

Ю.Д. ВЫБОРНОВА, В.В. СЕРГЕЕВ
**МЕТОД ЗАЩИТЫ АВТОРСКИХ ПРАВ НА ВЕКТОРНЫЕ
КАРТОГРАФИЧЕСКИЕ ДАННЫЕ**

Выборнова Ю.Д., Сергеев В.В. Метод защиты авторских прав на векторные картографические данные.

Аннотация. Предложен метод защиты авторских прав на векторные картографические данные на основе встраивания растровых цифровых водяных знаков. Метод сочетает оригинальные авторские идеи, а именно: подход к встраиванию скрытой защитной информации в графические данные, не искажающей координатную информацию векторных объектов, и синтез шумоподобных изображений, выступающих в качестве контейнера для битовой последовательности цифровых водяных знаков. Шумоподобный сигнал кодирует биты цифровых водяных знаков в виде синусоидальных функций и таким образом отображает бинарную последовательность в растровое изображение, непосредственно встраиваемое в защищаемые данные. Применение шумоподобных сигналов в качестве цифровых водяных знаков значительно упрощает процедуру верификации, а также позволяет обеспечить устойчивость скрытой битовой последовательности при различных искажениях изображения цифровых водяных знаков, в том числе при интерполяции.

Целью экспериментальных исследований являлась оценка достижимой вероятности правильного извлечения двоичной последовательности цифровых водяных знаков при различных параметрах и условиях встраивания.

Исследование информационной емкости показало, что потенциальный объем информации, встраиваемый в каждый полигон без искажения битовой последовательности цифровых водяных знаков, зависит от типа карты, а именно от количества вершин, составляющих каждый полигон.

Проведено экспериментальное исследование стойкости полученного метода к потенциально возможным преобразованиям, направленным на злоумышленное удаление цифровых водяных знаков из векторной карты. Разработанный метод демонстрирует стойкость к аффинным преобразованиям, кадрированию, добавлению, удалению и переупорядочиванию вершин/объектов, и может применяться в качестве решения задачи защиты авторских прав на векторные данные.

Проведен анализ качества метода по критериям точности, стойкости, информационной емкости, вычислительной сложности. Результаты всех проведенных исследований подтверждают возможность использования и эффективность предложенного метода защиты векторных картографических данных, а также его преимуществ перед существующими методами встраивания цифровых водяных знаков.

Ключевые слова: геоинформационные системы, векторные карты, защита авторских прав, цифровой водяной знак, растровое изображение, дискретное преобразование Фурье, битовая последовательность

1. Введение. Создание векторных картографических данных представляет собой ресурсоемкий процесс, требующий наличия квалифицированных специалистов и лицензионного программного обеспечения. В связи с высокой стоимостью производства векторных карт их владельцы заинтересованы в сохранении своих авторских прав.

Для решения задачи защиты авторских прав применяется технология встраивания цифровых водяных знаков (ЦВЗ). Предполагается,

что собственник данных обеспечивает их встроенной защитной информацией, которая впоследствии позволяет доказать факт несанкционированного распространения. Кроме того, этап верификации ЦВЗ может включать и процедуру аутентификации на предмет нелегитимных изменений. Поставленные задачи защиты предопределяют уровень стойкости встраиваемых ЦВЗ: для детектирования подделки защитная информация (полухрупкий ЦВЗ) должна разрушаться при определенных преобразованиях векторной карты, но при защите авторских прав ЦВЗ должен быть как можно более устойчив как к легальным, так и злоумышленным изменениям (такие ЦВЗ называются стойкими).

Качество метода встраивания ЦВЗ характеризуется степенью выполнения следующих критериев [1]:

- точность данных контейнера (визуальная неразличимость встроенной информации);
- стойкость ЦВЗ (устойчивость карты со встроенным ЦВЗ к преобразованиям);
- информационная ёмкость контейнера (количество бит ЦВЗ, которые можно встроить);
- вычислительная сложность (время, требуемое для реализации процедур встраивания/извлечения ЦВЗ);
- безопасность расположения ЦВЗ (непредсказуемость расположения ЦВЗ на карте).

Нулевое встраивание ЦВЗ представляет собой аналог процедуры хеширования: для защищаемой карты вычисляется некоторая идентифицирующая информация, которая впоследствии хранится отдельно. На этапе «извлечения» ключевые характеристики вычисляются заново, после чего сформированный ЦВЗ сравнивается с исходным. Например, в [2] вычисляется отношение расстояний между вершинами, после чего для большей секретности объединяется с битами ЦВЗ. В [3] ЦВЗ строится на основе триангуляции и вычисления локальных характеристик внутри каждого треугольника.

Несомненным плюсом таких схем является отказ от внесения искажений в координатную информацию, однако встает вопрос о необходимости регистрации таких ЦВЗ в уполномоченных органах.

При адаптивном подходе к встраиванию защитной информации ЦВЗ содержит данные для идентификации и при этом встраивается в векторную карту. Так, в [4] идентификационная информация строится на основе характерных точек, которые вычисляются с помощью алгоритма упрощения Дугласа – Пекера. Для того чтобы разграничить легальные и злоумышленные преобразования векторной карты, ЦВЗ встраивается не только в характерные точки, которые должны оста-

ваться неизменными, но и в нехарактерные. В [5] информация для аутентификации вычисляется на основе объединения векторных объектов в группы и перехода в полярную систему координат. В [6] ЦВЗ формируется на основе вычисления логарифмических полярных координат, разности которых являются устойчивыми к геометрическим преобразованиям векторной карты. При этом в [4-6] сама процедура встраивания реализуется за счет небольшого изменения значений координат с помощью стратегии модуляции квантования. В [7] для построения ЦВЗ вычисляются углы векторных объектов. Целые значения каждого угла изменяются в соответствии с ключом. Встраивание в векторный объект реализуется путем замены дробной части угла на полученное для этого угла значение ЦВЗ.

Большинство существующих методов защиты векторных данных реализуют классический подход к встраиванию ЦВЗ, когда встраиваемая защитная информация представляет собой битовую последовательность или цифровое изображение, формируемые независимо от защищаемых данных.

В [8] ЦВЗ встраивается в векторную карту за счет изменения координат вершин таким образом, чтобы внутри некоторого кластера длина всех линий (или площадь всех полигонов) изменилась на заданную величину. В [9] авторы предлагают с помощью стратегии модуляции квантования изменять координаты вершин таким образом, чтобы значение отношения расстояний между характерными вершинами изменялось на заданную величину. При этом каждый бит ЦВЗ внедряется в несколько объектов: такого рода избыточность позволяет повысить стойкость, но вместе с тем значительно уменьшает потенциальную емкость контейнера.

В [10] авторы также применяют стратегию модуляции квантования, но при этом встраиваемая информация представлена набором бинарных последовательностей ЦВЗ. Векторная карта разбивается на блоки заданного размера, и для каждого блока формируется и встраивается соответствующий битовый вектор.

Еще одной стратегией встраивания ЦВЗ является непосредственное изменение значений координат вершин путем внесения небольших погрешностей в зависимости от значения бита ЦВЗ [11].

В [12] данная стратегия реализуется на основе поблочного встраивания ЦВЗ. Сначала производится адаптивное разбиение карты на прямоугольные области таким образом, чтобы достичь требуемой плотности вершин внутри каждой из них. Затем короткое бинарное сообщение повторно встраивается в координаты вершин, принадлежащих полученным областям разбиения, за счет внесения погрешностей непосредственно в координатные значения.

Большинство существующих методов встраивания ЦВЗ в векторные данные направлено на решение одной из задач обеспечения безопасности векторных данных: защиту от несанкционированного распространения (защиту авторских прав) или защиту от изменений. Подход, позволяющий одновременно обеспечивать защиту авторских прав и защиту подлинности векторных данных, носит название составного встраивания ЦВЗ. При реализации данного подхода часть вершин (например, характерные точки) выбирается в качестве контейнера для стойких ЦВЗ, а оставшиеся вершины – для хрупких ЦВЗ (т.е. таких ЦВЗ, которые будут разрушены при несанкционированных изменениях). Такой подход предложен, например, в [13], он позволяет детектировать изменение векторных объектов, а также их добавление или удаление.

Очевидно, сохранение точности значений координат после встраивания ЦВЗ является критическим вопросом в данной предметной области и ключевой проблемой перечисленных методов, поскольку внесение даже незаметных на первый взгляд погрешностей может отрицательно сказаться на практической пригодности векторной карты (например, кадастровая карта с неверными границами участков потеряет свою ценность).

В этой связи в работах [14-17] были предложены методы обратимого встраивания ЦВЗ: данный подход позволяет сохранить точность исходных данных путем их восстановления после извлечения ЦВЗ. Поскольку после процедуры восстановления исходной карты встроенный ЦВЗ будет полностью удален, такой подход к встраиванию пригоден только для защищенной передачи и не подходит для защищенного хранения данных.

Кроме того, все перечисленные методы обладают еще одним существенным недостатком: защитная информация, внесенная в наименее значимые биты координат, представленных дробными числами, может быть удалена при экспорте векторных данных в другой формат.

Ранее в [18] авторами настоящей статьи был предложен новый подход к неискажающему встраиванию защитной информации – шумоподобных ЦВЗ [19] – в векторные картографические данные, основанный на циклическом сдвиге вершин полигональных графических объектов карты и последующей интерпретации центров тяжести полигонов как случайного множества пикселей растрового изображения, наложенного на карту и несущего ЦВЗ. Данный подход не предполагает внесение изменений в координатную информацию, что является его основным преимуществом перед известными методами.

Работа [18] посвящена преимущественно теоретическому описанию формирования шумоподобных изображений и глубокому ис-

следованию информационной емкости метода с простейшим алгоритмом детектирования амплитудных пиков.

Предложенный подход исследуется в задаче защиты авторских прав: повышена стойкость метода к преобразованиям с помощью введения нового детектора последовательностей ЦВЗ. Кроме того, приведено сравнение с методом [18] по критерию информационной емкости. В отличие от исследований в [18] эксперименты проведены не на одной карте, а на наборе карт различного размера, что позволяет более рационально подбирать параметры метода в зависимости от размера карты и выбранного детектора. Помимо информационной емкости, исследованы стойкость и вычислительная сложность предложенного метода. Показано, что полученный метод встраивания ЦВЗ может применяться для решения задачи защиты авторских прав.

В разделе 2 коротко описаны идеи предлагаемого подхода к встраиванию ЦВЗ в векторные данные. Раздел 3 посвящен описанию алгоритма формирования шумоподобного изображения на основе битовой последовательности ЦВЗ и алгоритма извлечения такой последовательности соответственно. В разделах 4-6 приведены результаты экспериментальных исследований метода по различным критериям качества.

2. Краткое описание предложенного подхода. В качестве контейнера для встраивания ЦВЗ используется множество объектов полигонального типа. Каждый полигон представляет собой замкнутый объект (многоугольник), который может быть однозначно определен списком координат последовательно пронумерованных вершин. Таким образом, циклический сдвиг списка вершин полигона не повлияет на значения их координат. Эта идея есть суть предлагаемого подхода к встраиванию ЦВЗ без внесения искажений в координатную информацию.

В качестве ЦВЗ предлагается использовать растровое изображение, наложенное на выбранный фрагмент векторного слоя путем разбиения карты на прямоугольные ячейки и отображения полученного разбиения на сетку пикселей растра.

В каждый полигон будет встроено тот пиксель, в котором расположен центр тяжести этого полигона. Очевидно, далеко не все пиксели будут встроены в векторную карту. В этой связи необходимо обеспечить возможность восстановить изображение ЦВЗ по заданному набору пикселей и при этом однозначно верифицировать восстановленный ЦВЗ. Процедура проверки чаще всего требует визуального или корреляционного сопоставления с эталоном, а также дальнейшего анализа полученных результатов.

Для того чтобы упростить процедуру верификации ЦВЗ, предлагается синтезировать шумоподобные сигналы, которые кодируют

битовый ЦВЗ в виде синусоидальных функций и тем самым отображают бинарную последовательность в растровое изображение, непосредственно встраиваемое в защищаемые данные. Таким образом, на этапе проверки будет анализироваться не само извлеченное изображение ЦВЗ, а скрытая в нем последовательность.

Полученные шумоподобные изображения ЦВЗ обеспечивают устойчивость скрытой в них битовой последовательности при различных искажениях, в том числе при интерполяции. Это обусловлено тем фактом, что после внесенных изменений (в том числе значительных) сохраняется амплитудный спектр, сформированный на этапе построения изображения ЦВЗ.

Шумоподобный ЦВЗ встраивается в векторную карту на основе циклического сдвига вершин полигонов следующим образом.

Сначала рассчитываются координаты ограничивающего прямоугольника $x_{\min}, y_{\min}, x_{\max}, y_{\max}$, и для каждого i -того объекта карты вычисляется отображение следующего вида: $x_i, y_i \rightarrow n_1, n_2$:

$$n_1 = \frac{x_i - x_{\min}}{step_X}, n_2 = \frac{y_{\max} - y_i}{step_Y}, step_X = \frac{x_{\max} - x_{\min}}{N}, step_Y = \frac{y_{\max} - y_{\min}}{N}.$$

Затем для каждого полигона выполняется следующая процедура:

- а) рассчитываются координаты центраида x_{ci}, y_{ci} ;
- б) на основе положения центраида определяются координаты пикселя, который будет встроен в полигон;
- в) число вершин полигона V_p представляется в виде $V_p \geq 2^{b-1}$, после чего выбираются b старших бит значения пикселя (число для встраивания);
- г) старший бит вносимого двоичного числа встраивается путем задания направления считывания вершин: по часовой стрелке или наоборот (данный шаг не является обязательным, однако позволяет значительно повысить стойкость метода к атакам переупорядочивания вершин);
- д) из центра тяжести проводятся $(b-1)^2$ равноотстоящих луча и маркируются $(b-1)$ -битными числами;
- е) для каждой вершины полигона определяется угловое расстояние $[0, 359^\circ]$ относительно луча, направленного на север;
- ж) список вершин полигона циклически сдвигается до тех пор, пока вершина, ближайшая к лучу со встраиваемым числом, не окажется первой.

На рисунке 1 представлен пример встраивания в полигон трех бит информации. Поскольку представленный векторный объект явля-

ется четырехугольником, то чтобы извлечь ЦВЗ без ошибок, необходимо внести в полигон не более трех бит информации: два бита – путем циклического сдвига номеров вершин, и один бит – путем задания направления обхода вершин полигона.

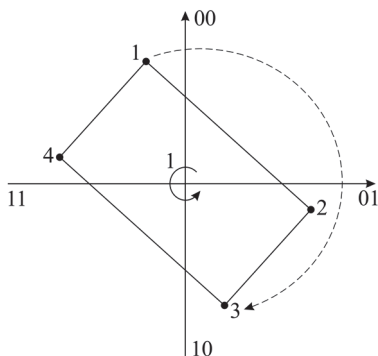


Рис. 1. Пример встраивания трех бит информации в полигональный объект

При извлечении информации, скрытой внутри векторной карты, для каждого полигона определяется пространственная ориентация первой вершины. Старший бит определяется в соответствии с обходом вершин (если этот шаг не был пропущен при встраивании).

На рисунке 2 представлен пример извлечения из полигона трех бит информации.

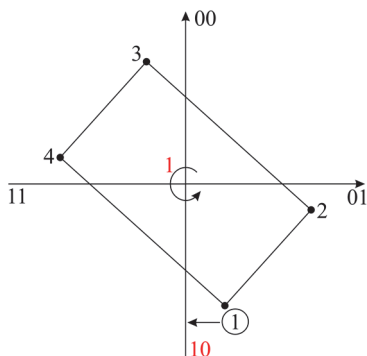


Рис. 2. Пример извлечения трех бит информации из полигонального объекта

Аналогично встраиванию карта отображается на изображении (изначально пустое). Извлеченные из полигонов значения при-

сваиваются значениям яркости пикселей, соответствующих центрам. Пиксели, огрубленные на этапе встраивания, приводятся к 8-битным значениям. Ячейки, оставшиеся пустыми, восстанавливаются методом ступенчатой интерполяции на основе триангулированной нерегулярной сети [20]. Подробное исследование алгоритмов встраивания и извлечения приведено в [21].

3. Формирование изображения ЦВЗ. В качестве ЦВЗ предлагается использовать шумоподобное изображение размером $N_1 \times N_2$, формируемое путем синтеза комплексного спектра на основе некоторой двоичной последовательности длины L (первичного ЦВЗ, служащего в качестве проверочной информации в процессе извлечения). Спектр шумоподобного изображения представляет собой набор дельта-импульсов, расположенных на двух кольцах в двумерной плоскости. Порядок импульсов кодирует бинарную последовательность ЦВЗ: «нули» помещаются на внутреннем круге радиуса r , а «единицы» – на внешнем круге радиуса $r + \Delta r$. Все импульсы расположены с определенным шагом, кроме специальной метки синхронизации, которая сигнализирует о начале последовательности: метка содержит два импульса, расположенных без отступа по углу.

Процедура формирования пространственного спектра для последовательности $S = s_1 \dots s_L = \{101101001011101\}$ проиллюстрирована на рисунке 3.

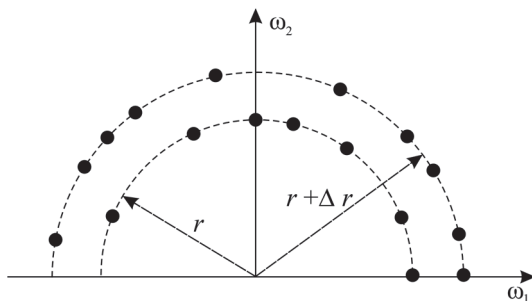


Рис. 3. Синтез спектра шумоподобного сигнала [18]

Очевидно, шумоподобное изображение ЦВЗ, которое впоследствии будет встроено в векторную карту, вычисляется с помощью двумерного обратного дискретного преобразования Фурье (ДПФ).

Например, в результате обратного ДПФ спектра на рисунке 3 вычислено изображение, представленное на рисунке 4.

Для обеспечения непредсказуемости шумоподобных изображений, синтезируемых для некоторой битовой последовательности, предложено формировать комплексный спектр, задавая значения дельта-импульсов с помощью датчика случайных чисел (ДСЧ):

$$\begin{aligned} \operatorname{Re} F(u_l, v_l) &= \cos(\operatorname{rand}(90)), \\ \operatorname{Im} F(u_l, v_l) &= \sin(\operatorname{rand}(90)). \end{aligned} \quad (1)$$

Здесь $u_l = (r + s_l \Delta r) \times \cos \frac{\pi l}{L+1}$, $v_l = (r + s_l \Delta r) \times \sin \frac{\pi l}{L+1}$, $1 \leq l \leq L+1$, $\operatorname{rand}(90)$ – псевдослучайное число, значение которого лежит в диапазоне $[0, 90]$.

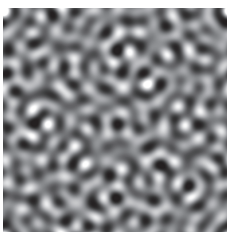


Рис. 4. Изображение ЦВЗ ($r=8$, $\Delta r=4$)

Таким образом, даже если в качестве ЦВЗ для целого набора карт будет выбрана одна и та же битовая последовательность, порождаемые для каждой карты изображения будут разными.

Очевидно, для извлечения последовательности ЦВЗ необходимо перейти к спектру извлеченного шумоподобного изображения и определить, какие компоненты имеют наибольшую амплитуду (являются импульсами, кодирующими биты ЦВЗ). Алгоритмы формирования изображения ЦВЗ и извлечения скрытой битовой последовательности подробно описаны в [18].

Степень стойкости зависит, в первую очередь, от алгоритма детектирования амплитудных пиков. В исследовании [18] применялся простейший детектор пиков, основанный на эвристическом предположении о том, что амплитудный пик превышает половину максимума модуля спектра Фурье. В данной работе будем называть его «детектор на основе пороговой обработки». Такой детектор не учитывает тот факт, что при сильных искажениях (особенно при кадрировании) спектральные характеристики могут меняться, например, в силу элайзинга (эффекта наложения спектральных составляющих).

В настоящей статье улучшены показатели стойкости к искажениям, а именно достигнута возможность кадрирования до 43% контейнера, содержащего ЦВЗ. Данные показатели были достигнуты путем разработки нового алгоритма детектирования амплитудных пиков спектра Фурье на основе локальной фильтрации, в котором используется скользящее окно размером 3×3 .

Внутри локального окна вычисляются локальные максимумы модуля ДПФ:

$$|F(k_1, k_2)| = 0, \text{ если } |F(k_1, k_2)| < \max_{m_1, m_2} |F(k_1 + m_1, k_2 + m_2)|, m_1, m_2 = \overline{-1, 1}.$$

Полученные значения максимумов сортируются по убыванию: $2 \times (L+2)$ наибольших значения есть искомые импульсы.

Экспериментально установлены минимальные параметры для работоспособности данного алгоритма детектирования: $r \geq 0,83 L$, $\Delta r = 8$.

4. Исследование информационной емкости. В [18] исследованы потенциальные возможности использования шумоподобных изображений для решения задачи защиты векторных карт. При этом, как уже было отмечено ранее, вычислительные эксперименты были проведены только для детектора на основе пороговой обработки.

В данной работе повторим эксперимент по моделированию погрешностей (эксперимент 1) для детектора на основе локальной фильтрации и сравним полученные для разных детекторов результаты, а также расширим эксперимент на реальных данных (эксперимент 2) путем увеличения тестового набора и представим результаты, полученные для обоих детекторов.

Для формирования тестовых наборов ЦВЗ были сгенерированы 100 псевдослучайных последовательностей, на основе которых для каждого сочетания параметров синтезировались шумоподобные изображения. Поскольку, как было показано ранее, параметры минимальных радиусов влияют на работоспособность алгоритмов детектирования спектральных импульсов, тестовые наборы формировались согласно выдвигаемым ограничениям.

Эксперимент 1. Данный эксперимент направлен на моделирование искажений, вносимых в изображение ЦВЗ предлагаемым методом встраивания в полигоны векторного слоя. Как уже было отмечено, в силу особенностей предлагаемого подхода к неискажающему встраиванию, изображение ЦВЗ не может быть встроено целиком: векторная карта с ЦВЗ будет содержать только некоторую долю всех пикселей. При этом значение каждого встраиваемого пиксе-

ля огрубляется до нескольких старших бит в зависимости от числа вершин полигона-контейнера.

Данный эксперимент направлен на оценку устойчивости шумоподобного ЦВЗ к перечисленным искажениям. Для этого изображение ЦВЗ размером $N_1 \times N_2 = 512 \times 512$ подвергалось преобразованию квантования на 2^b уровней, после чего каждый пиксель принимал значение b -разрядного двоичного числа. Далее с помощью ДСЧ выбиралось заданное число пикселей K , моделирующее количество полигональных объектов на карте. Затем по выбранному набору пикселей строилась триангуляция Делоне, на основе которой прореженные изображения восстанавливались методом ступенчатой интерполяции. После этого производилась попытка извлечения битовой последовательности. Оценка вероятности правильного извлечения p рассчитывалась по всему тестовому набору как доля изображений (из ста), для которых последовательность ЦВЗ была извлечена без ошибок.

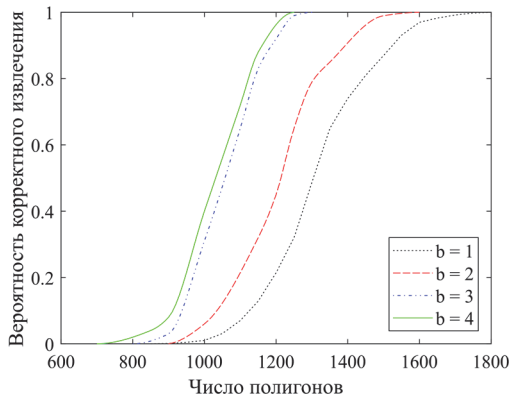
Рисунок 5 демонстрирует результаты эксперимента, проведенного для детектора на основе локальной фильтрации. Представлена зависимость вероятности правильного извлечения от числа опорных пикселей при различных значениях разрядности b . Результаты аналогичного эксперимента для детектора на основе пороговой обработки приведены в [18].

Количество опорных точек, моделирующих объекты векторной карты, очевидно, влияет на точность извлечения битовой последовательности. Чем больше размер карты, тем больше потенциальная длина встраиваемого двоичного слова. Погрешность квантования уменьшается с ростом разрядности пикселей, однако для $b > 3$ эффект повышения качества значительно замедляет свой рост.

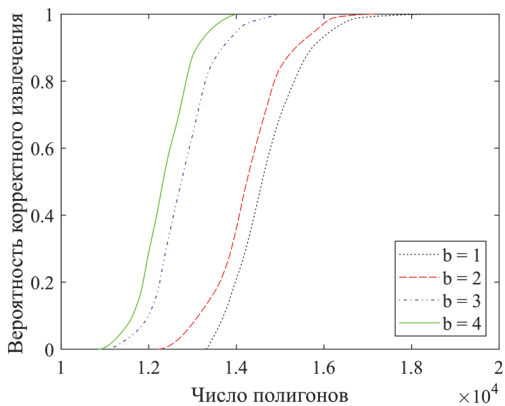
На рисунке 6 приведено сравнение двух детекторов по критерию информационной емкости, вычисляемой как $b \times L$: представлены графики зависимостей емкости от числа опорных пикселей при различных значениях вероятности p . При этом параметр $b=3$ фиксирован.

Согласно результатам, представленным на рисунке 6, оба детектора обеспечивают точное извлечение встроенной последовательности ЦВЗ. Однако в случае детектора на основе локальной фильтрации минимально необходимое число пикселей значительно больше.

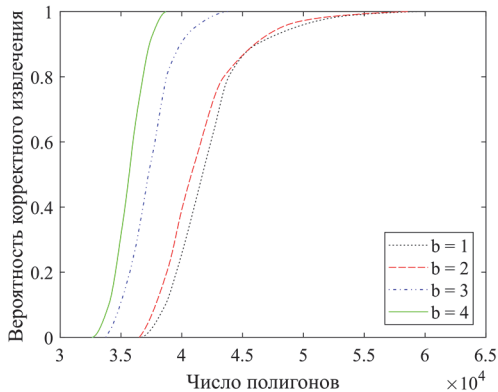
Дело в том, что в силу ограничений, накладываемых на минимальные значения радиусов синтезируемых спектральных колец, изображения ЦВЗ, формируемые для этого детектора, представляют собой более высокочастотные сигналы, и для их корректной интерполяции требуется больше опорных точек.



(а)

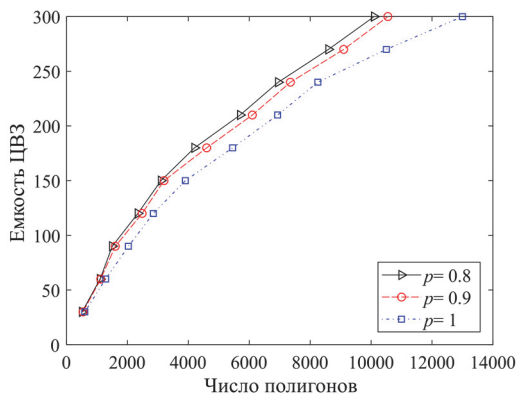


(б)

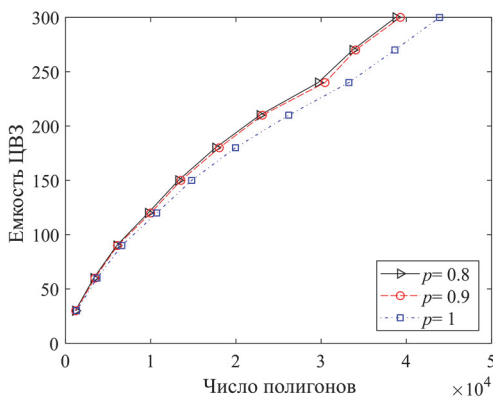


(в)

Рис. 5. Вероятность корректного извлечения а) $L = 10, r = 10$; б) $L = 50, r = 60$;
в) $L = 100, r = 116$



(a)



(б)

Рис. 6. Информационная емкость: а) детектор на основе пороговой обработки; б) детектор на основе локальной фильтрации

Эксперимент 2. В отличие от предыдущего эксперимента, моделирующего потенциальные искажения, в настоящем эксперименте исследуется процесс встраивания в реальные картографические данные.

В качестве тестового набора использованы фрагменты карт городской застройки различного размера P : от 1000 до 100000 полигональных объектов.

Размеры встраиваемых изображений ЦВЗ, в зависимости от размера векторной карты, приведены в таблице 1.

Эксперимент направлен на анализ искажений, вносимых при встраивании в карты, относительно модельного случая из предыдущего эксперимента путем вычисления вероятности правильного извлечения для трех случаев:

1. Квантование всех пикселей изображения производится по фиксированному уровню. Опорные точки для интерполяции расставляются равномерно с помощью ДСЧ (аналогично эксперименту 1).

2. Квантование всех пикселей изображения производится по фиксированному уровню. Для интерполяции строится нерегулярная сеть, отображающая центры полигонов векторной карты (рис. 7). Этот случай направлен на демонстрацию погрешностей, вносимых при прореживании изображения ЦВЗ и его дальнейшей интерполяции.

3. Встраивание ЦВЗ в реальные картографические данные. Значение каждого пикселя квантуется в зависимости от числа вершин полигона, в который этот пиксель будет встроен. Этот случай позволит продемонстрировать влияние распределения вершин полигонов на результат извлечения.

Таблица 1. Требования к размерам встраиваемых изображений

Размер карты, полигонов	Размер встраиваемого ЦВЗ, пикселей
1000 – 30000	512×512
30000 – 80000	1024×1024
от 80000 – 100000	2048×2048

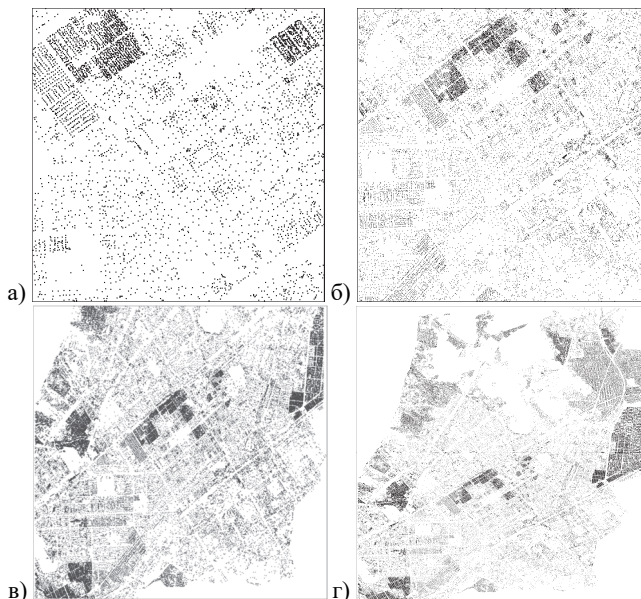


Рис. 7. Точечное представление векторной карты (нерегулярная сеть): а) 5 тыс. полигонов; б) 20 тыс. полигонов; в) 60 тыс. полигонов; г) 100 тыс. полигонов

Согласно предлагаемому подходу к неискажающему встраиванию, внесение b -бит информации в полигон без погрешностей возможно при условии, что данный полигон состоит как минимум из 2^{b-1} вершин. Поскольку исследуемый тестовый набор векторных данных представлен картами городской застройки, встраивание пяти и более бит в каждый полигон маловероятно, так как подавляющее большинство векторных объектов (городских зданий) содержит менее 16 вершин. По результатам предыдущего эксперимента, наиболее вероятные случаи $b=3$ и $b=4$ практически идентичны. Таким образом, далее встраивание в реальные карты будет сравниваться с результатами моделирования случая $b = 3$.

Для данного эксперимента были сформированы наборы шумоподобных ЦВЗ для обоих детекторов: 100 изображений для каждого значения L , варьируемого в диапазоне $L = \overline{10, 100}$.

Зависимости вероятности корректного извлечения двоичной последовательности ЦВЗ от размера контейнера для детектора на основе пороговой обработки приведены на рисунке 8.

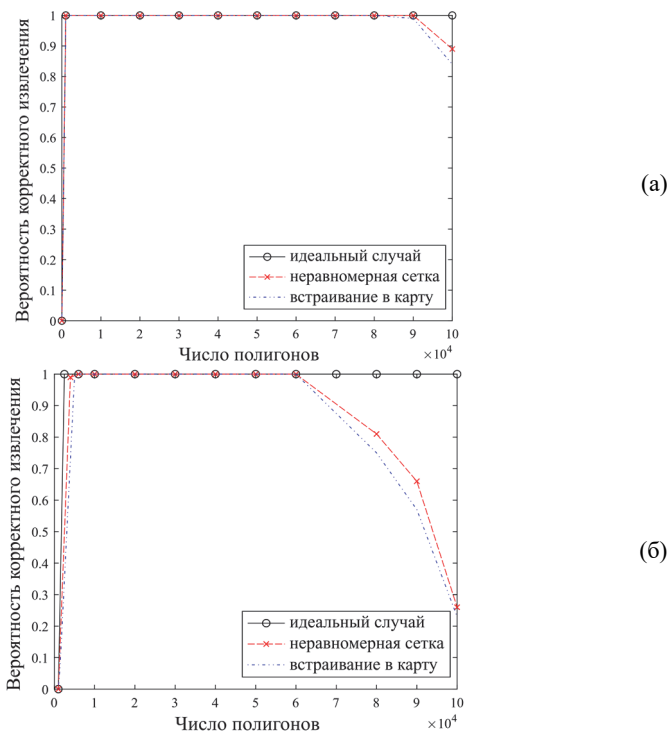


Рис. 8. Вероятность корректного извлечения для детектора на основе пороговой обработки: а) $L = 10$; б) $L = 30$;

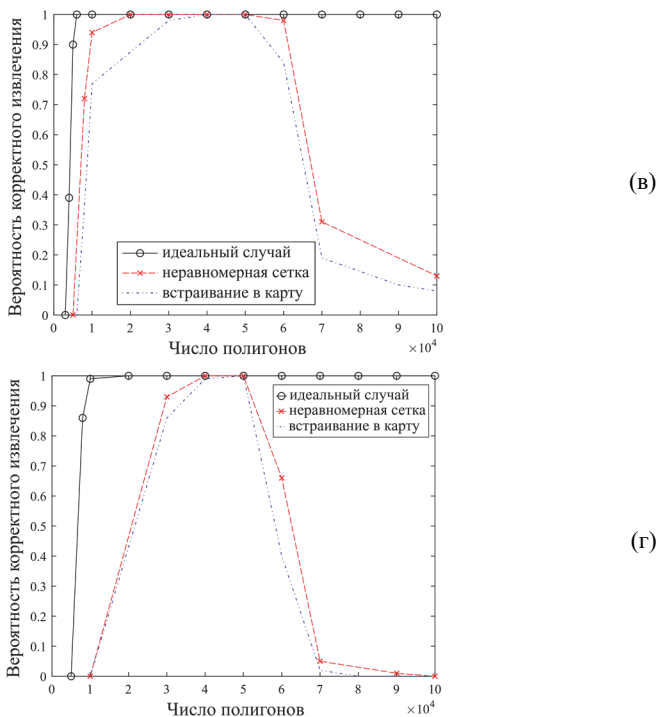


Рис. 8. Вероятность корректного извлечения для детектора на основе пороговой обработки: в) $L = 60$; г) $L = 80$

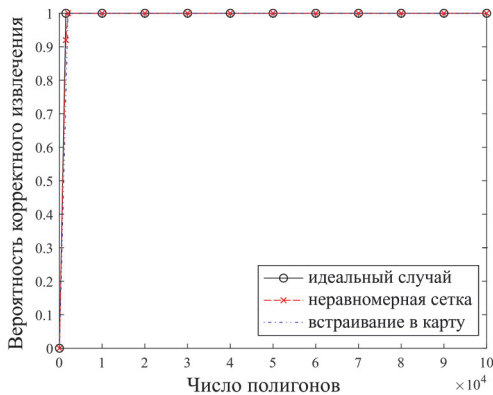
По результатам эксперимента 1, качество извлечения ЦВЗ растет с числом объектов на карте. Однако апробация на реальных данных показала, что увеличение размера карты может отрицательно повлиять на корректность извлечения. Схожее поведение синей и красной кривых на графиках позволяет сделать вывод о том, что ошибки возникают в силу неравномерности расположения опорных точек при интерполяции. В действительности, согласно рисунку 7, для случаев $P \geq 60000$ нерегулярные сетки, моделирующие расположение объектов на карте, заполнены неравномерно.

Крупные пустые области по краям значительно влияют на качество восстановления изображения ЦВЗ методами интерполяции. Во избежание возникновения подобных ошибок извлечения большие карты целесообразно разбивать на фрагменты.

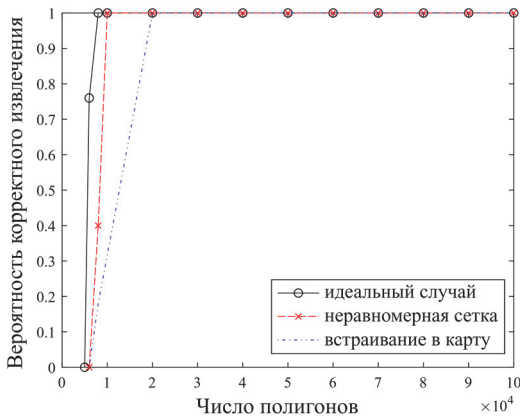
Сложность извлечения последовательности ЦВЗ также возрастает с ростом L . В случае $L \geq 90$ корректно извлечь скрытую информацию из реальных картографических данных не удалось.

Зависимости вероятности корректного извлечения двоичной последовательности ЦВЗ от размера контейнера для детектора на основе локальной фильтрации приведены на рисунке 9.

Согласно графикам при $L \leq 30$ неравномерное расположение объектов на карте при больших значениях P не повлияло на качество извлечения, что свидетельствует о более высокой устойчивости данного детектора к погрешностям интерполяции. Однако, аналогично результатам эксперимента 1 информационная емкость детектора на основе локальной фильтрации оказалась ниже. Максимальная длина извлеченной корректно последовательности составляет $L = 60$.

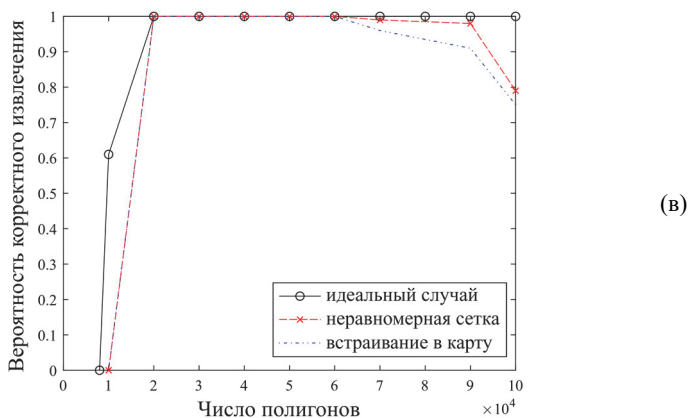


(а)

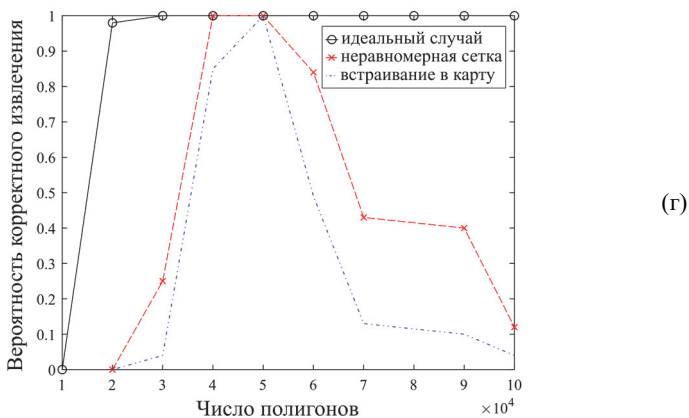


(б)

Рис. 9. Вероятность корректного извлечения для детектора на основе локальной фильтрации: а) $L = 10$; б) $L = 30$



(в)



(г)

Рис. 9. Вероятность корректного извлечения для детектора на основе локальной фильтрации: в) $L = 40$; г) $L = 60$

5. Исследование стойкости к преобразованиям. Несмотря на то, что детектор на основе пороговой обработки по результатам двух экспериментов демонстрирует повышенную информационную емкость, данный алгоритм не может использоваться в составе метода защиты авторских прав на картографические данные, поскольку, как было отмечено ранее, не является стойким к кадрированию, а также недостаточно устойчив к интерполяции по нерегулярной сетке. С другой стороны, данный детектор может найти применение в ряде задач, требующих встраивания большого объема информации, например, задаче аутентификации векторных данных.

Таким образом, в настоящей работе для решения задачи защиты авторских прав на векторные данные предлагается использовать метод встраивания ЦВЗ, включающий алгоритм детектирования на основе локальной фильтрации.

Далее приведено исследование стойкости полученного метода встраивания ЦВЗ к возможным преобразованиям векторных карт, которое позволит сделать выводы о его применимости для решения поставленной задачи. Эксперимент представляет собой оценку максимальности ЦВЗ может быть извлечена без ошибок.

Сначала приведем доказательство стойкости к геометрическим преобразованиям сдвига и масштабирования, построенное на инвариантности отображения растрового изображения на векторную карту относительно данных преобразований. Напомним, что построение такого отображения начинается с построения ограничивающего прямоугольника векторной карты и его разбиения на двумерную сетку, после чего пиксели изображения отображаются на те векторные объекты, центры которых находятся в соответствующей ячейке прямоугольного разбиения. Далее показано, что при сдвиге карты или изменении ее масштаба координаты центра и координаты ограничивающего прямоугольника изменяются пропорционально, что обеспечивает свойство инвариантности.

1. Сдвиг. При сдвиге карты на Δx по горизонтальной оси и на Δy по вертикальной оси координаты каждого (i -того) полигона изменятся на соответствующую величину: $x_{ci} + \Delta x, y_{ci} + \Delta y$.

Изменяются и координаты ограничивающего прямоугольника: $x_{\min} + \Delta x, y_{\min} + \Delta y, x_{\max} + \Delta x, y_{\max} + \Delta y$.

Отображение изображения на карту (см. раздел 2) примет вид:
$$\frac{x_i + \Delta x - (x_{\min} + \Delta x)}{step_X} = \frac{x_i - x_{\min}}{step_X}, \quad \frac{y_{\max} + \Delta y - (y_i + \Delta y)}{step_Y} = \frac{y_{\max} - y_i}{step_Y},$$
 что совпадает с исходным отображением.

2. Масштабирование. При изменении масштаба карты в k_{sc} раз соответственно изменятся и координаты каждого (i -того) полигона: $k_{sc} \cdot x_{ci}, k_{sc} \cdot y_{ci}$. Координаты ограничивающего прямоугольника также будут умножены на коэффициент масштабирования: $k_{sc} \cdot x_{\min}, k_{sc} \cdot y_{\min}, k_{sc} \cdot x_{\max}, k_{sc} \cdot y_{\max}$.

Тогда отображение изображения ЦВЗ на карту примет вид:
$$\frac{k_{sc} \cdot x_i - k_{sc} \cdot x_{\min}}{k_{sc} \cdot step_X} = \frac{x_i - x_{\min}}{step_X}, \quad \frac{k_{sc} \cdot y_{\max} - k_{sc} \cdot y_i}{k_{sc} \cdot step_Y} = \frac{y_{\max} - y_i}{step_Y},$$
 что совпадает с исходным отображением.

Для экспериментальной оценки стойкости метода к атакам были смоделированы возможные злоумышленные преобразования. Как и в предыдущем эксперименте, тестовый набор содержит векторные карты городской застройки различного размера. В каждую карту последовательно встраивались 100 изображений ЦВЗ, сформированных для последовательностей длины $L = 10$ ($r = 10$). Карта со встроенным ЦВЗ подвергалась преобразованию заданной степени, после чего оценивалась вероятность корректного извлечения ЦВЗ. Максимально допустимой будем полагать ту степень преобразования, при которой последовательность ЦВЗ была извлечена без ошибок из всех 100 изображений.

3. Поворот. В настоящем эксперименте каждая карта из тестового набора поворачивалась относительно центра на заданный угол. При повороте меняются координаты минимумов и максимумов по обим осям (т.е. меняется ограничивающий прямоугольник). Извлеченное изображение ЦВЗ при этом представляет собой повернутое отображение векторной карты внутри нового ограничивающего прямоугольника. В связи с этим на краях изображения могут возникнуть пустые области, которые необходимо кадрировать, чтобы избежать ошибок интерполяции.

Результаты эксперимента представлены в таблице 2. Согласно полученным результатам предложенный метод демонстрирует устойчивость к повороту при размере карты $P \geq 3000$ полигонов. Для больших карт максимальный угол поворота достигает 25° .

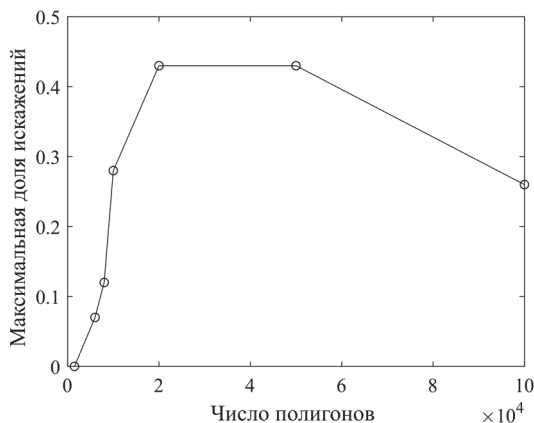
4. Кадрирование. Преобразование кадрирования смоделировано путем обрезки изображения, извлеченного из векторной карты. При этом центр кадрируемого фрагмента может либо совпадать с центром изображения, либо быть выбран произвольно.

Таблица 2. Максимально допустимый угол поворота для карт различного размера

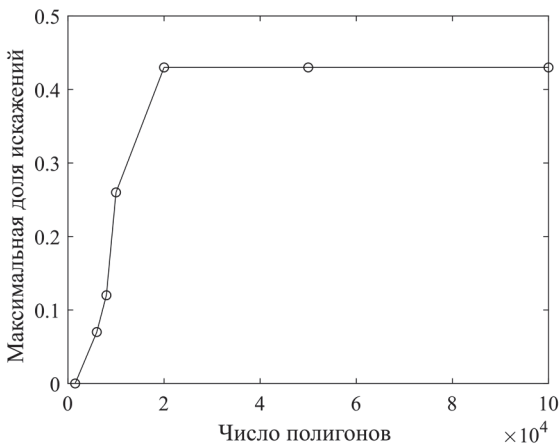
Число полигонов	2000	3000	4000	6000	8000	10000	20000	50000	10000
Угол, °	0	5	5	15	20	20	25	25	25

Результаты эксперимента представлены на рисунке 10. В качестве параметра стойкости выбран коэффициент $k_{cr} = 1 - \frac{N_{cr} \times N_{cr}}{N \times N}$. Здесь $N_{cr} \times N_{cr}$ – размер изображения ЦВЗ после кадрирования.

Из рисунков видно, что для карт $P \leq 50000$ метод демонстрирует устойчивость к кадрированию независимо от положения кадрируемого фрагмента.



(a)



(б)

Рис. 10. Максимально допустимая доля кадрирования для карт различного размера: а) кадрирование относительно произвольной точки; б) кадрирование относительно центра изображения

Небольшое падение кривой на рисунке 10а обусловлено тем, что при обрезке карты относительно случайной точки полученный фрагмент может включать пустые территории, которые, как уже было отмечено выше, присутствуют на тестовых картах размером $P \geq 60000$.

Стоит отметить, что при размере карт $20000 \leq P \leq 50000$ коэффициент k_{cr} достигает 43% при любом положении вырезаемого фрагмента.

5. *Добавление объектов.* Данная атака была смоделирована путем добавления случайных пикселей в пустые ячейки извлеченного изображения ЦВЗ.

На рисунке 11 представлена зависимость максимально допустимого коэффициента $k_{add} = \frac{P_{add}}{P}$ от размера карты P . Здесь P_{add} – количество объектов на карте после осуществления атаки.

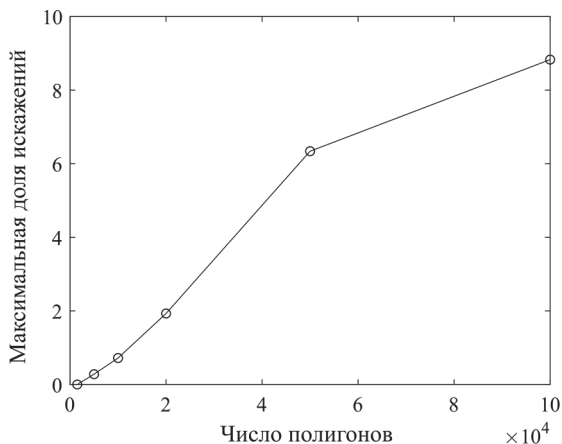


Рис. 11. Максимально допустимая доля добавленных объектов для карт различного размера

Согласно рисунку 11 коэффициент k_{add} растет с увеличением числа полигонов на карте. Например, при $P = 20000$ коэффициент достигает значения $k_{add} = 1,93$, что означает добавление объектов, почти в два раза превышающих исходное число объектов на карте. Очевидно, после такой атаки векторная карта полностью потеряет свою ценность, а значит, невыгодна злоумышленнику.

6. *Удаление объектов.* Данная атака была смоделирована путем удаления заданной доли случайно выбранных полигонов.

На рисунке 12 представлена зависимость максимально допустимого коэффициента $k_{del} = \frac{P_{del}}{P}$ от размера карты P . Здесь P_{del} – количество объектов на карте после осуществления атаки.

Кривая на рисунке 12 демонстрирует быстрый рост коэффициента k_{del} . Например, для $P = 3000$ коэффициент достигает значения

$k_{del} = 0,29$, то есть в результате данной атаки почти треть всех полигонов карты будет удалена. Поскольку попытка удаления ЦВЗ путем удаления объектов значительно повлияет на практическую ценность карты, можно заключить, что исследуемый метод является устойчивым к удалению объектов.

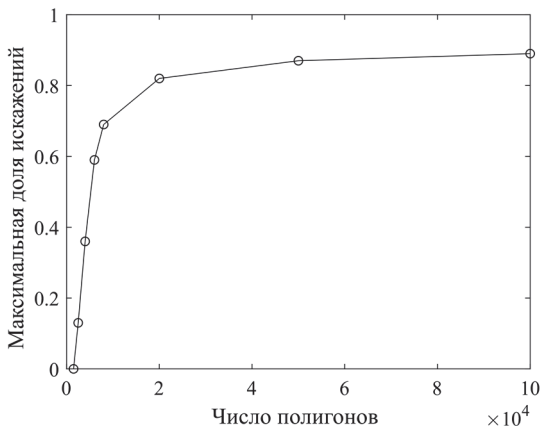


Рис. 12. Максимально допустимая доля удаленных объектов для карт различного размера

7. *Добавление вершин.* Данная атака смоделирована таким образом, чтобы при добавлении вершины на векторный объект его форма изменялась незначительно и оставалась естественной. Для этого случайно выбранные полигоны векторной карты подвергались преобразованию по следующему алгоритму.

На произвольно выбранном ребре полигона с координатами $(x_1, y_1), (x_2, y_2)$, $x_1 \leq x_2$ выбирается случайная точка (x_{edge}, y_{edge}) , $x_{edge} = x_1 + x_{shift}$, $y_{edge} = k_{edge} \cdot x_{edge} + b_{edge}$.

$$\text{Здесь } x_{shift} = \text{random}(0, x_2 - x_1), \quad k_{edge} = \begin{cases} \frac{(y_2 - y_1)}{(x_2 - x_1)}, & x_2 \neq x_1 \\ 0, & \text{иначе} \end{cases}$$

$$b_{edge} = y_2 - k_{edge} \cdot x_2.$$

В результате вычисляются координаты новой вершины: $(x_{edge}, y_{edge} + y_{shift})$, $y_{shift} = \text{random}(0, \frac{y_2 - y_1}{100})$.

В качестве параметра стойкости выбран коэффициент $k_{vertadd} = \frac{V_{add}}{V}$, где V – общее число вершин на карте, а V_{add} – число добавленных вершин.

Исследование показало, что последовательность ЦВЗ извлекается без ошибок даже в случае $k_{vertadd} = 10000$, то есть предлагаемый метод является стойким к атаке добавления вершин. Такой результат возникает вследствие особенностей предлагаемого подхода к встраиванию информации в полигональные объекты: во-первых, наибольшие значащие биты изображения ЦВЗ встраиваются путем изменения направления считывания вершин, которое, очевидно, не изменится при их добавлении. Во-вторых, несмотря на то что остальные биты ЦВЗ кодируются местоположением первой вершины, искусственно добавленные вершины должны быть расположены близко к остальным, в противном случае форма полигонального объекта будет сильно искажена. Таким образом, даже если добавленная вершина окажется первой в списке вершин, биты ЦВЗ будут извлечены верно, поскольку положение первой вершины относительно центра полигона практически не изменится.

8. Удаление вершин. Очевидно, если случайно удалять произвольные вершины, то многоугольные полигональные объекты могут стать треугольными: такая атака вряд ли будет реализована злоумышленником, поскольку в его интересах сохранить вид карты, близкий к первоначальному. В связи с этим при моделировании данной атаки множество вершин, которые потенциально можно удалить, было ограничено: данному преобразованию подвергались только полигоны, содержащие как минимум шесть вершин.

Суть данной атаки заключается в следующем: если произвольно выбранный полигон состоит из достаточного количества вершин, то одна из вершин, выбранная с помощью ДСЧ, удаляется. Если в случайно выбранном полигоне осталось менее 6 вершин, то этот объект пропускается.

В таблице 3 перечислены максимально допустимые коэффициенты $k_{vertdel} = \frac{V_{del}}{V}$ в зависимости от количества объектов на карте. Здесь V – общее число вершин на карте, а V_{del} – число удаленных вершин.

Очевидно, что в силу накладываемого ограничения вершины можно удалять только до тех пор, пока на карте есть многоугольники с шестью и более вершинами, то есть величина $k_{vertdel}$ ограничена сверху.

Таблица 3. Максимально допустимая доля удаленных вершин для карт различного размера

Число полигонов	2000	2500	3000	4000	8000	10000	20000	50000	100000
$k_{vertdel}$	0	0.2	0.2	+	+	+	+	+	+

Согласно полученным результатам $k_{vertdel}$ достигает максимума уже при $P \geq 4000$ (в таблице отмечено «+»), то есть предлагаемый метод является в полной мере устойчивым к атаке удаления вершин.

9. Переупорядочение вершин. Атака переупорядочивания вершин может быть реализована двумя способами: злоумышленник может либо сдвинуть вершины в списке на произвольную случайную величину (атака первого типа), либо хаотически задать направление обхода вершин для каждого полигона (атака второго типа).

Как было показано в разделе 2, встраивание информации в полигон реализуется как за счет сдвига порядка вершин, так и путем изменения направления их обхода (по часовой или против часовой стрелки в зависимости от старшего бита).

Моделирование обоих типов атаки переупорядочивания показало, что при кодировании старшей битовой плоскости изображения ЦВЗ посредством задания направления считывания вершин метод является стойким только к атаке первого типа. Если направление считывания вершин не учитывается, то метод является устойчивым только к атаке второго типа.

Тем не менее устойчивость к двум атакам одновременно может быть достигнута с помощью составного встраивания двух ЦВЗ: бинарный ЦВЗ (старшая битовая плоскость) – путем задания порядка обхода, полутоновый ЦВЗ (несколько старших битовых плоскостей, включая первую) – путем циклического сдвига списка вершин.

6. Исследование качества предложенного метода. В разделе 1 были перечислены основные требования, выдвигаемые к методам встраивания ЦВЗ. Настоящий раздел резюмирует полученные в работе результаты согласно каждому критерию качества.

1. Точность (визуальная неразличимость). Предлагаемый метод защиты авторских прав основан на принципе неискажающего встраивания, обеспечивающем неизменность значений координат вершин, в связи с чем ни злоумышленнику, ни легальному пользователю не удастся визуально определить наличие встроеной информации.

2. Информационная емкость. В задаче защиты авторских прав размер встраиваемого ЦВЗ не играет роли, поэтому длина последовательности ЦВЗ была выбрана наименьшей для обеспечения макси-

мальной стойкости к атакам. Однако, как показали исследования раздела 4, потенциальный объем встраиваемой информации достигает 80 бит при использовании детектора на основе пороговой обработки и 60 бит при использовании детектора на основе локальной фильтрации, что говорит о применимости метода в задаче проверки подлинности векторных карт, а также для стеганографической (скрытой) передачи информации внутри векторной карты.

3. *Стойкость.* Результаты экспериментов, приведенные в разделе 5, показывают, что при верно подобранных параметрах формирования шумоподобных изображений ЦВЗ предложенный метод встраивания ЦВЗ в векторные данные является в достаточной мере устойчивым ко всем возможным типам атак, направленных на удаление ЦВЗ. Для каждого преобразования показатели стойкости растут по мере увеличения размера векторной карты, при этом достаточный уровень этих показателей достигается уже при небольших размерах контейнера.

Таблица 4 объединяет результаты анализа стойкости для всех исследуемых типов преобразований. В таблице каждая строка отображает показатели стойкости к конкретному преобразованию (1 – сдвиг; 2 – масштабирование; 3 – поворот; 4 – кадрирование; 5 – добавление объектов; 6 – удаление объектов; 7 – добавление вершин; 8 – удаление вершин; 9 – переупорядочение вершин) в зависимости от размера карты. Плюс обозначает инвариантность к преобразованию; V – суммарное число вершин; V_{max} – максимальное число вершин, которые могут быть удалены.

Таблица 4. Результаты исследования стойкости

P , тыс.	2	3	4	6	8	10	20	50	100
1	+	+	+	+	+	+	+	+	+
2	+	+	+	+	+	+	+	+	+
3	0°	5°	5°	15°	20°	20°	25°	25°	25°
4	3%	5%	5%	7%	12%	26%	43%	43%	43%
5	$0,05 \cdot P$	$0,15 \cdot P$	$0,21 \cdot P$	$0,5 \cdot P$	$0,61 \cdot P$	$0,72 \cdot P$	$1,93 \cdot P$	$6,34 \cdot P$	$8,83 \cdot P$
6	$0,05 \cdot P$	$0,29 \cdot P$	$0,36 \cdot P$	$0,59 \cdot P$	$0,69 \cdot P$	$0,71 \cdot P$	$0,82 \cdot P$	$0,87 \cdot P$	$0,89 \cdot P$
7	+	+	+	+	+	+	+	+	+
8	0	$0,2 \cdot V$	V_{max}	V_{max}	V_{max}	V_{max}	V_{max}	V_{max}	V_{max}
9	+	+	+	+	+	+	+	+	+

4. *Безопасность.* Непредсказуемость встраиваемых изображений ЦВЗ обеспечивается за счет рандомизации значений импульсов

синтезируемых спектров. Согласно формуле (1) каждый импульс может принимать 1 из 90 значений. Таким образом, для последовательности длины L существует 90^{L+1} комбинаций вещественной части комплексного спектра и столько же комбинаций мнимой, что в совокупности дает $90^{2(L+1)}$ различных изображений ЦВЗ для каждой бинарной последовательности из конечного множества мощности 2^L .

5. *Вычислительная сложность.* Далее приведены результаты оценки вычислительной сложности для предлагаемых в составе метода алгоритмов.

Эксперименты проводились на вычислительной машине с характеристиками, приведенными в таблице 5. Полученные результаты приведены в таблицах 6-9.

Таблица 5. Параметры вычислительной машины

Тип обеспечения	Характеристика
Процессор	CPU Intel Core i5-2400, 4-ядерный, 3100 МГц
Оперативная память	16 Гб
Операционная система	Windows 7 Professional (x64)

Таблица 6. Среднее время синтеза шумоподобного изображения

Размер, пикселей	512×512	1024×1024	2048×2048
Время, мс	59	344	1536

Таблица 7. Среднее время встраивания растрового изображения в карту

Размер, полигонов	2500	5000	10000	20000	50000	100000
Время, мс	413	421	470	574	1754	6653

Таблица 8. Среднее время извлечения растрового изображения из карты

Размер, полигонов	2500	5000	10000	20000	50000	100000
Время, мс	69	80	91	115	380	1657

Таблица 9. Среднее время извлечения последовательности ЦВЗ алгоритмом детектирования на основе локальной фильтрации

Размер, пикселей	512×512	1024×1024	2048×2048
Время, мс	611	3589	20079

Согласно результатам проведенных экспериментов, а также согласно данным таблицы 1 обработка больших карт (от 100 тысяч полигональных объектов) и соответствующих им изображений ЦВЗ (2048×2048) требует больших вычислительных ресурсов. Время, необходимое для реализации процедур встраивания и извлечения ЦВЗ, можно сократить путем разбиения больших карт на фрагменты меньшего размера, которые могут быть обработаны как последовательно, так и параллельно.

7. Заключение. Предложен метод защиты векторных картографических данных от несанкционированного распространения с помощью стойких цифровых водяных знаков.

Метод сочетает оригинальные авторские идеи, а именно: подход к встраиванию скрытой защитной информации, не искажающий координатную информацию векторных объектов, и синтез шумоподобных сигналов, отображающих битовую последовательность в виде растрового изображения, непосредственно встраиваемого в защищаемые данные.

В сравнении с предыдущими исследованиями авторов, проведенными в рамках решения задач защиты векторных данных, значительно повышена стойкость встраиваемых шумоподобных ЦВЗ путем модификации алгоритма извлечения битовых ЦВЗ.

Проведен анализ качества метода по критериям точности, стойкости, информационной емкости, вычислительной сложности. Результаты всех проведенных исследований подтверждают применимость и эффективность предложенного метода защиты векторных картографических данных, а также его преимущества перед существующими методами встраивания ЦВЗ.

Применимость предложенного метода в задаче защиты авторских прав на векторные карты подтверждается тем, что входящие в его состав алгоритмы не влияют на точность координатных значений и при этом обеспечивают стойкость к аффинным преобразованиям, кадрированию, добавлению, удалению и переупорядочиванию вершин/объектов векторного слоя.

Единственное ограничение накладывает сама идея неискажающего встраивания, основанная на замкнутости полигональных объектов: точки и линии не могут служить контейнером для встраивания.

Развитие предложенного подхода к защите векторных данных планируется вести в следующих направлениях:

- более детальное исследование шумоподобных сигналов, направленное на повышение информационной емкости ЦВЗ и их устойчивости к злоумышленным атакам;
- разработка методов аутентификации векторных данных и алгоритмов локализации нелегитимных изменений;
- разработка алгоритмов встраивания ЦВЗ в трехмерные векторные данные для защиты от несанкционированного распространения и изменений.

Литература

1. *Abubahia A., Cocea M.* Advancements in GIS map copyright protection schemes – a critical review // *Multimedia Tools and Applications*. 2017. vol. 76. no. 10. pp. 12205–12231.
2. *Peng Y., Yue M.* A Zero-Watermarking Scheme for Vector Map Based on Feature Vertex Distance Ratio // *Journal of Electrical and Computer Engineering*. 2015. vol. 2015. pp. 1–6.
3. *Li A., Lin B.-X., Chen Y.A.* Study on copyright authentication of GIS vector data based on Zero-watermarking // *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*. 2008. vol. 37(B4). pp. 1783–1786.
4. *Ren N., Wang Q., Zhu C.* Selective authentication algorithm based on semi-fragile watermarking for vector geographical data // *22nd International Conference on Geoinformatics*. 2014. vol. 1. pp. 1–6.
5. *Da Q. et al.* A Novel Hybrid Information Security Scheme for 2D Vector Map // *Mobile Networks and Applications*. 2018. vol.1. pp. 1–9.
6. *Wang N., Bian J., Zhang H.* RST Invariant Fragile Watermarking for 2D Vector Map Authentication // *International Journal of Multimedia and Ubiquitous Engineering*. 2015. vol. 10. no. 4. pp. 155–172.
7. *Kim J.* Robust Vector Digital Watermarking Using Angles and a Random Table // *Advances in Information Sciences and Service Sciences*. 2010. vol. 2. no.4.
8. *Lee S.H., Kwon K.R.* Vector watermarking scheme for GIS vector map management // *Multimedia Tools and Applications*. 2013. vol. 63. no. 3. pp. 757–790.
9. *Peng Z., Yue M., Wu X., Peng Y.* Blind watermarking scheme for polylines in vector geospatial data // *Multimedia Tools and Applications*. 2015. vol. 74. pp. 11721–11739.
10. *Wang Y., Yang C., Zhu C.* A multiple watermarking algorithm for vector geographic data based on coordinate mapping and domain subdivision // *Multimedia Tools and Applications*. 2017. pp. 1–19.
11. *Voigt M., Busch C.* Watermarking 2D-vector data for geographical information systems // *Proceedings of the SPIE, security and watermarking of multimedia content*. 2002. vol. 4675. pp. 621–628.
12. *Ohbuchi R., Ueda H., Endoh S.* Robust Watermarking of Vector Digital Maps // *Proceedings of IEEE International Conference on Multimedia and Expo*. 2002. vol. 1. pp. 577–580.
13. *Peng Y., Lan H., Yue M., Xue Y.* Multipurpose watermarking for vector map protection and authentication // *Multimedia Tools and Applications*. 2017. vol. 77. no.1. pp. 1–21.
14. *Peng F., Yan Z.J., Long M.* A Reversible Watermarking for 2D Vector Map Based on Triple Differences Expansion and Reversible Contrast Mapping // *LNCS*. 2017. vol. 10658. pp. 147–158.
15. *Wang N., Zhao X., Xie C.* RST Invariant Reversible Watermarking for 2D Vector Map // *International Journal of Multimedia and Ubiquitous Engineering*. 2016. vol. 11. no. 2. pp. 265–276.
16. *Cao L., Men C., Li X.* Iterative Embedding-Based Reversible watermarking for 2d-Vector Maps // *Proceedings of 17th IEEE International Conference on Image Processing (ICIP)*. 2010. vol. 1. pp. 3685–3688.
17. *Wang N., Men C.* Reversible Watermarking for 2-D Vector Map Authentication with Localization // *Computer Aided Design Journal*. 2012. vol. 44. no. 4. pp. 230–330.
18. *Выборнова Ю.Д., Сергеев В.В.* Метод защиты векторных карт с использованием изображения ЦВЗ как вторичного контейнера // *Компьютерная оптика*. 2019. Т. 43. № 3. С. 474–483.
19. *Глумов Н.И., Митекин В.А.* Алгоритм поблочного встраивания стойких ЦВЗ в крупноформатные изображения // *Компьютерная оптика*. 2011. Т. 35. № 3. С. 368–372.

20. *Vybornova Y.D.* Application of spatial interpolation methods for restoration of partially defined images // CEUR Workshop Proceedings. 2018. vol. 2210. pp. 89–95.
21. *Выборнова Ю.Д., Сергеев В.В.* Новый метод встраивания цифровых водяных знаков в векторные картографические данные // Компьютерная оптика. 2017. Т. 41. № 6. С. 913–919.

Выборнова Юлия Дмитриевна – канд. техн. наук, младший научный сотрудник, научно-исследовательская лаборатория геоинформатики и информационной безопасности, Федеральное государственное автономное образовательное учреждение высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева» (Самарский университет). Область научных интересов: защита данных, криптография, цифровые водяные знаки, обработка изображений. Число научных публикаций – 18. vybornovamail@gmail.com; ул. Лукачева, 39Б, 443086, Самара, Россия; р.т.: 8 (846) 267-49-05.

Сергеев Владислав Викторович – д-р техн. наук, профессор, директор, институт информатики, математики и электроники, Федеральное государственное автономное образовательное учреждение высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева» (Самарский университет); ведущий лабораторией, лаборатория математических методов обработки изображений, Институт систем обработки изображений РАН (ИСОИ РАН) – филиал ФНИЦ «Кристаллография и фотоника» РАН. Область научных интересов: цифровая обработка сигналов, анализ изображений, распознавание образов, геоинформатика, информационная безопасность. Число научных публикаций – около 300. vserg@geosamara.ru; ул. Лукачева, 39Б, 443086, Самара, Россия; р.т.: 8 (846) 267-49-06.

Поддержка исследований. Исследование выполнено при финансовой поддержке РФФИ в рамках научных проектов № 19-07-00474, № 19-29-09045, № 20-37-70053, № 19-07-00138.

Y. VYBORNOVA, V. SERGEEV
**METHOD FOR PROTECTION OF COPYRIGHT ON VECTOR
DATA**

Vybornova Y., Sergeev V. Method for Protection of Copyright on Vector Data.

Abstract. The paper proposes a method of copyright protection for vector maps, based on the embedding of raster digital watermarks. The method combines original ideas, namely, a vector data watermarking approach that does not distort the coordinate information of vector objects and embedding of noise-like images that encode a binary sequence. The use of noise-like carrier allows to simplify the verification procedure, and also to ensure the resistance of the hidden bit sequence to distortions, including interpolation errors. In comparison with previous investigations made by the authors when solving problems of vector data protection, the robustness of the embedded noise-like digital watermarks has been significantly increased by developing a new algorithm for detection of the binary sequence hidden in the spectrum of a noise-like image. The purpose of the experimental studies was to assess the attainable probability of correct sequence extraction for various parameters and embedding conditions. The study of information capacity showed that the potential amount of information embedded in each polygon without distorting the watermark sequence depends on the type of a map, namely on the number of vertices that make up each polygon. An experimental study on robustness against potentially possible transformations aimed at maliciously deleting the digital watermark from the vector map is performed. The developed method demonstrates resistance to affine transformations, cropping, addition, removal and reordering of vertices / objects, and, thus, seems to be the optimal solution to the problem of copyright protection for vector data. The analysis of the method quality according to the criteria of accuracy, durability, information capacity, and computational complexity is performed. The results of all conducted studies confirm the efficiency and the effectiveness of the proposed method for vector map protection, as well as its distinct advantage over the prior art.

Keywords: Geographic Information Systems, Vector Map, Copyright Protection, Digital Watermarking, Raster Image, Discrete Fourier Transform, Pseudorandom Sequences

References

1. Abubahia A., Cocea M. Advancements in GIS map copyright protection schemes – a critical review. *Multimedia Tools and Applications*. 2017. vol. 76. no. 10. pp. 2205–2231.
2. Peng Y., Yue M. A Zero-Watermarking Scheme for Vector Map Based on Feature Vertex Distance Ratio. *Journal of Electrical and Computer Engineering*. 2015. pp. 1–6.
3. Li A., Lin B.-X., Chen Y.A. Study on copyright authentication of GIS vector data based on Zero-watermarking. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*. 2008. vol. 37 (B4). pp. 1783–1786.
4. Ren N., Wang Q., Zhu C. Selective authentication algorithm based on semi-fragile watermarking for vector geographical data. *22nd International Conference on Geoinformatics*. 2014. vol. 1. pp. 1–6.
5. Da Q. et al. A Novel Hybrid Information Security Scheme for 2D Vector Map. *Mobile Networks and Applications*. 2018. vol. 1. pp. 1–9.
6. Wang N., Bian J., Zhang H. RST Invariant Fragile Watermarking for 2D Vector Map Authentication. *International Journal of Multimedia and Ubiquitous Engineering*. 2015. vol.10. no.4. pp. 155–172.
7. Kim J. Robust Vector Digital Watermarking Using Angles and a Random Table. *Advances in Information Sciences and Service Sciences*. 2010. vol. 2. no. 4.

8. Lee S.H., Kwon K.R. Vector watermarking scheme for GIS vector map management. *Multimedia Tools and Applications*. 2013. vol. 63. no. 3. pp. 757–790.
9. Peng Z., Yue M., Wu X., Peng Y. Blind watermarking scheme for polylines in vector geo-spatial data. *Multimedia Tools and Applications*. 2015. vol. 74. pp. 11721–11739.
10. Wang Y., Yang C., Zhu C. A multiple watermarking algorithm for vector geographic data based on coordinate mapping and domain subdivision. *Multimedia Tools and Applications*. 2017. pp. 1–19.
11. Voigt M., Busch C. Watermarking 2D-vector data for geographical information systems. *Proceedings of the SPIE*. 2002. vol. 4675. pp. 621–628.
12. Ohbuchi R., Ueda H., Endoh S. Robust Watermarking of Vector Digital Maps. *Proceedings of IEEE International Conference on Multimedia and Expo*. 2002. pp. 577–580.
13. Peng Y., Lan H., Yue M., Xue Y. Multipurpose watermarking for vector map protection and authentication. *Multimedia Tools and Applications*. 2017. vol. 77. no. 1. pp. 1–21.
14. Peng F., Yan Z.J., Long M. A Reversible Watermarking for 2D Vector Map Based on Triple Differences Expansion and Reversible Contrast Mapping. *LNCS*. 2017. vol. 10658. pp. 147–158.
15. Wang N., Zhao X., Xie C. RST Invariant Reversible Watermarking for 2D Vector Map. *International Journal of Multimedia and Ubiquitous Engineering*. 2016. vol. 11. no. 2. pp. 265–276.
16. Cao L., Men C., Li X. Iterative Embedding-Based Reversible watermarking for 2d-Vector Maps. *Proceedings of 17th IEEE International Conference on Image Processing (ICIP)*. 2010. vol. 1. pp. 3685–3688.
17. Wang N., Men C. Reversible Watermarking for 2-D Vector Map Authentication with Localization. *Computer Aided Design Journal*. 2012. vol. 44. no. 4. pp. 230–330.
18. Vybornova Y.D., Sergeev V.V. [New method for GIS vector data protection based on the use of secondary watermark]. *Komp'yuternaya optika – Computer Optics*. 2019. Issue 43. vol. 3. pp. 474–483. (In Russ.).
19. Glumov N.I., Mitekin V.A. [The new blockwise algorithm for large-scale images robust watermarking]. *Komp'yuternaya optika – Computer Optics*. 2011. Issue 35. vol. 3. pp. 368–372. (In Russ.).
20. Vybornova, Y.D. Application of spatial interpolation methods for restoration of partially defined images. *CEUR Workshop Proceedings*. 2018. vol. 2210. pp. 89–95.
21. Vybornova Y.D., Sergeev V.V. [A new watermarking method for vector map data]. *Komp'yuternaya optika – Computer Optics*. 2017. vol. 41. no. 6. pp. 913–919. (In Russ.).

Yuliya Vybornova – Ph.D., Research Fellow, Laboratory of Geoinformatics and Information Security, Samara National Research University. Research interests: data protection, cryptography, digital watermarking, image processing. The number of scientific publications – 18. vybornovamail@gmail.com; Lukacheva str., 39B, 443086, Samara, Russia; office phone: +7 (846) 267-49-05.

Vladislav Sergeev – Ph.D., Dr. Sci., Professor, Director, Institute of Informatics, Mathematics and Electronics, Samara National Research University; Head of the Laboratory, Laboratory of Mathematical Methods for Image Processing, Image Processing Systems Institute of the RAS – Branch of the FSRC “Crystallography and Photonics” RAS. Research interests: digital signal processing, image analysis, pattern recognition, geoinformatics, information security. The number of scientific publications is about 300. vsereg@geosamara.ru; Lukacheva str., 39B, 443086, Samara, Russia; office phone: +7 (846) 267-49-06.

Acknowledgements. The reported study was funded by RFBR (Russian Foundation for Basic Research): projects № 19-07-00474, № 19-29-09045, № 20-37-70053, № 19-07-00138.