УДК 004.56+003.26

М. Г. Савельева, П. П. Урбанович
Белорусский государственный технологический университет

МЕТОД СТЕГАНОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ WEB-ДОКУМЕНТОВ НА ОСНОВЕ РАСТРОВОЙ ГРАФИКИИ МОДЕЛИ RGB

Представлены метод и реализующие его алгоритмы стеганографического преобразования, использующие в качестве контейнера элементы web-приложения на основе растровой графики. В качестве базового элемента контейнера, цветовые параметры которого модифицируются в модели RGB при осаждении информации, выступает пиксель изображения. Внедрение (извлечение) информации происходит в пикселях, имеющих одинаковое значение (одно из 256) в одном или нескольких цветовых каналах. Особенностью разработанного метода является то, что процессы внедрения (извлечения) информации осуществляются при сравнительном анализе значений одного или двух цветовых координат базового пикселя и пикселя для внедрения. Количество каналов (R, G, B) для выбора пикселей и для внедрения сообщения зависит от цветовых характеристик изображения и длины (объема) сообщения. В изображениях с большим количеством полутонов, монохроматических или черно-белых изображениях выбор пикселей, в которых будет происходить внедрение, целесообразно осуществлять по двум цветовым каналам. При этом непосредственно для внедрения информации в выбранные пиксели целесообразно использовать один канал. В полноцветных изображениях можно ограничиться одним каналом для выбора пикселей. Использовать одни и те же каналы для внедрения и выбора пикселей нельзя, так как их суммарное количество должно быть не более трех. Пропускная способность метода зависит от характеристик изображения-контейнера.

Ключевые слова: стеганография, авторское право, изображение, осаждение, алгоритм, модель, цвет, пространственная область.

Для цитирования: Савельева М. Г., Урбанович П. П. Метод стеганографического преобразования web-документов на основе растровой графики и модели RGB // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. 2022. № 2 (260). С. 99–107.

M. G. Saveleva, P. P. Urbanovich
Belarusian State Technological University

METHOD OF STEGANOGRAPHIC TRANSFORMATION OF WEB-DOCUMENTS BASED ON RASTER GRAPHICS AND RGB MODEL

The method and algorithms of steganographic transformation implementing it, using elements of a web application based on raster graphics as a container, are presented. The image pixel acts as the base element of the container, the color parameters of which are modified in the RGB model when information is deposited. Information is embedded/extracted in pixels having the same value (one of 256) in one or more color channels. The peculiarity of the developed method is that the processes of embedding/extracting information are carried out with a comparative analysis of the values of one or two color coordinates of the base pixel and the pixel for embedding. The number of channels (R, G, B) for selecting pixels and for embedding a message depends on the color characteristics of the image and the length (volume) of the message. In images with a large number of halftones, monochromatic or black-and-white images, it is advisable to select pixels in which the embedding will take place using two color channels. At the same time, it is advisable to use one channel directly to embed information into the selected pixels. In full-color images, you can limit yourself to one channel for selecting pixels. It is impossible to use the same channels for embedding and selecting pixels, since their total number should be no more than three. The throughput of the method depends on the characteristics of the container image.

Key words: steganography, copyright, image, precipitation, algorithm, color, spatial domain.

For citation: Saveleva M. G., Urbanovich P. P. Method of steganographic transformation of web-documents based on raster graphics and RGB model. *Proceedings of BSTU, issue 3, Physics and Mathematics. Informatics*, *2022*, no. 2 (260), pp. 99–107 (In Russian).

Введение. При разработке web-приложений используются технологии на основе как растровой, так и векторной графики. С помощью растровой графики (форматы JPEG, GIF, PNG, ICO, BMP) можно создавать графические объекты практически различной сложности. В этом заключается

ее преимущество. Однако необходимо учитывать, что растровые рисунки могут терять качество при их масштабировании.

Доступность цифрового контента, легкость, с которой могут быть сделаны идеальные копии электронных документов, вызывает обоснованные опасения по поводу защиты авторских прав и требует разработки соответствующих методов и инструментальных средств для решения задач по защите этого права [1]. Одним из основных направлений разработки упомянутых средств является стеганография.

Как известно, стеганографическая система, которая не требует предварительного обмена некоторой секретной информацией (например, стеганографическим ключом), относится к так называемой «чистой стеганографии» [2]. Формально процесс встраивания (осаждения) тайных сообщений M, с помощью которого, в частности, можно решать упомянутую задачу защиты авторского права на контент, содержащийся в документах из множества C, можно описать как отображение E:

$$E : C \cdot M \rightarrow S. \qquad (1)$$

Процесс извлечения M из стеганоконтейнеров S (документов C с размещенной в нем авторской информацией M) описывается функцией, обратной к E:

$$D = E^{-1} : S \rightarrow M, C. \qquad (2)$$

Очевидно, необходимо, чтобы объем (длина) контейнера был не меньше объема (длины) осаждаемого сообщения.

И отправитель, и получатель должны иметь доступ к алгоритмам внедрения и извлечения тайного сообщения. Но эти алгоритмы не должны быть общедоступными, поскольку они могут соотноситься с ключом стенографического преобразования. В большинстве практических стеганографических систем набор C выбирается таким образом, чтобы он состоял из осмысленных и безвредных сообщений.

Некоторые стеганографические методы сочетают традиционную криптографию со стеганографией: отправитель шифрует секретное сообщение до процесса внедрения. Очевидно, что такая комбинация повышает безопасность всего процесса коммуникации, так как злоумышленнику сложнее обнаружить встроенный в контейнер шифротекст. Сильные стеганографические системы, однако, не нуждаются в предварительном шифровании [3].

Существуют различные подходы к классификации стеганографических методов. В качестве критерия для классификации может использоваться тип контейнера, методы модификации некоторых элементов или параметров документа-контейнера, за счет чего, собственно, и реализуется внедрение секретного сообщения [4].

Для второго подхода актуальны два основных принципа [3, 5, 6]:

– файлы, содержащие оцифрованное изображение или звук, могут быть до некоторой степени видоизменены без потери функциональности, в отличие от других типов данных, требующих абсолютной точности;

– неспособность органов чувств человека различить незначительные изменения в цвете изображения или качестве звука, что особенно легко использовать применительно к объекту, несущему избыточную информацию, будь то 16-битный звук, 8-битное или, еще лучше, 24-битное изображение (если речь идет об изображении, то изменение значений наименее важных битов, отвечающих за цвет пикселя, не приводит к сколь-нибудь заметному для человека изменению цвета, что также объясняет невозможность использовать изменение значений яркости для внедрения секретной информации).

Стеганографическая система на основе секретного ключа похожа на симметричную криптосистему: отправитель выбирает контейнер c ($c \in C$) и внедряет секретное сообщение m ($m \in M$) в c с помощью секретного ключа k ($k \in K$). Массив из шести множеств:

$$\xi = < C, M, K, S, D_K, E_K >, \qquad (3)$$

где

$$E_K : C \cdot M \cdot K \rightarrow S; \qquad (4)$$

$$D_K : C \cdot K \rightarrow M \qquad (5)$$

описывают стеганосистему с одним или несколькими стеганографическими ключами [7].

Формулы (4) и (5) справедливы только со свойством:

$$D_K(E_K(c, m, k), k) = m; (D_K)^{-1} = E_K. \qquad (6)$$

Известны стеганографические методы, основанные на преобразовании цветовых параметров (RGB) контента [3, 8, 9] и использовании модели системы в соответствии с (3)–(5).

Предметом анализа в данной статье являются новый стеганографичекий метод и реализующие его алгоритмы на основе модификации цветовых параметров текстовых элементов web-приложений на базе растровой графики.

Основная часть. Особенностью разработки цветовых компонент web-приложений является наличие известной палитры Websafe, состоящей из 216 (из общего числа – 256) основных цветовых оттенков, которые были отобраны для кросс-платформенной работы. Эти оттенки отображаются максимально точно независимо от монитора компьютера или выбранного браузера, способного отображать, по крайней мере, 8-битный цвет (256 цветов) при использовании в HTML, CSS и в изображениях, встроенных в

web-страницы. Это позволяет разработчикам указывать цвета таким образом, чтобы интегрировать их в графическую среду операционной системы.

RGB – цветовая модель, представление цвета которой задается совокупностью трех цветовых каналов: красного, зеленого и синего. Каждый из каналов имеет размер в один байт, из чего следует, что цвет одного пикселя представляется в виде трех байтов. Каждый цветовой канал задается 8-разрядным двоичным вектором либо соответствующим десятичным числом [3, 8, 9].

Далее рассмотрим алгоритмические особенности реализации предлагаемого метода, в котором внедрение информации производится путем модификации цвета пикселей в цветовой модели RGB (рис. 1).

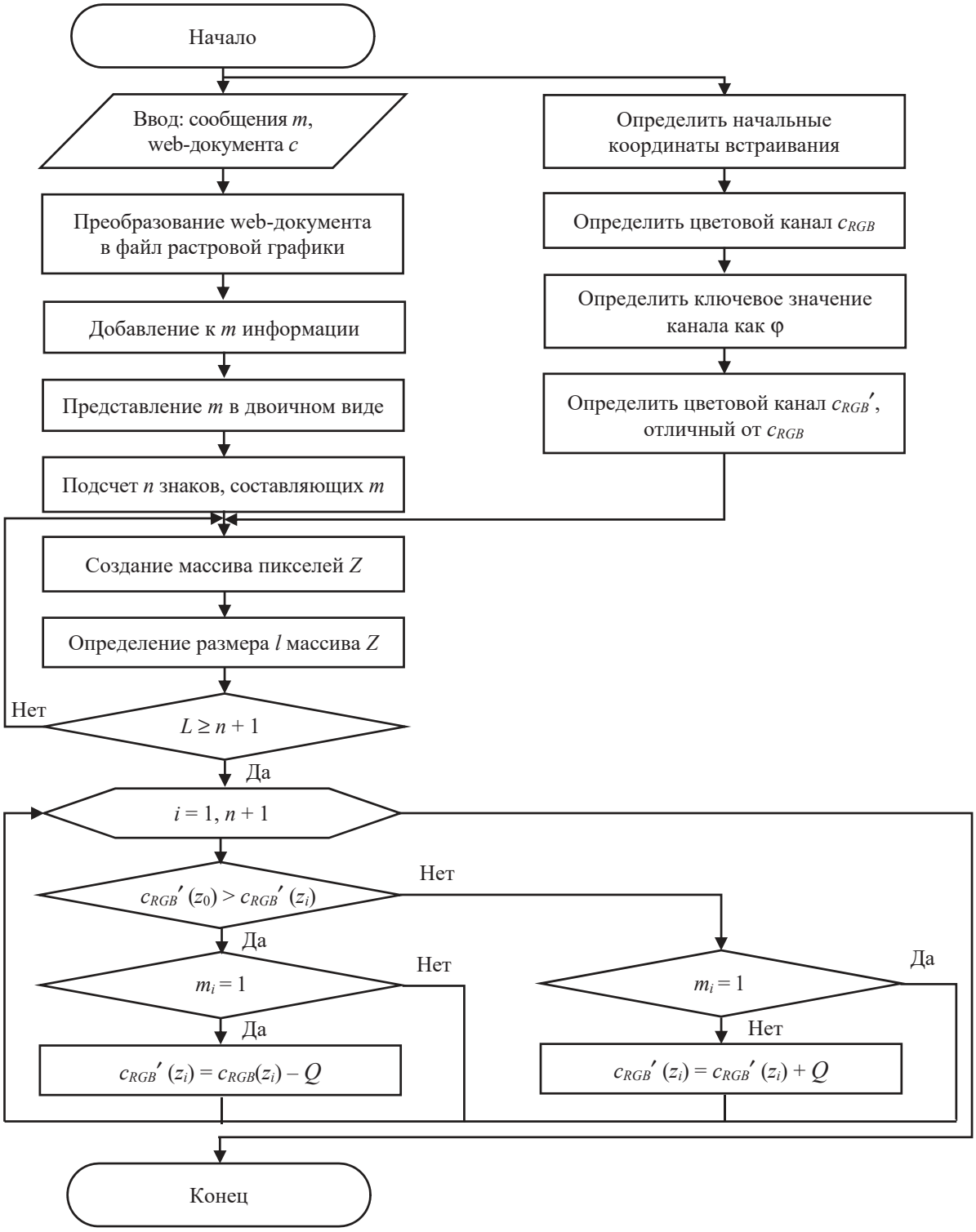

Рис. 1. Алгоритм внедрения сообщения

Данный метод подразумевает рассмотрение, например, текстового документа как объекта растровой графики. В качестве базового элемента контейнера (c), свойства которого модифицируются при осаждении информации (m), выступает пиксель изображения, входящего в массив пикселей, служащих для отображения символа текста.

Начальным шагом алгоритма прямого преобразования (в соответствии с (4)) является конвертирование web-документа (c) в файл растровой графики формата, например PNG (без сжатия), и генерация секретного сообщения (m). Примем параметры (в пикселях) контейнера c: t – высота, r – ширина; длина (объем) внедряемого сообщения – N_m.

Сообщение m необходимо преобразовать для его внедрения и обеспечения возможности извлечения. Поскольку при извлечении сообщения необходимо указать окончание сообщения, то к нему следует добавить вспомогательную информацию: число разрядов длины сообщения, длину сообщения. На данном этапе используется кодировка ASCII, в которой один символ представлен 8 битами. Следовательно, N_m = length (m) · 8, бит. Для примера реализации метода используем сообщение «стего» (m = «*стего*»), length (m) = 5. После добавления вспомогательной информации осаждаемое сообщение принимает вид «15 стего» (m_1 – число разрядов длины сообщения, m_2 – длина сообщения, m_3, .., m_7 – исходное сообщение), т. е. length (m) = 7. Следовательно, $N_m = 7 \cdot 8 = 56$ бит. Итоговое сообщение m в двоичном виде: 00110001 00110101 11110001 11110010 11100101 11100011 11101110.

Для внедрения m необходимо выбрать массив пикселей, для которых совпадает значение координат одного или двух цветовых каналов. В изображениях с большим количеством полутонов (рис. 2, 3, розово-фиолетовые полутона), монохроматических (рис. 4, 5, синий цвет) или черно-белых (рис. 6, 7) изображений выбор пикселей, в которых будет происходить внедрение, целесообразно осуществлять по двум цветовым каналам. При этом непосредственно для внедрения информации в выбранные пиксели следует использовать один канал. В полноцветных изображениях также можно ограничиться одним каналом для выбора пикселей.

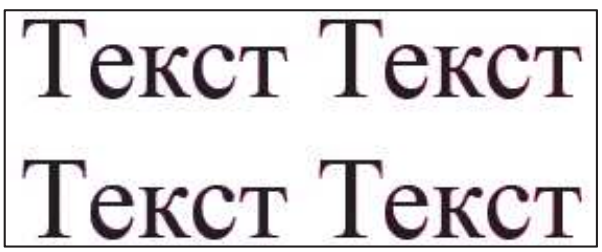

Рис. 2. Изображение-контейнер с большим количеством полутонов

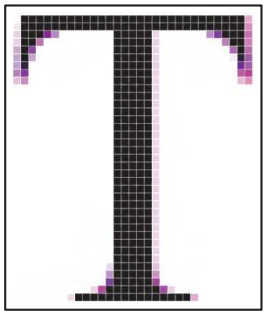

Рис. 3. Фрагмент изображения-контейнера с большим количеством полутонов

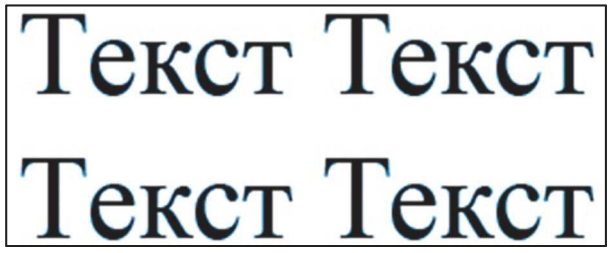

Рис. 4. Монохромное изображение-контейнер

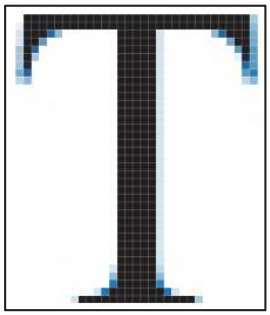

Рис. 5. Фрагмент монохромного изображения-контейнера

Рис. 6. Черно-белое изображение-контейнер

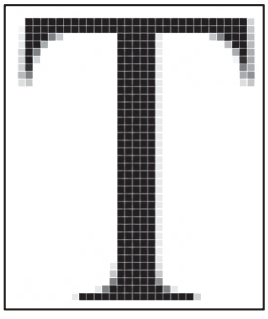

Рис. 7. Фрагмент черно-белого изображения-контейнера

Для демонстрации метода используем в качестве контейнера черно-белое изображение (рис. 6).

Ключевым этапом алгоритма внедрения является выбор массива пикселей, Z. Алгоритм создания массива Z представлен на рис. 8, где c_{RGB} – цветовой канал с совпадающими цветовыми параметрами пикселя, $c_{RGB} \in R, G, B$; c_{RGB}' – цветовой канал для внедрения сообщения, $c_{RGB}' \in R, G, B$; s_{jn} – пиксель web-документа, $s_{00}, .., s_{jn} \in c$; t – ширина c в пикселях; r – высота c в пикселях; φ – ключевое значение цветового кода канала c_{RGB}, $\varphi \in \{0, 1, \ldots, 255\}$. Последний параметр используется для увеличения пропускной способности метода. Для этого следует провести анализ того, в каком цветовом канале имеется больше пикселей с одинаковым значением цветового кода (c_{RGB}) и выбрать это значение в качестве параметра φ. Канал для внедрения (c_{RGB}') выбирается произвольно из оставшихся двух (или оба). Канал c_{RGB}' не должен использоваться при выборе массива пикселей Z. Например, после проанализированного фрагмента изображения-контейнера (рис. 9) (пиксели, имеющие черный (0, 0, 0) и белый (255, 255, 255) цвета, не отмечены) можно сказать, что $c_{RGB} = R$, $c_{RGB}' = G$ (как следующий после R), φ = 233. После проведенного анализа также можно отметить, что в данном фрагменте контейнера для выбора пикселей достаточно одного цветового канала, так как количество пикселей для внедрения сообщения превышает необходимое (при выборе по двум каналам их станет меньше, чем нужно). В целях упрощения и повышения наглядности метода используем один цветовой канал для внедрения.

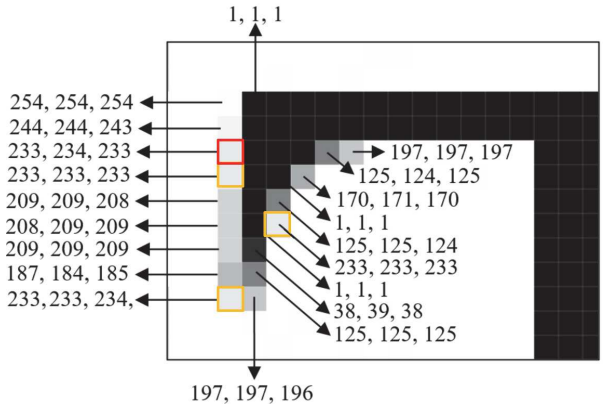

Рис. 9. Фрагмент черно-белого изображения-контейнера

Из массива Z выбирается базовый пиксель. Внедрение m будет происходить в канал c_{RGB}' при сравнении значений цветовых кодов канала c_{RGB}' пикселя для внедрения ($c_{RGB}'(z_0)$) ($z_0..z_i \in Z$) и базового пикселя ($c_{RGB}'(z_i)$). В данном примере базовым пикселем выбран первый (с цветовым кодом 233, 234, 233) (рис. 9, 10). Далее внедрение будет происходить при сравнении значений кода канала G базового (первого) и второго, базового и третьего и т. д.; в конечном итоге – базового и n-го пикселей массива Z.

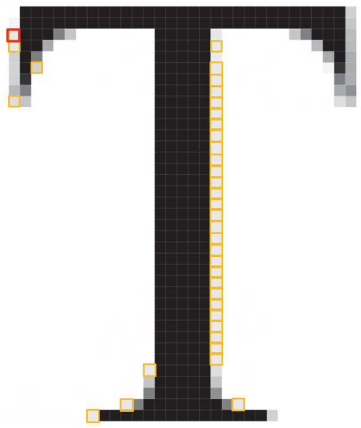

Рис. 10. Первый 31 пиксель массива Z

Следующим шагом алгоритма внедрения (см. рис. 1) является проверка необходимости изменений значения цветового кода канала для внедрения. С этой целью производится сравнительный анализ $c_{RGB}'(z_0)$ и $c_{RGB}'(z_i)$. Примем, что в случае, если $c_{RGB}'(z_0) > c_{RGB}'(z_i)$, то бит внедряемого сообщения равен 0. Если $c_{RGB}'(z_0) \le c_{RGB}'(z_i)$, то бит внедряемого сообщения равен 1. Если бит, полученный при сравнении цветовых кодов канала пикселя для внедрения и базового пикселя, не совпадает с битом внедряемого сообщения, то $c_{RGB}'(z_i)$ нужно изменить на Q, где Q – число для модификации значений цветовых кодов каналов и выбора массива пикселей (рекомендуется выбирать $4 < Q < 10$, так как существенное изменение цветового кода пикселя будет заметно человеческому глазу). Если бит сообщения равен 1, а $c_{RGB}'(z_0) > c_{RGB}'(z_i)$, то $c_{RGB}'(z_i) = c_{RGB}'(z_i) - Q$, если же бит сообщения равен 0, а $c_{RGB}'(z_0) \le c_{RGB}'(z_i)$, то $c_{RGB}'(z_i) = c_{RGB}'(z_i) + Q$.

В примере цветовой код первого (базового) пикселя z_0 массива Z – 233, 234, 233, код второго пикселя z_1 массива Z – 233, 233, 233. При сравнении значений канала $c_{RGB}'(G)$ получаем бит сообщения, равный 0 (234 > 233 ($c_{RGB}'(z_0) = 234$, $c_{RGB}'(z_1) = 233$)). Так как нам необходимо внедрить 0, то $c_{RGB}'(z_1)$ изменять не нужно. Цветовой код z_1 после внедрения – 233, 233, 233. Цветовой код третьего пикселя (z_2) массива Z – 233, 235, 234. При сравнении значений цветового кода канала G пикселя для внедрения и базового пикселя получаем бит сообщения, равный 1 (234 < 235 ($c_{RGB}'(z_0) = 234$, $c_{RGB}'(z_2) = 235$)). Так как нам необходимо внедрить 0, то $c_{RGB}'(z_2)$ нужно изменить на Q ($Q = 4$). Цветовой код (z_2) после внедрения – 233, 231, 234. Аналогично обрабатываются все остальные пиксели.

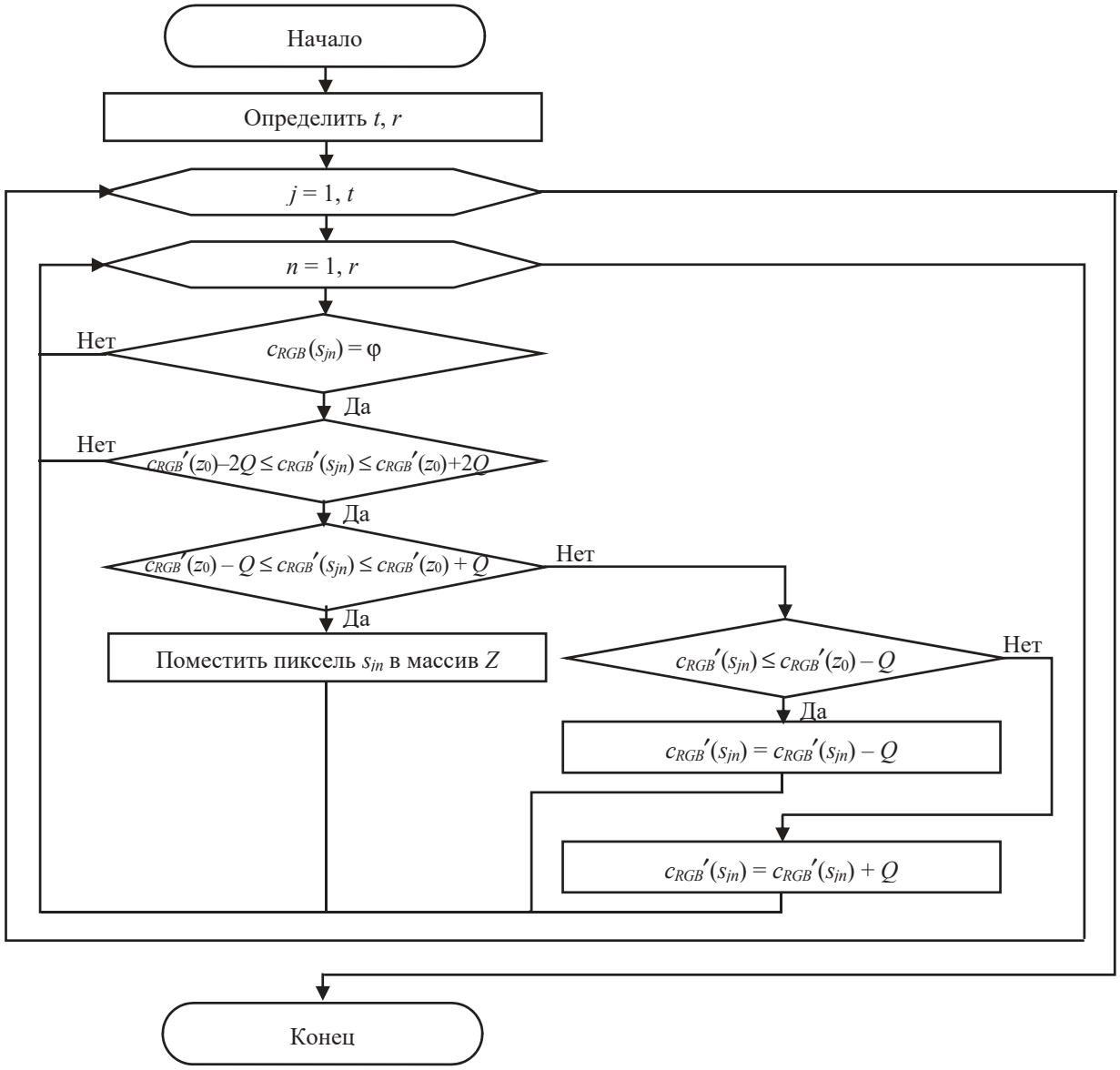

Рис. 8. Создание массива пикселей Z

Если значение цветового кода канала пикселя c ($c_{RGB}'(s_{jn})$) значительно отличается от $c_{RGB}'(z_0)$ (на Q и более), то $c_{RGB}'(s_{jn})$ следует изменить на Q. Если

$$c_{RGB}'(s_{jn}) \geq c_{RGB}'(z_0) + Q, \quad (7)$$

то

$$c_{RGB}'(s_{jn}) = c_{RGB}'(s_{jn}) + Q; \quad (8)$$

если же

$$c_{RGB}'(s_{jn}) \leq c_{RGB}'(z_0) - Q, \quad (9)$$

то

$$c_{RGB}'(s_{jn}) = c_{RGB}'(s_{jn}) - Q. \quad (10)$$

Таким образом, пиксель s_{jn} не будет попадать в массив пикселей для внедрения.

Для извлечения внедренного сообщения необходимо выбрать массив пикселей Z_D (пример показан на рис. 11), где совпадает значение кода одного или нескольких цветовых каналов, аналогично массиву Z. В отличие от массива Z в массив Z_D помещаются пиксели, где $c_{RGB}'(s_{jn})$ отличается от $c_{RGB}'(z_0)$ на $2Q$ единиц в любую сторону (диапазон для выбора $c_{RGB}'(z_0) - Q \leq c_{RGB}'(s_{jn}) \leq c_{RGB}'(z_0) + Q$, при внедрении значение может измениться еще на Q единиц) (выбора $c_{RGB}'(z_0) - 2Q \leq c_{RGB}'(s_{jn}) \leq c_{RGB}'(z_0) + 2Q$).

При извлечении примем во внимание, что максимальное число разрядов длины внедренного сообщения – 9. Для восстановления сообщения сначала извлекается первый символ сообщения, состоящий из 8 битов, содержащий в себе информацию о количестве разрядов длины сообщения. Полученная битовая строка переводится в десятичную систему. Исходя из полученного числа, извлекается следующее количество битов,

обозначающих длину сообщения. Например, если после извлечения первых 8 битов получается битовая строка 0000 0001, то следующим извлекается один символ сообщения (8 бит). После этого, зная длину сообщения, можно извлечь само сообщение.

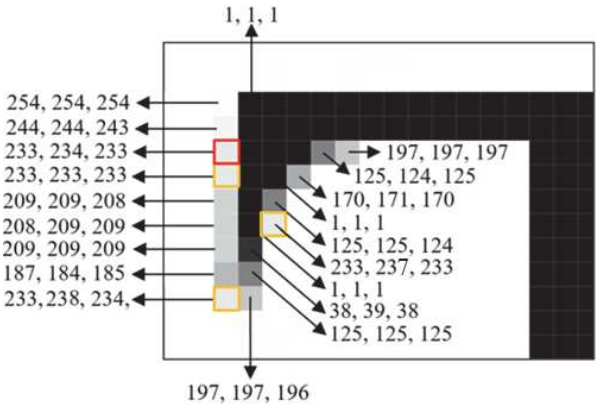

Рис. 11. Массив Z_D на фрагменте изображения

В качестве ключей стеганографического преобразования может использоваться информация о том, какой канал или несколько каналов используются для выбора пикселей для внедрения, номер базового пикселя в массиве или алгоритм выбора базового пикселя из массива пикселей для внедрения, канал для внедрения, значение φ, значение Q.

Простой ключ для реализуемого примера: «R233G1Q4», где R – используемый канал для выбора пикселей; 233 – значение цветового кода канала R для выбора пикселей (φ = 233); G – канал для внедрения; 1 – номер базового пикселя в массиве пикселей; Q4 – значение $Q = 4$.

Алгоритм характеризуется линейной сложностью $O(n)$.

Исходя из того, что в среднем примерно 5% пикселей будут соответствовать требованиям, определяемым алгоритмом внедрения (в проанализированном изображении из 1470 пикселей для внедрения подошли 45 (~3%), при внедрении в цветовой области в границах черного цвета из 1470 пикселей для внедрения подходят 105 (~7%)), то для внедрения сообщения длиной 8 бит необходимо изображение 15×15 пикселей, для внедрения сообщения длиной 80 битов – 45×45 пикселей.

Сравним предложенный метод с одним из самых известных методов – LSB [10, 11] на основе такого параметра, как пропускная способность. С помощью метода LSB максимально можно встроить 1/8 от объема контейнера за счет внедрения 1 бита в каждый канал каждого пикселя. В исходное изображение размером 100×100 пикселей (размер изображения – 30 000 байтов) методом LSB можно внедрить 30 000 битов (12,5% от объема контейнера). Предложенный метод максимально позволяет встроить 1/25 от объема контейнера. В то же исходное изображение размером 100×100 пикселей, используя предложенный метод, можно внедрить 1000 битов (5% в два канала), т. е. 4% от объема контейнера. Изображения с большим количеством полутонов, черно-белые и монохромные изображения будут иметь большую пропускную способность, так как они построены на основе большего количества пикселей с совпадающими значениями цветового канала.

Предложенный метод будет иметь преимущество перед стандартным вариантом метода LSB при использовании дополнительных ключей стеганографического преобразования.

К недостаткам LSB также относится возможность детектирования сообщения простейшими методами, например посредством статистического анализа LSB контейнера. Предложенный метод устойчив к подобного рода атакам.

Заключение. В качестве метода для контроля целостности данных, защиты прав собственности на мультимедийную информацию, отслеживания распространения информации предложен стеганографический метод, основанный на изменении пространственной области документа-контейнера.

Данный метод может применяться для текстовых документов в формате растровой графики. Пропускная способность метода зависит от характеристик изображения-контейнера: количества пикселей со сходными значениями одного или нескольких цветовых каналов. Данный метод можно применять и для форматов изображений с незначительным сжатием, используя большее значение Q. Однако такое внедрение будет также более очевидно.

Предложенный метод уступает методу LSB по максимальной пропускной способности, но выигрывает в устойчивости к некоторым видам атак.

Список литературы

1. Шутько Н. П., Листопад Н. И., Урбанович П. П. Моделирование стеганографической системы в задачах по охране авторских прав // Информационные технологии в промышленности (ITI`2015): тез. докл. Восьмой Междунар. науч.-техн. конф. Минск, 2015. С. 30–31.

2. Information Hiding Techniques for Steganography and Digital Watermarking / ed. Stefan Katzenbeisser, Fabien A. P. Petitcolas. London: Artech House, Inc., 2000. P. 20–22.

3. Урбанович П. П. Защита информации методами криптографии, стеганографии и обфускации. Минск: БГТУ, 2016. 220 с.

4. Maheswari S. Uma, Hemanth D. Jude. Different methodology for image steganography-based data hiding: review paper // International Journal of Information and Communication Technology. 2015. Vol. 7, no. 4/5. P. 521–536. DOI:10.1504/IJICT.2015.070330.

5. Shutko, N., Urbanovich P., Zukowski P. Method of syntactic text steganography based on modification of the document-container aprosh // PrzeglądElektrotechniczny. 2018. Vol. 6. P. 82–85. DOI:10.15199/48.2018.06.15.

6. Blinova E. A, Urbanovich P. P. Steganographic method based on hidden messages embedding into Bezier curves of SVG images // Journal of the Belarusian State University. Mathematics and Informatics. 2021. No. 3. P. 68–83. DOI: https://doi.org/10.33581/2520-6508-2021-3-68-83.

7. Urbanovich, P., Shutko N. Theoretical Model of a Multi-Key Steganography System // Recent Developments in Mathematics and Informatics. Contemporary Mathematics and Computer Science. Lublin: KUL, 2016. Vol. 2, chapter 11. P. 181–202.

8. Шутько Н. П., Урбанович П. П. Защита авторских прав на текстовые документы на основе стеганографической модификации цвета символов текста // Информационные технологии: материалы 83-й науч.-техн. конф. проф.-препод. состава, науч. сотр. и асп. (с междунар. участием), Минск, 4–15 февраля 2019 г. Минск: БГТУ, 2019. С. 41–43.

9. Prasad S., Pal A. K. An RGB colour image steganography scheme using overlapping block-based pix-el-value differencing // Royal Society Open Science. 2017. Vol. 4. 161066. DOI: 10.1098/ rsos.161066.

10. Chang C. C., Lin M. H. and Hu Y. C. A fast and secure image hiding scheme based on LSB sub-stitution // International Journal of Pattern Recognition and Artificial Intelligence. 2002. Vol. 16, no. 4. P. 399–416. DOI:10.1142/S0218001402001770.

11. Tran Ninh, Zepernick Hans-Jürgen, Chu Thi My Chinh. LSB Data Hiding in Digital Media: A Survey // Industrial Networks and Intelligent Systems. 2022. P. 1–50. DOI:10.4108/eai.5-4-2022.173783.

References

1. Shutko N., Listopad N., Urbanovich P. Modeling a steganographic system in problems of copyright protection. *Informatsionnyye tekhnologii v promyshlennosti (ITI`2015): tezisy dokladov Vos'maoy Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii* [Information Technologies in Industry (ITI`2015): abstracts Eighth International Scientific and Technical Conference]. Minsk, 2015, pp. 30–31 (In Russian).

2. Information Hiding Techniques for Steganography and Digital Watermarking. Ed. Stefan Katzenbeisser, Fabien A. P. Petitcolas. London, Artech House, Inc. Publ., 2000, pp. 20–22.

3. Urbanovich P. P. *Zashchita informatsii metodami kriptografii, steganografii i obfuskatsii* [The protection of information based on the methods by cryptography, steganography and obfuscation]. Minsk, BGTU Publ., 2016. 220 p. (In Russian).

4. Maheswari S. Uma, Hemanth D. Jude. Different methodology for image steganography-based data hiding: review paper. *International Journal of Information and Communication Technology*, 2015, vol. 7, no. 4/5, pp. 521–536. DOI:10.1504/IJICT.2015.070330.

5. Shutko N., Urbanovich P., Zukowski P. A method of syntactic text steganography based on modification of the document-container aprosh. *PrzeglądElektrotechniczny*, 2018, vol. 6, pp. 82–85. DOI: 10.15199/48.2018.06.15.

6. Blinova E. A., Urbanovich P. P. Steganographic method based on hidden messages embedding into Bezier curves of SVG images. *Journal of the Belarusian State University. Mathematics and Informatics*, 2021, no. 3, pp. 68–83. DOI: https://doi.org/10.33581/2520-6508-2021-3-68-83.

7. Urbanovich, P., Shutko N. Theoretical Model of a Multi-Key Steganography System. *Recent Developments in Mathematics and Informatics. Contemporary Mathematics and Computer Science*. Lublin, 2016, vol. 2, chapter 11, pp. 181–202.

8. Shutko, N., Urbanovich P. Copyright protection for text documents based on steganographic modification of the color of text symbols. *Informatsionnyye tekhnologii*: *materialy 83-y nauchno-tekhnicheskoy konferentsii professorsko-prepodavatel'skogo sostava, nauchnykh sotrudnikov i aspirantov (s mezhdunarodnym uchastiyem*) [Information technologies: materials of the 83rd scientific and technical conference of the faculty, researchers and graduate students (with international participation)]. Minsk, 2019, pp. 41–43 (In Russian).

9. Prasad S., Pal A. K. An RGB colour image steganography scheme using overlapping block-based pixel-value differencing. *Royal Society Open Science*, 2017, vol. 4. 161066. DOI: 10.1098/rsos.161066.

10. Chang C. C., Lin M. H. and Hu Y. C. A fast and secure image hiding scheme based on LSB substitution. *International Journal of Pattern Recognition and Artificial Intelligence*, 2002, vol. 16, no. 4, pp. 399–416. DOI:10.1142/S0218001402001770.

11. Tran Ninh, Zepernick Hans-Jürgen, Chu Thi My Chinh. LSB Data Hiding in Digital Media: A Survey. *Industrial Networks and Intelligent Systems*, 2022. DOI:10.4108/eai.5-4-2022.173783.

Информация об авторах

Савельева Маргарита Геннадьевна – аспирант кафедры информационных систем и технологий. Белорусский государственный технологический университет (220006, г. Минск, ул. Свердлова, 13а, Республика Беларусь). E-mail: saveleva@belstu.by

Урбанович Павел Павлович – доктор технических наук, профессор. Белорусский государственный технологический университет (220006, г. Минск, ул. Свердлова, 13а, Республика Беларусь). E-mail: p.urbanovich@belstu.by

Information about the authors

Saveleva Margarita Gennadievna – PhD student, the Department of Information Systems and Technologies. Belarusian State Technological University. (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: saveleva @belstu.by

Urbanovich Pavel Pavlovich – DSc (Engineering), Professor, Professor, the Department of Information Sistems and Technologies. Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: p.urbanovich@belstu.by

Поступила 25.04.2022