УДК 004.56+003.26
doi:10.31799/1684-8853-2024-6-2-14
EDN: AOSASL

Научные статьи
Articles

Стеганографическое преобразование на основе модификации полутоновых оттенков растрированных документов

М. Г. Савельева[a], *аспирант, orcid.org/0009-0000-3250-8317*
П. П. Урбанович[a,б], *доктор техн. наук, профессор, orcid.org/0000-0003-2825-4777, p.urbanovich@belstu.by*
[a]*Белорусский государственный технологический университет, Свердлова ул., 13а, Минск, 220006, Республика Беларусь*
[б]*Люблинский католический университет Иоанна Павла II, Рацлавицке ал., 14, Люблин, 20-950, Польша*

Введение: *всё возрастающую актуальность приобретают исследования, направленные на использование скрытых каналов передачи и хранения информации на основе стеганографии. Одним из видов преобразований электронных текстовых документов является их растрирование. Особенности и результат этой операции могут быть положены в основу нового метода стеганографического преобразования.* ***Цель:*** *разработать модель и на ее основе синтезировать структурную схему стеганографической системы, а также разработать метод стеганографического преобразования, в которых используется пиксельное представление символов текста-контейнера, полученное при растрировании текста.* ***Результаты:*** *структура предложенной стеганографической системы основана на использовании особенностей растрирования документов-контейнеров. Разработана математическая модель такой системы, базирующаяся на теоретико-множественном представлении основных компонентов системы, а также на мультипараметрическом представлении ключа прямого и обратного стеганографического преобразования. При этом элементы ключа соотносятся, в том числе, с цветовыми и пространственно-геометрическими свойствами и параметрами отдельных пикселей документа-контейнера. Разработаны метод и алгоритмы стеганографического внедрения и извлечения тайной информации, базирующиеся на упомянутой модели. Выполнена сравнительная оценка пропускной способности стегоканала (бит/пиксель), создаваемого на основе предложенного метода.* ***Практическая значимость:*** *полученные теоретические результаты отражают общие особенности синтеза и анализа стеганографических систем, преобразования в которых основаны на использовании полутоновых оттенков электронных документов при их растрировании. С помощью предложенного метода можно внедрять в растрированный документ-контейнер тайную информацию для ее передачи, контроля целостности, а также защиты авторских прав на этот документ.*

Ключевые слова *— стеганография, растрирование, математическая модель, цвет, полутоновые оттенки, пропускная способность стегоканала.*

Для цитирования: Савельева М. Г., Урбанович П. П. Стеганографическое преобразование на основе модификации полутоновых оттенков растрированных документов. *Информационно-управляющие системы*, 2024, № 6, с. 2–14. doi:10.31799/1684-8853-2024-6-2-14, EDN: AOSASL

For citation: Saveleva M. G., Urbanovich P. P. Steganographic transformation based on the modification of halftone shades of rasterized documents. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 6, pp. 2–14 (In Russian). doi:10.31799/1684-8853-2024-6-2-14, EDN: AOSASL

Введение

Всё возрастающие объемы данных передаются и хранятся в цифровой форме. Вместе с этим возрастает степень угроз цифровому киберпространству, связанных с несанкционированным копированием, использованием и распространением, а также модификацией информации [1, 2].

Понимая важность проблемы защиты своего интеллектуального труда, авторы стремятся найти и использовать способы и инструментальные средства для ее решения. Именно поэтому стеганография, наука о скрытом размещении и передаче данных, приобретает все большую популярность. С ее помощью можно встраивать секретные (авторские) данные в цифровые документы, тем самым обеспечивая, в том числе, доказательство прав на интеллектуальную собственность [3–6].

Следует также отметить важную особенность современных информационных технологий, связанную с возможностью интегрировать на одной аппаратно-программной платформе различные компоненты цифрового контента, построенные на различных архитектурных принципах, с использованием различных языков программирования, библиотек и фреймворков.

Объектом нашего исследования служат электронные текстовые документы, подвергающиеся преднамеренным или непреднамеренным конвертациям, в результате чего изменяется исходный (оригинальный) формат документа. Такие документы могут быть рассмотрены как изображения в форматах растровой либо векторной

графики, описываемых с помощью соответствующих пространственно-геометрических и цветовых параметров.

Оригинальный контент может быть преобразован из одного формата графики в другой без согласования с авторами. При различных изменениях и преобразованиях текстовых документов (являющихся контейнерами стеганографической системы) одна из важных проблем связана с растрированием текста: контуры букв становятся нечеткими, а цвет по контуру переходит в градиент.

Как известно, основные принципы векторной графики основаны на математическом аппарате, отличном от математического описания объектов растровой (пиксельной) графики, и связаны с построением линейных контуров, составленных из элементарных кривых, описываемых математическими выражениями [7, 8]. При редактировании элементов векторной графики можно изменять параметры линий, переносить элементы, менять их размер, форму и цвет, и это не отразится на качестве их визуального представления. Кроме того, векторная графика не зависит от разрешения выходных устройств визуализации информации.

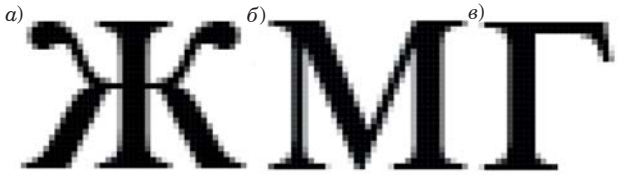
Электронный контент условно можно разделить на три категории: текст, изображение, изображение + текст (включая изображение-текст). Информативная, содержательная основа практически любого документа заключается в семантике текста, который может строиться на основе различных технологий. В свою очередь графемы (иначе — буквы) в векторном формате могут разделяться на различные группы. Такая классификация строчных и прописных графем может основываться, например, на учете совокупности конструктивных особенностей символов (форме штрихов, наличии засечек и др.) [9]. Совокупность упомянутых особенностей называют гарнитурой и шрифтом. При этом все буквы алфавита, например русского языка, условно можно отнести к трем классам (рассматриваем наиболее часто используемую гарнитуру — Times New Roman):

1) буквы имеют относительно сложную форму: содержат верхние выносные и нижние выносные элементы, акценты, хвосты, капли, наплывы, овалы (специфические элементы графем) и т. д., различные комбинации этих элементов (рис. 1, *а*);

2) буквы имеют простую структуру: горизонтальные или вертикальные штрихи в комбинации с более сложными элементами (рис. 1, *б*);

3) буквы характеризуются самой простой структурой: большое количество горизонтальных или вертикальных штрихов (рис. 1, *в*).

Растрированные документы могут быть сохранены в различных форматах в зависимости



■ ***Рис. 1.*** Примеры растрированных букв, относящихся к первой (*а*), второй (*б*) и третьей (*в*) группам

■ ***Fig. 1.*** Examples of rasterized letters belonging to the first (*а*), second (*б*) and third (*в*) groups

от потребностей пользователя. Использование особенностей растрированных символов позволяет создавать новые стеганографические методы, обеспечивающие достаточно высокую пропускную способность (отношение объема осаждаемой информации к объему контейнера).

Особенности контура растрированных букв можно использовать для скрытого внедрения тайной информации (цифрового водяного знака) в защищаемый цифровой контент. Чтобы увеличить пропускную способность создаваемого таким образом скрытого канала передачи/хранения данных, можно использовать преобладающие оттенки среди переходных оттенков растрированных символов [9].

Специфика рассматриваемого типа стеганографического преобразования (или стегопреобразования) обусловливает необходимость внесения соответствующих изменений в известные математические модели и структуру стеганографических систем, основанных на модификации цветовых и пространственно-геометрических параметров документов [3–5, 10–16] с учетом их адаптации под содержание процессов внедрения информации в растрированный документ-контейнер, а также извлечения этой информации. Указанные особенности моделирования и структурного построения стеганографических систем определяют объект и предмет исследования в данной статье.

Общая модель стеганографической системы

Мы определим абстрактную стеганографическую систему (стегосистему) *SF* как набор преобразований некоторого пространства, которое включает в себя множество **M** возможных сообщений ($\mathbf{M} = \{M_1, M_2, \ldots, M_n\}$) и множество **C** возможных контейнеров ($\mathbf{C} = \{C_1, C_2, \ldots, C_r\}$) в другое пространство: множество **S** возможных стегосообщений или стегоконтейнеров — файловых документов с размещенными в них сообщениями или цифровыми водяными знаками *M* ($\mathbf{S} = \{S_1, S_2, \ldots, S_t\}$). При этом переход из одного

пространства в другое и наоборот осуществляется с использованием элементов еще одного множества — ключей $\mathbf{K} = \{K_1, K_2, \ldots, K_a\}$. Для упрощения считаем, что указанные множества являются конечными. При этом $t \geq nra$, откуда предполагается, что разным наборам элементов из множеств **M**, **C**, **K** будут соответствовать разные элементы из множества **S**.

Формально процесс встраивания (осаждения) тайных сообщений из **M** в документы-контейнеры из **C** можно описать как преобразование **F** (в общем случае — отображение) в виде декартова произведения:

$$\mathbf{F}: \mathbf{M} \times \mathbf{C} \times \mathbf{K} \rightarrow \mathbf{S}. \quad (1)$$

Каждый стегоконтейнер S из множества **S** можно отождествлять со скрытым каналом SC хранения или передачи информации: $SC \in \mathbf{SC}$.

Обратный процесс (извлечение сообщения) из стегоконтейнера описывается функцией $\mathbf{F}^{-1}$:

$$\mathbf{F}^{-1}: \mathbf{S} \times \mathbf{K} \rightarrow \mathbf{M}, \mathbf{C}. \quad (2)$$

Строго говоря, здесь мы используем термин «преобразование» в несколько ином значении по сравнению с тем, как это используется в математике. Речь идет о декартовых произведениях не для целых множеств ($\mathbf{M} \times \mathbf{C} \times \mathbf{K}$), а лишь для определенной тройки элементов, относящихся к каждому из указанных множеств [14]: $M \in \mathbf{M}$, $C \in \mathbf{C}$, $K \in \mathbf{K}$ и $\mathbf{F} = \{F_1, F_2, \ldots, F_t\}$, $\mathbf{F}^{-1} = \{(F_1)^{-1}, (F_2)^{-1}, \ldots, (F_t)^{-1}\}$.

Таким образом, в наиболее общем случае стеганографическая система может быть формально определена следующим выражением:

$$\mathbf{SF} = (\mathbf{SC}, \mathbf{C}, \mathbf{M}, \mathbf{K}, \mathbf{S}, \mathbf{F}, \mathbf{F}^{-1}). \quad (3)$$

В статьях [14, 16] рассмотрено представление множества ключей **K** в виде непересекающихся подмножеств: $\mathbf{K} = \{\mathbf{K}_0, \mathbf{K}_{д1}, \mathbf{K}_{д2}\}$. Основные ключи, относящиеся к подмножеству $\{\mathbf{K}_0\}$, определяют базовый метод стеганографического преобразования (например, наименее значащих битов, LSB — Least Significant Bits). Дополнительные ключи первого рода $\{\mathbf{K}_{д1}\}$ соотносятся с дополнительными преобразованиями осаждаемой в контейнер информации (например, с помехоустойчивым кодированием, сжатием или шифрованием сообщения M) и с соответствующим обратным преобразованием при извлечении информации из стегоконтейнера S; особенности реализации комбинаций стеганографии с другими методами преобразований рассмотрены, например, в [17–24]. Дополнительные ключи второго рода $\{\mathbf{K}_{д2}\}$ определяют выбор элементов и параметров документа-контейнера (цветовых компонентов, отдельных символов текста и т. д.) при выполнении процедур внедрения/извлечения сообщения M. К примеру, последний тип ключей при использовании метода LSB в качестве базового (определяется ключом из подмножества $\{\mathbf{K}_0\}$) может соотноситься с различными модификациями LSB [5, 15, 25–27]. В частности, в статье [27] для устранения эффекта ложных контуров предлагается использовать компенсацию серой шкалы с учетом особенности зрительной системы человека.

Модель и структура стеганографической системы при использовании растрированных текстов-контейнеров

Основой предлагаемого решения является многоключевая модель стегосистемы, описываемая соотношениями (1)–(3).

Предлагается далее представить ключи **K** семейством множеств $\mathbf{K} = \{\mathbf{K}_г, \mathbf{K}_п\}$, где $\mathbf{K}_г$ — ключи, определяющие операции подготовки (генерации) сообщения M к его размещению в выбранном контейнере C (фрагментация, параметры кодирования, шифрования или сжатия M или его блоков; иначе — преобразование M в $M_г$), а $\mathbf{K}_п$ — множество ключей, определяющих особенности метода внедрения сообщения $M_г$ (базовый стегометод, количественные характеристики изменения пространственно-геометрических параметров или свойств растрированных символов, фрагментация контейнера и др.). В соответствии с этим преобразования **F** и $\mathbf{F}^{-1}$, представленные формальными соотношениями (1) и (2), можно несколько видоизменить:

$$\mathbf{F}: \mathbf{M} \times \mathbf{C} \times \mathbf{K}_г \times \mathbf{K}_п \rightarrow \mathbf{S}; \quad (4)$$

$$\mathbf{F}^{-1}: \mathbf{S} \times \mathbf{K}_г \times \mathbf{K}_п \rightarrow \mathbf{M}, \mathbf{C}. \quad (5)$$

Ключи $\mathbf{K}_г$ предлагается представить двумя подмножествами: $\mathbf{K}_{г1}$ и $\mathbf{K}_{г2}$. Некоторый ключ $K_{г1}$ из подмножества $\mathbf{K}_{г1}$ ($K_{г1} \in \mathbf{K}_{г1}$; $\mathbf{K}_{г1} \in \mathbf{K}_г$) отождествляется с необходимыми операциями преобразования M в $M_г$, а также с типом используемого контейнера C; имеется в виду, что растровые электронные документы могут создаваться в форматах PNG, BMP, JPEG и т. д., каждому из которых соответствует отдельный ключ. Некоторый ключ $K_{г2}$ из подмножества $\mathbf{K}_{г2}$ ($K_{г2} \in \mathbf{K}_{г2}$; $\mathbf{K}_{г2} \in \mathbf{K}_г$) предлагается использовать для обозначения, собственно, стеганографического преобразования, взятого за основу (например, LSB, дискретного косинусного преобразования, дискретного вейвлет-преобразования и т. д.).

В свою очередь ключи из подмножества $\mathbf{K}_{\text{п}}$ представляются в виде четырех новых подмножеств: $\mathbf{K}_{\text{п}} = \{\mathbf{K}_{\text{п1}}, \mathbf{K}_{\text{п2}}, \mathbf{K}_{\text{п3}}, \mathbf{K}_{\text{п4}}\}$.

При этом ключ $K_{\text{п1}}$ ($K_{\text{п1}} \in \mathbf{K}_{\text{п1}}$) определяет выбранный цветовой канал в используемой цветовой модели кодирования отдельных пикселей: в модели RGB — это один или из каналов: R (красный), G (зеленый), B (синий), в модели CMYK — соответственно C (циан), M (пурпурный), Y (желтый), K (черный).

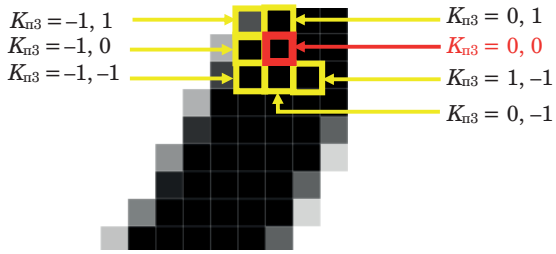
Ключ $K_{\text{п2}}$ ($K_{\text{п2}} \in \mathbf{K}_{\text{п2}}$) будет соотноситься с выбранным (базовым) пикселем или некоторым его параметром. Такой пиксель создает своеобразную точку отсчета, по отношению к которой определяются параметры или координаты остальных задействованных для осаждения сообщения $M_{\text{г}}$ пикселей, формирующих структуру буквы. Например, в двумерном растровом массиве некоторому пикселю могут соответствовать координаты x, y ($x \in [1, X]$, $y \in [1, Y]$). Для каналов в модели RGB диапазон значений для цветовой характеристики (кода) пикселя будет изменяться от 0 до 255, в модели CMYK — от 0 до 100.

Ключу $K_{\text{п3}}$ ($K_{\text{п3}} \in \mathbf{K}_{\text{п3}}$) соответствуют параметры непосредственно стеганографического преобразования, например, выбор канала для внедрения сообщения, порядок преобразования (псевдослучайный порядок или иная последовательность), сдвиг при выборе пикселей для внедрения и т. д. Под сдвигом понимается смещение фокуса для стеганографического преобразования с базового пикселя на пиксель, находящийся на удалении (Δx, Δy) от базового. Значение Δx задает сдвиг по горизонтали, Δy — по вертикали; (Δx, Δy) $\in K_{\text{п3}}$: $\Delta x = K_{\text{п3},x}$, $\Delta y = K_{\text{п3},y}$. Разумно выбирать значение Δx и Δy в диапазоне [–1, 1]. При $K_{\text{п3}} = (0, 0)$ сдвига нет; такой пиксель можно рассматривать как базовый (на рис. 2 обозначен красным контуром), так как больший сдвиг снижает стегостойкость, и факт внедрения информации будет более очевиден для стегоаналитика. Влияние параметров ключа $K_{\text{п3}}$ на выбор соответствующего пикселя для модификации кода показано на рис. 2.

Известно, что осаждение информации изменяет цветовой код модифицируемого пикселя. При этом следует определять границы диапазона такого изменения, чтобы минимизировать эффективность визуальных и иных атак на стегоконтейнер. Выбор границ диапазона задается ключом $K_{\text{п4}}$ ($K_{\text{п4}} \in \mathbf{K}_{\text{п4}}$).

С учетом описанных преобразований и соответствующих ключей предлагаемую формальную модель стеганографической системы можно представить следующим образом:

$$\mathbf{F}: \mathbf{M} \times \mathbf{C} \times \mathbf{K}_{\text{г1}} \times \mathbf{K}_{\text{г2}} \times \mathbf{K}_{\text{п1}} \times \times \mathbf{K}_{\text{п2}} \times \mathbf{K}_{\text{п3}} \times \mathbf{K}_{\text{п4}} \to \mathbf{S}; \quad (6)$$



■ ***Рис. 2.*** Относительное пространственное положение пикселя в зависимости от ключа $K_{\text{п3}}$

■ ***Fig. 2.*** Relative spatial position of a pixel depending on the key $K_{\text{п3}}$

$$\mathbf{F}^{-1}: \mathbf{S} \times \mathbf{K}_{\text{г1}} \times \mathbf{K}_{\text{г2}} \times \mathbf{K}_{\text{п1}} \times \mathbf{K}_{\text{п2}} \times \times \mathbf{K}_{\text{п3}} \times \mathbf{K}_{\text{п4}} \to \mathbf{M}, \mathbf{C}. \quad (7)$$

Дополнительно предлагается использовать два набора функций и соответствующие им множества: функции $F_E \in \mathbf{F}_E$ и $F_W \in \mathbf{F}_W$.

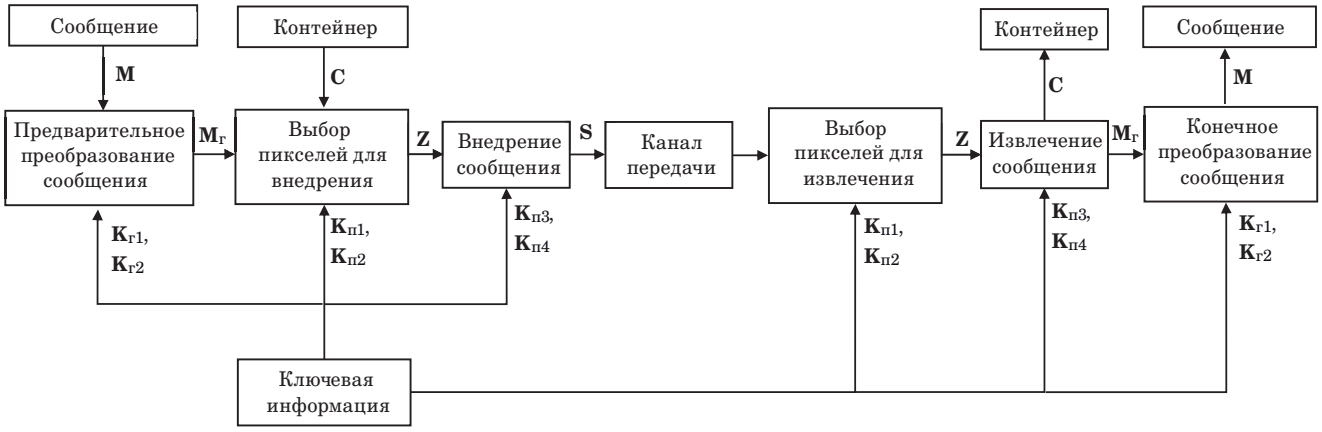
Множество $\mathbf{F}_E$ включает функции F_E, определяющие выбор пикселей контейнера C для стеганографического преобразования с учетом определенных ключей. Сформированный в конечном итоге массив пикселей предназначается для размещения тайной информации; обозначим его Z, $Z \in \mathbf{Z}$; $\mathbf{Z}$ — множество возможных массивов, зависящих от различных сообщений, контейнеров, ключей и функций множества $\mathbf{F}_E$. Функции $F_W \in \mathbf{F}_W$ определяют порядок следования блоков сообщения и соответствующую декомпозицию контейнера на блоки.

Таким образом, стеганографическая система, которая может быть синтезирована на основе рассмотренной модели, формально определяется выражением

$$\mathbf{SF} = (\mathbf{SC}, \mathbf{C}, \mathbf{M}, \mathbf{K}, \mathbf{S}, \mathbf{F}, \mathbf{F}^{-1}, \mathbf{Z}, \mathbf{F}_E, \mathbf{F}_W). \quad (8)$$

Структурная схема стеганографической системы, построенная на основе модели (8), представлена на рис. 3.

Предложенная модель отличается представлением основных элементов стеганографической системы (сообщения, контейнера, мультинабора ключей) в виде связанных между собой компонентов, учитывающих специфику растрированных текстов-контейнеров. Принятый уровень детализации позволяет упростить определение логических связей между блоками стеганографической системы, реализуемыми в них процессами и в конечном итоге — строить достаточно легкие для программной реализации алгоритмы стеганографического преобразования на базе растрирования документа-контейнера.



■ ***Рис. 3.*** Структурная схема описанной стеганографической системы
■ ***Fig. 3.*** Structural diagram of the steganographic system

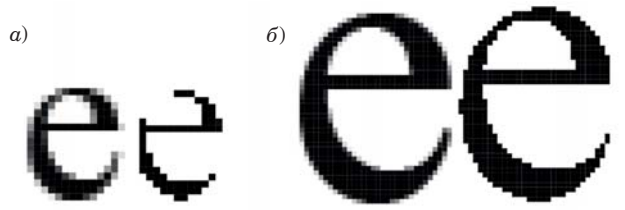
Стеганографический метод на основе предложенной модели и алгоритмические особенности его реализации

Рассмотрим сущность и алгоритмические особенности реализации метода, основанного на модели (8), при внедрении/извлечении сообщения $M_г$ с использованием растрирования символов документа-контейнера C в цветовой модели RGB.

Суть метода заключается в изменении оттенков растрированных пикселей. При растрировании цвет по контуру переходит в градиент, за счет чего общее количество пикселей для отображения буквы увеличивается. Это происходит в том числе из-за невозможности квадратных матриц пикселей отобразить элементы символов, имеющих наклонные, округлые черты. Именно в эти полутоновые пиксели можно внедрять информацию за счет изменения оттенка.

При растрировании цветовые характеристики пикселей принимают 16 оттенков (R, G, B) с кодами от 0 до 255: (0, 0, 0), (17, 17, 17), …, (255, 255, 255). Так как белый цвет (255, 255, 255) — это фон страницы, то только 15 оттенков используются для отображения символов. Среди последних можно выделить более часто встречающиеся оттенки, которым соответствуют следующие цветовые коды: (17, 17, 17), (34, 34, 34), (68, 68, 68), (102, 102, 102), (136, 136, 136), (153, 153, 153), (187, 187, 187) [28]. Эти особенности примерно в одинаковой степени свойственны преобразованиям файлов из формата PDF в форматы PNG, GIF, TIF, BMP. Черные пиксели (0, 0, 0) являются основой символа и в зависимости от кегля их количество может меняться (рис. 4).

Например, растрированная буква «е» размером 8 пт состоит из 115 цветных пикселей, из которых 54 окрашены в черный цвет (47 % от общего количества), а та же буква размером

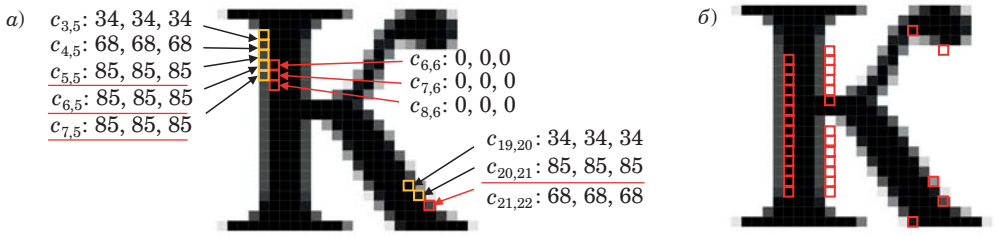


■ ***Рис. 4.*** Пример растрированного символа размером 8 пт (*а*) и 20 пт (*б*) и отображение пикселей черного цвета в нем (справа в каждой паре)
■ ***Fig. 4.*** An example of a rasterized symbol of size 8 pt (*а*) and 20 pt (*б*) and the display of black pixels in it (on the right in each pair)

20 пт состоит из 612 пикселей, из которых 464 черного цвета (75,8 % от общего количества). Кроме того, единичные изменения в монотонных областях (это касается и белого (255, 255, 255)) легче обнаружить.

Отметим, что при определении параметров используемых ключей целесообразно выполнить предварительный анализ распределения отдельных букв по их числу в контейнере C, относящихся к упомянутым выше группам, а также проанализировать частоты появления пикселей с различными цветовыми кодами. Результат такого анализа дополнительно помогает определить пропускную способность скрытого стегоканала SC (или информационную емкость контейнера, определяемую допустимым размером осаждаемого сообщения).

Предположим, что контейнером является документ в формате PNG (без сжатия). Преобразованное с использованием ключей $\mathbf{K}_г$ сообщение $M_г = f(M, \mathbf{K}_г)$ будет состоять из трех частей: непосредственно сообщения M, длины L сообщения M в бинарном представлении, числа l разрядов в L.



■ ***Рис. 5.*** Увеличенные копии изображения-контейнера с указанием параметров некоторых пикселей и дополнительным обозначением базовых пикселей (*а*), а также пикселей, вошедших в массив *Z* (*б*)

■ ***Fig. 5.*** Enlarged copies of the image-container with the parameters of some pixels indicated and additional designation of the base pixels (*а*), as well as the pixels included in the *Z* array (*б*)

Важнейшим шагом прямого стегопреобразования в соответствии с выражением (6) является выбор пикселей для осаждения сообщения. Пиксели, которые будут входить в массив *Z*, должны иметь одинаковые $K_{п1}$ и $K_{п2}$. Ключ $K_{п3}$ задает шаг сдвига Δx и Δy (см. рис. 2). Если значение цветового канала $K_{п1}$ пикселя $c_{i,j}$ ($c_{i,j}$ — пиксель, находящийся на пересечении i-й строки и j-го столбца изображения-контейнера) равно $K_{п2}$, то пиксель $c_{i+\alpha,\, j+\beta}$ заносится в массив *Z*; при этом $x = i + \Delta x$ и $y = j + \Delta y$. Ключ $K_{п4}$ задает изменение кодов цветовых каналов пикселя $c_{i+\Delta x, j+\Delta y}$, поэтому для увеличения стегостойкости метода $K_{п4}$ целесообразно выбирать как минимальное нечетное число, кратное шагу разницы градиента серого, полученного при растрировании. Исходя из этого $K_{п4} = 17$. Примем, что четный цветовой код канала пикселя соответствует биту сообщения «0», нечетный — «1». Нужно также принять во внимание, что при слишком значительном изменении числового кода пиксель, прошедший через стеганографическое преобразование, будет выбиваться из общей палитры документа-контейнера, что негативно влияет на уровень стегостойкости.

Для демонстрации выбора пикселей для массива *Z* используем в качестве контейнера черно-белое изображение документа, который состоит из одного символа размером 14 пт. Увеличенная копия символа с дополнительными пояснениями, касающимися координат и цветовых параметров некоторых пикселей, представлена на рис. 5, *а*. Общий размер изображения — 550 пикселей, из которых белых (цвет фона) — 297, иных оттенков — 253. Примем $K_{п1} = R$; $K_{п2} = 85$ (по статистике, наиболее часто встречающийся параметр кода); $K_{п3} = (K_{п3,x}, K_{п3,y})$, $K_{п3,x} = \Delta x = 1$, $K_{п3,y} = \Delta y = -1$ (ключ определяет смещение от базового пикселя по диагонали вправо и вниз на прилегающий пиксель); $K_{п4} = 17$.

Здесь значение $K_{п1}$ выбрано произвольно и может быть изменено на любой другой канал данной цветовой модели (G или B). В соответствии с приведенными на рис. 5, *а* цветовыми координатами четыре пикселя могут быть отнесены к базовым: $c_{5,5}$, $c_{6,5}$, $c_{7,5}$ и $c_{20,21}$ (на рис. 5, *а* соответствующие коды подчеркнуты). Следовательно, к массиву *Z* будут отнесены пиксели, находящиеся вправо и вниз по отношению к базовым в соответствии с ключом $K_{п3}$. Они выделены красным контуром. После обработки всего массива пикселей, формирующих исходный документ-контейнер, получим итоговый массив *Z*, состоящий из 32 пикселей (рис. 5, *б*). Как видно из рисунка, в *Z* вошли пиксели разнородные по значениям цветовых координат. Обнаружить такой массив — непростая задача.

Дальнейшие преобразования будут происходить в соответствии с алгоритмом, псевдокод которого представлен в листинге 1 (соответствует общему случаю). Здесь используются дополнительные к вышерассмотренным параметры: *cl* — цветовой код каналов R, G, B (для серых полутоновых пикселей, полученных в результате растрирования, он будет одинаковый во всех каналах); $Z[p]$ — p-й элемент массива *Z*; $M_{г2,p}$ — p-й символ сообщения $M_г$ в бинарном виде.

Например, M = «Text», тогда $L = 4$, $l = 1$; $M_г$ = «14Text» или в битовом представлении $M_{г2}$ = 00110001001101000111010001100101011110 0001110100.

Листинг 1. Псевдокод алгоритма прямого стеганографического преобразования

Listing 1. Pseudocode of the direct steganographic transformation algorithm

Входные: изображение-контейнер *C*, сообщение *M*, ключи $K_{п1}$, $K_{п2}$, $K_{п3,x}$, $K_{п3,y}$, $K_{п4}$;

Выходные: стегоконтейнер *S*;

(1) Вычислить *L*;

(2) Вычислить *l*;

(3) Сформировать внедряемое сообщение $M_г$: $M_г = (M, L, l)$;

(4) Перевести $M_г$ в двоичный формат и принять его за $M_{г2}$;

(5) Вычислить *n* — битовую длину сообщения $M_{г2}$;

(6) Определить X, Y;

(7) Сформировать пустой массив Z[];
(8) для i от 0 до X–1:
(9) для j от 0 до Y–1:
(10) Определить $cl(K_{п1}(c_{i,j}))$ — цветовой код канала $K_{п1}$ пикселя $c_{i,j}$
(11) если $cl(K_{п1}(c_{i,j}))$ = = $K_{п2}$ то
(12) записать в массив Z[] координаты пикселя $c_{i+Kп3,x,\ j+Kп3,y}$;
(13) $j = j+1$;
(14) $i = i+1$;
(15) Вычислить n_z — размер полученного массива Z[];
(16) если n_z > = n+1 тогда
(17) для p от 0 до n+1:
(18) определить $cl(Z[p])$;
(19) если $cl(Z[p])$% 2 = 1 то
(20) если $M_{г2,p}$ = 0 то
(21) $cl(Z[p]) = cl(Z[p])+K_{п4}$;
(22) иначе
(23) если $M_{г2,p}$ = 1 то
(24) $cl(Z[p]) = cl(Z[p])+K_{п4}$;
(25) $p = p+1$;
(26) Сохранить преобразованный стегоконтейнер C как S;

Строки 8–14 листинга 1 реализуют алгоритм создания массива Z. По окончании работы всего алгоритма будет получен стегоконтейнер S. На рис. 6 представлены для визуального сравнения исходный C и заполненный S контейнеры для рассматриваемого примера. Поскольку массив Z имеет размер 32, а n = 48, было использовано два экземпляра контейнера (32 бита сообщения — в первом экземпляре, оставшиеся 16 — во втором). Даже самый тщательный визуальный анализ не позволяет отличить контейнер с внедренной информацией от органического распределения оттенков в исходном контейнере.

Для извлечения внедренного сообщения необходимо создать и заполнить массив пикселей, повторяющий Z (обозначим его здесь Z_D). Для восстановления сообщения M сначала извлекается первый символ сообщения $M_{г2}$ — число l. Исходя из этого далее извлекается L.

Псевдокод алгоритма обратного стеганографического преобразования представлен в листинге 2. Здесь используются дополнительные к вышерассмотренным параметры: $Z_D[p]$ — p-й элемент массива Z_D; M_2 — двоичная форма сообщения M; $s_{i,j}$ — пиксель в изображении-стегоконтейнере S.

Листинг 2. Псевдокод алгоритма обратного стеганографического преобразования
Listing 2. Pseudocode of the inverse steganographic transformation algorithm

Входные: стегоконтейнер S, ключи $K_{п1}$, $K_{п2}$, $K_{п3,x}$, $K_{п3,y}$, $K_{п4}$;
Выходные: сообщение M;
(1) Создать пустой массив Z_D[] и *пустую строку* M_2 = '';
(2) Определить X, Y, l, L;
(3) для i от 0 до X–1:
(4) для j от 0 до Y–1:
(5) Определить $cl(K_{п1}(s_{i,j}))$ – цветовой код канала $K_{п1}$ пикселя $s_{i,j}$
(6) если $cl(K_{п1}(s_{i,j}))$ = = $K_{п2}$ то
(7) Записать в массив Z_D[] координаты пикселя $s_{i+Kп3,x,\ j+Kп3,y}$;;
(8) $j = j+1$;
(9) $i = i+1$;
(10) для p от 0 до 7:
(11) Определить $cl(Z_D[p])$ — цветовой код пикселя $Z_D[p]$;
(12) $l = l \ || \ cl(Z_D[p]) \ \% \ 2$;
(13) $p = p+1$;
(14) для p от 8 до 8l:
(15) Определить $cl(Z_D[p])$ — цветовой код пикселя $Z_D[p]$;
(16) $L = L \ || \ cl(Z_D[p]) \ \% \ 2$;
(17) $p = p+1$;
(18) для p от l(8+1) до 8L+7:
(19) Определить $cl(Z_D[p])$ — цветовой код пикселя $Z_D[p]$;
(20) $M = M \ || \ (cl(Z_D[p])\%2)$;
(21) $p = p + 1$;
(22) Перевести M_2 в текстовый формат, M;
(23) Сохранение извлеченного сообщения, M;

В строках 12, 16 и 20 листинга 2 используется символ в виде двух параллельных вертикальных линий (||), соответствующий операции склеивания (конкатенации).

Для анализа пропускной способности стеганоканала, создаваемого на основе описанного метода, рассмотрим вариант контейнера в виде текста, соответствующего стандартам оформления: полностью заполненная страница формата А4 (21 × 29,7 см), сформированная из 898 219 пикселей, со стандартными полями. Используемая гарнитура — Times New Roman.

Полученные границы диапазонов изменения количества полутоновых оттенков при различ-

а) *б*)

■ ***Рис. 6.*** Исходный (*а*) и заполненный (*б*) контейнеры
■ ***Fig. 6.*** Source (*а*) and filled (*б*) containers

ных размерах шрифта (кегля) (рис. 7, *а* и *б*) могут быть использованы в качестве критерия отнесения символа к соответствующему классу.

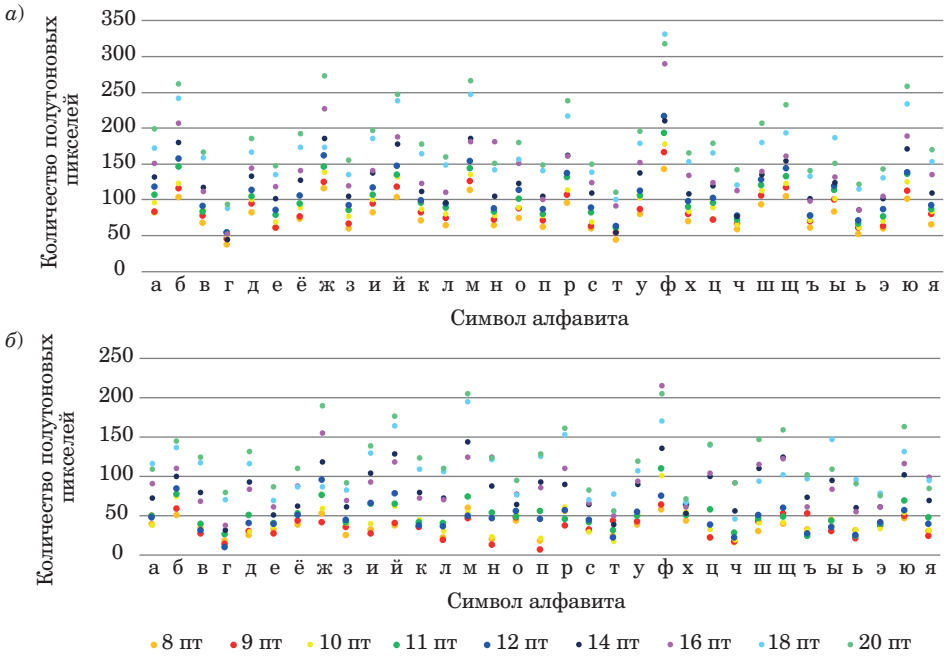
На основе количества полутоновых оттенков каждого растрированного символа в размерах от 8 до 20 пт было рассчитано среднее значение пропускной способности этого символа при условии внедрения одного бита информации в один оттенок. Рассмотрены два варианта: внедрение во все оттенки, кроме белого и черного (см. рис. 7, *а*), и внедрение только в часто встречающиеся (см. рис. 7, *б*). Результат представлен в виде гистограммы (рис. 8, *а*).

Учитывая количество полутоновых оттенков, содержащихся в графеме в зависимости от кегля, в табл. 1 представлена пропускная способность стегоканала, формируемого на основе предложенного метода при внедрении во все полутоновые пиксели и при внедрении только в часто встречающиеся оттенки пикселей, в зависимости от размера шрифта и вероятности (частости — принято во внимание количество появлений в анализируемом тексте каждой буквы) появления символов русского алфавита [29]. Пропускная способность вычисляется как отношение количества битов для внедрения к общему количеству пикселей контейнера (898 219).

Как видно, при меньшем кегле пропускная способность выше. Чем меньше кегль, тем из меньшего количества чисто черных пикселей будет состоять символ. Мелкие элементы буквы требуют отображения, но из-за растрирования теряют черный цвет и приобретают оттенок серого. Таким образом, количество пикселей, которые могут быть использованы для стеганографического преобразования, возрастает.

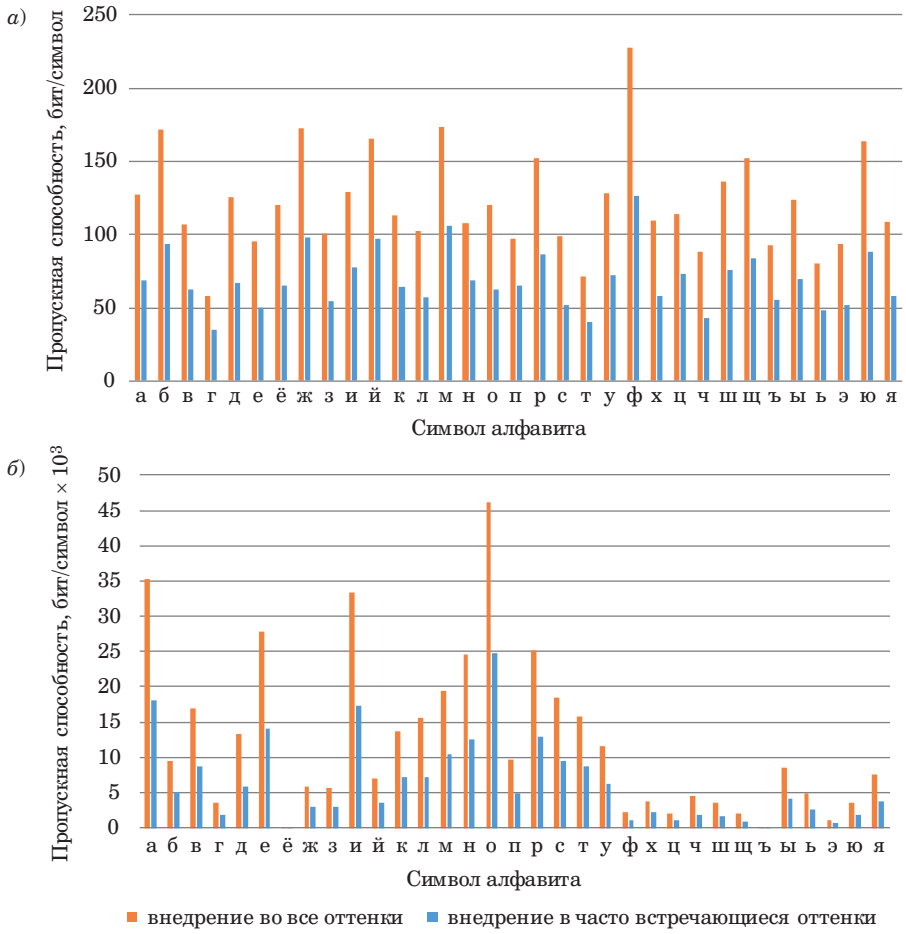
Гистограмма для средней пропускной способности одностраничного текста из анализируемого примера в зависимости от средней пропускной способности символа и частости его появления представлена на рис. 9, *б*. Понятно, что бóльшую пропускную способность имеют символы, которые встречаются чаще, т. е. знаки, которым соответствует бóльшая энтропия.

Для оценки метода был проведен анализ пропускной способности создаваемых стегоканалов в сравнении с другими стегометодами, где в качестве контейнеров используются изображения. По результатам сравнения (табл. 2) можно сделать вывод, что эффективность предложенного метода, оцениваемая пропускной способностью создаваемого стегоканала, либо соответствует известным аналогам, либо превосходит их.



■ ***Рис. 7.*** Зависимость количества всех полутоновых оттенков (*а*) и только чаще встречающихся полутоновых оттенков, соответствующих цветовым кодам в каждом канале: 17, 34, 68, 102, 136, 153, 187 (*б*) от размера шрифта для символов алфавита русского языка

■ ***Fig. 7.*** Dependence of the number of all halftone shades (*a*) and only the most frequently occurring halftone shades corresponding to color codes in each channel: 17, 34, 68, 102, 136, 153, 187 (*б*) on the font size for the symbols of the Russian alphabet



■ ***Рис. 8.*** Пропускная способность одного символа растрированного текста (*а*) и символов текста-контейнера (*б*)
■ ***Fig. 8.*** Bandwidth of one symbol of rasterized text (*а*) and of text of text-container (*б*)

■ ***Таблица 1.*** Пропускная способность стеганографических каналов при сокрытии информации в полутоновых оттенках
■ ***Table 1.*** Bandwidth of steganographic channels when hiding information in halftone shades

Размер, пт	Печатные символы	Внедрение во все полутоновые оттенки		Внедрение только в часто встречающиеся оттенки	
		Количество битов	Пропускная способность, бит/пиксель	Количество битов	Пропускная способность, бит/пиксель
8	8598	675 962	0,753	364 531	0,406
9	6809	606 127	0,675	299 494	0,333
10	5492	539 873	0,601	274 721	0,306
11	4494	479 024	0,533	266 924	0,297
12	3782	440 937	0,491	227 903	0,254
14	2761	373 852	0,416	244 545	0,272
16	2100	342 526	0,381	228 073	0,254
18	1662	320 081	0,356	221 371	0,246
20	1326	287 762	0,320	201 115	0,224

■ ***Таблица 2.*** Сравнительная характеристика стеганографических методов
■ ***Table 2.*** Bandwidth of steganographic methods

Стеганографический метод	Пропускная способность, бит/пиксель	Параметры внедрения
Предложенный метод	0,32–0,75	1 бит на 1 пиксель полутонового оттенка при размерах символов от 20 до 8 пт
Mid Position Value [23]	0,25	1 бит на блок 2 × 2 пикселя
Pixel-Value Differencing [24]	0,50	1 бит на 2 пикселя
Discrete Hadamard Transform [25]	1–8	С ростом пропускной способности снижается стеганографическая стойкость

Заключение

Особенности и результаты растрирования текстовых электронных документов предоставляют хорошие возможности для реализации стеганографических методов размещения тайной информации в этих документах-контейнерах. В статье предложены модель и синтезированная на ее основе структурная схема стеганографической системы, основанные на модификации пространственной области и цветовых параметров пикселей растрированного документа-контейнера. Основу модели составляет теоретико-множественное определение и взаимосвязь основных компонентов системы, представляющей собой совокупность множеств стегоканалов, контейнеров, сообщений и ключей. Последние соотносятся с процедурами подготовки (генерации) сообщения, с особенностями алгоритмов прямого и обратных стегопреобразований, выбором пикселей и модификацией (в процессе внедрения информации) их цветовых кодов и др. Ключевым отличием модели от известных является определение компонент системы с учетом полутонового (в оттенках серого) представления символов контейнера (растрирования текста). Из-за естественных вариаций кодов каждого цветового канала отдельно взятого пикселя после растрирования изображения, проявляющихся в том, что эти коды не всегда будут одинаковыми (например, может быть (17, 17, 17) в модели RGB, а может быть (17, 18, 17) или (18, 17, 17)), предложенный метод и реализующие его алгоритмы обеспечивают достаточно высокий уровень стойкости к атакам, направленным на обнаружение и извлечение информации из стегоконтейнера, при высоком уровне пропускной способности создаваемого стегоканала.

Оценка стеганостойкости основывается на следующих постулатах:

— извлечь размещенную в контейнер информацию можно, как правило, зная ключи; особенность метода состоит в использовании многопараметрического ключа преобразования, что значительно снижает эффективность стеганографического;

— при определенных условиях (небольшом размере тайного сообщения, псевдослучайном характере его размещения внутри контейнера и др.) и с учетом того, что даже в оригинальном контейнере после его растрирования цветовые коды отдельных пикселей отличаются, выявить осажденное сообщение практически невозможно.

Финансовая поддержка

Исследование выполнено при финансовой поддержке Правительства Республики Беларусь в рамках НИР «Методы, алгоритмы и программные средства размещения невидимой идентификационной информации в электронных картах и текстовых документах на основе стеганографии и избыточного кодирования».

Литература

1. **Haas T. C.** Adapting cybersecurity practice to reduce wildlife cybercrime. *Journal of Cybersecurity*, 2023, vol. 9, no. 1. doi:10.1093/cybsec/tyad004, EDN: CRUSLY
2. **Admass W. S., Munaye Y. Y., Diro A. A.** Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, 2024, vol. 2, Article 100031. doi:10.1016/j.csa.2023.100031, EDN: DEXDKS
3. **Blinova E. A., Urbanovich P. P.** Steganographic method based on hidden messages embedding into Bezier curves of SVG images. *Журнал Белорусского государственного университета. Математика. Информатика*, 2021, № 3, с. 68–83. doi:10.33581/2520-6508-2021-3-68-83
4. **Аграновский А. В., Балакин А. В., Грибунин В. Г.** *Стеганография, цифровые водяные знаки и стеганоанализ*: Монография. М., Вузовская книга, 2009. 217 с.

5. **Шутько Н. П.** Защита авторских прав на электронные текстовые документы методами стеганографии. *Труды БГТУ. № 6. Физико-математические науки и информатика*, 2013, № 6 (162), с. 131–134. EDN: TKARYJ
6. **Blinova E. A., Stashevskaya I. Y., Urbanovich P. P.** A steganographic method of embedding an identifier into the spatial data of an electronic map. *Журнал Белорусского государственного университета. Математика. Информатика*, 2023, № 1, с. 76–87. doi:10.33581/2520-6508-2023-1-76-87
7. **Foley J. D., van Dam A., Feiner S. K., Hughes J. F.** *Computer Graphics: Principles and Practice*. 2nd ed. C. Addison-Wesley Professional, 1996. 1175 p.
8. **Shirley P., Ashikhmin M., Marschner S.** *Fundamentals of Computer Graphics*. AK Peters/CRC Press, 2009. 804 p. doi:org/10.1201/9781439865521
9. **Савельева М. Г., Урбанович П. П.** Использование статистических характеристик растрирования текстовых документов в стеганографических приложениях. *Труды БГТУ. Сер. 3: Физико-математические науки и информатика,* 2023, № 2 (272), *с.* 89–96. doi:10.52065/2520-6141-2023-272-2-13, EDN: ZZMGFZ
10. **Cachin C.** An information-theoretic model for steganography. *Information and Computation*, 2004, vol. 192, iss. 1, pp. 41–56. doi:10.1016/j.ic.2004.02.003
11. **Sallee P.** Model-Based Steganography. *International Workshop on Digital Watermarking*. Berlin, Heidelberg, Springer Berlin Heidelberg, 2003, pp. 154–167. doi:10.1007/978-3-540-24624-4_12
12. **Kuznetsov A., Smirnov A., Meleshko E.** The mathematical model and flow diagram of the steganography system. *Technika v Silskogospodarskomu Virobnictvi, Galuzevie Mašinobuduvannia, Avtomatizacja*, 2012, no. 1 (25), pp. 273–281.
13. **Koptyra K., Ogiela M. R**. Key generation for multi-secret steganography. *2015 2nd Intern. Conf. on Information Science and Security (ICISS)*, 14–16 December 2015, Seoul, Korea (South), IEEE, 2015, pp. 1–4. doi:10.1109/ICISSEC.2015.7371013
14. **Urbanovich P., Shutko N.** Theoretical Model of a Multi-Key Steganography System. *Recent Developments in Mathematics and Informatics. Contemporary Mathematics and Computer Science. Part II Computer Science*. Wydawnictwo KUL, 2016, pp. 181–202.
15. **Shutko N., Urbanovich P. P., Zukowski P.** A method of syntactic text steganography based on modification of the document-container aprosh. *Przegląd Elektrotechniczny*, 2018, R. 94, NR 6, pp. 82–85. doi:10.15199/48.2018.06.15
16. **Блинова Е. А.** Математическая модель стеганографической системы на основе ключевой информации в виде стеганонаборов. *Системный анализ и прикладная информатика*, 2022, № 3, с. 67–74. doi:10.21122/2309-4923-2022-3-67-74
17. **Mumthas S., Lijiya A.** Transform domain video steganography using RSA, random DNA encryption and Huffman encoding. *Procedia Computer Science*, 2017, vol. 115, pp. 660–666. doi:10.1016/J.PROCS.2017.09.152
18. **Taha M. S., Mohd Rahim M. S., Lafta S. A., Hashim M. M., Alzuabidi H. M.** Combination of steganography and cryptography: A short survey. *IOP Conf. Series Materials Science and Engineering*, IOP Publishing, 2019, vol. 518, no. 5, pp. 052003. doi:10.1088/1757-899X/518/5/052003
19. **Majeed M. A., Sulaiman R., Shukur Z.** New text steganography technique based on multilayer encoding with format-preserving encryption and Huffman coding. *International Journal of Advanced Computer Science and Applications*, 2022, vol. 13(12), pp. 163–172. doi:10.14569/IJACSA.2022.0131222
20. **Zainal N., Hoshi A. R., Ismail M., Rahem R. T., Wadi S. M.** A hybrid steganography and watermark algorithm for copyright protection by using multiple embedding approaches. *Bulletin of Electrical Engineering and Informatics*, 2024, vol. 13, no. 3, pp. 1877–1896. doi:10.11591/eei.v13i3.6337
21. **Crandall R.** Some notes on steganography. *Posted on Steganography Mailing List*, 1998. http://os.inf.tu-dresden.de/west-feld/crandall.pdf (дата обращения: 12.07. 2024).
22. **Fridrich J., Goljan M., Soukal D.** Efficient wet paper codes. *International Workshop on Information Hiding*. Berlin, Heidelberg, Springer Berlin Heidelberg, 2005, pp. 204–218. doi:10.1007/11558859_16
23. **Bierbrauer J., Fridrich J.** Constructing good covering codes for applications in steganography. *Transactions on Data Hiding and Multimedia Security III*. Berlin, Heidelberg, Springer Berlin Heidelberg, 2008. doi:10.1007/978-3-540-69019-1_1
24. **Wu D. C., Tsai W. H.** A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, 2003, vol. 24, no. 9-10, pp. 1613–1626. doi:10.1016/S0167-8655(02)00402-6
25. **Zhang Y. Q., Zhong K., Wang X. Y.** High-capacity image steganography based on discrete Hadamard transform. *IEEE Access*, 2022, vol. 10, pp. 65141–65155. doi: 10.1109/ACCESS.2022.3181179
26. **Sahu A. K., Swain G.** A novel multi stego-image based data hiding method for gray scale image. *Pertanika Journal of Science & Technology*, 2019, vol. 27, no. 2, pp. 753–768.
27. **Lee Y. K., Chen L. H.** High capacity image steganographic model. *IEE Proceedings-Vision, Image and Signal Processing*, 2000, vol. 147, no. 3, pp. 288–294. doi:10.1049/ip-vis:20000341
28. **Савельева М. Г., Урбанович П. П.** Растрирование web-документов и использование его характеристик для стеганографической защиты авторских прав на электронный контент. *Труды БГТУ. Сер. 3, Физико-математические науки и информатика*, 2023, № 1 (266), с. 54–63. doi:10.52065/2520-6141-2023-266-1-10
29. **Ляшевская О. Н.** *Частотный словарь современного русского языка (на материалах Национального корпуса русского языка).* М., Азбуковник, 2009. 1090 с.

UDC 004.56+003.26
doi:10.31799/1684-8853-2024-6-2-14
EDN: AOSASL

Steganographic transformation based on the modification of halftone shades of rasterized documents

M. G. Saveleva[a], Post-Graduate Student, orcid.org/0009-0000-3250-8317
P. P. Urbanovich[a,b], Dr. Sc., Tech., Professor, orcid.org/0000-0003-2825-4777, p.urbanovich@belstu.by
[a]Belarusian State Technological University, 13a, Sverdlov St., 220006, Minsk, Republic of Belarus
[b]John Paul II Catholic University of Lublin, 14, Racławickie Al., 20-950, Lublin, Poland

Introduction: Research aimed at using hidden channels for transmitting and storing information based on steganography is becoming increasingly important. One of the types of transformations of electronic text documents is their rasterization. The features and result of this operation can be used as the basis for a new method of steganographic transformation. **Purpose:** To develop a model, and on its basis — to synthesize a structural diagram of a steganographic system, as well as to develop a method of steganographic transformation, which uses the pixel representation of container text characters obtained by rasterizing the text. **Results:** The structure of the proposed steganographic system is based on the use of the features of rasterization of container documents. We develop a mathematical model of such a system, based on a set-theoretical representation of the main components of the system, as well as on a multiparametric representation of the key for direct and reverse steganographic transformations. In this case, the elements of the key are related, among other things, to the color and spatial-geometric properties and parameters of individual pixels of the container-document. We also develop a method and algorithms for steganographic embedding and extraction of secret information based on the above-mentioned model. We perform a comparative assessment of the throughput of the steganographic channel (bit/pixel) created on the basis of the proposed method. **Practical relevance:** The obtained theoretical results reflect general features of the synthesis and analysis of steganographic systems, the transformations in which are based on the use of halftone shades of electronic documents when rasterizing the latter. Using the proposed method, it is possible to embed secret information into a rasterized container document for its transmission, integrity control, and protection of copyrights on this document.

Keywords — steganography, rasterization, algorithm, mathematical model, color, spatial domain, steganographic methods.

For citation: Saveleva M. G., Urbanovich P. P. Steganographic transformation based on the modification of halftone shades of rasterized documents. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 6, pp. 2–14 (In Russian). doi:10.31799/1684-8853-2024-6-2-14, EDN: AOSASL

Financial support

The investigation was carried out with the financial support of the Government of the Republic of Belarus within the framework of the research project “Methods, algorithms and software for placing invisible identification information in electronic cards and text documents based on steganography and redundant coding”.

References

1. Haas T. C. Adapting cybersecurity practice to reduce wildlife cybercrime. *Journal of Cybersecurity*, 2023, vol. 9, no. 1. doi:10.1093/cybsec/tyad004, EDN: CRUSLY
2. Admass W. S., Munaye Y. Y., Diro A. A. Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, 2024, vol. 2, Article 100031. doi:10.1016/j.csa.2023.100031, EDN: DEXDKS
3. 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:10.33581/2520-6508-2021-3-68-83
4. Agranovskiy A. V., Balakin A. V., Gribunin V. G. *Steganografiya, tsifrovyye vodyanyye znaki i steganoanaliz* [Steganography, digital watermarking and steganalysis]. Moscow, Vuzovskaya kniga Publ., 2009. 217 p. (In Russian).
5. Shutko N. P. Copyright protection of electronic text documents using steganography methods. *Trudy BGTU. № 6. Fiziko-matematicheskie nauki i informatika* [Proceedings of BSTU. No. 6. Physics and Mathematics. Informatics], 2013, no. 6 (162), pp. 131–134 (In Russian). EDN: TKARYJ
6. Blinova E. A., Stashevskaya I. Y., Urbanovich P. P. A steganographic method of embedding an identifier into the spatial data of an electronic map. *Journal of the Belarusian State University. Mathematics and Informatics*, 2023, no. 1, pp. 76–87. doi: 10.33581/2520-6508-2023-1-76-87
7. Foley J. D., van Dam A., Feiner S. K., Hughes J. F. *Computer Graphics: Principles and Practice*. 2nd ed. C. Addison-Wesley Professional, 1996. 1175 p.
8. Shirley P., Ashikhmin M., Marschner S. *Fundamentals of Computer Graphics*. AK Peters/CRC Press, 2009. 804 p. doi:org/10.1201/9781439865521
9. Saveleva M. G., Urbanovich P. P. Usage of statistical characteristics of text documents halftone screening in steganographic applications. *Proceedings of BSTU. Issue 3, Physics and Mathematics. Informatics*, 2023, no. 2 (272), pp. 89–96 (In Russian). doi:10.52065/2520-6141-2023-272-2-13, EDN: ZZMGFZ
10. Cachin C. An information-theoretic model for steganography. *Information and Computation*, 2004, vol. 192, iss. 1, pp. 41–56. doi:10.1016/j.ic.2004.02.003
11. Sallee P. *Model-Based Steganography*. In: *International Workshop on Digital Watermarking*. Berlin, Heidelberg, Springer Berlin Heidelberg, 2003, pp. 154–167. doi:10.1007/978-3-540-24624-4_12
12. Kuznetsov A., Smirnov A., Meleshko E. The mathematical model and flow diagram of the steganography system, *Technika v Silskogospodarskomu Virobnictvi, Galuzevie Mašinobuduvannia, Avtomatizacja*, 2012, no. 1 (25), pp. 273–281.
13. Koptyra K., Ogiela M. R. Key generation for multi-secret steganography. *2015 2nd Intern. Conf. on Information Science and Security (ICISS)*, IEEE, 2015, pp. 1–4. doi: 10.1109/ICISSEC.2015.7371013
14. Urbanovich P., Shutko N. *Theoretical Model of a Multi-Key Steganography System*. In: *Recent Developments in Mathematics and Informatics. Contemporary Mathematics and Computer Science. Part II Computer Science*. Wydawnictwo KUL, 2016, pp. 181–202.
15. Shutko N., Urbanovich P. P., Zukowski P. A method of syntactic text steganography based on modification of the document-container aprosh. *Przegląd Elektrotechniczny*, 2018, R. 94, no. 6, pp. 82–85. doi:10.15199/48.2018.06.15
16. Blinova E. A. Mathematical model of a steganographic system based on key information in the form of stegosets. *System Analysis and Applied Information Science*, 2022, no. 3, pp. 67–74 (In Russian). doi:10.21122/2309-4923-2022-3-67-74
17. Mumthas S., Lijiya A. Transform domain video steganography using RSA, random DNA encryption and Huffman encoding. *Procedia Computer Science*, 2017, vol. 115, pp. 660–666. doi:10.1016/J.PROCS.2017.09.152
18. Taha M. S., Mohd Rahim M. S., Lafta S. A., Hashim M. M., Alzuabidi H. M. Combination of steganography and cryptography: A short survey. *IOP Conf. Series Materials Science and Engineering*, IOP Publishing, 2019, vol. 518, no. 5, pp. 052003. doi:10.1088/1757-899X/518/5/052003

19. Majeed M. A., Sulaiman R., Shukur Z. New text steganography technique based on multilayer encoding with format-preserving encryption and Huffman coding. *International Journal of Advanced Computer Science and Applications*, 2022, vol. 13(12), pp. 163–172. doi:10.14569/IJACSA.2022.0131222
20. Zainal N., Hosh A. R., Ismail M., Rahem R. T., Wadi S. M. A hybrid steganography and watermark algorithm for copyright protection by using multiple embedding approaches. *Bulletin of Electrical Engineering and Informatics*, 2024, vol. 13, no. 3, pp. 1877–1896. doi:10.11591/eei.v13i3.6337
21. Crandall R. Some notes on steganography. *Posted on Steganography Mailing List*, 1998. Available at: http://os.inf.tu-dresden.de/west-feld/crandall.pdf (accessed 20 July 2024).
22. Fridrich J., Goljan M., Soukal D. *Efficient wet paper codes*. In: *International Workshop on Information Hiding*. Berlin, Heidelberg, Springer Berlin Heidelberg, 2005, pp. 204–218. doi:10.1007/11558859_16
23. Bierbrauer J., Fridrich J. *Constructing good covering codes for applications in steganography*. In: *Transactions on Data Hiding and Multimedia Security III*. Berlin, Heidelberg, Springer Berlin Heidelberg, 2008. doi:10.1007/978-3-540-69019-1_1
24. Wu D. C., Tsai W. H. A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, 2003, vol. 24, no. 9-10, pp. 1613–1626. doi:10.1016/S0167-8655(02)00402-6
25. Zhang Y. Q., Zhong K., Wang X. Y. High-capacity image steganography based on discrete Hadamard transform. *IEEE Access*, 2022, vol. 10, pp. 65141–65155. doi:10.1109/ACCESS.2022.3181179
26. Sahu A. K., Swain G. A novel multi stego-image based data hiding method for gray scale image. *Pertanika Journal of Science & Technology*, 2019, vol. 27, no. 2, pp. 753–768.
27. Lee Y. K., Chen L. H. High capacity image steganographic model. *IEE Proceedings-Vision, Image and Signal Processing*, 2000, vol. 147, no. 3, pp. 288–294. doi:10.1049/ip-vis:20000341
28. Saveleva M. G., Urbanovich P. P. Rasterization of web documents and the use of its characteristics for steganographic copyright protection of electronic content. *Proceedings of BSTU. Issue 3, Physics and Mathematics. Informatics*, 2023, no. 1 (266), pp. 54–63 (In Russian). doi:10.52065/2520-6141-2023-266-1-10
29. Lyashevskaya O. N. *Chastotnyy slovar' sovremennogo russkogo yazyka (na materialakh Natsional'nogo korpusa russkogo yazyka)* [Frequency dictionary of the modern Russian language (based on the materials of the National Corpus of the Russian language)]. Moscow, Azbukovnik Publ., 2009. 1090 p. (In Russian).