	НС (автоэнкодер)	Aegean Wi-Fi Intrusion Dataset (AWID) [59]	Точность (accuracy); объем передаваемого трафика (Мб)
[60]	НС (сверточная НС)	CICIDS-2017 [61]	Точность (accuracy)
[62]		NSL-KDD [57]	Точность (accuracy), TPR, FPR; время обучения модели в федеративном режиме
[63]		N-BaIoT [64]	Точность (accuracy), полнота, точность (precision), F-мера; объем передаваемого сетевого трафика во время обучения
[65]		NSL-KDD [57]	Точность (accuracy), FPR; время обучения модели в федеративном режиме
[66]		UNSW-NB15 [67]; CICIDS-2018 [61]	Точность (accuracy), loss (значение функции потерь)
[68]		CIC-DDoS-2019 [69]	Точность (accuracy), полнота, точность (precision), F-мера
[70]		NSL-KDD [57]	Точность (accuracy); вознаграждение в обучении с подкреплением
[71]	НС	NSL-KDD [57]	Точность (accuracy), полнота, точность (precision), F-мера, ROC-AUC; время обучения модели в федеративном режиме
[72]	НС	TON-IoT-v2 [73], UNSW-NB15-v2 [67], BoT-IoT-v2 [74], CSECIC-IDS2018-v2 [61]	Точность (accuracy), полнота, точность (precision), F-мера, FPR
[75]		NSL-KDD [57]	Точность (accuracy)
[76]	ансамбль 4 НС (LSTM НС с блоками GRU с разным размером окна)	сетевые данные протокола Modbus [77]	Точность (accuracy), полнота, точность (precision), F-мера; время обучения модели в федеративном режиме
[78]	логистическая регрессия	TON-IoT [73]	Точность (accuracy); время на генерацию шума в механизме дифференциальной приватности
[79]	НС с блоками GRU и SVM классификатором в качестве выходного слоя	KDD CUP99 [80]; CICIDS2017 [61]; WSN-DS[3]	Точность (accuracy), FPR, F-мера; число раундов агтрегирования для оценки скорости обучения модели
[81]	Градиентный бустинг на деревья решений (GBDT)	CIC-DDoS-2019 [69]	Точность (accuracy), FNR; теоретическая оценка объема предаваемой информации
[82]	GAN НС + сверточная НС	NSL-KDD [57], KDD CUP99 [80], UNSW-NB15 [67]	Точность (accuracy), полнота, точность (precision), F-мера, потери (loss), AUC, скорость сходимости

[3] https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds

Таблица 2. Сравнительный анализ работ (IoT устройства)

Ref.	Модель анализа	Набор данных	Оцениваемые показатели
[83]	НС (автоэнкодер)	UNSW-NB15 [67]	F-мера
[84]		NSL-KDD [57]	Точность (accuracy)
[85]	НС (рекуррентная нейронная сеть с блоками GRU)	собственный набор данных от IoT устройств (33 устройства), атаки выполнялись путем заражения ботнетом Mirai	FPR, TPR; время обучения модели и время классификации объекта
[86]	НС	CICIDS-2017 [61], CICDDoS-2019 [69]	FPR, FNR
[87]	НС (сверточная НС)	CICIDS-2017 [61]; NSL-KDD [57]; набор данных от IoT устройств [88]	Точность (accuracy), TPR, FPR
[89]	НС (полносвязная НС)	NSL-KDD [57]	Точность (accuracy), полнота, точность (precision), F-мера
[90]	НС (автоэнкодер)	N-BaIoT [64] – сетевой трафик от 9 устройств, атаки выполнялись путем заражения BASHLITE и ботнетом Mirai	Точность (accuracy), полнота, точность (precision), F-мера
[22]	НС (полносвязная сеть и автоэнкодер)		Точность (accuracy), полнота, точность (precision), F-мера; теоретические оценки генерируемого трафика и вычислительной нагрузки во время обучения

Таблица 3. Сравнительный анализ работ (медицинские устройства)

Ref.	Модель анализа	Набор данных	Оцениваемые показатели
[91]	иерархическая LSTM НС	NSL-KDD [57]; TON-IoT [73]	Точность (accuracy), полнота, точность (precision), F-мера
[92]	НС (сверточная)	набор данных, сгенерированный с использованием симулятора реакции на глюкозу [93]	Точность (accuracy), полнота, точность (precision), F-мера
[94]	GAN-сеть	Набор медицинских данных CHARIS [95]; UNSW-NB [67]	Точность (accuracy), полнота, точность (precision), F-мера, ROC-AUC

Таблица 4. Сравнительный анализ работ (промышленные КФС)

Ref.	Модель анализа	Набор данных	Оцениваемые показатели
[96]	НС (сверточная нейронная сеть с блоками GRU)	набор данных от системы газоснабжения [97]	Точность (accuracy), полнота, точность (precision), F-мера
[98]	НС (автоэнкодер)		Точность (accuracy), полнота, точность (precision)
[99]	НС (автоэнкодер), Трансформер, и преобразование Фурье	набор данных от системы газоснабжения [100]; SWaT [101]; HAI [102]; измерения потребляемой мощности [103]; измерения сердцебиения [103]; измерения частоты дыхания пациента [103]; координаты правой руки при выполнении различных действий [103]; измерения тока для космического шаттла [103]; информация о пассажирах Нью-Йоркского такси [104]	Полнота, точность (precision), F-мера; использование памяти, использование графического процессора, время выполнения, пропускная способность обучения, потребляемая мощность

Таблица 5. Сравнительный анализ работ (интеллектуальные транспортные системы)

Ref.	Модель анализа	Набор данных	Оцениваемые показатели
[105]	НС	KDD Cup99 [80]	Точность (accuracy), полнота, точность (precision); метрики, характеризующие временные затраты на применение технологии блокчейн, в частности, время генерации блока блокчейна
[106]	НС (трансформер)	TON-IoT [73]; Набор данных ль взлома автомобилей	Полнота, точность (precision), F-мера; время обучения модели в федеративном режиме
[107]	случайный лес	OTIDS[4]	Точность (accuracy), полнота, точность (precision), F-мера; время обучения модели в федеративном режиме; загрузка ЦПУ и память (RAM)

[4] https://ocslab.hksecurity.net/Dataset/CAN-intrusion-dataset

Таблица 6. Анализ настроек ФО при построение СОВ

Ref.	Алгоритм агрегирования	Наличие тестбеда/ используемый фреймворк ФО	Другие особенности СОВ
[20,58,60]	FedAvg		
[53, 84]	FedAvg		
[87]	FedAvg		использование трансферного обучения (transfer learning)
[81, 86]	FedAvg		
[108]	FedAvg		гомоморфное шифрование (схема Пейе)
[68]	FedAvg	да/Flower FL	дифференциальная приватность
[83,89,98]	FedAvg		
[56]	FedSGD, FedAVG		
[70]	FedSGD	да/PySyft	использование трансферного обучения (transfer learning); устойчивость к data poisoning атакам
[78]	Fed+		дифференциальная приватность
[72]	Fed+, CM+		
[79]	FedAGRU		оценка устойчивости СОВ к атакам на изменение меток обучающего набора
[22]	FedAVG (агрегирование каждую итерацию и агрегирование каждые n эпох), FED CM (на основе координатно-медианного градиентного спуска)		оценка устойчивости СОВ к атакам на изменение меток обучающего набора
[63, 71] [62,65,66, 75,91,107]			
[76, 106]		да/PySyft FL	
[94]		да/Flower FL	
[90]		да/PySyft FL	
[92]	FedAVG	свой тестбед	применение для выявления аномалий
[54]	FedAvg		набор данных журналов, содержащих команды сервера
[99]	FedAvg [109]	FedML	применение для выявления аномалий
[82]		свой тестбед	использование трансферного обучения (transfer learning)

6.1. Архитектурные решения по построению СОВ на основе федеративного обучения. Наиболее часто используемым архитектурным решением ФО для построения СОВ является централизованная схема обучения, в которой глобальная модель формируется отдельным выделенным доверенным сервером. Данная схема используется для построения иерархических распределенных СОВ в системах Интернета вещей и СОВ, развернутых в облачных средах [58, 60, 62, 63, 65, 66, 68, 70, 83 – 87, 89, 91]. Типовая архитектура СОВ на основе централизованного ФО представлена на рисунке 8. В ней ряд узлов осуществляют сбор данных от устройств и выполняют обучения локальной модели анализа для выявления атак и/или аномалий, далее локально обученные модели отсылаются выделенному серверу безопасности, который формирует глобальную модель, агрегируя локальные. Данный процесс осуществляется итеративно, поэтому необходимо учитывать пропускную способность канала, связывающего клиентов и сервер безопасности. На рисунке 8 в качестве клиента выступает платформа приложений мобильных граничных вычислений (MEC, Mobile Edge Computing), которая собирает данные от одной подсети IoT устройств [87, 107], однако клиентами могут быть шлюзы безопасности локальных сетей, как в [20], а также сами устройства [58, 83, 98], однако в последнем случае следует учитывать вычислительные ресурсы, которыми они обладают.

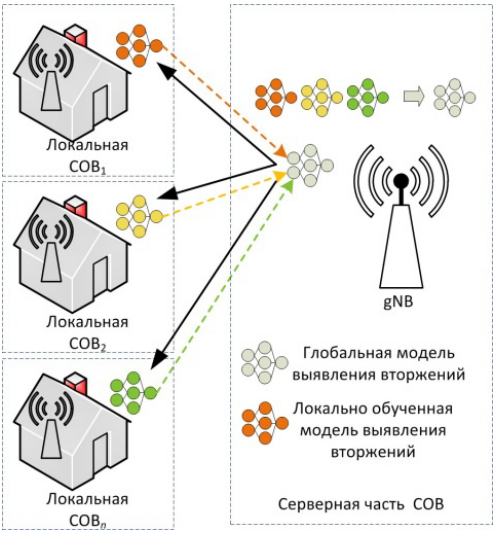


Рис. 8. Распределенная СОВ с централизованной схемой взаимодействия между клиентами [67]

Для масштабных, географически распределенных вычислительных сетей предложена иерархическая архитектура СОВ, в которой вычисление глобальной модели анализа, используемой для выявления аномалий, также формируется иерархически на уровне сегментов [53, 91]. Все участники процесса объединяются в группы или сегменты, и каждая группа выполняет обучение некоторой промежуточной модели в федеративном режиме обучения, после чего глобальная модель вычисляется путем агрегирования таких промежуточных моделей. При этом, на каждом этапе формирования глобальной модели, происходит оценка того, насколько веса локальной модели каждого участника отличаются от весов глобальной модели, и если отличия в весах моделей превышают некоторый заданный порог, то такой клиент исключает из группы [79]. Такое решение позволяет повысить устойчивость моделей выявления атак, обучаемых на несбалансированных наборах данных [53, 79]. Децентрализованная схема ФО предложена для построения СОВ, разрабатываемых для интеллектуальных транспортных систем [105 – 107]. Данное решение обусловлено, в первую очередь, географической распределенностью таких систем, и высокой мобильностью транспортных средств, которые являются неотъемлемыми компонентами таких систем. Транспортное средство, перемещаясь в пространстве, подключается к разным базовым станциям или интеллектуальным придорожным устройствам, получая таким образом актуальную дорожную информацию и обновленную модель обнаружения атак и аномалий. Типовая архитектура СОВ в этом случае имеет двухуровневую систему: на нижнем уровне транспортные средства загружают от базовых станций модели анализа, используемые в СОВ, и обновляют их с учетом собираемых ими данных, после чего отправляют их обратно базовым станциям. Базовые станции получают локальные модели от подключенных к ним устройств, проверяют их корректность, и участвуют в формировании новой глобальной модели. Таким образом, на верхнем уровне, центральный агрегирующий сервер безопасности замещен множеством распределенных взаимодействующих базовых станций. Такое решение позволяет повысить устойчивость СОВ к вредоносным действиям, направленным на нарушение функционирования центрального узла и снизить риски утечки данных, в т. ч. персональных. На рисунке 9 представлена схема построения СОВ на основе децентрализованного ФО.

Несколько иной подход к построению СОВ на основе ФО для самоуправляемых транспортных систем предложен в [107]. Авторы

предложили передать функции агрегирования локальных моделей на уровень конечных узлов, т.е. транспортным средствам, а сбор данных и обучение локальных моделей осуществлять на уровне базовых станций, т.к. это позволяет снизить вычислительную нагрузку на граничные устройства, поскольку операция агрегирования значительно менее ресурсоемкая, чем процесс локального обучения модели анализа. В обоих случаях для обеспечения целостности и неизменности локальных и глобальных моделей в условиях распределенных вычислений применяются технологии блокчейна. Использование блокчейна с одной стороны решает задачи, связанные с верификацией и проверкой аутентичности моделей анализа, с другой стороны, порождает новые задачи, обусловленные применением ресурсоемких операций, специфичных для блокчейна, таких как шифрование, дешифрация, генерация ключей, выработка консенсуса и т.д.

Рис. 9. Распределенная схема СОВ на основе децентрализованного ФО [105]

6.2. Схемы разделения данных между клиентами СОВ и используемые наборы данных. Анализ работ показал, что представленные в литературе СОВ поддерживают только горизонтальную схему распределения данных, т.е. все клиенты обладают одинаковым набором атрибутов. Данное решение выглядит естественным с учетом того, что в большинстве случаев входные данные представлены сетевым трафиком или статистическими характеристиками, сформированными на основе анализа сетевых потоков. В качестве наборов данных в основном используются такие

наборы как CICIDS2017 [61], NSL-KDD [57], горизонтальное разделение данных моделируется путем группировки пакетов по IP адресам источников сетевых потоков или случайным образом. В работах [96, 107] в качестве входных данных используются данные специализированных коммуникационных протоколов, таких как ModBus, CAN. В них также формируется единый для всех участников набор атрибутов. Например, в [107] применяется частотный анализ сообщений CAN-шины с последующим применением преобразования Фурье для формирования множества анализируемых признаков. В [71, 85] проблему формирования общего набора атрибутов для разнородных устройств предлагается решать путем определения множества атрибутов для каждого типа устройства, таким образом, модель анализа обучается в федеративном режиме на «горизонтальных» данных для каждого типа устройства, а в основе СОВ лежит ансамбль таких моделей. Также было показано, что такое решение позволяет значительно снизить уровень ложно положительных срабатываний [71]. В [84] предлагается выполнять обучение модели в федеративном режиме для выявления определенного типа атак, что предполагает определение набора анализируемых атрибутов для каждого типа атаки, который является одинаковым для всех клиентов. Такое решение обеспечивает горизонтальное разделение данных между клиентами.

В [99], несмотря на то, что авторы используют достаточно разнообразные наборы данных – сетевые данные, данные от датчиков системы очистных сооружений [101] и т.д., схема разделения данных является горизонтальной: для моделирования взаимодействия между множеством сторон набор данных последовательно делится на несколько частей, что позволяет сохранить логическую структуру временных рядов.

Случай вертикального распределения данных среди взаимодействующих клиентов для построения СОВ практически не изучен. Исключение составляет работа [4], в которой предпринята попытка моделирования данной схемы разделения данных. Авторы использовали набор данных SWAT [101], который содержит данные от шести различных технологических процессов, описываемых разными наборами сенсоров и актуаторов. Для моделирования вертикального распределения данных между клиентами, он был поделен по процессам. Обучение глобальной модели анализа для выявления атак осуществлялось с помощью специализированного фреймворка FATE [110], и, несмотря на полученные высокие показатели точности обнаружения атак, авторы продемонстрировали, что текущая

реализация схемы федеративного обучения не может быть использована для оперативного выявления вторжений в силу высоких требований к вычислительным ресурсам и времени, необходимому как для обучения такой модели, так и для классификации данных, подаваемых ей на вход.

6.3. Моделирование неидентично распределенных данных. Влияние неидентично распределенных данных исследуется довольно часто, и можно выделить два основных способа моделирования такого распределения данных. В первом случае один набор данных делится между клиентами, и каждый клиент получает определенный тип атак (или несколько типов атак) [63, 71]. Например, для моделирования взаимодействия 8 устройств с неидентично распределенными данными набора NSL-KDD был разделен следующим образом:

– «нормальный» трафик был поделен на 8 частей;

– трафик с атаками был разбит по типу атак, а затем каждое полученное подмножество записей было разделено между двумя клиентами, т.е. устройства № 0 и № 1 имели данные по атаке на отказ в обслуживании (DoS атаке), устройства № 2 и № 3 – по атакам типа Probe, устройства № 4 и № 5 – по атакам типа R2L, и устройства № 6 и № 7 – по атакам U2R.

В случае, когда речь идет о выявлении аномалий, тип атаки не учитывается, и неиндентично распределенные данные моделируются, варьируя процентное содержание нормальных или аномальных данных в наборе данных одного устройства. Например, в [70] для моделирования неидентично распределенных данных «нормальный» трафик был распределен по 10 устройствам в процентном отношении следующим образом: 25%, 50%, 75%, 25%, 50%, 75%, 25%, 50%, 75%, 50%, соответственно, тип атаки не учитывался.

Во втором случае используются разные наборы данных с одинаковыми параметрами, и каждый набор играет роль данных одного устройства [72, 87]. Например, в [72] используются 4 разных набора данных – ToNIoT-v2 [73], UNSW-NB15-v2 [67], BoT-IoT-v2 [74], CSECIC-IDS2018-v2 [61], для моделирования взаимодействия четырех шлюзов безопасности, установленных в разных беспроводных сетях. Для выравнивания множества атрибутов из наборов данных были извлечены все признаки, связанные с сетевыми потоками. Каждый набор данных характеризуется разным составом атак, кроме того, различна их доля присутствия в обучающих выборках. Было показано, что ФО позволяет достичь достаточно высоких показателей обнаружения атак (минимальное значение точности (precision) на тестовых наборах данных – 90.20%, а максимальное – 99.98%) при

сравнительно низком уровне ложно положительных срабатываний (максимальное значение этого показателя на одном из наборов равно 5.38%, а минимальное – 0.04%). Таким образом, этот же подход к подготовке обучающих выборок взаимодействующих устройств может быть использован для оценки обобщающей способности СОВ, построенных на ФО, т.е. способности обнаруживать новые виды атак, которых нет в исходном обучающем наборе отдельного участника (клиента) такой системы. Однако в общем случае точность обнаружения атак зависит от репрезентативности таких атак в обучающих наборах данных [98].

Проблема оценки обобщающей способности аналитической модели, обученной федеративном режиме, представлена не достаточно полно. На рисунке 10 представлено распределение работ с учетом выполненной оценки способности аналитической модели, обученной в федеративном режиме, выявлять новые типы атак, которые отсутствуют в обучающей выборке клиента.

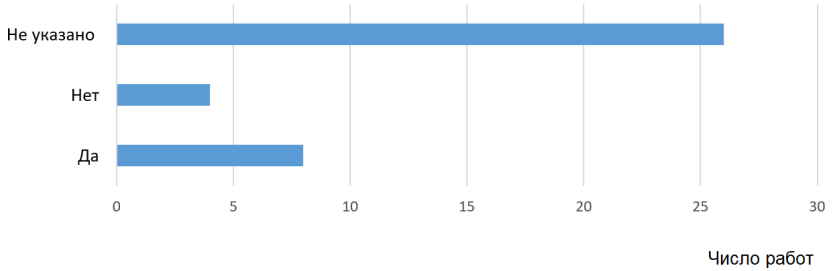


Рис. 10. Доля работ, в которых выполнялась оценка способности модели, обученной в федеративном режиме, к выявлению новых типов атак, которых нет в обучающей выборке клиента

6.4. Методы машинного обучения, используемых в СОВ на основе ФО. В основном для обнаружения атак и аномалий в СОВ на основе ФО используются глубокие нейронные сети: полносвязные, сверточные сети, рекуррентные сети, а также сети долгой краткосрочной памяти (LSTM-сети). Методы классического машинного обучения, такие как деревья решений, логистическая регрессия, методы опорных векторов практически не используются. Этот факт в первую очередь объясняется тем, что само ФО было предложено для обучения глубоких нейронных сетей, и функции агрегирования локальных моделей в основном разработаны для таких типов моделей анализа. Для выявления аномалий в основном применяются нейронные сети автоэнкодеры [83, 98].

Предложены интересные решения по использованию ФО в сочетании с трансферным обучением, т.е. использованием предобученных моделей. Ключевой идеей использования трансферного обучения является применение знаний, полученных в одной области к новой предметной области, для ускорения процесса обучения модели анализа, повышения ее точности и снижения вычислительных ресурсов. Трансферное федеративное обучение позволяет ускорить процесс обучения локальных моделей. Это достигается путем обучения исходной модели на открытом наборе данных, и использовании ее в качестве исходной для обучения локальных моделей [70, 87]. Например, в [70] исходная сверточная сеть обучается на наборе NSL-KDD [57], затем она передается в качестве предобученной клиентам, и во время локального обучения выполняется подстройка только последнего полносвязного слоя на другом наборе данных UNSW-NB15 [67].

Следует также отметить, что для формирования глобальной модели чаще всего используется алгоритм агрегирования FedSGD, который предполагает агрегирование параметров локальной модели в конце каждой эпохи локального обучения, и FedAvg, отличающийся тем, что он позволяет задать количество эпох локального обучения, по завершении которых выполняется вычисление параметров глобальной модели. Алгоритм FedAvg является основным способом формирования моделей анализа в СОВ на основе ФО, поскольку является более эффективным с точки зрения сетевого взаимодействия между клиентами. Между тем показано, что и FedSGD, и FedAvg плохо обрабатывают разнородные и неидентично распределенные данные: эффективность моделей анализа, полученных с их помощью, значительно снижается при обучении на таких данных [72].

6.5. Метрики оценки разработанных решений. Для оценки разработанных решений в основном используются метрики, связанные с оценкой эффективности моделей анализа, такие как доля верно классифицированных объектов, доля ложно положительных срабатываний, чувствительность классификатора и т.д. В ряде работ выполняется оценка времени обучения модели в централизованном и федеративном режиме, и авторы исследований показывают, что время обучения модели в федеративном режиме значительно снижается, что в условиях ограниченности энергетических ресурсов IoT устройств выглядит достаточно привлекательно. Однако практически ни в одной работе не уточняются условия проведения данного эксперимента, в частности, не указывается размер обучающей выборки, используемой при централизованном обучении, и размеры данных, которыми

владеют взаимодействующие участники при федеративном обучении; а также режим применения ФО. Очевидно, что время обучения моделей анализа зависит в том числе и от размера обучающей выборки, и если выборка данных, находящаяся на устройстве при федеративном обучении, является частью исходной, то можно предположить, что длительность обучения при прочих равных настройках может быть значительно меньше, а при равных размерах обучающих выборок может оказаться даже больше за счет необходимости синхронизации клиентов и передачи данных в процессе обучения. Последний параметр сильно зависит от того, в каком режиме развернуто ФО. Оно может быть использовано в симуляционном или реальном федеративном режиме. В первом случае вся система, включая взаимодействующие узлы, развертывается на одном вычислительном узле, сетевое взаимодействие практически отсутствует, такой режим используется для выбора и настройки параметров ФО и аналитической модели. В федеративном режиме узлы разворачиваются на нескольких физических или виртуальных узлах, в этом случае имеет место настоящее сетевое взаимодействие. Между тем, разница в пропускной способности обучения в федеративном и симуляционном режимах может быть значительной в зависимости от типа модели анализа и настроек функции агрегирования [49]. Только в незначительной части работ [22, 99, 107] авторы исследуют другие параметры ФО, такие как загрузка ЦПУ, объем передаваемого сетевого трафика, объем используемой оперативной памяти, при этом в [22] данные параметры оцениваются в контексте применения технологии блокчейна, в частности исследуются параметры механизма консенсуса при генерации нового блока, а в [107] даны теоретические оценки ожидаемого сетевого трафика и загрузки ЦПУ во время обучения. Между тем, большая часть исследовательских работ позиционируют ФО как способ построения СОВ именно в сетях IoT-устройств [22, 83 – 87], которые могут характеризоваться ограниченными вычислительными и энергетическими ресурсами, низкой полосой пропускания канала связи, поэтому исследование таких параметров является критически важным при определении архитектуры СОВ, параметров ФО, и непосредственно модели анализа. Исследование перечисленных параметров может быть выполнено при развертывании СОВ на основе ФО на экспериментальном стенде состоящем как из виртуальных, так и физических устройств.

6.6. Использование программных средств и фреймворков для построения экспериментальных стендов. В большей части

работ данные по развертыванию и использованию экспериментальных стендов отсутствуют. В [68, 76, 90, 94, 106] используются специализированные библиотеки для построения ФО, в частности PySyft, Flower. Согласно [49], PySyft v0.6 и ниже не поддерживается реальный федеративный режим, а последующие версии данного фреймворка реализуют несколько иную концепцию распределенного обучения, в которой сущности, имеющие роль Data Analyst (аналитика данных), удаленно обучают модель на данных, принадлежащих другой сущности – владельцу данных (Data owner), таким образом, взаимодействие между несколькими сущностями, владеющими данными, практически отсутствует. Библиотека Flower поддерживает и симуляционный и федеративный режимы обучения, а также предоставляет достаточно широкий спектр различных функций агрегирования, что делает ее использование предпочтительным при тестировании подходов к обнаружению вторжений и аномалий на основе ФО.

6.7. Приватность данных и устойчивость СОВ к атакам на изменение разметки. Федеративное обучение, как и классическое машинное обучение, уязвимо к ряду атак: состязательным атакам, связанным с изменением функциональности обучаемой модели анализа, и атакам на логический вывод, целью которых является получение информации об используемых наборах данных и/или их свойствах. Однако в отличие от централизованной схемы обучения, когда все данные собираются и контролируются одним субъектом, в случае федеративного обучения данными и их качеством управляют их владельцы, таким образом, расширяется поверхность атаки, и у злоумышленника появляется больше возможностей для ее успешного проведения. С учетом этого, вопросы, связанные с уязвимостями машинного обучения, в СОВ, построенных на федеративном обучении, приобретают особую актуальность. Вместе с тем систематический анализ литературы показал, что данный вопрос практически не исследован. Наиболее полное исследование представлено в [22], авторы изучили влияние нескольких типов атак, в т.ч. подмену меток обучающей выборки ("отравление" данных), изменение градиентов локальных моделей ("отравление" модели) и показали, что без использования функций агрегирования, устойчивых к неидентично распределенным данным, достаточно одного атакующего клиента в федерации, чтобы нарушить сходимость глобальной модели.

Вопросы приватности наборов данных также практически не исследованы, в работах [68, 78] выполнены оценки влияния на точность глобальной модели механизмов дифференциальной приватности,

авторы показали, что снижение точности глобальной модели при добавлении шума к градиентам локальной модели не значительно, тем не менее не выработаны единые рекомендации по выбору параметров дифференциальной приватности, которая бы обеспечивала заданный уровень точности глобальной модели анализа при допустимой вероятности компрометации обучающих наборов. В [108] проблема конфиденциальности данных решается путем применения гомоморфного шифрования (схема Пейе), эксперименты показывают, что в этом случае не происходит потери точности глобальной модели, однако авторы не указывают влияние шифрования на время ее формирования. Вместе с тем в [16] экспериментально показано, что время обучения и объем сетевого трафика сильно зависят от протокола шифрования, сетевой трафик при обучении полносвязной нейронной сети на наборе данных, состоящем из 10000 строк-векторов, и размере батча, равного 100, может достигать от 1.78 ГБ до 36 ГБ.

7. Выводы: преимущества использования и открытые задачи. Проведенные исследования показали, что федеративное обучение может быть успешно использовано для построения распределенных систем обнаружения вторжений, которые обладают несколькими важными свойствами. Во-первых, такие системы позволяют обрабатывать данные с ограниченным доступом, например, персональные данные и/или конфиденциальные данные. К таким данным также относятся данные от критических инфраструктур, в т. ч. сетевой трафик и данные от технологических процессов, и применение ФО позволяет настраивать модели обнаружения вторжений и аномалий на таких наборах без компрометации их конфиденциальности, стимулируя тем самым взаимодействия между различными организациями и киберфизическими объектами. Особенно перспективным видятся решения по построению СОВ, сочетающие ФО с методами трансферного обучения.

Во-вторых, модели выявления аномалий и/или атак, обученные в федеративном режиме на нескольких наборах данных, которые содержат разные типы атак, обладают более высоким уровнем детектирования ранее неизвестных атак по сравнению с моделями, обученными на одном наборе данных. Таким образом, такие модели обладают более высокой обобщающей способностью, формируемой за счет расширения обучающей выборки.

В-третьих, возможность построения децентрализованной СОВ на основе ФО позволяет решить проблему нарушения работоспособности центрального узла, управляющего процессом обнаружения вторжения и/или аномалий, включая переобучение

соответствующих моделей анализа. Данная проблема известна как единая точка отказа (single point of failure), для которой характерно наличие одного критического компонента, выход из строя которого приводит к нарушению функционирования всей системы. В случае же ФО, способности системы к обнаружению вторжений сохраняются, они лишь ограничены возможностями локальных моделей анализа. Основной открытой проблемой является отсутствие подходов к построению ФО, позволяющих эффективно выполнять обучение на вертикально распределенных данных. Такой тип распределения данных характерен для киберфизических систем, в которых объекты представлены неоднородными наборами датчиков, и соответственно, их поведение описывается различными атрибутами. Представленные решения по обнаружению вторжений на основе ФО предложены только для горизонтально разделенных данных, а именно для анализа сетевых данных; соответственно, задача выявления аномалий в технологических процессах методами федеративного обучения остается нерешенной.

Также следует отметить, что в большинстве работ для формирования общей глобальной аналитической модели используются два классических подхода к агрегированию локальных моделей – это алгоритмы FedSGD и FedAvg. Вместе с тем в [22, 72] было показано, что разные алгоритмы агрегирования могут оказывать значительное влияние на обобщающую способность глобальных аналитических моделей. Таким образом, сценарии экспериментальной оценки ФО для построения СОВ должны также включать анализ различных алгоритмов агрегирования, в т. ч. тех, которые доказуемо устойчивы к неидентично распределенным данным, например, Fed+ и FEDMO [111].

Из всего вышесказанного можно сделать вывод, что существует назревшая необходимость в создании и стандартизации методологии оценки СОВ, построенных на основе принципов ФО, которая будет определять требования как к наборам данных для тестирования, их распределению (в том числе эксперименты с неидентично распределенными данными), оцениваемым метрикам, так и учитывать характеристики анализируемой СОВ, включая различные алгоритмы агрегирования, архитектуру и устойчивость к разного рода атакам, и характеристики среды проведения экспериментов. Также остается ряд открытых проблем, большей частью связанных с практическими аспектами применения ФО, в частности, остаются открытыми вопросы, связанные с определением требований к вычислительным ресурсам, пропускной способности канала связи, что особенно важно для систем, построенных на основе технологии Интернета Вещей.

Фактически, текущий подход к анализу применимости ФО к обнаружению аномалий и вторжений заключается в использовании современного и актуального набора данных и моделированию его распределения по множеству взаимодействующих клиентов. В таких экспериментах в основном исследуются различные сценарии распределения данных, и оценивается их влияние на точность обнаружения аномалий и атак. Вместе с тем эксперименты должны включать также описания топологии сети, архитектуру СОВ, характеристики вычислительных узлов. Это позволит получить реалистичные оценки по вычислительной эффективности и длительности обучения модели в федеративном режиме. Решением данной проблемы является развертывание СОВ на основе ФО на экспериментальном стенде, сочетающем как виртуальные, так и физические устройства. Примером такого стенда может служить программно-аппаратный комплекс, описанный в [68].

В заключение также стоит отметить, что в настоящий момент большинство исследований в области применения ФО для построения СОВ сфокусировано на задаче обнаружения вторжений и классификации атак. Задача, связанная с разработкой технологии применения контрмер на основе ФО, практически не представлена в научной литературе. Вместе с тем, применение ФО может значительно повысить эффективность подсистем предотвращения вторжений, особенно развернутых в программно-определяемых сетях и реализующих технологии самовосстановления и самозащиты.

Литература

1. McMahan B., Moore E., Ramage D., Hampson S., Arcas B.A. Communication-Efficient Learning of Deep Networks from Decentralized Data // Artificial intelligence and statistics. 2017. pp. 1273–1282.
2. Lwakatare L.E., Raj A., Bosch J., Olsson H.H., Crnkovic I.A Taxonomy of Software Engineering Challenges for Machine Learning Systems: An Empirical Investigation (Eds.: Kruchten P., Fraser S., Coallier F.) // Agile Processes in Software Engineering and Extreme Programming: Proceedings of 20th International Conference. 2019. pp. 227–243.
3. Antonakakis M., April T., Bailey M., Bernhard M., Bursztein E., Cochran J., Durumeric Z., Halderman J.A., Invernizzi L., Kallitsis M., Kumar D., Lever C., Ma Z., Mason J., Menscher D., Seaman C., Thomas K., Zhou Y. Understanding the Mirai Botnet // 26th USENIX Security Symposium (USENIX Security 17). 2017. pp. 1093–1110.
4. Novikova E., Doynikova E., Golubev S. Federated Learning for Intrusion Detection in the Critical Infrastructures: Vertically Partitioned Data Use Case // Algorithms. 2022. vol. 15(4). no. 104. DOI: 10.3390/a15040104.
5. Ludwig H, et al. IBM Federated Learning: an Enterprise Framework White Paper V0.1. ArXiv preprint arXiv:2007.10987. 2020.

6. Lo S.K. Lu Q., Zhu L., Paik H.Y., Xu X., Wang C. Architectural Patterns for the Design of Federated Learning Systems // Journal of Systems and Software. 2022. vol. 191. no. 111357.
7. Sannara E.K., Portet F., Lalanda P., German V.E.G.A. A Federated Learning Aggregation Algorithm for Pervasive Computing: Evaluation and Comparison // IEEE International Conference on Pervasive Computing and Communications (PerCom). 2021. pp. 1–10. DOI: 10.1109/PERCOM50583.2021.9439129.
8. Yurochkin M., Agarwal M., Ghosh S., Greenewald K., Hoang N., Khazaeni Y. Bayesian Nonparametric Federated Learning of Neural Networks // International conference on machine learning. 2019. pp. 7252–7261.
9. Mansour A.B., Carenini G., Duplessis A., Naccache D. Federated Learning Aggregation: New Robust Algorithms with Guarantees. 21st IEEE International Conference on Machine Learning and Applications (ICMLA). 2022. pp. 721–726. DOI: 10.48550/ARXIV.2205.10864.
10. Shahid O., Pouriyeh S., Parizi R.M., Sheng Q.Z., Srivastava G., Zhao L. Communication Efficiency in Federated Learning: Achievements and Challenges // ArXiv preprint arXiv:2107.10996. 2021.
11. Juvekar C., Vaikuntanathan V., Chandrakasan A. GAZELLE: A Low Latency Framework for Secure Neural Network Inference // Proceedings of the 27th USENIX Security Symposium (USENIX Security 18). 2018. pp. 1651–1669.
12. Zhang C., Li S., Xia J., Wang W., Yan F., Liu Y. BatchCrypt: Efficient Homomorphic Encryption for Cross-Silo Federated Learning // Proceedings of the 2020 USENIX Conference on Usenix Annual Technical Conference. USENIX annual technical conference (USENIX ATC 20). 2020. pp. 493–506.
13. Kairouz P., et al. Advances and Open Problems in Federated Learning. Foundations and Trends in Machine Learning. 2021. vol. 14. no. 1–2. pp. 1–210.
14. Truex S., Liu L., Chow K.H., Gursoy M.E., Wei W. LDP-Fed: federated learning with local differential privacy // Proceedings of the Third ACM International Workshop on Edge Systems, Analytics and Networking. 2020. pp. 61–66.
15. Shokri R., Shmatikov V. Privacy-preserving deep learning // Proceedings of the 22nd ACM SIGSAC conference on computer and communications security. 2015. pp. 1310–1321. DOI: 10.1109/ALLERTON.2015.7447103.
16. Novikova E, Fomichov D., Kholod I., Filippov E. Analysis of Privacy-Enhancing Technologies in Open-Source Federated Learning Frameworks for Driver Activity Recognition // Sensors. 2022. vol. 22(8). no. 2983. DOI: 10.3390/s22082983.
17. Запечников С. Модели и алгоритмы конфиденциального машинного обучения // Безопасность информационных технологий. 2020. Т. 27. № 1. С. 51–67. DOI: 10.26583/bit.2020.1.05.
18. Rieke N., Hancox J., Li W., Milletarì F., Roth H.R., Albarqouni S., Bakas S., Galtier M.N., Landman B.A., Maier-Hein K., Ourselin S., Sheller M., Summers R.M., Trask A., Xu D., Baust M., Cardoso M.J. The future of digital health with federated learning // NPJ Digital Medicine. 2020. vol. 3. no. 119. DOI: 10.1038/s41746-020-00323-1.
19. Antunes R.S., André da Costa C., Küderle A., Yari I.A., Eskofier B. Federated Learning for Healthcare: Systematic Review and Architecture Proposal // ACM Transactions on Intelligent Systems and Technology (TIST). 2022. vol. 13(4). no. 54. DOI: 10.1145/3501813.
20. Nguyen T.D., Marchal S., Miettinen M., Fereidooni H., Asokan N., Sadeghi A.R. DIoT: A Federated Self-learning Anomaly Detection System for IoT // IEEE 39th International Conference on Distributed Computing Systems (ICDCS). 2019. pp. 756–767.
21. Li B., Wu Y., Song J., Lu R., Li T., Zhao L. DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber-Physical Systems // IEEE Transactions on

Industrial Informatics. 2020. vol. 17. no. 8. pp. 5615–5624. DOI: 10.1109/TII.2020.3023430.
22. Rey V., Sánchez P.M.S., Celdrán A.H., Bovet G. Federated learning for malware detection in IoT devices // Computer Networks. 2022. vol. 204. no. 108693. DOI: 10.1016/j.comnet.2021.108693.
23. Huong T.T., Bac T.P., Long D.M., Thang B.D., Binh N.T., Luong T.D., Phuc T.K. LocKedge: Low-Complexity Cyberattack Detection in IoT Edge Computing // IEEE Access. 2021. vol. 9. pp. 29696–29710. DOI: 10.1109/ACCESS.2021.3058528.
24. Khoa T.V., Saputra Y.M., Hoang D.T., Trung N.L., Nguyen D., Ha N.V., Dutkiewicz E. Collaborative Learning Model for Cyberattack Detection Systems in IoT Industry 4.0 // IEEE Wireless Communications and Networking Conference (WCNC). 2020. pp. 1–6. DOI: 10.1109/WCNC45663.2020.9120761.
25. Long G., Tan Y., Jiang J., Zhang C. Federated Learning for Open Banking // Federated Learning: Privacy and Incentive. 2020. pp. 240–254.
26. Ahmed U., Srivastava G., Lin J.C.-W. Reliable customer analysis using federated learning and exploring deep-attention edge intelligence // Future Generation Computer Systems. 2022. vol. 127. pp. 70–79. DOI: 10.1016/j.future.2021.08.028.
27. Li J., Cui T., Yang K., Yuan R., He L., Li M. Demand Forecasting of E-Commerce Enterprises Based on Horizontal Federated Learning from the Perspective of Sustainable Development // Sustainability. 2021. vol. 13(23). no. 13050. DOI: 10.3390/su132313050.
28. Дзюба В.И. Применение концепции федеративного обучения для решения задачи классификации текста // Процессы управления и устойчивость. 2022. Т. 9. № 1. С. 210–214.
29. Гонсалес П.Ю., Холод И.И. Архитектура многоагентных систем для федеративного обучения. Компьютерные инструменты в образовании. 2022. № 1. С. 30–45. DOI: 10.32603/2071-2340-2022-1-30-45.
30. Холод И.И., Ефремов М.А. Разработка архитектуры универсального фреймворка федеративного обучения // Программные продукты и системы. 2022. Т. 35. № 2. С. 263–272. DOI: 10.15827/0236-235X.138.263-272.
31. Swarm learning: Driving advances both practical and profound. URL: https://www.hpe.com/us/en/insights/articles/swarm-learning-driving- advances-both-practical-and-profound-2111.html. (accessed 24.10.2022).
32. Bellatreche L., Boukhalfa K., Richard P. Data Partitioning in Data Warehouses: Hardness Study, Heuristics and ORACLE Validation // Data Warehousing and Knowledge Discovery: Proceedings of the 10th International Conference on Data Warehousing and Knowledge Discovery. 2008. pp. 87–96. DOI: 10.1007/978-3-540-85836-2_9.
33. Khraisat A., Gondal I., Vamplew P., Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges // Cybersecurity. 2019. vol. 2. no. 1. pp. 1–22. DOI: 10.1186/s42400-019-0038-7.
34. Kotenko I., Saenko I., Branitskiy A. Framework for Mobile Internet of Things Security Monitoring Based on Big Data Processing and Machine Learning // IEEE Access. 2018. vol. 6. pp. 72714–72723. DOI: 10.1109/ACCESS.2018.2881998.
35. Bukhanov D.G., Polyakov V.M. Detection of network attacks based on adaptive resonance theory // Journal of Physics: Conference Series. 2018. vol. 1015(4). no. 042007. DOI: 10.1088/1742-6596/1015/4/042007.
36. Yunwu W. Using Fuzzy Expert System Based on Genetic Algorithms for Intrusion Detection System // International Forum on Information Technology and Applications. 2009. vol. 2. pp. 221–224. DOI: 10.1109/IFITA.2009.107.

37. Dave M.H., Sharma S.D. Improved Algorithm for Intrusion Detection Using Genetic Algorithm and SNORT. International Journal of Emerging Technology and Advanced Engineering. 2014. vol. 4. no. 8. pp. 273–276.
38. Ranjan R., Sahoo G. A New Clustering Approach for Anomaly Intrusion Detection // International Journal of Data Mining and Knowledge Management Process (IJDKP). 2014. vol. 4. no. 2. pp. 29–38. DOI: 10.5121/ijdkp.2014.4203.
39. Li Z., Qin Z., Huang K., Yang X., Ye S. Intrusion Detection Using Convolutional Neural Networks for Representation Learning // International conference on neural information processing. 2017. pp. 858–866.
40. Hu J., Liu C., Cui Y. An Improved CNN Approach for Network Intrusion Detection System // International Journal of Network Security. 2021. vol. 23. no. 4. pp. 569–575.
41. Vinayakumar R., Soman K., Poornachandran P. Evaluation of Recurrent Neural Network and Its Variants for Intrusion Detection System IDS // International Journal of Information System Modeling and Design (IJISMD). 2017. vol. 8. no. 3. pp. 43–63.
42. Song Y., Hyun S., Cheong Y.-G. Analysis of Autoencoders for Network Intrusion Detection // Sensors. 2021. vol. 21(13). no. 4294. DOI: 10.3390/s21134294.
43. Gajewski M., Batalla J.M., Mastorakis G., Mavromoustakis C.X. A distributed IDS architecture model for Smart Home systems // Cluster Computing. 2019. vol. 22. pp. 1739–1749.
44. Shterenberg S.I., Poltavtseva M.A. A Distributed Intrusion Detection System with Protection from an Internal Intruder // Automatic Control and Computer Sciences. 2018. vol. 52. pp. 945–953.
45. Schueller Q., Basu K., Younas M., Patel M., Ball F. A Hierarchical Intrusion Detection System using Support Vector Machine for SDN Network in Cloud Data Center // 28th International Telecommunication Networks and Applications Conference (ITNAC). 2018. pp. 1–6. DOI: 10.1109/ATNAC.2018.8615255.
46. Saghezchi F.B., Mantas G., Ribeiro J., Al-Rawi M., Mumtaz S., Rodriguez J. Towards a secure network architecture for smart grids in 5G era // 13th International Wireless Communications and Mobile Computing Conference (IWCMC). 2017. pp. 121–126. DOI: 10.1109/IWCMC.2017.7986273.
47. Zhang Y. Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids // IEEE Transactions on Smart Grid. 2011. vol. 2. no. 4. pp. 796–808. DOI: 10.1109/TSG.2011.2159818.
48. Javed Y., Felemban M., Shawly T., Kobes J., Ghafoor A. A Partition-Driven Integrated Security Architecture for Cyberphysical Systems // Computer. 2020. vol. 53. no. 3. pp. 47–56. DOI: 10.1109/MC.2019.2914906.
49. Kholod I., Yanaki E., Fomichev D., Shalugin E., Novikova E., Filippov E., Nordlund M. Open-Source Federated Learning Frameworks for IoT: A Comparative Review and Analysis // Sensors. 2020. vol. 21(1). no. 167. DOI: 10.3390/s21010167.
50. Kitchenham B.A. Procedures for Performing Systematic Reviews // Keele, UK, Keele University. 2004. vol. 33. pp. 1–26.
51. Campos E.M., Saura P.F., González-Vidal A., Hernández-Ramos J.L., Bernabé J.B., Baldini G., Skarmeta A. Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges // Computer Networks. 2022. vol. 203. no. 108661. DOI: 10.1016/j.comnet.2021.108661.
52. Agrawal S., Sarkar S., Aouedi O., Yenduri G., Piamrat K., Alazab M., Bhattacharya S., Reddy Maddikunta P.K., Gadekallu T.R. Federated Learning for Intrusion Detection System: Concepts, Challenges and Future Directions // Computer Communications. 2022. vol. 195. pp. 346–361. DOI: 10.1016/j.comcom.2022.09.012

53. Sun Y., Ochiai H., Esaki H. Intrusion Detection with Segmented Federated Learning for Large-Scale Multiple LANs // International Joint Conference on Neural Networks (IJCNN). 2020. pp. 1–8. DOI: 10.1109/IJCNN48605.2020.9207094.
54. Zhao R., Yin Y., Shi Y., Xue Z. Intelligent intrusion detection based on federated learning aided long short-term memory // Physical Communication. 2020. vol. 42. no. 101157. DOI: 10.1016/j.phycom.2020.101157.
55. Kholidy H.A., Baiardi F., Hariri S. DDSGA: A Data-Driven Semi-Global Alignment Approach for Detecting Masquerade Attacks // IEEE Transactions on Dependable and Secure Computing. 2014. vol. 12. no. 2. pp. 164–178. DOI: 10.1109/TDSC.2014.2327966.
56. Saadat H., Aboumadi A., Mohamed A., Erbad A., Guizani M. Hierarchical Federated Learning for Collaborative IDS in IoT Applications // 10th Mediterranean Conference on Embedded Computing (MECO). 2021. pp. 1–6. DOI: 10.1109/MECO52532.2021.9460304.
57. University of New Brunswick dataset. NSL-KDD dataset. URL: https://www.unb.ca/cic/datasets/nsl.html. (accessed 15.05.2022).
58. Cetin B, Lazar A., Kim J., Sim A., Wu K. Federated Wireless Network Intrusion Detection // IEEE International Conference on Big Data (Big Data). 2019. pp. 6004–6006. DOI: 10.1109/BigData47090.2019.9005507.
59. Kolias C., Kambourakis G., Stavrou A., Gritzalis S. Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset // IEEE Communications Surveys and Tutorials. 2015. vol. 18. no. 1. pp. 184–208. DOI: 10.1109/COMST.2015.2402161.
60. Ayed M.A., Talhi C. Federated Learning for Anomaly-Based Intrusion Detection // International Symposium on Networks, Computers and Communications (ISNCC). 2021. pp. 1–8. DOI: 10.1109/ISNCC52172.2021.9615816.
61. Sharafaldin I., Lashkari A.H., Ghorbani A.A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization // International Conference on Information Systems Security and Privacy (ICISS). 2018. vol. 1. pp. 108–116.
62. Luo J., Yang X., Mohammed M.N. Federation Learning for Intrusion Detection Methods by Parse Convolutional Neural Network // Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT). 2022. pp. 1–7. DOI: 10.1109/ICAECT54875.2022.9807989.
63. Zhao R., Wang Y., Xue Z., Ohtsuki T., Adebisi B., Gui G. Semisupervised Federated-Learning Based Intrusion Detection Method for Internet of Things // IEEE Internet of Things Journal. 2022. vol. 10. pp. 8645–8657. DOI: 10.1109/JIOT.2022.3175918.
64. Meidan Y., Bohadana M., Mathov Y., Mirsky Y., Shabtai A., Breitenbacher D., Elovici Y. N-BaIoT-Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders // IEEE Pervasive Computing. 2018. vol. 17. no. 3. pp. 12–22. DOI: 10.1109/MPRV.2018.03367731.
65. Yang X., Luo J., Mohammed M.N. Federation Learning of Optimized Convolutional Neural Network Structure for Intrusion Detection // Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT). 2022. pp. 1–7. DOI: 10.1109/ICAECT54875.2022.9807964.
66. Shi J., Ge B., Liu Y., Yan Y., Li S. Data Privacy Security Guaranteed Network Intrusion Detection System Based on Federated Learning // IEEE INFOCOM 2021 – IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). 2021. pp. 1–6. DOI: 10.1109/INFOCOMWKSHPS51825.2021.9484545.
67. Moustafa N., Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set) // Military Communications and Information Systems Conference (MilCIS). 2015. pp. 1–6. DOI: 10.1109/MilCIS.2015.7348942.

68. Duy P.T., Van Hung T., Ha N.H., Do Hoang H., Pham V.H. Federated learning-based intrusion detection in SDN-enabled IIoT networks // 8th NAFOSTED Conference on Information and Computer Science (NICS). 2021. pp. 424–429. DOI: 10.1109/NICS54270.2021.9701525.
69. Sharafaldin I., Lashkari A.H., Hakak S., Ghorbani A.A. Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy // International Carnahan Conference on Security Technology (ICCST). 2019. pp. 1–8. DOI: 10.1109/CCST.2019.8888419.
70. Cheng Y., Lu J., Niyato D., Lyu B., Kang J., Zhu S. Federated Transfer Learning With Client Selection for Intrusion Detection in Mobile Edge Computing // IEEE Communications Letters. 2022. vol. 26. no. 3. pp. 552–556. DOI: 10.1109/LCOMM.2022.3140273.
71. Wang N., Chen Y., Hu Y., Lou W., Hou Y.T. FeCo: Boosting Intrusion Detection Capability in IoT Networks via Contrastive Learning // IEEE INFOCOM 2022 – IEEE Conference on Computer Communications. 2022. pp. 1409–1418. DOI: 10.1109/INFOCOM48880.2022.9796926.
72. Popoola S.I., Gui G., Adebisi B., Hammoudeh M., Gacanin H. Federated Deep Learning for Collaborative Intrusion Detection in Heterogeneous Networks // IEEE 94th Vehicular Technology Conference (VTC2021-Fall). 2021. pp. 1–6. DOI: 10.1109/VTC2021-Fall52928.2021.9625505.
73. Alsaedi A., Moustafa N., Tari Z., Mahmood A., Anwar A. TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems // IEEE Access. 2020. vol. 8. pp. 165130–165150. DOI: 10.1109/ACCESS.2020.3022862.
74. Koroniotis N., Moustafa N., Sitnikova E., Turnbull B. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset // Future Generation Computer Systems. 2019. vol. 100. pp. 779–796. DOI: 10.1016/j.future.2019.05.041.
75. Al-Marri N.A.A.-A., Ciftler B.S., Abdallah M.M. Federated Mimic Learning for Privacy Preserving Intrusion Detection // IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom). 2020. pp. 1–6.
76. Mothukuri V., Khare P., Parizi R.M., Pouriyeh S., Dehghantanha A., Srivastava G. Federated-Learning-Based Anomaly Detection for IoT Security Attacks // IEEE Internet of Things Journal. 2021. vol. 9. no. 4. pp. 2545–2554. DOI: 10.1109/JIOT.2021.3077803.
77. Frazao I., Abreu P.H., Cruz T., Araújo H., Simões P. Denial of Service Attacks: Detecting the Frailties of Machine Learning Algorithms in the Classification Process // Critical Information Infrastructures Security 13th International Conference (CRITIS 2018). 2019. pp. 230–235.
78. Ruzafa-Alcazar P., Fernández-Saura P., Mármol-Campos E., González-Vidal A., Hernández-Ramos J.L., Bernal-Bernabe J., Skarmeta A.F. Intrusion Detection Based on Privacy- Preserving Federated Learning for the Industrial IoT // IEEE Transactions on Industrial Informatics. 2021. vol. 19. no. 2. pp. 1145–1154. DOI: 10.1109/TII.2021.3126728.
79. Chen Z., Lv N., Liu P., Fang Y., Chen K., Pan W. Intrusion Detection for Wireless Edge Networks Based on Federated Learning // IEEE Access. 2020. vol. 8. pp. 217463–217472. DOI: 10.1109/ACCESS.2020.3041793.
80. KDD dataset. URL: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. (accessed 15.03.2022).
81. Dong T., Qiu H., Lu J., Qiu M., Fan C. Towards Fast Network Intrusion Detection based on Efficiency-preserving Federated Learning // IEEE Intl Conf on Parallel and Distributed Processing with Applications, Big Data and Cloud Computing,

Sustainable Computing & Communications, Social Computing and Networking (ISPA/BDCloud/SocialCom/SustainCom). 2021. pp. 468–475. DOI: 10.1109/ISPA-BDCloud-SocialCom-SustainCom52081.2021.00071.

82. Tabassum A., Erbad A., Lebda W., Mohamed A., Guizani M FEDGAN-IDS: Privacy-preserving IDS using GAN and Federated Learning // Computer Communications. 2022. vol. 192. pp. 299–310. DOI: 10.1016/j.comcom.2022.06.015.
83. Aouedi O., Piamrat K., Muller G., Singh K. FLUIDS: Federated Learning with semi-supervised approach for Intrusion Detection System // IEEE 19th Annual Consumer Communications and Networking Conference (CCNC). 2022. pp. 523–524. DOI: 10.1109/CCNC49033.2022.9700632.
84. Qin Y., Kondo M. Federated Learning-Based Network Intrusion Detection with a Feature Selection Approach // International Conference on Electrical, Communication, and Computer Engineering (ICECCE). 2021. pp. 1–6. DOI: 10.1109/ICECCE52056.2021.9514222.
85. Nguyen T.D., Marchal S., Miettinen M., Fereidooni H., Asokan N., Sadeghi A.R. DIoT: A Federated Self-learning Anomaly Detection System for IoT // IEEE 39th International Conference on Distributed Computing Systems (ICDCS). 2019. pp. 756–767.
86. Qin T., Cheng G., Chen W., Lei X. FNEL: An Evolving Intrusion Detection System Based on Federated Never-Ending Learning // 17th International Conference on Mobility, Sensing and Networking (MSN). 2021. pp. 239–246. DOI: 10.1109/MSN53354.2021.00047.
87. Fan Y., Li Y., Zhan M., Cui H., Zhang Y. IoTDefender: A Federated Transfer Learning Intrusion Detection Framework for 5G IoT // IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE). 2020. pp. 88–95. DOI: 10.1109/BigDataSE50710.2020.00020.
88. Kang H., Ahn D.H., Lee G.M., Yoo J., Park K.H., Kim H.K. IoT network intrusion dataset. IEEE Dataport. 2019. vol. 10. DOI: 10.21227/q70p-q449.
89. Mirzaee P.H., Shojafar M., Pooranian Z., Asefy P., Cruickshank H., Tafazolli R. FIDS: A Federated Intrusion Detection System for 5G Smart Metering Network // 17th International Conference on Mobility, Sensing and Networking (MSN). 2021. pp. 215–222. DOI: 10.1109/MSN53354.2021.00044.
90. Regan C., Nasajpour M., Parizi R.M., Pouriyeh S., Dehghantanha A., Choo K.K.R. Federated IoT security attack detection using decentralized edge data // Machine Learning with Applications. 2022. vol. 8. no. 100263. DOI: 10.1016/j.mlwa.2022.100263.
91. Singh P., Gaba G. S., Kaur A., Hedabou M., Gurtov A. Dew-Cloud-Based Hierarchical Federated Learning for Intrusion Detection in IoMT // IEEE Journal of Biomedical and Health Informatics. 2022. vol. 27. no. 2. pp. 722–731. DOI: 10.1109/JBHI.2022.3186250.
92. Astillo P.V. Federated intelligence of anomaly detection agent in IoTMD-enabled Diabetes Management Control System // Future Generation Computer Systems. 2022. vol. 128. pp. 395–405. DOI: 10.1016/j.future.2021.10.023.
93. Astillo P.V., Jeong J., Chien W.C., Kim B., Jang J., You I. SMDAps: A specification-based misbehavior detection system for implantable devices in artificial pancreas system // Journal of Internet Technology. 2021. vol. 22. no. 1. pp. 1–11.
94. Siniosoglou I., Sarigiannidis P., Argyriou V., Lagkas T., Goudos S.K., Poveda M. Federated Intrusion Detection In NG- IoT Healthcare Systems: An Adversarial Approach // ICC 2021 – IEEE International Conference on Communications. 2021. pp. 1–6. DOI: 10.1109/ICC42927.2021.9500578.

95. Kim N.H., Krasner A., Kosinski C., Wininger M., Qadri M., Kappus Z., Danish S., Craelius W. Trending autoregulatory indices during treatment for traumatic brain injury // Journal of Clinical Monitoring and Computing. 2016. vol. 30. pp. 821–831.
96. Li B., Wu Y., Song J., Lu R., Li T., Zhao L. DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber–Physical Systems // IEEE Transactions on Industrial Informatics. 2020. vol. 17. no. 8. pp. 5615–5624. DOI: 10.1109/TII.2020.3023430.
97. Morris T., Gao W. Industrial Control System Traffic Data Sets for Intrusion Detection Research // Critical Infrastructure Protection VIII: 8th IFIP WG 11.10 International Conference (ICCIP). 2014. pp. 65–78.
98. Aouedi O., Piamrat K., Muller G., Singh K. Federated Semisupervised Learning for Attack Detection in Industrial Internet of Things // IEEE Transactions on Industrial Informatics. 2022. vol. 19. no. 1. pp. 286–295. DOI: 10.1109/TII.2022.3156642.
99. Truong T., Ta B.P., Le Q.A., Nguyen D.M., Le C.T., Nguyen H.X., Do H.T., Nguyen H.T., Tran K.P. Light-weight federated learning- based anomaly detection for time-series data in industrial control systems // Computers in Industry. 2022. vol. 140. no. 103692. DOI: 10.1016/j.compind.2022.103692.
100. Turnipseed I.P. A new scada dataset for intrusion detection research // Mississippi State University. 2015.
101. Secure Water Treatment (SWaT). URL: https://itrust.sutd.edu.sg/itrust-labs_datasets/dataset_info/. (accessed 25.06.2022).
102. HAI (HIL-based Augmented ICS) Security Dataset. URL: https://github.com/icsdataset/hai. (accessed 01.03.2023).
103. Keogh E., Lin J., Fu A. HOT SAX: efficiently finding the most unusual time series subsequence // Fifth IEEE International Conference on Data Mining (ICDM'05). 2005. pp. 226–233. DOI: 10.1109/ICDM.2005.79.
104. NYC taxi and limousine commission. URL: https://www.nyc.gov/site/tlc/index.page. (accessed 01.03.2023).
105. Liu H., Zhang S., Zhang P., Zhou X., Shao X., Pu G., Zhang Y. Blockchain and Federated Learning for Collaborative Intrusion Detection in Vehicular Edge Computing // IEEE Transactions on Vehicular Technology. 2021. vol. 70. no. 6. pp. 6073–6084. DOI: 10.1109/TVT.2021.3076780.
106. Abdel-Basset M., Moustafa N., Hawash H., Razzak I., Sallam K.M., Elkomy O.M. Federated Intrusion Detection in Blockchain-Based Smart Transportation Systems // IEEE Transactions on Intelligent Transportation Systems. 2021. vol. 23. no. 3. pp. 2523–2537. DOI: 10.1109/TITS.2021.3119968.
107. Aliyu I., Feliciano M.C., Van Engelenburg S., Kim D.O., Lim C. G.A Blockchain-Based Federated Forest for SDN – Enabled In-Vehicle Network Intrusion Detection System // IEEE Access. 2021. vol. 9. pp. 102593–102608. DOI: 10.1109/ACCESS.2021.3094365.
108. Li Q., He B., Song D. Model-Contrastive Federated Learning. Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2021. pp. 10713–10722.
109. McMahan H., Moore E., Ramage D., Arcas B.A. Federated Learning of Deep Networks using Model Averaging. ArXiv preprint arXiv:1602.05629. 2016. URL: https://fate.fedai.org/. (accessed 25.06.2022).
110. FATE. An Industrial Grade Federated Learning Framework. URL: https://fate.fedai.org/. (accessed 25.06.2022).
111. Yin D., Chen Y., Kannan R., Bartlett P. Byzantine-Robust Distributed Learning: Towards Optimal Statistical Rates // Proceedings of the 35th International Conference on Machine Learning. 2018. vol. 80. pp. 5650–5659.

Новикова Евгения Сергеевна — канд. техн. наук, старший научный сотрудник, лаборатория проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки "Санкт-Петербургский Федеральный исследовательский центр Российской академии наук" (СПб ФИЦ РАН). Область научных интересов: безопасность информационных систем, обнаружение аномалий методами машинного обучения, конфиденциальность данных. Число научных публикаций — 60. novikova@comsec.spb.ru; 14 линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)328-7181.

Федорченко Елена Владимировна — канд. техн. наук, старший научный сотрудник, лаборатория проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки "Санкт-Петербургский Федеральный исследовательский центр Российской академии наук" (СПб ФИЦ РАН). Область научных интересов: безопасность информационных систем, методы анализа рисков компьютерных сетей, управление информационными рисками, анализ данных, поддержка принятия решений по повышению защищенности. Число научных публикаций — 100. doynikova@comsec.spb.ru; 14 линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)328-7181.

Котенко Игорь Витальевич — д-р техн. наук, профессор, руководитель лаборатории, лаборатория проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки "Санкт-Петербургский Федеральный исследовательский центр Российской академии наук" (СПб ФИЦ РАН). Область научных интересов: безопасность компьютерных сетей, в том числе управление политиками безопасности, разграничение прав доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибер-терроризму. Число научных публикаций — 450. ivkote@comsec.spb.ru; 14 линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)328-7181.

Холод Иван Иванович — д-р техн. наук, доцент, декан факультета, факультета компьютерных технологий и информатики, Санкт-Петербургский Электротехнический университет «ЛЭТИ». Область научных интересов: распределенные параллельные алгоритмы машинного обучения. Число научных публикаций — 50. iiholod@etu.ru; улица Профессора Попова, 5, 197022, Санкт-Петербург, Россия; р.т.: +7(812)234-2746.

Поддержка исследований. Работа выполнена при финансовой поддержке РНФ (проект № 22-21-00724).

DOI 10.15622/ia.22.5.4

E. NOVIKOVA, E. FEDORCHENKO, I. KOTENKO, I. KHOLOD

ANALYTICAL REVIEW OF INTELLIGENT INTRUSION DETECTION SYSTEMS BASED ON FEDERATED LEARNING: ADVANTAGES AND OPEN CHALLENGES

Novikova E., Fedorchenko E., Kotenko I., Kholod I. **Analytical Review of Intelligent Intrusion Detection Systems Based on Federated Learning: Advantages and Open Challenges.**

Abstract. To provide an accurate and timely response to different types of attacks, intrusion detection systems collect and analyze a large amount of data, which may include information with limited access, such as personal data or trade secrets. Consequently, such systems can be seen as an additional source of risks associated with handling sensitive information and breaching its security. Applying the federated learning paradigm to build analytical models for attack and anomaly detection can significantly reduce such risks because locally generated data is not transmitted to any third party, and model training is done locally - on the data sources. Using federated training for intrusion detection solves the problem of training on data that belongs to different organizations, and which, due to the need to protect commercial or other secrets, cannot be placed in the public domain. Thus, this approach also allows us to expand and diversify the set of data on which machine learning models are trained, thereby increasing the level of detectability of heterogeneous attacks. Due to the fact that this approach can overcome the aforementioned problems, it is actively used to design new approaches for intrusion and anomaly detection. The authors systematically explore existing solutions for intrusion and anomaly detection based on federated learning, study their advantages, and formulate open challenges associated with its application in practice. Particular attention is paid to the architecture of the proposed systems, the intrusion detection methods and models used, and approaches for modeling interactions between multiple system users and distributing data among them are discussed. The authors conclude by formulating open problems that need to be solved in order to apply federated learning-based intrusion detection systems in practice.

Keywords: intrusion detection, anomalies, federated learning, analysis models, data partition.

References

1. McMahan B., Moore E., Ramage D., Hampson S., Arcas B.A. Communication-Efficient Learning of Deep Networks from Decentralized Data. Artificial intelligence and statistics. 2017. pp. 1273–1282.
2. Lwakatare L.E., Raj A., Bosch J., Olsson H.H., Crnkovic I.A Taxonomy of Software Engineering Challenges for Machine Learning Systems: An Empirical Investigation. Agile Processes in Software Engineering and Extreme Programming: Proceedings of 20th International Conference. 2019. pp. 227–243.
3. Antonakakis M., April T., Bailey M., Bernhard M., Bursztein E., Cochran J., Durumeric Z., Halderman J.A., Invernizzi L., Kallitsis M., Kumar D., Lever C., Ma Z., Mason J., Menscher D., Seaman C., Thomas K., Zhou Y. Understanding the Mirai Botnet. 26th USENIX Security Symposium (USENIX Security 17). 2017. pp. 1093–1110.
4. Novikova E., Doynikova E., Golubev S. Federated Learning for Intrusion Detection in the Critical Infrastructures: Vertically Partitioned Data Use Case. Algorithms. 2022. vol. 15(4). no. 104. DOI: 10.3390/a15040104.

5. Ludwig H, et al. IBM Federated Learning: an Enterprise Framework White Paper V0.1. ArXiv preprint arXiv:2007.10987. 2020.
6. Lo S.K. Lu Q., Zhu L., Paik H.Y., Xu X., Wang C. Architectural Patterns for the Design of Federated Learning Systems. Journal of Systems and Software. 2022. vol. 191. no. 111357.
7. Sannara E.K., Portet F., Lalanda P., German V.E.G.A. A Federated Learning Aggregation Algorithm for Pervasive Computing: Evaluation and Comparison. IEEE International Conference on Pervasive Computing and Communications (PerCom). 2021. pp. 1–10. DOI: 10.1109/PERCOM50583.2021.9439129.
8. Yurochkin M., Agarwal M., Ghosh S., Greenewald K., Hoang N., Khazaeni Y. Bayesian Nonparametric Federated Learning of Neural Networks. International conference on machine learning. 2019. pp. 7252–7261.
9. Mansour A.B., Carenini G., Duplessis A., Naccache D. Federated Learning Aggregation: New Robust Algorithms with Guarantees. 21st IEEE International Conference on Machine Learning and Applications (ICMLA). 2022. pp. 721–726. DOI: 10.48550/ARXIV.2205.10864.
10. Shahid O., Pouriyeh S., Parizi R.M., Sheng Q.Z., Srivastava G., Zhao L. Communication Efficiency in Federated Learning: Achievements and Challenges. ArXiv preprint arXiv:2107.10996. 2021.
11. Juvekar C., Vaikuntanathan V., Chandrakasan A. GAZELLE: A Low Latency Framework for Secure Neural Network Inference. Proceedings of the 27th USENIX Security Symposium (USENIX Security 18). 2018. pp. 1651–1669.
12. Zhang C., Li S., Xia J., Wang W., Yan F., Liu Y. BatchCrypt: Efficient Homomorphic Encryption for Cross-Silo Federated Learning. Proceedings of the 2020 USENIX Conference on Usenix Annual Technical Conference. USENIX annual technical conference (USENIX ATC 20). 2020. pp. 493–506.
13. Kairouz P., et al. Advances and Open Problems in Federated Learning. Foundations and Trends in Machine Learning. 2021. vol. 14. no. 1–2. pp. 1–210.
14. Truex S., Liu L., Chow K.H., Gursoy M.E., Wei W. LDP-Fed: federated learning with local differential privacy. Proceedings of the Third ACM International Workshop on Edge Systems, Analytics and Networking. 2020. pp. 61–66.
15. Shokri R., Shmatikov V. Privacy-preserving deep learning. Proceedings of the 22nd ACM SIGSAC conference on computer and communications security. 2015. pp. 1310–1321. DOI: 10.1109/ALLERTON.2015.7447103.
16. Novikova E, Fomichov D., Kholod I., Filippov E. Analysis of Privacy-Enhancing Technologies in Open-Source Federated Learning Frameworks for Driver Activity Recognition. Sensors. 2022. vol. 22(8). no. 2983. DOI: 10.3390/s22082983.
17. Zapechnikov S. [Models and algorithms of the confidential machine learning]. Bezopasnost' informacionnih technologii – IT security. 2020. vol. 27. no. 1. pp. 51–67. DOI: 10.26583/bit.2020.1.05. (In Russ.).
18. Rieke N., Hancox J., Li W., Milletarì F., Roth H.R., Albarqouni S., Bakas S., Galtier M.N., Landman B.A., Maier-Hein K., Ourselin S., Sheller M., Summers R.M., Trask A., Xu D., Baust M., Cardoso M.J. The future of digital health with federated learning. NPJ Digital Medicine. 2020. vol. 3. no. 119. DOI: 10.1038/s41746-020-00323-1.
19. Antunes R.S., André da Costa C., Küderle A., Yari I.A., Eskofier B. Federated Learning for Healthcare: Systematic Review and Architecture Proposal. ACM Transactions on Intelligent Systems and Technology (TIST). 2022. vol. 13(4). no. 54. DOI: 10.1145/3501813.
20. Nguyen T.D., Marchal S., Miettinen M., Fereidooni H., Asokan N., Sadeghi A.R.. DIoT: A Federated Self-learning Anomaly Detection System for IoT. IEEE 39th

International Conference on Distributed Computing Systems (ICDCS). 2019. pp. 756–767.
21. Li B., Wu Y., Song J., Lu R., Li T., Zhao L. DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber-Physical Systems. IEEE Transactions on Industrial Informatics. 2020. vol. 17. no. 8. pp. 5615–5624. DOI: 10.1109/TII.2020.3023430.
22. Rey V., Sánchez P.M.S., Celdrán A.H., Bovet G. Federated learning for malware detection in IoT devices. Computer Networks. 2022. vol. 204. no. 108693. DOI: 10.1016/j.comnet.2021.108693.
23. Huong T.T., Bac T.P., Long D.M., Thang B.D., Binh N.T., Luong T.D., Phuc T.K. LocKedge: Low-Complexity Cyberattack Detection in IoT Edge Computing. IEEE Access. 2021. vol. 9. pp. 29696–29710. DOI: 10.1109/ACCESS.2021.3058528.
24. Khoa T.V., Saputra Y.M., Hoang D.T., Trung N.L., Nguyen D., Ha N.V., Dutkiewicz E. Collaborative Learning Model for Cyberattack Detection Systems in IoT Industry 4.0. IEEE Wireless Communications and Networking Conference (WCNC). 2020. pp. 1–6. DOI: 10.1109/WCNC45663.2020.9120761.
25. Long G., Tan Y., Jiang J., Zhang C. Federated Learning for Open Banking. Federated Learning: Privacy and Incentive. 2020. pp. 240–254.
26. Ahmed U., Srivastava G., Lin J.C.-W. Reliable customer analysis using federated learning and exploring deep-attention edge intelligence. Future Generation Computer Systems. 2022. vol. 127. pp. 70–79. DOI: 10.1016/j.future.2021.08.028.
27. Li J., Cui T., Yang K., Yuan R., He L., Li M. Demand Forecasting of E-Commerce Enterprises Based on Horizontal Federated Learning from the Perspective of Sustainable Development. Sustainability. 2021. vol. 13(23). no. 13050. DOI: 10.3390/su132313050.
28. Dzyaba V.I. [Application of the federated learning to text classification.] Processy upravlenija i ustojchivost – Control processes and stability. 2022. vol. 9. no. 1. pp. 210–214.
29. Gonsales P.Yu., Kholod I.I. [Multi-agent architecture for federated learning]. Komp'juternye instrumenty v obrazovanii – Computer tools in Education. 2022. no. 1. pp. 30–45. DOI: 10.32603/2071-2340-2022-1-30-45.
30. Holod I.I., Efremov M.A. [Developing universal framework design for federated learning]. Programmnye produkty i sistemy – Software products and systems. 2022. vol. 35. no. 2. pp. 263–272. DOI: 10.15827/0236-235X.138.263-272.
31. Swarm learning: Driving advances both practical and profound. Available at: https://www.hpe.com/us/en/insights/articles/swarm-learning-driving- advances-both-practical-and-profound-2111.html. (accessed 24.10.2022).
32. Bellatreche L., Boukhalfa K., Richard P. Data Partitioning in Data Warehouses: Hardness Study, Heuristics and ORACLE Validation. Data Warehousing and Knowledge Discovery: Proceedings of the 10th International Conference on Data Warehousing and Knowledge Discovery. 2008. pp. 87–96. DOI: 10.1007/978-3-540-85836-2_9.
33. Khraisat A., Gondal I., Vamplew P., Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity. 2019. vol. 2. no. 1. pp. 1–22. DOI: 10.1186/s42400-019-0038-7.
34. Kotenko I., Saenko I., Branitskiy A. Framework for Mobile Internet of Things Security Monitoring Based on Big Data Processing and Machine Learning. IEEE Access. 2018. vol. 6. pp. 72714–72723. DOI: 10.1109/ACCESS.2018.2881998.
35. Bukhanov D.G., Polyakov V.M. Detection of network attacks based on adaptive resonance theory. Journal of Physics: Conference Series. 2018. vol. 1015(4). no. 042007. DOI: 10.1088/1742-6596/1015/4/042007.

36. Yunwu W. Using Fuzzy Expert System Based on Genetic Algorithms for Intrusion Detection System. International Forum on Information Technology and Applications. 2009. vol. 2. pp. 221–224. DOI: 10.1109/IFITA.2009.107.
37. Dave M.H., Sharma S.D. Improved Algorithm for Intrusion Detection Using Genetic Algorithm and SNORT. International Journal of Emerging Technology and Advanced Engineering. 2014. vol. 4. no. 8. pp. 273–276.
38. Ranjan R., Sahoo G. A New Clustering Approach for Anomaly Intrusion Detection. International Journal of Data Mining and Knowledge Management Process (IJDKP). 2014. vol. 4. no. 2. pp. 29–38. DOI: 10.5121/ijdkp.2014.4203.
39. Li Z., Qin Z., Huang K., Yang X., Ye S. Intrusion Detection Using Convolutional Neural Networks for Representation Learning. International conference on neural information processing. 2017. pp. 858–866.
40. Hu J., Liu C., Cui Y. An Improved CNN Approach for Network Intrusion Detection System. International Journal of Network Security. 2021. vol. 23. no. 4. pp. 569–575.
41. Vinayakumar R., Soman K., Poornachandran P. Evaluation of Recurrent Neural Network and Its Variants for Intrusion Detection System IDS. International Journal of Information System Modeling and Design (IJISMD). 2017. vol. 8. no. 3. pp. 43–63.
42. Song Y., Hyun S., Cheong Y.-G. Analysis of Autoencoders for Network Intrusion Detection. Sensors. 2021. vol. 21(13). no. 4294. DOI: 10.3390/s21134294.
43. Gajewski M., Batalla J.M., Mastorakis G., Mavromoustakis C.X. A distributed IDS architecture model for Smart Home systems. Cluster Computing. 2019. vol. 22. pp. 1739–1749.
44. Shterenberg S.I., Poltavtseva M.A. A Distributed Intrusion Detection System with Protection from an Internal Intruder. Automatic Control and Computer Sciences. 2018. vol. 52. pp. 945–953.
45. Schueller Q., Basu K., Younas M., Patel M., Ball F. A Hierarchical Intrusion Detection System using Support Vector Machine for SDN Network in Cloud Data Center. 28th International Telecommunication Networks and Applications Conference (ITNAC). 2018. pp. 1–6. DOI: 10.1109/ATNAC.2018.8615255.
46. Saghezchi F.B., Mantas G., Ribeiro J., Al-Rawi M., Mumtaz S., Rodriguez J. Towards a secure network architecture for smart grids in 5G era. 13th International Wireless Communications and Mobile Computing Conference (IWCMC). 2017. pp. 121–126. DOI: 10.1109/IWCMC.2017.7986273.
47. Zhang Y. Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids. IEEE Transactions on Smart Grid. 2011. vol. 2. no. 4. pp. 796–808. DOI: 10.1109/TSG.2011.2159818.
48. Javed Y., Felemban M., Shawly T., Kobes J., Ghafoor A. A Partition-Driven Integrated Security Architecture for Cyberphysical Systems. Computer. 2020. vol. 53. no. 3. pp. 47–56. DOI: 10.1109/MC.2019.2914906.
49. Kholod I., Yanaki E., Fomichev D., Shalugin E., Novikova E., Filippov E., Nordlund M. Open-Source Federated Learning Frameworks for IoT: A Comparative Review and Analysis. Sensors. 2020. vol. 21(1). no. 167. DOI: 10.3390/s21010167.
50. Kitchenham B.A. Procedures for Performing Systematic Reviews. Keele, UK, Keele University. 2004. vol. 33. pp. 1–26.
51. Campos E.M., Saura P.F., González-Vidal A., Hernández-Ramos J.L., Bernabé J.B., Baldini G., Skarmeta A. Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges. Computer Networks. 2022. vol. 203. no. 108661. DOI: 10.1016/j.comnet.2021.108661.
52. Agrawal S., Sarkar S., Aouedi O., Yenduri G., Piamrat K., Alazab M., Bhattacharya S., Reddy Maddikunta P.K., Gadekallu T.R. Federated Learning for Intrusion Detection System: Concepts, Challenges and Future Directions. Computer Communications. 2022. vol. 195. pp. 346–361. DOI: 10.1016/j.comcom.2022.09.012

53. Sun Y., Ochiai H., Esaki H. Intrusion Detection with Segmented Federated Learning for Large-Scale Multiple LANs. International Joint Conference on Neural Networks (IJCNN). 2020. pp. 1–8. DOI: 10.1109/IJCNN48605.2020.9207094.
54. Zhao R., Yin Y., Shi Y., Xue Z. Intelligent intrusion detection based on federated learning aided long short-term memory. Physical Communication. 2020. vol. 42. no. 101157. DOI: 10.1016/j.phycom.2020.101157.
55. Kholidy H.A., Baiardi F., Hariri S. DDSGA: A Data-Driven Semi-Global Alignment Approach for Detecting Masquerade Attacks. IEEE Transactions on Dependable and Secure Computing. 2014. vol. 12. no. 2. pp. 164–178. DOI: 10.1109/TDSC.2014.2327966.
56. Saadat H., Aboumadi A., Mohamed A., Erbad A., Guizani M. Hierarchical Federated Learning for Collaborative IDS in IoT Applications. 10th Mediterranean Conference on Embedded Computing (MECO). 2021. pp. 1–6. DOI: 10.1109/MECO52532.2021.9460304.
57. University of New Brunswick dataset. NSL-KDD dataset. Available at: https://www.unb.ca/cic/datasets/nsl.html. (accessed 15.05.2022).
58. Cetin B, Lazar A., Kim J., Sim A., Wu K. Federated Wireless Network Intrusion Detection. IEEE International Conference on Big Data (Big Data). 2019. pp. 6004–6006. DOI: 10.1109/BigData47090.2019.9005507.
59. Kolias C., Kambourakis G., Stavrou A., Gritzalis S. Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset. IEEE Communications Surveys and Tutorials. 2015. vol. 18. no. 1. pp. 184–208. DOI: 10.1109/COMST.2015.2402161.
60. Ayed M.A., Talhi C. Federated Learning for Anomaly-Based Intrusion Detection. International Symposium on Networks, Computers and Communications (ISNCC). 2021. pp. 1–8. DOI: 10.1109/ISNCC52172.2021.9615816.
61. Sharafaldin I., Lashkari A.H., Ghorbani A.A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. International Conference on Information Systems Security and Privacy (ICISS). 2018. vol. 1. pp. 108–116.
62. Luo J., Yang X., Mohammed M.N. Federation Learning for Intrusion Detection Methods by Parse Convolutional Neural Network. Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT). 2022. pp. 1–7. DOI: 10.1109/ICAECT54875.2022.9807989.
63. Zhao R., Wang Y., Xue Z., Ohtsuki T., Adebisi B., Gui G. Semisupervised Federated-Learning Based Intrusion Detection Method for Internet of Things. IEEE Internet of Things Journal. 2022. vol. 10. pp. 8645–8657. DOI: 10.1109/JIOT.2022.3175918.
64. Meidan Y., Bohadana M., Mathov Y., Mirsky Y., Shabtai A., Breitenbacher D., Elovici Y. N-BaIoT-Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders. IEEE Pervasive Computing. 2018. vol. 17. no. 3. pp. 12–22. DOI: 10.1109/MPRV.2018.03367731.
65. Yang X., Luo J., Mohammed M.N. Federation Learning of Optimized Convolutional Neural Network Structure for Intrusion Detection. Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT). 2022. pp. 1–7. DOI: 10.1109/ICAECT54875.2022.9807964.
66. Shi J., Ge B., Liu Y., Yan Y., Li S. Data Privacy Security Guaranteed Network Intrusion Detection System Based on Federated Learning. IEEE INFOCOM 2021 – IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). 2021. pp. 1–6. DOI: 10.1109/INFOCOMWKSHPS51825.2021.9484545.
67. Moustafa N., Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). Military Communications and Information Systems Conference (MilCIS). 2015. pp. 1–6. DOI: 10.1109/MilCIS.2015.7348942.

68. Duy P.T., Van Hung T., Ha N.H., Do Hoang H., Pham V.H. Federated learning-based intrusion detection in SDN-enabled IIoT networks. 8th NAFOSTED Conference on Information and Computer Science (NICS). 2021. pp. 424–429. DOI: 10.1109/NICS54270.2021.9701525.
69. Sharafaldin I., Lashkari A.H., Hakak S., Ghorbani A.A. Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. International Carnahan Conference on Security Technology (ICCST). 2019. pp. 1–8. DOI: 10.1109/CCST.2019.8888419.
70. Cheng Y., Lu J., Niyato D., Lyu B., Kang J., Zhu S. Federated Transfer Learning With Client Selection for Intrusion Detection in Mobile Edge Computing. IEEE Communications Letters. 2022. vol. 26. no. 3. pp. 552–556. DOI: 10.1109/LCOMM.2022.3140273.
71. Wang N., Chen Y., Hu Y., Lou W., Hou Y.T. FeCo: Boosting Intrusion Detection Capability in IoT Networks via Contrastive Learning. IEEE INFOCOM 2022 – IEEE Conference on Computer Communications. 2022. pp. 1409–1418. DOI: 10.1109/INFOCOM48880.2022.9796926.
72. Popoola S.I., Gui G., Adebisi B., Hammoudeh M., Gacanin H. Federated Deep Learning for Collaborative Intrusion Detection in Heterogeneous Networks. IEEE 94th Vehicular Technology Conference (VTC2021-Fall). 2021. pp. 1–6. DOI: 10.1109/VTC2021-Fall52928.2021.9625505.
73. Alsaedi A., Moustafa N., Tari Z., Mahmood A., Anwar A. TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems. IEEE Access. 2020. vol. 8. pp. 165130–165150. DOI: 10.1109/ACCESS.2020.3022862.
74. Koroniotis N., Moustafa N., Sitnikova E., Turnbull B. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. Future Generation Computer Systems. 2019. vol. 100. pp. 779–796. DOI: 10.1016/j.future.2019.05.041.
75. Al-Marri N.A.A.-A., Ciftler B.S., Abdallah M.M. Federated Mimic Learning for Privacy Preserving Intrusion Detection. IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom). 2020. pp. 1–6.
76. Mothukuri V., Khare P., Parizi R.M., Pouriyeh S., Dehghantanha A., Srivastava G. Federated-Learning-Based Anomaly Detection for IoT Security Attacks. IEEE Internet of Things Journal. 2021. vol. 9. no. 4. pp. 2545–2554. DOI: 10.1109/JIOT.2021.3077803.
77. Frazao I., Abreu P.H., Cruz T., Araújo H., Simões P. Denial of Service Attacks: Detecting the Frailties of Machine Learning Algorithms in the Classification Process. Critical Information Infrastructures Security 13th International Conference (CRITIS 2018). 2019. pp. 230–235.
78. Ruzafa-Alcazar P., Fernández-Saura P., Mármol-Campos E., González-Vidal A., Hernández-Ramos J.L., Bernal-Bernabe J., Skarmeta A.F. Intrusion Detection Based on Privacy- Preserving Federated Learning for the Industrial IoT. IEEE Transactions on Industrial Informatics. 2021. vol. 19. no. 2. pp. 1145–1154. DOI: 10.1109/TII.2021.3126728.
79. Chen Z., Lv N., Liu P., Fang Y., Chen K., Pan W. Intrusion Detection for Wireless Edge Networks Based on Federated Learning. IEEE Access. 2020. vol. 8. pp. 217463–217472. DOI: 10.1109/ACCESS.2020.3041793.
80. KDD dataset. Available at: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. (accessed 15.03.2022).
81. Dong T., Qiu H., Lu J., Qiu M., Fan C. Towards Fast Network Intrusion Detection based on Efficiency-preserving Federated Learning. IEEE Intl Conf on Parallel and Distributed Processing with Applications, Big Data and Cloud Computing,

Sustainable Computing and Communications, Social Computing and Networking (ISPA/BDCloud/SocialCom/SustainCom). 2021. pp. 468–475. DOI: 10.1109/ISPA-BDCloud-SocialCom-SustainCom52081.2021.00071.

82. Tabassum A., Erbad A., Lebda W., Mohamed A., Guizani M FEDGAN-IDS: Privacy-preserving IDS using GAN and Federated Learning. Computer Communications. 2022. vol. 192. pp. 299–310. DOI: 10.1016/j.comcom.2022.06.015.
83. Aouedi O., Piamrat K., Muller G., Singh K. FLUIDS: Federated Learning with semi-supervised approach for Intrusion Detection System. IEEE 19th Annual Consumer Communications and Networking Conference (CCNC). 2022. pp. 523–524. DOI: 10.1109/CCNC49033.2022.9700632.
84. Qin Y., Kondo M. Federated Learning-Based Network Intrusion Detection with a Feature Selection Approach. International Conference on Electrical, Communication, and Computer Engineering (ICECCE). 2021. pp. 1–6. DOI: 10.1109/ICECCE52056.2021.9514222.
85. Nguyen T.D., Marchal S., Miettinen M., Fereidooni H., Asokan N., Sadeghi A.R. DIoT: A Federated Self-learning Anomaly Detection System for IoT. IEEE 39th International Conference on Distributed Computing Systems (ICDCS). 2019. pp. 756–767.
86. Qin T., Cheng G., Chen W., Lei X. FNEL: An Evolving Intrusion Detection System Based on Federated Never-Ending Learning. 17th International Conference on Mobility, Sensing and Networking (MSN). 2021. pp. 239–246. DOI: 10.1109/MSN53354.2021.00047.
87. Fan Y., Li Y., Zhan M., Cui H., Zhang Y. IoTDefender: A Federated Transfer Learning Intrusion Detection Framework for 5G IoT. IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE). 2020. pp. 88–95. DOI: 10.1109/BigDataSE50710.2020.00020.
88. Kang H., Ahn D.H., Lee G.M., Yoo J., Park K.H., Kim H.K. IoT network intrusion dataset. IEEE Dataport. 2019. vol. 10. DOI: 10.21227/q70p-q449.
89. Mirzaee P.H., Shojafar M., Pooranian Z., Asefy P., Cruickshank H., Tafazolli R. FIDS: A Federated Intrusion Detection System for 5G Smart Metering Network. 17th International Conference on Mobility, Sensing and Networking (MSN). 2021. pp. 215–222. DOI: 10.1109/MSN53354.2021.00044.
90. Regan C., Nasajpour M., Parizi R.M., Pouriyeh S., Dehghantanha A., Choo K.K.R. Federated IoT security attack detection using decentralized edge data. Machine Learning with Applications. 2022. vol. 8. no. 100263. DOI: 10.1016/j.mlwa.2022.100263.
91. Singh P., Gaba G. S., Kaur A., Hedabou M., Gurtov A. Dew-Cloud-Based Hierarchical Federated Learning for Intrusion Detection in IoMT. IEEE Journal of Biomedical and Health Informatics. 2022. vol. 27. no. 2. pp. 722–731. DOI: 10.1109/JBHI.2022.3186250.
92. Astillo P.V. Federated intelligence of anomaly detection agent in IoTMD-enabled Diabetes Management Control System. Future Generation Computer Systems. 2022. vol. 128. pp. 395–405. DOI: 10.1016/j.future.2021.10.023.
93. Astillo P.V., Jeong J., Chien W.C., Kim B., Jang J., You I. SMDAps: A specification-based misbehavior detection system for implantable devices in artificial pancreas system. Journal of Internet Technology. 2021. vol. 22. no. 1. pp. 1–11.
94. Siniosoglou I., Sarigiannidis P., Argyriou V., Lagkas T., Goudos S.K., Poveda M. Federated Intrusion Detection In NG- IoT Healthcare Systems: An Adversarial Approach. ICC 2021 – IEEE International Conference on Communications. 2021. pp. 1–6. DOI: 10.1109/ICC42927.2021.9500578.

95. Kim N.H., Krasner A., Kosinski C., Wininger M., Qadri M., Kappus Z., Danish S., Craelius W. Trending autoregulatory indices during treatment for traumatic brain injury. Journal of Clinical Monitoring and Computing. 2016. vol. 30. pp. 821–831.
96. Li B., Wu Y., Song J., Lu R., Li T., Zhao L. DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber–Physical Systems. IEEE Transactions on Industrial Informatics. 2020. vol. 17. no. 8. pp. 5615–5624. DOI: 10.1109/TII.2020.3023430.
97. Morris T., Gao W. Industrial Control System Traffic Data Sets for Intrusion Detection Research. Critical Infrastructure Protection VIII: 8th IFIP WG 11.10 International Conference (ICCIP). 2014. pp. 65–78.
98. Aouedi O., Piamrat K., Muller G., Singh K. Federated Semisupervised Learning for Attack Detection in Industrial Internet of Things. IEEE Transactions on Industrial Informatics. 2022. vol. 19. no. 1. pp. 286–295. DOI: 10.1109/TII.2022.3156642.
99. Truong T., Ta B.P., Le Q.A., Nguyen D.M., Le C.T., Nguyen H.X., Do H.T., Nguyen H.T., Tran K.P. Light-weight federated learning- based anomaly detection for time-series data in industrial control systems. Computers in Industry. 2022. vol. 140. no. 103692. DOI: 10.1016/j.compind.2022.103692.
100. Turnipseed I.P. A new scada dataset for intrusion detection research. Mississippi State University. 2015.
101. Secure Water Treatment (SWaT). Available at: https://itrust.sutd.edu.sg/itrust-labs_datasets/dataset_info/. (accessed 25.06.2022).
102. HAI (HIL-based Augmented ICS) Security Dataset. Available at: https://github.com/icsdataset/hai. (accessed 01.03.2023).
103. Keogh E., Lin J., Fu A. HOT SAX: efficiently finding the most unusual time series subsequence. Fifth IEEE International Conference on Data Mining (ICDM'05). 2005. pp. 226–233. DOI: 10.1109/ICDM.2005.79.
104. NYC taxi and limousine commission. Available at: https://www.nyc.gov/site/tlc/index.page. (accessed 01.03.2023).
105. Liu H., Zhang S., Zhang P., Zhou X., Shao X., Pu G., Zhang Y. Blockchain and Federated Learning for Collaborative Intrusion Detection in Vehicular Edge Computing. IEEE Transactions on Vehicular Technology. 2021. vol. 70. no. 6. pp. 6073–6084. DOI: 10.1109/TVT.2021.3076780.
106. Abdel-Basset M., Moustafa N., Hawash H., Razzak I., Sallam K.M., Elkomy O.M. Federated Intrusion Detection in Blockchain-Based Smart Transportation Systems. IEEE Transactions on Intelligent Transportation Systems. 2021. vol. 23. no. 3. pp. 2523–2537. DOI: 10.1109/TITS.2021.3119968.
107. Aliyu I., Feliciano M.C., Van Engelenburg S., Kim D.O., Lim C. G.A Blockchain-Based Federated Forest for SDN – Enabled In-Vehicle Network Intrusion Detection System. IEEE Access. 2021. vol. 9. pp. 102593–102608. DOI: 10.1109/ACCESS.2021.3094365.
108. Li Q., He B., Song D. Model-Contrastive Federated Learning. Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2021. pp. 10713–10722.
109. McMahan H., Moore E., Ramage D., Arcas B.A. Federated Learning of Deep Networks using Model Averaging. ArXiv preprint arXiv:1602.05629. 2016. Available at: https://fate.fedai.org/. (accessed 25.06.2022).
110. FATE. An Industrial Grade Federated Learning Framework. Available at: https://fate.fedai.org/. (accessed 25.06.2022).
111. Yin D., Chen Y., Kannan R., Bartlett P. Byzantine-Robust Distributed Learning: Towards Optimal Statistical Rates. Proceedings of the 35th International Conference on Machine Learning. 2018. vol. 80. pp. 5650–5659.

Novikova Evgenia — Ph.D., Senior researcher, Laboratory of computer security problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: privacy and personal data security, privacy-preserving computations, and machine learning-based anomaly and intrusion detection. The number of publications — 60. novikova@comsec.spb.ru; 39, 14 line V.O., 199178, St. Petersburg, Russia; office phone: +7(812)328-7181.

Fedorchenko Elena — Ph.D., Senior researcher, Laboratory of computer security problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: information systems security, risk analysis methods for computer networks, information security risk management, data analysis, security decisions support. The number of publications — 100. doynikova@comsec.spb.ru; 39, 14 line V.O., 199178, St. Petersburg, Russia; office phone: +7(812)328-7181.

Kotenko Igor — Head of the laboratory, Laboratory of computer security problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: computer network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital right management, modeling, simulation and visualization technologies for counteraction to cyber terrorism. The number of publications — 450. ivkote@comsec.spb.ru; 39, 14 line V.O., 199178, St. Petersburg, Russia; office phone: +7(812)328-7181.

Kholod Ivan — Ph.D., Dr.Sci., Associate Professor, Dean of the faculty, Faculty of computer science and technology, Saint Petersburg State Electrotechnical University “LETI”. Research interests: distributed parallel machine learning algorithms. The number of publications — 50. iiholod@etu.ru; 5, Professor Popov St., 197022, St. Petersburg, Russia; office phone: +7(812)234-2746.

Acknowledgements. This research is supported by RSF (grant 22-21-00724).

DOI 10.15622/ia.22.5.5

A.E. ASFHA, A. VAISH

INFORMATION SECURITY RISK ANALYSIS IN FOOD PROCESSING INDUSTRY USING A FUZZY INFERENCE SYSTEM

Asfha A.E., Vaish A. **Information Security Risk Analysis in Food Processing Industry Using a Fuzzy Inference System.**

Abstract. Recently, different attempts have been made to characterize information security threats, particularly in the industrial sector. Yet, there have been a number of mysterious threats that could jeopardize the safety of food processing industry data, information, and resources. This research paper aims to increase the efficiency of information security risk analysis in food processing industrial information systems, and the participants in this study were experts in executive management, regular staff, technical and asset operators, third-party consultancy companies, and risk management professionals from the food processing sector in Sub-Saharan Africa. A questionnaire and interview with a variety of questions using qualitative and quantitative risk analysis approaches were used to gather the risk identifications, and the fuzzy inference system method was also applied to analyze the risk factor in this paper. The findings revealed that among information security concerns, electronic data in a data theft threat has a high-risk outcome of 75.67%, and human resource management (HRM) in a social engineering threat has a low-risk impact of 26.67%. Thus, the high-probability risk factors need quick action, and the risk components with a high probability call for rapid corrective action. Finally, the root causes of such threats should be identified and controlled before experiencing detrimental effects. It's also important to note that primary interests and worldwide policies must be taken into consideration while examining information security in food processing industrial information systems.

Keywords: food processing industry, information security, risk identification, risk analysis, fuzzy inference system, ISO 27005.

1. Introduction. In order to address the problems with nutrition and food security in sub-Saharan Africa, food processing might be extremely important. In actuality, the robustness of the food processing sector directly affects the creation of an abundance of high-quality, wholesome, and secure meals that are accessible to customers and reasonably priced. Processing food is essential to preventing losses after harvest and maximizing harvest usage, especially during drought and seasons of low production, and plays a crucial role in providing income for farmers [1].

In any industry, information is one of the most valuable assets and resources, but it's also the most fragile element, particularly in the food processing industry. It is a value, and every food processing sector has understood that information security threats can negatively affect firm process stability and public image, as well as financial loss, environmental impact, and client and partner satisfaction. Thus, information security applies to the protection of data and information, information systems, and their essential components from unauthorized access, use, exposure, and modification in order to ensure confidentiality, integrity, and availability [2].

In the past, all industries used to be built on mechanical devices and closed systems [3], which meant that most industrial systems were not connected to each other or to public networks such as the Internet. During the risk analysis of these industries, the security-related risks posed by accidental component failures and human errors must be considered. Yet, the scenario is somewhat different now; shifting away from analog or traditional equipment and toward technology offers many advantages in terms of production, but it also has a number of disadvantages [4]. As a result, the most popular sectors are subject to a variety of internal and external security threats, including human, environmental, physical, and natural risks, all of which can have disastrous consequences.

This argument demonstrates that industries are confronting a larger security flaw, an increase in the number and effectiveness of assault scenarios, and increased network complexity [5]. As a result, all industries are confronted with a number of Internet-related concerns, including security risks, intellectual property violations, and personal data privacy. As a result, understanding information security threats in companies is critical in order to prevent future harm.

In reality, in this food processing business, information security risk management is the most important way to reduce losses or damages caused by a variety of security risks. By employing a risk management approach and assuring stakeholders that risks are effectively handled, information security management systems (ISMS) secure the confidentiality, integrity, and availability of information [6].

Therefore, information security risk management aims to protect the security of systems that identify, analyze, and evaluate industrial data, and in order to manage risks, a strategy for assessing the level of risks and identifying potential dangers should exist [7]. Based on ISO 27005, risk analysis is the first step in the risk management process. Evaluating information security risks entails detecting threats and vulnerabilities, calculating the likelihood and impact of known threats, and finally prioritizing the risks to determine the appropriate amount of training and controls needed for effective mitigation [8].

The purpose of this paper is to analyze information security risk in the Sub-Saharan Africa food processing industry information system, and in this study, the authors proposed fuzzy inference system (FIS) methods based on ISO 27005 standards. Inaccuracy and uncertainty in the real world and human thought are modeled by a mathematical technique called fuzzy logic. This essay will demonstrate how fuzzy logic may be used to evaluate risk [9]. In this paper, the authors studied five critical food processing industry assets. Therefore, the five critical assets are briefly characterized

here, such as electronic data, physical hardware, software revenue management systems, food processing industry reputation, or intangible assets, and human resource management (HRM) or employers.

Finally, this paper covers the above-mentioned food industrial assets, the mathematical foundations of fuzzy logic, as well as membership functions, fuzzy sets, and logic rules. Fuzzy expert systems turn input numbers into linguistic values, which are adjusted by if-then rules provided by a human expert. The concept of a fuzzy expert system is explored in detail, along with its rule base and set membership functions.

2. Literature review. Over the years, many studies have been conducted on the topic of information security risk analysis, with various techniques and objectives, but with the fundamental purpose of providing some kind of information about the dangers that could harm an industrial organization's assets. In order to unravel the problem of information security risk analysis, various software packages have been developed based on the developed methods.

There are over 30 methodologies and frameworks that can be used for security risk analysis and assessment. During the risk identification process, potential events are identified based on their positive or negative impact on the main mission goals [10]. Also, the main purpose of the risk analysis is to evaluate the identified risks based on the frequency of their occurrence and their perceived consequences for the mission goals. As a result, one of the most practical methods in this context is to use experts' opinions to identify the rate and potential consequences of risks; thus, after fully recognizing the risks, it is possible to improve opportunities and reduce threats posed by industry risks by implementing risk response strategies [11].

The scenario in information security can be defined as a combination of assets, vulnerability, threat, controls, and consequences [12]. With strong information security, the food processing industry decreases its risk of both inside and outside assaults on information technology systems. They also keep sensitive data safe, protect systems from cyberattacks, provide continuity for the company, and provide peace of mind to everyone in the organization by keeping confidential information safe from security threats.

The risk analysis for seeking goals is very useful due to the definition and nature of risks, and the risk analysis that focuses on examining the effects of risks on industry goals can play a vital role in information security risk management. This, along with risk analysis, is a great help in developing response strategies and reducing unexpected consequences [13]. Accordingly, two general approaches to information security industry risk analysis can be derived by reviewing the existing literature on risk analysis: qualitative and quantitative risk analysis.

To perform a comprehensive assessment of risk in industrial information systems, both quantitative and qualitative methods should be employed. Knowledge of methodology in this area is the prerequisite for accurate risk evaluation, i.e., the combined use of quantitative and qualitative methods ensures more accurate risk estimation [14]. The qualitative method is influenced by subjective judgments and provides poor results for assessing risks because risk analysts mostly depend on their judgments based on their previous knowledge and experiences.

For this purpose and to overcome the inherent limitations in the qualitative approaches to risk analysis, quantitative approaches have been developed, as have various mathematical approaches, for example, fuzzy logic. This method is an advanced model in the information security risk analysis of industrial information systems. Thus, fuzzy logic tools allow us to assess the level of risk using quantitative and qualitative indicators and expert knowledge, whose values are constantly changing over time and which take into consideration the nonlinearity of process growth probabilities and dependability [15].

Fuzzy logic is a type of many-valued logic that deals with approximate reasoning rather than fixed and accurate reasoning, and it is a useful approach to plotting an input space to an output space [16]. It is a type of logic utilized in some expert systems and other artificial intelligence applications in which variables' degrees of truthfulness are represented by a range of values ranging from 0 (false) to 1 (true) [17]. In this way, the membership function of an event on those sets represents the degree to which it belongs to the sets of outcomes and considers a method based on a fuzzy risk matrix that allows expert knowledge to be recorded in an intelligible manner, [18] proves that the fuzzy risk matrix is compatible with the Mamdani fuzzy inference system.

The most important element of risk analysis in the food industry based on fuzzy logic is that the entire process leads to the development of a control system capable of effectively reducing risk. Because of the exact output of analysis and consideration of countermeasures, it can repeat risk analysis on a regular basis with valuable output [19]. Furthermore, it reduced subjectivity to an appropriate standard by using fuzzy logic and methods based on fuzzy logic because of quantitative input data, so subjectivity was moved to the process of creating relations and dependencies between input data and risk assessment, where it could be better controlled [20]. A fuzzy inference engine, a set of fuzzy membership functions, and a set of fuzzy rules are the key elements of a fuzzy expert system. They’re used in a variety of fields, including data analysis, financial systems, pattern recognition, and linear and nonlinear control [21].

Finally, the fuzzy logic approach has been recommended as the appropriate tool to improve food industrial processing information security and may help analyze complex conditions. Thus, the main purpose of this paper is to evaluate risk values in a more reliable, flexible, and objective manner by using this proposed method and prioritizing the level of risk value.

3. Material and Methods. This methodology research was based on ISO 27005, and was completed in 2022. The participants in this study were experts and staff from different sections of the food processing industry in the Sub-Saharan Africa information system (N = 145). The participants were executive management, regular staff, technical and asset operators, and third-party consulting companies.

Participants were asked to evaluate five different information assets based on a scale of ten points (one, two, …. and ten) to estimate the likelihood and severity of the threat and group them into a three-point Likert scale (low, medium, and high) as shown in Table 1. The collected data was analyzed to calculate the likelihood of related threats and their severity. Some specialists in the field of food processing industry information systems confirmed the reliability of the questionnaires. For each question and its corresponding criticality, the average scores were calculated based on the answers of the participants. Finally, all of these average values were used in the FIS model to calculate the final risk values.

Table 1. Likert-scale questionnaires

Likelihood and severity of data collection									
Low			Medium				High		
1	2	3	4	5	6	7	8	9	10

These questionnaires and interviews had three parts, such as:

– Personal information: this is very basic personal information about the participant in the food processing industry;

– The characteristics of systems and the state of information security in the food processing industry's information system (context);

– Risk identification: this part included natural disasters, human threats, and physical and environmental threats.

Based on ISO 27005, the information security risk analysis techniques provide a number of ways. Therefore, it has indicated the following processes.

3.1. Risk Identification Process. The process of recording any hazards that could prevent an organization or program from achieving its goal is known as risk identification. It is the first phase in the risk assessment process, which is used to find, allocate, and describe the types of risks. Therefore, the main goal of risk identification is to determine what,

where, when, why, and how something can impact a company's capacity to operate. All aspects of the risk assessment process are included asset identification and its values, impact level, and threat frequency. This involves eight steps. These steps are:

Step 1. Identify assets and their values. Identifying and valuing food processing industrial assets is a crucial step in determining the appropriate level of protection in the food processing industry. Therefore, an asset's value to any industry, especially the food processing sector, can be quantifiable based on expense, sensitivity, mission criticality, and/or a combination of these factors. In this study, the values of assets were evaluated by executive managers, technical asset operators, and risk management experts in the food processing industry.

Step 2. Threat identification and analysis. A threat is someone, something, an event, or a thought that causes or poses a risk to an asset. By exploiting vulnerabilities or a state of weakness, threats can compromise the confidentiality, integrity, and availability (CIA) of food processing industry assets. Thus, threat analysis is the act of investigating threat detection sources and comparing them to an information system's flaws.

The study's purpose is to identify the threats that could jeopardize an information system in the food processing industry, as the authors noted in the above top five assets in industry information system.

Step 3: Identify the vulnerability and its level. Vulnerability is described as a lack of security in a security system. Threats can take advantage of a vulnerable position because it provides or creates an opportunity for them to do so. The interrelationships between threats and vulnerabilities are examined to determine a likelihood level.

The level of susceptibility is visibly lowered as a high countermeasure is implemented in any manufacturing facility. In this study, just like asset value, the level of vulnerability and threat were evaluated by experts and participants in the food processing industry in Sub-Saharan Africa's information systems.

Step 4. Likelihood. When assessing the likelihood, it needs to be considered how often a specific threat might occur and how easily related vulnerabilities can be exploited. This information can be collected from the food processing industry information system in sub-Saharan Africa through questionnaires and interviews.

The possibility of each situation and its impact occurring must be determined after the incidents have been identified. This can be done using qualitative or quantitative analysis methodologies. The frequency of the threats and the ease with which the vulnerabilities might be exploited should be described.

Step 5. Impact. A degree of loss and harm resulting from some failure might be referred to as event repercussions or impact. Each systemic failure has certain knock-on effects. A failure may result in economic loss, environmental harm, personal injury, or death, among other conceivable outcomes. For various outcome types of facility risk analysis, repercussions need to be quantified using relative or absolute measures.

3.2. FIS process steps. The technique of mapping from a given input set to an output set using fuzzy logic is known as a fuzzy inference system. In our risk assessment model, the Mamdani Fuzzy Inference System (FIS) was employed for fuzzification, rule evaluation, and defuzzification according to Figure 1.

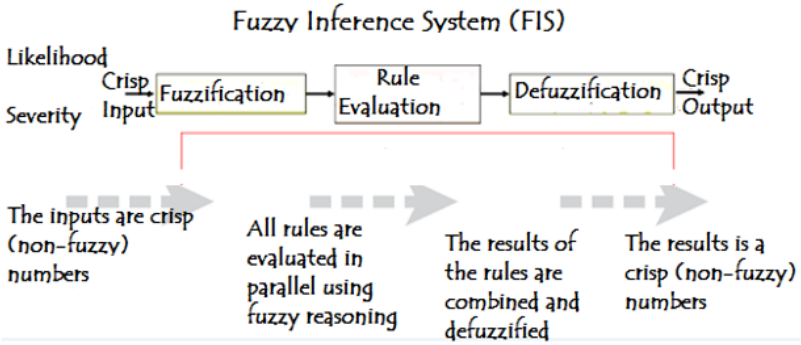


Fig. 1. Risk analysis process based on a fuzzy inference system

Step 6. Fuzzification. The first step is to use membership functions (MF) to assess the inputs' degree of membership in each of the relevant fuzzy sets (fuzzification). In this case, we used MATLAB software to solve all the equations. The fuzzy membership function is a graphical representation of the degree of membership of any value in a particular fuzzy collection. The X-axis of the graph indicates the universe of discourse, while the Y-axis reflects the degree of membership in the range [0, 1]. In this paper, we used Trapezoidal MF (TMF) in likelihood and Gaussian MF (GMF) in severity. TMF has four parameters: “a, b, c, and d”. The Range ‘b’ to ‘c’ represents the element's maximum membership value. And if x is between (a, b) or (c, d), its membership value will be between 0 and 1. A GMF is defined by two parameters, ‘a’ and ‘b’, and can be written as follows: The mean / center of the Gaussian curve is represented by ‘a’ in this function, while the dispersion of the curve is represented by ‘b’.

According to steps 4 and 5, likelihood and ***impact*** (severity) are used as **crisp inputs** to start a FIS process, and the interval range for both indicators is from 0 to 10, as shown in Figure 2.

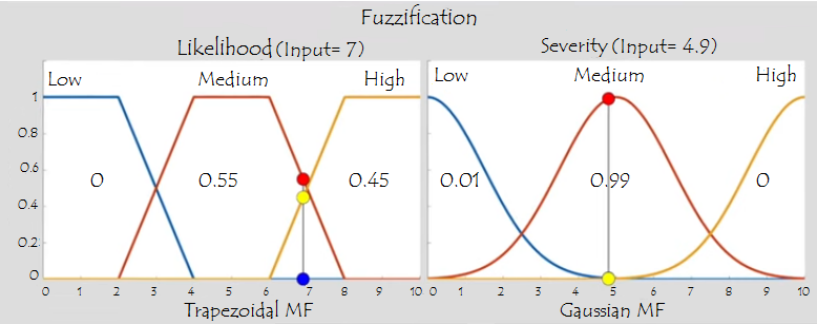


Fig. 2. Fuzzification methods

Step 7. Rule evaluation. Subsequently defining fuzzy membership functions, in this paper, nine fuzzy rules were constructed for the fuzzy inference system (FIS).

Syntax. Based on the Mamdani fuzzy inference system: If (Input 1 is membership function 1) and/or (Input 2 is membership function; 2) then (Output is output membership function). The number of terms used to assess risk variables is assumed to be three, namely *"high", "medium", and "low"* as noted in Table 2.

Table 2. Risk matrix based the above rules

	Severity		
Likelihood	**Low**	**Medium**	**High**
Low	Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	High

Step 7.1. Apply fuzzy operators. After fuzzifying the inputs, you know how well every part of the antecedent fulfills the requirements for each rule. If a rule's antecedent consists of a number of parts, the fuzzy operator is used to generate one number which symbolizes the outcome of the rule's antecedent. This value is subsequently passed on to the output function. The fuzzy operator takes multiple membership values from fuzzified input variables as input. The output consists of a single truth value. In this case, the authors apply the AND operator, as shown below.

Based on Table 2, the authors constructed nine fuzzy rules using the fuzzy operator process.

Rule 1: If likelihood is ***high*** and severity is ***medium*** then risk value is ***high***;

Rule 2: If likelihood is ***medium*** and severity is ***medium*** then risk value is ***medium***;

Rule 3: If likelihood is ***high*** and severity is ***low*** then risk value is ***medium***;

Rule 4: If likelihood is ***medium*** and severity is ***low*** then risk value is ***low***.

Based on Table 2 and Figure 2 membership function, the rules were evaluated in the following process:

Rule 1: Risk value is *high*: $\mu(x_1) = \min(0.45, 0.99) = \mathbf{0.45;}$

Rule 2: Risk value is ***medium***: $\mu(x_2) = \min(0.55, 0.99) = 0.55;$

Rule 3: Risk value is ***medium***: $\mu(x_3) = \min(0.45, 0.01) = 0.01;$

Rule 4: Risk value is *low*: $\mu(x_4) = \min(0.55, 0.01) = \mathbf{0.01;}$

N.B. All other rules have ***zero*** true values. As a result, there is no need to be concerned with them during the composition sub-process.

Step 7.2. Apply Implication Method**.** You must first establish the rule weight before using the implication approach. Every rule has a weight (a value between 0 and 1) that is applied to the antecedent's number. This weight is often 1 and hence has no effect on the implication process. However, you can reduce the impact of one rule compared to the others by changing its weight value from 1 to something else.

The implication approach is used when suitable weighting has been applied to each rule. A consequent is a fuzzy set symbolized by a membership function that properly values the linguistic characteristics assigned to it. The antecedent's function (a single number) is used to alter the consequent. The implication procedure takes a single number from the antecedent and outputs a fuzzy set. The implication is used for each rule, as shown in Figure 3.

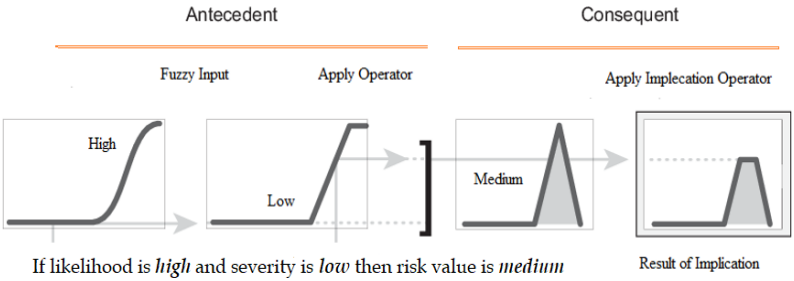


Fig. 3. Implication method

Step 7.3. Aggregate all outputs. The aggregation will be done according to the fuzzy criteria for each risk. The aggregation method seeks to combine all previously scaled and grouped rule consequent MF into a single fuzzy set.

The results of the two rules are alike (as it is for this example: medium), the degree of membership: Based on step 7.2, to be selected OR operator to choice one:

Risk value is ***medium*** = max ($\mu(x_2)$, $\mu(x_3)$) =Max (0.55; 0.01) = **0.55.**

Using the above results:

Risk value is *high*: = **0.45;**

Risk value is *medium* = **0.55;**

Risk value is *low*: = **0.01.**

Step 8. Defuzzification. It is the final step in the fuzzy rule inference model and is used to resolve a crisp value from the results of the FIS process. There are a number of methods available for Defuzzification, for example, max membership principle, centroid method, weighted average method, mean max membership, center of sums, center of largest area, and first or last of maxima. The centroid computation is one of the most used Defuzzification methods**.** In this case, the authors applied the centroid or center of gravity (COG) technique to evaluate the risk value, as shown in Figure 4.

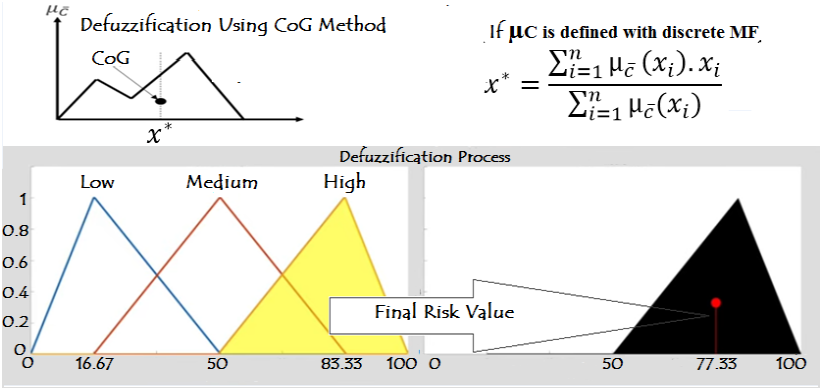


Fig. 4. Defuzzification methods using center of gravity

4. Result and Discussion. This part uses a variety of statistical approaches to evaluate the quantitative data and provide the results of the data analysis in order to test the research hypotheses generated for the current study in the Sub-Saharan Africa food processing industry information system. The response rate of participants is noted in Table 3.

Table 3. Response rate of participant in this study

Questionnaire	Number	Percentage
Distributed	165	100 %
Received	150	90.90%
practical	145	96.67%
Impractical	5	3.33%

Based on Table 3, considering the chosen strategy of handing out the questionnaires to specific individuals one at a time, and 165 were distributed. As a consequence, 145 of the 150 questionnaires received were complete and functional, yielding a response rate of 96.67%, which is regarded as excellent in research using a survey method and is displayed in Table 3. However, 15 employees failed to submit their surveys, and the remaining five – representing 3.33% of the impractical forms – were incomplete and contained inconsistent answers.

In this study, the distribution of participants in Sub-Saharan Africa's food processing industry is shown in Table 4.

Table 4. Distribution of participant in this study

Sex	**Men**		**Female**	
	N = 122, 84.14%		N=23, 15.86%	
Average Age	34.33± 6.79			
Position	Management and Executive Management	Regular Staff	Technical and Asset operators	Third-party consultancy companies
	N=21, 14.48%	N=48, 33.10%	N=67, 46.21%	N=9, 6.21%
Work of experience	=< 2 years	>2 & ≤ 5	>5 & ≤ 10	>10 years
	N=18, 12.41%	N=48, 33.10%	N=67, 46.21%	N=12, 8.28%
Education	Ph.D.	MSc	BSc/Diploma	Vocational and =<High school
	N=7, 4.83%,	N=15, 10.34%	N=50, 34.48%	N=73, 50.34%

Based on Table 4, the majority of respondents had between five and ten years of work experience, which may imply a fair amount of knowledge of the physical security system. The majority of respondents, however, had only completed high school and a vocational program, making up 50.34% of the total and demonstrating a high level of knowledge. A bachelor's degree (BSc) and diploma are the next most common levels of education, coming in at 34.48%, and the Ph.D. level is the least common, at 4.83%.

Additionally, job position data show that workers at the technical and asset operator's personnel level were the most prevalent, totaling 46.21%, followed by "regular staff" at 33.10%, and third-party consultant organizations, the lowest, represented by 6.21% of the total respondents.

According to the risk identification process, the identification of threats for each asset is listed in Table 5.

Table 5. Asset, threat, and vulnerability outcome in this study

Asset Name	Threat Code	Threat	Vulnerability
Electronic Data (ED)	T1	SQL injection	Outdated DBMS
	T2	Data theft	Breaching legal requirements
	T3	User error	Negligence
Physical Hardware (PH)	T4	Power interruptions	Inability to operate without power supply
	T5	Heat	Vulnerability of Processor Chips to melt at high temperatures
	T6	Fire	Vulnerability physical problem/damage
Software Revenue Management System (SRMS)	T7	Cross-site Scripting	Vulnerability to malicious code
	T8	Stack-Overflow attacks	Bad coding conducts
	T9	Denial-of-Service (DoS)	Low memory resources
Industry Reputation or intangible asset (IRIA)	T10	Fraud	Staff deceitfulness
	T11	Data breach	Outdated Security Software
	T12	Misuse of resources	Poor resources management
Human Resource Management /Employee (HRME)	T13	Accident	Ignorance to precaution
	T14	Social engineering	Inclination to improved status gain
	T15	Illness	Illness due to change of weather

Based on sections 3.1 and 3.2, the final risk level of each asset is noted in Table 6 and also ranked from maximum to minimum risk value.

Table 6. Final risk values in this study

	Threats	**Likelihood Level**	**Severity Level**	**Risk Level %**	**Rank**
		Input variable to Fuzzification		Defuzzification	
		Level Value: 0-10	**Level Value: 0-10**	**Value: 100%**	
ED	T1	7	8	66.33	3
	T2	5	9.1	75.67	1
	T3	4	4	48.33	8
PH	T4	8.5	2.5	57.67	5
	T5	5.5	3.4	45.67	10
	T6	9.4	8	70	2
SRMS	T7	2.9	5.2	39.67	13
	T8	3	7	42	11
	T9	7.5	1.5	50.67	6
IRIA	T10	1.8	8.8	48.33	8
	T11	7	4.6	58.67	4
	T12	8.1	0.1	50	7
HRME	T13	1.5	5.8	38.67	14
	T14	4.8	1.5	26.67	15
	T15	3.5	6.1	40.67	12

Based on the fuzzy logic designer, nine fuzzy rules were constructed. The inference engine maps input fuzzy sets (likelihood and severity) into fuzzy output sets (risk value). Figure 5 shows the number of if-then rules in order to provide a better understanding of the proposed fuzzy inference system framework, and with the input of likelihood of occurrence and risk severity, the risk size can be calculated. For instance, with 5 and 5 for likelihood and risk severity, the risk size would be 50%. A likelihood of 5 is related to rules 4-6, and a risk severity of 5 is related to rules 2, 5, and 8. The fuzzy model designed by combining these rules estimates the risk value.

The authors generated and plotted an output surface map for the food processing industry information system fuzzy model using surface viewer to visualize the dependence of one of the outputs on any one or two of the inputs. According to Mamdani, Figure 6 depicts the food processing fuzzy model's output surface viewer.

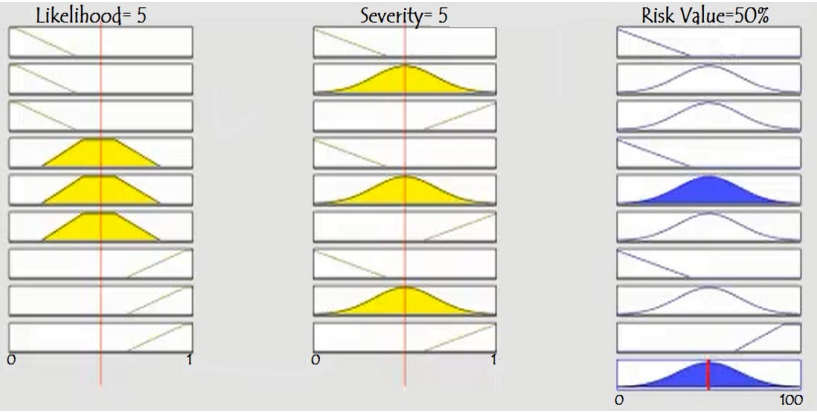


Fig. 5. Fuzzy rules according to Mamdani method

Based on Tables 5 and 6, electronic data in T2 (data theft) has a high effect risk of 75.67%, and human resource management in T14 (social engineering) has a low-risk impact of 26.67%. As a result of this risk assessment, the food processing industry's high-probability risk items necessitate immediate remedial action to mitigate the risk (Figure 7).

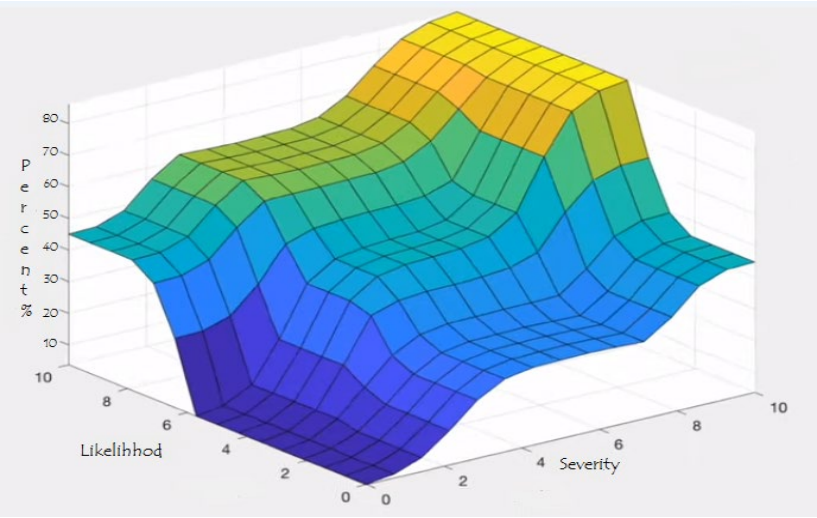


Fig. 6. 3D plots for 9 rules according to Mamdani method

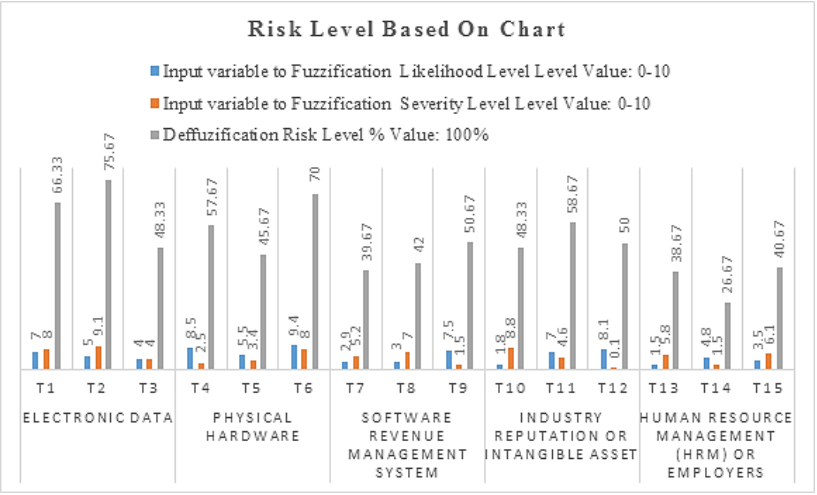


Fig. 7. Risk level based on the chart

5. Conclusion. According to the results of this study, the authors developed a flow model for assessing the risks of activities in the Sub-Saharan food industry. The authors identified five critical food processing industry information systems, including electronic data, physical hardware, software revenue management systems, food processing industry reputation (intangible) assets, and human resource management (HRM).

In order to obtain a more reliable and less subjective method for the risk assessment process, a fuzzy inference system has been used in this model. Nine fuzzy decision rules were constructed for some of the chosen risks by using likelihood, severity, and risk values. Finally, the risk values were calculated in the aggregation and defuzzification processes. Finally, based on the final information security risk values, the risks were ranked from maximum to minimum risk values obtained in the Sub-Saharan African food processing industry.

References

1. Food processing in Sub-Saharan Africa: Solutions for African Food Enterprises. TechnoServes, 2017. 44 p. Available at: https://www.technoserve.org/wp-content/uploads/2018/04/solutions-for-african-food-enterprises-final-report.pdf. (accessed 26.07.2023).
2. Whitman M.E., Mattord H.J. Principles of Information Security. Cengage Learning. 2018. 750 p.
3. Kriaa S., Bouissou M., Laarouchi Y. A Model Based Approach for SCADA Safety and Security Joint Modelling: S-Cube. 10th IET System Safety and Cyber-Security Conference. 2015. DOI: 10.1049/cp.2015.0293.

4. Shin J., You I., Seo J.T. Investment priority analysis of ICS information security resources in smart mobile IoT network environment using the analytic hierarchy process. Mobile Information Systems. 2020. vol. 2020. DOI: 10.1155/2020/8878088.
5. Shamala P., Ahmad R., Zolait A.H., Bin Sahib S. Collective information structure model for information security risk assessment (ISRA). Journal of Systems and Information Technology. 2015. vol. 17. no. 2. pp. 193–219. DOI: 10.1108/JSIT-02-2015-0013.
6. Abbass W., Baina A., Bellafkih M. Improvement of information system security risk management. 4th IEEE International Colloquium on Information Science and Technology (CiSt). 2016. pp. 182–187. DOI: 10.1109/CIST.2016.7805039.
7. Yang M. Information Security Risk Management Model for Big Data. Advances in Multimedia. 2022. vol. 2022. DOI: 10.1155/2022/3383251.
8. Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools. Risks. 2022.
9. Ebrat M., Ghodsi R. Construction project risk assessment by using adaptive-network-based fuzzy inference system: An empirical study. KSCE Journal of Civil Engineering. 2014. vol. 18. pp. 1213–1227. DOI: 10.1007/s12205-014-0139-5.
10. Stebbins-Wheelock E.J., Turgeon A. Guide to Risk Assessment and Response. The University of Vermont, 2018. 17 p.
11. Sobel P.J., Prawitt D.F., Dohrer R.D., Murdock D.C., Thomson J.C., Miller P.K. Compliance risk management: applying the COSO ERM framework. Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2020. 48 p.
12. Chandra N.A., Ramli K., Ratna A.A.P., Gunawan T.S. Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools. Risks. 2022. vol. 10(8). no. 165. DOI: 10.3390/risks10080165.
13. Crotty J., Daniel E. Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment. Applied Computing and Informatics. 2022. DOI: 10.1108/ACI-07-2022-0178.
14. Carlsson E., Mattsson M. The MaRiQ model: A quantitative approach to risk management in cybersecurity. 2019. Uppsala: Uppsala Universitet, 2019. 97 p.
15. Fadyeyeva I., Gryniuk O. Fuzzy modelling in risk assessment of oil and gas production enterprises' activity. Baltic Journal of Economic Studies. 2017. vol. 3. no. 4. pp. 256–264.
16. Papageorgiou E.I., Aggelopoulou K., Gemtos T.A., Nanos G.D. Development and Evaluation of a Fuzzy Inference System and a Neuro-Fuzzy Inference System for Grading Apple Quality. Applied Artificial Intelligence. 2018. vol. 32. no. 3. pp. 253–280. DOI: 10.1080/08839514.2018.1448072.
17. Blasi A.H. The use of Fuzzy Logic Control in Manufacturing Systems. 2020. 12 p.
18. Kotenko I., Saenko I., Ageev S. Countermeasure Security Risks Management in the Internet of Things Based on Fuzzy Logic Inference. IEEE TrustCom/BigDataSE/ISPA. 2015. pp. 654-659. DOI: 10.1109/Trustcom.2015.431.
19. Hadacek L., Sivakova L., Sousek R., Zeegers M. Assessment of security risks in railway transport using the fuzzy logical deduction method. Communications – Scientific Letters of the University of Zilina. 2020. vol. 22. no. 2. pp. 79–87. DOI: 10.26552/com.C.2020.2.79-87.
20. Kaka S., Hussin H., Khan R., Akbar A., Sarwar U., Ansari J. Fuzzy logic-based quantitative risk assessment model for hse in oil and gas industry. Universiti Teknologi PETRONAS, 2022. DOI: 10.17605/OSF.IO/WVG2H.
21. Zhao Y., Talha M. Evaluation of food safety problems based on the fuzzy comprehensive analysis method. Food Science and Technology. 2021. vol. 42. no. e47321. DOI: 10.1590/FST.47321.

Asfha Amanuel — Post-graduate student, ITMO University. Research interests: information security methods and systems, information and cyber security, risk management. The number of publications — 3. baquesti2003@gmail.com; 49, Kronverksky Av., 197101, St. Petersburg, Russia; office phone: +7(952)378-2147.

Vaish Abhishek — Ph.D., Assistant professor, It department, Indian Institute of Information Technology, Allahabad. Research interests: information security, information security laws and regulations, cyber diplomacy, network security, IT Governance, enterprise recourses planning. The number of publications — 66. abhishek@iiita.ac.in; Uttar Pradesh, 211015, Deghat Jhalwa, India; office phone: +91(790)535-6150.

УДК 004.056 **DOI** 10.15622/ia.22.5.5

А.Э. Асфха, А. Вайш

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПИЩЕВОЙ ПРОМЫШЛЕННОСТИ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ НЕЧЕТКОГО ВЫВОДА

Асфха А.Э., Вайш А. **Анализ рисков информационной безопасности в пищевой промышленности с использованием системы нечеткого вывода.**

Аннотация. В последнее время предпринимались различные попытки охарактеризовать угрозы информационной безопасности, особенно в промышленном секторе. Тем не менее, существует ряд загадочных угроз, которые могут поставить под угрозу безопасность данных, информации и ресурсов пищевой промышленности. Целью данного исследования было изучение рисков для информационной безопасности в информационной системе пищевой промышленности, а участниками этого исследования были эксперты исполнительного руководства, штатный персонал, технические и активные операторы, сторонние консалтинговые компании и управление рисками, специалисты пищевой промышленности в информационной системе стран Африки к югу от Сахары. Анкета и интервью с различными вопросами с использованием подходов качественного и количественного анализа рисков были использованы для сбора идентификаций рисков, а также метод системы нечётких выводов, приманенный для анализа фактора риска в этой статье. Выводы показали, что среди проблем информационной безопасности электронные данные в угрозе кражи данных имеют высокий риск 75,67%, а управление человеческими ресурсами (HRM) в угрозе социальной инженерии имеет низкий риск воздействия 26,67%. В результате факторы риска с высокой вероятностью требуют оперативных действий. Компоненты риска с высокой вероятностью требуют быстрых корректирующих действий. В результате необходимо выявить и контролировать первопричины таких угроз до того, как возникнут пагубные последствия. Также важно отметить, что при изучении информационной безопасности в промышленных информационных системах пищевой промышленности необходимо принимать во внимание основные интересы и глобальную политику.

Ключевые слова: пищевая промышленность, информационная безопасность, идентификация рисков, анализ рисков, система нечеткого вывода, ISO 27005.

Литература

1. Food processing in Sub-Saharan Africa: Solutions for African Food Enterprises. TechnoServes, 2017. 44 p. Available at: https://www.technoserve.org/wp-content/uploads/2018/04/solutions-for-african-food-enterprises-final-report.pdf. (accessed 26.07.2023).
2. Whitman M.E., Mattord H.J. Principles of Information Security. Cengage Learning. 2018. 750 p.
3. Kriaa S., Bouissou M., Laarouchi Y. A Model Based Approach for SCADA Safety and Security Joint Modelling: S-Cube. 10th IET System Safety and Cyber-Security Conference. 2015. DOI: 10.1049/cp.2015.0293.
4. Shin J., You I., Seo J.T. Investment priority analysis of ICS information security resources in smart mobile IoT network environment using the analytic hierarchy process. Mobile Information Systems. 2020. vol. 2020. DOI: 10.1155/2020/8878088.
5. Shamala P., Ahmad R., Zolait A.H., Bin Sahib S. Collective information structure model for information security risk assessment (ISRA). Journal of Systems and Information Technology. 2015. vol. 17. no. 2. pp. 193–219. DOI: 10.1108/JSIT-02-2015-0013.

6. Abbass W., Baina A., Bellafkih M. Improvement of information system security risk management. 4th IEEE International Colloquium on Information Science and Technology (CiSt). 2016. pp. 182–187. DOI: 10.1109/CIST.2016.7805039.
7. Yang M. Information Security Risk Management Model for Big Data. Advances in Multimedia. 2022. vol. 2022. DOI: 10.1155/2022/3383251.
8. Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools. Risks. 2022.
9. Ebrat M., Ghodsi R. Construction project risk assessment by using adaptive-network-based fuzzy inference system: An empirical study. KSCE Journal of Civil Engineering. 2014. vol. 18. pp. 1213–1227. DOI: 10.1007/s12205-014-0139-5.
10. Stebbins-Wheelock E.J., Turgeon A. Guide to Risk Assessment and Response. The University of Vermont, 2018. 17 p.
11. Sobel P.J., Prawitt D.F., Dohrer R.D., Murdock D.C., Thomson J.C., Miller P.K. Compliance risk management: applying the COSO ERM framework. Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2020. 48 p.
12. Chandra N.A., Ramli K., Ratna A.A.P., Gunawan T.S. Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools. Risks. 2022. vol. 10(8). no. 165. DOI: 10.3390/risks10080165.
13. Crotty J., Daniel E. Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment. Applied Computing and Informatics. 2022. DOI: 10.1108/ACI-07-2022-0178.
14. Carlsson E., Mattsson M. The MaRiQ model: A quantitative approach to risk management in cybersecurity. 2019. Uppsala: Uppsala Universitet, 2019. 97 p.
15. Fadyeyeva I., Gryniuk O. Fuzzy modelling in risk assessment of oil and gas production enterprises' activity. Baltic Journal of Economic Studies. 2017. vol. 3. no. 4. pp. 256–264.
16. Papageorgiou E.I., Aggelopoulou K., Gemtos T.A., Nanos G.D. Development and Evaluation of a Fuzzy Inference System and a Neuro-Fuzzy Inference System for Grading Apple Quality. Applied Artificial Intelligence. 2018. vol. 32. no. 3. pp. 253–280. DOI: 10.1080/08839514.2018.1448072.
17. Blasi A.H. The use of Fuzzy Logic Control in Manufacturing Systems. 2020. 12 p.
18. Kotenko I., Saenko I., Ageev S. Countermeasure Security Risks Management in the Internet of Things Based on Fuzzy Logic Inference. IEEE TrustCom/BigDataSE/ISPA. 2015. pp. 654-659. DOI: 10.1109/Trustcom.2015.431.
19. Hadacek L., Sivakova L., Sousek R., Zeegers M. Assessment of security risks in railway transport using the fuzzy logical deduction method. Communications – Scientific Letters of the University of Zilina. 2020. vol. 22. no. 2. pp. 79–87. DOI: 10.26552/com.C.2020.2.79-87.
20. Kaka S., Hussin H., Khan R., Akbar A., Sarwar U., Ansari J. Fuzzy logic-based quantitative risk assessment model for hse in oil and gas industry. Universiti Teknologi PETRONAS, 2022. DOI: 10.17605/OSF.IO/WVG2H.
21. Zhao Y., Talha M. Evaluation of food safety problems based on the fuzzy comprehensive analysis method. Food Science and Technology. 2021. vol. 42. no. e47321. DOI: 10.1590/FST.47321.

Асфха Амануэль Эстифанос — аспирант, Университета ИТМО. Область научных интересов: методы и системы защиты информации, информационная и кибербезопасность, управление рисками. Число научных публикаций — 3. baquesti2003@gmail.com; Кронверкский проспект, 49, 197101, Санкт-Петербург, Россия; р.т.: +7(952)378-2147.

Вайш Абхишек — Ph.D., доцент, кафедра информационных технологий, Индийский институт информационных технологий, Аллахабад. Область научных интересов: информационная безопасность, законы и нормативные акты в области информационной безопасности, кибердипломатия, сетевая безопасность, управление ИТ, планирование ресурсов предприятия. Число научных публикаций — 66. abhishek@iiita.ac.in; Уттар-Прадеш, 211015, Дегхат Джалва, Индия; р.т.: +91(790)535-6150.

DOI 10.15622/ia.22.5.6

U. PILANIA, M. KUMAR, T. ROHIT, N. NANDAL

A WALK-THROUGH TOWARDS NETWORK STEGANOGRAPHY TECHNIQUES

Pilania U., Kumar M., Rohit T., Nandal N. **A Walk-through towards Network Steganography Techniques.**

Abstract. 2D and 3D digital multimedia files offer numerous benefits like excellent quality, compression, editing, reliable copying, etc. These qualities of the multimedia files, on the other hand, are the cause of fear including the fear of getting access to data during communication. Steganography plays an important role in providing security to the data in communication. Changing the type of cover file from digital multimedia files to protocols improve the security of the communication system. Protocols are an integral part of the communication system and these protocols can also be used to hide secret data resulting in low chances of detection. This paper is intended to help improve existing network steganography techniques by enhancing bandwidth and decreasing detection rates through reviewing previous related work. Recent papers of the last 21 years on network steganography techniques have been studied, analyzed, and summarized. This review can help researchers to understand the existing trends in network steganography techniques to pursue further work in this area for algorithms' improvement. The paper is divided according to the layers of the OSI model.

Keywords: network steganography, open system interconnection model, protocol, bandwidth, embedding capacity, physical layer, data link layer, network layer, transmission layer, application layer.

1. Introduction. With the enhancement in network technologies multimedia files are used for the transfer of secret data using different protocols. Various protocols are there which can be used to transfer required data from one place to another place [1, 2]. Network steganography is gaining the attention of researchers day by day over other multimedia steganography techniques. Because of increasing reliance on digital communication and data transfer over networks, there is a growing need to secure sensitive information from unauthorized access. Network steganography offers a covert means of hiding data within network traffic, providing an additional layer of security and privacy. Protocols from mostly five layers (Physical, Data Link, Network, Transport, Application) of the OSI (Open System Interconnection) model can be used to hide secret data [3]. The presentation and session layers of the OSI model are responsible for aspects such as data formatting, encryption, establishing and maintaining communication sessions between network entities these two layer does not deal with data hiding. The steganography technique which uses a single protocol to hide secret data is known as intra-protocol steganography. These types of techniques are based on modification in PDU (Protocol Data Unit). Whereas, Inter-protocol steganography uses more than one protocol to hide secret data [4, 5]. It includes padding steganography

which uses more than one protocol to hide the existence of secret data resulting in large embedding capacity, more security, and is highly robust. It has many advantages over 2D and 3D multimedia steganography techniques as follows [6, 7, 8]:

– In network steganography, there are options to design hidden channels on mostly five layers of the OSI model.

– In it, hidden secret data flow in both directions which results in more security and robustness.

– Also, it has short life on the network during the transfer from source to destination.

– In it, the network itself acts as the carrier file, unlike other multimedia steganography techniques.

– The bandwidth of the communication channel is affected by the type of multimedia carrier file used. But bandwidth of network steganography depends only on the type of protocol used to transfer secret data from source to destination.

Steganography started in ancient Greece in the classical form [15, 83, 84]. During that time secret data was embedded in the objects used in daily life. These objects include hair, wax, printer ink, skin, wood table, etc. After that digital steganography came into existence. In digital steganography, multimedia files such as text, images, audio, and video were used to hide secret data. Among multimedia steganography techniques, video steganography has drawn the attention of researchers for many years. But video steganography also has some demerits associated with it. These demerits include low embedding capacity, chances of detection of secret data, and poor visual quality of the stego file.

Classification of network steganography techniques is shown in Figure 1. Intra-protocol network steganography techniques can be broadly defined as updating network packet headers, updating network packet payload, updating the structure of packets, and hybrid techniques. [10, 11]. In the packet header, specific fields of the header of the protocol are modified for the embedding of secret data. Such types of techniques have good embedding capacity but are not very robust against attackers. Steganography techniques are based on the application layer of network model update payload to embed secret data. These techniques have low embedding capacities and are robust against attacks. Steganography techniques based on the structure of the packet may embed data in both headers and payload. In hybrid techniques, the header of the packet as well as time dependencies are modified for the embedding of secret data. Retransmission steganography is one of the best examples of this type of technique.

The efficiency of the network steganography technique can be measured based on the evaluation parameters. These parameters are embedding capacity, robustness, imperceptibility, and bandwidth [12, 13, 14].

– Embedding capacity is the amount of secret information that can be hidden in the protocol header.

– Imperceptibility is the invisibility of secret data inside the cover protocol.

– Robustness is the ability of the stego file to remain unaltered against attacks and stego file is a file that contains concealed or secret data embedded within it.

– Bandwidth is the average concealing capacity of every packet.

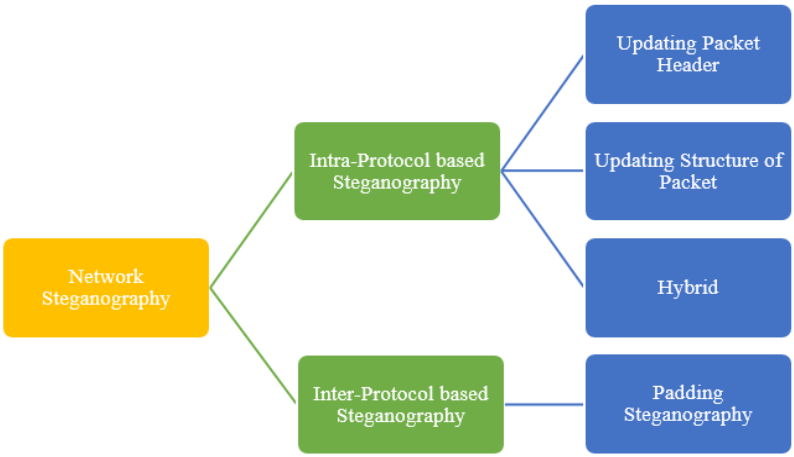


Fig. 1. Network Steganography Classifications [9]

To overcome the demerits of 2D and 3D multimedia steganography techniques, modern steganography came into existence. Network steganography is the modern steganography technique for providing safety to secret data. It provides the next level of security to secret data in a modified way. It hides the secret data into various protocols used at the different layers of the OSI model [17]. The proposed paper reviewed various network steganography techniques based on different layers of the OSI Model. A relationship was identified between the user's need and the steganography techniques to find its applications in hidden communication [6].

2. Methodology. Initially, 154 papers are selected for the review process. Then by applying certain filters, some papers are excluded as

shown in Figure 2. The network protocol-based papers are included for further processing. These network steganography papers are further segregated based on OSI model layers. An analysis of the reviewed techniques is done based on various parameters such as energy efficiency, bandwidth, visual quality of stego file, year-wise, layerwise, implementation tools, the combination of steganography and cryptography tools, etc.

The selected papers were published between the years 2002 to 2023. Papers for the review process are selected from various databases like the Web of Science, Science Direct, IEEE, Springer, Scopus, etc. Initial for the selection of articles for the proposed review paper following two quality assessment criteria have been set:

– Is the literature search likely to have covered all relevant studies?

– Are the review's inclusion and exclusion criteria described and appropriate?

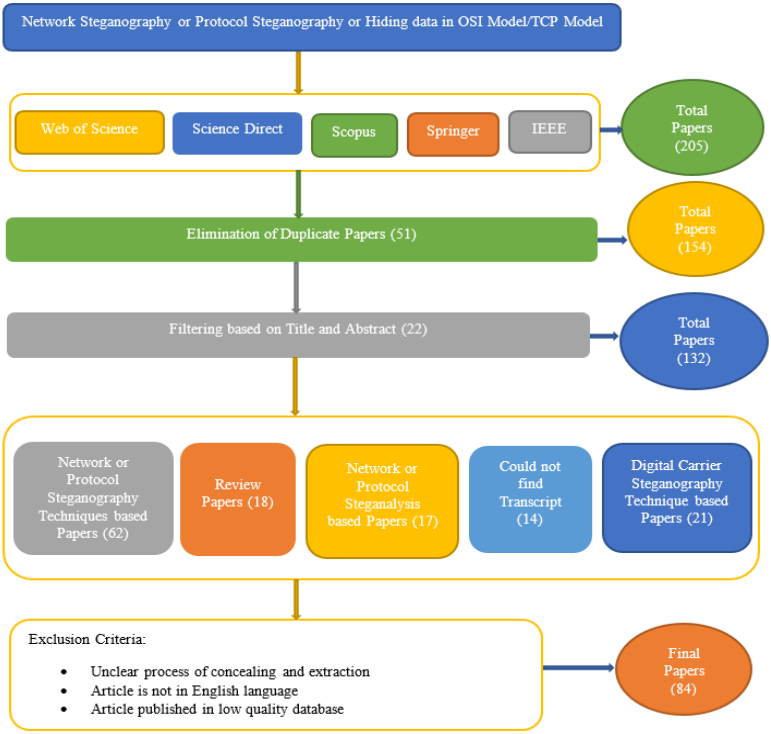


Fig. 2. Identification and selection of articles

All the included articles are published in the English language. Articles that satisfy the above-mentioned quality assessment criteria are selected for the review paper and the required information is retrieved for inclusion in our review paper.

In the research work, 84 articles have been studied and analyzed based on the statistical values. The details such as which layer of OSI model work has been done, which part of a protocol such as body or header has been used to hide secret data, what is the outcome of work in terms of bandwidth, whether work done is robust against attacks or not, steganography technique is combined with cryptography or not, on which tool implementation of work is done, etc. is being retrieved from the selected articles.

The methodology is divided into four stages, as shown in Figure 3.

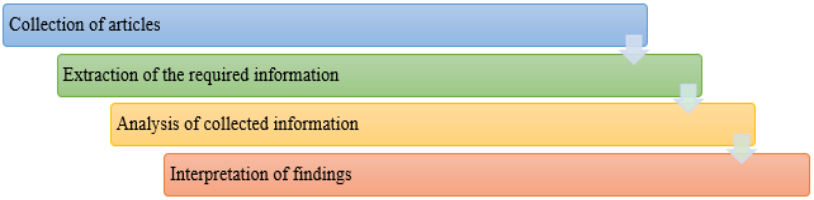


Fig. 3. Methodology Used

In the first stage, articles have been selected from different databases such as IEEE, Scopus, Springer, Web of Science, Science Direct, ACM, etc. for the review process. Duplicate papers are eliminated from the initial selection of 154 papers. The selected papers have keywords like "protocol" or "network steganography." Some papers are again eliminated based on the title and abstract of the paper. Exclusion criteria also include some critical points such as: the concealing and extraction processes are unclear, the published article is not in English, the type of carrier file used to hide secret data, the type of journal or conference, and so on. In the second stage, after exploring the article, the required information is collected and retrieved. The information is collected in the form of tables and diagrams with explanations. The explanation includes where secret data can be concealed and what the impact of hiding secret data has on the carrier file. In the third stage, an analysis of the retrieved information is done based on various evaluation parameters for the network steganography techniques. Various charts have been plotted for the analysis of the work done in the reviewed papers. Last, the statistical analysis was done for the survey of the protocol steganography techniques.

2.1. Hiding Secret Data in OSI Model. OSI model is the reference model for communication over the web. It has seven layers and each layer has its predefined functions. Each layer has a specific set of protocols. These protocols can be used to hide secret data in a different layer of the OSI model [15, 18]. Many papers have been reviewed in this section based on the reference model to analyze how protocol steganography is different from digital steganography.

2.1.1. Hiding Secret Data in Physical Layer. It is responsible for providing all the necessary connections. Data may be transmitted either through a wired connection or through a wireless connection. It decides the mode of transmission of secret data. It converts data into binary form. It has various protocols which can be used to hide secret data [19]. The protocol has various fields in its header format, and these fields can be used to hide secret data. Depending upon the size of the field used to hide secret data, the amount of secret data varies [20]. Some of the papers based on the physical layer protocol steganography are given in the section.

OFDM (Orthogonal Frequency Division Multiplexing) is used in various telecommunication applications. OFDM was the procedure of multicarrier modulation like sound, video, and images. In it, information was sent serially. In OFDM, secret data was hidden in the cyclic prefixes because cyclic prefixes are not read by any of the radio receivers. OFDM converts cyclic prefixes into codes and then converts them into fragments. Generally, prefixes were added earlier to the symbol communication but afterward its modulation. So, the fragments of the secret data should be modulated [21].

Because of modulation, the proposed method was not as effective and secure. So, to improve the security, a pseudo-random number generator (PRNG) was used by both the sender and receiver. With the PRNG, both parties were well synchronised in terms of time. Both the sender and receiver also used the private secret key to protect the data. In the proposed research work, the cost of the steganography technique was increased compared to the normal network. Implementation was done in MATLAB with many configurations of the networks. For the work, SNR (Signal Noise Ratio) was calculated as 4 DB. The embedding capacity was calculated at 3.25 Mbps to 19.5 Mbps, depending upon modulation [22].

In the previous paper, the concealing capacity achieved was very low. So, to achieve high concealing capacity again, the OFDM protocol was chosen by the author, and secret data was hidden in different parts of the protocol. It comes under the 802.11 standards. Its transmission limit of only 100 meters exists in the absence of amplification. As OFDM has its own specific format, fewer amounts of data can be hidden in it and transmitted to

the destination. In the proposed research work, it hides secret data in the padding field of the protocol. Padding carries three subfields, which are data unit, service, and tail. The size of the service and tail is fixed in the case of OFDM, but the size of the data unit may vary with the type of operation performed by the user. OFDM takes input from the user in the form of a signal. It then performed modulation on the given input signal. An Inverse Fast Fourier Transform was applied to hide the secret signals. Again, modulation was done to generate the OFDM signals. Now the transformed data is travelling through the web for its delivery to its destination. A reverse process was performed at the destination to get the original output data.

In the research work, it was considered that there were frames that were ready to transmit. The error rate was fixed by the authors to maximise the bandwidth. The rate of data transmission was also fixed for all the stations in the network. All the frames were carried at a constant length. Data frames and acknowledgment frames were exchanged between nodes for communication purposes. For the work, the maximum bandwidth obtained was calculated as 1.54 Mbps. For the data frame, it was calculated at 1.1 Mbps and for the acknowledgment field, it was calculated at 0.44 Mbps. The bit error rate was calculated as 10-5 for the research work, which was not noticeable by naked human eyes [23].

Worldwide Interoperability for WiMAX (Microwave Access) is a broadband IEEE 802.16 standard model. It can deliver advanced data rates with improved coverage. It works on the MAN (Metropolitan Area Network). It efficiently encodes and decodes the signal without information loss and then transmits it to the destination. It is commonly used in video conferencing and streaming, VoIP (Voice over Internet Protocol), e-learning, etc. WiMAX uses TDD (Time Division Duplex) and FDD (Frequency Division Duplex) for bidirectional communication. In the proposed work, WiMAX frame padding and the RS (Reed-Solomon) were both used to hide the secret data. The efficiency of the proposed work depends on the resources used and the network conditions. Implementation of the work was done in MATLAB and its performance was evaluated based on parameters such as duplex type, bandwidth, frame duration, guard intervals, etc. In the padding field of 802.16, sequences of zeros were stored. Sequences of zeros were replaced by the secret data and then transmitted to the destination. The stego file was transmitted through downlink frames. Each downlink frame has a header, a broadcast message, and data. The data field was almost 2035 bytes long, and the header has a length of 6 bytes.

The size of the secret data embedded depends on the network conditions. On embedding a large amount of secret data, noise increases,

resulting in the detection of secret data. WiMAX can operate on two networks: ATM (Asynchronous Transmission Machine) and packet network. cell has a size of 53 bytes, and the size of an IP (Internet Protocol) packet varies from 40 to 1500 bytes. As IP packets have a very large size compared to the ATM packet, they could hide a large amount of secret data without its detection. Apart from that, RS codes were also used to hide and send the secret data. This secret data was hidden in binary form in the sequences of RS code. The RS encoder helped to hide the secret data, and on the receiver side, the RS reader read the secret data. After reading secret bits of data, the receiver side retrieved them. On hiding secret data in IP packets at the rate of 60.4 Kbps, SNR was calculated as 25 DB. But hiding secret data in RS code at the rate of 0.8 Kbps SNR was calculated as 25 DB again [25].

ZigBee is the IEEE 802.15.4 standard PAN (Personal Area Network) protocol. It has applications in home automation, radios, medical devices, heating controls, smoking sensors, science, etc. ZigBee has four types of data frames that could be used to hide secret data. The ZigBee protocol stores secret data in the reserve bits of the protocol for security purposes in the proposed research work. The process of secret data transfer must be hidden from a third party; otherwise, hackers may detect it. Secret data was first encrypted by using the public key, and at the receiver side, it was decrypted using the private key. Secret data was taken in the form of text. ZigBee uses AES 128-bit encryption for security purposes. It has a low embedding capacity of 64 bits but has fewer chances of detection of secret data [26].

Figure 4 shows the summary of the work done on the physical layer of the OSI model. For the analysis of the research, the authors have taken different parameters like BER, Bandwidth, Embedded capacity, SNR, etc. BER is the error rate per pixel. SNR is the signal-to-noise ratio in the carrier file. Bandwidth is the amount of secret information that can be embedded per unit of time. Embedding capacity is the total amount of secret information that can be hidden in a carrier file.

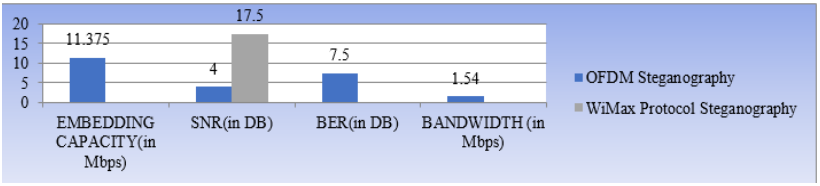


Fig. 4. Overview of Network Steganography in Physical Layer

2.1.2. Hiding Data in Link Layer. The data link layer is the second layer of the OSI model. It carries data in the form of frames. It is responsible for flow control, error control, and access control. It has many

protocols such as stop and wait, selective repeat ARQ, aloha, slotted aloha, CDMA, and many more to perform various tasks. Flow control, speed of the source, and destination need to be synchronized to minimize the traffic and to get the maximum throughput [27].

In the proposed work [28], DCT (Discrete Cosine Transform) and CDMA techniques were combined to hide the secret data. DCT was used to convert the given signal from the spatial to the frequency domain. DCT was performed up to two levels for finding the most refined coefficients and the noisy coefficients. Noisy coefficients were used to hide the secret data. Each DCT transformed coefficient was able to hide 1 byte of secret data. On increasing embedding capacity stego file might result in more distortion. The proposed codebook steganography technique divided the secret data into binary forms. A unique pseudo-random number sequence was used to divide the secret data. CDMA generated the pseudo-random number by utilising the concept of direct spread spectrum. With the help of pseudo-random numbers generated, multiple accesses on the channel could be performed without any interference. Pseudo-random numbers were transformed to status bits-1 and 1 [29]. These status bits were then multiplied by bits of secret data to produce sequences of data. These produced sequences were then added to get the complete data. The concept of CDMA improved the embedding capacity of the proposed work. The highest embedding capacity of the work was calculated at 9728 bytes, and the highest PSNR (Peak Signal to Noise Ratio) was calculated at 53.80 DB.

With the advancement in computer technology, the day-to-day security of online data is becoming a major concern among users. So, in this paper, cryptography, compression, and steganography were combined by the authors to provide security to the online data during communication. The authors used the blowfish-448 encryption algorithm for the compression of the file. Passphrase encryption was also applied to convert the secret messages into the scrambled form. Then the stop-and-wait protocol was used to hide the secret data inside the image. The amount of secret data embedded was 255 Kb without compression. The proposed work was also analysed for the security measure. The stop-and-wait protocol is the simplest protocol at the data link layer of the OSI model. It synchronises the speeds of the sender and receiver, resulting in low traffic and high throughput. In the proposed work, secret data was embedded in the retransmitted frame [30].

JPEG (Joint Photograph Expert Group) image was taken as the frame for the transmission of secret data. Secret data was taken as text in the proposed work. A passphrase was generated by the sender to avoid the detection of secret data. A key agreement was required between the sender and receiver of secret data. The same key was used at both ends for

encryption purposes. DH (Diffie–Hellman) key exchange protocol was for the key. The keys were exchanged in the numerical form resulting in no doubt to the third person. The encrypted secret data was then compressed using the blowfish-448 algorithm. The blowfish algorithm could use the variable key length varying from 32 bits to 448 bits resulting in the improved security. Because of the compression the embedding capacity was also improved. At last secret data was embedded into the image and it was transferred to the destination in the retransmission frames. The blowfish algorithm avoids the detection of secret data by applying different attacks. The proposed work embedded the secret data of approximately 255 Kb. Histogram was plotted for the original and the stego image. The histogram showed the frequency distribution of both images. The quality of original and stego images seemed to be almost equal resulting in less chance of detection of secret data [31].

The utilization of steganography and cryptography together elevates the complexity of the technique. However, when employed in combination, this approach can enhance the security of the technique to a certain degree. 802.15.4 also works on the data link layer of the OSI model. It is a part of the MAC (Media Access Control) layer under the data link layer. It is also known as the low-rate wireless personal area network. It was defined in 2003, and it acts as the base for Zigbee. It has essential support for the secure transmission of secret data. It is also able to manage the energy of wireless networks [32].

The frames in it contain many fields like frame control, the sequence number of data, source address, destination address, payload, reserved bits, command type, acknowledgment, etc. Any of these fields could be used to hide the secret data. Depending upon the size of the field secret data size varies. For the implementation of the research work, the AvroraZ simulator was used. The payload part of the frame has a large concealing capacity. In the proposed work data was hidden in the data frame. All 5 fields of the data frame were used to hide secret data one by one. The proposed work was robust against attacks and carried good embedding capacity [33].

Figure 5 shows the summary of the papers reviewed at the data link layer of the OSI model. For the evaluation of the work, different parameters were used by the authors. Some of the parameters are also given in the table such as concealing capacity, PSNR, energy consumption, histogram analysis, etc. The histogram analysis showed the frequency distribution of the stego and the original image. PSNR finds the error present between the original and the stego file. Concealing capacity is the amount of secret information that can be embedded inside the carrier. Energy consumption is the amount of energy used to conceal and extract secret information.

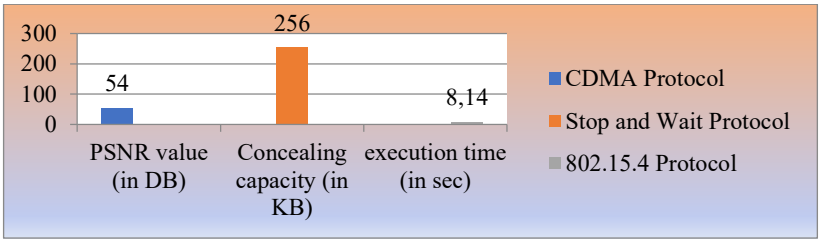


Fig. 5. Overview of Network Steganography in Data Link Layer

2.1.3. Network Layer Steganography Techniques. It is the third layer of the OSI model. It is responsible for providing routing. Routing helps to find the shortest path having low traffic. At the network layer concept of IP address is introduced. The IP address is 32-bits long and can be represented in either binary format or decimal format. Protocols such as IPv4 (Internet Protocol Version 4), IPv6 (Internet Protocol Version 6), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol), etc., at the network layer, can be used to hide the secret data [34, 35]. Every protocol has its header format and various fields. More than one field can be used to hide the secret data. Hiding secret data in more than one field of protocol results in high security and large embedding capacity.

IPv4 works on the 3rd layer of the OSI model. It helps to find out the shortest possible path with almost no traffic. IPv4 has routing protocols such as border gateway protocol, routing information protocol, open shortest path first algorithm, etc. IPv4 creates a routing table for all the nodes in that particular network. Then smartly calculate the distance between a set of nodes along with measuring traffic. In the proposed research work, option field of the IPv4 protocol was used to hide the secret data. LAN (Local Area Network) was chosen to hide the secret data. LAN consists of a sender, receiver, router, and other intermediate nodes. The nodes in the LAN are connected either by wireless connection or through a wired connection. The sender has chosen 20 bits of input from the customer and then decomposes these 20 bits into 5 parts of each 4 bits. These decomposed bits are converted into a timestamp for sending data to the destination host. The overflow field was used to find the number of routers that are ideal in the network. Ideal routers did not create any timestamps. So, these timestamps were used to deliver secret data to a destination.

IPv4 used UDP (User Datagram Protocol) to transmit the packet from the sender to the receiver. To send secret data port number 11234 was used. At the receiver end, a Python script was used to retrieve secret data from the timestamps. In Python, the Scapy library is suitable to examine the packets and retrieve the secret data. All the five-time stamps were examined

to retrieve complete secret data. 10-time stamps were also created with the help of the same protocols to check the variation in the result. In the research work overall, bandwidth was calculated at almost 20 bits/packet. In the research work, packet loss was found to be almost zero [12].

In the above research work, the bandwidth was used to measure the performance of the work. The bandwidth was found to be very low for the mentioned work. So, to overcome the issue of low bandwidth some other protocols from the same layer were used. At the network layer, both ARP and RARP work. ARP has the IP address of the destination node and calculates the physical address of the same node. As the name suggests RARP is the reverse of the ARP protocol. Both ARP and RARP send the multicast request. Multicast means the request is sent to all the nodes connected to the network. The reply is unicast in the case of both protocols [36].

ARP network steganography was proposed in the local area network. LAN has sender and receiver nodes with lots of intermediate nodes. Secret message length was calculated and then the encoding of the secret message was done in hexadecimal notation. An unallocated IP address was searched for steganography. For finding an unallocated IP address a request was broadcasted to all the nodes in the local area network. Based on the reply an unallocated list of IP addresses was created. This process is repeated to make sure about the unused IP addresses. Then a seed value was entered to produce a set of random numbers. Seed value again helps to find the unallocated IP address. Now the receiver sends the ARP broadcast reply to the nodes in the network. The source host sends the unicast reply with the embedded bits of secret data on the physical address of the sender. At a time, the source node sends only 11 bits of secret data. On the receiver side, the same procedure was repeated to find the list of unallocated IP addresses. Then the value of the seed was inputted to confirm the unallocated IP address. Both source and receiver nodes put the same seed values. Now the receiver node retrieves the secret message. By using the ARP protocol 44-bit message was embedded in the ARP reply [37].

Hidden communication that does not depend on direct traffic between a sender and receiver is known as a "dead drop." In this proposed paper, ARP and SNMP (Simple Network Management Protocol) were used to hide the secret data. SNMP is the most commonly used protocol for reading information about the configuration and status of network devices. It can also modify the information of the network devices to change the behaviour of the network. Network devices commonly include cables, routers, switches, hubs, bridges, computers, servers, printers, and many more.

ARP cache was used to hide the secret data for the research work. The Sender's IP address and the physical address were utilized to hide the secret data. The complete process was done in a LAN environment. The IP address was controlled in the LAN environment due to the explicit subnet and isolated IP range. Along with that sender also monitor the traffic so that the existing address does not collide. The physical address has 48 bits so out of these bits last three bytes could be used to encode the secret data. As physical address was less controlled in the LAN resulting in a low chance of detection of secret data. Secret data was also decomposed into multiple parts to fit into the available space in the physical address of the ARP packet. Now at the receiver end, SNMP read the secret data that were hidden by ARP. Retrieved secret data by the SNMP was combined back to obtain the complete secret data. The hidden secret data was not detectable by any steganalysis technique [38].

A very less amount of secret data that is 11 bits per packet were hidden in the above research work. Steganography is not a simple task. It takes a lot of time and computer resources to hide the secret data. So to justify the research work a reasonable amount of secret data needs to be sent to the third party. IPv4 is the older version of internet protocol and its position is overtaken by IPv6. Several covert channel options were available in internet protocol to hide the secret data [39]. IPv6 could be used to hide secret data. The size of secret data hidden varies with the size of the field chosen. Bandwidth is also affected by the selection of fields for hiding secret data. As IPv6 has many fields and any field can be used to hide data. In the proposed research workflow label field was chosen to hide secret data. The flow label is 20 bits so the maximum of 20 bits can be hidden at a time. RSA (Rivest-Shamir-Adleman) encryption was applied to scramble the secret data. Chaos theory was also used to encode the secret data. Chaos theory is subtle to the initial settings, it is non-repeating and constrained. It introduces randomness in the input secret data. By using encryption and chaos theory along with network steganography security of the system was improved.

At the side of the sender, secret data was inputted as shown in Figure 6. On the input data, the fifth-order chaotic map was applied to encode the data. On the generated encoded data RSA was applied for scrambling. Generated ciphertext was converted to ASCII value first and then into hexadecimal. Again, the hexadecimal was converted to the binary value. The binary value was converted into sets of 20 bits each. Then one by one these sets were embedded into 20 bits' flow label field of IPv6. The packet number of IPv6 was sent to the destination and at the destination, the receiver retrieves secret data by applying a decoding algorithm. During decoding reverse process takes place. The proposed work was robust against attacks [40].

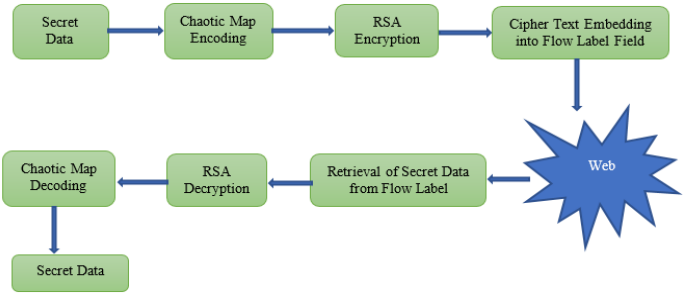


Fig. 6. Secret Data Hiding in IPv6 Flow Label [40]

Figure 7 shows the performance of the network layer protocol steganography techniques. For the evaluation of the work concealing capacity, concealing and retrieval time were used by the authors. Concealing time is the amount of time used to hide the secret data inside the carrier file. Retrieval time is the amount of time required to extract the secret data hidden in the stego file. Concealing capacity is the amount of secret data that can be embedded inside the carrier. Network steganography is most commonly used by many researchers to hide secret data.

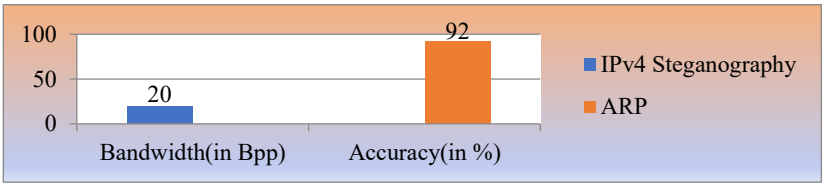


Fig. 7. Summary of Network-Layer Protocol Steganography Techniques

2.1.4. Transport Layer Protocol Steganography Techniques. It is the heart of the OSI model. On this layering concept of a port, address is introduced. It has protocols like TCP, UDP, SCTP (Stream Control Transmission Protocol), and many more. This layer provides both types of services such as connection-oriented and connectionless. TCP is a reliable protocol as its receiver after receiving a message sends an acknowledgment to the sender [41]. On the other hand, UDP is a connectionless and unreliable protocol. Again, the protocol header, as well as the data part, can be used to hide the secret data at this layer also.

The limitation of low embedding capacity can be enhanced by taking video as a carrier file. Popular social networking sites like Facebook, Skype, YouTube, and Wireless network are the focus of attackers for the detection of secret data. Along with carrier file protocols are also used to provide

security to personal data. In the proposed research work network steganography was performed by the authors to hide data. PRNG was used to minimize the chances of detecting secret data. For decoding secret data secret key was used which was generated using PRNG. This processed data was hidden in the header field of the TCP/IP protocol. Proposed techniques include sender, receiver as well attacker for the detection of secret data.

After embedding of data compression of stego file was done to reduce its size back to normal. Secret data embedding was done in the various fields of TCP/IP protocol. Embedding data in more than one part of the carrier file results in good embedding capacity as well as improved security.

The introduction of random number generation increased the security of the system. Along with that, the concept of the fake key was also introduced to mislead the attacker in case they got access to concealed information. Secret data and keys, along with fake keys, were sent to the receiver. The generated key and location of bits of secret data were shared by the sender with the receiver. At the receiver end, the same key was used to encode data that was previously generated by the sender. The Stego file was decrypted and decompressed to retrieve the secret data. The quality of the recovered secret data is high [4].

The mechanism of using keys in steganography increases the security of the techniques, but along with that, complexity also increases. The security of secret data also varies with the size of the packet used to hide it. Secret data can be distributed randomly over the UDP protocol, resulting in more security. The secret message was decomposed into N 4-bit numbers. A matrix with 16 rows was created to store the decomposed numbers. The 4-bit number was converted to binary form before being sent to the destination. This binary secret data was sent successively through the chatting system. The length of the original cover file as well as the stego file was calculated by the receiver. For the retrieval of secret data, modular arithmetic was calculated by the receiver [9].

Research work was simulated for the 50 different chat models. The length of the original and stego files was calculated for all 50 chat files. Time series were performed for both original and the stego files. Time series has shown the difference in packet length pattern of both files. So, secret data could be detected with the help of time series performed on the chat group. By using the UDP protocol difference in the packet length pattern could be reduced. Because UDP introduces randomness in the packet length resulting in more security [9].

Detection of secret data has become easy on concealing a large amount of secret data. The proposed research work used TCP and UDP for concealing secret information as shown in Figure 8. Hiding data into two

protocols avoid network traffic and increases randomness. Randomness results in high robustness for the proposed work.

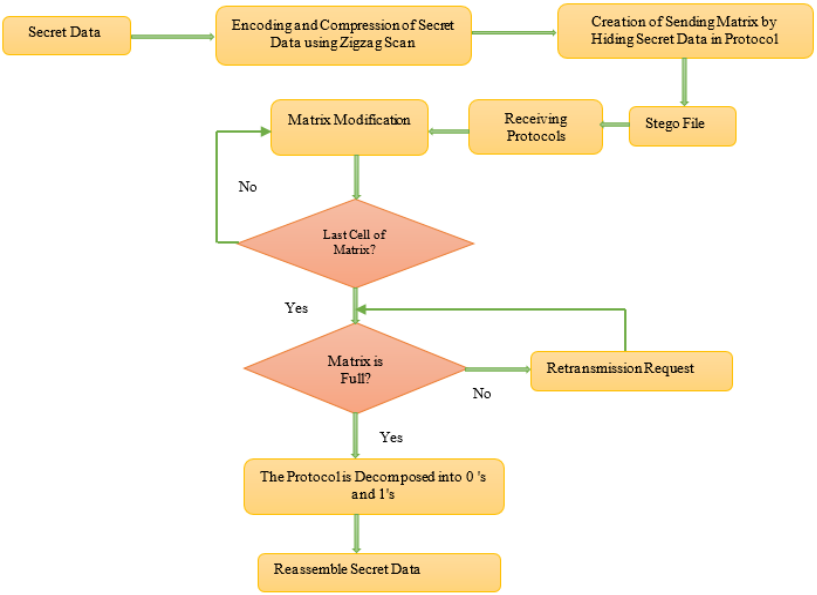


Fig. 8. Embedding and Retrieval of Secret Data [42]

The feasibility test as well as the bandwidth of the proposed work was calculated to analyze imperceptibility. For checking feasibility secret image was converted into binary form. These binary values were stored in the matrix. Each cell of the matrix has a decimal number that was equal to a pixel in the secret image. The dimensions of the matrix were reduced by using the zigzag method. This reduced matrix was sent to the receiver under TCP or UDP protocol. The receiver first converts the reduced matrix to the original matrix then-secret data was retrieved. The retrieved data was compared to the original secret data to compare the quality of the research work. The process was repeated 100 times for the set of images. The average bit error rate was calculated as 0%. The relationship between bandwidth and undetectability was also found by the authors in the proposed work. To provide no packet loss and almost no traffic bits of secret data need to be embedded is 1 bit per packet. In case of loss of secret bit, retransmission of a particular packet takes place resulting in low bandwidth. The bandwidth for the proposed research work was calculated as 0.998 Bpp [42].

In the world of the computer, everyone tries to transfer data in digital form. Transfer of online data also results in concerns about security issues. Using steganography, secret data can be transferred to the destination without the third party's knowledge. RSTEG (Retransmission Steganography) is applied when retransmission of packets is required. If TTL (Total Time to Leave) expires and no acknowledgment is received from the destination, then retransmission of the packet takes place. The RSTEG was applied to the TCP as it is the most reliable protocol. RSTEG comes under the hybrid class of network steganography techniques. Its main objective is to check the number of retransmissions, not to recognise the received packets.

In the process of sending secret data through RSTEG, both the sender and the receiver should be aware. When retransmission of the packet was required, then-secret data was encapsulated inside the packet itself. On the other hand, the receiver extracts secret data from the packet. Depending upon the amount of secret data embedded and the retransmission rate, the performance of the technique can be measured. RSTEG was implemented in the Linux environment. Its performance was measured through bandwidth, retransmission differences in packets, and the throughput of TCP. The proposed method has high bandwidth and embedding capacity compared to other existing network steganography techniques [44].

SCTP (Stream Control Transmission Protocol) was developed in 2000 and is the replacement for the TCP protocol. It is also a reliable protocol like TCP and sends data in sequence. It is also able to provide congestion control at the transport layer of the OSI model. SCTP overcomes the demerits of the TCP protocol. It sends a packet in the same order in which it receives the packets. It informs the receiver in advance about the non-transmission of a particular packet. In TCP, complete data is sent in one stream, but in SCTP, data can be sent into multiple streams. These multiple streams are independent of each other and can be transmitted independently.

The author proposed 13 chunks in the paper to hide the secret data, which were: init, ack, data, authorized, pad, etc. In the second method, SCTP packets were updated to hide the secret data. Multihoming was the main feature that could be updated. In this method, first, a path was tried to send the hidden secret data; when communication failed through this path, another path was chosen to transmit the data. Multi-streaming is another way to transmit secret data. SCTP used multiple streams to transmit the data. The value of the data was different for different streams. The last method was a hybrid of both the above-mentioned methods. Steganalysis techniques were also tried in the proposed work to identify the hidden secret data. But the hidden data was not exposed by any of the steganalysis techniques. Bandwidth was calculated to measure the quality of research work. The maximum bandwidth of 320 Bps was calculated

for the variable parameters under the category of the content modification method of SCTP. The minimum bandwidth calculated was 4 bits per chunk for authenticating parameters [45].

Improvements in the concealing capacity or the bandwidth of the technique may result in the loss of secret data because of compression. LACK (Lost Audio Steganography) was created in 2008, as shown in Figure 9 [46]. has its application in telephony steganography? To hide the secret data, it updates the RTP (Real-time Transport Protocol) packet in terms of audio and time dependencies. The sender chooses RTP from the audio stream and then its payload is replaced by the bits of secret data. RTP was an extremely overdue packet, and such types of packets were not used in the reform of secret data. These chosen RTP packets were intentionally overdue before transmission took place [47].

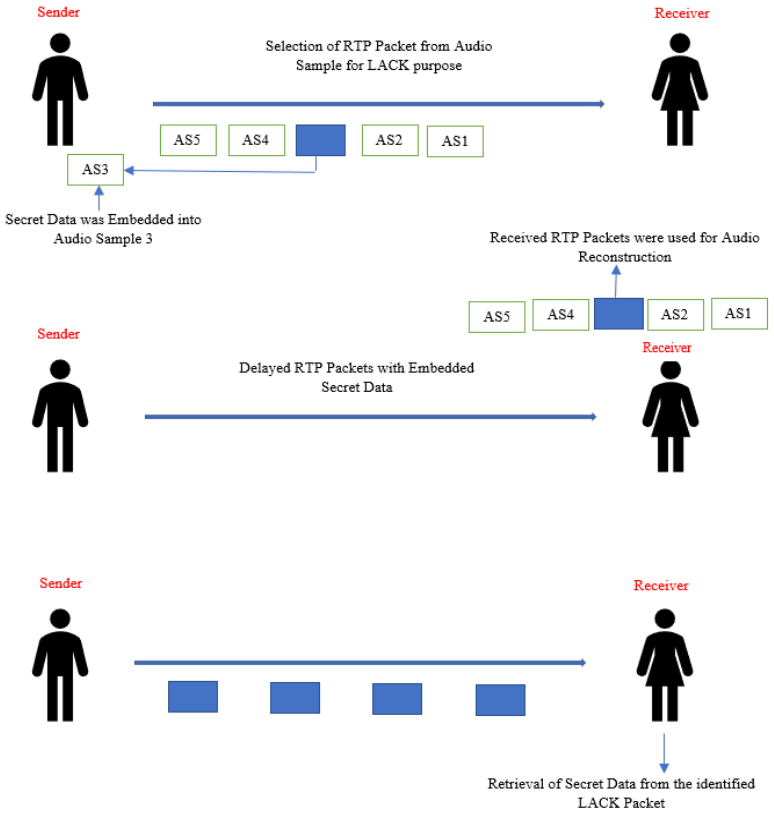


Fig. 9. LACK Steganography Process [46]

When these packets reach the receiver then he/she ignores these packets unaware of the hidden data. In case when the receiver is aware of the hidden data then he/she must retrieve it. LACK followed the hybrid method as it was the combination of time and storage. Time helped in the selection of RTP packets and storage would be responsible for hiding secret data. LACK could also be combined with the VoIP technique [48, 49]. In LACK with VoIP worked with a sequence number and the timestamp field. This technique was further extended by many authors. LACK was also combined with TCP protocol.

StegBlocks-based network steganography technique was proposed by the authors. Using it secret data was hidden in the network traffic. The performance of the research work was checked against malware. Static and dynamic analysis was done for the exposure of secret data. The behaviour of the network traffic was also studied for the detection of secret data. StegBlock used transport layer protocol to hide the secret data. It used two guards or the uniquely created packets which act as the separation between the characters. In the given Figure 10 block 1 and block 5 acted as the guards. Sending no packet between the guards means the value field has 0. Next time 4 packets were sent between blocks 1 and 5 which means value field=5.

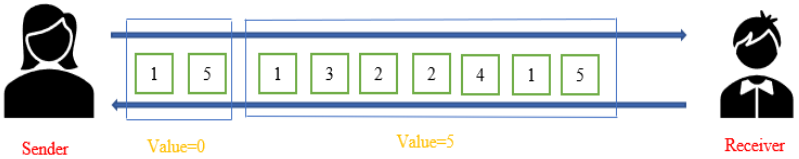


Fig. 10. StegBlock Process [50]

In the process of StegBlock, originally the SCTP protocol was used, and then many researchers used the TCP protocol as well. It usually transmits secret data in the form of text. It converts text data into binary form and then transmits it in the form of 0 and 1. In the SCTP protocol, guards act as the streams of blocks. One guard acts as the encoder and the second acts as the decoder. The proposed work has a low bit rate as compared to the existing research work. The bitrate depends on the traffic of the network. It was also carried out through lossy compression, in which case part of the secret data might be lost. As the bitrate increased, the chances of detection of secret data also increased. One more thing that needed to be taken care of was the involvement of the client [50].

In network steganography, secret data is hidden in protocols. It is a trend since 2003 and is growing among researchers. In this research article, the concept of the dead drop was applied to hide the secret data. When

secret data is not passed directly between sender and receiver but comes through a third person, that process is known as a "dead drop". But in Dead Drop, the third person is not aware of the hidden secret data. A dead drop is also known as the broadcast of secret data. NTP (Network Time Protocol) is the most commonly used protocol for providing time synchronisation for all the devices connected to the network. The data transmission of the NTP protocol is based on the routing protocols. NTP can also handle the monitoring and configuration mode using UDP protocol.

The NTP client and server carry data about the communication partner in the variables. These variables are of two types: system variables and peer variables. System variables carry data about themselves, but the peer variable has info about its surrounding system also. In this paper, the peer variables were used. Peer variables carry the IP address, physical address, port number, subnet mask, etc. The proposed work represents two methods that were discussed for reading and writing secret data to and from the NTP protocol based on a dead drop [51].

Data Hiding in Refid: In NTP refid field was used for hiding the secret data. The refid field carried the complete information of synchronizing the time of the server and the associated devices. Primary servers are connected to the secondary servers and so on. Through the mentioned connectivity complete information of time synchronization was provided for all the devices connected in the network. The IP address of the devices helps to synchronize the time of the whole network. Secret data was hidden in the IP address and no one was aware of it except the sender and receiver. As the IP address is 32 bits so a total of 32 bits of secret data can be hidden. Now NTP utilized broadcast mode which was: the client might have the broadcast IP address in that case all the packets sent to the broadcast address were accepted by the client.

Data Hiding in MRU (Most Recently Used) List: This method used a list of the most recent client and servers for hiding the secret data. For editing and writing data to the MRU list a request needed to be sent to the dead drop. MRU list has all the information about the request made by the client. So, no association was required between the drop and the sender of the data. NTP clients were requested to share the data about local time with everyone on the list. The address field of the MRU list was used to hide the secret data. 4 bytes of secret data could be hidden in the address field. Port addresses could also store 2 bytes of secret data. For retrieval of secret data at the receiver end, the receiver needs to answer some queries. After getting a satisfactory answer from the receiver within 20 seconds secret data can be retrieved.

Both the proposed covert channel was implemented into the Python language using the Scapy library. The reliability of the proposed work was also checked by the authors. The throughput of the proposed work was measured in the number of bits transferred per unit of time. Throughput was calculated as 240 bytes per minute. It is the secret data communicated with the number of entries on dead drops. A detectability test was also performed by the authors to check the robustness of the proposed work [52].

Figure 11 shows the summary of the transport layer protocol steganography. Different evaluation parameters were used to evaluate the research work. The evaluation parameters used were BER, bandwidth, variance, skew, mean, median, and payload capacity. All the parameters measure the quality of research work in different aspects. The original cover protocols were studied and then secret data was hidden in the suitable fields which are less exposed to the third person. Transport layer protocols are very useful in hiding secret data in various fields.

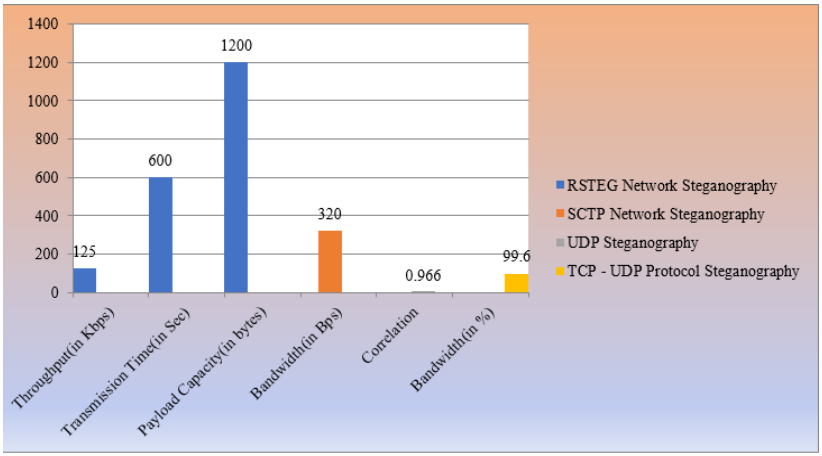


Fig. 11. Summary of Transport Layer Steganography Techniques

2.1.5. Hiding Data at Application Layer. The application layer is the uppermost layer of the OSI model. It is responsible for the user interface. With the help of the application, layer users interact with the system for performing various applications. It has many protocols like HTTP (Hyper Text Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name Server), FTP (File Transfer Protocol), POP (Post Office Protocol), SNMP, Telnet, and many more [54]. Header as well as data part of these protocols can be used to hide the secret data.

HTTP is the best option to hide secret data. The web is growing dynamically these days so the use of HTTP protocol is also increased. HTTP is the binary protocol having many features such as [55, 56]:

– At a time, several HTTP requests can be transferred through TCP connections as distinct streams. HTTP reply might be received in some other order. HTTP can use the same connection to transfer more than one request at a time.

– It can perform server push. In server push, if the server knows that some resources are needed by a particular website then it can fulfill the request.

– It can compress the header size of the file drastically.

– It can set priority among the multiple requests sent by the client.

– It is bidirectional or it can transfer data in both directions.

– The padding field of HTTP protocol can also be used to hide the secret data.

DNS-based network steganography was performed in the paper. DNS is the protocol that converts the domain name of any website into an IP address. Any field from the header format of DNS can be used to hide the secret data like name, type, class, TTL, message length, IP address, etc. In the proposed work secret data was hidden in more than one above-mentioned field. Secret data was converted to the binary form and then the complete message was divided into the block of 4 bits each. The DNS application was written in Java language. Java helps to manage the network tasks and supports multithreading. It is a real-time algorithm with no delay. Testing was done on a virtual machine having window7. LAN having a router was used to experiment. Users browse the web according to his/her interest. He/she searches the content on the web and then moves to another website. In this way, many web pages were visited by the user. During web browsing, the malware was launched. The malware sent a number of packets carrying secret data to cooperating server every second. The process of browsing was monitored by malware continuously. In 600 seconds, 17.3 Kb of secret data was sent by the proposed technique. The proposed research has high security [57].

In the proposed paper, DNS transmits secret data by establishing a connection. As it worked along with TCP so it guarantees the delivery of packets. After the connection was established, the selection of secret data was done. A personal ID was generated for the user. The seed was generated that helped in producing a random number. The secret message was checked for its type. HMAC (Hash-based Message Authentication Code) was applied to encrypt secret data. The encrypted message was encoded by a random number. The complete process on the client-side is explained with the help of Figure 12.

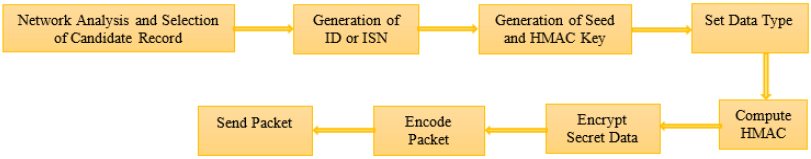


Fig. 12. Data Transmission from Client-Side [58]

At the receiving end, decoding of the secret data was done as shown in Figure 13. Then it was decrypted using the HMAC algorithm. The retrieved secret data was matched with the original secret data. HMAC helped in checking the integrity and authenticity of secret data.

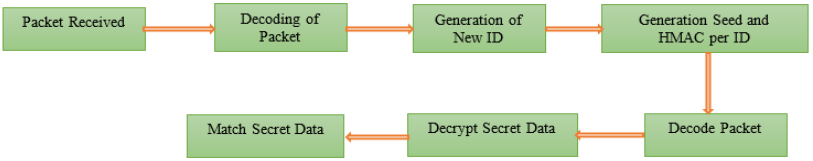


Fig. 13. Data Transmission at Server-Side [58]

Simulation of work was done in Python programming. User records used were of character and integer type. Two datasets were taken to check the traffic and other characteristics of the channel. One dataset was chosen from the home network and the other from the xDSL network. Different sizes and format files of secret data were tried to check the performance of the work. The average embedding capacity of 2.65 bytes of secret data was hidden in a packet. About 72 packets were transferred in 30 seconds [58].

Energy efficiency is also the most important parameter in network steganography. It is a new concept that uses the protocol to hide secret data. CoAP (Constrained Application Protocol) is a unique protocol that can constrain the devices in the network. CoAP works on the client-server model. The client sends the request to the server and then the server search for the result in its database. After collecting a response, it sends back the reply to the client. It describes 4 categories of communications: Confirmable (CON), Non-Confirmable (NON), Acknowledgment (ACK), and Reset (RST). Reliable service provided by this protocol is known as CON and unreliable services are known as NON [59].

The version field represents the current version of the protocol and requires two bits. The 2-bit Type field represents the 4 categories of communication i.e., CON, NON, RST, and ACK. 4-bit token length field and represent the error in the message format. The 8-bit code field is divided into two parts: the most significant and the least significant bit. It

determines the type of message: client request, client error response, server response, server error response. 16-bit message perceives matching communication and acknowledgment. 64-bit token field used to associate request and response. The 64-bit option field represents a set of options for the request and response query. Payload is another field in the protocol which represents the request and responses from users. Any of the fields of the CoAP protocol can be used to hide the secret data. If a particular field is represented in more than one way that means secret data can also be hidden. The embedding capacity and robustness of the technique change as the covert channel changes. The quality of the research work was measured in terms of PRBR and concealing capacity. A maximum of 2040 PRBR was obtained for the case-insensitive part of URI in 10 seconds. A low of 1 PRBR was calculated for many options such as delete, conditional request, piggybacking, re-transmission and accept in 10 seconds [60].

Complexity is also one of the major concerns in steganography. Because of the increased complexity, concealing time, retrieval time, key management, cost, etc. need to be adjusted. SCONeP (Steganography and Cryptography over Network Protocols) is the process of hiding secret data inside network protocols. It utilises the protocols ICMP (Internet Control Message Protocol) and UDP for its work. The proposed research work provides additional security through the encryption process. Before embedding the secret data, it was encrypted using Huffman coding. Then secret data was hidden inside either ICMP or UDP. After hiding secret data, compression was done, which resulted in improved embedding capacity. At last, an active warden was used to avoid the attacks [61]. The proposed work of the SCONeP model is shown in Figure 14.

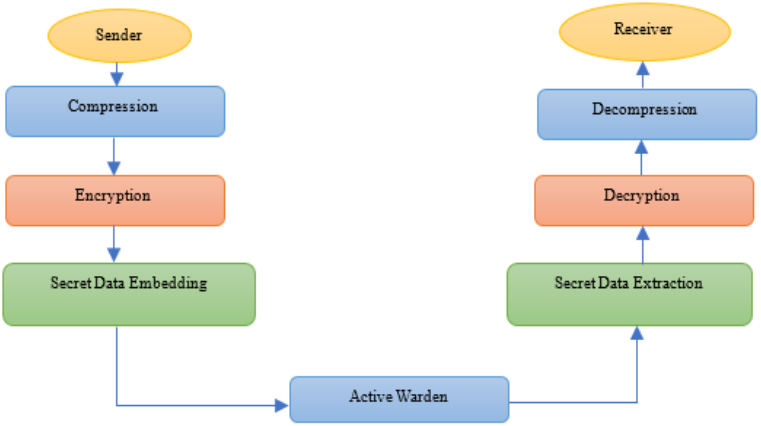


Fig. 14. SCONeP Working Model [61]

Compression was done using the Huffman coding algorithm. This algorithm converts the given file into binary form. A list of binaries was created and then transmitted for the next process. The next process was the compression module first; two bytes of the file contain information about whether compression is needed or not. If the value carried out by the first byte was the negative value that means no compression was done. The value between 1 to 7 represents the number of bits changed in the original file. Now in the second module encryption took place using both the private and the shared keys. Private key encryption was done using RSA and shared key encryption was done using triple-DES (Data Encryption Standard) or Vigenère algorithm. For both, the algorithm OpenSSL library was used. A random value generated at run time was used to decide which one shared key algorithm is needed to apply. If the random value was found to be odd that means the Vigenère algorithm will be required. Even the value generated means the RSA algorithm was used. To make the encryption module more general 24 bits' keys were used.

SCONeP was used to embed the secret data into the header of any of the protocols TCP, IP, UDP, and ICMP. In TCP, ISH (Initial Sequence Header) was used to hide the secret data. In ISH 32 bits of secret data were embedded. On the receiver side, the same processes take place in the reverse direction. The receiver first extracts the secret data from the protocol. The extracted secret data was then decrypted using the Huffman coding algorithm. At last decompression of secret data was done to get the complete secret data. Warden was used to checking the delectability of the proposed work. Both active and passive wardens were used to test the delectability. SCONeP was able to hide a maximum of 6 bytes of secret data [62].

MKIPS (Master Key Identifier-based Protocol Steganography), was proposed by authors in this research work. Initially, VoIP was developed to transfer audio over the web but these days its applications are increasing. It is used in traffic management, security, online gaming, video conferencing, and many more. SRTP (Secure Real-time Transfer Protocol) could also be used for providing all the mentioned applications along with confidentiality, replay protection of messages, and authentication. SRTP working was based on the random keys generated by MKI (Master Key Identifier). With the help of MKI, it did encryption and decryption of secret data and revived key values after a time interval. It worked efficiently when used in video conferencing with multiple users. It decreased the chance of detection of secret data because of refreshing the master key periodically. A refreshment table of the MKI was provided to the list of users. MKI was added to every packet before its transmission. At the destination, the receiver has chosen

the key from the MKI for the decryption of secret data. Depending upon the value of the master key size of secret data varies.

In the proposed work SRTP packets were used to hide the secret data. Secret data was concealed in the MKI field of the SRTP protocol. SRTP maintained the replay protection, confidentiality, and authorization of secret data. The receiver needs to first select the correct key from the set of keys and then retrieve the secret data. After retrieval of secret data, it was decrypted. The research work was implemented in Python using a Wireshark analyzer. The flow chart in Figures 15 and 16 represent the embedding and extraction of secret data. In the work maximum of 128 bytes were provided for the MKI and 80 bits were provided for the authentication purpose.

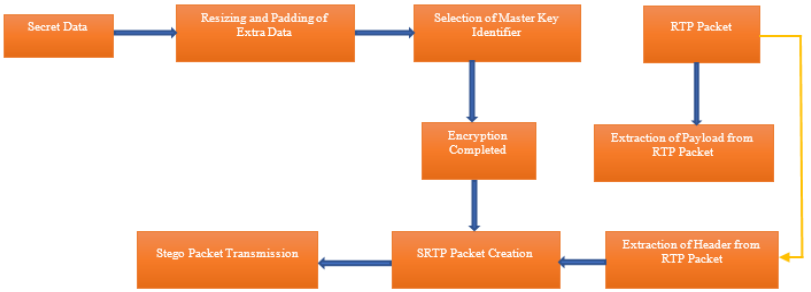


Fig. 15. Embedding of Secret Data using MKI [63]

Fig. 16. Extraction of Secret Data using MKI [63]

Experimental results were compared with the existing work as well. The research work has a high embedding capacity with almost no disturbance in the cover protocol. The data communication speed of the work is dependent upon the chosen MKI field. The size of the MKI field varies from 1 byte to 128 bytes but it was fixed for a specific session. An embedding capacity of 128 bytes was provided by the proposed work along with authentication, confidentiality, and replay protection. It provided a double level of security because of the combination of encryption and steganography techniques [63].

In today's world communication of digital information through email, the system is most common. So steganography in email does not result in the detection of secret data. SMTP and POP work on the application layer of the OSI model. Both protocols are used by email systems to send and transmit the data. Initially, SMTP was handling only the text files but now it handles MIME (Multipurpose Internet Mail Extension) files as well. Secret data transmission can be done through an email system. In the proposed work secret data was hidden in the body of the email. As email has some hidden field where secret data could be embedded. Part of email like headers and some other fields are not visible to the user as well to the intermediate agents. So, these fields were neither used by the agents nor updated by anyone. These fields just look like the ASCII strings and their usages were also restricted to end-users. These fields could be used to hide the secret data following certain rules for the integrity, confidentiality, and authentication of secret data. It does not matter where the sender and receiver are sitting and sending mail messages to each other. For retrieval of secret data embedded receiver must have prior information.

SMTP has two parts body and the header. The body may have normal text or a MIME file as the attachment. The complete mailing system is divided into four parts. Both sender and receiver were required to run MAU (Mail User Agent) on their machine. The sender prepared the message body and then established a connection with MAU. MAU checked the header part of the mail for finding the recipient's mailing address. MAU then requested DNS for resolving the IP of the destination. The receiver side MAU then sends mail to the particular user. With the help of the POP protocol receiver later on, after login can download the mail. Secret data could also be sent through spam mail. MAU directly sends them through their anti-spam scanners. Spam was considered unwanted stuff and it was stored in the spam folder directly by the MAU.

Figure 17 represents the complete flow of the process of embedding and retrieval of secret data. Secret data was compressed using Deflate compression algorithm. The compressed data was divided into parts and converted to binary form. Using the PBKDF2 encryption algorithm two keys were generated. The hash function was selected using the MD5 hashing algorithm. After applying hashing and encryption on the secret data, segregated secret data were combined back to get the complete message. HMAC was used to provide integrity, authentication, and confidentiality to the secret data. Timestamp was also used to verify the time of each operation performed and to avoid the attacks. Secret data was embedded in the header of the email. The index field contains the sequence

number of the segregated secret data and it was required during the process of obtaining the complete secret data through concatenation. At the time of retrieval of secret data reverse process of encryption takes place.

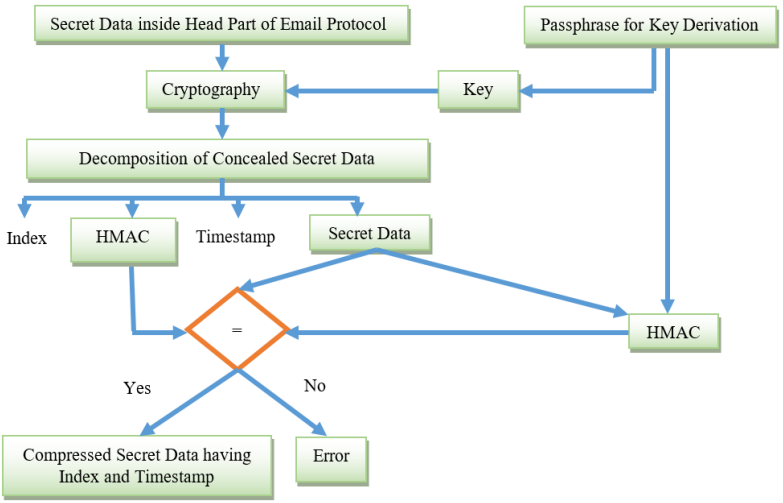


Fig. 17. Retrieval of Secret Data from Email Header [64]

HMAC, timestamp, and secret data retrieved were compared for finding whether any error was present or not. Bandwidth, embedding capacity, and detection of secret data all are directly related to each other. Bandwidth can be defined as the number of bits of secret data embedded per unit of time. So, on increasing bandwidth embedding capacity automatically increases. The improved embedding capacity increases the chances of detection of secret data. For the proposed research work embedding capacity was calculated as 50 bytes per second [64].

In almost all the steganography techniques author compromise with the concealing capacity because on increasing concealing capacity chances of detection of secret data increase. SSH (Secure Shell) is the protocol for providing secure remote login. It has built-in encryption techniques for security purposes. It works on the client-server architecture. SSH client sends the request to its server. They establish a connection and then communicate through that connection. SSH uses public-key cryptography and hashing for the security of data transmission. It provides the following functionality to the users [65]:

– It first establishes the connection and then transmits data through that connection.

– It can provide remote login using some set of commands.

– It is the authentication protocol. With the help of a password or some other option, it provides an authentication mechanism.

The packet size field is 32-bits long and represents the size of the packet. Padding size is the length of the packet to represent the padding in the packet. The payload is the real information inside the packet. Random padding is the additional data required to provide security. MAC provides the required authentication code for security. As shown in the figure first four fields are already encrypted. Packet payload and random padding fields are already encrypted.

In the research work, secret data was hidden in the traffic generated by the network. For traffic analysis, PT (Packet Transmogrifies) was used which was written in C language. It has been calculated that SSH in a session has 48 to 80 bytes to hide the secret data. PT selected a random packet for hiding secret data and at the receiver side, it was retrieved. PT used many protocols precise packet converters as the connector modules for selecting specific packets to hide secret data. 12 octets of secret data were hidden in the payload field of the packet. Before hiding secret data, it was divided into smaller chunks and converted into binary form. The CRC (Cyclic Redundancy Checksum) was used to check the integrity of secret data. The bandwidth for the proposed research work was found to be good as compared to other existing work [65].

A trade-off exists between bandwidth, security, and robustness in network steganography. VoIP is the most commonly used network steganography technique these days. VoIP uses the LSB (Least Significant Bit) technique to hide secret data. Embedding capacity can be improved by hiding secret data in voice packets during transmission. Random numbers in the selection of LSB bits improve the security of the research work. Embedding capacity varies from sample to sample of voice packet [66, 67]. Analysis of a few VoIP steganography techniques is shown as follows:

– Another way to hide secret data in the voice packet was using G.711 codec. The process includes compression of secret data and then it results in less embedding time. By doing so embedding capacity that is bandwidth can also be improved. By selecting 4-bits modification in the carrier can be reduced [68, 69, 70].

– In the proposed work Partial Similarity Value (PSV) between LSB of G.729a speech and secret data. This proposed combination resulted in high security and robustness. Concealing capacity was calculated by the number of similar bits and threshold. Embedding capacity was calculated at 1444 bits in 126 frames [71].

– A covert transmission scheme on G.711 stream over VoIP was proposed by the authors. It used sharp blocks to hide secret data for avoiding exposure. It carried an embedding capacity of 7.34 Kbps. It also avoided attacks from exposure to secret data [72].

The author proposed a real-time system for hidden transmission in VoIP using the LSB technique. First encryption of secret data was done and then embedding of encrypted secret data was done. The research work embedded 0.8 Kbps [73].

Figure 18 shows the summary of the work done at the application layer of the OSI model. Many papers have been published using the application layer protocols. Evaluation of the work published was done based on various parameters like bandwidth, concealing capacity, entropy, etc. Entropy is the measure of randomness in the carrier and the stego file. The higher is the randomness high are the chances of detection of secret data.

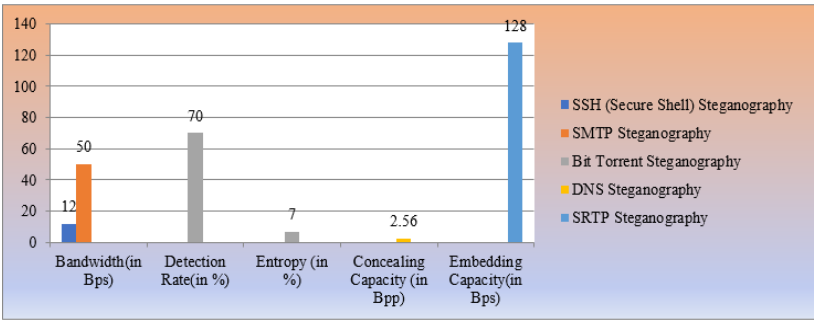


Fig. 18. Summary of Application Layer Steganography Techniques

3. Analysis of Research Trend in Network Steganography. Analysis of research trends is done on network steganography technique based on many parameters. The parameters include layer-wise analysis of the paper reviewed, year-wise analysis of the paper reviewed, bandwidth measure of the paper reviewed based on the layer of the OSI model, analysis based on steganalysis technique, the tool used to implement the research work, and, the combination of steganography with cryptography, etc. Analysis trend is explained in detail based on the mentioned parameters shown as follows:

3.1.1. Layer-Wise Analysis of Paper Reviewed. In the research work as shown in Figure 19, 73 papers related to network steganography techniques have been studied. Mainly three (Network, Transport, Application) layers of the OSI model are used by researchers to hide the secret data.

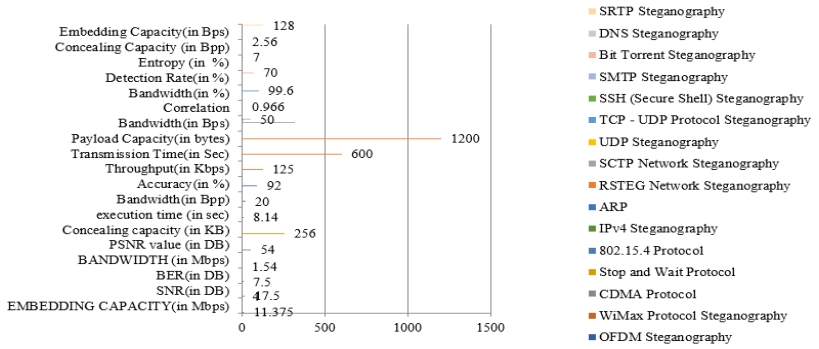


Fig. 19. Layer-wise summary of Steganography Techniques

These three layers are commonly used by steganography techniques to hide data but steganography can also be applied to other layers depending on the specific requirements and limitations of the application or system. The choice of layers depends on factors such as ease of implementation, the likelihood of detection, and the desired level of security or covert communication. The amount of secret data embedded depends on the type of protocol and the field used to hide it. Figure 20 is presenting the summary of all Layers based on the Steganography Techniques.

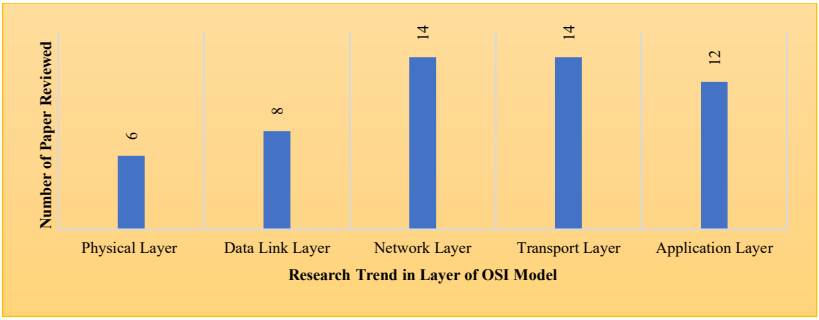


Fig. 20. Layer-Wise Count of Paper Published

TCP, UDP from the transport layer, and IP from the network layer are the mainly used protocols to hide secret data. Mainly during the retransmission of particular frames secret data is hidden in TCP protocol. Padding and option fields are mainly used by researchers to hide the secret data in IP and UDP protocols. It has been observed that physical and data link layer protocols are less used to hide the secret data.

3.1.2. Year-Wise Paper Reviewed. To prepare this research article, a total of 73 papers are reviewed. Network steganography has been investigated in 2003. Figure 21 shows the year-wise analysis of some of the papers from network steganography. These days' researchers are moving from digital steganography to modern steganography techniques. Modern steganography uses protocols of the OSI model to hide secret data.

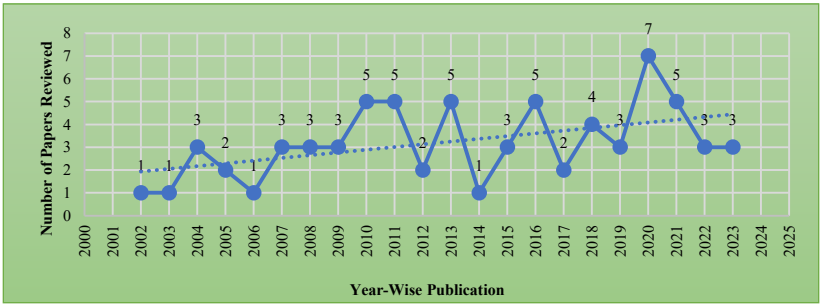


Fig. 21. Total Paper Reviewed

Papers are selected using network or protocol steganography keywords from several academic databases. As per a proposed paper lot of papers are published in the year 2020 and 2023. It has been observed that still; some issues exist with the network steganography techniques. Bandwidth and visual quality of the stego file are the issues of concern in the network steganography. On increasing the bandwidth of a particular technique visual quality of the stego file got compromised.

3.1.3. Layer-wise Bandwidth Measure of Reviewed Network Steganography Techniques. The performance of the network steganography techniques was measured by the authors in terms of bandwidth. In some papers, the correlation coefficient was also calculated to evaluate the research work. In this section, layer-wise evaluation of the research work is done based on the bandwidth. In some papers, steganography and cryptography techniques were combined to get better security.

Figure 22 showed the bandwidth achieved at the physical layer of the OSI model. Bandwidth is measured in the number of megabits per second for the physical layer steganography techniques. The value of bandwidth varies from protocol to protocol on the same layer. The maximum bandwidth is achieved by the OFDM technique and lowest by the ZigBee protocol steganography technique.

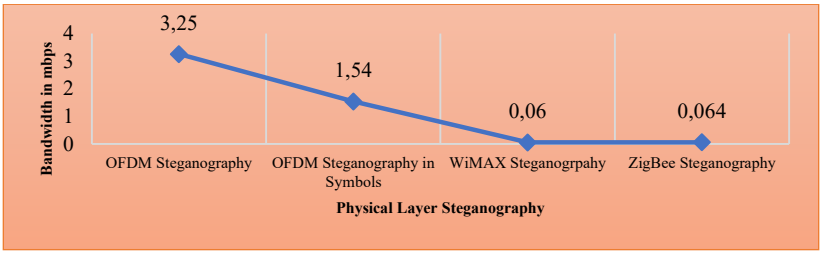


Fig. 22. Performance Measure at Physical Layer

Again, the performance of the data link layer protocols is calculated in terms of bandwidth as shown in Figure 23. This layer is responsible for flow control, access control, and error control. It has many protocols to provide the above-mentioned responsibilities. Bandwidth is measured in kilobits per second for the data link layer. Stop and wait protocol has a maximum bandwidth of 255 Kbps and CDMA has a minimum bandwidth of 77.8 Kbps.

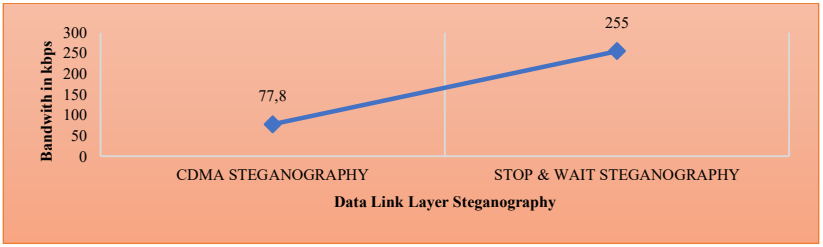


Fig. 23. Performance Measure at Data Link Layer

It mainly has IPv4, ARP, RARP, and IPv6 protocols. This layer works on the concept of IP address. Among the reviewed papers ARPNet has the highest bandwidth. As shown in Figure 24 bandwidth is measured in bits per second for the network layer. Bandwidth varies from protocol to protocol and the field was chosen to hide the secret data as well.

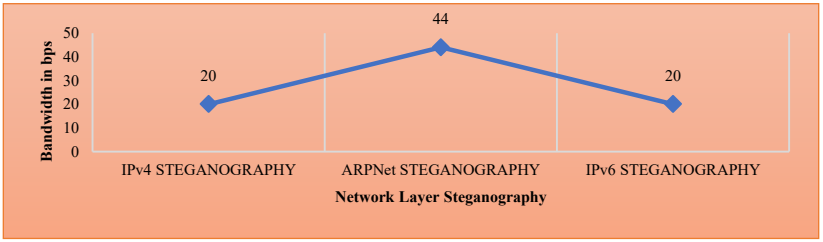


Fig. 24. Performance Measure at Network Layer

This layer provides reliable service as well as non-reliable service. Bandwidth is measured in kilobits per second for the transport layer. Maximum bandwidth is achieved by the combination of TCP and UDP protocols. Depending upon the application, the protocol is used to transfer data from source to destination. Figure 25 shows the bandwidth of the protocols used at the transport layer.

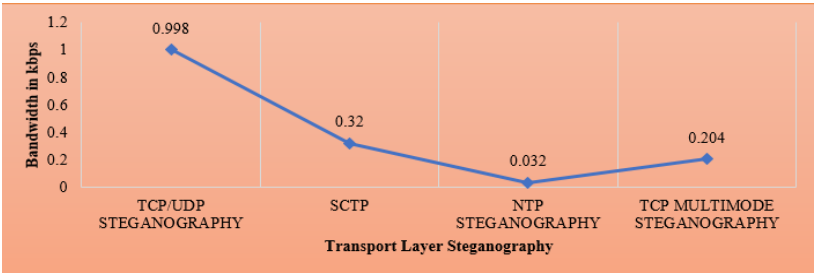


Fig. 25. Performance Measure at Transport Layer

Analysis of application-layer steganography techniques is shown with the help of Figure 26. The performance of these techniques is measured in terms of bandwidth. Bandwidth is the amount of secret data embedded per unit of time. The bandwidth of the technique depends on the size of the field of the protocol in which the secret was embedded.

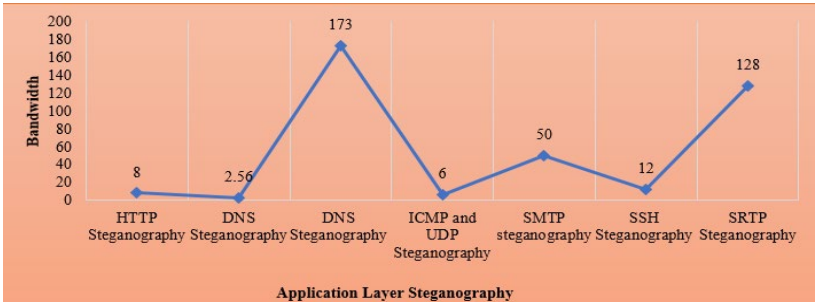


Fig. 26 Performance Measure at Application Layer

3.1.4. Analysis based on Steganalysis Technique. As we thoroughly reviewed different network steganography techniques. Some steganalysis techniques also exist to detect the hidden secret data. In some of the papers along with steganography, steganalysis techniques were also covered by the authors. In Table 1, 7 steganalysis techniques are analysed.

Table 1. Analysis of Steganalysis Techniques

Paper Title	Year	Method	Applied to
A Lightweight Adaptable DNS Channel for Covert Data Transmission [58]	2020	Opnsense 17.1 Firewall and Suricata 3.2.1 IDS	Open Sense and Suricata were run on the client-server machine. The firewall was installed on the same machine. When stego file was transferred, the firewall was not able to detect the hidden message.
A Multimode Network Steganography for Covert Wireless Communication Based on BitTorrent [53]	2020	Entropy Test	The regularity of data traffic is measured. The irregularity of traffic represents a high chance of detection of secret data.
An Approach of Covert Communication Based on the Adaptive Steganography Scheme on Voice over IP [72]	2011	RS Steganalysis	RS steganalysis is used to detect the hidden secret data. It is not able to detect the hidden data specifically in audio files.
Multilayer Detection of Network Steganography [2]	2020	Multilayer detection of RSTEG	Each layer used a different approach to detect the hidden secret data. It has been concluded that on the upper layers' detection is easy compared to the lower layers. For steganalysis, machine learning algorithms are applied.
Network Steganography and Steganalysis [74]	2013	GMM Model	Gaussian Mixture and Mel Frequency Cepstral Coefficients Model was used to detect the hidden secret data. The average detection possibility was found to be approximately equal to 89% in different formats of audio. Statistical properties were used to detect secret information.
Covert channel detection: A survey-based analysis [75]	2012	Irregularity in Time Intervals	In this paper, storage-based and timing-based covert channels were analysed to detect the secret message. It is very difficult or almost impossible to detect the hidden message. The irregularities in time intervals were used to detect the data.
Steganography and steganalysis in voice over ip: A review [76].	2021	VoIP Steganalysis	Steganalysis was done based on codebook destruction. Correlation between the pulse position of audio was calculated to detect secret messages. CNN and RNN models were also used to detect the hidden data but the presence of secret data was not detected.

For analysis paper title, year of publication, the method used, and work is included. For analysis statistical properties, traffic irregularities,

correlation, and many other parameters were used by the authors. It has been concluded from the analysis that it is not possible to detect the secret data.

3.1.5. Analysis based on Implementation Tool. Figure 27 shows the analysis of the tool used for the implementation of the reviewed techniques. Work is implemented using MATLAB, Python, and a network simulator as well. In most of the papers, the UNIX environment is used for implementation. Different simulators are used for the implementation of the work. Simulators have a component library and these are object-oriented. Simulators are wireless and discrete. By predicting the behaviour of a particular network on which the researcher is working secret data is concealed in protocols. Simulators are fast in calculating results. But simulators are difficult to build and also costly.

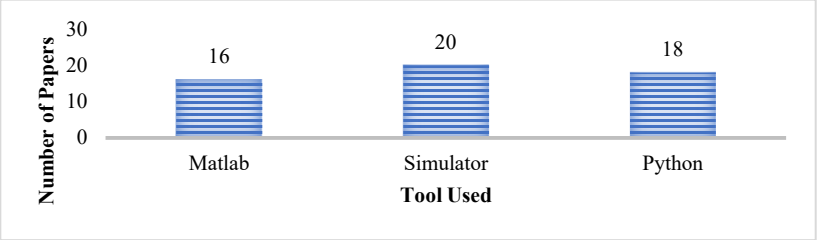


Fig. 27. Tool-wise Analysis

Python has very strong libraries as compared to MATLAB libraries [77]. Python can run on any type of platform. It has a good interface to all the databases. It is user-friendly and easy to maintain. MATLAB also has many built-in functions for plotting, visualization, numerical computation, and application development. MATLAB functions are written in C, C++, and Java. One major difference between mentioned two tools is that MATLAB treats every input as an array but Python takes input as objects [78, 79].

3.1.6. Analysis based on Combination of Cryptography and Steganography. A lot of work has already been done in the field of cryptography as well as steganography for security separately. Figure 28 shows how much work is done separately on steganography and how much on the combination of both steganography as well cryptography for the proposed paper based on the papers reviewed. Out of 73 papers reviewed for the proposed work, 43 are based on only steganography techniques and 21 are based on the combination of both techniques.

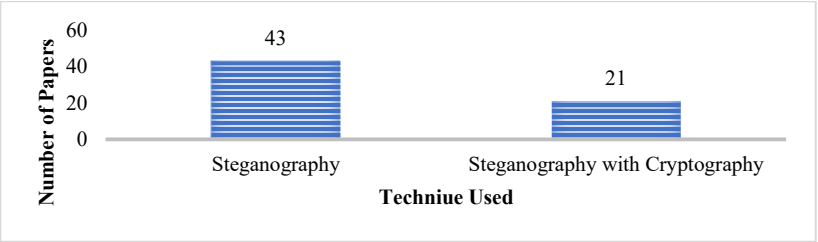


Fig. 28. Analysis based on Technique used

RSA, MD5, Digital Signature, DES, AES, HMAC, Blowfish, etc. are the most widely used cryptography techniques along with steganography [80, 81]. By combining these two techniques security is improved to some extent but complexity in terms of time and cost also increased [82]. So, to overcome the increased time and cost further research is required and that can be suggested as future research work.

4. Observations and Findings. A study of the last 21 years of network steganography techniques has been done in research work. A lot of pros and cons are associated with these techniques. These observations and findings are listed and will help researchers in future research. A few of the observations and finding are given as follows:

– **Overview of Network Steganography Techniques:** The paper would likely provide an introduction and overview of different network steganography techniques used to hide information within network communications.

– **Analysis of Steganography Methods:** The study examined different steganography methods employed in network environments, such as covert channels, protocol-based steganography, or payload-based techniques.

– **Evaluation of Security and Detection:** The researchers examined the security aspects of network steganography techniques, including the vulnerability of different methods to detection and countermeasures.

– **Challenges and Limitations:** The challenges or limitations associated with network steganography, including the potential for increased network traffic, limited payload capacity, or the risk of detection are highlighted in this paper.

– **Bandwidth and Detection of Secret Data:** Bandwidth and detection of secret data played an important role in all layers of the OSI model. Bandwidth is observed to be very low in the case of network steganography. Improvement in the bandwidth of a particular technique results in increased chances of detection of secret data.

– **Hybrid Technique:** To balance bandwidth and secret data detection, a hybrid of cryptography and steganography has also been implemented by the researchers. A hybrid of these two techniques improved the security, but the bandwidth was not improved.

5. Conclusion. In conclusion, various aspects of network steganography have been explored and examined its importance in securing data during communication. The paper has presented an in-depth analysis of existing network steganography techniques of the last 21 years. Exploration and examination of network steganography techniques have been done based on many parameters. The parameters include year-wise analysis of the reviewed paper, layer-wise analysis of the reviewed paper, bandwidth measure of the reviewed paper based on the layer of the OSI model, analysis based on steganalysis technique, analysis of the tool used to implement the research work, and the combination of steganography with cryptography. By examining and summarizing these techniques, researchers and practitioners can gain valuable insights into the current trends and advancements in the area of network steganography. This review serves as a foundation for future work, encouraging further research and development in network steganography algorithms and methodologies.

References

1. Mortazavian P., Jahangiri M., Fatemizadeh E. A Low-Degradation Steganography Model for Data Hiding in Medical Images. Proceedings of the Fourth Lasted International Conference Visualization, Imaging and Image Processing. 2004. pp. 914–920.
2. Smolarczyk M., Szczypiorski K., Pawluk J. Multilayer detection of network steganography. Electronics. 2020. vol. 9. no. 12. pp. 1–14. DOI: 10.3390/electronics9122128.
3. Szczypiorski K. HICCUPS: Hidden communication system for corrupted networks. Internation Multi-Conference Advance Computing System. 2003. pp. 31–40.
4. Sekhar A., Kumar G.M., M A.R. A Novel Approach for Hiding Data in Videos Using Network Steganography Methods. Procedia Computer Science. 2015. vol. 7. no. 4. pp. 49–61. DOI: 10.5121/ijwmn.2015.7404.
5. Almohammedi A.A., Shepelev V. Saturation Throughput Analysis of Steganography in the IEEE 802.11p Protocol in the Presence of Non-Ideal Transmission Channel. IEEE Access. 2021. vol. 9. pp. 14459–14469. DOI: 10.1109/ACCESS.2021.3052464.
6. Seo J.O., Manoharan S., Mahanti A. A Discussion and Review of Network Steganography. IEEE 14th International Confernce Pervasive Intelligent Computer. 2016. pp. 384–391. DOI: 10.1109/DASC-PICom-DataCom-CyberSciTec.2016.80.
7. Ouda A.H., El-Sakka M.R. A step towards practical steganography systems. Lecture Notes Computer Science. LNCS. 2005. vol. 3656. pp. 1158–1166. DOI: 10.1007/11559573_140.
8. Tanwar R., Pilania U., Zamani M., Manaf A.A. An Analysis of 3D Steganography Techniques. Electronics. 2021. vol. 10. no. 19. p. 2357. DOI: 10.3390/electronics10192357.

9. Nair A.S., Kumar A., Sur A., Nandi S.иLength based network steganography using UDP protocol. IEEE 3rd International Conference Communication Software Networks, ICCSN 2011. 2011. pp. 726–730. DOI: 10.1109/ICCSN.2011.6014994.
10. Zander S., Armitage G., Branch P. A survey of covert channels and countermeasures in computer network protocols. IEEE Communications Surveys and Tutorials 2007. vol. 9. no. 3. pp. 44–57.
11. Huang Z., Sun X., Luo J., Wang J. Security Against Hardware Trojan Attacks Through a Novel Chaos FSM and Delay Chains Array PUF Based Design Obfuscation Scheme. Lecture Notes Computer Science. 2015. vol. 9483. pp. 14–24. DOI: 10.1007/978-3-319-27051-7.
12. Bedi P., Dua A. Network Steganography using the Overflow Field of Timestamp Option in an IPv4 Packet. Procedia Computer Science. 2020. vol. 171. pp. 1810–1818. DOI: 10.1016/j.procs.2020.04.194.
13. Pilania U., Tanwar R., Gupta P. Stable High Capacity Video Steganography in Wavelet Domain. Turkish Journal of Computer and Mathematics Education Research Article. 2021. vol. 12. no. 7. pp. 2142–2158.
14. Pilania U. A Proposed Optimized Steganography Technique using ROI, IWT and SVD. International Journal of Information Systems and Management Science. 2018. pp. 313–318.
15. Zielińska E., Mazurczyk W., Szczypiorski K. Trends in steganography. Communication ACM. 2014. vol. 57. no. 3. pp. 86–95. DOI: 10.1145/2566590.2566610.
16. Zielińska E., Mazurczyk W., Szczypiorski K. Developement Trends in steganography. Communication ACM. 2014. vol. 57. no. 3. pp. 86–95. DOI: 10.1145/2566590.2566610.
17. Amirtharajan R., Rayappan J.B.B. Steganography-time to time: A review. Journal Information Technology. 2013. vol. 5. no. 2. pp. 53–66. DOI: 10.3923/rjit.2013.53.66.
18. Theodore G., Maxwell T., Sandford I.I. Hiding data in the OSI network model. Lecture Notes Computer Science. 1996. vol. 1174. pp. 24–38. DOI: 10.1007/3-540-61996-8_29.
19. Frikha L., Trabelsi Z. A new Covert channel in WIFI networks. Proceeding 2008 3rd International Conference on Risks and Security of Internet and Systems. 2008. pp. 255–260. DOI: 10.1109/CRISIS.2008.4757487.
20. Martins D., Guyennet H. Attacks with Steganography in PHY and MAC Layers of 802.15.4 Protocol. Fifth International Conference on Systems and Networks Communications. 2010. DOI: 10.1109/ICSNC.2010.11.
21. Shah D.C., Rindhe B.U., Narayankhedkar S.K. Effects of cyclic prefix on OFDM system. Proceeding of International Conference and Workshop on Emerging Trends in Technology (ICWET). 2010. pp. 420–424. DOI: 10.1145/1741906.1741996.
22. Grabski S., Szczypiorski K. Steganography in OFDM symbols of fast IEEE 802.11n networks. IEEE Security and Privacy Workshops. 2013. pp. 158–164. DOI: 10.1109/SPW.2013.20.
23. Szczypiorski K., Mazurczyk W. Steganography in IEEE 802.11 OFDM symbols. Security and Communication Networks. 2016. vol. 9. no. 2. pp. 118–129. DOI: 10.1002/sec.306.
24. Khan M.N., Ghauri S. The WiMAX 802.16e Physical Layer Model. IET Conference on Wireless, Mobile and Multimedia Networks. 2008. pp. 117–120. DOI: 10.1049/cp:20080159.
25. Grabska I., Szczypiorski K. Steganography in WiMAX networks. 5th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). 2013. pp. 20–27. DOI: 10.1109/ICUMT.2013.6798399.

26. Hussain I., Negi M.C., Pandey N. Security in ZigBee Using Steganography for IoT Communications. System Performance and Management Analytics. 2019. pp. 217–227.
27. Jankowski B., Mazurczyk W., Szczypiorski K. Information hiding using improper frame padding. Proceedings of 14th Internationl Telecommunication Network Strategy Planning Symposium (Networks). 2010. DOI: 10.1109/NETWKS.2010.5624901.
28. Banoci V., Bugar G., Levicky D. Steganography systems by using CDMA techniques. Proceedings of 19th International Conference Radioelektronika. 2009. pp. 183–186. DOI: 10.1109/RADIOELEK.2009.5158731.
29. Khalife J., Kassas Z.M. Navigation with Cellular CDMA Signals-Part II: Performance Analysis and Experimental Results. IEEE Transaction Signal Processing. 2018. vol. 66. no. 8. pp. 2204–2218. DOI: 10.1109/TSP.2018.2799166.
30. Hasan O., Tahar S. Performance analysis and functional verification of the stop-and-wait protocol in HOL. Journal Automation Reason. 2009. vol. 42. no. 1. pp. 1–33. DOI: 10.1007/s10817-008-9105-6.
31. Shukla V., Chaturvedi A., Srivastava N. A Secure Stop and Wait Communication Protocol for Disturbed Networks. Wireless Communication. 2020. vol. 110. no. 2. pp. 861–872. DOI: 10.1007/s11277-019-06760-w.
32. Kim B., Lee B., Cho J. ASRQ: Automatic segment repeat request for IEEE 802.15.4-based WBAN. IEEE Sensor Journal. 2017. vol. 17. no. 9. pp. 2925–2935. DOI: 10.1109/JSEN.2017.2676163.
33. Martins D., Guyennet H. Steganography in MAC Layers of 802.15.4 Protocol for Securing Wireless Sensor Networks. International Conference on Multimedia Information Networking and Security. 2010. pp. 824–828. DOI: 10.1109/MINES.2010.175.
34. Xue P.F., Hu J.S., Liu H.L., Hu R.G. A new network steganographic method based on the transverse multi-protocol collaboration. Journal Information Hiding Multimedia Signal Processing. 2017. vol. 8. no. 2. pp. 445–459.
35. Maya A. Steganology and information hiding: Stegop2py: embedding data in TCP and IP headers. Centria University of Applied Science. 2021. 59 p.
36. Maulana B., Rahim R. Go-Back-N Arq Approach for Identification and Repairing Frame in Transmission Data. International Journal Resource Science Engineering. 2016. vol. 2. no. 6. pp. 208–212.
37. Bedi P., Dua A. ARPNetSteg: Network steganography using address resolution protocol. International Journal Electronic Telecommunication. 2020. vol. 66. no. 4. pp. 671–677. DOI: 10.24425-ijet.2020.134026/769.
38. Schmidbauer T., Wendzel S., Mileva A., Mazurczyk W. Introducing Dead Drops to Network Steganography using ARP-Caches and SNMP-Walks. Proceedings of the 14th International Conference on Availability, Reliability and Security. 2019. pp. 1–10. DOI: 10.1145/3339252.3341488.
39. Llamas D., Miller A., Allison C. Covert channels in internet protocols: A survey. Proceedings of the 6th Annual Postgraduate Symposium about the Convergence of Telecommunications, Networking and Broadcasting, PGNET. 2005. vol. 2005.
40. Bobade S., Goudar R. Secure data communication using protocol steganography in IPv6. Proceedings of the 1st International Conference on Computing Communication Control and Automation (ICCUBEA). 2015. pp. 275–279. DOI: 10.1109/ICCUBEA.2015.59.
41. Miller P. Applying Steganography to Standard Network Traffic. Proceedings of the 4th Winona Computer Science Undergraduate Research Symposium. 2004. pp. 3–6.

42. Xue P.F., Hu J.S., Hu R.-G., Liu H.-L., Gu Y. A new DHT: Network steganography based on distributed coding. Journal of Information Hiding and Multimedia Signal Processing. 2018. vol. 9. no. 2. pp. 355–369.
43. Mazurczyk W., Smolarczyk M., Szczypiorski K. On information hiding in retransmissions. Telecommunication System. 2013. vol. 52. no. 2. pp. 1113–1121. DOI: 10.1007/s11235-011-9617-y.
44. Mazurczyk W., Smolarczyk M., Szczypiorski K. Retransmission steganography applied. Proceedings of 2nd International Conference on Multimedia Information Networking and Security. 2010. pp. 846–850. DOI: 10.1109/MINES.2010.179.
45. Siddiqui F., Zeadally S. Stream control transmission protocol (SCTP). Encyclopedia Internet Technology Application. 2007. pp. 575–582. DOI: 10.4018/978-1-59140-993-9.ch081.
46. Mazurczyk W., Szczypiorski K. Steganography of VoIP streams, Lecture Notes Computer Science. 2008. vol. 5332. LNCS, no. PART 2, pp. 1001–1018. DOI: 10.1007/978-3-540-88873-4_6.
47. Lubacz J., Mazurczyk W., Szczypiorski K. Principles and overview of network steganography. IEEE Communications Magazine. 2014. vol. 52(5). pp. 225–229.
48. Hamdaqa M., Tahvildari L. ReLACK: A reliable VoIP steganography approach. Proceedings of 5th International Conference Security Software Integration Reliability Improvement. 2011. pp. 189–197. DOI: 10.1109/SSIRI.2011.24.
49. Na S., Yoo S. Allowable Propagation Delay for VoIP Calls. International Workshop on Advanced Internet Services and Applications. 2002. pp. 47–55.
50. Bak P., Bieniasz J., Krzeminski M., Szczypiorski K. Application of perfectly undetectable network steganography method for malware hidden communication. 4th International Conference Frontier Signal Processing (ICFSP). 2018. pp. 34–38. DOI: 10.1109/ICFSP.2018.8552057.
51. Mills D.L. A brief history of NTP time: Memoirs of an Internet timekeeper. Computer Communication Reverse. 2003. vol. 33. no. 2. pp. 9–21. DOI: 10.1145/956981.956983.
52. Schmidbauer T., Wendzel S. Covert storage caches using the NTP protocol. Proceedings of the 15th International Conference on Availability, Reliability and Security. 2020. DOI: 10.1145/3407023.3409207.
53. Wang M., Gu W., Ma C. A Multimode Network Steganography for Covert Wireless Communication Based on BitTorrent. Security Communication Networks. 2020. vol. 2020. DOI: 10.1155/2020/8848315.
54. K Shah M., Virparia A.M., Sharma K. An Overview of Advanced Network Steganography. International Journal Computer Application. 2015. vol. 118. no. 21. pp. 23–26. DOI: 10.5120/20871-3364.
55. Dimitrova B., Mileva A. Steganography of Hypertext Transfer Protocol Version 2 (HTTP/2). Journal of Computer Communication. 2017. vol. 05. no. 05. pp. 98–111. DOI: 10.4236/jcc.2017.55008.
56. Collins J., Agaian S. Trends Toward Real-Time Network Data Steganography. International Journal Network Security and Its Applications. 2016. vol. 8. no. 2. pp. 01–21. DOI: 10.5121/ijnsa.2016.8201.
57. Drzymała M., Szczypiorski K., Urbański M.Ł. Network Steganography in the DNS Protocol. International Journal of Electronic and Telecommunications. 2016. vol. 62. no. 4. pp. 343–346. DOI: 10.1515/eletel-2016-0047.
58. Nazari M., Tarahomi S., Aliabady S. A Lightweight Adaptable DNS Channel for Covert Data Transmission. arXiv preprint arXiv:2003.14094. 2020.
59. Bormann C., Castellani A.P., Shelby Z. CoAP: An application protocol for billions of tiny internet nodes. IEEE Internet Computing. 2012. vol. 16. no. 2. pp. 62–67. DOI: 10.1109/MIC.2012.29.

60. Mileva A., Velinov A., Stojanov D. New Covert Channels in Internet of Things. 12th International Conference on Emerging Security Information, Systems and Technologies. 2018. pp. 30–36.
61. Patuck R., Hernandez-Castro J. Steganography using the Extensible Messaging and Presence Protocol (XMPP). arXiv:1310.0524. 2013. DOI: 10.48550/arXiv.1310.0524.
62. Ciobanu R.I., Tirsa M.O., Lupu R., Stan S., Andreica M.I. SCONeP: Steganography and Cryptography approach for UDP and ICMP. Proceedings of RoEduNet IEEE International Conference. 2011. pp. 1–6. DOI: 10.1109/RoEduNet.2011.5993700.
63. Alishavandi A.M., Fakhredanesh M. MKIPS: MKI-based protocol steganography method in SRTP. ETRI Journal. 2021. vol. 43. no. 3. pp. 561–570. DOI: 10.4218/etrij.2018-0410.
64. Castiglione A., De Santis A., Fiore U., Palmieri F. E-mail-based covert channels for asynchronous message steganography. Proceedings of 5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computer. 2011. pp. 503–508. DOI: 10.1109/IMIS.2011.133.
65. Lucena N.B., Pease J., Yadollahpour P., Chapin S.J. Syntax and Semantics-Preserving Application-Layer Protocol Steganography. Information Hiding: 6th International Workshop. 2004. pp. 164–179. DOI: 10.1007/978-3-540-30114-1_12.
66. Ali A.H., Mokhtar M.R., George L.E. Recent approaches for VoIP steganography. Indian Journal Science Technology. 2016. vol. 9. no. 38. DOI: 10.17485/ijst/2016/v9i38/101283.
67. Mazurczyk W. VoIP steganography and its detection – a survey. ACM Computer Surve s. 2013. vol. 46. no. 2. DOI: 10.1145/2543581.2543587.
68. Wang C., Wu Q. Information hiding in real-time VoIP streams. Proceedings of the 9th IEEE International Symposium Multimedia (2007). 2007. pp. 255–262. DOI: 10.1109/ISM.2007.33.
69. Xu T., Yang Z. Simple and effective speech steganography in G.723.1 low-rate codes. 2009 International Conference on Wireless Communication and Signal Processing. 2009. pp. 1–5. DOI: 10.1109/WCSP.2009.5371745.
70. Ito A., Suzuki Y. Information hiding for G.711 speech based on substitution of least significant bits and estimation of tolerable distortion. IEICE Transaction Fundamentals of Electronics, Communications and Computer Science. 2010. vol. 93. no. 7. pp. 1279–1286. DOI: 10.1587/transfun.E93.A.1279.
71. Tian H., Zhou K., Jiang H., Huang Y., Liu J., Feng D. An adaptive steganography scheme for voice over IP. Proceedings of the IEEE International Symposium on Circuits Systems. 2009. pp. 2922–2925. DOI: 10.1109/ISCAS.2009.5118414.
72. Miao R., Huang Y. An approach of covert communication based on the adaptive steganography scheme on voice over IP. IEEE International Conference on Communications (ICC). 2011. DOI: 10.1109/icc.2011.5962657.
73. Tian H., Zhou K., Huang Y., Feng D., Liu J. A covert communication model based on least significant bits steganography in voice over IP. Proceeding of the 9th International Conference for Young Computer Scientists. 2008. pp. 647–652. DOI: 10.1109/ICYCS.2008.394.
74. Janicki A., Mazurczyk W., Szczypiorski K. Steganalysis of transcoding steganography. annals of telecommunications-annales des télécommunications. 2014. vol. 69. pp. 449–460.
75. Goher S., Javed B., Saqib N. Covert channel detection: A survey-based analysis. High-Capacity Optical Networks and Emerging/Enabling Technologies. 2012. pp. 057–065.
76. Wu Z., Guo J., Zhang C., Li C. Steganography and steganalysis in voice over ip: A review. Sensors. 2021. vol. 21. no. 4.

77. Neubert T., Caballero Morcillo A.J., Vielhauer C. Improving Performance of Machine Learning based Detection of Network Steganography in Industrial Control Systems. Proceedings of the 17th International Conference on Availability, Reliability and Security. 2022. pp. 1–8.
78. Zhang X.-G., Yang G.-H., Ren X.-X. Network steganography based security framework for cyber-physical systems. Information Sciences. 2022. vol. 609. pp. 963–983.
79. Tymchenko O., Havrysh B. Steganography in TCP/IP Networks. International Conference of Artificial Intelligence, Medical Engineering, Education. 2023. pp. 47–56.
80. Chai H., Li Z., Li F., Zhang Z. An end-to-end video steganography network based on a coding unit mask. Electronics. 2022. vol. 11. no. 7. pp. 1142.
81. Olawoyin L.A., Abdul-Rahman M., Faruk N., Oloyede A., Adeniran C., Lasisi O., Sikiru I., Baba B.A. Hybridization of OFDM and Physical Layer Techniques for Information Security in Wireless System. SLU Journal of Science and Technology. 2023. vol. 6. no. 1, 2. pp. 21–29.
82. Rajesh S., Joshi A. Estimation of Transmission Bandwidth for VoIP Signals over IP Packet Transmission Network using Capacity Computing Method. IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS). 2023. pp. 01–07. DOI: 10.1109/ICICACS57338.2023.10100177.
83. Pilania U., Tanwar R., Zamani M., Manaf A.A. Framework for video steganography using integer wavelet transform and JPEG compression. Future Internet. 2022. vol. 14(9). pp. 1–16. DOI: 10.3390/fi14090254.
84. Pilania U., Kumar M., Kaur G. Region of Interest Using Viola-Jones Algorithm for Video Steganography. Applied Computational Technologies: Proceedings of ICCET 2022. 2022. pp. 405–415. DOI: 10.1007/978-981-19-2719-5_38.

Pilania Urmila — Ph.D., Associate professor, Department of computer science and technology, Manav Rachna University. Research interests: computer vision, image processing, information security. The number of publications — 25. urmilapilania@gmail.com; Aravali Hills, Faridabad, 121004, Haryana, India; office phone: +91(129)419-8000.

Kumar Manoj — Ph.D., Associate professor, Department of computer science and technology, Manav Rachna University. Research interests: computer vision, image processing, machine learning. The number of publications — 21. manojattri003@gmail.com; Aravali Hills, Faridabad, 121004, Haryana, India; office phone: +91(129)419-8000.

Rohit Tanwar — Ph.D., Associate professor, Department of computer science and technology, University of Petroleum and Energy Studies. Research interests: information security, machine learning. The number of publications — 80. rohit.tanwar.cse@gmail.com; P.O. Kandoli (Via Prem Nagar), Dehradun, 248007, Uttarakhand, India; office phone: +91(999)225-7914.

Nandal Neha — Ph.D., Associate professor of the department, Department of computer science and engineering, Geethanjali College of Engineering and Technology. Research interests: machine learning, deep learning, pattern recognition, data mining. The number of publications — 22. nehanandal012@gmail.com; Medchal, Cheeryal, 501301, Hyderabad, Telangana, India; office phone: +91(720)771-4441.

DOI 10.15622/ia.22.5.6

У. Пилания, М. Кумар, Т. Рохит, Н. Нандал

КРАТКИЙ ОБЗОР МЕТОДОВ СЕТЕВОЙ СТЕГАНОГРАФИИ

Пилания У., Кумар М., Рохит Т., Нандал Н. **Краткий обзор методов сетевой стеганографии.**

Аннотация. Цифровые мультимедийные файлы 2D и 3D обладают многочисленными преимуществами, такими как отличное качество, сжатие, редактирование, надежное копирование и т. д. С другой стороны, эти качества мультимедийных файлов являются причиной опасений, в том числе боязни получить доступ к данным во время общения. Стеганография играет важную роль в обеспечении безопасности передаваемых данных. Изменение типа файла покрытия с цифровых мультимедийных файлов на протоколы повышает безопасность системы связи. Протоколы являются неотъемлемой частью системы связи, и эти протоколы также могут использоваться для сокрытия секретных данных, что снижает вероятность их обнаружения. Этот документ призван помочь улучшить существующие методы сетевой стеганографии за счет увеличения пропускной способности и снижения скорости обнаружения путем анализа предыдущей связанной работы. Были изучены, проанализированы и обобщены последние статьи о методах сетевой стеганографии за последний 21 год. Этот обзор может помочь исследователям понять существующие тенденции в методах сетевой стеганографии, чтобы продолжить работу в этой области для улучшения алгоритмов. Статья разделена по уровням модели OSI.

Ключевые слова: сетевая стеганография, модель взаимосвязи открытых систем, протокол, пропускная способность, возможности внедрения, физический уровень, канальный уровень, сетевой уровень, уровень передачи, прикладной уровень.

Литература

1. Mortazavian P., Jahangiri M., Fatemizadeh E. A Low-Degradation Steganography Model for Data Hiding in Medical Images. Proceedings of the Fourth Lasted International Conference Visualization, Imaging and Image Processing. 2004. pp. 914–920.
2. Smolarczyk M., Szczypiorski K., Pawluk J. Multilayer detection of network steganography. Electronics. 2020. vol. 9. no. 12. pp. 1–14. DOI: 10.3390/electronics9122128.
3. Szczypiorski K. HICCUPS: Hidden communication system for corrupted networks. Internation Multi-Conference Advance Computing System. 2003. pp. 31–40.
4. Sekhar A., Kumar G.M., M A.R. A Novel Approach for Hiding Data in Videos Using Network Steganography Methods. Procedia Computer Science. 2015. vol. 7. no. 4. pp. 49–61. DOI: 10.5121/ijwmn.2015.7404.
5. Almohammedi A.A., Shepelev V. Saturation Throughput Analysis of Steganography in the IEEE 802.11p Protocol in the Presence of Non-Ideal Transmission Channel. IEEE Access. 2021. vol. 9. pp. 14459–14469. DOI: 10.1109/ACCESS.2021.3052464.
6. Seo J.O., Manoharan S., Mahanti A. A Discussion and Review of Network Steganography. IEEE 14th International Confernce Pervasive Intelligent Computer. 2016. pp. 384–391. DOI: 10.1109/DASC-PICom-DataCom-CyberSciTec.2016.80.
7. Ouda A.H., El-Sakka M.R. A step towards practical steganography systems. Lecture Notes Computer Science. LNCS. 2005. vol. 3656. pp. 1158–1166. DOI: 10.1007/11559573_140.

8. Tanwar R., Pilania U., Zamani M., Manaf A.A. An Analysis of 3D Steganography Techniques. Electronics. 2021. vol. 10. no. 19. p. 2357. DOI: 10.3390/electronics10192357.
9. Nair A.S., Kumar A., Sur A., Nandi S.иLength based network steganography using UDP protocol. IEEE 3rd International Conference Communication Software Networks, ICCSN 2011. 2011. pp. 726–730. DOI: 10.1109/ICCSN.2011.6014994.
10. Zander S., Armitage G., Branch P. A survey of covert channels and countermeasures in computer network protocols. IEEE Communications Surveys and Tutorials 2007. vol. 9. no. 3. pp. 44–57.
11. Huang Z., Sun X., Luo J., Wang J. Security Against Hardware Trojan Attacks Through a Novel Chaos FSM and Delay Chains Array PUF Based Design Obfuscation Scheme. Lecture Notes Computer Science. 2015. vol. 9483. pp. 14–24. DOI: 10.1007/978-3-319-27051-7.
12. Bedi P., Dua A. Network Steganography using the Overflow Field of Timestamp Option in an IPv4 Packet. Procedia Computer Science. 2020. vol. 171. pp. 1810–1818. DOI: 10.1016/j.procs.2020.04.194.
13. Pilania U., Tanwar R., Gupta P. Stable High Capacity Video Steganography in Wavelet Domain. Turkish Journal of Computer and Mathematics Education Research Article. 2021. vol. 12. no. 7. pp. 2142–2158.
14. Pilania U. A Proposed Optimized Steganography Technique using ROI, IWT and SVD. International Journal of Information Systems and Management Science. 2018. pp. 313–318.
15. Zielińska E., Mazurczyk W., Szczypiorski K. Trends in steganography. Communication ACM. 2014. vol. 57. no. 3. pp. 86–95. DOI: 10.1145/2566590.2566610.
16. Zielińska E., Mazurczyk W., Szczypiorski K. Developement Trends in steganography. Communication ACM. 2014. vol. 57. no. 3. pp. 86–95. DOI: 10.1145/2566590.2566610.
17. Amirtharajan R., Rayappan J.B.B. Steganography-time to time: A review. Journal Information Technology. 2013. vol. 5. no. 2. pp. 53–66. DOI: 10.3923/rjit.2013.53.66.
18. Theodore G., Maxwell T., Sandford I.I. Hiding data in the OSI network model. Lecture Notes Computer Science. 1996. vol. 1174. pp. 24–38. DOI: 10.1007/3-540-61996-8_29.
19. Frikha L., Trabelsi Z. A new Covert channel in WIFI networks. Proceeding 2008 3rd International Conference on Risks and Security of Internet and Systems. 2008. pp. 255–260. DOI: 10.1109/CRISIS.2008.4757487.
20. Martins D., Guyennet H. Attacks with Steganography in PHY and MAC Layers of 802.15.4 Protocol. Fifth International Conference on Systems and Networks Communications. 2010. DOI: 10.1109/ICSNC.2010.11.
21. Shah D.C., Rindhe B.U., Narayankhedkar S.K. Effects of cyclic prefix on OFDM system. Proceeding of International Conference and Workshop on Emerging Trends in Technology (ICWET). 2010. pp. 420–424. DOI: 10.1145/1741906.1741996.
22. Grabski S., Szczypiorski K. Steganography in OFDM symbols of fast IEEE 802.11n networks. IEEE Security and Privacy Workshops. 2013. pp. 158–164. DOI: 10.1109/SPW.2013.20.
23. Szczypiorski K., Mazurczyk W. Steganography in IEEE 802.11 OFDM symbols. Security and Communication Networks. 2016. vol. 9. no. 2. pp. 118–129. DOI: 10.1002/sec.306.
24. Khan M.N., Ghauri S. The WiMAX 802.16e Physical Layer Model. IET Conference on Wireless, Mobile and Multimedia Networks. 2008. pp. 117–120. DOI: 10.1049/cp:20080159.

25. Grabska I., Szczypiorski K. Steganography in WiMAX networks. 5th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). 2013. pp. 20–27. DOI: 10.1109/ICUMT.2013.6798399.
26. Hussain I., Negi M.C., Pandey N. Security in ZigBee Using Steganography for IoT Communications. System Performance and Management Analytics. 2019. pp. 217–227.
27. Jankowski B., Mazurczyk W., Szczypiorski K. Information hiding using improper frame padding. Proceedings of 14th Internationl Telecommunication Network Strategy Planning Symposium (Networks). 2010. DOI: 10.1109/NETWKS.2010.5624901.
28. Banoci V., Bugar G., Levicky D. Steganography systems by using CDMA techniques. Proceedings of 19th International Conference Radioelektronika. 2009. pp. 183–186. DOI: 10.1109/RADIOELEK.2009.5158731.
29. Khalife J., Kassas Z.M. Navigation with Cellular CDMA Signals-Part II: Performance Analysis and Experimental Results. IEEE Transaction Signal Processing. 2018. vol. 66. no. 8. pp. 2204–2218. DOI: 10.1109/TSP.2018.2799166.
30. Hasan O., Tahar S. Performance analysis and functional verification of the stop-and-wait protocol in HOL. Journal Automation Reason. 2009. vol. 42. no. 1. pp. 1–33. DOI: 10.1007/s10817-008-9105-6.
31. Shukla V., Chaturvedi A., Srivastava N. A Secure Stop and Wait Communication Protocol for Disturbed Networks. Wireless Communication. 2020. vol. 110. no. 2. pp. 861–872. DOI: 10.1007/s11277-019-06760-w.
32. Kim B., Lee B., Cho J. ASRQ: Automatic segment repeat request for IEEE 802.15.4-based WBAN. IEEE Sensor Journal. 2017. vol. 17. no. 9. pp. 2925–2935. DOI: 10.1109/JSEN.2017.2676163.
33. Martins D., Guyennet H. Steganography in MAC Layers of 802.15.4 Protocol for Securing Wireless Sensor Networks. International Conference on Multimedia Information Networking and Security. 2010. pp. 824–828. DOI: 10.1109/MINES.2010.175.
34. Xue P.F., Hu J.S., Liu H.L., Hu R.G. A new network steganographic method based on the transverse multi-protocol collaboration. Journal Information Hiding Multimedia Signal Processing. 2017. vol. 8. no. 2. pp. 445–459.
35. Maya A. Steganology and information hiding: Stegop2py: embedding data in TCP and IP headers. Centria University of Applied Science. 2021. 59 p.
36. Maulana B., Rahim R. Go-Back-N Arq Approach for Identification and Repairing Frame in Transmission Data. International Journal Resource Science Engineering. 2016. vol. 2. no. 6. pp. 208–212.
37. Bedi P., Dua A. ARPNetSteg: Network steganography using address resolution protocol. International Journal Electronic Telecommunication. 2020. vol. 66. no. 4. pp. 671–677. DOI: 10.24425-ijet.2020.134026/769.
38. Schmidbauer T., Wendzel S., Mileva A., Mazurczyk W. Introducing Dead Drops to Network Steganography using ARP-Caches and SNMP-Walks. Proceedings of the 14th International Conference on Availability, Reliability and Security. 2019. pp. 1–10. DOI: 10.1145/3339252.3341488.
39. Llamas D., Miller A., Allison C. Covert channels in internet protocols: A survey. Proceedings of the 6th Annual Postgraduate Symposium about the Convergence of Telecommunications, Networking and Broadcasting, PGNET. 2005. vol. 2005.
40. Bobade S., Goudar R. Secure data communication using protocol steganography in IPv6. Proceedings of the 1st International Conference on Computing Communication Control and Automation (ICCUBEA). 2015. pp. 275–279. DOI: 10.1109/ICCUBEA.2015.59.

41. Miller P. Applying Steganography to Standard Network Traffic. Proceedings of the 4th Winona Computer Science Undergraduate Research Symposium. 2004. pp. 3–6.
42. Xue P.F., Hu J.S., Hu R.-G., Liu H.-L., Gu Y. A new DHT: Network steganography based on distributed coding. Journal of Information Hiding and Multimedia Signal Processing. 2018. vol. 9. no. 2. pp. 355–369.
43. Mazurczyk W., Smolarczyk M., Szczypiorski K. On information hiding in retransmissions. Telecommunication System. 2013. vol. 52. no. 2. pp. 1113–1121. DOI: 10.1007/s11235-011-9617-y.
44. Mazurczyk W., Smolarczyk M., Szczypiorski K. Retransmission steganography applied. Proceedings of 2nd International Conference on Multimedia Information Networking and Security. 2010. pp. 846–850. DOI: 10.1109/MINES.2010.179.
45. Siddiqui F., Zeadally S. Stream control transmission protocol (SCTP). Encyclopedia Internet Technology Application. 2007. pp. 575–582. DOI: 10.4018/978-1-59140-993-9.ch081.
46. Mazurczyk W., Szczypiorski K. Steganography of VoIP streams, Lecture Notes Computer Science. 2008. vol. 5332. LNCS, no. PART 2, pp. 1001–1018. DOI: 10.1007/978-3-540-88873-4_6.
47. Lubacz J., Mazurczyk W., Szczypiorski K. Principles and overview of network steganography. IEEE Communications Magazine. 2014. vol. 52(5). pp. 225–229.
48. Hamdaqa M., Tahvildari L. ReLACK: A reliable VoIP steganography approach. Proceedings of 5th International Conference Security Software Integration Reliability Improvement. 2011. pp. 189–197. DOI: 10.1109/SSIRI.2011.24.
49. Na S., Yoo S. Allowable Propagation Delay for VoIP Calls. International Workshop on Advanced Internet Services and Applications. 2002. pp. 47–55.
50. Bak P., Bieniasz J., Krzeminski M., Szczypiorski K. Application of perfectly undetectable network steganography method for malware hidden communication. 4th International Conference Frontier Signal Processing (ICFSP). 2018. pp. 34–38. DOI: 10.1109/ICFSP.2018.8552057.
51. Mills D.L. A brief history of NTP time: Memoirs of an Internet timekeeper. Computer Communication Reverse. 2003. vol. 33. no. 2. pp. 9–21. DOI: 10.1145/956981.956983.
52. Schmidbauer T., Wendzel S. Covert storage caches using the NTP protocol. Proceedings of the 15th International Conference on Availability, Reliability and Security. 2020. DOI: 10.1145/3407023.3409207.
53. Wang M., Gu W., Ma C. A Multimode Network Steganography for Covert Wireless Communication Based on BitTorrent. Security Communication Networks. 2020. vol. 2020. DOI: 10.1155/2020/8848315.
54. K Shah M., Virparia A.M., Sharma K. An Overview of Advanced Network Steganography. International Journal Computer Application. 2015. vol. 118. no. 21. pp. 23–26. DOI: 10.5120/20871-3364.
55. Dimitrova B., Mileva A. Steganography of Hypertext Transfer Protocol Version 2 (HTTP/2). Journal of Computer Communication. 2017. vol. 05. no. 05. pp. 98–111. DOI: 10.4236/jcc.2017.55008.
56. Collins J., Agaian S. Trends Toward Real-Time Network Data Steganography. International Journal Network Security and Its Applications. 2016. vol. 8. no. 2. pp. 01–21. DOI: 10.5121/ijnsa.2016.8201.
57. Drzymała M., Szczypiorski K., Urbański M.Ł. Network Steganography in the DNS Protocol. International Journal of Electronic and Telecommunications. 2016. vol. 62. no. 4. pp. 343–346. DOI: 10.1515/eletel-2016-0047.
58. Nazari M., Tarahomi S., Aliabady S. A Lightweight Adaptable DNS Channel for Covert Data Transmission. arXiv preprint arXiv:2003.14094. 2020.

59. Bormann C., Castellani A.P., Shelby Z. CoAP: An application protocol for billions of tiny internet nodes. IEEE Internet Computing. 2012. vol. 16. no. 2. pp. 62–67. DOI: 10.1109/MIC.2012.29.
60. Mileva A., Velinov A., Stojanov D. New Covert Channels in Internet of Things. 12th International Conference on Emerging Security Information, Systems and Technologies. 2018. pp. 30–36.
61. Patuck R., Hernandez-Castro J. Steganography using the Extensible Messaging and Presence Protocol (XMPP). arXiv:1310.0524. 2013. DOI: 10.48550/arXiv.1310.0524.
62. Ciobanu R.I., Tirsa M.O., Lupu R., Stan S., Andreica M.I. SCONeP: Steganography and Cryptography approach for UDP and ICMP. Proceedings of RoEduNet IEEE International Conference. 2011. pp. 1–6. DOI: 10.1109/RoEduNet.2011.5993700.
63. Alishavandi A.M., Fakhredanesh M. MKIPS: MKI-based protocol steganography method in SRTP. ETRI Journal. 2021. vol. 43. no. 3. pp. 561–570. DOI: 10.4218/etrij.2018-0410.
64. Castiglione A., De Santis A., Fiore U., Palmieri F. E-mail-based covert channels for asynchronous message steganography. Proceedings of 5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computer. 2011. pp. 503–508. DOI: 10.1109/IMIS.2011.133.
65. Lucena N.B., Pease J., Yadollahpour P., Chapin S.J. Syntax and Semantics-Preserving Application-Layer Protocol Steganography. Information Hiding: 6th International Workshop. 2004. pp. 164–179. DOI: 10.1007/978-3-540-30114-1_12.
66. Ali A.H., Mokhtar M.R., George L.E. Recent approaches for VoIP steganography. Indian Journal Science Technology. 2016. vol. 9. no. 38. DOI: 10.17485/ijst/2016/v9i38/101283.
67. Mazurczyk W. VoIP steganography and its detection – a survey. ACM Computer Surve s. 2013. vol. 46. no. 2. DOI: 10.1145/2543581.2543587.
68. Wang C., Wu Q. Information hiding in real-time VoIP streams. Proceedings of the 9th IEEE International Symposium Multimedia (2007). 2007. pp. 255–262. DOI: 10.1109/ISM.2007.33.
69. Xu T., Yang Z. Simple and effective speech steganography in G.723.1 low-rate codes. 2009 International Conference on Wireless Communication and Signal Processing. 2009. pp. 1–5. DOI: 10.1109/WCSP.2009.5371745.
70. Ito A., Suzuki Y. Information hiding for G.711 speech based on substitution of least significant bits and estimation of tolerable distortion. IEICE Transaction Fundamentals of Electronics, Communications and Computer Science. 2010. vol. 93. no. 7. pp. 1279–1286. DOI: 10.1587/transfun.E93.A.1279.
71. Tian H., Zhou K., Jiang H., Huang Y., Liu J., Feng D. An adaptive steganography scheme for voice over IP. Proceedings of the IEEE International Symposium on Circuits Systems. 2009. pp. 2922–2925. DOI: 10.1109/ISCAS.2009.5118414.
72. Miao R., Huang Y. An approach of covert communication based on the adaptive steganography scheme on voice over IP. IEEE International Conference on Communications (ICC). 2011. DOI: 10.1109/icc.2011.5962657.
73. Tian H., Zhou K., Huang Y., Feng D., Liu J. A covert communication model based on least significant bits steganography in voice over IP. Proceeding of the 9th International Conference for Young Computer Scientists. 2008. pp. 647–652. DOI: 10.1109/ICYCS.2008.394.
74. Janicki A., Mazurczyk W., Szczypiorski K. Steganalysis of transcoding steganography. annals of telecommunications-annales des télécommunications. 2014. vol. 69. pp. 449–460.
75. Goher S., Javed B., Saqib N. Covert channel detection: A survey-based analysis. High-Capacity Optical Networks and Emerging/Enabling Technologies. 2012. pp. 057–065.

76. Wu Z., Guo J., Zhang C., Li C. Steganography and steganalysis in voice over ip: A review. Sensors. 2021. vol. 21. no. 4.
77. Neubert T., Caballero Morcillo A.J., Vielhauer C. Improving Performance of Machine Learning based Detection of Network Steganography in Industrial Control Systems. Proceedings of the 17th International Conference on Availability, Reliability and Security. 2022. pp. 1–8.
78. Zhang X.-G., Yang G.-H., Ren X.-X. Network steganography based security framework for cyber-physical systems. Information Sciences. 2022. vol. 609. pp. 963–983.
79. Tymchenko O., Havrysh B. Steganography in TCP/IP Networks. International Conference of Artificial Intelligence, Medical Engineering, Education. 2023. pp. 47–56.
80. Chai H., Li Z., Li F., Zhang Z. An end-to-end video steganography network based on a coding unit mask. Electronics. 2022. vol. 11. no. 7. pp. 1142.
81. Olawoyin L.A., Abdul-Rahman M., Faruk N., Oloyede A., Adeniran C., Lasisi O., Sikiru I., Baba B.A. Hybridization of OFDM and Physical Layer Techniques for Information Security in Wireless System. SLU Journal of Science and Technology. 2023. vol. 6. no. 1, 2. pp. 21–29.
82. Rajesh S., Joshi A. Estimation of Transmission Bandwidth for VoIP Signals over IP Packet Transmission Network using Capacity Computing Method. IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS). 2023. pp. 01–07. DOI: 10.1109/ICICACS57338.2023.10100177.
83. Pilania U., Tanwar R., Zamani M., Manaf A.A. Framework for video steganography using integer wavelet transform and JPEG compression. Future Internet. 2022. vol. 14(9). pp. 1–16. DOI: 10.3390/fi14090254.
84. Pilania U., Kumar M., Kaur G. Region of Interest Using Viola-Jones Algorithm for Video Steganography. Applied Computational Technologies: Proceedings of ICCET 2022. 2022. pp. 405–415. DOI: 10.1007/978-981-19-2719-5_38.

Пилания Урмила — Ph.D., доцент, факультет компьютерных наук и технологий, Международный университет Манав Рахна. Область научных интересов: компьютерное зрение, обработка изображений, информационная безопасность. Число научных публикаций — 25. urmilapilania@gmail.com; Холмы Аравали, Фаридабад, 121004, Харьяна, Индия; р.т.: +91(129)419-8000.

Кумар Маной — Ph.D., доцент, факультет компьютерных наук и технологий, Международный университет Манав Рахна. Область научных интересов: компьютерное зрение, обработка изображений, машинное обучение. Число научных публикаций — 21. manojattri003@gmail.com; Холмы Аравали, Фаридабад, 121004, Харьяна, Индия; р.т.: +91(129)419-8000.

Рохит Танвар — Ph.D., доцент, департамент компьютерных наук и технологий, Университет нефтяных и энергетических исследований. Область научных интересов: информационная безопасность, машинное обучение. Число научных публикаций — 80. rohit.tanwar.cse@gmail.com; П.О. Кандоли (Прем-Нагар), Дехрадун, 248007, Уттаракханд, Индия; р.т.: +91(999)225-7914.

Нандал Неха — Ph.D., доцент кафедры, кафедра компьютерных наук и инженерии, Гитанджалиский инженерно-технологический колледж. Область научных интересов: машинное обучение, глубокое обучение, распознавание образов, интеллектуальный анализ данных. Число научных публикаций — 22. nehanandal012@gmail.com; Медчал, Чирил, 501301, Хайдарабад, Телангана, Индия; р.т.: +91(720)771-4441.

DOI 10.15622/ia.22.5.7

S.I. ABUDALFA

EVALUATION OF SKELETONIZATION TECHNIQUES FOR 2D BINARY IMAGES

Abudalfa S.I. **Evaluation of Skeletonization Techniques for 2D Binary Images.**

Abstract. In the realm of modern image processing, the emphasis often lies on engineering-based approaches rather than scientific solutions to address diverse practical problems. One prevalent task within this domain involves the skeletonization of binary images. Skeletonization is a powerful process for extracting the skeleton of objects located in digital binary images. This process is widely employed for automating many tasks in numerous fields such as pattern recognition, robot vision, animation, and image analysis. The existing skeletonization techniques are mainly based on three approaches: boundary erosion, distance coding, and Voronoi diagram for identifying an approximate skeleton. In this work, we present an empirical evaluation of a set of well-known techniques and report our findings. We specifically deal with computing skeletons in 2d binary images by selecting different approaches and evaluating their effectiveness. Visual evaluation is the primary method used to showcase the performance of selected skeletonization algorithms. Due to the absence of a definitive definition for the "true" skeleton of a digital object, accurately assessing the effectiveness of skeletonization algorithms poses a significant research challenge. The experimental results shown in this work illustrate the performance of the three main approaches in applying skeletonization with respect to different perspectives.

Keywords: image processing, skeletonization techniques, skeleton, 2d binary images.

1. Introduction. The skeleton is a simplified representation of an object that preserves its key topological and geometrical characteristics while being equidistant to its boundaries. Its purpose is to extract a shape feature that represents the general form of an object. The concept of a skeleton was introduced by H. Blum [1] as a result of the Medial Axis Transform (MAT) or Symmetry Axis Transform (SAT), which determines the closest boundary point(s) for each point in an object. An inner point belongs to the skeleton if it has at least two closest boundary points.

The skeleton [2] is much thinner than the original object as it contains far fewer points. It captures local object symmetries and the topological structure of the object while preserving its shape and topology. However, MATs are curves (1D) in a 2D object and surfaces (2D) in a 3D object that are not stable under boundary perturbation, and the same skeleton may belong to different elongated objects.

Skeletons are crucial for object representation in computer graphics and image shape analysis, including bio-medical image analysis and recognition in different fields. Methods based on the computation of an object's skeleton are widely used in pattern recognition and image shape classification, as the skeleton or MAT of the object is an essential descriptor

of its shape. Skeletons are used to generate features for determining the similarity measures of various shapes in constructing classifiers.

Various approaches exist for identifying skeletons and they are mainly based on boundary erosion, distance coding, and Voronoi diagram. The primary aim of this work is to implement and evaluate various skeletonization techniques drawn from the literature that embody different approaches to the task.

The remainder of this paper is structured as follows: Section 2 presents a background for this research direction. Section 3 provides a review of relevant studies. Section 4 details the methodology employed to address the research problem. Section 5 analyzes the results obtained from the experiments. Lastly, Section 6 concludes the paper and highlights potential avenues for future research.

2. Background. In this section, brief descriptions are introduced for presenting the approaches and techniques used for applying skeletonization to 2D binary images. The next subsections present the techniques used with the three main approaches of Skeletonization.

2.1. Erosion-Based Skeletonization. This approach of skeletonization can be implemented by using two methods as described in the next subsections.

2.1.1. Morphological-Based Skeletonization. In this method, we use morphological operation [3] to compute object skeletons. The skeleton of image A can be expressed in terms of erosions and openings as shown in Equation (1):

$$S(A) = \bigcup_{k=0}^{K} S_k(A), where\ K = \max\{k | A \Theta kB\ \neq \emptyset\}, \tag{1}$$

$$S_k(A) = (A \Theta kB) - (A \Theta kB) \circ B,$$

where B is a structuring element, and $(A \Theta kB)$ indicates k successive erosions of A as shown in Equation (2):

$$(A \Theta kB) = ((\dots((A \Theta B) \Theta B) \Theta \dots) \Theta B. \tag{2}$$

From the other side, A (original object) can be reconstructed from these subsets by using Equation (3):

$$A = \cup_{k=0}^{K} (S_k(A) \oplus kB)\,, \tag{3}$$

where $S_k(A) \oplus kB$ denotes k successive dilations of $S_k(A)$ as shown in equation (4):

$$(S_k(A) \oplus kB) = ((\dots((S_k(A) \oplus B) \oplus B) \oplus B) \dots) \oplus B. \quad (4)$$

2.1.2. Thinning-Based Skeletonization. We can use morphological thinning operations [4] to identify the skeleton by iteratively removing pixels on the boundaries of objects and preserving object topology from breaking it into parts as shown in Figure 1.

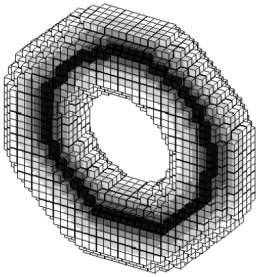


Fig. 1. The darkest voxels belong to the computed skeleton
(Retrieved from http://www.inf.u-szeged.hu/~palagyi/skel/skel.html)

The thinning method is known to possess certain advantageous characteristics. For instance, it helps retain the original shape and topology of an object while positioning the skeleton in the center of the object, resulting in a skeleton that is one pixel/voxel wide. However, it may not always preserve the topology completely, as it may lead to object disconnection, complete object removal, or formation of cavities (i.e., white connected components enclosed by an object).

2.2. Voronoi Diagram-Based Skeletonization. Under this approach, as the density of boundary points (i.e., generating points) tends towards infinity, the associated Voronoi diagram gradually approaches the skeleton [5]. Figure 2 illustrates the idea by showing Voronoi diagram and skeleton for the rectangular object.

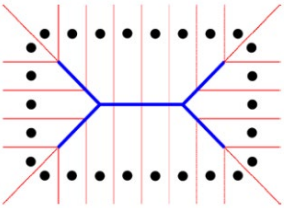


Fig. 2. The skeleton is marked by blue lines
(Retrieved from http://www.inf.u-szeged.hu/~palagyi/skel/skel.html)

By exclusively utilizing pixels located on an object's boundary, this approach proves to be highly efficient for thick objects, with efficiency increasing in proportion to the object's radius, rather than its overall area. However, it may be susceptible to minor defects present on the boundaries (or small holes within the object). Additionally, this approach is capable of analytically determining the topology of the skeleton and can produce output that includes the vertices and edges of the skeleton graph.

2.3. Distance Map-Based Skeletonization. Under this approach, the distance transform [6] assigns a value to each pixel in the binary image *B*, representing the distance between that pixel and the nearest non-zero pixel of *B*. The ridges, which refer to local extremes, are subsequently identified as skeletal points. Figure 3 offers a visual depiction of the distance transformation and illustrates the ridges that form part of the skeleton.

a) b)

Fig. 3. Distance Map-Based Skeletonization: a) binary image; b) distance map (non-binary image)
(Retrieved from http://www.inf.u-szeged.hu/~palagyi/skel/skel.html)

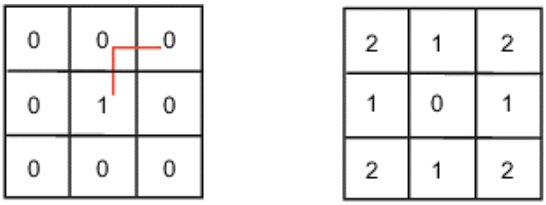
Numerous distance measures [7] can be used to compute distance maps. The next subsections describe the distance measures that are used in our work. In the last subsection, we introduce a brief description of the Fast Marching algorithm which is used for improving the accuracy of distance map-based skeletonization.

2.3.1. City-Block Distance. This measure is based on 4-neighbor adjacency in calculating distance. Equation 5 illustrates how to calculate the distance in two-dimensional space with respect to two points – (x1,y1) and (x2,y2):

$$\left| x1 - x2 \right| + \left| y1 - y2 \right| . \quad (5)$$

Figure 4 shows a simple example of calculating distances between the center and their neighbors by using city-block measure. As illustrated in the figure, the distance which is calculated between the original pixel and its

diagonal neighbors (N_D) is 2 while the distance value is 1 for the 4-neighbors (N_4) because this measure is specifically based on 4-neighbor adjacency.

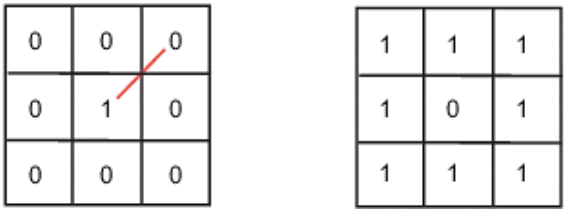


a) b)

Fig. 4. Distance transform using city-block measure: a) image; b) distance transform (Retrieved from https://www.mathworks.com/help/images/distance-transform-of-a-binary-image.html)

2.3.2. Chess-Board Distance. This measure is based on 8-neighbor adjacency for calculating distance by using Equation 6. As illustrated in Figure 5 the distance between the original pixel and its 8-neighbor (N_8) is 1 because this measure based on 8-neighbor adjacency.

$$\max(\left|x1 - x2\right|, \left|y1 - y2\right|), \tag{6}$$

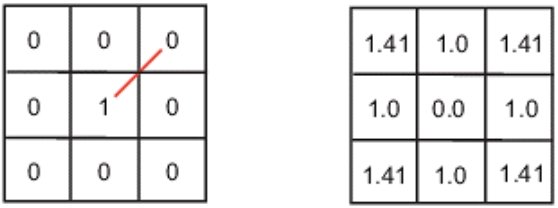


a) b)

Fig. 5. Distance transform using Chess-Board measure: a) image; b) distance transform (Retrieved from https://www.mathworks.com/help/images/distance-transform-of-a-binary-image.html)

2.3.3. Euclidean Distance. Euclidean distance is a famous distance measure and it is used widely in many applications by using the following Equation 7. Figure 6 shows that N_D took more distance value than N_4 based on the Euclidean distance measure. However, this value is less than 2 which is calculated by using the city-block measure.

$$\sqrt{(x_1 - x_2)^2 + (y_1 - y_{2)}{}^2} \tag{7}$$



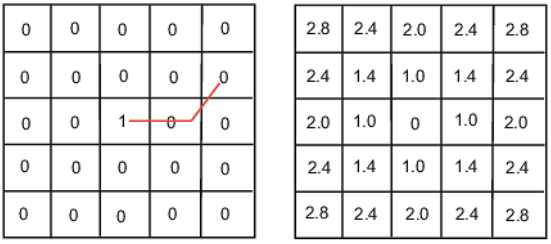
a) b)

Fig. 6. Distance transform using Euclidean measure: a) image; b) distance transform (Retrieved from https://www.mathworks.com/help/images/distance-transform-of-a-binary-image.html)

2.3.4. Quasi-Euclidean Distance. The quasi-Euclidean distance measure is an improved version of the Euclidean measure which is calculated by using Equation 8. The effect of this measure on the neighbor distances is more widely as illustrated in Figure 7:

$$|x_1 - x_2| + (\sqrt{2} - 1)|y_1 - y_2|, |x_1 - x_2| > |y_1 - y_2|, \quad (8)$$

$$(\sqrt{2} - 1)|x_1 - x_2| + |y_1 - y_2|, otherwise.$$



a) b)

Fig. 7. Distance transform using the quasi-Euclidean measure: a) image; b) distance transform
(Retrieved from https://www.mathworks.com/help/images/distance-transform-of-a-binary-image.html)

2.3.5. Improving Distance Map Based Skeletonization. The basic algorithm for finding local maximum ridges through computing skeletons is based on comparing N_4 neighbors. In this work, we evaluate also the performance of using N_8 neighbors in detecting the local maximum to increase the accuracy of resulted skeletons. Based on the results of our experiments, we have observed that increasing the number of selected neighbors enhances the performance of distance map-based skeletonization.

2.3.6. Fast Marching Algorithm. The Fast Marching algorithm [8] is a numerical technique that accurately captures the viscosity solution of the Eikonal equation, norm(grad(D))=P. The level set {x \ F(x)=t} represents a front that progressively advances with a speed of P(x). The resultant function D acts as a distance function, and if the velocity P remains constant, it can be viewed as the distance function for a group of initial points. The Fast Marching is very similar to the Dijkstra algorithm [9] that finds the shortest paths on graphs. Therefore, we can use the Fast Marching technique to compute the distance map for a more accurate resulted transformation.

3. Literature Review. We surveyed two main aspects related to skeletonization of 2d binary images in order to conduct experiment work. The first aspect leads us to explore several approaches for evaluating the skeletonization techniques. The second aspect is to evaluate the performance of some selected techniques.

The literature classifies the skeletonization techniques into three main categories based on the implementation view [10]. The first group of skeletonization techniques computes skeletons by detecting ridges in the distance map of the boundary points [11]. The second category is based on calculating the Voronoi diagram generated by the boundary points [12]. While the third group employs a layer-by-layer erosion technique known as thinning [13].

In digital spaces, only an approximation of the "true skeleton" can be extracted. There are two requirements to be complied with: 1) Topological [14] to retain the topology of the original object. 2) Geometrical [15] to force the skeleton to be in the middle of the object and invariance under the most important geometrical transformation including translation, rotation, and scaling.

Skeletonization methods that rely on the distance transform can only retain geometrical properties, whereas those based on thinning can solely preserve topological properties. On the other hand, skeletonization techniques that utilize Voronoi-Skeleton can successfully retain both sets of requirements. Table 1 illustrates a comparison between these three approaches.

Table 1. Comparison between three skeletonization approaches

Approach	Geometrical	Topological
Distance Transform	Yes	No
Voronoi-Skeleton	Yes	Yes
Thinning	No	Yes

While skeletons can be obtained from both 2D and 3D objects [16], our primary focus in this project centers on generating skeletons from 2D images. Consequently, we restrict our analysis solely to skeletonization methods that are applicable to 2D images.

Numerous enhancements have recently been introduced to several existing algorithms presented in the literature, all of which aim to enhance the efficiency of specific tasks by using 2D binary image skeletonization. For example, in paper [17] employ 2D skeleton features with an automated system that overcomes the dimensionality problems with human action recognition. Whereas, in paper [18] the authors present a new framework for extracting skeletons from noisy images and apply this framework to the task of hand gesture recognition.

Some related works evaluated the performance of skeletonization techniques. However, our work is still unique since our evaluation covers different perspectives. In paper [19] the authors present their approach for evaluating the performance of skeletonization methods for document images with rotation states, along with experimental results and discussions. The article discusses the importance of skeletonization in document image analysis and presents various methods used for skeletonization. In the same context, in [20] the authors compare the performance of different image skeletonization methods in biometric security systems.

Skeletonization is widely used for automating in many fields such as biomedical, natural language processing and animation. This high exploitation of skeletonization encouraged us for evaluating the performance of some skeletonization techniques by using images selected from different domains. Thereby, we can claim that our work is unique in comparison with other related works. The next paragraphs present recent works that use skeletonization for conducting many tasks.

In paper [21] the authors discuss the technique of digital skeletonization, which is a widely used method for extracting the structural information of objects in biomedical images. In the same field, in [22] the authors present a study on the analysis of blood vessels in angiogenesis using 3D visualization, skeletonization, and branching analysis techniques.

It is worth mentioning here that skeletonization is widely used for improving the segmentation accuracy of specific areas in biomedical images. For example, in study [23] the authors propose a method for segmenting abdominal arteries from an abdominal computed tomography (CT) volume by leveraging artery skeleton information. Another example was recently revealed with work presented in [24]. The authors propose a new segmentation method based on skeletonization for the cross-sectional optic nerve on magnetic resonance (MR) images.

Skeletonization is also used as a basic approach for action recognition [25]. For example, in study [26] the authors extract skeletal data for utilizing a human tracking. Whereas, in [27] the authors present a method based on skeletonization for recognizing the campus violence. In

the same context, in [28] the authors extract the skeleton of the person in the video as a first step for developing a multi-speed transformer network that improves the performance of action recognition. In paper [29] the authors employ as well skeletonization for recognizing human gait gender. Similarly, study [30] present a hybrid network for improving the performance of skeleton-based action recognition.

Additionally, there are a lot of uses for skeletonization with natural language processing. For example, study [31] present a model that employs skeletonization for generating stories in a coherent manner. Whereas, in [32] the authors propose a skeleton Filter for improving the performance of skeletonization in noisy text images.

The skeletonization is widely used as well for detecting text in images and segmenting the resulting text into words and characters. Therefore, the skeletonization is sufficiently used for developing optical character recognition (OCR) systems [33] with natural languages. For example, in [34] the authors present a technique for analyzing the Arabic text documents. The authors evaluated the performance of their work on a set of text images selected from the King Fahd University of Petroleum and Minerals (KFUPM) handwritten Arabic text (KHATT) database.

In the same context, study [35] presents a segmentation algorithm for handwritten Arabic word recognition. Their presented algorithm provides a description of skeleton points including their coordinates, types, and the number of neighboring points in the 8-neighborhood. This enables the extraction of representative primitives of characteristic points, which are utilized in the segmentation phase.

It is worth mentioning here that our study does not deal with the skeletonization in terms of computational efficiency. Skeletonization techniques can be categorized into two types: sequential methods, such as those described in references [36, 37], and parallel methods, as described in references [38, 39, 40].

Of course, employing parallel methods will reduce computational time in comparison with sequential methods. However, certain types of skeletons can only be calculated using sequential algorithms, while other types can only be obtained through parallel algorithms. Whereas, for many types of skeletons, both sequential and parallel algorithms can be used, especially when working with digital structures.

With sequential algorithms, there is a risk of producing different skeletons depending on the order in which the elements are processed. In contrast, parallel algorithms are generally faster, but maintaining topology preservation can be a challenging task.

To understand the efficacy of employing methods with skeletonization techniques, the reader may refer to the recent work presented in [41]. The authors present a fully parallel thinning algorithm through a thorough examination of the popular Zhang-Suen (ZS) series algorithms and the one-pass thinning algorithm (OPTA) series algorithms. In terms of handling boundary noise, their algorithm has demonstrated greater robustness than the OPTA-series algorithms. Furthermore, it exhibits a faster thinning speed compared to the ZS-series algorithms.

Based on our knowledge, modern skeletonization methods [42, 43] have often been developed and tailored to address specific domains, limiting their applicability across diverse domains. Therefore, there are still some challenges that should be addressed in this research direction.

4. Methodology. In this section, we describe the methodology used for conducting the empirical analysis. The main objective of this research work is to compute approximate skeletons for 2D objects using different techniques. We collected binary images that contain different 2D objects to extract skeletons. We selected images from different domains to make our empirical analysis unique. Thereby, this work shows different perspectives for analyzing the selected models. Some of these images are cropped from the KHATT database to compute also skeletons for characters. In order to achieve this objective the following tools and programs are used for conducting our experiments:

– Matlab: is used for image processing and programming purposes.
– C++ compiler: is used to compile a code that is related to building Voronoi diagram in reasonable time-consuming.
– We use qhull tool[1] for computing voronoi diagram.
– Using Toolbox entitled Fast Marching[2] for implementing the Fast Marching algorithm.

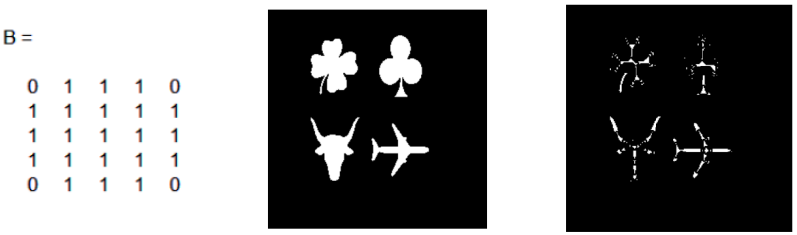
In this work, we use visual evaluation for showing the performance of the selected skeletonization algorithms. The lack of a clear definition for the "true" skeleton of a digital object presents a significant research challenge when it comes to evaluating the performance of skeletonization algorithms [44]. Therefore, visual evaluation is still the most traded method used for assessing the performance of different skeletonization algorithms. There are some attempts made by researchers for presenting a quantitative assessment of skeletonization algorithms [45]. However, the resulting measures are used for custom domains and do not fit our work.

[1] http://www.qhull.org/
[2] https://www.mathworks.com/matlabcentral/fileexchange/6110-toolbox-fast-marching

5. Experiment Results. This section presents all results of our experiments conducted to evaluate the selected skeletonization techniques. The next subsections show the results with sufficient analysis.

5.1. Morphological-Based Skeletonization. Figure 8 shows the results of applying 7 iterations of erosion and opening morphological operations to compute skeletons. Matrix B illustrates the structural element that used in this experiment. We selected circular shape structural elements to increase the accuracy of computing the skeleton based on finding MAT.

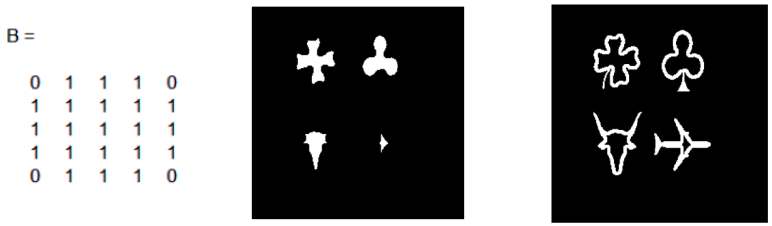
We can note from the figure that the results are not accurate and the skeleton width is more than one pixel whereas it is not connected. Thus, we can conclude that using morphological operations is not an accurate technique for computing skeletons.



a) b) c)

Fig. 8. Morphological Based Skeletonization: a) Structural Element; b) Original Image A (256x256); c) Skeleton

Figure 9 shows the results of applying dilation morphological operations to reconstruct the object from the skeleton. The figure also shows the accuracy of the reconstructed objects by subtracting the reconstructed image from the original image. We can conclude that this reconstruction technique generated interesting results, but it is not good enough to reconstruct the original shape of objects.

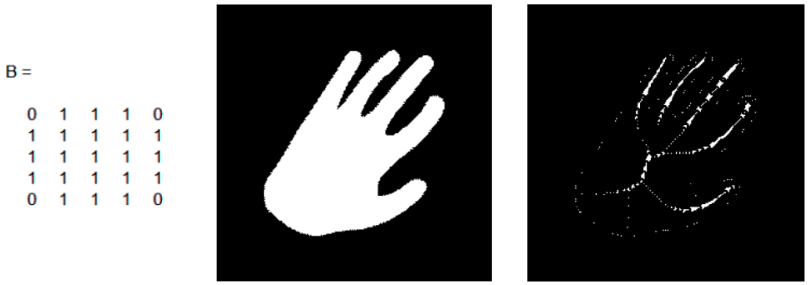


a) b) c)

Fig. 9. Reconstruction from Morphological Based Skeletonization: a) Structural Element; b) Partial Reconstruction; c) Difference Between Original and Partial Reconstruction

Figure 10 shows the results of computing the skeleton by applying 23 iterations of erosion and opening morphological operations to a large object (hand shape). We can clearly note that the result is not accurate, but the interesting observation is shown in Figure 11 which illustrates that a very small portion of the hand object (without even identifying the object shape) is reconstructed using dilation morphological operations.

Thus, we can conclude that using large objects is not suitable with this technique because the size of the structural element is very small in comparison with the object size. This means that the morphological-based Skeletonization technique is sensitive to the size of the structural element.



a) b) c)

Fig. 10. Morphological-Based Skeletonization (Large Object): a) Structural Element; b) Original Image A (256x256); c) Skeleton

a) b) c)

Fig. 11. Reconstruction from Morphological-Based Skeletonization: a) Structural Element; b) Partial Reconstruction; c) Difference Between Original and Partial Reconstruction

5.2. Thinning-Based Skeletonization. Figure 12 shows the results of using thinning morphological operations to compute the skeleton with using different numbers of thinning operations (k). In this experiment, we

used the same image illustrated in Figure 10. We can note that this technique generates very accurate results and preserves the object's shape.

Figure 13 shows the results of applying this technique on medical images (blood vessels) whereas Figure 14 and Figure 15 show the results of applying this technique on cropped images selected from the KHATT dataset for computing skeletons of text.

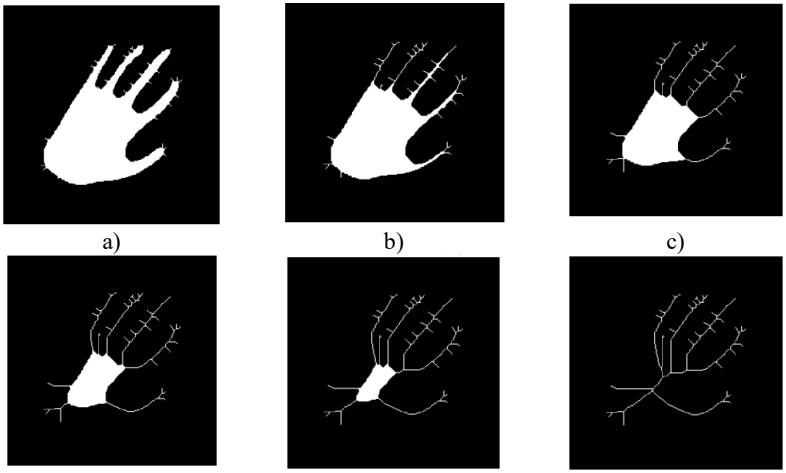
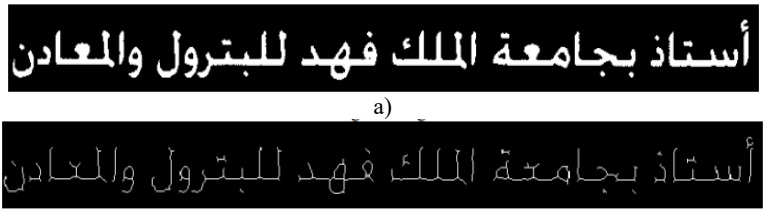


Fig. 12. Thinning-Based Skeletonization: a) Skeletonization with k=5; b) Skeletonization with k=10; c) Skeletonization with k=20; d) Skeletonization with k=30; e) Skeletonization with k=40; f) Skeletonization with k>50

Fig. 13. Thinning-Based Skeletonization: a) Original Image; b) Skeleton



a)

b)

Fig. 14. Thinning-Based Skeletonization: a) Original Image; b) Skeleton

a) b)

Fig. 15. Thinning Based Skeletonization: a) Original Image; b) Skeleton

5.3. Voronoi Diagram-Based Skeletonization. Figure 16 shows a sample result of applying Voronoi diagram-based skeletonization to an image that includes a hand object. When we compare the results of this technique with the results of morphological and thinning-based skeletonization, it is worth noting that this technique outperforms morphological techniques in terms of achieving better results. However, it is not better than thinning-based skeletonization.

a) b)

Fig. 16. Voronoi Diagram Based Skeletonization: a) Original Image; b) Skeleton

5.4. Distance Map-Based Skeletonization. Figure 17 shows the results of applying distance map-based skeletonization by using four distance measures [46]. We can note that using city-block distance performs the best results since it generates the most accurate skeleton with preserving object shape. However, this technique is not better than thinning-based skeletonization nor Voronoi diagram-based skeletonization since the skeleton shape is not connected. We can also say that it is better than morphological-based technique.

5.5. Improved Distance Map-Based Skeletonization. We tried to do some improvements to the distance map-based technique by applying alternative methods for detecting local maximum values from the distance map when computing the skeleton. The detail of this method is presented in Section 2.3.5.

Figure 18 shows the results of our suggested improvement. We can note that the results are less sensitive in comparison with the original algorithm of skeletonization which is based on distance measure.

We can also note that the best results are provided with the skeleton that is computed by using chess-board distance followed by removing many useless branches from the first version of the skeleton shape. This result reveals that our work may be extended by evaluating the performance of applying more distance measures and employing suitable modifications that provide an accurate form of skeleton shape.

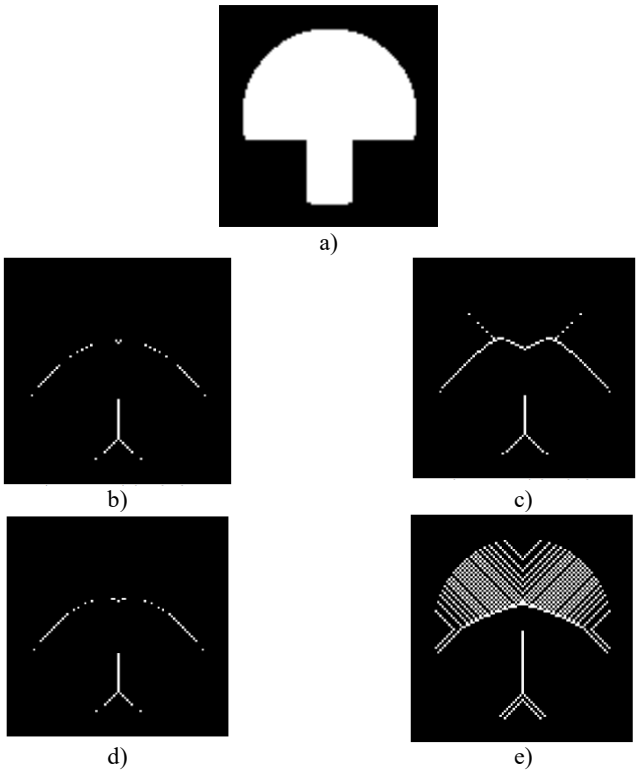


Fig. 17. Distance Map-Based Skeletonization: a) Original Image; b) Euclidean Distance; c) City-Block Distance; d) Quasi-Euclidean Distance e) Chess-Board Distance

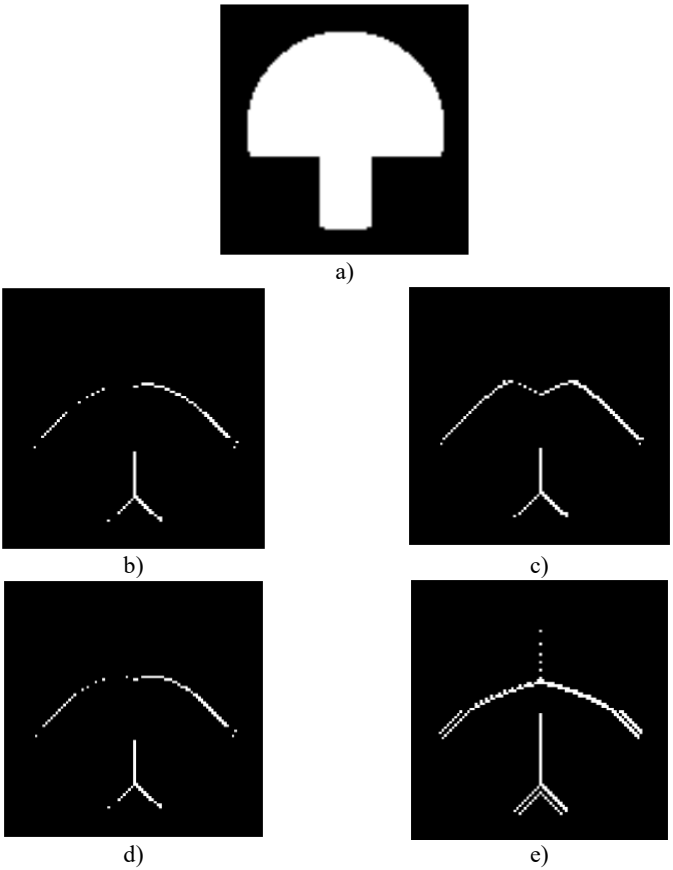
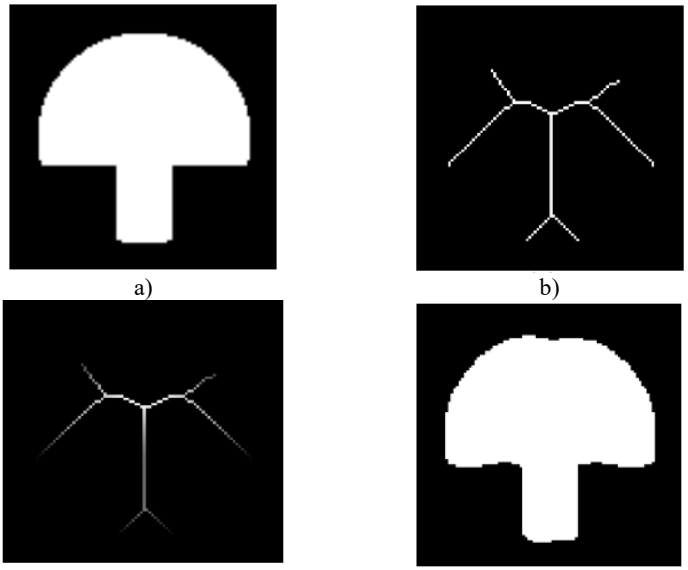


Fig. 18. Improved Distance Map-Based Skeletonization: a) Original Image; b) Euclidean Distance; c) City-Block Distance; d) Quasi-Euclidean Distance e) Chess-Board Distance

We can also inversely employ the distance transformation technique to reconstruct approximated shapes for the original object. Figure 19 shows the results of using this technique to reconstruct the approximated shape of a mushroom object. We can note from the figure that this technique is good enough for computing the approximate shape of the original object. However, we cannot claim that the reconstructed shape is the original object since the same skeleton may belong to different objects.

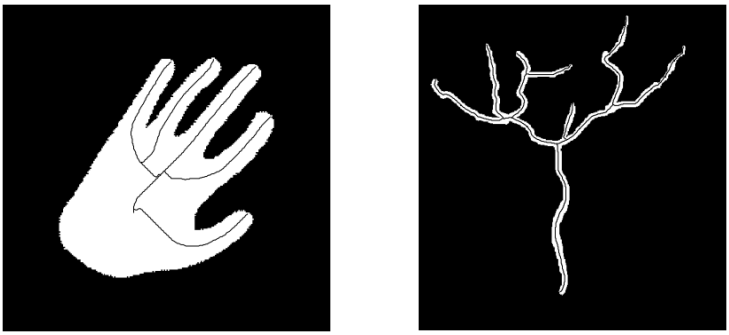


a) b)

c) d)

Fig. 19. Object Reconstruction using Distance Transform: a) Original Image; b) Skelton; c) Skelton + Distance Transform; d) Inverse Distance Transform

5.6. Distance Map-Based Skeletonization using the Fast Marching Algorithm. Figure 20 shows the results of computing a very accurate skeleton by using the fast marching algorithm. We can note that this technique is robust and computes skeletons that preserve the topological and geometrical requirements of objects.



a) b)

Fig. 20. Distance Map-Based Skeletonization using Fast Marching: a) Extracted Skeleton; b) Extracted Skeleton

6. Conclusion and Future Work. In this work, we present a comparative study to evaluate three categories of skeletonization techniques: boundary erosion, distance coding, and Voronoi diagram. Based on our experiment results, thining-based skeletonization performs the best results.

In digital spaces, only an approximation of the "true skeleton" can be extracted. Thus, depending on the excepted outcomes, the developed experiment can compute skeletons that are approximate to the optimal skeletons in 2d binary images.

In this work, we evaluate the effectiveness and performance of skeletonization techniques by presenting visualization techniques for image skeletonization. We also visualize the efficiency of reconstructing objects from skeletons.

This work can be extended in different directions. Exploring enhanced approaches for distance map-based skeletonization would be an intriguing direction to pursue. Employing more distance measures may reveal competitive results in detecting skeletons. Additionally, evaluating the performance of merging more than one skeletonization technique may provide competitive performance and this direction should be explored from numerous perspectives.

Another promising approach would be also an intriguing direction to pursue based on converting a binary image to grayscale by summing pixels within a square mask. Thereby, optimal halftone image approximations can be calculated based on standard deviation. This approach may potentially result in a highlighted skeleton effect and may be used for evaluating the performance of skeletonization techniques.

References

1. Blum H. Biological Shape and Visual Science. J. Theor. Biol. 1973. vol. 38. pp. 205–287.
2. Zhang Y, Sang L, Grzegorzek M, See J, Yang C. BlumNet: Graph component detection for object skeleton extraction. Proceedings of the 30th ACM International Conference on Multimedia. 2022. pp. 5527–5536.
3. Sanchez-Salvador J.L., Campano C., Lopez-Exposito P., Tarrés Q., Mutjé P., Delgado-Aguilar M., Monte M.C. Blanco A. Enhanced morphological characterization of cellulose nano/microfibers through image skeleton analysis. Nanomaterials. 2021. vol. 11. no. 8. DOI: 10.3390/nano11082077.
4. Zhang F., Chen X., Zhang X. Parallel thinning and skeletonization algorithm based on cellular automaton. Multimedia Tools and Applications. 2020. vol. 79. pp. 33215–33232.
5. Kotsur D., Tereshchenko V. An optimized algorithm for computing the Voronoi skeleton. International Journal of Computing. 2020. vol. 19. no. 4. pp. 542–554.
6. Wang Y., Xu Y., Tsogkas S., Bai X., Dickinson S, Siddiqi K. Deepflux for skeletons in the wild. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2019. pp. 5287–5296.

7. Cha S.H. Comprehensive survey on distance/similarity measures be-tween probability density functions. International Journal of Mathe-matical Models and Methods in Applied Sciences. 2007. vol. 1(4). pp. 300–307.
8. Yatziv L., Bartesaghi A., Sapiro G. O(N) implementation of the fast marching algorithm. Journal of computational physics. 2006. vol. 212. no. 2. pp. 393–399.
9. Wang H., Yu Y., Yuan Q. Application of Dijkstra algorithm in robot path-planning. Second international conference on mechanic automation and control engineering. 2011. pp. 1067–1069.
10. Gonzalez R.C., Woods R.E. Digital Image Processing, 3rd edition. Pearson Education, 2010. 185 p.
11. Song C., Pang Z., Jing X., Xiao C. Distance field guided L1-median skeleton extraction. The Visual Computer. 2018. vol. 34. pp. 243–55.
12. Langer M., Gabdulkhakova A., Kropatsch W.G. Non-centered Voronoi skeletons. Discrete Geometry for Computer Imagery: 21st IAPR International Conference. 2019. pp. 355–366.
13. Boudaoud L.B., Solaiman B., Tari A. A modified ZS thinning algorithm by a hybrid approach. The Visual Computer. 2018. vol. 34. pp. 689–706.
14. Morbiducci U., Mazzi V., Domanin M., De Nisco G., Vergara C., Steinman D.A., Gallo D. Wall shear stress topological skeleton independently predicts long-term restenosis after carotid bifurcation endarterectomy. Annals of biomedical engineering. 2020. vol. 48. pp. 2936–2949.
15. Breuß M., Bruckstein A.M., Kiselman C.O., Maragos P. Shape Analysis: Euclidean, Discrete and Algebraic Geometric Methods. Dagstuhl Reports. 2018. vol. 8. no. 10. pp. 87–103.
16. Zhang W., Wang X., Li X., Chen J. 3D skeletonization feature based computer-aided detection system for pulmonary nodules in CT datasets. Computers in biology and medicine. 2018. vol. 92. pp. 64–72.
17. Malik N.U., Sheikh U.U., Abu-Bakar S.A., Channa A. Multi-View Human Action Recognition Using Skeleton Based-FineKNN with Extraneous Frame Scrapping Technique. Sensors. 2023. vol. 23. no. 5. DOI: 10.3390/s23052745.
18. Ma J., Ren X., Li H., Li W., Tsviatkou V.Y., Boriskevich A.A. Noise-Against Skeleton Extraction Framework and Application on Hand Gesture Recognition. IEEE Access. 2023. vol. 11. pp. 9547–9559.
19. Bataineh B., Alqudah M.K. Evaluation of Skeletonization Methods for Document Images with Rotation States. Amity International Conference on Artificial Intelligence. 2019. pp. 424–428. DOI: 10.1109/AICAI.2019.8701352.
20. Nazarkevych M., Dmytruk S., Hrytsyk V., Vozna O., Kuza A., Shevchuk O., Voznyi Y., Maslanych I., Sheketa V. Evaluation of the effectiveness of different image skeletonization methods in biometric security systems. International Journal of Sensors Wireless Communications and Control. 2021. vol. 11. no. 5. pp. 542–552.
21. Perumalla S.R., Alekhya B., Raju M.C. Digital Skeletonization for Bio-Medical Images. Proceedings of Third International Conference on Sustainable Expert Systems. 2023. pp. 277–291.
22. Ramakrishnan V., Schönmehl R., Artinger A., Winter L., Böck H., Schreml S., Gürtler F., Daza J., Schmitt V.H., Mamilos A., Arbelaez P. 3D Visualization, Skeletonization and Branching Analysis of Blood Vessels in Angiogenesis. International Journal of Molecular Sciences. 2023. vol. 24. no. 9. DOI: 10.3390/ijms24097714.
23. Zhu R., Oda M., Hayashi Y., Kitasaka T., Misawa K., Fujiwara M., Mori K. A skeleton context-aware 3D fully convolutional network for abdominal artery segmentation. International Journal of Computer Assisted Radiology and Surgery. 2023. vol. 18. no. 3. pp. 461–472.

24. Feng Y., Chow L.S., Gowdh N.M., Ramli N., Tan L.K., Abdullah S., Tiang S.S. Gradient-based edge detection with skeletonization (GES) segmentation for magnetic resonance optic nerve images. Biomedical Signal Processing and Control. 2023. vol. 1. no. 80. DOI: 10.3390/ijms24097714.
25. Feng M., Meunier J. Skeleton Graph-Neural-Network-Based Human Action Recognition: A Survey. Sensors. 2022. vol. 22. no. 6. DOI: 10.3390/s22062091.
26. Chen D., Zhang T., Zhou P., Yan C., Li C. OFPI: Optical Flow Pose Image for Action Recognition. Mathematics. 2023. vol. 11. no. 6. DOI: 10.3390/math11061451.
27. Xing Y., Dai Y., Hirota K., Jia A. Skeleton-based method for recognizing the campus violence. Proceedings of the 9th International Symposium on Computational Intelligence and Industrial Applications. 2020. pp. 19–20.
28. Cheriet M., Dentamaro V., Hamdan M., Impedovo D., Pirlo G. Multi-Speed Transformer Network for Neurodegenerative disease assessment and activity recognition. Computer Methods and Programs in Biomedicine. 2023. vol. 230(3). DOI: 10.1016/j.cmpb.2023.107344.
29. Alsaif O.I., Hasan S.Q., Maray A.H. Using skeleton model to recognize human gait gender. IAES International Journal of Artificial Intelligence. 2023. vol. 12. no. 2. pp. 974–983. DOI: 10.11591/ijai.v12.i2.pp974-983.
30. Yang W., Zhang J., Cai J., Xu Z. HybridNet: Integrating GCN and CNN for skeleton-based action recognition. Applied Intelligence. 2023. vol. 53. no. 1. pp. 574–585.
31. Xu J., Zhang Y., Zeng Q., Ren X., Cai X., Sun X. A skeleton based model for promoting coherence among sentences in narrative story generation. arXiv preprint arXiv:1808.06945, 2018.
32. Bai X., Ye L., Zhu J., Zhu L., Komura T. Skeleton filter: a self-symmetric filter for skeletonization in noisy text images. IEEE Transactions on Image Processing. 2019. vol. 29. pp. 1815–1826.
33. Faizullah S., Ayub M.S., Hussain S., Khan M.A. A Survey of OCR in Arabic Language: Applications, Techniques, and Challenges. Applied Sciences. 2023. vol. 13. no. 7. DOI: 10.3390/app13074584.
34. Abdo H.A., Abdu A., Manza R.R., Bawiskar S. An approach to analysis of Arabic text documents into text lines, words, and characters. Indonesian Journal of Electrical Engineering and Computer Science. 2022. vol. 26. no. 2. pp. 754–763.
35. Kiamouche O., Bennia A. Segmentation of Handwritten Arabic Words Using High Level Informative Scheme. 2nd International Conference on Advanced Electrical Engineering. 2022. 7 p. DOI: 10.1109/ICAEE53772.2022.9962062.
36. Arcelli C., Sanniti di Baja G., Serino L. Distance-driven skeletonization in voxel images. IEEE Trans. Pattern Anal. Mach. Intell. 2011. vol. 33. no. 4. pp. 709–720.
37. Bitter I., Kaufman A.E., Sato M. Penalized-distance volumetric skeleton algorithm, IEEE Trans. Vis. Comput. Graph. 2001. vol. 7. no. 3. pp. 195–206.
38. Lohou C., Bertrand G. A 3D 12-subiteration thinning algorithm based on P-simple points, Discrete Appl. Math. 2004. vol. 139. no. 1. pp. 171–195.
39. Lohou C., Bertrand G. A 3D 6-subiteration curve thinning algorithm based on P-simple points, Discrete Appl. Math. 2005. vol. 151. no. 1. pp. 198–228.
40. Németh G., Kardos P., Palágyi K., Thinning combined with iteration-by-iteration smoothing for 3D binary images, Graph. Models. 2011. vol. 73. pp. 335–345.
41. Ma J., Ren X., Tsviatkou V.Y., Kanapelka V.K. A novel fully parallel skeletonization algorithm. Pattern Analysis and Applications. 2022. vol. 25. 169–188. DOI: 10.1007/s10044-021-01039-y.
42. Perumalla S.R., Alekhya B., Raju MC. Digital Skeletonization for Bio-Medical Images. Proceedings of Third International Conference on Sustainable Expert Systems: ICSES. 2023. pp. 277–291.

43. Pinyoanuntapong E., Ali A., Wang P., Lee M., Chen C. GaitMixer: skeleton-based gait representation learning via wide-spectrum multi-axial mixer. Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2023. DOI: 10.48550/arXiv.2210.15491.
44. Saha P.K., Borgefors G., di Baja G.S. A survey on skeletonization algorithms and their applications. Pattern recognition letters. 2016. vol. 76. pp. 3–12. DOI: 10.1016/j.patrec.2015.04.006.
45. Gittoes W., Botterill T., Green R. Quantitative analysis of skeletonisation algorithms for modelling of branches. Proceedings of Image and Vision Computing New Zealand. 2011. 6 p.
46. Abudalfa S., Mikki M. K-means algorithm with a novel distance measure. Turkish Journal of Electrical Engineering and Computer Sciences. 2013. vol. 21. no. 6. pp. 1665–1684.

Abudalfa Shadi — Ph.D., Dr.Sci., Assistant professor, University College of Applied Sciences. Research interests: artificial intelligence, data mining, sentiment analysis. The number of publications — 25. sabudalfa@ucas.edu.ps; Aoun Al-Shawa Street, Tel Al-Hawa, 1415, Gaza, Palestine, State of; office phone: +970(8)262-4999.

УДК 006.72 **DOI** 10.15622/ia.22.5.7

Ш.И. Абудальфа

ОЦЕНКА МЕТОДОВ СКЕЛЕТИЗАЦИИ ДВУМЕРНЫХ БИНАРНЫХ ИЗОБРАЖЕНИЙ

Абудальфа Ш.И. **Оценка методов скелетизации двумерных бинарных изображений.**

Аннотация. В сфере современной обработки изображений упор часто делается на инженерные подходы, а не на научные решения разнообразных практических задач. Одна из распространенных задач в этой области включает скелетирование бинарных изображений. Скелетонизация — это мощный процесс извлечения скелета объектов, находящихся в цифровом бинарном изображении. Этот процесс широко используется для автоматизации многих задач в различных областях, таких как распознавание образов, техническое зрение, анимация и анализ изображений. Существующие методы скелетизации в принципе основаны на трех подходах: эрозии границ, дистанционном кодировании и диаграмме Вороного для идентификации приблизительного скелета. В работе представлены результаты эмпирического оценивания набора хорошо известных методов. Затем выполнен расчет скелетов в двумерном бинарном изображении с выбором различных подходов и оценкой их эффективности. Визуальная оценка – это основной метод, используемый для демонстрации производительности выбранных алгоритмов скелетирования. Из-за отсутствия окончательного определения «истинного» скелета цифрового объекта точная оценка эффективности алгоритмов скелетирования представляет собой серьезную исследовательскую задачу. Были попытки проведения количественной оценки, однако применяемые меры обычно адаптировали для конкретных областей. Экспериментальные результаты, показанные в этой работе, иллюстрируют эффективность трех основных подходов к скелетизации изображений в различных перспективных приложениях.

Ключевые слова: обработка изображений, техники скелетирования, скелет, двумерные бинарные изображения.

Литература

1. Blum H. Biological Shape and Visual Science. J. Theor. Biol. 1973. vol. 38. pp. 205–287.
2. Zhang Y, Sang L, Grzegorzek M, See J, Yang C. BlumNet: Graph component detection for object skeleton extraction. Proceedings of the 30th ACM International Conference on Multimedia. 2022. pp. 5527–5536.
3. Sanchez-Salvador J.L., Campano C., Lopez-Exposito P., Tarrés Q., Mutjé P., Delgado-Aguilar M., Monte M.C. Blanco A. Enhanced morphological characterization of cellulose nano/microfibers through image skeleton analysis. Nanomaterials. 2021. vol. 11. no. 8. DOI: 10.3390/nano11082077.
4. Zhang F., Chen X., Zhang X. Parallel thinning and skeletonization algorithm based on cellular automaton. Multimedia Tools and Applications. 2020. vol. 79. pp. 33215–33232.
5. Kotsur D., Tereshchenko V. An optimized algorithm for computing the Voronoi skeleton. International Journal of Computing. 2020. vol. 19. no. 4. pp. 542–554.
6. Wang Y., Xu Y., Tsogkas S., Bai X., Dickinson S, Siddiqi K. Deepflux for skeletons in the wild. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2019. pp. 5287–5296.

7. Cha S.H. Comprehensive survey on distance/similarity measures be-tween probability density functions. International Journal of Mathe-matical Models and Methods in Applied Sciences. 2007. vol. 1(4). pp. 300–307.
8. Yatziv L., Bartesaghi A., Sapiro G. O(N) implementation of the fast marching algorithm. Journal of computational physics. 2006. vol. 212. no. 2. pp. 393–399.
9. Wang H., Yu Y., Yuan Q. Application of Dijkstra algorithm in robot path-planning. Second international conference on mechanic automation and control engineering. 2011. pp. 1067–1069.
10. Gonzalez R.C., Woods R.E. Digital Image Processing, 3rd edition. Pearson Education, 2010. 185 p.
11. Song C., Pang Z., Jing X., Xiao C. Distance field guided L1-median skeleton extraction. The Visual Computer. 2018. vol. 34. pp. 243–55.
12. Langer M., Gabdulkhakova A., Kropatsch W.G. Non-centered Voronoi skeletons. Discrete Geometry for Computer Imagery: 21st IAPR International Conference. 2019. pp. 355–366.
13. Boudaoud L.B., Solaiman B., Tari A. A modified ZS thinning algorithm by a hybrid approach. The Visual Computer. 2018. vol. 34. pp. 689–706.
14. Morbiducci U., Mazzi V., Domanin M., De Nisco G., Vergara C., Steinman D.A., Gallo D. Wall shear stress topological skeleton independently predicts long-term restenosis after carotid bifurcation endarterectomy. Annals of biomedical engineering. 2020. vol. 48. pp. 2936–2949.
15. Breuß M., Bruckstein A.M., Kiselman C.O., Maragos P. Shape Analysis: Euclidean, Discrete and Algebraic Geometric Methods. Dagstuhl Reports. 2018. vol. 8. no. 10. pp. 87–103.
16. Zhang W., Wang X., Li X., Chen J. 3D skeletonization feature based computer-aided detection system for pulmonary nodules in CT datasets. Computers in biology and medicine. 2018. vol. 92. pp. 64–72.
17. Malik N.U., Sheikh U.U., Abu-Bakar S.A., Channa A. Multi-View Human Action Recognition Using Skeleton Based-FineKNN with Extraneous Frame Scrapping Technique. Sensors. 2023. vol. 23. no. 5. DOI: 10.3390/s23052745.
18. Ma J., Ren X., Li H., Li W., Tsviatkou V.Y., Boriskevich A.A. Noise-Against Skeleton Extraction Framework and Application on Hand Gesture Recognition. IEEE Access. 2023. vol. 11. pp. 9547–9559.
19. Bataineh B., Alqudah M.K. Evaluation of Skeletonization Methods for Document Images with Rotation States. Amity International Conference on Artificial Intelligence. 2019. pp. 424–428. DOI: 10.1109/AICAI.2019.8701352.
20. Nazarkevych M., Dmytruk S., Hrytsyk V., Vozna O., Kuza A., Shevchuk O., Voznyi Y., Maslanych I., Sheketa V. Evaluation of the effectiveness of different image skeletonization methods in biometric security systems. International Journal of Sensors Wireless Communications and Control. 2021. vol. 11. no. 5. pp. 542–552.
21. Perumalla S.R., Alekhya B., Raju M.C. Digital Skeletonization for Bio-Medical Images. Proceedings of Third International Conference on Sustainable Expert Systems. 2023. pp. 277–291.
22. Ramakrishnan V., Schönmehl R., Artinger A., Winter L., Böck H., Schreml S., Gürtler F., Daza J., Schmitt V.H., Mamilos A., Arbelaez P. 3D Visualization, Skeletonization and Branching Analysis of Blood Vessels in Angiogenesis. International Journal of Molecular Sciences. 2023. vol. 24. no. 9. DOI: 10.3390/ijms24097714.
23. Zhu R., Oda M., Hayashi Y., Kitasaka T., Misawa K., Fujiwara M., Mori K. A skeleton context-aware 3D fully convolutional network for abdominal artery segmentation. International Journal of Computer Assisted Radiology and Surgery. 2023. vol. 18. no. 3. pp. 461–472.

24. Feng Y., Chow L.S., Gowdh N.M., Ramli N., Tan L.K., Abdullah S., Tiang S.S. Gradient-based edge detection with skeletonization (GES) segmentation for magnetic resonance optic nerve images. Biomedical Signal Processing and Control. 2023. vol. 1. no. 80. DOI: 10.3390/ijms24097714.
25. Feng M., Meunier J. Skeleton Graph-Neural-Network-Based Human Action Recognition: A Survey. Sensors. 2022. vol. 22. no. 6. DOI: 10.3390/s22062091.
26. Chen D., Zhang T., Zhou P., Yan C., Li C. OFPI: Optical Flow Pose Image for Action Recognition. Mathematics. 2023. vol. 11. no. 6. DOI: 10.3390/math11061451.
27. Xing Y., Dai Y., Hirota K., Jia A. Skeleton-based method for recognizing the campus violence. Proceedings of the 9th International Symposium on Computational Intelligence and Industrial Applications. 2020. pp. 19–20.
28. Cheriet M., Dentamaro V., Hamdan M., Impedovo D., Pirlo G. Multi-Speed Transformer Network for Neurodegenerative disease assessment and activity recognition. Computer Methods and Programs in Biomedicine. 2023. vol. 230(3). DOI: 10.1016/j.cmpb.2023.107344.
29. Alsaif O.I., Hasan S.Q., Maray A.H. Using skeleton model to recognize human gait gender. IAES International Journal of Artificial Intelligence. 2023. vol. 12. no. 2. pp. 974–983. DOI: 10.11591/ijai.v12.i2.pp974-983.
30. Yang W., Zhang J., Cai J., Xu Z. HybridNet: Integrating GCN and CNN for skeleton-based action recognition. Applied Intelligence. 2023. vol. 53. no. 1. pp. 574–585.
31. Xu J., Zhang Y., Zeng Q., Ren X., Cai X., Sun X. A skeleton based model for promoting coherence among sentences in narrative story generation. arXiv preprint arXiv:1808.06945, 2018.
32. Bai X., Ye L., Zhu J., Zhu L., Komura T. Skeleton filter: a self-symmetric filter for skeletonization in noisy text images. IEEE Transactions on Image Processing. 2019. vol. 29. pp. 1815–1826.
33. Faizullah S., Ayub M.S., Hussain S., Khan M.A. A Survey of OCR in Arabic Language: Applications, Techniques, and Challenges. Applied Sciences. 2023. vol. 13. no. 7. DOI: 10.3390/app13074584.
34. Abdo H.A., Abdu A., Manza R.R., Bawiskar S. An approach to analysis of Arabic text documents into text lines, words, and characters. Indonesian Journal of Electrical Engineering and Computer Science. 2022. vol. 26. no. 2. pp. 754–763.
35. Kiamouche O., Bennia A. Segmentation of Handwritten Arabic Words Using High Level Informative Scheme. 2nd International Conference on Advanced Electrical Engineering. 2022. 7 p. DOI: 10.1109/ICAEE53772.2022.9962062.
36. Arcelli C., Sanniti di Baja G., Serino L. Distance-driven skeletonization in voxel images. IEEE Trans. Pattern Anal. Mach. Intell. 2011. vol. 33. no. 4. pp. 709–720.
37. Bitter I., Kaufman A.E., Sato M. Penalized-distance volumetric skeleton algorithm, IEEE Trans. Vis. Comput. Graph. 2001. vol. 7. no. 3. pp. 195–206.
38. Lohou C., Bertrand G. A 3D 12-subiteration thinning algorithm based on P-simple points, Discrete Appl. Math. 2004. vol. 139. no. 1. pp. 171–195.
39. Lohou C., Bertrand G. A 3D 6-subiteration curve thinning algorithm based on P-simple points, Discrete Appl. Math. 2005. vol. 151. no. 1. pp. 198–228.
40. Németh G., Kardos P., Palágyi K., Thinning combined with iteration-by-iteration smoothing for 3D binary images, Graph. Models. 2011. vol. 73. pp. 335–345.
41. Ma J., Ren X., Tsviatkou V.Y., Kanapelka V.K. A novel fully parallel skeletonization algorithm. Pattern Analysis and Applications. 2022. vol. 25. 169–188. DOI: 10.1007/s10044-021-01039-y.
42. Perumalla S.R., Alekhya B., Raju MC. Digital Skeletonization for Bio-Medical Images. Proceedings of Third International Conference on Sustainable Expert Systems: ICSES. 2023. pp. 277–291.

43. Pinyoanuntapong E., Ali A., Wang P., Lee M., Chen C. GaitMixer: skeleton-based gait representation learning via wide-spectrum multi-axial mixer. Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2023. DOI: 10.48550/arXiv.2210.15491.
44. Saha P.K., Borgefors G., di Baja G.S. A survey on skeletonization algorithms and their applications. Pattern recognition letters. 2016. vol. 76. pp. 3–12. DOI: 10.1016/j.patrec.2015.04.006.
45. Gittoes W., Botterill T., Green R. Quantitative analysis of skeletonisation algorithms for modelling of branches. Proceedings of Image and Vision Computing New Zealand. 2011. 6 p.
46. Abudalfa S., Mikki M. K-means algorithm with a novel distance measure. Turkish Journal of Electrical Engineering and Computer Sciences. 2013. vol. 21. no. 6. pp. 1665–1684.

Абудальфа Шади Ибрагим — Ph.D., Dr.Sci., доцент, Университетский колледж прикладных наук. Область научных интересов: искусственный интеллект, интеллектуальный анализ данных, анализ настроений. Число научных публикаций — 25. sabudalfa@ucas.edu.ps; улица Аун Аль-Шава, Тель Аль-Хава, 1415, Газа, Палестина; р.т.: +970(8)262-4999.

УДК 004 **DOI** 10.15622/ia.22.5.8

А.В. Воробьев, А.Н. Лапин, Г.Р. Воробьева

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ АВТОМАТИЗИРОВАННОГО РАСПОЗНАВАНИЯ И ОЦИФРОВКИ АРХИВНЫХ ДАННЫХ ОПТИЧЕСКИХ НАБЛЮДЕНИЙ ПОЛЯРНЫХ СИЯНИЙ

Воробьев А.В., Лапин А.Н., Воробьева Г.Р. **Программное обеспечение для автоматизированного распознавания и оцифровки архивных данных оптических наблюдений полярных сияний.**

Аннотация. Одним из основных инструментов регистрации полярных сияний является оптическое наблюдение небосвода в автоматическом режиме с помощью камер всего неба. Результаты наблюдений фиксируются в специальных мнемонических таблицах, аскаплотах. Аскаплоты предоставляют суточную информацию о наличии или отсутствии облачного покрова и полярных сияний в различных частях небосвода и традиционно используются для исследования суточного распределения полярных сияний в заданном регионе, а также для расчета вероятности их наблюдения в других регионах в соответствии с уровнем геомагнитной активности. Обработка аскаплотов в настоящее время осуществляется вручную, что сопряжено с существенными временными затратами и высокой долей ошибок, возникающих по причине человеческого фактора. Для повышения эффективности обработки аскаплотов авторами предложен подход, обеспечивающий автоматизацию распознавания и оцифровки данных оптических наблюдений полярных сияний. Предложена формализация структуры аскаплота, применяемая для обработки его изображения, а также извлечение соответствующих результатов наблюдений и формирование результирующего набора данных. Подход предусматривает использование алгоритмов машинного зрения (в частности, в данном случае имеет место применение алгоритма классификации по правилам) и применение специализированной маски – отладочного изображения для оцифровки, представляющего собой цветное изображение, в котором задано общее положения ячеек аскаплотов. Предложенный подход и соответствующие алгоритмы реализованы в форме программного обеспечения для распознавания и оцифровки архивных данных оптических наблюдений полярных сияний. Решение представляет собой однопользовательское настольное программное обеспечение, позволяющее пользователю в пакетном режиме выполнять преобразование изображений аскаплотов в таблицы, доступные для последующей обработки и анализа. Результаты проведенных вычислительных экспериментов показали, что применение предложенного программного обеспечения позволит избежать ошибок при оцифровке аскаплотов, с одной стороны, и существенно повысить скорость соответствующих вычислительных операций, с другой. В совокупности это позволит повысить эффективность обработки аскаплотов и проведения исследований в соответствующей области.

Ключевые слова: обработка данных, оцифровка данных наблюдений, аскаплоты, программное обеспечение.

1. Введение. В условиях интенсивного освоения космического пространства и совершенствования систем наземной и космической навигации все большее значение приобретает исследование характеристик полярных сияний. Основанием тому является подтвержденная многими исследованиями взаимосвязь между

характеристиками полярных сияний и различными геофизическими процессами, протекающими в высокоширотной ионосфере Земли и способными негативно повлиять на различные объекты и системы техносферы [1].

В настоящее время основным инструментом оптического наблюдения полярных сияний являются автоматические камеры всего неба (All-Sky Camera), снабженные объективами с полем зрения в 180 [2]. При этом для исследования полярных сияний, зарегистрированных камерами всего неба, необходима первичная обработка проведенных наблюдений, что в значительной степени повышает эффективность соответствующих научных исследований [3].

Для первичной обработки наблюдений камер всего неба используются так называемые аскафильмы (all sky camera films – кадры непрерывной регистрации небосвода камерой всего неба [4]). В результате обработки аскафильмов составляются мнемонические таблицы, называемые аскаплотами (all sky camera plots [4]). В соответствии с предопределенной нотацией аскаплоты предоставляют суточную информацию о наличии или отсутствии облачного покрова и полярных сияний в различных частях небосвода [4, 5].

Результаты обработки аскаплотов используются для исследования суточного распределения полярных сияний в заданном пространственном регионе и для расчета вероятности наблюдения в других регионах в зависимости от уровня локальной геомагнитной активности. При этом обработка полученных из аскафильмов аскаплотов осуществляется преимущественно вручную, что крайне негативно сказывается на оперативности соответствующих исследований. Немаловажно отметить и высокую вероятность ошибок в результатах интерпретации аскаплотов, обусловленную человеческим фактором. Перечисленные недостатки практикуемого в настоящее время подхода [4] существенно снижают эффективность применения результатов анализа аскаплотов для исследования пространственной и временной анизотропии полярных сияний.

В этой связи ожидается, что переход к автоматической обработке аскаплотов позволит существенно повысить эффективность исследований в обозначенной области. Многоэтапная автоматическая проверка промежуточных результатов обработки аскаплотов позволит избежать или существенно сократить число ошибок интерпретации данных, характерных для неавтоматического разбора результатов наблюдений полярных сияний. Кроме того, возможность пакетной

обработки суточных аскаплотов в автоматическом режиме ожидаемо повысит скорость и удобство получения результатов наблюдений в виде, приемлемом для последующего анализа сторонними программными системами и библиотеками.

Таким образом, обработка результатов оптического наблюдения полярных сияний практически невозможна без создания системы автоматической интерпретации аскаплотов. Известные подходы к анализу аскаплотов не предполагают существенной автоматизации, но в то же время предоставляют методический базис для разработки соответствующей информационной системы [5 – 7]. При этом регламентированная отраслевыми спецификациями структура аскаплота позволяет разработать универсальное решение, не привязанное к результатам наблюдений конкретных научных организаций. Создание и внедрение обозначенной системы позволит повысить эффективность научных изысканий с исследовательской точки зрения, а также существенно повысить реактивность сопутствующего программного обеспечения с точки зрения инженерной реализации.

2. Постановка задачи. Для достижения поставленной цели представляется целесообразным решить ряд задач научного и прикладного характера. На первом этапе необходимо формализовать структуру аскаплота таким образом, чтобы полученная в итоге математическая модель могла быть положена в основу соответствующих методов обработки и анализа данных. Далее на имеющихся тестовых данных необходимо разработать алгоритм оцифровки аскаплотов, предусматривающий последовательную обработку данных, а также проверку и корректировку промежуточных результатов. На завершающем этапе предполагается разработка исследовательского прототипа соответствующего программного обеспечения, чему предшествует определение его архитектуры, инфраструктуры и стека используемых технологий с учетом особенностей обрабатываемой информации.

Существующие подходы к оцифровке табличных данных применяют методы интеллектуального анализа [8], такие как графовые нейронные сети [9 – 11], рекуррентные нейронные сети [12 – 14], семантическая сегментация [15] и сверточные нейронные сети [16, 17], что позволяет выделять сложную табличную архитектуру [18], а также корректировать дефекты изображения, вызванные фотокамерой. Для последующей оцифровки символов внутри ячеек таблицы, как правило, применяются методы оптического распознавания символов [19 – 21]. Проведенный авторами анализ показал, что основными

недостатками рассмотренных методов являются высокие требования к используемым вычислительным ресурсам, а также необходимость проведения дополнительных этапов предобработки и постобработки данных.

При этом важно отметить, что в данной статье в качестве входных данных используются аскаплоы, которые имеют табличную структуры и представлены в виде матрицы размером 5 х 48 ячеек. Также стоит отметить, что в отличие от классических табличных данных, которые представлены в виде текстовых символов, в ячейках аскаплота находятся геометрические фигуры, которым свойственны графические неточности, такие как сдвиг относительно центра самой ячейки и выход фигуры за пределы одной ячейки. Немаловажным является и тот факт, что одной рассматриваемых фигур является полностью закрашенный прямоугольник, что накладывает определенные трудности при определении границ столбцов таблицы, поскольку не представляется возможным локально определить раздел между фигурой и границей ячейки.

С учетом сказанного, применение перечисленных и иных подобных им методов оцифровки табличных данных в рассматриваемом случае не представляется авторам возможным. В этой связи представляется целесообразным разработать специализированный алгоритм для оцифровки аскаплотов с применением машинного зрения.

Для формализации и реализации решений поставленных задач предполагается использовать модели и методы распознавания образов, элементы теоретико-множественного базиса для описания структуры аскаплотов, подходы к построению схем алгоритмов, а также технологии обработки и анализа информации.

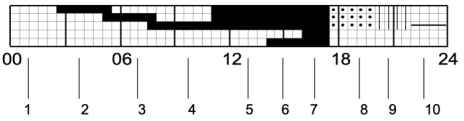
В качестве информационного обеспечения, а также используемой для эмпирических исследований входной информации, в рамках настоящей работы выступают результаты оптических наблюдений полярных сияний, зарегистрированные камерами всего неба на Кольском полуострове, в обсерватории Ловозеро [22 – 24]. Указанные данные оформлены в аскаплоты, которые, в свою очередь, представлены в виде документов формата pdf, содержащих соответствующие таблицы данных, которые построены по спецификациям описания таких данных.

3. Описание и формализация исходных данных. В качестве исходных данных используются результаты оптических наблюдений полярных сияний, зарегистрированные камерами всего неба. При этом важным параметром является так называемый зенит обсерватории,

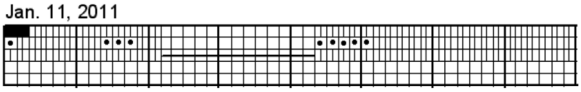
характеризующий направление вертикального подъема над точкой наблюдения [4]. Для корректной записи аскафильмов зенит обсерватории должен располагаться в центре кадра [25]. Исправленный геомагнитный меридиан обсерватории располагается вдоль линии, проходящей в направлении сверху вниз через центр кадра и указывающей на север. Соответственно при этом запад и восток находятся в правой и левой частях кадра соответственно.

Каждый аскаплот описывает результаты суточного наблюдения полярных сияний камерой всего неба. Данные фиксируются в пятистрочной таблице, столбцы которой соответствуют последовательным получасовым временных интервалам (рисунок 1). Первые три строки показывают факт наличия полярного сияния в северной, зенитной и южной частях неба соответственно [5]. Четвертая и пятая строки стандартного пятистрочного аскаплота характеризуют интенсивность полярного сияния в зенитном диапазоне.

Кроме того, непосредственно в таблице аскаплота результаты наблюдений определенным образом маркируются. Специальные обозначения используются, в частности, в пяти различных случаях: при отсутствии сияния, наблюдении сияния, в условиях частичной или сплошной облачности, отсутствия наблюдений и пр. Такая детальная нотация позволяет с высокой степенью информативности описать результаты наблюдения полярных сияний с учетом их видимости и интенсивности в соответствующие периоды времени [4, 5].



а)



б)

Рис. 1. Формат представления данных в виде аскаплота: а) 1 – сияние не наблюдаются; 2 – сияние наблюдается в северной области; 3 – сияние в зените; 4 – сияние на юге; 5 – сияние наблюдается в зените, северной и южной областях; 6 – в зените наблюдаются умеренное сияние, кроме этого свечение присутствует в северной и южной областях; 7 – в зените наблюдается сильное сияние, кроме этого свечение присутствует в северной и южной областях; 8 – частичная облачность; 9 – сплошная облачность; 10 – регистрация не проводилась; б) пример аскаплота ГС LOZ за 11.01.2011 г. [22]

Представляется целесообразным формализованное описание структуры аскаплота в теоретико-множественном базисе. Пусть суточные оптические наблюдения полярных сияний представлены в аскаплоте A, составленном из подмножеств H:

$$A = \bigcup_{i=0}^{47} H_i, \tag{1}$$

где каждому подмножеству H_i соответствует получасовой интервал наблюдений (таким образом, $i = 0,\ldots,47$).

Каждый интервал H_i представляет собой последовательность из 5 значений в соответствии с пятистрочной структурой аскаплота, описанной выше. Каждое из 5 значений характеризует определенный параметр наблюдения в соответствии с наличием и интенсивностью полярного сияния в соответствующем пространственном направлении относительно камеры всего неба. Структуру интервала с учетом сказанного можно представить следующим образом:

$$H_i = \{h_0^i, h_1^i, \ldots, h_4^i\}, \tag{2}$$

где h_j^i – результат оптического наблюдения полярного сияния в H_i-й получасовой интервал, характеризующий значение j-го параметра ($j = 0,\ldots,4$).

Каждый из пяти обозначенных параметров, представленных в интервале аскаплота, может принимать одно из 5 предопределенных значений. При этом непосредственно в исходном аскаплоте соответствующее значение помечается посредством заданной графической нотации (заливка цветом, вертикально или горизонтально перечеркнутая ячейка, пустая ячейка и пр.). Поскольку параметры результатов наблюдений в аскаплоте могут принимать строго определенные значения, представляется целесообразным формализовать их в виде соответствующего домена.

Домен допустимых значений элементов аскаплота может быть описан в виде множества, состоящего из пяти возможных значений:

$$D = \bigcup_{j=0}^{4} d_j, \tag{3}$$

где d_j – атомарное значение, доступное для использования при описании результатов наблюдений полярных сияний.

Каждому элементу аскаплота ставится в соответствие один и только один элемент из домена D. При этом количество элементов с одинаковыми значениями в составе одного аскаплота не ограничено, равно как и не требуется наличия каждого из предусмотренных доменом значений:

$$h_j^i = d;\ h_j^i \in H_i, d\ \in D, \tag{4}$$

где d – значение j-го параметра i-го элемента аскаплота H.

Кроме того, представляется целесообразным отметить, что в составе аскаплота не допускаются параметры с отсутствующими значениями. В этой связи во избежание возможных коллизий в аскаплоте используются значения по умолчанию из имеющегося домена, выбор которого определяется разработчиками:

$$h_j^i = d;\ h_j^i \in H_i, d\ \in D, d \neq \emptyset, \tag{5}$$

где d – значение j-го параметра i-го элемента аскаплота H.

Важно отметить, что в одном наборе результатов оптических наблюдений за заданный временной интервал могут присутствовать как уникальные, так и повторяющиеся аскаплоты, что, в свою очередь, свидетельствует о вариациях соответствующих анализируемых параметров. При этом возможны ситуации, при которых в течение заданного временного периода в наборе данных присутствуют такие аскаплоты, которые содержат как все доступные в домене значения, так и их подмножества. Последний вариант развития событий является наиболее часто встречаемым в реальных наблюдениях полярных сияний.

Кроме того, ввиду различных факторов техногенного и естественного происхождения в течение определенного аскаплотом периода (одного или нескольких получасовых, либо полного суточного временного интервала) оптические наблюдения полярных сияний могут отсутствовать. Соответствующие аскаплоты помечаются предусмотренной нотацией, характеризующей отсутствие наблюдений, а также частичную или полную облачность в анализируемые периоды времени.

Рассмотрим далее изображение страницы аскаплота как монохромное изображение, описываемое в формате $I(x, y)$, где x, y – координаты пикселя. При этом изображения аскаплота и

маски могут быть рассмотрены как множество пикселей с координатами x, y и значениями (R, G, B) для цветного изображения.

Тогда пусть изображение маски представляет собой цветное отмасштабированное изображение $I_{mask}(x, y)$ с красным, зеленым и синим каналами (RGB). Маска имеет размер M x N, где M и N – количество столбцов и строк изображения соответственно.

С учетом сказанного множество пикселей, относящихся ячейкам табличного представления аскаплота, может быть представлено как множество C вида:

$$c_j^i = \{I(x + \Delta x, y + \Delta y) | I_{mask}(x, y) = (50j, 5i, 0)\},$$

$$c_j^i \in C, C \to H, c_j^i \neq \emptyset, \quad (6)$$

где $\Delta x, \Delta y$ – смещение маски относительно начала координат изображения аскаплота; c_j^i – подмножество пикселей монохромного изображения страницы аскаплота, которые соответствуют ячейке в i-м столбце и j-й строке; C – множество пикселей, относящихся ячейкам табличного представления аскаплота; $I(x + \Delta x, y + \Delta y)$ – множество пикселей монохромного изображения страницы аскаплота с учетом смещения маски; $I_{mask}(x, y)$ – изображение маски; x, y – координаты, изменяемые от 0 до M и N соответственно.

Смещение $\Delta x, \Delta y$ определяется на предварительном этапе оцифровки. Также на этом этапе определяется и масштабирование маски так, чтобы ее края соответствовали краям изображения аскаплота. Поэтому значения M и N не будут постоянными и будут изменяться в зависимости от аскаплота.

При этом условие проверки принадлежности пикселя маски к конкретному цвету ячейки таблицы может быть сформулировано как:

$$R_j^i = (50j, 5i, 0), \quad (7)$$

где R_j^i – уникальный для каждой ячейки цвет, который можно идентифицировать по индексу строки j = 0,…,4 и столбца i = 0,…,47.

Еще одной важной особенностью рассматриваемого подхода к представлению результатов наблюдений является как совместное применение нескольких аскаплотов, характеризующее данные за несколько суток, так и фрагментарное использование тех же данных, относящееся к исследованию соответствующих характеристик полярного сияния в течение одного или нескольких получасовых

интервалов. Комбинирование перечисленных подходов позволяет достаточно гибко формировать наборы обрабатываемых данных за различные периоды времени для последующего анализа.

4. Характеристика решения. Для повышения эффективности обработки и анализа аскаплотов авторами было предложено программное средство, автоматизирующее указанные информационные процессы. Предусловием автоматизированной обработки является размещение pdf-документов или png-изображения с анализируемыми аскаплотами в одной директории, именованной последовательностью латинских символов.

При этом при первом запуске разработанного приложения пользователю необходимо напрямую указать целевую директорию с соответствующими аскаплотами. Кроме того, для упрощения понимания пользователем рекомендуется соблюдать предусмотренную разработчиками схему именования файлов с аскаплотами, предполагающую следующий формат:

$$A = YYYY\text{-}MM\_DD.[pdf \mid png], \quad (8)$$

где A – имя документа, YYYY – четырехсимвольное обозначение года, MM – двухсимвольное обозначение порядкового номера месяца, DD – двухсимвольное обозначение порядкового номера дня в соответствующем месяце.

На основании параметров расположения указанной пользователем директории с аскаплотами приложение начинает их последовательную загрузку и обработку. При этом для повышения реактивности разработанного программного обеспечения выполняется распараллеливание выполнения соответствующих вычислительных процессов в соответствии с вычислительными мощностями пользовательского компьютера.

При работе с предложенным приложением пользователь может дополнительно верифицировать промежуточные результаты, получаемые на различных этапах обработки рассматриваемых данных. Так, к примеру, одна из таких пользовательских проверок доступна после загрузки и первичной обработки файлов аскаплотов, что позволяет еще на ранних этапах при необходимости скорректировать действия используемого программного обеспечения.

Предложенное приложение по обработке аскаплотов также выполняет предварительную проверку значений анализируемого временного интервала, автоматически удаляя некорректные даты и исправляя имеющиеся последовательности значений. Это также

позволяет избежать некорректной интерпретации аскаплотов, что, в свою очередь, может негативно сказаться на результатах анализа соответствующих оптических наблюдений полярных сияний. При этом важно отметить, что некорректные даты появляются в результате ошибок работы оптического распознавания текста, а также ошибок записи строкового представления даты в исходных данных.

Результатом работы приложения является один или несколько (в зависимости от заданных конечным пользователем настроек) документов в csv-подобном формате. Такое представление результатов обработки позволяет продолжить анализ соответствующими инструментально-программными средствами, либо посредством специализированных программных библиотек в составе сторонних информационных систем. Кроме того, для первичного просмотра и анализа полученных в ходе работы приложения результатов конечному пользователю достаточно использовать стандартные офисные пакеты для работы с электронными таблицами, что также, в свою очередь, призвано повысить доступность соответствующих данных.

5. Архитектура решения. Предлагаемое решение на программном уровне предполагает декомпозицию на четыре взаимосвязанных модуля:

1) Оцифровка датасета.
2) Первичное восстановление дат.
3) Проверка последовательности дат.
4) Совмещение первичного датасета и восстановленного списка дат.

Модуль оцифровки датасета предусматривает обработку (в том числе параллельную) N страниц, где N – натуральное число, максимальное количество ядер процессора на компьютере или заданное пользователем значение. В ходе выполнения модуля из исходных данных (файлов для оцифровки) создается первичный датасет, используемый последующими программными модулями.

Первичный датасет представляет собой таблицу со следующими столбцами:

– date – оцифрованное изображение даты в строковом формате “DD.MM.YYYY”. Если произошла ошибка оцифровки даты, то значение применяется равным «NaT».

– time – время съемки.

– add_data – путь к изображению, на котором присутствует данный аскаплот.

– North, Zenith, South, medium, strong – оцифрованные ячейки аскаплота.

Для группировки аскаплотов по датам из первичного датасета удаляется столбец с временем и оставляется каждая 48-я строка. Приложение проверяет и исправляет пропуски, которые стоят внутри линейной последовательности дат с шагом в 1 день.

Модуль первичного восстановления дат предполагает создание списка дат из первичного датасета, а также восстановление очевидных последовательностей. При этом на начальном этапе предусмотрена замена NaT значений вручную.

Модуль проверки последовательности дат отвечает за вывод на экран дат, нарушающих последовательность, а также их замену в случае необходимости. Например, в данной последовательности дат (19, 20, 21, NaT, 23, 24, 25, 26), «NaT» является очевидным пропуском и его можно заменить на 22, чтобы восстановить последовательность. В целом пользователь проверяет полученный набор дат и исправляет значения «NaT».

Модуль совмещения первичного датасета и восстановленного списка дат предусматривает сохранение финального датасета в формате csv.

В общем виде соответствующая диаграмма компонентов может быть представлена так, как показано на рисунке 2.

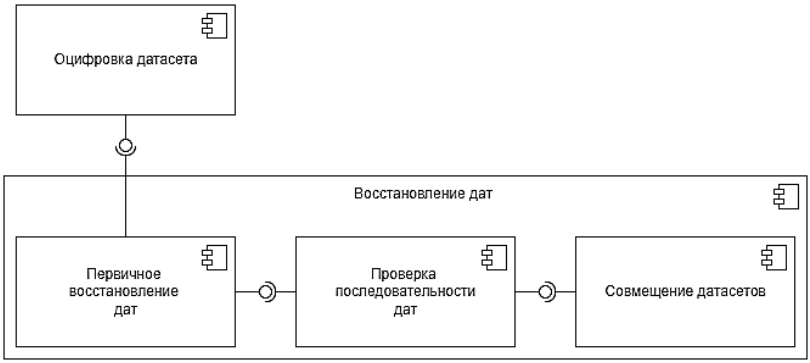


Рис. 2. Диаграмма компонентов разработанной системы

Высокая сложность пользовательского сценария связана с нетривиальностью задачи и необходимостью вносить пользовательские правки на разных стадиях работы приложения. На тестовом датасете аскаплотов пользователю вручную необходимо

проверить и/или исправить 5 значений, что составляет 0.004% от количества строк конечного датасета.

6. Алгоритм решения. В общем виде алгоритм предложенного решения декомпозируется на несколько последовательных процессов (рисунок 3). Каждый из процессов представляет собой этап оцифровки аскаплотов и верификации полученных результатов. По завершению каждого из перечисленных процессов конечному пользователю доступны для проверки и корректировки (в случае необходимости) соответствующие промежуточные результаты. При этом по выбору пользователя соответствующие действия могут быть проигнорированы.

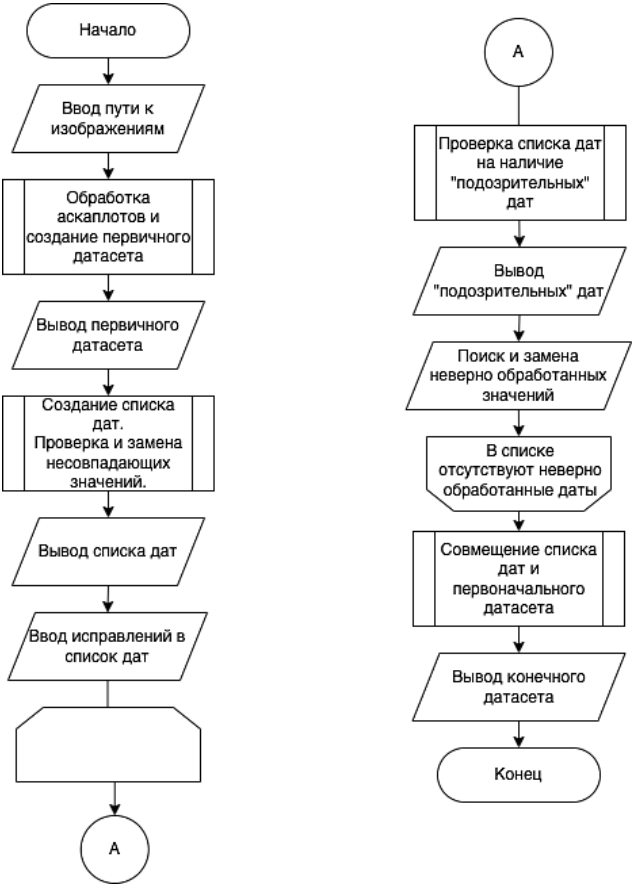


Рис. 3. Обобщенная схема алгоритма, реализующего предлагаемый подход

На первом этапе выполнения алгоритма осуществляется загрузка и обработка исходных данных на основании параметров физического расположения директории, содержащей оцифровываемые аскаплоты (рисунок 4). Пользователь вручную или посредством соответствующих интерфейсных элементов управления выбирает искомую директорию, абсолютный путь к которой фиксируется в соответствующей переменной для последующего применения по мере выполнения обозначенного алгоритма.

На втором этапе выполняется непосредственно обработка аскаплотов и формирование первичного датасета с полученными при этом промежуточными результатами выполнения алгоритма. Схема соответствующего алгоритма представлена на рисунке 4.

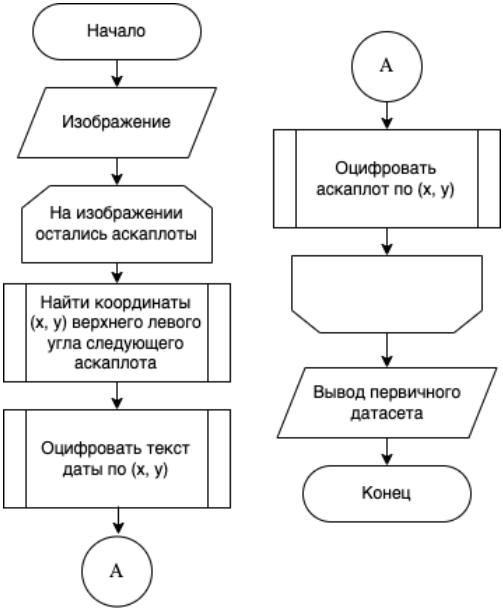


Рис. 4. Схема алгоритма формирования первичного датасета

Первичный датасет представляет собой структурированную таблицу, содержащую временную метку и соответствующее ей значение, извлеченное из аскаплота. Сформированный датасет выводится для обзора конечным пользователем. При этом основной акцент делается на проверку сформированных в ходе выполнения алгоритма временных меток. Алгоритм предусматривает автоматический поиск и замену несовпадающих значений. При этом

непосредственно конечный пользователь может также внести соответствующие исправления вручную.

Далее пользователю демонстрируются даты, разделенные не характерным для датасета промежутком времени. Так, к примеру, если за данными, зарегистрированными 26 февраля, следуют результаты оптических наблюдений за 1 марта, соответствующая информация становится доступна пользователю. В интерфейсе приложения соответствующие потенциально некорректные временные метки помечаются дополнительно отличными от основного цветом и начертанием используемого шрифта. Кроме того, формируется соответствующее сообщение по типу записи в журнале ошибок [26].

Дальнейшие действия полностью определяются конечным пользователем. В случае, если нарушение периодичности в последовательности временных меток соответствует действительности (к примеру, соответствующих аскаплотов нет в распоряжении пользователя или по каким-то иным причинам), то выявленное несоответствие не считается ошибкой и игнорируется. В противном случае пользователь исправляет выделенную последовательность и запускает процедуру выполнения соответствующих этапов алгоритма заново.

По завершении проверки и корректировки выводимых в ходе выполнения алгоритма последовательностей дат соответствующая процедура запускается повторно. Пользователю снова демонстрируются соответствующие выделенные из заданных для обработки аскаплотов списки дат, содержащие, возможно, только те несоответствия в последовательности, которые были одобрены пользователем и помечены как корректные.

На следующем этапе алгоритм предусматривает сопоставление первичного датасета, сформированного на начальных этапах, и восстановленного списка дат из предшествующего этапа выполнения алгоритма. Полученный в результате выполнения обозначенного этапа окончательный датасет передается конечному пользователю в csv-формате для последующей обработки, анализа и визуализации, в том числе сторонними программными системами и библиотеками.

Важный момент касательно предусмотренного в алгоритме предопределенного подпроцесса оцифровки аскаплотов сопряжен с применением специализированной маски поиска значимых данных в файлах аскаплотов, имеющих характерную и описанную соответствующими профильными спецификациями структуру. Анализ спецификаций, а также результаты проведенных вычислительных экспериментов показали, что данные для оцифровки в файле аскаплота

представлены в сегменте шириной 420 и длиной 75 пикселей соответственно (само изображение маски составляет 1668x183 пикселей). При этом весь документ и каждая его составляющая для оцифровки сопровождается координатной системой с параметрами x и y соответственно.

Представляется целесообразным отметить ряд важных для оцифровки параметров. На начальном этапе задается так называемый параметр x_0 – смещение (отступ поиска) по оси x, значение которого было получено экспериментально и составило 1900 пикселей. По сути, данный параметр ограничивает виртуальную линию поиска аскаплотов в анализируемом документе, на протяжении которой не встречается название страницы, номер страницы и время замера.

Кроме того, на предварительном этапе оцифровки алгоритм предусматривает поиск границ рассматриваемой области обрабатываемого документа / изображения на предмет определения верхнего левого угла аскаплота. Проведенные вычислительные эксперименты показали, что для анализируемых данных (для изображения размером 2480x3507 пикселей) соответствующие параметры составляют (x, y) = (350, 200) и (x, y) = (350 <= x <= 700, 200 <= y <= 3307) соответственно.

После обнаружения искомого верхнего левого угла начинается непосредственно оцифровка аскаплота. Создается двумерный массив для обработки каждой ячейки и считывания ее значения. Попиксельно анализируется содержимое ячейки аскаплота и в соответствии с заданной на этапе предварительной настройки алгоритма маски определяется положение соответствующего пикселя. Для этого последовательно анализируется каждый из трех цветовых каналов, и в совокупности эти значения позволяют определить цвет и его интенсивность в соответствующей ячейке.

При этом во избежание коллизий отдельно рассматриваются несколько случаев расположения анализируемого пикселя относительно ячейки аскаплота в целом:

– пиксель граничит с верхней стороной ячейки;
– пиксель граничит с правой стороной ячейки;
– пиксель граничит с левой стороной ячейки;
– пиксель граничит с нижней стороной ячейки;
– пиксель не граничит ни с одной из сторон ячейки.

Принципы классификации каждого символа могут быть сформулированы следующим образом:

– отсутствие символа можно определить по отсутствию черных пикселей в ячейке;

– в случае, если в ячейке все символы закрашены черным, то символ является черным квадратом;

– в случае, если черные пиксели есть только у верхнего и нижнего края ячейки, но их нет у левого и нижнего края, то символом является вертикальная линия;

– в случае, если черные пиксели есть только у левого и правого края ячейки, но их нет у верхнего и нижнего края, то символом является горизонтальная линия;

– в иных случаях символом ячейки считается закрашенная окружность.

В общем виде схема алгоритма оцифровки аскаплота и классификации типа ячеек представлена на рисунке 5.

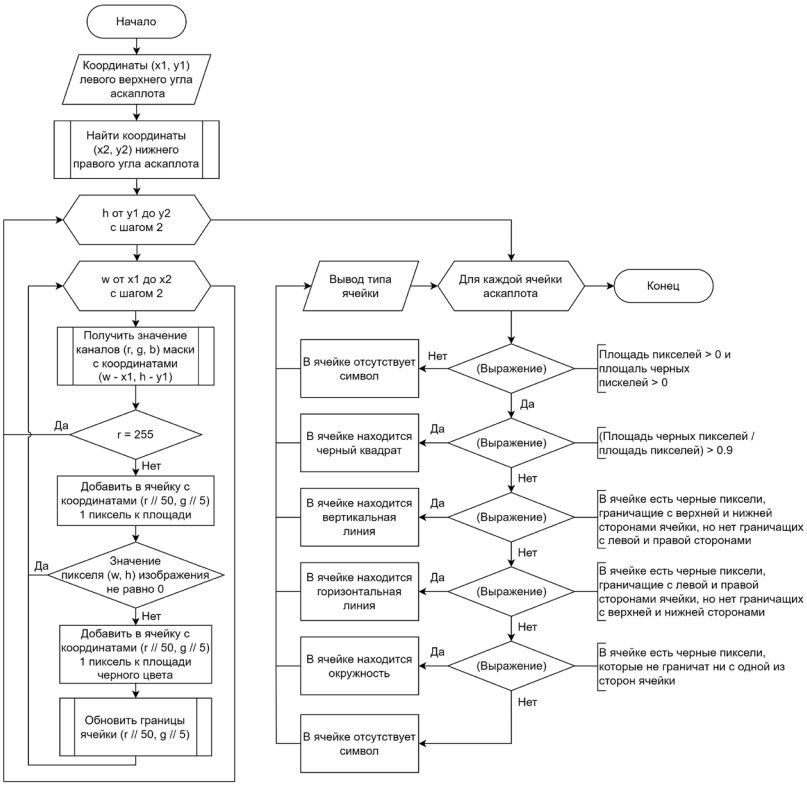


Рис. 5. Схема алгоритма оцифровки аскаплота

Важным этапом оцифровки аскаплотов является маскирование. При этом маска представляет собой цветное изображение в формате png, на котором изображено общее положение ячеек аскаплотов. При этом каждый цветовой канал соответствует определенному компоненту данных о соответствующей маске.

Так, красный канал соответствует индексу строки ячейки аскаплота, который равен результату целочисленного деления значения красного канала на 50. Зеленый канал сопоставлен с индексом столбца ячейки аскаплота, который определяется как результат целочисленного деления значения зеленого канала на 5. И, наконец, синий канал соответствует разделителю столбцов в сетке ячеек аскаплота. Кроме того, отдельно помечается белый пиксель, характеризующий пропуск данной строки в цикле изображения маски.

В общем виде процедуру построения маски можно описать следующим образом. На начальном этапе проводится выборка случайных аскаплотов из общего набора данных. Далее выбранные аскплоты масштабируются таким образом, чтобы их внешние границы совпадали по горизонтали. При этом изображения аскаплотов переводятся в бинарный формат и накладываются друг на друга с применением логического оператора «или». Полученное в результате изображение представляет собой генерализированный образ аскаплотов. Далее найденные общие границы увеличиваются и все изображение переводится обратно в цветной формат. Каждая ячейка маски закрашивается в цвет, соответствующий ее координатам, а остальная часть маски закрашивается в соответствии с вышеописанными правилами.

В общем виде пример отладочного изображения при оцифровке аскаплотов представлен на рисунке 6. Здесь может быть выделено несколько важных для оцифровки составляющих:

1. Непосредственно описание оцифрованной ячейки, состоящее из двух символов. Первый из них характеризует результат наблюдения в соответствии с принятой классификацией (например, 0 – отсутствие сияния, 1 – наблюдение сияния, 2 – полная облачность, 3 – отключенная камера, 4 – частичная облачность и т.д.). Второй символ содержит булево значение (T / F), показывающее, есть ли в анализируемой ячейке данные.

2. Обрабатываемые пиксели закрашены в цвет, который означает соседство с краем рассматриваемой области ячейки. Например, желтый цвет означает соседство пикселя с нижней границей ячейки.

3. Область наложения маски на начальное изображение аскаплота.
4. Отображение времени суток для данного столбца.
5. Обнаруженные границы аскаплота.
6. Области, соответствующие левой верхней и правой нижней границ аскаплота.

Получаемое отладочное изображение тождественно описанной маске.

Здесь представляется целесообразным отметить, что в подавляющем большинстве случаев исходные аскаплоты представляют собой pdf-документы с результатами многодневных оптических наблюдений полярных сияний. Поскольку непосредственно алгоритм оцифровки ориентирован на работу с единичными аскаплотами, предварительная обработка исходных данных может включать в себя извлечение таблиц аскаплотов из страниц наблюдений.

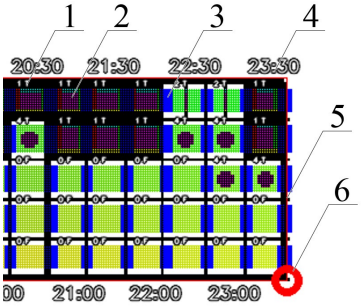


Рис. 6. Пример отладочного изображения для оцифровки аскаплота

При этом непосредственно дата наблюдений, зафиксирована в метаданных соответствующего аскаплота в тексте исходного pdf-документа. Для повышения эффективности работы и во избежание задания этих данных вручную самим пользователем, дата также оцифровывается и ставится в соответствие полученному в ходе работы алгоритма результату.

В ряде случаев возникает необходимость масштабирования маски под оцифровываемые данные. В этом случае алгоритм предусматривает дополнительную обработку и подготовку маски, интерполируя данные на основе метода ближайшего соседа.

7. Стек технологий. Предложенный алгоритм реализован с помощью языка программирования Python [28, 29, 30], при этом

конечный результат представляет собой настольное однопользовательское приложение. Сохранение пользовательских данных между сеансами работы пользователя с приложением не предусмотрено ни задачей, ни соответствующим алгоритмом. По этой причине в архитектуре приложения не предусмотрена база данных, а источником исходных данных выступает пользовательская файловая система.

При выборе языка программирования для реализации предложенных подхода и алгоритма в качестве возможных альтернатив были рассмотрены следующие языки: C++ [31], C# [32], Python [33] и JavaScript [33, 34]. Выбранные альтернативы сравнивались по следующим критериям:

– кроссплатформенность.
– скорость выполнения идентичного кода.
– наличие необходимых для реализации приложения библиотек.
– сложность разработки.
– читаемость кода.

Сравнение выделенных альтернатив было выполнено с использованием метода анализа иерархий [35, 36] по указанным критериям. Результаты проведенной сравнительной оценки показали, что наилучшие характеристики по всем заявленным критериям свойственны языку программирования Python.

8. Описание исследовательского прототипа программного обеспечения. В общем виде разработанное на основе предложенных подхода и алгоритма оцифровки аскаплотов программное обеспечение представляет собой настольное приложение, которое должно быть развернуто и применено с использованием вычислительных мощностей компьютера конечного пользователя.

При этом в зависимости от выбора пользователя предусмотрены два варианта развертывания. Первый из них связан с формированием исполняемого exe-файла, который тем или иным способом передается пользователю. В свою очередь, пользователь, получив указанный исполняемый файл, запускает его на выполнение, получая доступ к искомой функциональности.

Второй вариант сопряжен с передачей пользователю вместе с файлом программы также сопровождающих его интерпретатора Python соответствующей версии с необходимыми для работы приложения библиотеками. Для сохранения зависимостей компонент используется контейнеризация приложения через Docker, что по умолчанию обеспечивает его высокую портируемость. Докеризированная

программа размещается в Docker Hub, откуда любой пользователь может получить к ней доступ.

Следует отметить, что второй из перечисленных вариантов распространения разработанного настольного приложения является предпочтительным для передачи программы конечным пользователям. В первую очередь, это сопряжено с соблюдением требований информационной безопасности. Известно, что исполняемые файлы могут содержать код или выполнять произвольные команды, заложенные злоумышленниками, которые перехватили передаваемый пользователю файл.

Прототип приложения, реализующего предложенный алгоритм, реализован в однооконном формате, предполагающем разделение интерфейсной составляющей на две вертикальные секции. В одной из них (слева) имитируется структура директории с оцифровываемыми аскаплотами: задается непосредственно имя директории в корневом узле иерархии, а соответствующие обрабатываемые файлы представляют собой узлы иерархии в виде имени и расширения каждого файла.

В оставшейся секции пользователь может наблюдать за ходом выполнения процесса оцифровки аскаплотов. Здесь же доступна, в частности, интерактивная составляющая при работе с полученным на этапе предварительной обработки списком дат. Так, к примеру, в случае автоматического обнаружения выделенные некорректные даты могут быть помечены пользователем как корректные.

В интерфейсе приложения предусмотрены и стандартные для оконного приложения элементы управления. В частности, присутствует меню, пункты которого позволяют пользователю открыть диалоговое окно выбора директории для обработки данных, а также аналогичное окно для указания размещения результирующего документа с данными оцифровки. В дальнейшем планируется в элементы управления добавить возможность настройки внешнего вида страницы, вывод на печать и прочие стандартные опции.

При работе с приложением на предварительном этапе пользователь формирует директорию с подлежащими оцифровке аскаплотами. После запуска приложения осуществляется начальная оцифровка исходных данных: определяется тип файла, при необходимости извлекается изображение, которое содержит аскаплоты для обработки. При этом представляется целесообразным отметить, что в существующей версии приложения предполагается централизованное хранение всех оцифровываемых аскаплотов.

В дальнейшем предполагается реализовать поддержку выборочного набора обрабатываемых файлов с аскаплотами.

При запуске последующей процедуры проверки дат из обработанных аскаплотов извлекаются соответствующие параметры. При этом формируемый приложением набор дат автоматически проверяется, а даты, нарушающие последовательность, визуально выделяются в результирующем списке. Пользователь может выбрать действия с выделенными датами, после чего процесс обработки аскаплотов запускается на выполнение с обновленным набором параметров.

Каждый из этапов обработки регистрируется конечным пользователем в режиме реального времени. На завершающем этапе формируется результирующий датасет, который выводится в табличный файл, доступный для последующего просмотра, обработки и анализа сторонними средствами. Для последующих операций и новых итераций оцифровки пользователь указывает целевую директорию и повторяет все перечисленные выше действия.

В перспективе развития предложенного решения планируется расширение приложения на веб-ориентированную архитектуру. Это позволит расширить круг его пользователей, с одной стороны, и снизить требования к их вычислительным мощностям, с другой.

9. Вычислительный эксперимент. Для оценки эффективности предложенного решения был проведен ряд вычислительных экспериментов, в ходе которых осуществлялась оцифровка pdf-документов с аскаплотами. Исходные данные были взяты из документов «PGI Geophysical Data» за период с 2012 по 2020 гг, в котором помимо непосредственно данных оптических наблюдений полярных сияний представлены и другие результаты измерений, в частности наблюдения геомагнитного поля и космических лучей.

Выбранные для оцифровки аскаплоты обрабатывались двумя способами. В первом случае контрольная группа выполняла оцифровку вручную, последовательно перебирая соответствующие документы и формируя строки результирующей таблицы с результатами наблюдений. Во втором случае оцифровка выполнялась одним пользователем с применением разработанного приложения, реализующего предложенные подходы и алгоритмы.

В ходе проведенных вычислительных экспериментов в каждом из обоих случаев были оцифрованы 1 035 аскаплотов за девятилетний период наблюдений. При использовании практикуемого в настоящее время подхода обработки вручную, формирование результирующей таблицы в совокупности заняло 5 100 человеко-минут. При этом

последующий анализ показал, что в ходе оцифровки было допущено более 200 ошибок в 76 аскаплотах (это составляет ~7.34 % от общего числа аскаплотов).

При оцифровке тех же аскаплотов с применением разработанного программного обеспечения скорость обработки одного аскаплота составила в среднем 0,5 с, что в совокупности для всех аскаплотов заняло ~8,6 минуты (технические характеристики вычислительной машины: CPU: Intel Core I7-9700KF, частота на момент замеров составляла 4.57 ГГц). При этом проведенный последующий анализ результатов оцифровки не выявил ошибок обработки результатов оптических наблюдений.

Для ускорения процесса оцифровки с использованием предложенного программного обеспечения было применено распараллеливание на 8 процессов [37], каждый из которых обрабатывал отдельную страницу. Благодаря этому время оцифровки удалось снизить более чем в 5.2 раза (технические характеристики вычислительной машины: CPU: Intel Core I7-9700KF, частота на момент замеров составляла 4.57 ГГц). В результате общее время оцифровки (с учетом вывода отладочных изображений) ~ 1,7 мин.

По данным проведенных вычислительных экспериментов в 1 035 обработанных аскаплотах ошибок оцифровки не обнаружено. По сравнению с ручным методом разработанное программное обеспечение позволило ускорить процесс оцифровки аскаплотов примерно в 3000 раз.

10. Заключение. В настоящее время задача оптического наблюдения полярных сияний успешно решается с применением камер всего неба, которые ведут непрерывную фото- и / или видеорегистрацию небосвода в режиме реального времени. Результаты наблюдений фиксируются в специализированных документах, известных как «аскаплоты». Каждый из аскаплотов в заданной нотации характеризует результаты оптических наблюдений, фиксируя их в пятистрочной таблице, столбцы которой соответствуют последовательным получасовым временным интервалам.

При этом на данный момент времени все аскаплоты обрабатываются вручную. Такой способ регистрации наблюдений используется на всех этапах. На первом из них записываемые камерами аскафильмы переводятся в аскаплоты и далее, на втором этапе, так же вручную строятся таблицы с результатами наблюдений. Соответствующие процессы сопряжены с высокими человеческими и временными затратами, а также существенной долей ошибок, возникающих в ходе обработки результатов наблюдений.

В этой связи в настоящей работе предложен подход, обеспечивающий автоматизацию распознавания и оцифровки данных оптических наблюдений полярных сияний. В рамках обозначенного подхода предложен вариант формализации аскаплота, используемый в дальнейшем для последовательного попиксельного считывания данных регистрации и формирования итоговой таблицы наблюдений в текстовом csv-подобном формате, доступном для последующей обработки, анализа и визуализации сторонними средствами.

Отличительной особенностью предложенного подхода является применение специального вспомогательного изображения для оцифровки, используемого в качестве маски для обработки данных. В общем виде маска представляет собой цветное изображение, в котором заданы общие положения ячеек аскаплотов. Каждый цветовой канал при этом соответствует определенному компоненту данных.

В ходе выполнения исследований был предложен ряд алгоритмов, обеспечивающих процесс оцифровки аскаплотов, с одной стороны, и поддерживающих взаимодействие соответствующего приложения с пользователем, с другой. На каждом этапе выполнения алгоритма пользователю доступны действия, позволяющие скорректировать последующую обработку.

На основе предложенных подхода и алгоритмов было разработано соответствующее настольное программное обеспечение. Проведенные вычислительные эксперименты показали, что применение предложенного программного обеспечения для обработки аскаплотов позволит избежать ошибок при оцифровке. Кроме того, время, затрачиваемое на обработку каждого аскаплота, существенно сокращается и для одного аскаплота составляет в среднем 0,1 с (с учетом распараллеливания выполнения).

В контексте перспективы развития предложенного подхода планируется его перевод на веб-ориентированную платформу с поддержкой многопользовательского режима работы. Это позволит, с одной стороны, расширить круг потенциальных пользователей приложения, и снизит нагрузку на клиентские вычислительные мощности, с другой.

Элементы предложенных решений в настоящее время используются авторами статьи в том числе и для решения задач локальной диагностики наличия полярных сияний [38].

Литература

1. Kozyreva O.V., Pilipenko V.A., Bland E.C., Baddeley L.J., Zakharov V.I. Periodic modulation of the upper ionosphere by ULF waves as observed simultaneously by

SuperDARN radars and GPS/TEC technique // Journal of Geophysical Research: Space Physics. 2020. vol. 125(7). no. e2020JA028032. DOI: 10.1029/2020JA028032.
2. Klimov P., Kozelov B., Roldugin A., Sigaeva K. Joint Recording of Pulsating Auroras on Board the Lomonosov Satellite and by All-Sky Cameras on the Kola Peninsula // Bulletin of the Russian Academy of Sciences: Physics. 2022. vol. 86. no. 3. pp. 300–304. DOI: 10.3103/S106287382203011X.
3. Yang X., Shang Zh., Hu K., Hu Y., Ma B., Wang Y., Wang W. Cloud cover and aurora contamination at dome A in 2017 from KLCAM // Monthly Notices of the Royal Astronomical Society. 2021. vol. 501. no. 3. pp. 3614–3620. DOI: 10.1093/mnras/staa3824.
4. Ягодкина О.И., Воробьев В.Г., Шекунова Е.С. Наблюдения полярных сияний над Кольским полуостровом // Труды Кольского научного центра РАН. 2019. Т. 10. № 8(5). С. 43–55.
5. Nakamura J., Kitamura T., Fukushima S. Auroral ASCAPLOT at Syowa Station in 1959 and 1960 // Antarctic record. 1962. no. 16. pp. 1339–1360.
6. Feldstein Y.I. The discovery and the first studies of the auroral oval: A review // Geomagnetism and Aeronomy. 2016. vol. 56. pp. 129–142. DOI: 10.1134/S0016793216020043.
7. Feldstein Y.I., Vorobjev V.G., Zverev V.L. Planetary features of aurorae: Results of the IGY (a review) // Geomagnetism and Aeronomy. 2010. vol. 50. pp. 413–435. DOI: 10.1134/S0016793210040018.
8. Hashmi K.A., Liwicki M., Stricker D., Afzal M.A., Afzal M.A., Afzal M.Z. Current Status and Performance Analysis of Table Recognition in Document Images With Deep Neural Networks // IEEE Access. 2021. vol. 9. pp. 87663–87685. DOI: 10.1109/ACCESS.2021.3087865.
9. Namysł M., Esser A.M., Behnke S., Kohler J. Flexible Hybrid Table Recognition and Semantic Interpretation System // SN Computer Science. 2023. vol. 4. no. 246. DOI: 10.1007/s42979-022-01659-z.
10. Lee E., Park J., Koo H.I., Cho N.I. Deep-learning and graph-based approach to table structure recognition // Multimedia Tools and Applications. 2022. vol. 81. no. 4. pp. 5827–5848. DOI: 10.1007/s11042-021-11819-7.
11. Li X.H., Yin F., Dai H.S., Liu C.L. Table Structure Recognition and Form Parsing by End-to-End Object Detection and Relation Parsing // Pattern Recognition. 2022. vol. 132. no. 108946. DOI: 10.1016/j.patcog.2022.108946.
12. Sage C., Aussem A., Elghazel H., Eglin V., Espinas J. Recurrent Neural Network Approach for Table Field Extraction in Business Documents // International Conference on Document Analysis and Recognition (ICDAR). 2019. pp. 1308–1313. DOI: 10.1109/ICDAR.2019.00211.
13. Khan S.A., Khalid S.M.D., Shahzad M.A., Shafait F. Table Structure Extraction with Bi-Directional Gated Recurrent Unit Networks // International Conference on Document Analysis and Recognition (ICDAR). 2019. pp. 1366–1371. DOI: 10.1109/ICDAR.2019.00220.
14. Hochreiter S., Schmidhuber J. Long Short-Term Memory // Neural computation. 1997. vol. 9. no. 8. pp. 1735–1780. DOI: 10.1162/neco.1997.9.8.1735.
15. Paliwal S.S., Vishwanath D., Rahul R., Sharma M., Vig L. TableNet: Deep Learning Model for End-to-end Table Detection and Tabular Data Extraction from Scanned Document Images // International Conference on Document Analysis and Recognition (ICDAR). 2019. pp. 128–133. DOI: 10.1109/ICDAR.2019.00029.
16. Tensmeyer C., Morariu V.I., Price B., Cohen S., Martinez T. Deep Splitting and Merging for Table Structure Decomposition // International Conference on Document Analysis and Recognition (ICDAR). 2019. pp. 114–121. DOI: 10.1109/ICDAR.2019.00027.

17. Siddiqui S.A., Fateh I.A., Rizvi S.T.R., Dengel A., Ahmed S. DeepTabStR: Deep Learning based Table Structure Recognition // International Conference on Document Analysis and Recognition (ICDAR). 2019. pp. 1403–1409. DOI: 10.1109/ICDAR.2019.00226.
18. Couasnon B., Lemaitre A. Recognition of Tables and Forms // Handbook of Document Image Processing and Recognition. Chapter Recognition of Tables and Forms. 2014. pp. 647–677. DOI: 10.1007/978-0-85729-859-1_20.
19. Zucker A., Belkada Y., Vu H., Nguyen V.N. ClusTi: Clustering Method for Table Structure Recognition in Scanned Images // Mobile Networks and Applications. 2021. vol. 26. no. 4. pp. 1765–1776. DOI: 10.1007/s11036-021-01759-9.
20. Nguyen Q.D., Le D.A., Phan N.M., Zelinka I. OCR error correction using correction patterns and self-organizing migrating algorithm // Pattern Analysis and Applications. 2021. vol. 24. pp. 701–721. DOI: 10.1007/s10044-020-00936-y.
21. Patel C., Patel A., Patel D. Optical Character Recognition by Open source OCR Tool Tesseract: A Case Study // International Journal of Computer Applications. 2014. vol. 55(10). pp. 50–56. DOI: 10.5120/8794-2784.
22. Vorobjev V. PGI Geophysical data. 2015. October, November, December. Murmansk, Apatity: PGI KSC RAS, 2016.
23. Vorobjev V.G., Roldugin V.C., Yagodkina O.I. Large Amplitude Undulations of Evening Site Diffuse Aurorae. Optical Characteristics and Conditions of Generation // Geomagnetism and Aeronomy. 2015. vol. 55. pp. 45–50. DOI: 10.1134/S0016793215010132.
24. Vorobjev V.G., Yagodkina O.I., Antonova E.E. Ion Pressure in Different Regions of the Dayside Auroral Precipitation // Geomagnetism and Aeronomy. 2020. no. 60. pp. 727–736. DOI: 10.1134/S0016793220060146.
25. Popov L.N., Krakovetskiy Yu.K., Gokhberg M.B., Pilipenko V.A. Terrogenic effects in the ionosphere: a review // Physics of the Earth and Planetary Interiors. 1989. vol. 57. no. 1-2. pp. 115–128.
26. Zhang T., Qiu H., Castellano G., Rifai M., Chen C.S., Pianese F. System Log Parsing: A Survey // IEEE Transactions on Knowledge and Data Engineering. 2023. pp. 8596–8614. DOI: 10.1109/TKDE.2022.3222417.
27. Patil O., Chavan U. Rule Based Expert System for Error Log Analysis // International Journal of Innovative Technology and Exploring Engineering. 2020. vol. 9. no. 10. pp. 188–192. DOI: 10.35940/ijitee.J7466.0891020.
28. Peta S. Python- An Appetite for the Software Industry // International Journal of Programming Languages and Applications (IJPLA). 2022. vol. 12. DOI: 10.5121/ijpla.2022.12401.
29. Singh B.P. Python and Its Future Scope // International Journal of Advanced Research in Science, Communication and Technology. 2022. pp. 400–403. DOI: 10.48175/IJARSCT-4829.
30. Dr U., Patkar U. Python for web development // International Journal of Computer Science and Mobile Computing. 2022. vol. 11. no. 4. pp. 36–48. DOI: 10.47760/ijcsmc.2022.v11i04.006.
31. Rong W., Xu T., Sun, Z., Sun, Z., Ouyang, Y., Xiong, Z. An Object Tuple Model for Understanding Pointer and Array in C Language // IEEE Transactions on Education. 2023. pp. 1–12. DOI: 10.1109/TE.2023.3236027.
32. Peta S. C Programming Language–Still Ruling the World // Global Journal of Computer Science and Technology. 2022. vol. 22(1). pp. 9–13.
33. Park H., Kim S., Bae B. Dynamic code compression for JavaScript engine // Software: Practice and Experience. 2023. vol. 53. no. 5. pp. 1196–1217. DOI: 10.1002/spe.3186.

34. Wang Z., Bu D., Wang N., Yu S., Gou S., Sun A. An empirical study on bugs in JavaScript engines // Information and Software Technology. 2023. vol. 155. no. 107105. DOI: 10.1016/j.infsof.2022.107105.
35. Romanchuk V.M. The Problem of Adequacy of the Analytic Hierarchy Process // Modelling and Data Analysis. 2022. vol. 10. no. 4. pp. 79–87. DOI: 10.17759/mda.2020100407.
36. Polat T.K. An Application of Analytic Hierarchy Process and Fuzzy Analytic Hierarchy Process to the Case Type Selection Problem // Academic Perspective Procedia. 2018. vol. 1. no. 1. pp. 1179–1188. DOI: 10.33793/acperpro.01.01.188.
37. Vorobev A.V., Pilipenko V.A., Enikeev T.A., Vorobeva G.R. Geoinformation system for analyzing the dynamics of extreme geomagnetic disturbances from observations of ground stations // Computer Optics. 2020. vol. 44(5). pp. 782–790. DOI: 10.18287/2412-6179-CO-707.
38. Vorobev A.V., Soloviev A.A., Pilipenko V.A., Vorobeva G.R., Gainetdinova A.A., Lapin A.N., Belakhovsky V.B., Roldugin A.V. Local diagnostics of aurora presence based on intelligent analysis of geomagnetic data // Solar-Terrestrial Physics. 2023. vol. 9(2). pp. 22–30. DOI: 10.12737/stp-92202303.

Воробьев Андрей Владимирович — д-р техн. наук, профессор, кафедра геоинформационных систем факультета информатики и робототехники, Уфимский университет науки и технологий; старший научный сотрудник, Геофизический центр РАН. Область научных интересов: геоинформационные технологии, цифровая обработка сигналов. Число научных публикаций — 164. geomagnet@list.ru; улица Карла Маркса, 12, 450007, Уфа, Россия; р.т.: +7(917)345-2299.

Лапин Александр Николаевич — студент, кафедра геоинформационных систем факультета информатики и робототехники, Уфимский университет науки и технологий. Область научных интересов: математическое и компьютерное моделирование, цифровые двойники, машинное обучение. Число научных публикаций — 13. meccos160@yandex.ru; улица Карла Маркса, 12, 450008, Уфа, Россия; р.т.: +7(917)439-6040.

Воробьева Гульнара Равилевна — д-р техн. наук, профессор, кафедра вычислительной математики и кибернетики факультета информатики и робототехники, Уфимский университет науки и технологий. Область научных интересов: геоинформационные и веб-технологии, системы хранения и обработки информации. Число научных публикаций — 153. gulnara.vorobeva@gmail.com; улица Карла Маркса, 12, 450008, Уфа, Россия; р.т.: +7(917)417-4111.

Поддержка исследований. Исследование выполнено при финансовой поддержке РНФ, проект № 21-77-30010.

DOI 10.15622/ia.22.5.8

A. VOROBEV, A. LAPIN, G. VOROBEVA

SOFTWARE FOR AUTOMATED RECOGNITION AND DIGITIZATION OF ARCHIVE DATA OF AURORA OPTICAL OBSERVATIONS

Vorobev A., Lapin A., Vorobeva G. **Software for Automated Recognition and Digitization of Archive Data of Aurora Optical Observations.**

Abstract. One of the main tools for recording auroras is the optical observation of the sky in automatic mode using all-sky cameras. The results of observations are recorded in special mnemonic tables, ascaplots. Ascaplots provide daily information on the presence or absence of cloud cover and auroras in various parts of the sky and are traditionally used to study the daily distribution of auroras in a given spatial region, as well as to calculate the probability of their observation in other regions in accordance with the level of geomagnetic activity. At the same time, the processing of ascaplots is currently carried out manually, which is associated with significant time costs and a high proportion of errors due to the human factor. To increase the efficiency of ascaplot processing, we propose an approach that automates the recognition and digitization of data from optical observations of auroras. A formalization of the ascaplot structure is proposed, which is used to process the ascaplot image, extract the corresponding observation results, and form the resulting data set. The approach involves the use of machine vision algorithms and the use of a specialized mask - a debug image for digitization, which is a color image in which the general position of the ascaplot cells is specified. The proposed approach and the corresponding algorithms are implemented in the form of software that provides recognition and digitization of archival data from optical observations of auroras. The solution is a single-user desktop software that allows the user to convert ascaplot images into tables in batch mode, available for further processing and analysis. The results of the computational experiments have shown that the use of the proposed software will make it possible to avoid errors in the digitization of ascaplots, on the one hand, and significantly increase the speed of the corresponding computational operations, on the other. Taken together, this will improve the efficiency of processing ascaplots and conducting research in the relevant area.

Keywords: data processing, digitization of observational data, ascaplots, software.

References

1. Kozyreva O.V., Pilipenko V.A., Bland E.C., Baddeley L.J., Zakharov V.I. Periodic modulation of the upper ionosphere by ULF waves as observed simultaneously by SuperDARN radars and GPS/TEC technique. Journal of Geophysical Research: Space Physics. 2020. vol. 125(7). no. e2020JA028032. DOI: 10.1029/2020JA028032.
2. Klimov P., Kozelov B., Roldugin A., Sigaeva K. Joint Recording of Pulsating Auroras on Board the Lomonosov Satellite and by All-Sky Cameras on the Kola Peninsula. Bulletin of the Russian Academy of Sciences: Physics. 2022. vol. 86. no. 3. pp. 300–304. DOI: 10.3103/S106287382203011X.
3. Yang X., Shang Zh., Hu K., Hu Y., Ma B., Wang Y., Wang W. Cloud cover and aurora contamination at dome A in 2017 from KLCAM. Monthly Notices of the Royal Astronomical Society. 2021. vol. 501. no. 3. pp. 3614–3620. DOI: 10.1093/mnras/staa3824.
4. Yagodkina O.I., Vorobyov V.G., Shekunova E.S. [Observations of auroras over the Kola Peninsula]. Proceedings of the Kola Scientific Center of the Russian Academy of

Sciences – Trudy Kol'skogo nauchnogo tsentra RAN. 2019. vol. 10. no. 8(5). pp. 43–55. (in Russ.).
5. Nakamura J., Kitamura T., Fukushima S. Auroral ASCAPLOT at Syowa Station in 1959 and 1960 // Antarctic record. 1962. no. 16. pp. 1339–1360.
6. Feldstein Y.I. The discovery and the first studies of the auroral oval: A review. Geomagnetism and Aeronomy. 2016. vol. 56. pp. 129–142. DOI: 10.1134/S0016793216020043.
7. Feldstein Y.I., Vorobjev V.G., Zverev V.L. Planetary features of aurorae: Results of the IGY (a review). Geomagnetism and Aeronomy. 2010. vol. 50. pp. 413–435. DOI: 10.1134/S0016793210040018.
8. Hashmi K.A., Liwicki M., Stricker D., Afzal M.A., Afzal M.A., Afzal M.Z. Current Status and Performance Analysis of Table Recognition in Document Images With Deep Neural Networks. IEEE Access. 2021. vol. 9. pp. 87663–87685. DOI: 10.1109/ACCESS.2021.3087865.
9. Namysł M., Esser A.M., Behnke S., Kohler J. Flexible Hybrid Table Recognition and Semantic Interpretation System. SN Computer Science. 2023. vol. 4. no. 246. DOI: 10.1007/s42979-022-01659-z.
10. Lee E., Park J., Koo H.I., Cho N.I. Deep-learning and graph-based approach to table structure recognition. Multimedia Tools and Applications. 2022. vol. 81. no. 4. pp. 5827–5848. DOI: 10.1007/s11042-021-11819-7.
11. Li X.H., Yin F., Dai H.S., Liu C.L. Table Structure Recognition and Form Parsing by End-to-End Object Detection and Relation Parsing. Pattern Recognition. 2022. vol. 132. no. 108946. DOI: 10.1016/j.patcog.2022.108946.
12. Sage C., Aussem A., Elghazel H., Eglin V., Espinas J. Recurrent Neural Network Approach for Table Field Extraction in Business Documents. International Conference on Document Analysis and Recognition (ICDAR). 2019. pp. 1308–1313. DOI: 10.1109/ICDAR.2019.00211.
13. Khan S.A., Khalid S.M.D., Shahzad M.A., Shafait F. Table Structure Extraction with Bi-Directional Gated Recurrent Unit Networks. International Conference on Document Analysis and Recognition (ICDAR). 2019. pp. 1366–1371. DOI: 10.1109/ICDAR.2019.00220.
14. Hochreiter S., Schmidhuber J. Long Short-Term Memory. Neural computation. 1997. vol. 9. no. 8. pp. 1735–1780. DOI: 10.1162/neco.1997.9.8.1735.
15. Paliwal S.S., Vishwanath D., Rahul R., Sharma M., Vig L. TableNet: Deep Learning Model for End-to-end Table Detection and Tabular Data Extraction from Scanned Document Images. International Conference on Document Analysis and Recognition (ICDAR). 2019. pp. 128–133. DOI: 10.1109/ICDAR.2019.00029.
16. Tensmeyer C., Morariu V.I., Price B., Cohen S., Martinez T. Deep Splitting and Merging for Table Structure Decomposition. International Conference on Document Analysis and Recognition (ICDAR). 2019. pp. 114–121. DOI: 10.1109/ICDAR.2019.00027.
17. Siddiqui S.A., Fateh I.A., Rizvi S.T.R., Dengel A., Ahmed S. DeepTabStR: Deep Learning based Table Structure Recognition. International Conference on Document Analysis and Recognition (ICDAR). 2019. pp. 1403–1409. DOI: 10.1109/ICDAR.2019.00226.
18. Couasnon B., Lemaitre A. Recognition of Tables and Forms. Handbook of Document Image Processing and Recognition. Chapter Recognition of Tables and Forms. 2014. pp. 647–677. DOI: 10.1007/978-0-85729-859-1_20.
19. Zucker A., Belkada Y., Vu H., Nguyen V.N. ClusTi: Clustering Method for Table Structure Recognition in Scanned Images. Mobile Networks and Applications. 2021. vol. 26. no. 4. pp. 1765–1776. DOI: 10.1007/s11036-021-01759-9.

20. Nguyen Q.D., Le D.A., Phan N.M., Zelinka I. OCR error correction using correction patterns and self-organizing migrating algorithm. Pattern Analysis and Applications. 2021. vol. 24. pp. 701–721. DOI: 10.1007/s10044-020-00936-y.
21. Patel C., Patel A., Patel D. Optical Character Recognition by Open source OCR Tool Tesseract: A Case Study. International Journal of Computer Applications. 2014. vol. 55(10). pp. 50–56. DOI: 10.5120/8794-2784.
22. Vorobjev V. PGI Geophysical data. 2015. October, November, December. Murmansk, Apatity: PGI KSC RAS, 2016.
23. Vorobjev V.G., Roldugin V.C., Yagodkina O.I. Large Amplitude Undulations of Evening Site Diffuse Aurorae. Optical Characteristics and Conditions of Generation. Geomagnetism and Aeronomy. 2015. vol. 55. pp. 45–50. DOI: 10.1134/S0016793215010132.
24. Vorobjev V.G., Yagodkina O.I., Antonova E.E. Ion Pressure in Different Regions of the Dayside Auroral Precipitation. Geomagnetism and Aeronomy. 2020. no. 60. pp. 727–736. DOI: 10.1134/S0016793220060146.
25. Popov L.N., Krakovetskiy Yu.K., Gokhberg M.B., Pilipenko V.A. Terrogenic effects in the ionosphere: a review. Physics of the Earth and Planetary Interiors. 1989. vol. 57. no. 1-2. pp. 115–128.
26. Zhang T., Qiu H., Castellano G., Rifai M., Chen C.S., Pianese F. System Log Parsing: A Survey. IEEE Transactions on Knowledge and Data Engineering. 2023. pp. 8596–8614. DOI: 10.1109/TKDE.2022.3222417.
27. Patil O., Chavan U. Rule Based Expert System for Error Log Analysis. International Journal of Innovative Technology and Exploring Engineering. 2020. vol. 9. no. 10. pp. 188–192. DOI: 10.35940/ijitee.J7466.0891020.
28. Peta S. Python- An Appetite for the Software Industry. International Journal of Programming Languages and Applications (IJPLA). 2022. vol. 12. DOI: 10.5121/ijpla.2022.12401.
29. Singh B.P. Python and Its Future Scope. International Journal of Advanced Research in Science, Communication and Technology. 2022. pp. 400–403. DOI: 10.48175/IJARSCT-4829.
30. Dr U., Patkar U. Python for web development. International Journal of Computer Science and Mobile Computing. 2022. vol. 11. no. 4. pp. 36–48. DOI: 10.47760/ijcsmc.2022.v11i04.006.
31. Rong W., Xu T., Sun, Z., Sun, Z., Ouyang, Y., Xiong, Z. An Object Tuple Model for Understanding Pointer and Array in C Language. IEEE Transactions on Education. 2023. pp. 1–12. DOI: 10.1109/TE.2023.3236027.
32. Peta S. C Programming Language–Still Ruling the World. Global Journal of Computer Science and Technology. 2022. vol. 22(1). pp. 9–13.
33. Park H., Kim S., Bae B. Dynamic code compression for JavaScript engine. Software: Practice and Experience. 2023. vol. 53. no. 5. pp. 1196–1217. DOI: 10.1002/spe.3186.
34. Wang Z., Bu D., Wang N., Yu S., Gou S., Sun A. An empirical study on bugs in JavaScript engines. Information and Software Technology. 2023. vol. 155. no. 107105. DOI: 10.1016/j.infsof.2022.107105.
35. Romanchuk V.M. The Problem of Adequacy of the Analytic Hierarchy Process. Modelling and Data Analysis. 2022. vol. 10. no. 4. pp. 79–87. DOI: 10.17759/mda.2020100407.
36. Polat T.K. An Application of Analytic Hierarchy Process and Fuzzy Analytic Hierarchy Process to the Case Type Selection Problem. Academic Perspective Procedia. 2018. vol. 1. no. 1. pp. 1179–1188. DOI: 10.33793/acperpro.01.01.188.
37. Vorobev A.V., Pilipenko V.A., Enikeev T.A., Vorobeva G.R. Geoinformation system for analyzing the dynamics of extreme geomagnetic disturbances from observations of

ground stations. Computer Optics. 2020. vol. 44(5). pp. 782–790. DOI: 10.18287/2412-6179-CO-707.

38. Vorobev A.V., Soloviev A.A., Pilipenko V.A., Vorobeva G.R., Gainetdinova A.A., Lapin A.N., Belakhovsky V.B., Roldugin A.V. Local diagnostics of aurora presence based on intelligent analysis of geomagnetic data. Solar-Terrestrial Physics. 2023. vol. 9(2). pp. 22–30. DOI: 10.12737/stp-92202303.

Vorobev Andrei — Ph.D., Dr.Sci., Professor, Geoinformation systems department of computer science and robotics faculty, Ufa University of Science and Technology; Senior researcher, Geophysical Center of RAS. Research interests: geoinformation technologies, digital signal processing. The number of publications — 164. geomagnet@list.ru; 12, Karl Marx St., 450007, Ufa, Russia; office phone: +7(917)345-2299.

Lapin Alexander — Student, Geoinformation systems department of computer science and robotics faculty, Ufa University of Science and Technology. Research interests: mathematical and computer modeling, digital twins, machine learning. The number of publications — 13. meccos160@yandex.ru; 12, Karl Marx St., 450008, Ufa, Russia; office phone: +7(917)439-6040.

Vorobeva Gulnara — Ph.D., Dr.Sci., Professor, Computational mathematics and cybernetics department of computer science and robotics faculty, Ufa University of Science and Technology. Research interests: geoinformation and web technologies, systems of information storing and processing. The number of publications — 153. gulnara.vorobeva@gmail.com; 12, Karl Marx St., 450008, Ufa, Russia; office phone: +7(917)417-4111.

Acknowledgements. The reported study was funded by RSF, project number 21-77-30010.

УДК 004.22 **DOI** 10.15622/ia.22.5.9

И.А. Суров

ЦВЕТОВАЯ КОДИРОВКА КУБИТНЫХ СОСТОЯНИЙ

Суров И.А. **Цветовая кодировка кубитных состояний.**

Аннотация. Трудности алгоритмической имитации естественного мышления указывают на несовершенство используемых для этого форматов представления информации. В этом отношении перспективна кодировка информации кубитными состояниями квантовой теории, структура которых согласуется с крупными теориями когнитивной семантики. Представлено развитие этого подхода, связывающее кубитные состояния с цветом как самостоятельным носителем эмоционально-смысловых значений. Основой для этого стало геометрическое подобие цветовых тел и Гильбертова пространства кубитных состояний, позволившее установить между ними взаимооднозначное математическое отображение. Для этого использовано оригинальное разложение кубита по тройке неортогональных векторов, соответствующих красному, синему и зелёному цветам. Действительные коэффициенты такого разложения являются томограммами кубитного состояния по соответствующим направлениям, связанными с компонентами вектора Стокса операцией поворота. При этом композиционные соотношения чёрного, белого и шести основных цветов (красный, зелёный, синий, жёлтый, фиолетовый, голубой) выражаются аналогичными суперпозициями кубитных состояний. Чистые и смешанные цвета соответствуют чистым и смешанным состояниям на поверхности и внутри сферы Блоха, тогда как оттенки серого отображаются на вертикальный диаметр сферы. При этом светлость цвета соответствует вероятности базисного кубитного состояния «1», тогда как насыщенность цвета и цветовой тон кодируют когерентность и фазу кубитного состояния. Полученный результат открывает возможности для использования квантовой информатики в задачах семантического анализа данных, обработки изображений и создания природоподобных вычислительных архитектур.

Ключевые слова: квант, кубит, цвет, эмоциональный смысл, квантовая информатика, обработка изображений, квант, код.

1. Введение. Кодировка информации определяет возможности строящихся на её основе алгоритмов. Широкая применимость современного искусственного интеллекта, например, обусловлена простотой и универсальностью двоичного кода, технологизированного в середине прошлого века. Огромное разнообразие форматов текстовой, графической, звуковой и другой информации на деле сводится к этому фундаментальному мета-коду.

Возможности алгоритмов на основе двоичного кода, однако, не безграничны. Примером тому являются трудности современного ИИ в имитации образного и смыслового мышления[1], играющего ключевую роль в живой природе [1–3]. Даже в хорошо формализуемых задачах вроде шахмат и го естественное мышление намного эффективнее компьютерного вычисления: в сравнении с несколькими тысячами пройденных гроссмейстером партий и 20 Вт энергопотребления среднего мозга, для сравнимого результата суперкомпьютерные системы требуют много большего объёма ресурсов [4, 5].

Возникающая в этой связи задача нахождения более подходящих способов кодирования и алгоритмов обработки информации имеет множество решений. В их числе троичная логика [6, 7], волновые и (голо)графические вычисления [4, 8–10] и обработка образов [11–13]. Отдельным направлением «альтернативной» информатики является квантовая информатика, в которой информация кодируется квантовыми состояниями физических систем.

1.1. Кодирование информации квантовыми состояниями. Достигнутые таким образом преимущества в задачах поиска, оптимизации, шифрования и факторизации больших чисел обусловлены новыми возможностями для построения алгоритмов в этой кодировке [14–16]. Такие алгоритмы реализуются как с помощью квантово-физических, так и с помощью классических носителей и законов природы. Алгоритмы второго типа, называемые квантово-подобными, выполняются на обычных компьютерах без привлечения «настоящих» квантовых состояний. Их преимущество по сравнению с классическими аналогами [17, 18], обусловленное в том числе контекстуальностью соответствующей теории вероятности[2] [19, 20], показывают эффект от смены кодировки наиболее явно.

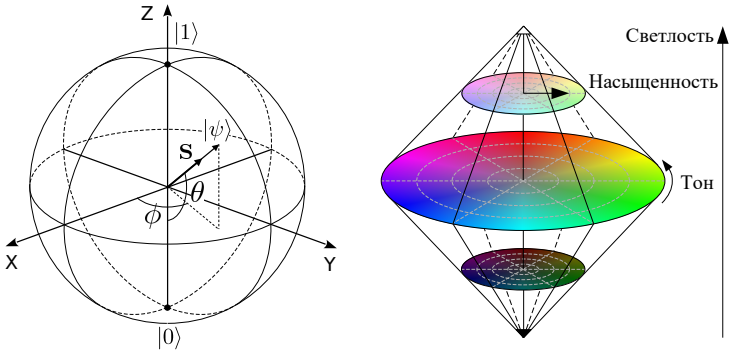
Использование квантовых форматов информации затруднено необходимостью их интерпретации, пригодной для применения за пределами элементарных физических систем. Главную трудность в этом отношении представляет комплекснозначность квантовых состояний, являющихся векторами в многомерных Гильбертовых пространствах [14, 21]. Компоненты таких векторов, в частности, несут фазовые параметры с круговой топологией, не имеющие аналогов в

[1]В отличие от машинного вычисления, естественное мышление работает с образами и знаками на основе их значений для субъекта. Термин «смысловое мышление» указывает на это свойство.

[2]Т.е. возможностью учитывать изменение вероятностных закономерностей в различных условиях наблюдения (контекстах).

двоичном коде; примером такого параметра является фаза ϕ кубитного состояния, структура которого показана на рисунке 1(а). В отсутствие интерпретации фазовых параметров использование квантовых кодировок носит формальный характер, что затрудняет развитие алгоритмов обработки данных на этой основе.

1.2. Интерпретации кубитного состояния в алгоритмах обработки изображений. Интерпретируемое кодирование информации квантовыми состояниями используется для обработки изображений. Как и в классических подходах, изображение кодируется путём его разбивки на элементарные ячейки – пиксели, цвет каждого из которых кодируется отдельным кубитным состоянием [22]. Использованная при этом цветовая разметка пространства кубитных состояний, однако, не полна. На рисунке 1(а) она задействует лишь полярный угол θ, тогда как фазы ϕ (представляющие наибольший интерес для интерпретации квантовых состояний) не используются [23–25]. Цвет пикселя при этом кодируется лишь частично, т.к. из трёх параметров тон – насыщенность – светлость, показанных на рисунке 1(б), охватывается только цветовой тон. Даже такой ограниченный формат, однако, позволил усовершенствовать алгоритмы хранения, сжатия, шифрования, поиска и других задач обработки изображений на основе методов квантовой информатики [28–31].



а) б)

Рис. 1. а) пространство кубитных состояний в представлении сферы Блоха; б) цветовое тело в модели оттенок – насыщенность – светлость (HSL) [26, 27]. Оттенок (тон, hue) определяет расположение цвета в хроматическом спектре (например, в радуге). Светлость (lightness) определяет близость цвета к белому и чёрному. Насыщенность цвета (чистота, saturation) определяет его похожесть на серый цвет той же светлости

1.3. Проблема и подход к решению. Расширенная цветовая кодировка кубитных состояний предложена рядом авторов в 2021-2022 г. В работе [32] цветовой тон впервые кодируется не полярным, а азимутальным углом ϕ в соответствии с циклической структурой цветового круга [33, 34]. Полярный угол при этом отводится для кодирования насыщенности, тогда как светлость записывается в дополнительном регистре кубитных состояний. В альтернативном подходе [35] насыщенность и цвет кодируются различными интервалами полярного угла.

Общим недостатком перечисленных способов кодировки является произвольность их построения, так что параметры цвета сопоставляются определённым диапазонам значений кубитных состояний без какого-либо теоретического основания. При трёх параметрах цвета, двух либо трёх параметрах кубитного состояния и неограниченной свободе соотнесения диапазонов соответствующих значений число возможных кодировок при таком подходе неограниченно велико. Нахождение наилучшей из них предполагает сравнение эффективности разработанных для каждого случая алгоритмов решения интересующих задач, что путём слепого перебора вряд ли возможно.

Решение этой проблемы возможно с помощью теории, ограничивающей число возможных кодировок на основе дополнительных соображений. Примером такого подхода является согласование искомой разметки со структурными моделями эмоций человека, напрямую связанных с цветом. Полученная таким образом цветовая кодировка азимутального угла ϕ [36] использована для создания эмоционально-компетентных роботов [37].

Более полная цветовая разметка кубитных состояний предложена в работе [38]. В отличие от вышеупомянутых эмпирических аналогов, эта разметка построена из первых принципов квантовой теории и согласуется с моделями функциональной семиотики (смыслопорождения), а также пространственными моделями цветосемантики и эмоционально-смысловых состояний [39, 40]. Полученное математическое отображение, однако, приведено иллюстративно без объяснения использованной логики и рассмотрения свойств, важных для практической работы с кодом. Эти недостатки устраняются в настоящей статье.

2. Кубитные состояния на сфере Блоха

2.1. Чистые состояния. Произвольное кубитное состояние представляется нормированным двумерным вектором

$$\begin{bmatrix} a_0 e^{i\phi} \\ a_1 \end{bmatrix} = a_0 e^{i\phi} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + a_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \tag{1}$$

где a_0 и a_1 есть действительные амплитуды, а $e^{i\phi}$ есть комплекснозначный множитель, определяемый значением фазы $\phi \in [0, 2\pi)$. В отличие от стандартной записи [21] этот множитель отнесён к нулевой компоненте вектора для удобства последующих вычислений. В обозначениях Дирака кубитные состояния отмечаются угловыми скобками, так что (1) принимает вид

$$|\psi\rangle = a_0 e^{i\phi} |0\rangle + a_1 |1\rangle, \tag{2}$$

где кубитное состояние $|\psi\rangle$ есть суперпозиция базисных векторов $|0\rangle$ и $|1\rangle$ в правой части (1).

Нормировка кубитного состояния выражается соотношением

$$\begin{aligned} &\langle\psi|\psi\rangle = a_0^2 + a_1^2 = 1, \\ &\langle\psi| = |\psi\rangle^\dagger = \begin{bmatrix} a_0 e^{-i\phi} & a_1 \end{bmatrix}, \end{aligned} \tag{3}$$

где $\langle\psi|$ есть Эрмитово сопряжение вектора (2). В силу (3) коэффициенты a допускают тригонометрическую параметризацию, в которой состояние (2) принимает вид

$$|\psi\rangle = \cos\frac{\theta}{2} e^{i\phi} |0\rangle + \sin\frac{\theta}{2} |1\rangle, \quad \theta \in [0, \pi]. \tag{4}$$

В результате произвольное кубитное состояние представляется единичным вектором в трёхмерном Евклидовом пространстве как показано на рисунке 1(а). Каждой точке на полученной сфере (Пуанкаре-Блоха) соответствует единственное кубитное состояние (1), (4), однозначно характеризуемое полярным углом θ и азимутальным углом ϕ. Такие состояния называются *чистыми*.

2.2. Смешанные состояния. Кубитные состояния, норма которых (3) меньше единицы, называются *смешанными*. Длина соответствующего вектора составляет дополнительную степень свободы смешанных состояний. Произвольное такое состояние характеризуется

вектором Стокса

$$\mathbf{S} = \begin{bmatrix} x \\ y \\ z \end{bmatrix}, \qquad |\mathbf{S}|^2 = x^2 + y^2 + z^2 \leqslant 1. \tag{5}$$

Компоненты этого вектора образуют Эрмитову матрицу

$$\hat{\rho} = \frac{1}{2} \begin{bmatrix} 1 - z & x + iy \\ x - iy & 1 + z \end{bmatrix}, \tag{6}$$

имеющую единичный след и неотрицательные собственные значения. Такая *матрица плотности* однозначно определяет любое кубитное состояние. Чистые состояния, в частности, соответствуют равенству в (5). В этом случае вектор Стокса состояния (4) есть

$$\mathbf{S} = \begin{bmatrix} \sin\theta\cos\phi \\ \sin\theta\sin\phi \\ -\cos\theta \end{bmatrix}, \tag{7}$$

как видно из рисунка 1(а).

Матрица плотности (6) также представима в виде

$$\hat{\rho} = \begin{bmatrix} p_0 & c\sqrt{p_0 p_1}e^{i\phi} \\ c\sqrt{p_0 p_1}e^{-i\phi} & p_1 \end{bmatrix}, \quad c \in [0, 1], \tag{8}$$

где на диагонали находятся вероятности $p_0 + p_1 = 1$ осуществления в эксперименте исходов 0 и 1, соответствующие квадратам амплитуд чистого состояния (3). При отсутствии недиагональных элементов $c = 0$ матрица плотности эквивалентна классическому вероятностному пространству двухвариантной неопределённости. Наибольшее значение $c = 1$ соответствует насыщению неравенства (5) и чистому состоянию (1), (4), не имеющему аналога в теории вероятности Колмогорова. Параметр

$$c\sqrt{p_0 p_1} = \frac{\sqrt{x^2 + y^2}}{2}, \qquad 0 \leqslant c\sqrt{p_0\, p_1} \leqslant 0{,}5, \tag{9}$$

таким образом характеризует «квантовость», т.е. *когерентность* кубитного состояния [41]. Вариация этой величины описывает переход между классическим и квантовым пределами квантовой теории вероятности [42].

3. Опорные точки

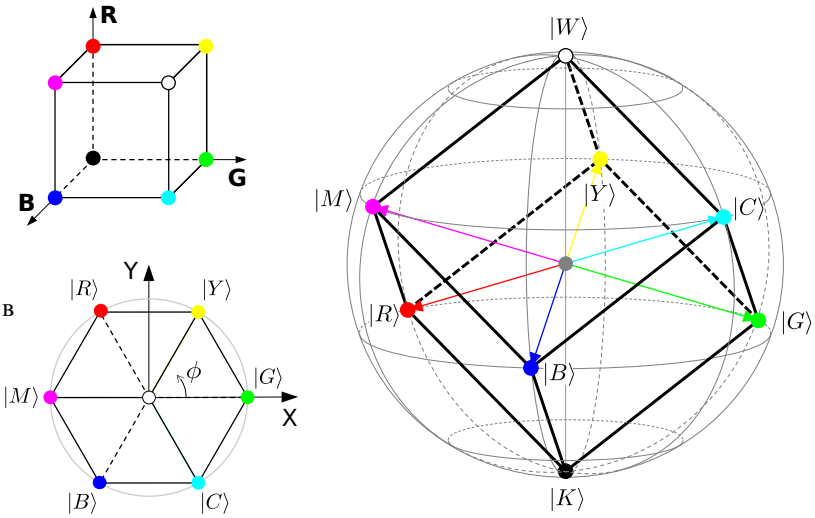
3.1. Красный, зелёный, синий. Цветовая кодировка кубитных состояний строится на основе трёх главных цветов: красного (R), зелёного (G) и синего (B). Этим цветам соответствуют кубитные состояния, нахождение которых показано на рисунке 2:

1. Цветовой куб RGB (а) вписывается в сферу Блоха так, что её полюса соответствуют белому (W) и чёрному (K) цветам (б)

$$|W\rangle = |1\rangle\,, \qquad |K\rangle = |0\rangle\,. \tag{10}$$

2. Угловое положение куба вокруг вертикальной оси Z фиксируется так, что зелёный цвет располагается в плоскости XZ (в).

3. Полученные точки касания сферы и куба определяют угловые координаты чистых кубитных состояний, соответствующих главным цветам согласно (4).



а) б)

Рис. 2. Кубитные состояния: а) восемь главных цветов в вершинах цветового куба, представляющего аддитивную цветовую модель RGB; б) вписание цветового куба в сферу Блоха (рисунок 1); в) расположение главных цветов в экваториальной плоскости XY

А именно, главные цвета R, G, B лежат в горизонтальной плоскости, определяемой полярным углом

$$\theta_{\mathrm{RGB}} = \arccos\frac{1}{3} \approx 1{,}23 \approx 70{,}5^\circ,$$
$$\cos\frac{\theta_{\mathrm{RGB}}}{2} = \sqrt{\frac{2}{3}}, \qquad \sin\frac{\theta_{\mathrm{RGB}}}{2} = \sqrt{\frac{1}{3}}. \tag{11}$$

Азимутальные углы этих цветов кратны 120° как следует из рисунка 2(в). Соответствующие кубитные состояния (4) есть

$$|R\rangle = \frac{1}{\sqrt{3}}\begin{bmatrix}\sqrt{2}e^{i\phi_{\mathrm{R}}}\\ 1\end{bmatrix}, \qquad \phi_{\mathrm{R}} = 2\pi/3,$$
$$|G\rangle = \frac{1}{\sqrt{3}}\begin{bmatrix}\sqrt{2}e^{i\phi_{\mathrm{G}}}\\ 1\end{bmatrix}, \qquad \phi_{\mathrm{G}} = 0, \tag{12}$$
$$|B\rangle = \frac{1}{\sqrt{3}}\begin{bmatrix}\sqrt{2}e^{i\phi_{\mathrm{B}}}\\ 1\end{bmatrix}, \qquad \phi_{\mathrm{B}} = 4\pi/3.$$

Эти состояния нормированы, однако не ортогональны между собой

$$\langle R|R\rangle = \langle G|G\rangle = \langle B|B\rangle = 1,$$
$$\langle G|R\rangle = \langle R|B\rangle = \langle B|G\rangle = i/\sqrt{3}. \tag{13}$$

3.2. Голубой, фиолетовый, жёлтый. Одновременно с главными определяются кубитные кодировки производных цветов: голубой (C, cyan), фиолетовый (M, magenta) и жёлтый (Y, yellow). Им соответствует полярный угол

$$\theta_{\mathrm{CMY}} = \arccos\frac{-1}{3} \approx 1{,}91 \approx 109{,}5^\circ,$$
$$\cos\frac{\theta_{\mathrm{CMY}}}{2} = \sqrt{\frac{1}{3}}, \qquad \sin\frac{\theta_{\mathrm{CMY}}}{2} = \sqrt{\frac{2}{3}}, \tag{14}$$

так что плоскости RGB и CMY делят вертикальный диаметр сферы Блоха на три равные части. Кубитные состояния этих цветов есть

$$
\begin{aligned}
|C\rangle &= \frac{1}{\sqrt{3}}\begin{bmatrix} e^{i\phi_{\mathrm{C}}} \\ \sqrt{2} \end{bmatrix}, \qquad \phi_{\mathrm{C}} = 5\pi/3, \\
|M\rangle &= \frac{1}{\sqrt{3}}\begin{bmatrix} e^{i\phi_{\mathrm{M}}} \\ \sqrt{2} \end{bmatrix}, \qquad \phi_{\mathrm{M}} = \pi, \\
|Y\rangle &= \frac{1}{\sqrt{3}}\begin{bmatrix} e^{i\phi_{\mathrm{Y}}} \\ \sqrt{2} \end{bmatrix}, \qquad \phi_{\mathrm{Y}} = \pi/3.
\end{aligned} \tag{15}
$$

Аналогично (13)

$$
\begin{aligned}
&\langle C|C\rangle = \langle M|M\rangle = \langle Y|Y\rangle = 1, \\
&\langle M|C\rangle = \langle C|Y\rangle = \langle Y|M\rangle = \frac{3 + i\sqrt{3}}{6}.
\end{aligned} \tag{16}
$$

3.3. Ортогональность. Противоположные вершины цветового куба (рисунок 2б) образуют четыре пары дополнительных цветов (т.е. таких, смешение которых в равных пропорциях даёт серый цвет в центре куба): белый-чёрный, красный-голубой, синий-жёлтый и зелёный-фиолетовый. Это свойство выражается ортогональностью соответствующих кубитных состояний. Например

$$
\langle R|C\rangle = \frac{1}{3}\begin{bmatrix} \sqrt{2}e^{-2i\pi/3} & 1 \end{bmatrix}\begin{bmatrix} e^{5i\pi/3} \\ \sqrt{2} \end{bmatrix} = \frac{\sqrt{2}}{3}\left(e^{i\pi} + 1\right) = 0,
$$

где использовано определение Эрмитова сопряжения (3); аналогично

$$
\langle G|M\rangle = \langle B|Y\rangle = \langle W|K\rangle = 0.
$$

Эти соотношения эквивалентны противоположности соответствующих векторов Стокса (7)

$$
\begin{aligned}
\mathbf{S}_{\mathrm{R}} &= \begin{bmatrix} -\sqrt{2}/3 & \sqrt{2/3} & -1/3 \end{bmatrix}^{\mathrm{T}} = -\mathbf{S}_{\mathrm{C}}, \\
\mathbf{S}_{\mathrm{G}} &= \begin{bmatrix} \sqrt{8/9} & 0 & -1/3 \end{bmatrix}^{\mathrm{T}} = -\mathbf{S}_{\mathrm{M}}, \\
\mathbf{S}_{\mathrm{B}} &= \begin{bmatrix} -\sqrt{2}/3 & -\sqrt{2/3} & -1/3 \end{bmatrix}^{\mathrm{T}} = -\mathbf{S}_{\mathrm{Y}}, \\
\mathbf{S}_{\mathrm{W}} &= \begin{bmatrix} 0 & 0 & 1 \end{bmatrix}^{\mathrm{T}} = -\mathbf{S}_{\mathrm{K}}.
\end{aligned} \tag{17}
$$

Таким образом дополнительность цветов в кубитной кодировке получает строгое геометрическое выражение[3].

3.4. Суперпозиция. Кубитные состояния голубого, фиолетового и жёлтого цветов (15) являются симметричными суперпозициями тройки базисных состояний (12). Например

$$\frac{|G\rangle + |B\rangle}{\sqrt{2}} = \frac{1}{\sqrt{6}} \begin{bmatrix} \sqrt{2}\left(1 + e^{4\pi i}\right) \\ 2 \end{bmatrix} = \frac{1}{\sqrt{3}} \begin{bmatrix} e^{5\pi i/3} \\ \sqrt{2} \end{bmatrix} = |C\rangle\,. \qquad (18)$$

Аналогично

$$\frac{|B\rangle + |R\rangle}{\sqrt{2}} = |M\rangle\,, \qquad \frac{|R\rangle + |G\rangle}{\sqrt{2}} = |Y\rangle\,. \qquad (19)$$

Эти соотношения выражают композицию дополнительных цветов C, M, Y в аддитивной цветовой модели согласно геометрии куба на рисунке 2(а)

$$\mathbf{C} = \mathbf{G} + \mathbf{B}, \qquad \mathbf{M} = \mathbf{B} + \mathbf{R}, \qquad \mathbf{Y} = \mathbf{R} + \mathbf{G}. \qquad (20)$$

Таким образом цветовая кодировка рассмотренных кубитных состояний сохраняет их суперпозиционные отношения, играющие ключевую роль в алгоритмах квантовой информатики.

Особенность приведённых суперпозиций в том, что суммируемые состояния не ортогональны (как например в простейшем кубитном состоянии $(|0\rangle + |1\rangle)/\sqrt{2}$), однако нормировочный множитель в левых частях (18), (19) тем не менее равен $1/\sqrt{2}$. Это объясняется мнимостью попарных перекрытий (13), в силу чего например

$$\langle M|M\rangle = \frac{\langle R| + \langle B|}{\sqrt{2}} \cdot \frac{|R\rangle + |B\rangle}{\sqrt{2}} =$$
$$\frac{\langle R|R\rangle + \langle B|B\rangle + \langle R|B\rangle + \langle B|R\rangle}{2} = \frac{1 + 1 + i/\sqrt{3} - i/\sqrt{3}}{2} = 1.$$

Этим же обусловлена величина знаменателя в кубитном разложении базисного состояния $|1\rangle$ (10)

$$|W\rangle = \frac{|R\rangle + |B\rangle + |G\rangle}{\sqrt{3}}, \qquad (21)$$

[3]Цвета в левой и правой частях строк (17) образуют два правильных тетраэдра, вершины каждого из которых равномерно покрывают сферу Блоха. Вершинам тетраэдра RGBW соответствуют четыре типа светочувствительных клеток в сетчатке человеческого глаза.

что соответствует композиции белого цвета

$$\mathbf{W} = \mathbf{R} + \mathbf{G} + \mathbf{B} \tag{22}$$

в аддитивной цветовой модели.

4. Чистые состояния

4.1. Начальное разложение. Цветовая кодировка произвольного чистого состояния следует из его разложения в базисе основных цветов (12)

$$|\psi\rangle = \begin{bmatrix} \cos\dfrac{\theta}{2}e^{i\phi} \\ \sin\dfrac{\theta}{2} \end{bmatrix} = r\,|R\rangle + g\,|G\rangle + b\,|B\rangle\,, \qquad r, g, b \in \mathbb{R}. \tag{23}$$

В отличие от стандартной в квантовой информатике формы (1), (2) с комплекснозначными амплитудами, коэффициенты разложения можно ограничить действительными числами благодаря использованию трёх базисных векторов.

Значения коэффициентов r, g, b определяются путём перекрытия состояния (23) с соответствующим базисным вектором (12) с учётом (13). Для зелёного цвета, например

$$\begin{aligned} \langle G|\psi\rangle = \begin{bmatrix} \sqrt{2/3} & \sqrt{1/3} \end{bmatrix} \begin{bmatrix} \cos\dfrac{\theta}{2}e^{i\phi} \\ \sin\dfrac{\theta}{2} \end{bmatrix} = \\ r\,\langle G|R\rangle + g\,\langle G|G\rangle + b\,\langle G|B\rangle = g + \frac{i}{\sqrt{3}}(r-b), \end{aligned} \tag{24}$$

откуда значение коэффициента g получается как функция от угловых координат раскладываемого состояния

$$g(\theta, \phi) = \mathrm{Re}\,\langle G|\psi\rangle = \frac{1}{\sqrt{3}}\left(\sin\frac{\theta}{2} + \sqrt{2}\cos\frac{\theta}{2}\cos\phi\right). \tag{25}$$

График этой функции показан на рисунке 3(а).

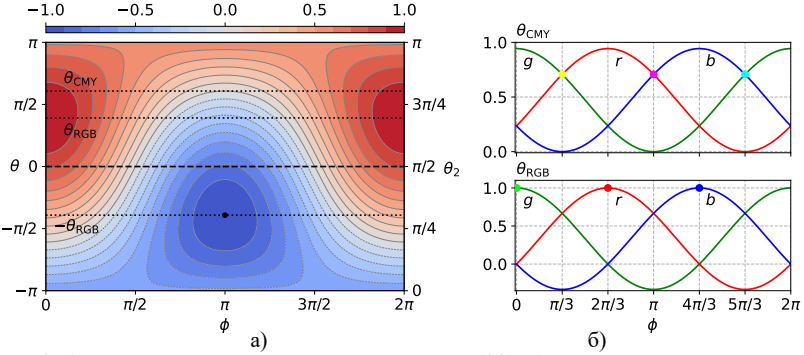


Рис. 3. Амплитуда зелёного цвета g разложения (23): а) в зависимости от угловых координат кубитного состояния (4) согласно решению (28); б) в зависимости от азимутального угла при фиксированных θ_{RGB} и θ_{CMY}

При $\phi = 0$, т.е. в плоскости ZX, функция (25) есть просто

$$g(\theta, 0) = \cos\frac{\theta - \theta_{\mathrm{RGB}}}{2} = \sqrt{\frac{1 + \cos(\theta - \theta_{\mathrm{RGB}})}{2}}, \tag{26}$$

откуда видно что величину (25) (с точностью до знака) также можно определить как

$$g^2(\theta, \phi) = \frac{1 + \mathbf{S} \cdot \mathbf{S}_{\mathrm{G}}}{2}, \tag{27}$$

где $\mathbf{S}$ и $\mathbf{S}_{\mathrm{G}}$ есть вектора Стокса (5) состояний $|\psi\rangle$ и $|G\rangle$ (23) [4]. При $\theta = 0$ – пунктир на рисунке 3(а) – также имеет место простая гармоническая зависимость. Аналогичные (25) функции для остальных коэффициентов

$$\begin{aligned} r(\theta, \phi) &= \mathrm{Re}\,\langle R|\psi\rangle = g\left(\theta, \phi - \frac{2\pi}{3}\right), \\ b(\theta, \phi) &= \mathrm{Re}\,\langle B|\psi\rangle = g\left(\theta, \phi - \frac{4\pi}{3}\right), \end{aligned} \tag{28}$$

получаются сдвигом азимутального угла на ϕ_{R} и ϕ_{B} (12) соответственно.

Значения амплитуд r, g, b в зависимости от азимутального угла ϕ при фиксированных значениях полярного угла θ показаны на рисунке 3(б) соответствующими цветами. Верхний график соответствует θ_{CMY},

[4] Функция (27) есть томограмма кубитного состояния по направлению $|G\rangle$, т.е. вероятность исхода $|G\rangle$ при измерении состояния (23) в базисе $|G\rangle, |M\rangle$ [43].

при котором значения $\phi = \pi/3$, π и $5\pi/3$ соответствуют жёлтому, фиолетовому и голубому цветам (раздел 3.2).

В этих точках амплитуды противоположных цветов равны нулю, тогда как остальные две равны $1/\sqrt{2}$ в соответствии с выражениями (18), (19). Нижний график соответствует θ_{RGB}, при котором $\phi = 0$, $2\pi/3$ и $4\pi/3$ соответствуют зелёному, красному и синему (раздел 3.1). Соответствующие амплитуды в этих точках принимают наибольшее значение 1, тогда как остальные равны нулю.

4.2. Геометрия решения. Величины (25), (28) удовлетворяют соотношению

$$r^2(\theta,\phi) + g^2(\theta,\phi) + b^2(\theta,\phi) \equiv 1. \tag{29}$$

как того требует нормировка $\langle\psi|\psi\rangle = 1$ правой части (23) при условии (13). Этот же результат можно получить прямым решением векторного уравнения (23), эквивалентного системе

$$\cos\frac{\theta}{2}e^{i\phi} = \sqrt{\frac{2}{3}}\left(re^{i\phi_{\mathrm{R}}} + ge^{i\phi_{\mathrm{G}}} + be^{i\phi_{\mathrm{B}}}\right), \tag{30a}$$

$$\sin\frac{\theta}{2} = \frac{r+g+b}{\sqrt{3}}. \tag{30b}$$

Таким образом, коэффициенты разложения любого чистого состояния (23) располагаются на единичной сфере (29) в трёхмерном Евклидовом пространстве. Сечение этой сферы плоскостью (30b) определяет вид решения в зависимости от полярного угла θ

– При максимальном для кубитного состояния (4) $\theta = \pi$ плоскость (30b) пересекается со сферой (29) в единственной точке касания $r = g = b = 1/\sqrt{3}$. Эта точка соответствует белому цвету (21) на северном полюсе сферы Блоха $|1\rangle$.

– При уменьшении θ пересечение становится окружностью, на которой точка с углом ϕ соответствует решению (25), (28). Соответствующая зависимость коэффициентов r, g, b от фазы ϕ при θ_{CMY} и θ_{RGB} показана на рисунке 3(б).

– При наименьшем для кубитного состояния (4) $\theta = 0$ плоскость (30b) пересекает сферу (29) по экватору $r + g + b = 0$, показанному на рисунке 3(а) пунктиром.

– Формальная подстановка $\theta = -\pi$ даёт симметричную точку касания $r = g = b = -1/\sqrt{3}$, снова соответствующую белому цвету (21) с отрицательным знаком.

Таким образом сфера Блоха на рисунке 1 соответствует половине сферы (29), вторая половина которой в разложении (23) не используется. Для построения искомой кодировки данное обстоятельство затруднительно т.к. полусфера топологически отличается и от сферы Блоха и от цветовых тел. Кроме того, южный полюс последней $|0\rangle$ соответствует всем цветам на экваторе сферы (29), т.е. разложение (23) для этого состояния не является однозначным. Эта неоднозначность проявляется также в функции (26), период которой составляет два оборота вокруг сферы Блоха. Данная проблема решается с помощью замены полярного угла в кубитном состоянии.

4.3. Замена полярного угла. Перечисленные затруднения устраняются параметризацией кубитного состояния полярным углом θ так, чтобы северному и южному полюсам $|1\rangle$, $|0\rangle$ соответствовали значения $\theta = \pm\pi$. Простейшая такая параметризация получается заменой в исходном кубитном состоянии (4) полярного угла θ на

$$\begin{gathered}\theta_2 = \frac{\theta+\pi}{2}, \qquad \theta \in [-\pi,\pi], \quad \theta_2 \in [0,\pi], \\ \sin\frac{\theta}{2} = -\cos\theta_2, \quad \cos\frac{\theta}{2} = \sin\theta_2.\end{gathered} \tag{31}$$

Вместе с исходным азимутальным углом ϕ новый угол θ_2 определяет кубитное состояние

$$|\psi_2\rangle = \cos\frac{\theta_2}{2}e^{i\phi}\,|0\rangle + \sin\frac{\theta_2}{2}\,|1\rangle\,, \tag{32}$$

сфера Блоха которого обладает требуемым свойством как показано на рисунке 4. В силу тождеств (31) и (11) амплитуда зелёного цвета для $\phi = 0$ (25) принимает вид

$$\begin{aligned} g(\theta_2,0) &= \frac{-1}{\sqrt{3}}\cos\theta_2 + \frac{2}{\sqrt{3}}\sin\theta_2 \\ &= \cos\left(\theta_2 - \left(\frac{\pi}{2}+\alpha\right)\right), \quad \alpha = \frac{\theta_{\mathrm{RGB}}}{2}. \end{aligned} \tag{33}$$

Согласно геометрии рисунка 4 величина $\alpha \approx 35^\circ$ есть угол между вектором $\mathbf{G}$ и горизонтальной плоскостью. Угол $\alpha + \pi/2 \approx 125^\circ$ задаёт направление вектора $\mathbf{G}$ на сфере Блоха кубита (32) при отсчёте от диаметра как показано на рисунке 4.

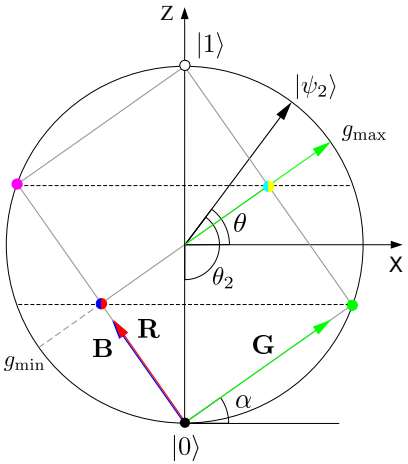


Рис. 4. Кубитное состояние (32), параметризованное симметричным диапазоном полярного угла $\theta \in [-\pi, \pi]$ с помощью замены (31). Показано сечение сферы Блоха плоскостью XZ. Вектора $\mathbf{R}$, $\mathbf{G}$, $\mathbf{B}$ соответствуют главным цветам в аддитивной цветовой модели (20), (22), рисунок 2(а). Серым показан контур цветового куба в соответствии с рисунком 2(б)

Для произвольной фазы ϕ, зависимость от которой остаётся без изменений, коэффициент (33) равен

$$g(\theta_2, \phi) = \frac{\sqrt{2}\sin\theta_2\cos\phi - \cos\theta_2}{\sqrt{3}} = \mathbf{S}_2 \cdot \mathbf{G}, \tag{34}$$

где $\mathbf{S}_2$ есть вектор Стокса чистого состояния (32). Величина (34) имеет максимум $g_{\max} = 1$ в точке $\phi = 0$, $\theta_2 = \alpha + \pi/2 \approx 125°$ и минимум $g_{\min} = -1$ в противоположной точке $\phi = \pi$, $\theta_2 = \pi/2 - \alpha \approx 55°$, как отмечено на рисунке 4. Минимум также показан точкой на рисунке 3(а). Амплитуды остальных цветов по-прежнему получаются из (34) смещением фазы ϕ согласно (28)

$$\begin{aligned} r(\theta_2, \phi) &= g\left(\theta_2, \phi - \frac{2\pi}{3}\right) = \mathbf{S}_2 \cdot \mathbf{R}, \\ b(\theta_2, \phi) &= g\left(\theta_2, \phi - \frac{4\pi}{3}\right) = \mathbf{S}_2 \cdot \mathbf{B}. \end{aligned} \tag{35}$$

Таким образом коэффициенты (25), (28) разложения (23) отображаются на всю поверхность сферы Блоха кубитного состояния (32). Для восьми опорных точек на поверхности сферы (раздел 3) эти коэффициенты в виде вектора $\mathbf{Q} = [r, g, b]^{\mathrm{T}}$ равны

$$\begin{aligned}
\mathbf{Q}_{\mathrm{R}} &= \frac{1}{\sqrt{3}}\begin{bmatrix}1 & -1 & -1\end{bmatrix}^{\mathrm{T}} = -\mathbf{Q}_{\mathrm{C}},\\
\mathbf{Q}_{\mathrm{G}} &= \frac{1}{\sqrt{3}}\begin{bmatrix}-1 & 1 & -1\end{bmatrix}^{\mathrm{T}} = -\mathbf{Q}_{\mathrm{M}},\\
\mathbf{Q}_{\mathrm{B}} &= \frac{1}{\sqrt{3}}\begin{bmatrix}-1 & -1 & 1\end{bmatrix}^{\mathrm{T}} = -\mathbf{Q}_{\mathrm{Y}},\\
\mathbf{Q}_{\mathrm{W}} &= \frac{1}{\sqrt{3}}\begin{bmatrix}1 & 1 & 1\end{bmatrix}^{\mathrm{T}} = -\mathbf{Q}_{\mathrm{K}}.
\end{aligned} \tag{36}$$

Эти вектора лежат в вершинах куба с длиной ребра $2/\sqrt{3}$, вписанного в единичную окружность как показано на рисунках 2(б) и 4.

4.4. Приведение к модели RGB. В силу одинаковой топологии сферические коэффициенты r, g, b (34), (35) соотносятся с компонентами аддитивной цветовой модели RGB на рисунке 2(а) простым геометрическим преобразованием. А именно, сфера единичного радиуса (29) растягивается так, что её поверхность ложится на поверхность куба со стороной 2, тогда как точки касания остаются на своих местах. Это достигается делением всех компонент разложения на модуль наибольшей из них. Полученный куб далее смещается в положительный октант $r, g, b \geqslant 0$ и сжимается вдвое. Полученные величины, лежащие в диапазоне $[0, 1]$, отождествляются с компонентами модели RGB

$$\big[R, G, B\big] = \frac{1}{2}\left(\mathbf{1} + \frac{\big[r, g, b\big]}{\max\{|r|, |g|, |b|\}}\right), \quad 0 \leqslant R, G, B \leqslant 1. \tag{37}$$

При этом вектора (36) преобразуются в стандартные коды восьми основных цветов: $R = (1, 0, 0)$, $G = (0, 1, 0)$, $Y = (1, 1, 0)$ и т. д.

Совместно с (34) и (35), преобразование (37) задаёт взаимооднозначное отображение между кубитными состояниями (32) и цветом в модели RGB. Двумерность чистых кубитных состояния позволяет представить это отображение в виде цветовых карт на рисунке 5.

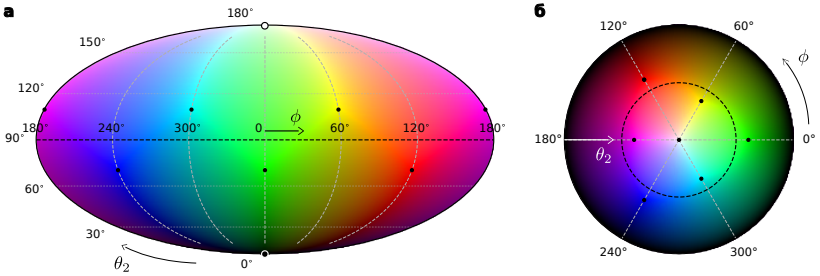


Рис. 5. Цветовая кодировка чистых кубитных состояний (34), (35), (37): а) картографическая проекция сферы Блоха; б) развёртка сферы в круг, при которой угловой и радиальной координатам соответствуют полярный и азимутальный углы кубитного состояния (32). Точками показаны положения основных цветов. Построено с помощью библиотеки Matplotlib версии 3.3.4 [44]

На графике (а) показана картографическая (сохраняющая площадь, Моллвейда) проекция сферы Блоха, при которой северный и южный полюса располагаются на вертикальной оси, а экватор показан горизонтальной прямой. На графике (б) азимутальный угол соответствует угловой координате, а полярный угол - радиальной. Точками показаны главные цвета, пунктиром - экватор сферы Блоха.

5. Смешанные состояния. Чистому кубитному состоянию (23) соответствует матрица плотности

$$\hat{\rho}_2 = |\psi_2\rangle\langle\psi_2| = \begin{bmatrix} \cos^2\dfrac{\theta_2}{2} & \sin\dfrac{\theta_2}{2}\cos\dfrac{\theta_2}{2}e^{i\phi} \\ \sin\dfrac{\theta_2}{2}\cos\dfrac{\theta_2}{2}e^{-i\phi} & \sin^2\dfrac{\theta_2}{2} \end{bmatrix},$$

которая в силу замены (31) приводится к виду

$$\hat{\rho}_2 = \frac{1}{2}\begin{bmatrix} 1-\sin\dfrac{\theta}{2} & \cos\dfrac{\theta}{2}e^{i\phi} \\ \cos\dfrac{\theta}{2}e^{-i\phi} & 1+\sin\dfrac{\theta}{2} \end{bmatrix}, \tag{38}$$

в котором элементы матрицы подчиняются уравнениям (30).

5.1. Переход к смешанным состояниям. Переход к смешанным состояниям производится заменой угловых параметров (31) на компоненты вектора Стокса (5) в соответствии с (7)

$$\sin\frac{\theta}{2} = -\cos\theta_2 \to z,$$
$$\cos\frac{\theta}{2}e^{i\phi} = \sin\theta_2 e^{i\phi} \to x + iy,$$

так что (38) совпадает с матрицей плотности (6). Соответственно, уравнения (30) принимают вид

$$x = \frac{\sqrt{2}}{\sqrt{3}}\left(g - \frac{r+b}{2}\right), \qquad y = \frac{r-b}{\sqrt{2}}, \qquad z = \frac{r+g+b}{\sqrt{3}}. \tag{39}$$

Решение этой системы

$$\begin{aligned} g &= \frac{z + \sqrt{2}x}{\sqrt{3}} = \mathbf{S}_2 \cdot \mathbf{G}, \\ r &= \frac{z - x/\sqrt{2} + \sqrt{3/2}y}{\sqrt{3}} = \mathbf{S}_2 \cdot \mathbf{R}, \\ b &= \frac{z - x/\sqrt{2} - \sqrt{3/2}y}{\sqrt{3}} = \mathbf{S}_2 \cdot \mathbf{B}, \end{aligned} \tag{40}$$

обобщает формулы (34), (35) на весь объём сферы Блоха. Как и раньше, $\mathbf{S}_2$ есть вектор Стокса (5) кодируемого состояния, а $\mathbf{R}, \mathbf{G}, \mathbf{B}$ – единичные рёбра RGB куба, показанные на рисунке 4 соответствующими цветами

$$\mathbf{R} = \begin{bmatrix} \cos\alpha\cos\phi_{\mathrm{R}} \\ \cos\alpha\sin\phi_{\mathrm{R}} \\ \sin\alpha \end{bmatrix}, \ \mathbf{G} = \begin{bmatrix} \cos\alpha\cos\phi_{\mathrm{G}} \\ \cos\alpha\sin\phi_{\mathrm{G}} \\ \sin\alpha \end{bmatrix}, \mathbf{B} = \begin{bmatrix} \cos\alpha\cos\phi_{\mathrm{B}} \\ \cos\alpha\sin\phi_{\mathrm{B}} \\ \sin\alpha \end{bmatrix}. \tag{41}$$

5.2. Компоненты Стокса и матрицы Паули. Согласно решению (40), цветовые амплитуды r, g, b и компоненты x, y, z вектора Стокса связаны операцией поворота, совмещающего обычный базис $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$ (рисунок 1) с базисом (41) кубической цветовой модели, показанным на рисунке 2 и 4

$$\mathbf{Q} = \begin{bmatrix} r \\ g \\ b \end{bmatrix} = \mathbf{U} \cdot \mathbf{S}_2, \qquad \mathbf{U} = \begin{bmatrix} \mathbf{R}^{\mathrm{T}} \\ \mathbf{G}^{\mathrm{T}} \\ \mathbf{B}^{\mathrm{T}} \end{bmatrix}, \tag{42}$$

причём длина вектора сферических цветовых амплитуд равна длине вектора Стокса кодируемого состояния

$$|\mathbf{Q}|^2 = r^2 + g^2 + b^2 = |\mathbf{S}_2|^2 = x^2 + y^2 + z^2.$$

В силу этих свойств цветовую кодировку произвольного кубитного состояния можно представить в матричном виде

$$\hat{\rho} = \frac{1}{2}\begin{bmatrix} 1-z & x+iy \\ x-iy & 1+z \end{bmatrix} = \frac{\hat{\mathbb{I}} + r\hat{\sigma}_r + g\hat{\sigma}_g + b\hat{\sigma}_b}{2} = \frac{\hat{\mathbb{I}} + \mathbf{Q}\cdot\hat{\boldsymbol{\sigma}}_{\mathrm{RGB}}}{2}, \quad (43)$$

где матрицы $\sigma_{r,g,b}$ соответствуют наблюдаемым кубита (32) по направлениям наибольших и наименьших значений цветовых амплитуд, показанных на рисунке 4 для зелёного цвета

$$\begin{aligned} \hat{\sigma}_r &= |r_{\max}\rangle\langle r_{\max}| - |r_{\min}\rangle\langle r_{\min}|\,, \\ \hat{\sigma}_g &= |g_{\max}\rangle\langle g_{\max}| - |g_{\min}\rangle\langle g_{\min}|\,, \\ \hat{\sigma}_b &= |b_{\max}\rangle\langle b_{\max}| - |b_{\min}\rangle\langle b_{\min}|\,. \end{aligned} \quad (44)$$

Выражение (43) аналогично стандартному разложению матрицы плотности кубитного состояния по матрицам Паули [21, раздел 1.7]. Вектор $\hat{\boldsymbol{\sigma}}_{\mathrm{RGB}}$ матриц (44) связан с вектором обычных матриц Паули оператором поворота $\mathbf{U}$ (42).

5.3. Приведение к модели RGB. Сферические коэффициенты (40) приводятся к стандартной RGB модели аналогично случаю чистых состояния в разделе 4.4. Для этого внутренние точки сферы Блоха растягиваются пропорционально своему расстоянию от центра $|\mathbf{Q}| = |\mathbf{S}_2|$, так, что

$$\begin{bmatrix} R, & G, & B \end{bmatrix}^{\mathrm{T}} = \frac{1}{2}\left(\mathbf{1} + \mathbf{Q}\,\frac{|\mathbf{Q}|}{\max\{|r|,|g|,|b|\}}\right). \quad (45)$$

Это выражение обобщает формулу (37).

Совместно с решениями (40), (42) формула (45) задаёт взаимооднозначное отображение между цветом и произвольным кубитным состоянием. При этом каждая точка в шаре Блоха кодируется цветовым вектором (45) в модели цвета RGB и каждому цвету соответствует единственное кубитное состояние. Это отображение показано на рисунке 6(б) в виде цветовых карт четырёх характерных сечений шара Блоха.

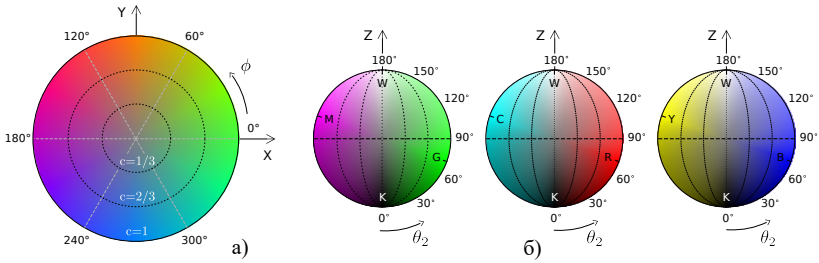


Рис. 6. Цветовая кодировка смешанных кубитных состояний (40), (45): а) экваториальное сечение сферы Блоха; б) вертикальные сечения сферы Блоха, проходящие через три пары противоположных цветов зелёный-фиолетовый, красный-голубой и синий-жёлтый. Пунктиром показаны состояния фиксированной чистоты (47). Построено с помощью Matplotlib 3.3.4 [44]

На графике (а) показано экваториальное сечение $z = 0$ плоскостью XY. На графике (б) показаны вертикальные сечения сферы Блоха, проходящие через три пары противоположных цветов зелёный-фиолетовый ($\phi = 0, \pi$, слева), красный-голубой ($\phi = 2\pi/3, 5\pi/3$, в середине) и синий-жёлтый ($\phi = 4\pi/3, \pi/3$, справа). В каждом сечении также находятся белый (W) и чёрный (K) цвет, лежащие на вертикальной оси Z.

5.4. Соответствие с моделью HSL. На практике интерес представляют цветовые кодировки таких параметров кубитного состояния, как вероятности получения базисных альтернатив, когерентность и фаза. Эти параметры соответствуют параметрам цвета в модели оттенок - насыщенность - светлость (HSL) [26, 27], показанной на рисунке 1(б), следующим образом.

5.4.1. Вероятность исхода «1»: светлость. Как видно из рисунка 6, на диаметре сферы Блоха $x = y = 0$ располагаются серые цвета, на полюсах переходящие в белый и чёрный. Согласно (40), произвольные оттенки серого кодируются равными суперпозициями базисных цветов с весами

$$r = g = b = \frac{z}{\sqrt{3}}, \quad \Leftrightarrow \quad R = G = B = \frac{z+1}{2} = p_1, \tag{46}$$

где правая часть получена посредством отображения (45).

В цветовой модели HSL вероятности $0 \leqslant p_1 \leqslant 1$ исхода 1 соответствует *светлость* цвета, также принимающая значения от 0 до 1. Для произвольного цвета светлость определяется последним равенством (46) и последним уравнением системы (39).

5.4.2. Когерентность: насыщенность (чистота). Заданной когерентности c кубитного состояния соответствуют эллипсоиды вращения, сечения которых для $c = 1/3$ и $c = 2/3$ показаны на рисунке 6 пунктиром. Цветовое выражение когерентности определяется посредством определения (9) и уравнений (39)

$$c\sqrt{p_0 p_1} = \sqrt{\frac{\left(r^2 + g^2 + b^2\right) - (gr + rb + bg)}{6}}. \tag{47}$$

В цветовом теле HSL, рисунок 1(б), эта величина определяет расстояние точки в цветовом теле от серого той же светлости, т.е. чистоту или *цветность* цвета. Относительная величина c соответствует насыщенности цвета, т.е. отношению его цветности к максимально возможной при данной светлости.

Максимальная когерентность кубитных состояний $c = 1$ задаёт поверхность шара Блоха $|\mathbf{Q}| = |\mathbf{S}_2| = 1$. Она же соответствует поверхности цветового тела, содержащей максимально насыщенные, т.е. *чистые* цвета. В этом пределе цветовая кодировка смешанных состояний (40) переходит в кодировку чистых состояний (34), (35), показанную на рисунке 5.

Нулевой когерентности $c = 0$ соответствуют рассмотренные выше оттенки серого на диаметре сферы Блоха. Таким образом переход от классической к квантовой теории вероятности (раздел 2.2) соответствует переходу от чёрно-белого к цветному изображению.

5.4.3. Фаза: цветовой оттенок (тон). Как показано на рисунке 1(а), фаза кубитного состояния ϕ, имеющая смысл только при ненулевой когерентности, определяет направление соответствующего вектора в плоскости XY. Цветовое выражение этой величины находится из уравнений (39) посредством определений (6) и (8):

$$\phi = \arctan\left(\frac{y}{x}\right) = \frac{\sqrt{3}(r - b)}{2g - r - b}. \tag{48}$$

В цветовой модели HSL, рисунок 1(б), этой величине соответствует цветовой *тон* или *оттенок* цвета.

Величины (46), (47), (48) выражены через сферические амплитуды r, g, b, откуда выражения через стандартные коэффициенты R, G, B можно получить посредством отображения (45). В этой форме рассмотренные величины, однако, принимают громоздкий и неудобный для использования вид в силу нелинейности этого отображения, связанной с негладкостью

кубической формы. Тем не менее, представленные выражения численно близки к определениям светлости, насыщенности и тона на основе линейной геометрии цветовых тел [26, 27].

6. Заключение. Формально, представленный результат есть сферическая модель цветового тела, геометрические аналоги которой рассматривались ранее наравне с кубической, конической, цилиндрической и другими формами [45, 46]. Оригинальность этой модели состоит в том, что посредством алгебры кубитных состояний сферическая геометрия цвета связывается с алгоритмами квантовых вычислений и квантово-подобными моделями когнитивной семантики и принятия решений [47, 48]. При этом эмоционально-смысловая функция цвета позволяет интерпретировать эти алгоритмы и модели в категориях естественного мышления. В частности, декартовы координаты X-Y-Z на сфере Блоха (рисунок 1) кодируют эмоционально-смысловые факторы сила – активность – оценка [49], тогда как фазовый параметр ϕ кодирует фазу жизненного цикла деятельности по разрешению базисной неопределённости [40]. Установленное математическое отображение может быть использовано для представления разномодальной информации в этой структуре.

Изоморфизм кубитной структуры с моделями классической и прикладной семиотики позволяет рассматривать её в качестве кванта смысловой информации в естественных когнитивных системах [38, 39]. Имея в виду определение искусственного интеллекта как имитации естественного [50], эта кодировка информации представляется естественным технологическим решением. Этот подход рассматривался как перспективный для развития информационных технологий ещё до установления отмеченных соответствий [51, 52], [53–56]. Полученная разметка пространства кубитных состояний в цветовых и эмоционально-смысловых категориях позволяет использовать её для преодоления современных ограничений при моделировании смысловых аспектов естественного мышления [57–60] и разработки природоподобных информационных систем следующего поколения.

В этой связи встаёт вопрос о сопряжимости такого подхода с существующими алгоритмами ИИ. Элемент такого сопряжения представлен в работе [49], где декартовы оси кубитного смыслового пространства (рисунок 1) найдены в 300-мерном пространстве машинной модели естественного языка. В целом же рассматриваемая сопряжимость обеспечена простым переходом между кубитными состояниями и двоичным кодом: альтернативным состояниям бита соответствуют полюса сферы Блоха, тогда как диаметр между ними соответствует

классической (Колмогоровской) вероятностной модели двоичной неопределённости; сферическое пространство кубитных состояний порождается дополнением этого отрезка фазовой степенью свободы. Таким образом бит является частным случаем представленной кодировки в пределе нулевой когерентности подобно тому, как чёрно-белое зрение является частным случаем цветного в пределе нулевой насыщенности. Переход в природоподобным информационным системам состоит в аналогичном обобщении алгоритмов и вычислительных архитектур.

Литература

1. Налимов В.В. Спонтанность сознания: вероятностная архитектура смыслов и смысловая архитектоника личности. М: Прометей, 1989. 288 с.
2. Петренко В.Ф. Основы психосемантики. М: Эксмо, 2010. 480 с.
3. Кузнецов О.П. Когнитивная семантика и искусственный интеллект // Искусственный интеллект и принятие решений. 2012. № 4. С. 32–42.
4. Кузнецов О.П. Модели голографических процессов обработки информации в нейронных сетях // Автомат. и телемех. 1993. Т. 7. С. 160–172.
5. Дурнев Р.А., Жданенко И.В., Крюков К.Ю. Будущее искусственного интеллекта в спасательном деле // Технологии гражданской безопасности. 2018. Т. 15. № 4. С. 25–29
6. Кудрин В.Б., Хруцкий К.С. Трехзначная логика и троичная информатика Н.П. Брусенцова: их аристотелевские основания // Biocosmology – neo-Aristotelism. 2018. Т. 7. С. 337–388.
7. Bessmertny I., Sukhikh N., Vedernikov Ju., Koroleva Ju. Ternary Logics in Decision Making // Reliability and Statistics in Transportation and Communication. (Eds.: Kabashkin I., Yatskiv I., Prentkovskis O.). 2021. pp. 411–419. DOI: 10.1007/978-3-030-68476-1_38.
8. Васильев В.Н., Павлов А.В. Голографические технологии для систем искусственного интеллекта // Научно-технический вестник информационных технологий, механики и оптики. 2005. Т. 21. № 5. С. 95–99.
9. Aerts D., Czachor M. Cartoon computation: Quantum-like computing without quantum mechanics // J. Phys. A Math. Theor. 2007. vol. 40. no. 13. pp. 259–266. DOI: 10.1088/1751-8113/40/13/F01.
10. Кудряшова Е.С., Михайлова Н.Н., Хусаинов А.А. Моделирование конвейерных и волновых вычислений // Науковедение. 2014. № 1. 12 р.
11. Павельева Е.А. Обработка и анализ изображений на основе использования информации о фазе // Компьютерная оптика. 2018. Т. 42. № 6. С. 1022–1034.
12. Павлов А.В. Начальное порождение понятий при обработке образов на алгебре фурье-дуальных операций // Искусственный интеллект и принятие решений. 2018. С. 84–97.
13. Фоминых И.Б. Инженерия образов, творческие задачи, эмоциональные оценки // Онтология проектирования. 2018. Т. 8. № 2. С. 175–189. DOI: 10.18287/2223-9537-2018-8-2-175-189.
14. Гуц А.К. Основы квантовой кибернетики. Омск: Полиграфический центр КАН, 2008. 204 с.
15. Соловьёв В.М. Квантовые компьютеры и квантовые алгоритмы. Часть 2. Квантовые алгоритмы // Известия Саратовского университета. Серия Математика, Механика,

Информатика. 2016. Т. 16. № 1. С. 104–112. DOI: 10.18500/1816-9791-2016-16-1-104-112.

16. Melnikov A., Kordzanganeh M., Alodjants A.P., Lee R.-K. Quantum Machine Learning: from physics to software engineering // Adv. in Physics X. 2023. vol. 8. no. 1. DOI: 10.1080/23746149.2023.2165452.
17. Manju A., Nigam M.J. Applications of quantum inspired computational intelligence: A survey // Artificial Intelligence Review. 2014. vol. 42. no. 1. pp. 79–156. DOI: 10.1007/s10462-012-9330-6.
18. Bhattacharyya S., Maulik U., Dutta P. Quantum Inspired Computational Intelligence. Morgan Kaufmann, 2017. 506 p. DOI: 10.1016/C2015-0-01859-7.
19. Howard M. Wallman J. Veitch V. Emerson J. Contextuality supplies the 'magic' for quantum computation // Nature. 2014. vol. 510. no. 7505. pp. 351–355. DOI: 10.1038/nature13460.
20. Khrennikov A. Contextuality, Complementarity, Signaling, and Bell Tests // Entropy. 2022. vol. 24. no. 10. pp. 1380. DOI: 10.3390/e24101380.
21. Холево А.С. Математические основы квантовой информатики. Лекционные курсы НОЦ. М: МИАН, 2018. 118 с.
22. Venegas-Andraca S.E., Bose S. Storing, processing, and retrieving an image using quantum mechanic // SPIE Quantum Information and Computation. (Eds.: Donkor E., Pirich A.R., Brandt H.E.). 2003. vol. 5105. DOI: 10.1117/12.485960.
23. Le P.Q., Dong F., Hirota K. A flexible representation of quantum images for polynomial preparation, image compression, and processing operations // Quantum Information Processing. 2011. vol. 10. no. 1. pp. 63–84. DOI: 10.1007/s11128-010-0177-y.
24. Yuan S., Mao X., Xue Y., Chen L., Xiong Q., Compare A. SQR: A simple quantum representation of infrared images // Quantum Inf. Process. 2014. vol. 13. no. 6. pp. 1353–1379. DOI: 10.1007/s11128-014-0733-y.
25. Sang J., Wang S., Li Q. A novel quantum representation of color digital images // Quantum Information Processing. 2017. vol. 16. no. 2. DOI: 10.1007/s11128-016-1463-0.
26. Levkowitz H., Herman G.T. GLHS: A Generalized Lightness, Hue, and Saturation Color Model // CVGIP: Graphical Models and Image Processing. 1993. vol. 55. no. 4. pp. 271–285. DOI: 10.1006/cgip.1993.1019.
27. Tian-Yuan S. The reversibility of six geometric color spaces // Photogrammetric Engineering Remote Sensing. 1995. vol. 61. no. 10. pp. 1223–1232.
28. Iliyasu A.M. Towards realising secure and efficient image and video processing applications on quantum computers // Entropy. 2013. vol. 15. no. 8. pp. 2874–2974. DOI: 10.3390/e15082874
29. Hai S.L., Qingxin Z., Ri G.Z. Multidimensional color image storage, retrieval, and compression based on quantum amplitudes and phases // Information Sciences. 2014. vol. 273. pp. 212–232. DOI: 10.1016/j.ins.2014.03.035.
30. Yan F., Iliyasu A.M., Venegas-Andraca S.E. A survey of quantum image representations // Quantum Information Processing. 2016. vol. 15. no. 1. pp. 1–35. DOI: 10.1007/s11128-015-1195-6.
31. Yan F, Iliyasu A.M., Le P.Q. Quantum image processing: A review of advances in its security technologies. International Journal of Quantum Information. 2017. vol. 15. no. 3. 18 p. DOI: 10.1142/S0219749917300017.
32. Yan F., Li N., Hirota K. QHSL: A quantum hue, saturation, and lightness color model // Information Sciences. 2021. vol. 577. pp. 196–213. DOI: 10.1016/j.ins.2021.06.077.
33. Pridmore R.W. Hue cycle described by graphs and color names // Color Research and Application. 1991. vol. 16. no. 2. pp. 114–121. DOI: 10.1002/col.5080160210.

34. McCamy C.S. The primary hue circle // Color Research and Application. 1993. vol. 18. no. 1. pp. 3–10. DOI: 10.1002/col.5080180104.
35. Li N., Yan F. A single-qubit-based HSL color model for efficient quantum image security applications // Optical and Quantum Electronics. 2022. vol. 54. pp. 1–39. DOI: 10.1007/s11082-022-04078-9.
36. Yan F., Iliyasu A.M., Zhen-Tao L. Bloch Sphere-Based Representation for Quantum Emotion Space // Journal of Advanced Computational Intelligence and Intelligent Informatics. 2019. vol. 19. no. 1. pp. 134–142. DOI: 10.20965/jaciii.2015.p0134.
37. Yan F., Iliyasu A.M., Sihao J. Quantum Structure for Modelling Emotion Space of Robots // Applied Sciences. 2019. vol. 9. no. 16. pp. 3351. DOI: 10.3390/app9163351.
38. Surov I.A. Quantum core affect. Color-emotion structure of semantic atom // Frontiers in Psychology. 2022. vol. 13. DOI: 10.3389/fpsyg.2022.838029.
39. Surov I.A. Natural Code of Subjective Experience // Biosemiotics. 2022. vol. 15. no. 2. pp. 109–139. DOI: 10.1007/s12304-022-09487-7.
40. Суров И.А. Какая разница? Прагматическая формализация смысла // Искусственный интеллект и принятие решений. 2023. № 1. С. 78–89. DOI: 10.14357/20718594230108.
41. Baumgratz T., Cramer M., Plenio M.B. Quantifying coherence // Physical Review Letters. 2014. vol. 113. no. 14. DOI: 10.1103/PhysRevLett.113.140401.
42. Warmuth M.K., Kuzmin D. Bayesian generalized probability calculus for density matrices // Machine Learning. 2010. vol. 78. no. 1-2. pp. 63–101. DOI: 10.1007/s10994-009-5133-7.
43. Fedorov A.K., Kiktenko E.O. Quaternion Representation and Symplectic Spin Tomography // Journal of Russian Laser Research. 2013. vol. 34. no. 5. pp. 477–487. DOI: 10.1007/s10946-013-9378-z.
44. Hunter J.D. Matplotlib: A 2D graphics environment // Computing in Science Engineering. 2007. vol. 9. no. 3. pp. 90–95. DOI: 10.1109/MCSE.2007.55.
45. Kuehni R.G. Color Space and Its Divisions. Color Order from Antiquity to the Present. New Jersey: Wiley-Interscience, 2003. 408 p.
46. Rossi M., Buratti G. The Architecture of Color: Number and Shapes as Measurement and Representation Tools // Nexus Network Journal. 2015. vol. 17. no. 2. pp. 547–569. DOI: 10.1007/s00004-015-0243-y.
47. Khrennikov A. Ubiquitous Quantum Structure. From psychology to finance. Springer. 2010. 216 p. DOI: 10.1007/978-3-642-05101-2.
48. Суров И.А. Алоджанц А.П. Модели принятия решений в квантовой когнитивистике (учебное пособие). Санкт-Петербург: Университет ИТМО, 2018. 63 с.
49. Суров И.А. Открытие чёрного ящика: Извлечение семантических факторов Осгуда из языковой модели word2vec // Информатика и автоматизация. 2022. Т. 21. № 5. С. 916–936. DOI: 10.15622/ia.21.5.3.
50. Указ президента Российской Федерации «О развитии искусственного интеллекта в Российской Федерации». 2019. URL: http://www.kremlin.ru/acts/bank/44731.
51. Widdows D., Bruza P. Quantum Information Dynamics and Open World Science // AAAI Spring Symposium: Quantum Interaction. 2007. pp. 126-133.
52. Widdows D., Kitto K., Cohen T. Quantum Mathematics in Artificial Intelligence // Journal of Artificial Intelligence Research. 2021. vol. 72. pp. 1307–1341. DOI: 10.1613/jair.1.12702.
53. Ezhov A.A, Ventura D. Quantum Neural Networks / (Eds.: Kasabov N.) // Future Directions for Intelligent Systems and Information Sciences. Springer. 2000. pp. 213–235. DOI: 10.1007/978-3-7908-1856-7_11.

54. Петренко В.Ф., Супрун А.П. Методологические пересечения психосемантики сознания и квантовой физики. М: УРСС, 2018. 304 с.
55. Кленов Н.В., Кузнецов А.В., Щеголев А.Е., Соловьев И.И., Куприянов М.Ю., Терешонок М.В., Бакурский С.В. Нейрон на основе одного потокового кубита // Физика низких температур. 2019. Т. 45. № 7. С. 898–905.
56. Колесниченко О.Ю., Смолин В.С., Щербаков Д.А., Колесниченко Ю.Ю. Нейросети и понимание работы мозга в квантовом мире // Материалы VIII Международный конференции: Знания – Онтологии – Теории. 2021. С. 112–121.
57. Brachman R.J. Systems that know what they're doing // IEEE Intelligent Systems. 2002. vol. 17. no. 6. pp. 67–71.
58. Samsonovich A., Goldin R.F., Ascoli G.A. Toward a semantic general theory of everything // Complexity. 2009. vol. 16. no. 4. pp. 12–18. DOI: 10.1002/cplx.20293.
59. Райков А.Н. Слабый vs сильный искусственный интеллект // Информатизация и связь. 2020. № 1. С. 81–88. DOI: 10.34219/2078-8320-2020-11-1-81-88.
60. Roli A., Jaeger J., Kauffman S.A. How Organisms Come to Know the World: Fundamental Limits on Artificial General Intelligence // Frontiers in Ecology and Evolution. 2022. vol. 9. DOI: 10.3389/fevo.2021.806283.

Суров Илья Алексеевич — канд. физ.-мат. наук, доцент, научный сотрудник, Университет ИТМО. Область научных интересов: когнитивно-поведенческое моделирование, квантовая семантика. Число научных публикаций — 30. ilya.a.surov@itmo.ru; Кронверкский проспект, 49А, 197101, Санкт-Петербург, Россия; р.т.: +7(812)232-1467.

Поддержка исследований. Исследование выполнено за счёт гранта Российского научного фонда (проект № 20-71-00136).

DOI 10.15622/ia.22.5.9

I.A. SUROV

COLOR CODING OF QUBIT STATES

Surov I.A. **Color Coding of Qubit States.**

Abstract. Difficulties in algorithmic simulation of natural thinking point to the inadequacy of information encodings used to this end. The promising approach to this problem represents information by the qubit states of quantum theory, structurally aligned with major theories of cognitive semantics. The paper develops this idea by linking qubit states with color as fundamental carrier of affective meaning. The approach builds on geometric affinity of Hilbert space of qubit states and color solids, used to establish precise one-to-one mapping between them. This is enabled by original decomposition of qubit in three non-orthogonal basis vectors corresponding to red, green, and blue colors. Real-valued coefficients of such decomposition are identical to the tomograms of the qubit state in the corresponding directions, related to ordinary Stokes parameters by rotational transform. Classical compositions of black, white and six main colors (red, green, blue, yellow, magenta and cyan) are then mapped to analogous superposition of the qubit states. Pure and mixed colors intuitively map to pure and mixed qubit states on the surface and in the volume of the Bloch ball, while grayscale is mapped to the diameter of the Bloch sphere. Herewith, the lightness of color corresponds to the probability of the qubit's basis state «1», while saturation and hue encode coherence and phase of the qubit, respectively. The developed code identifies color as a bridge between quantum-theoretic formalism and qualitative regularities of the natural mind. This opens prospects for deeper integration of quantum informatics in semantic analysis of data, image processing, and the development of nature-like computational architectures.

Keywords: qubit, color, semantic space, affective meaning, quantum information, image processing, quantum, code.

References

1. Nalimov V.V. Spontannost' soznanija: verojatnostnaja arhitektura smyslov i smyslovaja arhitektonika lichnosti [Spontaneity of consciousness: probabilistic architecture of meanings and semantic archinectonics of personality]. M: Prometey, 1989. 288 p. (In Russ.).
2. Petrenko V.F. Osnovy psihosemantiki. [Foundations of psychosemantics]. M: Eksmo, 2010. 480 p. (In Russ.).
3. Kuznetsov O.P. Cognitive semantics and artificial intelligence. Sci. Tech. Inf. Process. 2013. vol. 40. no. 5. pp. 269–276. DOI: 10.3103/S0147688213050067.
4. Kuznetsov O.P. [Models of golographic processes of information processing in neural networks]. Avtomatika i telemehanika – Automatics and telemechanics. 1993. vol. 7. pp. 160–172. (In Russ.).
5. Durnev R.A., Zhdanenko I.V., Krjukov K.Ju. [Future of artificial intelligence in resque practice]. Tehnologii grazhdanskoj bezopasnosti – Civil Security Technology. 2018. vol. 15. no. 4. pp. 25–29. (In Russ.).
6. Kudrin V.B., Hruckij K.S. [N.P. Brusentsov's Three-valued logic and Ternary Computer Science: their Aristotelian foundations]. Biocosmology – neo-Aristotelism. 2017. vol. 7. pp. 337–388. (In Russ.).
7. Bessmertny I., Sukhikh N., Vedernikov Ju., Koroleva Ju. Ternary Logics in Decision Making. Reliability and Statistics in Transportation and Communication. 2021. pp. 411–419. DOI: 10.1007/978-3-030-68476-1_38.

8. Vasil'ev V.N., Pavlov A.V. [Holographic technologies for artificial intelligence systems]. Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki – Scientific and Technical Journal of Information Technologies, Mechanics and Optics. 2005. vol. 21. no. 5. pp. 95–99. (In Russ.).
9. Aerts D., Czachor M. Cartoon computation: Quantum-like computing without quantum mechanics. J. Phys. A Math. Theor. 2007. vol. 40. no. 13. pp. 259–266. DOI: 10.1088/1751-8113/40/13/F01.
10. Kudrjashova E.S., Mihajlova N.N., Husainov A.A. [Modeling of pipeline and wave computations]. Naukovedenie – Science studies. 2014. no. 1. (In Russ.).
11. Pavel'eva E.A. [Image processing and analysis based on the use of phase information]. Komp'juternaja optika – Computer optics. 2018. vol. 42. no. 6. pp. 1022–1034. (In Russ.).
12. Pavlov A.V. [Conceptual thinking generation by patterns processing by algebra of fourier-dual operations]. Iskusstvennyj intellekt i prinjatie reshenij – Artificial intelligence and decision making. 2018. pp. 84–97. (In Russ.).
13. Fominyh I.B. [Mental image engineering, creative problems, emotional evaluations]. Ontologija proektirovanija – Ontology of designing. 2018. vol. 8. no. 2. pp. 175–189. DOI: 10.18287/2223-9537-2018-8-2-175-189. (In Russ.).
14. Guz A.K. Osnovy kvantovoj kibernetiki [Basics of quantum cybernetics]. Omsk: Polygraphic center KAN, 2008. 204 p. (In Russ.).
15. Solovyev V.M. [Quantum Computers and Quantum Algorithms. Part 2. Quantum Algorithms]. Izvestija Saratovskogo universiteta. Serija Matematika, Mehanika, Informatika – News of Saratov University. Mathematics, Mechanics, Computer Science Series. 2016. vol. 16. no. 1. pp. 104–112. DOI: 10.18500/1816-9791-2016-16-1-104-112. (In Russ.).
16. Melnikov A., Kordzanganeh M., Alodjants A.P., Lee R.-K. Quantum Machine Learning: from physics to software engineering. Adv. in Physics X. 2023. vol. 8. no. 1. DOI: 10.1080/23746149.2023.2165452.
17. Manju A., Nigam M.J. Applications of quantum inspired computational intelligence: A survey. Artificial Intelligence Review. 2014. vol. 42. no. 1. pp. 79–156. DOI: 10.1007/s10462-012-9330-6.
18. Bhattacharyya S., Maulik U., Dutta P. Quantum Inspired Computational Intelligence. Morgan Kaufmann, 2017. 506 p. DOI: 10.1016/C2015-0-01859-7.
19. Howard M. Wallman J. Veitch V. Emerson J. Contextuality supplies the 'magic' for quantum computation. Nature. 2014. vol. 510. no. 7505. pp. 351–355. DOI: 10.1038/nature13460.
20. Khrennikov A. Contextuality, Complementarity, Signaling, and Bell Tests. Entropy. 2022. vol. 24. no. 10. pp. 1380. DOI: 10.3390/e24101380.
21. Holevo A.S. Matematicheskie osnovy kvantovoj informatiki. [Mathematical foundations of quantum information]. M: MIAN, 2018. 118 p. (In Russ.).
22. Venegas-Andraca S.E., Bose S. Storing, processing, and retrieving an image using quantum mechanic. SPIE Quantum Information and Computation. 2003. vol. 5105. DOI: 10.1117/12.485960.
23. Le P.Q., Dong F., Hirota K. A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. Quantum Information Processing. 2011. vol. 10. no. 1. pp. 63–84. DOI: 10.1007/s11128-010-0177-y.
24. Yuan S., Mao X., Xue Y., Chen L., Xiong Q., Compare A. SQR: A simple quantum representation of infrared images. Quantum Inf. Process. 2014. vol. 13. no. 6. pp. 1353–1379. DOI: 10.1007/s11128-014-0733-y.
25. Sang J., Wang S., Li Q. A novel quantum representation of color digital images. Quantum Information Processing. 2017. vol. 16. no. 2. DOI: 10.1007/s11128-016-1463-0.

26. Levkowitz H., Herman G.T. GLHS: A Generalized Lightness, Hue, and Saturation Color Model. CVGIP: Graphical Models and Image Processing. 1993. vol. 55. no. 4. pp. 271–285. DOI: 10.1006/cgip.1993.1019.
27. Tian-Yuan S. The reversibility of six geometric color spaces. Photogrammetric Engineering and Remote Sensing. 1995. vol. 61. no. 10. pp. 1223–1232.
28. Iliyasu A.M. Towards realising secure and efficient image and video processing applications on quantum computers. Entropy. 2013. vol. 15. no. 8. pp. 2874–2974. DOI: 10.3390/e15082874.
29. Hai S.L., Qingxin Z., Ri G.Z. Multidimensional color image storage, retrieval, and compression based on quantum amplitudes and phases. Information Sciences. 2014. vol. 273. pp. 212–232. DOI: 10.1016/j.ins.2014.03.035.
30. Yan F., Iliyasu A.M., Venegas-Andraca S.E. A survey of quantum image representations. Quantum Information Processing. 2016. vol. 15. no. 1. pp. 1–35. DOI: 10.1007/s11128-015-1195-6.
31. Yan F, Iliyasu A.M., Le P.Q. Quantum image processing: A review of advances in its security technologies. International Journal of Quantum Information. 2017. vol. 15. no. 3. 18 p. DOI: 10.1142/S0219749917300017.
32. Yan F., Li N., Hirota K. QHSL: A quantum hue, saturation, and lightness color model. Information Sciences. 2021. vol. 577. pp. 196–213. DOI: 10.1016/j.ins.2021.06.077.
33. Pridmore R.W. Hue cycle described by graphs and color names. Color Research and Application. 1991. vol. 16. no. 2. pp. 114–121. DOI: 10.1002/col.5080160210.
34. McCamy C.S. The primary hue circle // Color Research and Application. 1993. vol. 18. no. 1. pp. 3–10. DOI: 10.1002/col.5080180104.
35. Li N., Yan F. A single-qubit-based HSL color model for efficient quantum image security applications. Optical and Quantum Electronics. 2022. vol. 54. pp. 1–39. DOI: 10.1007/s11082-022-04078-9.
36. Yan F., Iliyasu A.M., Zhen-Tao L. Bloch Sphere-Based Representation for Quantum Emotion Space. Journal of Advanced Computational Intelligence and Intelligent Informatics. 2019. vol. 19. no. 1. pp. 134–142. DOI: 10.20965/jaciii.2015.p0134.
37. Yan F., Iliyasu A.M., Sihao J. Quantum Structure for Modelling Emotion Space of Robots. Applied Sciences. 2019. vol. 9. no. 16. pp. 3351. DOI: 10.3390/app9163351.
38. Surov I.A. Quantum core affect. Color-emotion structure of semantic atom. Frontiers in Psychology. 2022. vol. 13. DOI: 10.3389/fpsyg.2022.838029.
39. Surov I.A. Natural Code of Subjective Experience. Biosemiotics. 2022. vol. 15. no. 2. pp. 109–139. DOI: 10.1007/s12304-022-09487-7.
40. Surov I.A. [What is the Difference? Pragmatic Formalization of Meaning]. Iskusstvennyj intellekt i prinjatie reshenij – Artificial intelligence and decision making. 2023. no. 1. p. 78–89. DOI: 10.14357/20718594230108. (In Russ.).
41. Baumgratz T., Cramer M., Plenio M.B. Quantifying coherence. Physical Review Letters. 2014. vol. 113. no. 14. DOI: 10.1103/PhysRevLett.113.140401.
42. Warmuth M.K., Kuzmin D. Bayesian generalized probability calculus for density matrices. Machine Learning. 2010. vol. 78. no. 1-2. pp. 63–101. DOI: 10.1007/s10994-009-5133-7.
43. Fedorov A.K., Kiktenko E.O. Quaternion Representation and Symplectic Spin Tomography. Journal of Russian Laser Research. 2013. vol. 34. no. 5. pp. 477–487. DOI: 10.1007/s10946-013-9378-z.
44. Hunter J.D. Matplotlib: A 2D graphics environment. Computing in Science and Engineering. 2007. vol. 9. no. 3. pp. 90–95. DOI: 10.1109/MCSE.2007.55.
45. Kuehni R.G. Color Space and Its Divisions. Color Order from Antiquity to the Present. New Jersey: Wiley-Interscience, 2003. 408 p.

46. Rossi M., Buratti G. The Architecture of Color: Number and Shapes as Measurement and Representation Tools. Nexus Network Journal. 2015. vol. 17. no. 2. pp. 547–569. DOI: 10.1007/s00004-015-0243-y.
47. Khrennikov A. Ubiquitous Quantum Structure. From psychology to finance. Springer. 2010. 216 p. DOI: 10.1007/978-3-642-05101-2.
48. Surov I.A., Alodjants A.P. Modeli prinjatija reshenij v kvantovoj kognitivistike [Models of decision making in quantum cognition]. Saint-Petersburg: ITMO University, 2018. 63 p. (in Russ.).
49. Surov I.A. [Opening the Black Box: Finding Osgood's Semantic Factors in Word2vec Space]. Informatizacija i svjaz' – Informatics and automation. 2022. vol. 21. no. 5. pp. 916–936. DOI: 10.15622/ia.21.5.3. (In Russ.).
50. Ukaz prezidenta Rossijskoj Federacii «O razvitii iskusstvennogo intellekta v Rossijskoj Federacii» [Decree of the President of the Russian Federation "On the development of artificial Intelligence in the Russian Federation"]. 2019. Available at: http://www.kremlin.ru/acts/bank/44731. (accessed 26.06.2023). (In Russ.).
51. Widdows D., Bruza P. Quantum Information Dynamics and Open World Science. AAAI Spring Symposium: Quantum Interaction. 2007. pp. 126–133.
52. Widdows D., Kitto K., Cohen T. Quantum Mathematics in Artificial Intelligence. Journal of Artificial Intelligence Research. 2021. vol. 72. pp. 1307–1341. DOI: 10.1613/jair.1.12702.
53. Ezhov A.A, Ventura D. Quantum Neural Networks. Future Directions for Intelligent Systems and Information Sciences. Springer. 2000. pp. 213–235. DOI: 10.1007/978-3-7908-1856-7_11.
54. Petrenko V.F., Suprun A.P. Metodologicheskie peresecheniya psihosemantiki soznaniya i kvantovoj fiziki. [Methodological intersections of psychosemantics of consciousness and quantum physics]. M: URSS, 2018. 304 p. (In Russ.).
55. Klenov N.V., Kuznecov A.V., Shchegolev A.E., Solov'ev I.I., Kupriyanov M.Yu., Tereshonok M.V., Bakurskij S.V. [Neuron based on a single flux qubit] Fizika nizkih temperatur – Low Temperature Physics. 2019. vol. 45. no. 7. pp. 898–905. (In Russ.).
56. Kolesnichenko O.Yu., Smolin V.S., Shcherbakov D.A., Kolesnichenko Yu.Yu. [Neural networks and understanding of the brain in the quantum world] Materialy VIII Mezhdunarodnyj konferencii: Znanija – Ontologii – Teorii [ZONT proceedings]. 2021. pp. 112–121. (In Russ.).
57. Brachman R.J. Systems that know what they're doing. IEEE Intelligent Systems. 2002. vol. 17. no. 6. pp. 67–71.
58. Samsonovich A., Goldin R.F., Ascoli G.A. Toward a semantic general theory of everything. Complexity. 2009. vol. 16. no. 4. pp. 12–18. DOI: 10.1002/cplx.20293.
59. Raikov A.N. [Weak vs strong artificial intelligence]. Informatizacija i svjaz' – Informatization and communication. 2020. no. 1. pp. 81–88. (In Russ.). DOI: 10.34219/2078-8320-2020-11-1-81-88.
60. Roli A., Jaeger J., Kauffman S.A. How Organisms Come to Know the World: Fundamental Limits on Artificial General Intelligence. Frontiers in Ecology and Evolution. 2022. vol. 9. DOI: 10.3389/fevo.2021.806283.

Surov Ilya — Ph.D., Associate Professor, Researcher, ITMO University. Research interests: cognitive-behavioral modeling, quantum semantics. The number of publications — 30. ilya.a.surov@itmo.ru; 49A, Kronverksky Av., 197101, St. Petersburg, Russia; office phone: +7(812)232-1467.

Acknowledgements. This research is supported by RNF (grant № 20-71-00136).

Руководство для авторов

Взаимодействие автора с редакцией осуществляется через личный кабинет на сайте журнала «Информатика и автоматизация» http://ia.spcras.ru/. При регистрации авторам рекомендуется заполнить все предложенные поля данных. Подготовка статьи ведется с помощью текстовых редакторов MS Word 2007 и выше или LaTex. Объем основного текста (до раздела Литература) - от 20 до 30 страниц включительно. Переносы разрешены. Номера страниц не проставляются. Основная часть текста статьи разбивается на разделы, среди которых являются обязательными: введение, хотя бы один «содержательный» раздел и заключение. Допускается также мотивированное содержанием и структурой материал а выделение подразделов. В основную часть опускается помещать рисунки, таблицы, листинги и формулы. Правила их оформления подробно рассмотрены на нашем сайте в разделе «Руководство для авторов».

Author guidelines

Interaction between each potential author and the Editorial board is realized through the pesoal account on the website of the journal “Informatics and Automation” http://ia.spcras.ru/. At the registration the authors are requested to fill out all data fields in the proposed form. The submissions should be prepared using MS Word 2007, LaTex. The text of the paper in the main part should not exceed 30 pages. Pages are not numbered; hyphenations are allowed. Certain figures, tables, listings and formulas are allowed in the main section, and their typography is considered in more detail at the journal web.

Signed to print 04.09.2023. Passed for print 01.10.2023.
Printed in Publishing center GUAP.
Address: 67 litera A, B. Morskaya, St. Petersburg, 190000, Russia

Founder and Publisher: SPC RAS.
Address: 39 litera A, 14th Line V.O., St.Peterburg, 199178, Russia.
The journal is registered in the Federal Service for Supervision of Communications, Information Technology, and Mass Media,
Registration Certificate (registration number) ПИ № ФС77-79228 dated September 25, 2020
Subscription Index П5513, Russian Post Catalog

Подписано к печати 05.09.2023. Дата выхода в свет 01.10.2023.
Формат 60×90 1/16. Усл. печ. л. 17,2. Заказ № 347. Тираж 300 экз., цена свободная.
Отпечатано в Редакционно-издательском центре ГУАП.
Адрес типографии: Б. Морская, д. 67, лит. А, г. Санкт-Петербург, 190000, Россия

Учредитель и издатель: СПб ФИЦ РАН.
Адрес учредителя и издателя: 14-я линия В.О., д. 39, лит. А, г. Санкт-Петербург, 199178, Россия
Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций,
свидетельство о регистрации (регистрационный номер) ПИ № ФС77-79228 от 25 сентября 2020 г.
Подписной индекс П5513 по каталогу «Почта России»