УДК 613.86;159.913

К.О. Гнидко, А.Г. Ломако, Р.Б. Жолус

ОБНАРУЖЕНИЕ ВИЗУАЛЬНЫХ КОНТАМИНАНТОВ НА ОСНОВЕ ВЫЧИСЛЕНИЯ ПЕРЦЕПТИВНОГО ХЭША

Гнидко К.О., Ломако А.Г., Жолус Р.Б. **Обнаружение визуальных контаминантов на основе вычисления перцептивного хэша.**

Аннотация. В настоящей работе предлагается подход к обнаружению широкого класса визуальных контаминантов на основе вычисления перцептивных хэшей и формирования эталонной базы данных потенциально опасных мультимедийных объектов для построения автоматической системы защиты потребителей мультимедийного контента от нежелательного воздействия на их психику и сознание.

Ключевые слова: психофизиологические воздействия, суггестия, подпороговые сообщения, скрытые изображения, распознавание образов, компьютерное зрение.

Gnidko K.O., Lomako A.G., Zholus R.B. **Detection of Visual Contaminants on the Basis of Perceptual Hash Calculation.**

Abstract. In this paper we propose an approach to the detection of a wide class of visual contaminants on the basis of visual perceptual hash calculation and formation of a reference database of potentially dangerous media objects for building an automated system to protect consumers of multimedia content from unwanted effects on their psychic and consciousness.

Keywords: psychophiziological affections, suggestion, subliminal messages, hidden images, image recognition, computer vision

1. Введение. Геополитические события последних лет, в частности череда «арабских революций», а также конфликт на Украине однозначно дают понять, что технологии воздействия на сознание окончательно вышли за пределы психологических лабораторий и стали неотъемлемой частью окружающей реальности. Сложно переоценить опасность, которую несет применение подобных технологий против Российской Федерации. Разработка эффективных мер противодействия технологиям манипулирования групповым и массовым сознанием требует всестороннего исследования особенностей психики человека, которые делают такое манипулирование возможным. Особый интерес вызывают те когнитивные искажения, которые не зависят от национальной, культурной, религиозной принадлежности и являются общими для всех представителей вида Homo sapiens.

2. Контаминация сознания как класс когнитивных искажений. Все многочисленные проявления когнитивных искажений могут быть отнесены к двум классам, первый из которых обусловлен незнанием фундаментальных закономерностей бытия или неумением применять эти знания на практике. Ко второму классу когнитивных искажений относятся случаи, когда неосознаваемые или неконтролируемые психические процессы становятся причиной нежелательной реакции индивида. В рамках настоящей работы для обозначения данного

класса ошибок мы будем использовать термин «контаминация сознания» (рисунок 1).

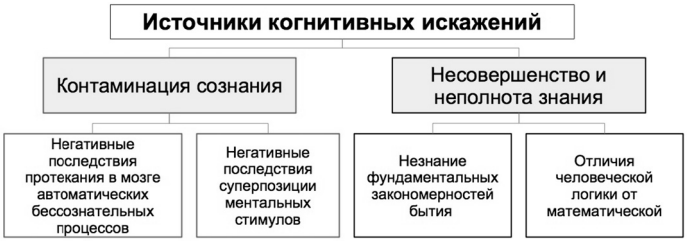

Рис. 1. Источники когнитивных искажений

Согласно английскому толковому словарю «Random House Dictionary» (1968 г.) глагол «to contaminate» означает «становиться грязным или непригодным для употребления в результате контакта или смешивания с чем-либо нечистым, плохим и т.д.» (с. 289). Другими словами, в случае контаминации приемлемое состояние системы становится менее приемлемым (желательным) в результате контакта системы с некоторым потенциально вредоносным агентом. Мы считаем, что многие нежелательные психические процессы и вызванные ими ошибки целесообразно рассматривать как итог воздействия на сознание и подсознание внутренних или внешних агентов-контаминантов.

Более формально определим контаминацию сознания как явление, при котором индивид формирует нежелательное суждение, испытывает нежелательные эмоции или демонстрирует нежелательное поведение вследствие неконтролируемого или бессознательного психического процесса. Под «нежелательным» мы имеем в виду тот факт, что индивид, принимающий решение, сознательно не хотел бы подвергнуться воздействию, которое в конечном счете имело место и повлияло на его решение.

Так, например, большинство преподавателей не хотели бы завышать или занижать оценки своим студентам, поддавшись влиянию своего личного субъективного отношения к ним (из-за внешнего вида, национальной принадлежности или, например, политических предпочтений). Напротив, желательной является ситуация, когда оценка является объективным отражением уровня знаний обучаемого. Однако многочисленные исследования (в частности, [1]) показали, что эффект негативного влияния сторонних факторов, не относящихся к уровню знаний обучаемого (так называемый «гало-эффект»), имеет место практически всегда. Большинство людей сознают, что реклама чаще

всего предоставляет необъективную, а порой и заведомо ложную информацию о продукте. Поэтому покупатели предпочитают, чтобы их решение о приобретении какого-либо товара не было бы инициировано просмотренной рекламой. В то же время множество примеров показывают, что в реальной жизни происходит обратное и реклама сильнейшим образом воздействует на конечное решение потенциальных потребителей [2–4].

Аналогия контаминации сознания с физическим загрязнением полезна по двум причинам. Во-первых, она подчеркивает тот факт, что сохранить «стерильность» сознания практически невозможно. При этом в реальной жизни вернуть загрязненную субстанцию в исходное «чистое» состояние как минимум непросто, а зачастую и вовсе невозможно, что, как мы полагаем, является вполне подходящей метафорой и для ментальных процессов. Контаминации сознания сложно избежать про ряду причин: неполнота знаний о законах функционирования сознания, ограниченная возможность контроля процессов, происходящих в сознании и подсознании, сложность (порой невозможность) обнаружения признаков протекания нежелательного ментального процесса.

Все проявления контаминации, в свою очередь, можно условно разделить на два типа. К первому типу относятся результаты некорректной автоматической обработки информации в сознании и подсознании индивида. Ко второму типу – последствия суперпозиции ментальных стимулов, порожденных памятью, мышлением, ощущениями, суждениями. В повседневной жизни реакции людей практически всегда определяются множеством совокупно действующих стимулов, так же, например, как оценка кандидата на вакантную должность складывается из множества факторов. Вместе с тем, большое количество проведенных исследований позволяют утверждать, что люди крайне редко способны корректно подвергнуть критическому анализу свои реакции и определить точный вклад каждого из факторов в итоговое суждение. Обычно индивид может только осознать саму мысль или ощущение, но не причины, их породившие [5, 6]. Данный эффект происходит автоматически, без контроля со стороны сознания [7], что имеет свои негативные стороны. В частности, изучение эффекта предшествования (прайминга) показало, что образы в памяти и соответствующие им модели поведения могут быть инициированы визуальной информацией, не имеющей прямого отношения к текущей ситуации.

3. Применение перцептивного хэша для автоматического обнаружения визуальных контаминантов. Мы вводим термин «ви-

зуальные контаминанты», в отношении изображений (в том числе последовательностей изображений, составляющих видеоряд), просмотр которых может приводить к нежелательному изменению мыслительных процессов и поведенческих реакций. К визуальным контаминантам могут быть отнесены, в частности, скрытые подпороговые вставки по типу «25 кадра», логотипы компаний-производителей, внедряемые в видеоряд в целях увеличения продаж, символика политических движений и т.д. В настоящей работе предлагается подход к обнаружению широкого класса визуальных контаминантов на основе вычисления перцептивных хэшей и формирования эталонной базы данных потенциально опасных мультимедийных объектов для построения автоматической системы защиты потребителей мультимедийного контента от нежелательного воздействия на их психику и сознание.

Перцептивные хэш-алгоритмы применяются для генерации на основе различных характеристик изображения индивидуальных (но не уникальных) «отпечатков» — хэшей [8]. В отличие от хэш-функций, применяемых в криптографии, перцептивные хэши можно сравнивать между собой и делать вывод о степени различия двух наборов данных (рисунок 2).

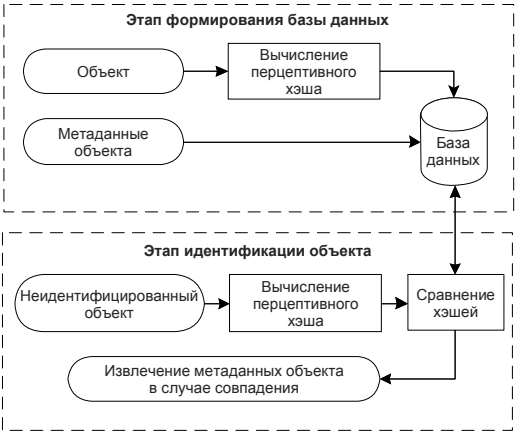

Рис. 2. Схема идентификации изображений на основе перцептивных хэшей

Перцептивные хэши устойчивы по отношению к таким преобразованиями изображений как изменение размера, изменение соотношения сторон, коррекция цветовых характеристик и незначительное вращение [9]. Данное свойство перцептивных хэшей обеспечивает обнаружение не только идентичных кадров, причем в различном разрешении, но и «похожих» с точки зрения человека образов: например,

различных картинок из одного фотосета, символов, логотипов компаний – производителей порнографической продукции. Перцептивные хэши могут успешно применяться и для обнаружения скрытых визуальных вставок в видеопотоке.

Для вычисления перцептивного хэша могут использоваться различные функции. Определим требования к ним, исходя из целевого предназначения. Введем следующие обозначения.

Пусть H — хэш-функция, которая принимает на вход объект (например, изображние) и возвращает битовую строку длины d;

x — мультимедийный объект;

$\hat{x}$ — модифицированный мультимедийный объект, перцептивно схожий с объектом x;

y — мультимедийный объект, перцептивно несхожий с x;

x' и y′ — значения перцептивных хэшей объектов x и y соответственно;

$\{0,1\}^d$ — бинарная строка длины d.

Функция перцептивного хэширования должна обладать следующими свойствами:

1. Равномерное распределение значений хэша:

$$P(H(x) = x') \approx \frac{1}{2^d}, \forall x' \in \{0,1\}^d.$$

2. Взаимная независимость для перцептивно несхожих объектов:

$$P(H(x) = x' | H(y) = y') \approx P(H(x) = x', \forall x', y' \in \{0,1\}^d.$$

3. Инвариантность относительно перцептивно схожих объектов x и $\hat{x}$:

$$P(H(x) = H(\hat{x})) \approx 1.$$

4. Высокая чувствительность к перцептивно несхожим объектам:

$$P(H(x) = H(y)) \approx 0.$$

Приведем краткое описание алгоритмов вычисления перцептивного хэша, удовлетворяющих перечисленным требованиям и наиболее часто применяемым на практике.

1. Дискретное косинусное преобразование. Пусть $x[m], m = 0, \dots, N-1$ — последовательность отсчетов сигнала длины N. Тогда дискретное косинусное преобразование:

$$X[n] = \sum_{m=0}^{N-1} c\,[n, m] \cdot x[m],$$

где матрица дискретного косинусного преобразования:

$$c[n,m] = \sqrt{\frac{2}{N}} \cdot cos\left(\frac{(2m+1)\cdot n\pi}{2N}\right), (m,n = 0,\dots,N-1).$$

Матрица $c[n,m]$ может быть вычислена заранее для любого заданного числа N, что существенно повышает скорость вычисления хэшей в случае программной реализации алгоритма.

2. Лапласиан гауссиана. Пусть $f_c(x,y)$ — функция яркости изображения в градациях серого. Тогда непрерывный лапласиан функции:

$$\nabla^2 f_c(x,y) = \nabla \cdot \nabla f_c(x,y) = \frac{\partial^2 f_c(x,y)}{\partial x^2} + \frac{\partial^2 f_c(x,y)}{\partial y^2}.$$

Фильтр Гаусса:

$$g_c(x,y) = e^{-\frac{x^2+y^2}{2\sigma^2}}.$$

Лапласиан гауссиана:

$$h_c(x,y) = \nabla^2 g_c(x,y) = \frac{x^2+y^2-2\sigma^2}{\sigma^4} \cdot e^{-\frac{x^2+y^2}{2\sigma^2}}.$$

Свертка лапласиана гауссиана с изображением:

$$[\nabla^2 g_c(x,y)] * f_c(x,y)] = \nabla^2[f_c(x,y) * g_c(x,y)].$$

3. Лучевой вектор дисперсии. Идея применения данного алгоритма состоит в построении лучевого вектора дисперсии на основе преобразования Радона, после чего к полученному вектору применяется дискретное косинусное преобразование и вычисляется хэш [10].

Пусть $I(x,y)$ — значение яркости пиксела изображения (x, y), тогда лучевой вектор дисперсии $R[\alpha]$:

$$R[\alpha] = \frac{\sum_{(x,y\in\Gamma(\alpha))} I^2(x,y)}{|\Gamma(\alpha)|} - \left(\frac{\sum_{(x,y\in\Gamma(\alpha))} I(x,y)}{|\Gamma(\alpha)|}\right)^2,$$

где угол поворота вектора проекции $\alpha = 0,1,\dots,179$; $|\Gamma(\alpha)|$ — мощность множества пикселей на линии проекции, соответствующей данному углу.

4. Вычисление хэша на основе средних значений низкочастотных характеристик изображения. Рассмотрим данный алгоритм подробнее в качестве примера. Основные шаги алгоритма описаны ниже:

Шаг 1. Удаление цветовой составляющей. Изображение конвертируется из исходного цветового пространства в градации серого.

Шаг 2. Уменьшение размера изображения для удаления высокочастотных компонент и сохранения низкочастотных. Выходной размер изображений может варьироваться (в приводимом примере используется значение 16 пикселей). Таким образом, общее число пикселей изображения после преобразования составляет $16 \times 16 = 256$ пикселей. Полученный после преобразования хэш будет соответствовать всем вариантам изображения, независимо от исходного размера и соотношения сторон (рисунок 3).

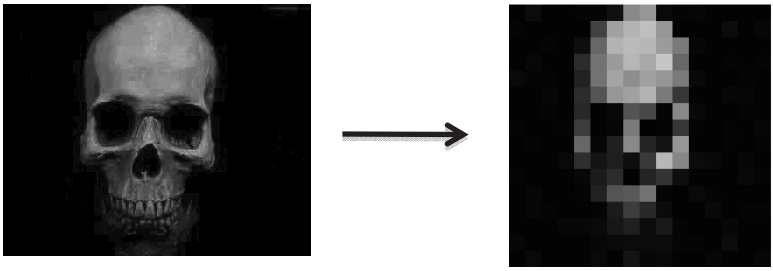

Рис. 3. Удаление высокочастотных компонент за счет уменьшения изображения

Шаг 3. Вычисление среднего значения. Для всех полученных значений градаций серого (в рассматриваемом примере - 256) рассчитывается арифметическое среднее значение.

Шаг 4. Бинаризация изображения. Для каждого пиксела изображения в градациях серого осуществляется сравнение с порогом - средним значением, вычисленным на предыдущем шаге алгоритма. Если значение пиксела превышает порог, значение пикселя заменяется на 1, в противном случае на 0 (рисунок 4).

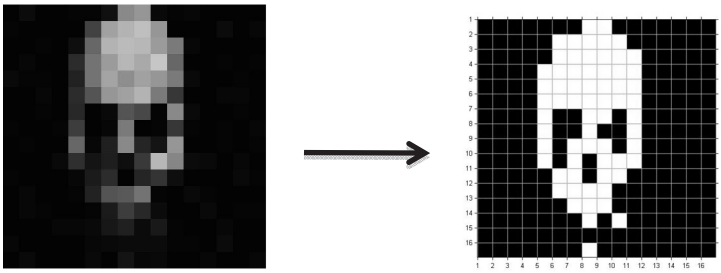

Рис. 4. Пороговая бинаризация изображения

Шаг 5. Построение хэша. Бинаризованное изображение 16×16 пикселей преобразуется в одно 256-битное значение или его 16-ричное представление. Порядок пикселей при этом не имеет значения, если он сохраняется постоянным (в применяемом алгоритме биты считываются слева направо, сверху вниз). В приведенном примере перцептивный хэш изображения черепа представлен двоичной последовательностью:

0000000110000000000001111100000000000111111000000000111111100
0000000111111100000000011111110000000000100110100000000010010010
0000000001011101000000000101011100000000001101100000000000011
1100000000000001110000000000000010100000000000000000000000000000
000100000000

или в шестнадцатеричном виде:

0x18007C007E00FE00FE00FE009A009200BA00AE006C0078003800140
00000100.

Для вычисления меры схожести между двумя изображениями в рассматриваемом алгоритме вычисляется расстояние Хэмминга между соответствующими хэшами:

Пусть A — алфавит конечной длины. $x = (x_1, x_2, \dots, x_n)$ и $y = (y_1, y_2, \dots, y_n)$ — строки символов одинаковой длины, где x, y ∈ A. Тогда расстояние Хэмминга Δ между x и y:

$$\Delta(x, y) = \sum_{x_i \neq y_i} 1\,, i = 1,2, \dots, n.$$

Нормированное расстояние хэмминга:

$$\Delta_{\mathrm{n}}(x, y) = \frac{1}{n} \sum_{x_i \neq y_i} 1\,, i = 1,2, \dots, n,$$

где n — длина сравниваемых строк.
Расстояние Хэмминга, таким образом, равно числу позиций, в которых векторы бинарных хэшей различны.

Продемонстрируем эффективность применения алгоритма, построенного на вычислении перцептивных хэшей, для автоматического обнаружения похожих изображений. Рассмотрим схожие между собой пары изображений, отличающиеся, тем не менее, размерами, соотношением сторон и отдельными деталями (рисунок 5).


Bear1.jpg


Bear2.jpg


Mouse1.jpg


Mouse2.jpg

Рис. 5. Исходные изображения для сравнения на основе перцептивного хэша

Соответствующие данным изображениям значения хэша на основе средних значений среднечастотных характеристик и расстояния Хэмминга между ними приведены в таблице 1.

Таблица 1. Расстояние Хэмминга между изображениями

Наименование изображения	Значение хэша	Расстояние Хэмминга			
		Bear1	Bear2	Mouse1	Mouse2
Bear1	FFFFF8FFF2C3F013F007E3C7F387F80FF01FEF1FCF1FCF0FF20FF81FFE1FFFFF	0	27	82	81
Bear2	FFFFF0C7F043F003E10FE3C7F38FF81FF01FE01FC80FE00FF00FF80FFE1FFFFF	27	0	71	74
Mouse1	FDFFF0C7F047FDC7F8DFF93FFC1FE03FE29FE19FF13FF83FFA7FCCFFFFE7FF80	82	71	0	43
Mouse2	FDFFF8CFF80FFDCFFC3FFC7FFC3FF07FF63FF1BFF87FFC7FFE3FE47FFBDFFF3F	81	74	43	0

Установив пороговое значение для расстояния Хэмминга, можно в автоматическом режиме делать вывод о близости анализируемого изображения к заданному эталону. Так, например, установив пороговое значение 50, получим вывод о том, что из четырех представленных изображений похожи между собой Bear1 и Bear2 (27<50), а также Mouse1 и Mouse2 (43<50), что, очевидно, соответствует действительности.

4. Применение перцептивных хэшей для обнаружения скрытых подпороговых вставок в видеопотоках. В настоящее время о сведения о наличии в Российской Федерации и за рубежом действующих систем технического мониторинга каналов сети Интернет в интересах защиты от скрытой передачи вредоносной информации в открытых источниках носят единичный и отрывочный характер. Их наиболее близким аналогом является прибор ОДСВ-1 (опытный детек-

тор скрытых вставок), разработанный в 2002 году ВНИИТР совместно с Национальным исследовательским центром телевидения и радио по заказу Министерства РФ по делам печати, телерадиовещания и средств массовых коммуникаций [11]. ОДСВ-1 производит запись телевизионных программ на видеопленку, после чего осуществляет в них поиск видеовставок типа «25 кадра». Решение о вредоносности выявленных вставок выносится экспертной группой при последующем просмотре. Очевидным недостатком описанного подхода является низкая оперативность и производительность.

Известны также подходы, основанные на анализе функции интегральной яркости кадров изображения в зависимости от времени (номера кадра) и поиске локальных аномалий на графике такой функции. В качестве основного признака, позволяющего выявить наличие скрытых вредоносных вставок в видеоданных, рассматривается суммарная яркость пикселов отдельного кадра. Под скрытой визуальной вставкой понимается кадр, содержащий зрительные образы, которые должны оказывать какое-либо воздействие на человека. Для того, чтобы человек смог подвергнуться такому воздействию, кадр-вставка должна отличаться и от предыдущего, и от следующего. При этом время демонстрации скрытого кадра не должно превышать 113 мс, иначе он будет сознательно восприниматься зрителем. Для обнаружения кадра-вставки вводится вспомогательная функция, которая вычисляет отличие яркости текущего кадра от последующего по абсолютному значению. Кадры, в которых за одним скачком значения функции следует другой, помечаются как подозрительные на наличие визуальной вставки в видеопотоке.

Логическим развитием метода вычисления интегральной яркости является алгоритм обнаружения кадров-вставок на основе вычисления кадра-разности, под которым понимается результат попиксельного вычитания текущего и последующего кадров. Те области, в которых соседние кадры имеют одинаковые области изображения, при попиксельном вычитании дают в результирующем кадре черные участки. Там же, где есть отличия, появляется область, имеющая цветовую окраску. Таким образом, если два кадра представляют собой обычную последовательность фильма, то кадры-разности содержат незначительные светлые участки, которые образуются в результате движения объектов на экране. При наличии скрытой визуальной вставки результирующий кадр-разность содержит обширные цветные участки, увеличивающие суммарную дифференциальную яркость.

Принцип работы алгоритма выявления видеовставки по экстремумам суммарной дифференциальной яркости видеокадров изображен на рисунке 6.

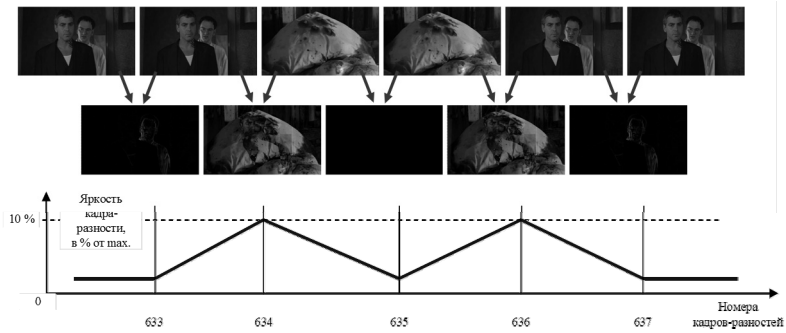

Рис. 6. Принцип работы алгоритма выявления видеовставки по экстремумам суммарной дифференциальной яркости видеокадров

Из последовательности видеокадров (верхний ряд) формируются кадры-разности (нижний ряд). Суммарная дифференциальная яркость кадров-разностей, в формировании которых были задействованы скрытые визуальные вставки, значительно превосходит соседние. Таким образом, визуальные вставки могут быть выявлены по экстремумам функции суммарной дифференциальной яркости. П-образные экстремумы характерны для визуальных вставок из одного кадра, а М-образные – для вставок двух-трех кадров.

Основным достоинством изложенного подхода является простота реализации и относительно низкая вычислительная сложность. К недостаткам следует отнести большое количество ложных срабатываний в моменты смены ракурса, высокую чувствительность метода к резким перепадам яркости (вспышка молнии, выстрел). При этом окончательное решение о наличии вредоносной вставки может быть сделано только экспертным путем.

Методы анализа кадров видеопотока, основанные на вычислении особых точек и дескрипторов изображения (SURF, SIFT и другие), устойчивы к различным искажениям и деформациям, однако существенно более ресурсоемки и, в большинстве своем, применяют защищенные патентным законодательством проприетарные алгоритмы и программные модули. Результаты проведенных нами экспериментальных исследований позволяют утверждать, что при наличии обширной базы заранее проиндексированных материалов соотношение точности

и скорости распознавания скрытых кадров-вставок в видеопотоках на основе вычисления перцептивных хэшей являются оптимальными.

В качестве примера рассмотрим фрагмент раскадровки музыкального видеоклипа, в котором присутствует скрытая полнокадровая вставка с изображением черепа (рисунок 7). Время демонстрации скрытой вставки при проигрывании клипа составляет 1/25 секунды, что не позволяет зрителю без специальной тренировки обнаружить и распознать предъявляемый таким образом эмоционально значимый символ.

кадр 136	кадр 137	кадр 138	кадр 139	кадр 140

Рис. 7. Музыкальный клип с видеовставкой

Технические характеристики анализируемого видеофайла представлены в таблице 2.

Таблица 2. Технические характеристики анализируемого видеофайла

Параметр	Значение
Формат видео:	Audio Video Interleave
Размер файла:	1,99 Мб
Длительность:	8,4 сек
Битрейт:	1 983 кБит/сек
Ширина кадра:	352 пикселов
Высота кадра:	288 пикселов
Частота демонстрации кадров:	25 кадров в секунду
Стандарт вещания:	PAL
Цветовое пространство:	YUV
Глубина цвета:	8 бит
Тип кодека:	DivX 5.1.1 (Maupiti)

Идея автоматического выявления скрытой полнокадровой вставки заключается в обнаружении единичного кадра, который перцептивно отличается как от последовательности кадров до него, так и от кадров после него. Такой кадр с высокой вероятностью является искусственно внедренным в видеопоток изображением. Для обнаружения скрытой вставки вычислим значения перцептивных хэшей всех кадров и значения расстояния Хэмминга между последовательными парами хэшей. Результат представлен в виде столбчатой диаграммы на рисунке 8. Два характерных пика на диаграмме говорят о наличии кадра (кадр №138), чей хэш «далек» от хэшей кадров, предшествую-

щих ему и следующих за ним. Данный факт позволяет строить автоматические распознаватели с настраиваемым порогом срабатывания и обнаруживать скрытые вставки в режиме времени, близком к реальному.

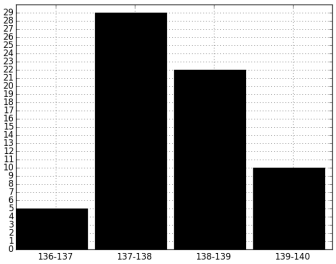

Рис. 8. Значения расстояния Хэмминга между парами хэшей кадров видеопотока, содержащего полнокадровую вставку

Важной задачей исследования является определение порогового значения расстояния Хэмминга, при котором кадр считается «отличным» от предыдущего и следующего за ним изображений. В общем случае установление порогового значения зависит от ценности защищаемого ресурса (значимости ошибок первого и второго рода), наличия сведений об априорной вероятности, появления фильтруемого контента в видеопотоке, и требований, предъявляемых к разрабатываемой системе фильтрации нежелательного видеоконтента. Сочетание данных факторов позволяет в каждом конкретном случае обоснованно применять различные статистические критерии выбора порогового значения (минимаксный критерий, критерий идеального наблюдателя и прочие).

В рамках проведенных авторами экспериментальных исследований для определения порога срабатывания программного фильтра применялся критерий Неймана-Пирсона с заданным максимальным значением вероятности ложного срабатывания $P = 0{,}1$. Исходные данные для проведения статистического эксперимента (фрагменты видеофайлов с кадрами-вставками и без них) были подготовлены с применением библиотеки компьютерного зрения OpenCV и функционально ориентированного языка программирования python. Полученные значения обработаны с помощью пакета Statistics Toolbox из состава среды инженерных вычислений Matlab. Результаты эксперимента представлены на рисунке 9.

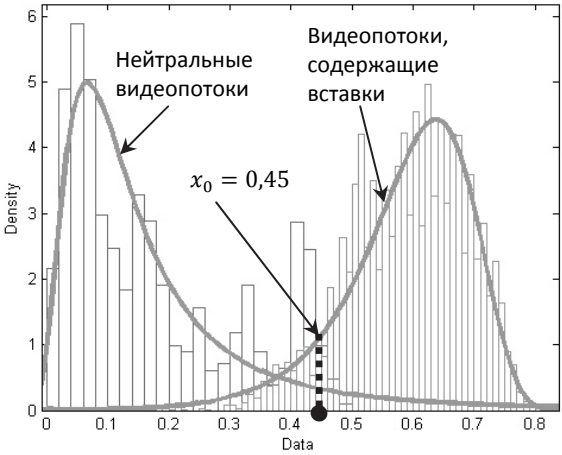

Рис. 9. Наложение гистограмм и графиков функций плотности распределения случайной величины – нормированного расстояния Хэмминга

Анализируемой случайной величиной являлось нормированное расстояние Хэмминга между соседними кадрами в видеопотоках. По оси абсцисс отложены значения рассматриваемой безразмерной случайной величины (от 0 до 1). Полученная точечная оценка позволяет установить следующий порог дифференцирования кадров:

$$x_0 = 0{,}45.$$

При этом вероятность ложных срабатываний в соответствии с критерием Неймана-Пирсона не превысит требуемой величины 0,1.

Избирательность фильтра в отношении кадров, которые не являются контаминантами, но существенно отличаются от соседних кадров видеоряда (например, смена сюжетного плана, склейка через пустой кадр), достигается добавлением в решающее правило дополнительных условий. Так, например, необходимым условием для принятия решения о наличии единичного скрытого кадра-вставки является последовательность из двух подряд идущих пиков на графике расстояния Хэмминга между парами хэшей, поскольку кадр-вставка должен существенно отличаться от соседних с ним изображений. В свою очередь, обычная смена плана приводит к появлению единичного пика на графике, что позволяет дифференцировать данные случаи. Несколько более сложной представляется задача правильного распознавания дефектов монтажа изображения. Однако и в данном случае мо-

жет быть предложено решение, основанное на сравнении хэша кадра, подозрительного на наличие визуального контаминанта, с хэшем «типового» дефекта, такого как пустой «черный» или «засвеченный» кадр.

Нейтрализация вредоносного воздействия обнаруженных скрытых кадров-вставок при условии сохранения целостности протокола передачи видеопотока может быть обеспечена путем дублирования вместо кадра-вставки предыдущего или последующего кадров из анализируемой последовательности. Однако детальное рассмотрение подходов к нейтрализации визуальных контаминантов выходит за рамки настоящей работы и является целью дальнейших исследований.

5. Заключение. Таким образом, применение перцептивного хэширования позволяет автоматизировать процесс идентификации «похожих» с точки зрения человека визуальных образов и создать базу данных хэшей потенциально опасных изображений, способных оказать нежелательное воздействие на психику и сознание. Простота реализации и относительно невысокая вычислительная сложность алгоритмов, реализующих перцептивное хэширование, делают возможным построение автоматических систем распознавания нежелательного мультимедийного контента. Вместе с тем, визуальные контаминанты являются наиболее широким, но не единственным источником суперпозиции стимулов, порождающих контаминацию сознания. Иные типы контаминантов (текстовые, аудио и т.д.) требуют разработки других подходов в рамках общей методологии распознавания образов и машинного обучения.

Противодействие контаминации второго типа, вызванной некорректной автоматической обработкой информации в сознании и подсознании индивида, с неизбежностью требует разработки моделей (в том числе динамических) индивидуального, группового и массового сознания, что является темой дальнейших исследований и публикаций.

Литература

1. *Landy D., Sigall H.* Beauty is talent: Task evaluation as a function of performer's phisical attractiveness // J. Personal. Soc. Physiol. 1974. vol. 29. pp. 299–304.
2. *Abraham M.M., Lodish L.M.* Getting the most out of advertising and promotion // Harv. Bus. Rev. 1990. vol. 68. pp. 50–58.
3. *Liebert R.M., Sprafkin J.* The early window // Elmsford. NY: Pergamon Press. 1988. Issue 3.
4. *Ryan B.J.* It works! How investment spending to adevrtising pays off // New York: 1991.
5. *Nisbett R.E., Wilson T.D.* Telling more than we can know: Verbal reports on mental processes. // Psychol. Rev. 1977. vol. 84. no. 3. 231 p.

6. *Wilson T.D. et al.* Introspection, attitude change, and attitude-behavior consistency: The disruptive effects of explaining why we feel the way we do // Orlando. FL: Academic Press. 1989. vol. 19. pp. 123-205.
7. *Bargh J.A.* Conditional automaticity: Varieties of automatic influence in social perception and cognition // Unintended thought. 1989. vol. 3. pp. 51–69.
8. *Beghdadi A. et al.* A survey of perceptual image processing methods // Signal Process. Image Commun. 2013. vol. 28. pp. 811–831.
9. *Wen Z.K. et al.* A robust and discriminative image perceptual hash algorithm // Proceedings of the 4th International Conference on Genetic and Evolutionary Computing (ICGEC 2010). 2010. pp. 709–712.
10. *Lei Y., Wang Y., Huang J.* Robust image hash in Radon transform domain for authentication // Signal Process. Image Commun. 2011. vol. 26. pp. 280–288.
11. *Паукова М.* Изобретен прибор для обнаружения 25-го кадра. URL: https://www.urfo.org/ekb/13_45277.html (дата обращения: 10.03.2015).

References

1. Landy D., Sigall H. Beauty is talent: Task evaluation as a function of performer's phisical attractiveness. *J. Personal. Soc. Physiol*. 1974. vol. 29. pp. 299–304.
2. Abraham M.M., Lodish L.M. Getting the most out of advertising and promotion. *Harv. Bus. Rev.* 1990. vol. 68. pp. 50–58.
3. Liebert R.M., Sprafkin J. The early window. Elmsford. NY: Pergamon Press. 1988. Issue 3.
4. Ryan B.J. It works! How investment spending to adevrtising pays off. New York: 1991.
5. Nisbett R.E., Wilson T.D. Telling more than we can know: Verbal reports on mental processes. *Psychol. Rev.* 1977. vol. 84. no. 3. 231 p.
6. Wilson T.D. et al. Introspection, attitude change, and attitude-behavior consistency: The disruptive effects of explaining why we feel the way we do. Orlando. FL: *Academic Press*. 1989. vol. 19. pp. 123–205.
7. Bargh J.A. Conditional automaticity: Varieties of automatic influence in social perception and cognition. *Unintended thought*. 1989. vol. 3. pp. 51–69.
8. Beghdadi A. et al. A survey of perceptual image processing methods. *Signal Process. Image Commun*. 2013. vol. 28. pp. 811–831.
9. Wen Z.K. et al. A robust and discriminative image perceptual hash algorithm. Proceedings of the 4th International Conference on Genetic and Evolutionary Computing (ICGEC 2010). 2010. pp. 709–712.
10. Lei Y., Wang Y., Huang J. Robust image hash in Radon transform domain for authentication. *Signal Process. Image Commun*. 2011. vol. 26. pp. 280–288.
11. Paukova M. Izobreten pribor dlya obnaruzheniya 25-go kadra [Device for detection of the hidden 25-th frame is invented]. Available at: https://www.urfo.org/ekb/13_45277.html (accessed: 22.01.2015). (In Russ.).

Гнидко Константин Олегович — к-т техн. наук, докторант, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: информационно-психологическая безопасность, распознавание образов, извлечение знаний из неструктурированных массивов данных. Число научных публикаций — 27. greeny598@gmail.com; ул. Ждановская, 13, 197198, Санкт-Петербург; р.т.: +7(812) 237-19-60.

Gnidko Konstantin Olegovich — Ph.D., doctoral student, Mozhaisky Military Space Academy. Research interests: information-psychological security, image recognition, data mining. The number of publications — 27. greeny598@gmail.com; 13, Zhdanovskaya street, St. Petersburg, 197198, Russia; office phone: +7(812) 237-19-60.

Ломако Александр Григорьевич — д-р техн. наук, профессор кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: информационная безопасность, теоретическое и системное программирование, синтез и верификация корректности моделей программ. Число научных публикаций — 250. lomako_ag@mail.ru; ул. Ждановская 13, 197198, Санкт-Петербург; р.т.: +7(812) 237-19-60.

Lomako Aleksandr Grigor'evich — Ph.D., Dr. Sci., professor of system for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: information security, theoretical and system programming, synthesis and verification of program models. The number of publications — 250. lomako_ag@mail.ru; 13, Zhdanovskaya street, St. Petersburg, 197198, Russia; office phone: +7(812) 237-19-60.

Жолус Роман Борисович — к-т биол. наук, соискатель кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: информационная безопасность; моделирование социальных систем. Число научных публикаций — 10. p.glybovsky@yandex.ru; ул. Ждановская, 13, Санкт-Петербург, 197198; р.т.: +7(812) 237-19-60.

Zholus Roman Borisovich — Ph.D., applicant of system for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: information security, modeling social systems. The number of publications — 10. p.glybovsky@yandex.ru; 13, Zhdanovskaya street, St. Petersburg, 197198, Russia; office phone: +7(812) 237-19-60.

РЕФЕРАТ

Гнидко К.О., Ломако А.Г., Жолус Р.Б. **Обнаружение визуальных контаминантов на основе вычисления перцептивного хэша.**

Контаминацией сознания называется ситуация, когда неосознаваемые или неконтролируемые психические процессы становятся причиной нежелательной реакции индивида. Все проявления контаминации можно условно разделить на два типа. К первому типу относятся результаты некорректной автоматической обработки информации в сознании и подсознании.

Ко второму типу – последствия суперпозиции ментальных стимулов, порожденных памятью, мышлением, ощущениями, суждениями. Контаминацию второго типа могут вызывать подпороговые вставки, логотипы компаний-производителей, эмоционально значимые символы и другие визуальные образы. В настоящей работе предлагается подход к обнаружению визуальных контаминантов на основе вычисления перцептивных хэшей и формирования эталонной базы данных потенциально опасных мультимедийных объектов. Устойчивость перцептивных хэшей к некоторым видам преобразований обеспечивает обнаружение не только идентичных кадров но и «похожих» с точки зрения человека изображений. Рассматриваются алгоритмы перцептивного хэширования, основанные на вычислении средних значений низкочастотных характеристик изображения, вычислении лапласиан гауссиана, вектора лучевой дисперсии, дискретном косинусном преобразовании. Приводится пример применения перцептивного хэширования для обнаружения скрытых подпороговых вставок в видеопотоке.

Противодействие контаминации, вызванной некорректной автоматической обработкой информации в сознании и подсознании индивида, является темой дальнейших исследований и требует разработки моделей индивидуального, группового и массового сознания.

SUMMARY

Gnidko K.O, Lomako A.G., Zholus R.B. **Detection of Visual Contaminants on the Basis of Perceptual Hash Calculation.**

Mental contamination is the situation, when unconscious or uncontrollable mental processes cause unwanted reactions of the individual. The all cases of contamination can be divided into two types. The first type is the result of incorrect automatic information processing in the conscious and subconscious. The second type – the unwanted consequences of superposition of mental stimuli generated by memory, thinking, feelings, judgments. The second type of contamination can be caused by subliminal images, logos of manufacturing companies, emotionally meaningful symbols and other visual images.

In this paper we propose an approach to the detection of contaminants on the basis of visual perceptual hash calculation and formation of a reference database of potentially dangerous multimedia objects. Stability of perceptual hashes to certain types of transforms not only makes it possible to detect identical image frames but also to find images "similar" in terms of human perception. Perceptual hashing algorithms based on the calculation of average values of low frequency features, computation of the Laplacian of the Gaussian, the radial vector dispersion and the discrete cosine transform are considered. An example of perceptual hashing usage to detect hidden subliminal images in a video stream is provided.

Contamination caused by unwanted automatic information conscious and subconscious is the subject of further research and requires the development of individual, group and mass consciousness models.