Robust Steganographic Method with Code-Controlled Information Embedding

Kobozeva A.A. Sokolov A.V

Odessa Polytechnic State University,
Odessa, Ukraine

Abstract. In view of the fact that most images are compressed when transmitted through telecommunication systems and telecommunication systems in the energetics, from the point of view of the practical use of steganographic algorithms in real information security systems, such as their property, the ability to effectively resist a compression attack, is of great interest. This work aims at increasing the robustness of steganographic system against compression attacks to ensure the reliability of the steganographic message perception by developing a steganographic method that implements the embedding of additional information in the spatial domain of the container, using the code control of the frequency components that are under perturbations resulting from the steganographic transformation. The goal was achieved using the code control of information embedding: due to preliminary additional coding of the embedded information with codewords for which the Walsh-Hadamard transformants have the specified properties, which leads to a given localization of disturbances in the Walsh-Hadamard domain of the container as a result of the information embedding. The most significant result is the steganographic method developed based on the formed theoretical basis, for which classes of codewords that provide the highest robustness against the compression attacks were constructed. The significance of the results obtained is that the developed method ensured a high reliability level of perception the steganographic messages, significant robustness against the compression attacks, as well as simplicity of algorithmic implementation and high performance.

***Keywords*:** steganography, Walsh-Hadamard transform, code control, compression attack, JPEG.
DOI: https://doi.org/10.52254/1857-0070.2021.4-52.11
UDC: 004.056

O metodă steganografică rezistentă cu încorporare de informații controlată de cod

Kobozeva A.A., Sokolov A.B.
Universitatea de Stat «Odeskaia politehnica», Odesa, Ucraina

Rezumat. Având în vedere faptul că majoritatea imaginilor transmise prin sistemele de telecomunicații, inclusiv sistemele de telecomunicații din sectorul energetic, sunt supuse compresiei, în ceea ce privește utilizarea practică a algoritmilor steganografici în sistemele reale de protecție a informațiilor, este de mare interes capacitatea lor de a rezista eficient la un atac de compresie. Scopul acestei lucrări este de a majora rezistența sistemului steganografic la atacurile de compresie și, în același timp, de a oferi fiabilitate în percepția unui mesaj steganografic prin dezvoltarea unei metode steganografice care implementează informații suplimentare în domeniul spațial al unui container folosind controlul codului componentelor de frecvență care suferă perturbații ca urmare a transformării steganografice. Acest obiectiv a fost atins prin controlul codului de încorporare a informației: precodificarea informației încorporate cu cuvinte-cod, pentru care transformantele Walsh-Adamar au anumite proprietăți, ceea ce conduce la o anumită localizare a perturbațiilor în regiunea Walsh-Adamar a containerului ca urmare a încorporării informației. În baza suportului teoretic formulat, a fost dezvoltată o metodă steganografică pregătită pentru implementare în practică, pentru care au fost construite clase de cuvinte-cod care asigură un nivel sporit de fiabilitate a percepției mesajului stegano, precum și o rezistență semnificativă la atacurile de compresie, fapt confirmat de experimentele efectuate în această lucrare și de o analiză comparativă cu analogii actuale. Implementarea și extragerea informației adiționale are loc în spațiul containerului, ce asigură metodei steganografice cât simplitatea de realizare algoritmică, atât și operativitate înaltă.

***Cuvinte-cheie*:** steganografie, transformarea Walsh-Adamar, prin cod, atac de compresie, JPEG.

Устойчивый стеганографический метод с кодовым управлением внедрением информации

Кобозева А.А., Соколов А.В.
Государственный университет «Одесская политехника»,
Одесса, Украина

Аннотация. В виду того, что большинство изображений при передаче через телекоммуникационные системы, в том числе, и в телекоммуникационных системах в энергетике подвергаются сжатию, с точки

© Кобозева А.А., Соколов А.В., 2021

зрения практического использования стеганографических алгоритмов в реальных системах защиты информации, большой интерес представляет их способность эффективно противостоять атаке сжатием. При этом большая часть современных стеганоалгоритмов являются неустойчивыми к атакам сжатием. Целью работы является повышение устойчивости стеганографической системы к атакам сжатием с одновременным обеспечением надежности восприятия стеганосообщения путем разработки стеганографического метода, осуществляющего внедрение дополнительной информации в пространственной области контейнера с использованием кодового управления частотными составляющими, претерпевающими возмущения в результате стеганопреобразования. Поставленная цель была достигнута за счет кодового управления внедрением информации: предварительного дополнительного кодирования внедряемой информации кодовыми словами, для которых трансформанты преобразования Уолша-Адамара имеют заданные свойства, что приводит к заданной локализации возмущений в области Уолша-Адамара контейнера в результате внедрения информации. Таким образом, манипулируя свойствами применяемых кодовых слов, становится возможным обеспечить конкретные свйства стеганосообщения. На основе сформированного теоретического базиса разработан готовый к практической реализации стеганографический метод, для которого построены классы кодовых слов, обеспечивающих высокий уровень надежности восприятия стеганосообщения, а также значительную устойчивость к атакам сжатием, что подтверждается проведенными в работе экспериментами и сравнительным анализом с современными аналогами. При этом внедрение и извлечение дополнительной информации происходит в пространственной области контейнера, что обеспечивает разработанному стеганографическому методу как простоту алгоритмической реализации, так и высокое быстродействие.
Ключевые слова: стеганография, преобразование Уолша-Адамара, кодовое управление, атака сжатием, JPEG.

1. ВВЕДЕНИЕ И ПОСТАНОВКА ЗАДАЧИ

Использование современных энергосетей в качестве среды для передачи информации, в частности, конфиденциальной, обуславливает высокую актуальность совершенствования методов её защиты.

Наряду с криптографической защитой информации, одним из основных звеньев современных систем кибербезопасности, является стеганографическая подсистема, обеспечивающая сокрытие самого факта передачи информации. Высокая востребованность стеганографических методов в современных информационных технологиях обуславливает значительное внимание исследователей, направленное на совершенствование их характеристик [1…5].

В настоящее время, существует и разрабатывается большое количество стеганографических методов, которые основаны на различных математических конструкциях и преобразованиях.

К современным стеганографическим методам, учитывая состояние информационных технологий, увеличение объемов информации, передаваемой по каналам связи, предъявляется ряд требований, основными из которых являются:

1. обеспечение надежности восприятия стеганосообщения;
2. устойчивость к атакам против встроенного сообщения;
3. устойчивость к атакам стеганоанализа;
4. для обеспечения возможности стеганопреобразования в режиме реального времени необходимым является обеспечение малой вычислительной сложности, а также существование потенциальной возможности распараллеливания стеганоалгоритмов.

При этом, под надежностью восприятия стеганосообщения понимается невозможность визуального определения наличия дополнительной информации в контейнере. Обеспечение данного требования было предметом исследования предыдущих работ авторов. В настоящей работе основное внимание авторов сконцентрировано на втором и четвертом требованиях.

Внедрение дополнительной информации (ДИ) может осуществляться в различных областях контейнера: пространственной (временной) [6-10], областях различных преобразований, в частности, частотной [11-14], области сингулярного (спектрального разложения) соответствующих матриц [15-18], области преобразования Уолша-Адамара [19-22] и др.

В качестве контейнера в работе рассматривается цифровое изображение (ЦИ).

Классическим стеганографическим методом принято считать метод LSB (Least Significant Bit), в основе которого лежит модификация одного или нескольких наименьших значащих бит значений яркости пикселей изображения. К несомненным

достоинствам данного метода необходимо отнести гарантированное обеспечение надежности восприятия стеганосообщения, а также простоту реализации процедуры погружения и извлечения информации. Недостатками указанного метода является его неустойчивость к атакам против встроенного сообщения, в частности, к атаке сжатием.

Устойчивость стеганометода обеспечивается, как правило, в областях преобразования ЦИ, хотя такое требование в свете [23] не является необходимым, более того, использование области различных преобразований, как указано в работе [6], повышает вычислительную сложность алгоритма из-за необходимости перехода из пространственной области в область выбранного преобразования и обратно, а также способствует накоплению дополнительной вычислительной погрешности, что затрудняет использование таких методов в режиме реального времени.

Подробный обзор современных стеганографических методов можно найти в работе [24]. Основной причиной предпочтения использования для погружения ДИ областей преобразования контейнера очевидно является тот факт, что обеспечить здесь устойчивость метода к атакам против встроенного сообщения легче, чем в пространственной [23], опираясь на имеющиеся достаточные условия такой устойчивости, однако не существует никаких принципиальных возражений для обеспечения устойчивости к возмущающим воздействиям при организации стеганопреобразования в пространственной области контейнера.

Среди стеганографических методов, работающих в пространствах преобразований исходного изображения особый интерес представляют стеганографические методы, основанные на внедрении информации в области преобразования Уолша-Адамара в виду высокого соответствия структуры данного преобразования принципам построения современной вычислительной техники (принадлежность элементов его базисных векторов множеству значений $\{+1,-1\}$, а также простота построения матриц преобразования).

Исследования, проведенные в данной работе, показывают возможности использования свойств преобразования Уолша-Адамара для построения нового стеганографического метода, работающего в пространственной области контейнера, который объединяет обеспечение высокой надежности восприятия, присущей методу LSB, а также высокой устойчивостью к атакам, направленным на разрушение стеганосообщения, прежде всего, к атаке сжатием.

На основе данных, представленных в открытом доступе, были выбраны методы [11, 15…,17] в виду того, что для данных методов известны достаточные количественные исследования относительно их устойчивости к атакам сжатием.

Разработанный в данной статье метод, в отличие от известных аналогов, основанных на внедрении информации в области сингулярного разложения блоков изображения [15…17], характеризуется значительно более высокой надежностью восприятия стеганосообщения, в то время как в отличие от метода [11] — большей стойкостью стеганосообщения к атакам сжатием.

Кроме того, разработанный метод, в отличие от аналогов [11, 15…17], выполняет внедрение и извлечение дополнительной информации в пространственной области, что обуславливает эффективность его алгоритмической реализации и высокое быстродействие.

Целью работы является повышение устойчивости стеганографической системы к атаке сжатием с одновременным обеспечением гарантированной надежности восприятия стеганосообщения путем разработки стеганографического метода, осуществляющего внедрение ДИ в пространственной области контейнера с использованием кодового управления частотными составляющими, претерпевающими возмущения в результате стеганопреобразования.

2. ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ

Рассмотрим основные определения, необходимые для проводимых в настоящей работе исследований.

Одним из основных видов преобразования, используемых в обработке (в частности, сжатии) изображений и видео является дискретное косинусное преобразование (ДКП), которое определяется следующим соотношением

$$S = C_N X C_N^T, \quad (1)$$

где X — фрагмент исходного изображения размера $N \times N$,

C_N — $N \times N$-матрица ДКП, элементы $C(i, j)$, $i, j = 0,1,...,N-1$ которой вычисляются в соответствии с формулой

$$C(i, j) = \begin{cases} \frac{1}{\sqrt{N}}, & \text{при } i = 0; \\ \sqrt{\frac{2}{N}} \cos(2j+1) \cdot i \cdot \pi, & \text{при } i > 0. \end{cases} \quad (2)$$

Трансформанты ДКП показывают распределение контента блока изображения по частотным составляющим.

При этом известно [25], что чувствительность стеганосообщения к возмущающим воздействиям зависит от того, какие именно частотные составляющие претерпели возмущение в процессе стеганопреобразования.

Устойчивость стеганометода к атакам против встроенного сообщения обеспечивается за счет возмущения низкочастотных составляющих ЦИ-контейнера.

Такие изменения с большой вероятностью негативно отразятся на надежности восприятия стеганосообщения, в силу чего на практике часто используется «компромиссный вариант», когда внедрение ДИ производится таким образом, чтобы возмущения получали среднечастотные составляющие цифрового контента.

Однако, такой подход обеспечивает устойчивость стеганометода лишь к незначительным возмущающим воздействиям, в то время как в реалиях атаки против встроенного сообщения могут быть значительными (например, сжатие стеганосообщения с малым коэффициентом качества).

Перспективным видом преобразований, которое используется для построения современных стеганографических методов [26], является двумерное преобразование Уолша-Адамара, которое задается с помощью следующего соотношения

$$W_X = H'_N X H'^T_N, \quad (3)$$

где $H'_N = \frac{1}{\sqrt{N}} H_N$, X — матрица размера $N \times N$, а матрица Адамара H_N порядка N задается с помощью конструкции Сильвестра

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, \; H_1 = 1. \quad (4)$$

Отметим, что помимо двумерного преобразования Уолша-Адамара в теории сигналов и криптографии широко применяется одномерное преобразование Уолша-Адамара вектора-строки Y длины N, которое записывается как

$$V = YH_N. \quad (5)$$

В предыдущих работах авторами настоящей статьи была установлена взаимосвязь между матрицей трансформант преобразования Уолша-Адамара W_X, матрицей трансформант ДКП S, и составляющих сингулярного разложения исходной матрицы X, что позволило сформировать соответствие между трансформантами преобразования Уолша-Адамара и ДПК для практически ценных значений порядка $N \in \{4,8,16\}$ матрицы X, которое отображено на рис. 1, где указаны индексы трансформант ДКП на местах соответствующих им трансформант преобразования Уолша-Адамара. По сути, рис. 1. устанавливает взаимосвязь между трансформантами преобразования Уолша-Адамара и ДКП. Например, для размера блока 4×4, трансформанта преобразования Уолша-Адамара (1,3) соответствует трансформанте ДКП (1,2), в то время как трансформанта преобразования Уолша-Адамара (3,1) соответствует трансформанте ДКП (2,1) и т.д.

Еще одним необходимым для решаемых в настоящей статье задач результатом, полученным в предыдущих работах авторов, является установленная взаимосвязь между двумерным (3) и одномерным (5) преобразованием Уолша-Адамара.

Так, с точностью до коэффициента $1/N$ двумерное преобразование Уолша-Адамара вида (3) может быть представлено через одномерное преобразование Уолша-Адамара (5) с помощью следующего соотношения

$$V = YH_{N_2}, \quad (6)$$

где V и Y — векторы-строки длины N^2, которые являются результатом последовательной конкатенации строк матриц W и X (3) размера $N \times N$, соответственно.

3. КОДОВОЕ УПРАВЛЕНИЕ ЧАСТОТНЫМИ СОСТАВЛЯЮЩИМИ, ПРЕТЕРПЕВАЮЩИМИ ВОЗМУЩЕНИЕ В РЕЗУЛЬТАТЕ ВНЕДРЕНИЯ ИНФОРМАЦИИ

В качестве основы предлагаемого стеганографического метода с кодовым управлением частотными составляющими, претерпевающими возмущение в результате внедрения информации, лежит классический метод LSB-matching [27],

(1,1)	(1,4)	(1,2)	(1,3)
(4,1)	(4,4)	(4,2)	(4,3)
(2,1)	(2,4)	(2,2)	(2,3)
(3,1)	(3,4)	(3,2)	(3,3)

а

(1,1)	(1,8)	(1,4)	(1,5)	(1,2)	(1,7)	(1,3)	(1,6)
(8,1)	(8,8)	(8,4)	(8,5)	(8,2)	(8,7)	(8,3)	(8,6)
(4,1)	(4,8)	(4,4)	(4,5)	(4,2)	(4,7)	(4,3)	(4,6)
(5,1)	(5,8)	(5,4)	(5,5)	(5,2)	(5,7)	(5,3)	(5,6)
(2,1)	(2,8)	(2,4)	(2,5)	(2,2)	(2,7)	(2,3)	(2,6)
(7,1)	(7,8)	(7,4)	(7,5)	(7,2)	(7,7)	(7,3)	(7,6)
(3,1)	(3,8)	(3,4)	(3,5)	(3,2)	(3,7)	(3,3)	(3,6)
(6,1)	(6,8)	(6,4)	(6,5)	(6,2)	(6,7)	(6,3)	(6,6)

б

(1,1)	(1,16)	(1,8)	(1,9)	(1,4)	(1,13)	(1,5)	(1,12)	(1,2)	(1,15)	(1,7)	(1,10)	(1,3)	(1,14)	(1,6)	(1,11)
(16,1)	(16,16)	(16,8)	(16,9)	(16,4)	(16,13)	(16,5)	(16,12)	(16,2)	(16,15)	(16,7)	(16,10)	(16,3)	(16,14)	(16,6)	(16,11)
(8,1)	(8,16)	(8,8)	(8,9)	(8,4)	(8,13)	(8,5)	(8,12)	(8,2)	(8,15)	(8,7)	(8,10)	(8,3)	(8,14)	(8,6)	(8,11)
(9,1)	(9,16)	(9,8)	(9,9)	(9,4)	(9,13)	(9,5)	(9,12)	(9,2)	(9,15)	(9,7)	(9,10)	(9,3)	(9,14)	(9,6)	(9,11)
(4,1)	(4,16)	(4,8)	(4,9)	(4,4)	(4,13)	(4,5)	(4,12)	(4,2)	(4,15)	(4,7)	(4,10)	(4,3)	(4,14)	(4,6)	(4,11)
(13,1)	(13,16)	(13,8)	(13,9)	(13,4)	(13,13)	(13,5)	(13,12)	(13,2)	(13,15)	(13,7)	(13,10)	(13,3)	(13,14)	(13,6)	(13,11)
(5,1)	(5,16)	(5,8)	(5,9)	(5,4)	(5,13)	(5,5)	(5,12)	(5,2)	(5,15)	(5,7)	(5,10)	(5,3)	(5,14)	(5,6)	(5,11)
(12,1)	(12,16)	(12,8)	(12,9)	(12,4)	(12,13)	(12,5)	(12,12)	(12,2)	(12,15)	(12,7)	(12,10)	(12,3)	(12,14)	(12,6)	(12,11)
(2,1)	(2,16)	(2,8)	(2,9)	(2,4)	(2,13)	(2,5)	(2,12)	(2,2)	(2,15)	(2,7)	(2,10)	(2,3)	(2,14)	(2,6)	(2,11)
(15,1)	(15,16)	(15,8)	(15,9)	(15,4)	(15,13)	(15,5)	(15,12)	(15,2)	(15,15)	(15,7)	(15,10)	(15,3)	(15,14)	(15,6)	(15,11)
(7,1)	(7,16)	(7,8)	(7,9)	(7,4)	(7,13)	(7,5)	(7,12)	(7,2)	(7,15)	(7,7)	(7,10)	(7,3)	(7,14)	(7,6)	(7,11)
(10,1)	(10,16)	(10,8)	(10,9)	(10,4)	(10,13)	(10,5)	(10,12)	(10,2)	(10,15)	(10,7)	(10,10)	(10,3)	(10,14)	(10,6)	(10,11)
(3,1)	(3,16)	(3,8)	(3,9)	(3,4)	(3,13)	(3,5)	(3,12)	(3,2)	(3,15)	(3,7)	(3,10)	(3,3)	(3,14)	(3,6)	(3,11)
(14,1)	(14,16)	(14,8)	(14,9)	(14,4)	(14,13)	(14,5)	(14,12)	(14,2)	(14,15)	(14,7)	(14,10)	(14,3)	(14,14)	(14,6)	(14,11)
(6,1)	(6,16)	(6,8)	(6,9)	(6,4)	(6,13)	(6,5)	(6,12)	(6,2)	(6,15)	(6,7)	(6,10)	(6,3)	(6,14)	(6,6)	(6,11)
(11,1)	(11,16)	(11,8)	(11,9)	(11,4)	(11,13)	(11,5)	(11,12)	(11,2)	(11,15)	(11,7)	(11,10)	(11,3)	(11,14)	(11,6)	(11,11)

в

Рис. 1. Взаимосвязь между трансформантами преобразования Уолша-Адамара и ДКП для *l*×*l*-блоков ЦИ:
а – *l*=4; б – *l*=8; в – *l*=16[1].

гарантирующий обеспечение надежности восприятия стеганосообщения, который предполагает последовательное поэлементное суммирование элементов контейнера $x_{i,j} \in \{0,1,...,255\}$ с внедряемой дополнительной информацией $d_i \in \{+1,0,-1\}$.

Рассмотрим теоретическую основу возможности кодового управления частотными составляющими без перехода в частотную область. Пусть блок $X = \|x_{i,j}\|, i, j, = 0,1,..., N-1$ некоторого изображения представляет собой матрицу размера $N \times N$, в то время как результат дополнительного кодирования ДИ — вектор $D = \{d_k\}, k = 0,1,..., N^2 - 1$. Под дополнительным кодированием тут понимается представление каждого бита ДИ в виде кодового слова, обладающего заданным видом вектора трансформант преобразования Уолша-Адамара.

Путем последовательной конкатенации строк матрицы X получаем новый вектор-строку Y. Тогда результирующее стеганосообщение будет иметь вид

$$M = Y + D. \quad (7)$$

Рассмотрим теперь преобразование Уолша-Адамара вектора-строки M, в соответствии с выражением (5)

[1] Appendix 1

$$V = MH_{N^2} = (Y + D)H_{N^2} = YH_{N^2} + DH_{N^2}. \quad (8)$$

Выражение (8) позволяет сделать фундаментальный вывод о природе возмущения трансформант преобразования Уолша-Адамара в стеганосообщении после внедрения в него дополнительной информации — величина и локализация подобных возмущений будет зависеть от конкретного вида слагаемого DH_{N^2}, которое представляет собой трансформанты преобразования Уолша-Адамара внедряемой дополнительной информации. В свою очередь, конкретная локализация и амплитуда вносимых в трансформанты преобразования Уолша-Адамара стеганосообщения возмущений будет зависеть от вида внедряемой в вектор-строку Y, а значит, и в блок X, последовательности D.

В виду бинарной природы последовательности D, для определения таких её видов, которые приводят к обеспечению нечувствительности стеганосообщения к возмущающим воздействиям, воспользуемся определением элементарной структуры [28].

Определение 1. Элементарной структурой вектора трансформант преобразования Уолша-Адамара назовем набор его различных спектральных компонент с указанием их частот в векторе.

Например, рассмотрим вектор $T = [++--++--++--++--]$ длины $N = 16$, а также его вектор трансформант преобразования Уолша-Адамара $W = [0,0,16,0,0,0,0,0,0,0,0,0,0,0,0,0]$, который имеет элементарную структуру $\{16(1), 0(15)\}$, где в круглых скобках указано количество раз, которое приведенная компонента встречается в векторе трансформант преобразования Уолша-Адамара. Это с учетом (8) говорит о том, что если в качестве вектора D, являющего результатом дополнительного кодирования ДИ, использовать строки матрицы Уолша-Адамара, то за счет выбора конкретной строки возможно управлять локализацией соответствующего возмущения в области Уолша-Адамара, а значит, с учетом информации, представленной на рис. 1, и в области трансформант ДКП контейнера.

Известно, что элементарной структурой $\{N(1), 0(N-1)\}$ характеризуются двоичные векторы, которые являются строками матрицы Уолша-Адамара порядка N и их инверсии, при этом значение равное N ($-N$ в случае инверсии строки матрицы Уолша-Адамара) стоит на позиции, соответствующей номеру строки Уолша-Адамара.

Рассмотрим конкретный пример. Пусть задана матрица-фрагмент исходного изображения, для которой в соответствии с выражением (3) найдем трансформанты преобразования Уолша-Адамара (с точностью до коэффициента $1/N$)

$$X = \begin{bmatrix} 127 & 123 & 119 & 119 \\ 124 & 125 & 124 & 124 \\ 123 & 122 & 123 & 124 \\ 123 & 121 & 122 & 125 \end{bmatrix}, W_X = \begin{bmatrix} 1968 & 2 & 8 & 10 \\ -8 & 6 & 12 & 2 \\ 2 & 4 & 18 & -4 \\ -10 & 4 & 10 & 8 \end{bmatrix}. \quad (9)$$

На основе матрицы-контейнера X получим стеганосообщение M производя сложение с последовательностью $T = [++--++--++--++--]$, которая представляет собой третью строку матрицы Уолша-Адамара порядка $N^2 = 16$. В соответствии с описанным в разделе 2 настоящей статьи соответствием между двумерным и одномерным преобразованием Уолша-Адамара, представим указанную последовательность в виде матрицы порядка $N = 4$, путем её разделения на сегменты длины $N = 4$ и их последующей вертикальной конкатенации.

Представим также результат преобразования Уолша-Адамара (с точностью до коэффициента $1/N$) полученного стеганосообщения M, вычисленный в соответствии с (3)

$$M = X + D = \begin{bmatrix} 127 & 123 & 119 & 119 \\ 124 & 125 & 124 & 124 \\ 123 & 122 & 123 & 124 \\ 123 & 121 & 122 & 125 \end{bmatrix} + \begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 128 & 124 & 118 & 118 \\ 125 & 126 & 123 & 123 \\ 124 & 123 & 122 & 123 \\ 124 & 122 & 121 & 124 \end{bmatrix}; \quad (10)$$

$$W_M = \begin{bmatrix} 1968 & 2 & 24 & 10 \\ -8 & 6 & 12 & 2 \\ 2 & 4 & 18 & -4 \\ -10 & 4 & 10 & 8 \end{bmatrix}.$$

Анализируя (9) и (10) нетрудно заметить, что изменению подверглась только трансформанта преобразования Уолша-Адамара (1,3), или соответствующая ей третья трансформанта преобразования Уолша-Адамара в случае одномерного представления.

В соответствии с данными, представленными на рис. 1, указанная трансформанта преобразования Уолша-Адамара соответствует (1,2) трансформанте ДКП, таким образом, внедрение дополнительной информации возмутило, главным образом, эту составляющую.

Представленный пример наглядно иллюстрирует сущность предлагаемого метода кодового управления частотными составляющими.

4. ОБЕСПЕЧЕНИЕ УСТОЙЧИВОСТИ СТЕГАНОМЕТОДА К АТАКЕ СЖАТИЕМ

В настоящей работе установлено, что использование кодового управления частотными составляющими, претерпевающими возмущение в результате внедрения информации, может быть основой стеганографического метода, обеспечивающего значительное снижение вероятности повреждения ДИ атаками сжатием при сохранении показателей качества исходного изображения на высоких уровнях, присущих методу LSB.

Для использования кодового управления частотными составляющими, претерпевающими возмущение в результате внедрения информации, нам необходимо установить те трансформанты преобразования Уолша-Адамара 8×8-блоков исходного изображения, которые получают наименьшее возмущение при его сжатии алгоритмом JPEG с различными настройками качества.

Такими трансформантами являются низкочастотные составляющие, соответствующие трансформантам ДКП (2,1), (1,2), (2,2), а также постоянная составляющая (1,1), которые, соответствуют (рис. 1) трансформантам преобразования Уолша-Адамара (1,5), (5,1), (5,5), а также постоянной составляющей (1,1).

Таким образом, наибольшую целесообразность представляет построение кодов, которые бы оказывали наибольшее воздействие именно на данные трансформанты.

В соответствии с установленным соответствием между двумерным и одномерным преобразованием Уолша-Адамара в качестве таких кодовых слов возьмем 5, 33, 37 и 1-ю строки матрицы Уолша-Адамара порядка $N^2 = 64$ (в виде соответствующих им матриц порядка $N = 8$), для каждой из которых в выражении (11) приведем соответствующую матрицу трансформант преобразования Уолша-Адамара (с точностью до коэффициента $1/N$).

Отметим также, что помимо представленных кодовых слов удается определить кодовые слова, производящие воздействие одновременно на 4 частотные составляющие, т.е. обладающие элементарной структурой $\{N/2(4), 0(N-4)\}$.

$$T_1^+ = \begin{bmatrix} 1111{-}1{-}1{-}1 \\ 1111{-}1{-}1{-}1 \\ 1111{-}1{-}1{-}1 \\ 1111{-}1{-}1{-}1 \\ 1111{-}1{-}1{-}1 \\ 1111{-}1{-}1{-}1 \\ 1111{-}1{-}1{-}1 \\ 1111{-}1{-}1{-}1 \end{bmatrix}, \quad W_1^+ = \begin{bmatrix} 000064000 \\ 0000\ 0\ 000 \\ 0000\ 0\ 000 \\ 0000\ 0\ 000 \\ 0000\ 0\ 000 \\ 0000\ 0\ 000 \\ 0000\ 0\ 000 \\ 0000\ 0\ 000 \end{bmatrix};$$

$$T_2^+ = \begin{bmatrix} 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1 \\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1 \\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1 \\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1 \\ {-}1{-}1{-}1{-}1{-}1{-}1{-}1{-}1 \\ {-}1{-}1{-}1{-}1{-}1{-}1{-}1{-}1 \\ {-}1{-}1{-}1{-}1{-}1{-}1{-}1{-}1 \\ {-}1{-}1{-}1{-}1{-}1{-}1{-}1{-}1 \end{bmatrix}, W_2^+ = \begin{bmatrix} 0\ 0000000 \\ 0\ 0000000 \\ 0\ 0000000 \\ 0\ 0000000 \\ 640000000 \\ 0\ 0000000 \\ 0\ 0000000 \\ 0\ 0000000 \end{bmatrix}; \qquad (11)$$

$$T_3^+ = \begin{bmatrix} 1\ 1\ 1\ 1{-}1{-}1{-}1{-}1 \\ 1\ 1\ 1\ 1{-}1{-}1{-}1{-}1 \\ 1\ 1\ 1\ 1{-}1{-}1{-}1{-}1 \\ 1\ 1\ 1\ 1{-}1{-}1{-}1{-}1 \\ {-}1{-}1{-}1{-}1\ 1\ 1\ 1\ 1 \\ {-}1{-}1{-}1{-}1\ 1\ 1\ 1\ 1 \\ {-}1{-}1{-}1{-}1\ 1\ 1\ 1\ 1 \\ {-}1{-}1{-}1{-}1\ 1\ 1\ 1\ 1 \end{bmatrix}, W_3^+ = \begin{bmatrix} 0000\ 0\ 000 \\ 0000\ 0\ 000 \\ 0000\ 0\ 000 \\ 0000\ 0\ 000 \\ 000064000 \\ 0000\ 0\ 000 \\ 0000\ 0\ 000 \\ 0000\ 0\ 000 \end{bmatrix};$$

$$T_4^+ = \begin{bmatrix} 11111111 \\ 11111111 \\ 11111111 \\ 11111111 \\ 11111111 \\ 11111111 \\ 11111111 \\ 11111111 \end{bmatrix}, \quad W_4^+ = \begin{bmatrix} 640000000 \\ 0\ 0000000 \\ 0\ 0000000 \\ 0\ 0000000 \\ 0\ 0000000 \\ 0\ 0000000 \\ 0\ 0000000 \\ 0\ 0000000 \end{bmatrix}.$$

Мы представляем в выражении (12) указанные кодовые слова длины $N = 64$, воздействующие одновременно на составляющие (1,5), (5,1), (5,5) и (1,1), а также соответствующие им матрицы трансформант преобразования Уолша-Адамара (с точностью до коэффициента $1/N$)

$$T_5^+ = \begin{bmatrix} 1111\ 1\ \ 1\ \ 1\ \ 1 \\ 1111\ 1\ \ 1\ \ 1\ \ 1 \\ 1111\ 1\ \ 1\ \ 1\ \ 1 \\ 1111\ 1\ \ 1\ \ 1\ \ 1 \\ 1111{-}1{-}1{-}1{-}1 \\ 1111{-}1{-}1{-}1{-}1 \\ 1111{-}1{-}1{-}1{-}1 \\ 1111{-}1{-}1{-}1{-}1 \end{bmatrix}, W_5^+ = \begin{bmatrix} 32000\ 32\ 000 \\ 0\ 000\ \ 0\ \ 000 \\ 0\ 000\ \ 0\ \ 000 \\ 0\ 000\ \ 0\ \ 000 \\ 32000{-}32000 \\ 0\ 000\ \ 0\ \ 000 \\ 0\ 000\ \ 0\ \ 000 \\ 0\ 000\ \ 0\ \ 000 \end{bmatrix};$$

$$T_6^+ = \begin{bmatrix} 1\ \ 1\ \ 1\ \ 1\ 1111 \\ 1\ \ 1\ \ 1\ \ 1\ 1111 \\ 1\ \ 1\ \ 1\ \ 1\ 1111 \\ 1\ \ 1\ \ 1\ \ 1\ 1111 \\ {-}1{-}1{-}1{-}11111 \\ {-}1{-}1{-}1{-}11111 \\ {-}1{-}1{-}1{-}11111 \\ {-}1{-}1{-}1{-}11111 \end{bmatrix}, W_6^+ = \begin{bmatrix} 32000{-}32000 \\ 0\ 000\ \ 0\ \ 000 \\ 0\ 000\ \ 0\ \ 000 \\ 0\ 000\ \ 0\ \ 000 \\ 32000\ 32\ 000 \\ 0\ 000\ \ 0\ \ 000 \\ 0\ 000\ \ 0\ \ 000 \\ 0\ 000\ \ 0\ \ 000 \end{bmatrix}; \quad (12)$$

$$T_7^+ = \begin{bmatrix} 1111{-}1{-}1{-}1{-}1 \\ 1111{-}1{-}1{-}1{-}1 \\ 1111{-}1{-}1{-}1{-}1 \\ 1111{-}1{-}1{-}1{-}1 \\ 1111\ 1\ \ 1\ \ 1\ \ 1 \\ 1111\ 1\ \ 1\ \ 1\ \ 1 \\ 1111\ 1\ \ 1\ \ 1\ \ 1 \\ 1111\ 1\ \ 1\ \ 1\ \ 1 \end{bmatrix} W_7^+ = \begin{bmatrix} 32\ 00032000 \\ 0\ \ 000\ 0\ 000 \\ 0\ \ 000\ 0\ 000 \\ 0\ \ 000\ 0\ 000 \\ {-}3200032000 \\ 0\ \ 000\ 0\ 000 \\ 0\ \ 000\ 0\ 000 \\ 0\ \ 000\ 0\ 000 \end{bmatrix};$$

$$T_8^+ = \begin{bmatrix} {-}1{-}1{-}1{-}11111 \\ {-}1{-}1{-}1{-}11111 \\ {-}1{-}1{-}1{-}11111 \\ {-}1{-}1{-}1{-}11111 \\ 1\ \ 1\ \ 1\ \ 1\ 1111 \\ 1\ \ 1\ \ 1\ \ 1\ 1111 \\ 1\ \ 1\ \ 1\ \ 1\ 1111 \\ 1\ \ 1\ \ 1\ \ 1\ 1111 \end{bmatrix} W_8^+ = \begin{bmatrix} 32\ 000{-}32000 \\ 0\ \ 000\ \ 0\ \ 000 \\ 0\ \ 000\ \ 0\ \ 000 \\ 0\ \ 000\ \ 0\ \ 000 \\ {-}32000{-}32000 \\ 0\ \ 000\ \ 0\ \ 000 \\ 0\ \ 000\ \ 0\ \ 000 \\ 0\ \ 000\ \ 0\ \ 000 \end{bmatrix}.$$

Внедрение ДИ.

Шаг 1. Производим сегментацию исходного изображения размера $m \times n$ на блоки $\mu \times \mu$.

Шаг 2. Каждому блоку исходного изображения $\mu \times \mu$, задействованному в процессе стеганопреобразования, ставим в соответствие λ бит ДИ, таким образом получаем матрицу ДИ D размера $\frac{m}{\mu} \times \frac{n}{\mu}$, каждый элемент которой содержит λ бит информации. При этом $\lambda = \log_2 J$, где J — количество используемых кодовых слов.

Шаг 3. Строим таблицу соответствия половины комбинаций из λ бит ДИ кодовым словам $\{T_i^+\}$ размера $\mu \times \mu$, в то время как вторая половина комбинаций из λ бит ДИ кодируется с помощью инверсий кодовых слов $\{T_i^-\}$. Получаем закодированную матрицу ДИ путем представления каждого её элемента из λ бит ДИ с помощью кодовых слов $\{T_i^+\}$ и $\{T_i^-\}$.

Шаг 4. Производим внедрение информации путем суммирования матрицы контейнера P с кодовой матрицей, полученной на *Шаге 3*, в результате чего получаем стеганосообщение M.

Декодирование ДИ

Шаг 1. Извлечение информации происходит путем вычитания из матрицы возможно возмущенного стеганосообщения $\overline{M}$ матрицы контейнера P, являющегося частью секретного ключа. В результате извлечения, для каждого i-го блока размера $\mu \times \mu$ получаем матрицу Δ_i.

Шаг 2. Для каждой матрицы T_i^+ производим поэлементное умножение каждой полученной на *Шаге* 1 матрицы Δ_i на матрицу T_i^+, после чего находим сумму всех элементов результирующей матрицы для каждого кодового слова T_i^+, т.е. рассчитываем значения $\sigma_j = \sum_{l=0}^{\mu-1} \sum_{k=0}^{\mu-1} \Delta_i(l,k) T^+(l,k)$, $j = 0,1,...,J/2-1$.

Шаг 3. Среди полученного для каждого блока множества значений σ_j находим максимальное по модулю значение. При этом индекс найденного значения будет соответствовать индексу декодированного кодового слова $T_i^?$, в то время как знак найденного максимума будет соответствовать знаку, с которым заданное кодовое слово было внедрено (прямой или инверсный вид).

Отметим, что *Шаг 2* и *Шаг 3* в представленном методе, по сути, реализуют алгоритм оптимального приема [29].

Замечание. В виду того, что большинство используемых изображений сегодня представлены с использованием модели RGB, где для кодирования каждого цвета отводится 1 байт (каждая цветовая составляющая представляется числами в диапазоне $[0,...,255]$), в случае наличия в блоке граничных для данного диапазона значений (0 или 255), указанный блок не используется в процессе стеганопреобразования в случае применения разработанного в настоящей статье стеганографического метода.

Основываясь на предложенном стеганографическим методе, представим на рис. 2 общую структурную схему стеганографической системы с кодовым управлением частотными составляющими.

Замечание. Предлагаемая стеганосистема является закрытой системой второго типа, использующей контейнер в качестве части секретного ключа, что повышает

устойчивость стеганосистемы к восстановлению секретного ключа, к декодированию скрытой информации, повышает имитостойкость системы по сравнению с использованием ключа, не включающего в свой состав контейнер. При этом сам ключ передается адресатам стандартным образом — по защищенному каналу связи.

Используя представленный стеганографический метод, были проведены следующие эмпирические исследования на основе базы изображений NRCS [30] в формате без потерь TIFF. В каждое изображение производилось внедрении ДИ, по $\lambda = 1$ бит данных на каждый блок с использованием различных кодовых слов, после чего выполнялось его сжатие алгоритмом JPEG с заданным качеством *QF*. Далее выполнялось извлечение ДИ из сжатого изображения. На рис. 3 представлены графики зависимости числа возникающих ошибок (в процентах от общего количества бит ДИ) от степени сжатия изображения *QF* алгоритмом JPEG для каждой из рассмотренных трансформант преобразования Уолша-Адамара, что позволяет оценить эффективность их использования для противостояния атакам сжатием на стеганосообщение. На рис. 3 в каждый блок 8×8 внедрялся $\lambda = 1$ бит ДИ. При этом, в виду того, что все кодовые слова (12), использующие одновременно все частотные составляющие показывают практически эквивалентные результаты, на графике (рис. 3) они показаны одной кривой.

Анализ данных, представленных на рис. 3, показывает, что внедрение информации как с использованием кодовых слов (11), так и кодовых слов (12) формирует стеганосообщение, нечувствительное к атаке сжатием. При этом, при сжатии с коэффициентом *QF* 60% (на практике крайне редко используются бóльшие степени сжатия), процент возникающих ошибок

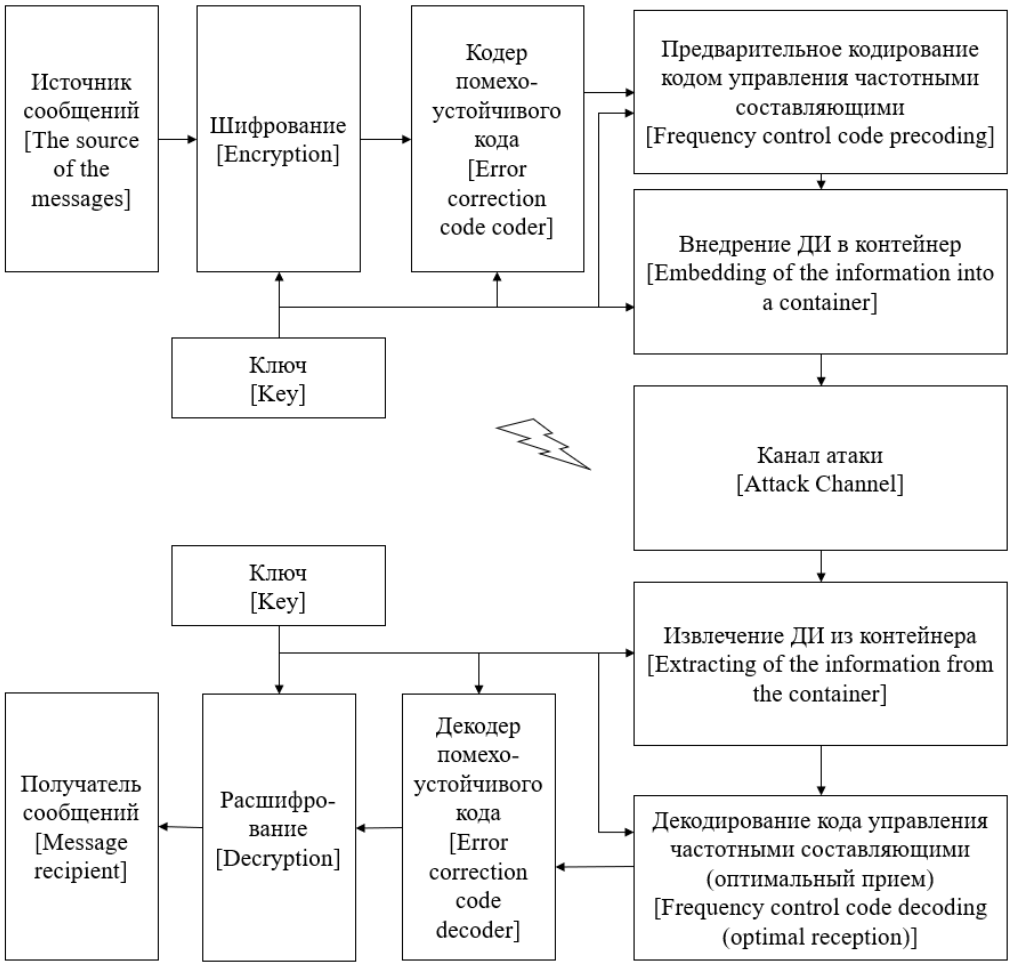


Рис. 2. Структурная схема стеганографической системы с кодовым управлением внедрением информации[2].

[2] Appendix 1

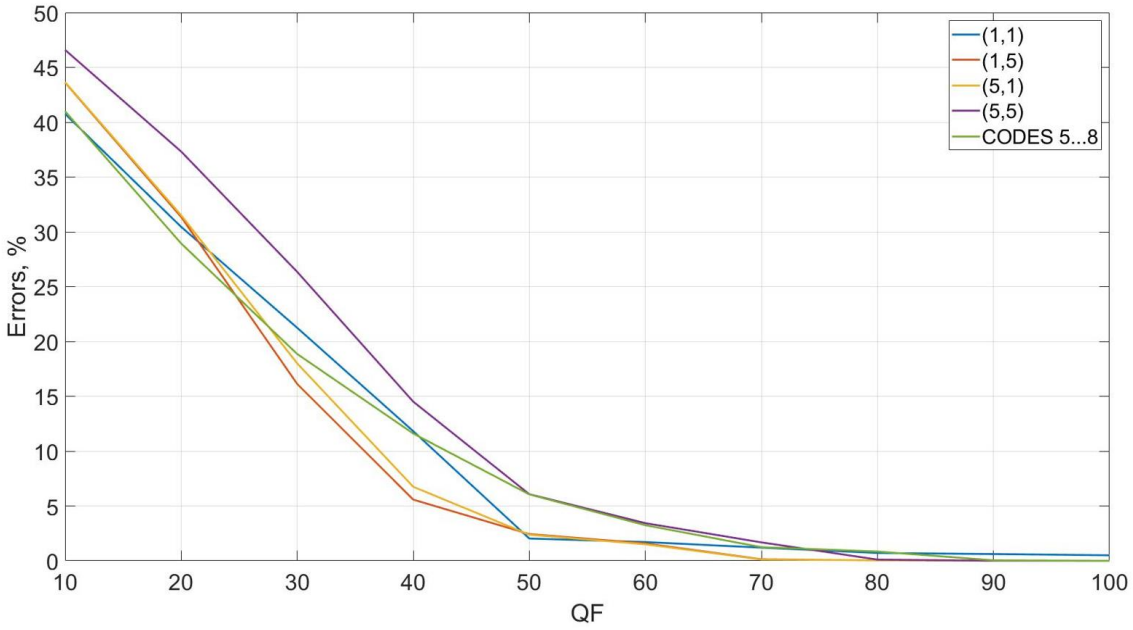


Рис. 3. График зависимости числа возникающих ошибок от степени сжатия стеганосообщения QF алгоритмом JPEG для различных трансформант преобразования Уолша-Адамара, в которые производится внедрение[3].

не превышает 5%, что может быть легко исправлено с помощью применения простейших корректирующих кодов на этапе подготовки внедряемой ДИ.

Физическая сущность устойчивости предлагаемого в работе метода к атакам сжатием заключается в накоплении энергии внедряемого сигнала в заданной частотной составляющей блока, несмотря на то, что амплитуда воздействия на каждый отдельный пиксель является незначительной (± 1).

Такой способ внедрения информации позволяет добиться высоких показателей устойчивости к атаке сжатием при гарантированном сохранении высокого уровня надежности восприятия, сравнимого с уровнем, предоставляемым методом LSB-matching.

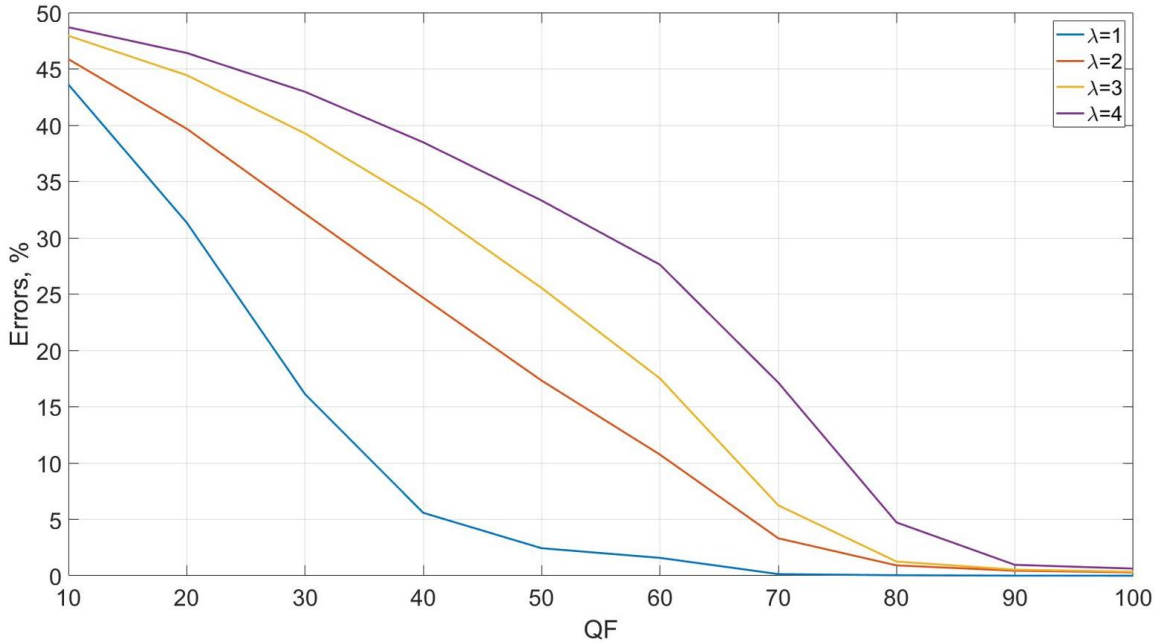


Рис. 4. График зависимости числа возникающих ошибок от степени сжатия стеганосообщения QF алгоритмом JPEG для различных значений λ [4].

[3,4] Appendix 1

Обратной стороной увеличения устойчивости предлагаемого метода является уменьшение его пропускной способности, по сравнению с методом LSB-matching. Тем не менее, поскольку пропускная способность предлагаемого метода определяется параметром λ, для конкретной алгоритмической реализации она может быть повышена за счет увеличения числа λ внедряемых в каждый блок сообщения бит.

На рис. 4 показан график зависимости числа возникших ошибок от степени сжатия изображения *QF* алгоритмом JPEG при различных значениях количества λ внедряемых бит в блок изображения, таким образом, для различных значений пропускной способности λ/μ^2. Отметим, что для значения $\lambda=1$ внедрение производилось с помощью кодового слова (1,5), в то время как при $\lambda=2,3$ задействовались кодовые слова (12), а при $\lambda=4$ использовались все кодовые слова (11) и (12).

Анализ данных, представленных на рис. 4 показывает ожидаемое увеличение количества ошибок, при увеличении пропускной способности, которое обусловлено появлением шумов неортогональности при увеличении количества применяемых кодовых слов. Таким образом, значения $\lambda>1$ могут использоваться в случае необходимости организации стеганографических каналов передачи информации с высокими требованиями к пропускной способности, и невысокими требованиями к качеству передачи информации, либо же в совокупности с корректирующими кодами. Отметим, что помимо увеличения количества бит, внедряемых в один блок контейнера, для повышения пропускной способности может быть уменьшен размер блока μ, в который происходит внедрение кванта информации. Так, при значении $\mu=4$, в соответствии с информацией, представленной на рис. 1, внедрение информации целесообразно проводить в трансформанты преобразования Уолша-Адамара (1,1), (1,3), (3,1) и (3,3). Приведем кодовые слова, позволяющие производить внедрение информации в данные коэффициенты, а также соответствующие им матрицы трансформант преобразования Уолша-Адамара (с точностью до коэффициента $1/N$)

$$T_1^+=\begin{bmatrix}1&1&-1&-1\\1&1&-1&-1\\1&1&-1&-1\\1&1&-1&-1\end{bmatrix},\quad W_1^+=\begin{bmatrix}0&0&16&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix};$$

$$T_2^+=\begin{bmatrix}1&1&1&1\\1&1&1&1\\-1&-1&-1&-1\\-1&-1&-1&-1\end{bmatrix},\ W_2^+=\begin{bmatrix}0&0&0&0\\0&0&0&0\\16&0&0&0\\0&0&0&0\end{bmatrix};$$

$$T_3^+=\begin{bmatrix}1&1&-1&-1\\1&1&-1&-1\\-1&-1&1&1\\-1&-1&1&1\end{bmatrix},\ W_3^+=\begin{bmatrix}0&0&0&0\\0&0&0&0\\0&0&16&0\\0&0&0&0\end{bmatrix};\qquad(13)$$

$$T_4^+=\begin{bmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{bmatrix},\qquad W_4^+=\begin{bmatrix}16&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix}.$$

При этом, также как в случае размера блока $\mu=8$, могут быть найдены кодовые слова, допускающие внедрение информации во все выбранные четыре частотные составляющие одновременно (их трансформанты преобразования Уолша-Адамара приведены с точностью до коэффициента $1/N$)

$$T_5^+=\begin{bmatrix}1&1&1&1\\1&1&1&1\\1&1&-1&-1\\1&1&-1&-1\end{bmatrix},\quad W_5^+=\begin{bmatrix}8&0&8&0\\0&0&0&0\\8&0&-8&0\\0&0&0&0\end{bmatrix};$$

$$T_6^+=\begin{bmatrix}1&1&-1&-1\\1&1&-1&-1\\1&1&1&1\\1&1&1&1\end{bmatrix},\quad W_6^+=\begin{bmatrix}8&0&8&0\\0&0&0&0\\-8&0&8&0\\0&0&0&0\end{bmatrix};$$

$$T_7^+=\begin{bmatrix}1&1&1&1\\1&1&1&1\\-1&-1&1&1\\-1&-1&1&1\end{bmatrix},\quad W_7^+=\begin{bmatrix}8&0&-8&0\\0&0&0&0\\8&0&8&0\\0&0&0&0\end{bmatrix};\qquad(14)$$

$$T_8^+=\begin{bmatrix}-1&-1&1&1\\-1&-1&1&1\\1&1&1&1\\1&1&1&1\end{bmatrix},\quad W_8^+=\begin{bmatrix}8&0&-8&0\\0&0&0&0\\-8&0&-8&0\\0&0&0&0\end{bmatrix}.$$

На рис. 5 представлены графики зависимости количества ошибок при извлечении информации при её кодировании каждым из представленных кодовых слов (13) и (14). При этом кодовые слова (14) соответствуют одной кривой на графике рис. 5 в виду их сходных результатов.

Анализ данных рис. 5 показывает, что при пропускной способности 1/16 при использовании кодового слова T_4^+, $\mu=4$, устойчивость стеганографического канала к сжатию алгоритмом JPEG даже превосходит устойчивость стеганографического канала при использовании всех кодовых слов (11) и

(12) для достижения значений $\lambda = 4$, $\mu = 8$. Таким образом, для достижения высокого значения пропускной способности равного $1/16$, использование кодового слова T_4^+ и значения $\mu = 4$ является более целесообразным, нежели использование значения размера блока $\mu = 8$. Тем не менее, при $\mu = 4$ использование кодовых слов T_1^+, T_2^+ и $T_5^+, T_6^+, T_7^+, T_8^+$ показывает практически сходные результаты со случаем применения разработанного метода с параметрами $\lambda = 4$, $\mu = 8$, в то время как использование кодового слова T_3^+ при $\mu = 4$ показывает худшие результаты.

Результаты сравнительного анализа эффективности алгоритмической реализации разработанного метода с современными аналогами представлены в табл. 1. В табл. 1 приняты следующие условные обозначения: S — внедрение информации происходит в пространственной области, DCT — внедрение информации происходит в области трансформант ДКП блоков изображения, SVD — внедрение информации происходит в области сингулярного разложения блоков изображения.

Анализ данных, представленных в табл. 1 позволяет сделать вывод о том, что разработанный стеганографический метод при сохранении высокой надежности восприятия стеганосообщения позволяет получить значительную устойчивость к атакам сжатием. Так, при практически ценных значениях коэффициента $QF \geq 60$ количество ошибок при декодировании у разработанного метода ниже, чем у современных аналогов.

Неоспоримым достоинством разработанного стеганографического метода в сравнении с аналогами также является то, что внедрение и декодирование информации происходит здесь в пространственной области изображения, вследствие чего отсутствуют дополнительные вычислительные затраты для перехода в область преобразования и обратно.

На рис. 6 представлен пример внедрения ДИ в контейнер с помощью разработанного в настоящей статье стеганографического метода, при этом использованы параметры $\lambda = 1$, $\mu = 8$, а также для внедрения информации применено кодовое слово T_2^+. Размер контейнера составляет 2592x3872, при этом внедрение информации происходило в каждую цветовую составляющую. Таким образом, общий объем внедренной информации для данного контейнера составил 470 448 бит.

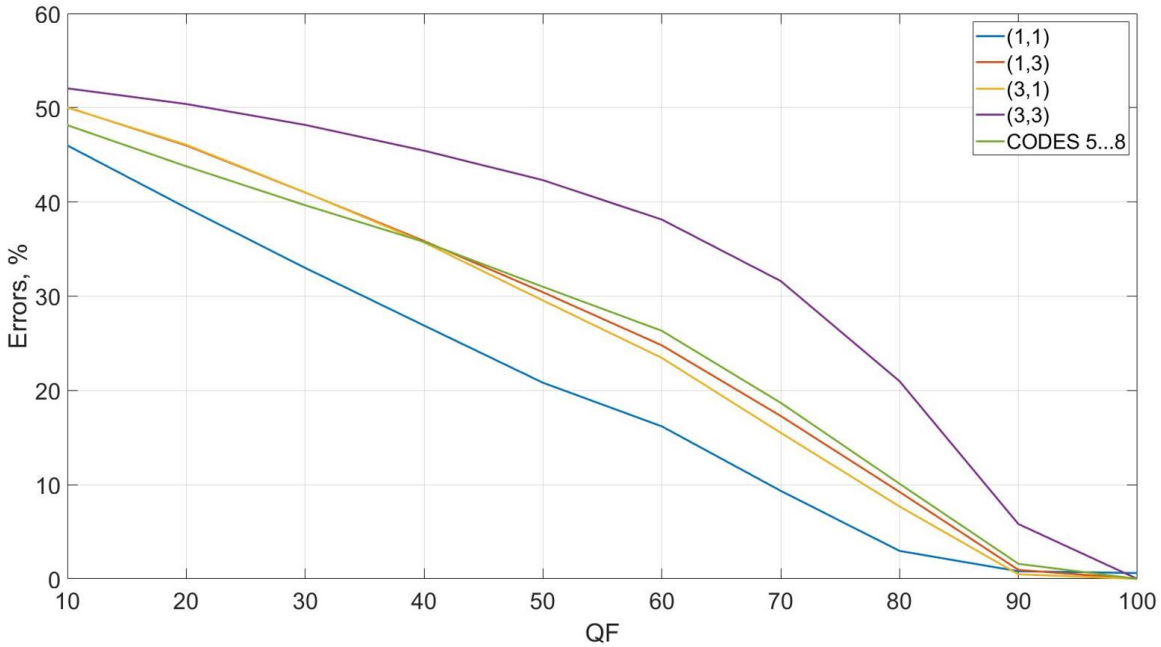


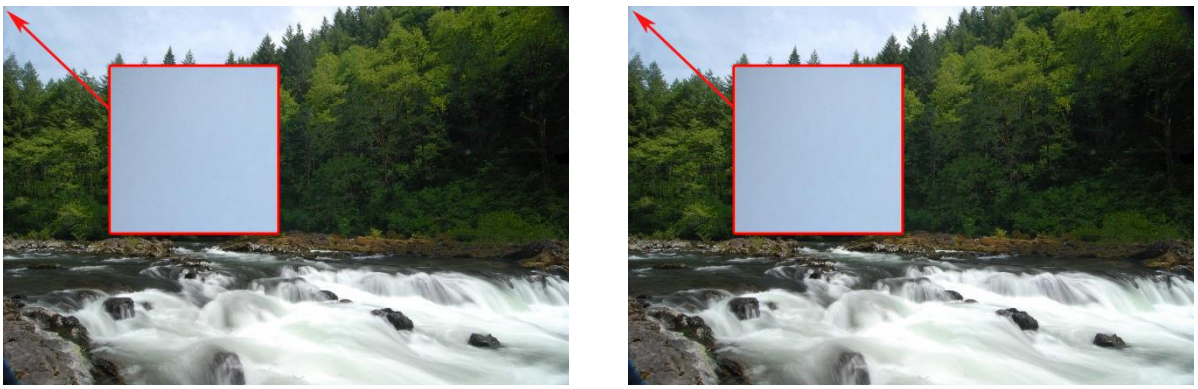
Рис. 5. График зависимости числа возникающих ошибок от степени сжатия изображения *QF* алгоритмом JPEG для $\mu = 4$ [5].

[5] Appendix 1

Таблица 1[6].
Table 1[6].

Результаты сравнительного анализа предложенного стеганографического метода с современными аналогами
Results of comparative analysis of the proposed steganographic method vs modern analogues

Алгоритм / Метод [Algorithm / Method]	% ошибок при заданном уровне QF [% of errors for a given value of QF]										PSNR, dB	R	Обл. вн. [Emb. domain]
	10	20	30	40	50	60	70	80	90	100			
Предложенный метод [Proposed method], $\mu=4, \lambda=1, T_4^+$	45.9923	39.3865	33.0043	26.8885	20.8169	16.1856	9.3461	2.9669	0.8089	0.6163	48.1308	1/16	S
Предложенный метод [Proposed method], $\mu=8$, $\lambda=1, T_1^+$	43.6133	31.3537	16.1266	5.5792	2.4352	1.5825	0.1392	0.0395	0.0055	0	48.1308	1/64	S
Алгоритм [Algorithm] [11]	—	—	—	—	—	—	33.85(QF=75)	7.39(QF=85)	0.34(QF=95)	—	~45	<1/8	DCT
Алгоритм [Algorithm] [15]	13	7	5	4	2	2	2	2	2	—	~34.7	1/64	SVD
Алгоритм [Algorithm] [16]	—	—	—	—	24.74	14.24	2.71	0.2	0.05	—	~32.66	1/64	SVD
Алгоритм [17]	—	—	—	—	23.88	14.12	2.76	0.08	0.08	—	~32.67	1/16	SVD



а) б)

Рис. 6. Пример использования разработанного стеганографического метода: а) контейнер, б) стеганосообщение[7].

Субъективное ранжирование изображений, представленных на рис. 6 не позволяет обнаружить артефакты, или какие-либо другие отличия стеганосообщения от исходного контейнера. Данный факт является ожидаемым, поскольку результатом стеганопреобразования является возмущение значений яркости пикселей контейнера на ± 1.

Количественная оценка искажения ЦИ-контейнера за счет внедрения ДИ

[6,7] Appendix 1

разработанным методом, проводимая с использование разностного показателя

$$PSNR = 20\lg\left(\frac{255}{\sqrt{MSE}}\right), \quad (15)$$

где

$$MSE = \frac{1}{nm}\sum_i\sum_j \left|X(i,j) - M(i,j)\right|^2, \quad (16)$$

не зависит от величины пропускной способности канала скрытой связи, размера ЦИ. Действительно

$$MSE = \frac{1}{nm}\sum_i\sum_j \left|X(i,j) - M(i,j)\right|^2 = \\ = \frac{1}{nm}\sum_i\sum_j 1^2 = 1, \quad (17)$$

тогда

$$PSNR = 20\lg(255) = 48.1308\ dB, \quad (18)$$

что говорит о практически достоверном факте обеспечения надежности восприятия стеганосообщения для произвольного ЦИ-контейнера.

Разработанный метод позволил повысить эффективность стеганографической системы: PSNR разработанного метода на $3.1308\,\text{dB}$ выше чем у метода [11], и более чем на $15.4708\,\text{dB}$ больше, чем у метода [16]. При этом, при значении коэффициента качества $QF = 70$ (что соответствует минимальным уровням качества, применяемым в большинстве современных систем передачи и обработки информации), разработанный метод обеспечивает на 33.7% меньшее количество ошибок при извлечении ДИ чем метод [11], и на 2.57% меньшее количество ошибок, чем метод [16].

Замечание 1. Вычислительная сложность алгоритмической реализации разработанного метода определяется количеством блоков, используемых в процессе стеганопреобразования, и в наихудшем случае составит $\underline{O}(nm)$ операций. С учетом блоковости метода очевидным является его внутренний параллелизм, что в совокупности с использованием пространственной области для стеганопреобразования обеспечивает потенциальную возможность его использования в режиме реального времени для потокового контейнера.

Замечание 2. Теоретические основы разработанного метода очевидно обеспечивают его устойчивость не только к атаке сжатием, рассмотренной авторами подробно, но и к любой другой атаке против встроенного сообщения, не меняющей геометрию ЦИ.

ВЫВОДЫ

Отметим основные результаты проведенных исследований:

1. Сформирован теоретический базис кодового управления внедрением информации, сущность которого заключается в предварительном кодировании ДИ с помощью кодовых слов с заданными свойствами трансформант преобразования Уолша-Адамара, внедрение которых приводит к строго определенному воздействию на трансформанты преобразования Уолша-Адамара, а, соответственно, и на трансформанты ДКП контейнера. Таким образом, манипулируя свойствами применяемых кодов становится возможным влиять на свойства стеганосообщения, например, на его способность противостоять атаке сжатием.

2. На основе сформулированного теоретического базиса разработан стеганографический метод, для которого построены множества кодовых слов практически ценных порядков $N = 4$ и $N = 8$, обеспечивающих наилучшую устойчивость стеганосообщения к атаке сжатием.

3. Экспериментальные исследования, а также проведенный сравнительный анализ алгоритмических реализаций разработанного стеганографического метода с современными аналогами показал, что он способен обеспечить надежность восприятия стеганосообщения (показатель PSNR является постоянным и равен 48.1308 дБ, что превосходит значения PSNR всех рассмотренных в работе современных аналогов), а также низкую вероятность ошибок при извлечении ДИ, которая при уровнях качества $QF \geq 60$ ниже, чем у рассмотренных аналогов. При этом, в отличие от рассмотренных аналогов, разработанный метод осуществляет внедрение ДИ в пространственной области, что определяет простоту его

алгоритмической реализации и высокое быстродействие, следствием чего является потенциальная возможность его использования в режиме реального времени для потокового контейнера.

APPENDIX 1 (ПРИЛОЖЕНИЕ 1)

[1]**Fig. 1.** The relationship between the Walsh-Hadamard and DCT transformants for $l \times l$-blocks of the Digital Image: a — $l = 4$; b — $l = 8$; c — $l = 16$.

[2]**Fig. 2.** Block diagram of a steganographic system with code-controlled information embedding

[3]**Fig. 3.** A graph of the dependence of the number of errors on the degree of steganographic message compression QF by the JPEG algorithm for various Walsh-Hadamard transformants, into which the embedding is performed.

[4]**Fig. 4.** A graph of the dependence of the number of errors on the degree of compression QF of the steganographic message by the JPEG algorithm for various values of λ.

[5]**Fig. 5.** A graph of the dependence of the number of errors on the degree of steganographic message compression QF by the JPEG algorithm for $\mu = 4$.

[6]**Table 1.** Results of a comparative analysis of the proposed steganographic method with modern analogues.

[7]**Fig. 6.** An example of using the developed steganographic method: a) container, b) steganographic message.

Литература (References)

[1] Shin F. Y. Digital Watermarking and Steganography: Fundamentals and Techniques. CRC Press, 2017. 292 p. doi: 10.1201/9781315219783-4

[2] Provos N., Honeyman P. Hide and seek: an introduction to steganography. IEEE security & privacy, 2003. Vol. 1. No. 3. pp. 32-44.

[3] Morkel T., Eloff J. H. P., Olivier M. S. An overview of image steganography. ISSA. 2005. Vol. 1, No. 2. pp. 322-330.

[4] Cheddad A., Condell J., Curran K., Mc.Kevitt P. Digital image steganography: Survey and analysis of current methods. Signal processing. 2010. Vol. 90, No. 3. pp. 727-752. doi: 10.1016/j.sigpro.2009.08.010

[5] Johnson N. F., Duric Z., Jajodia S. Information hiding: Steganography and watermarking – attacks and countermeasures. Kluwer Academic Publishers, 2000. 137 p. doi: 10.1007/978-1-4615-4375-6

[6] Kostyrka O.V. Analiz preimushhestv prostranstvennoj oblasti cifrovogo izobrazhenija-kontejnera dlja steganopreobrazovanija [Analysis on the benefits of spatial domain of cover image for steganography transformation]. Informatika ta matematichni metodi v modeljuvanni [Informatics and Mathematical Methods in Simulation]. №3. pp. 275-282. (In Russian)

[7] Jianhua Yang et al. Spatial Image Steganography Based on Generative Adversarial Network. Spatial Image Steganography Based on Generative Adversarial Network. arXiv:1804.07939v1. pp. 1-7.

[8] Hussain M. et al. Image steganography in spatial domain: A survey. Signal Processing: Image Communication, 2018. Vol. 65. pp. 46-66. doi: 10.1016/j.image.2018.03.012

[9] Samidha D., Agrawal D. Random image steganography in spatial domain. International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System, 2013. pp. 1-3. doi: 10.1109/icevent.2013.6496564

[10] Hu D. et al. A spatial image steganography method based on nonnegative matrix factorization. IEEE signal processing letters, 2018. Vol. 25, No. 9. pp. 1364-1368. doi: 10.1109/lsp.2018.2856630

[11] Zhu Z., Zheng N., Qiao T., Xu M. Robust Steganography by Modifying Sign of DCT Coefficients. IEEE Access, 2019. Vol. 7. pp. 168613-168628. doi: 10.1109/access.2019.2953504

[12] Bansal D., Chhikara R. An improved DCT based steganography technique. International Journal of Computer Applications. Vol. 102, No.14. pp. 46-49. doi: 10.5120/17887-8861

[13] Walia E., Jain P., Navdeep N. An analysis of LSB & DCT based steganography. Global Journal of Computer Science and Technology. 2010. 2010. Vol. 10, Issue 1. pp. 4-8.

[14] Rachmawanto E. H. et al. Secure image steganography algorithm based on dct with otp encryption. Journal of Applied Intelligent System, 2017. Vol. 2, No. 1. pp. 1-11. doi: 10.33633/jais.v2i1.1330

[15] Mel'nik M.A. Steganoalgoritm, ustojchivyj k szhatiju [Compression-resistant steganographic algorithm]. Informacijna bezpeka [Information security]. 2012. №2(8). pp. 99-106. (In Russian)

[16] Chang C.C., Lin C.C., Hu Y.S. An SVD oriented watermark embedding scheme with high qualities for the restored images. International journal of innovative computing, information & control, 2007.Vol. 3, No. 3. pp. 609-620.

[17] Chanu Y. J., Singh Kh. M., Tuithung T. A Robust Steganographic Method based on Singular Value Decomposition. International Journal of

Information & Computation Technology, 2014. Vol. 4, No. 7. pp. 717-726.
[18] Abdallah H. A., Hadhoud M. M., Shaalan A. A. An efficient SVD image steganographic approach. International Conference on Computer Engineering & Systems, 2009. pp. 257-262. doi: 10.1109/icces.2009.5383271
[19] Bhattacharyya S., Mondal S., Sanyal G. A Robust Image Steganography using Hadamard Transform. International Conference on Information Technology in Signal and Image Processing, Mumbai, 2013. pp. 416-426.
[20] Sheidaeian H., Zolfaghari B., Zobeiri M. An Efficient and Secure Approach to Multi-User Image Steganography Using CRC-Based CDMA. International Conference on Signal Acquisition and Processing. Singapore, 2011. Vol. 2. pp. 1-5.
[21] Amirtharajan R., Rayappan J. B. B. Covered CDMA multi-user writing on spatially divided image. International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011. pp. 1-5. doi: wirelessvitae.2011.5940912
[22] Sneha P. S., Sankar S., Kumar A. S. A chaotic colour image encryption scheme combining Walsh–Hadamard transform and Arnold–Tent maps. Journal of Ambient Intelligence and Humanized Computing, 2020. Vol. 11, No. 3. pp. 1289-1308. doi: 10.1007/s12652-019-01385-0
[23] Kobozeva A. A., Horoshko V. A. Analiz informacionnoj bezopasnosti [Information security analysis]. Kiev: Izd. GUIKT, 2009. 251 p. (In Russian)
[24] Evsutin O., Melman A., Meshcheryakov R. Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions. IEEE Access, 2020. No. 8. P. 166589-166611. doi: 10.1109/ACCESS.2020.3022779
[25] Lu Leng, Jiashu Zhang, Jing Xu et al. Dynamic weighted discrimination power analysis: A novel approach for face and palmprint recognition in DCT domain. International Journal of Physical Sciences. 2010. No. 5(17). pp.467-471.
[26] Logachev O. A., Sal'nikov A. A., Jashhenko V. V. Bulevy funkcii v teorii kodirovanija i kriptologii [Boolean functions in coding theory and cryptology]. M.: MCNMO, 2004. 472 p. (In Russian)
[27] Merzljakova E. Ju. Postroenie steganograficheskih sistem dlja rastrovyh izobrazhenij, bazirujushhihsja na teoretiko-informacionnyh principah: avtoreferat dissertacii na soiskanie uchenoj stepeni kandidata tehnicheskih nauk, special'nost' 05.13.19 – Metody i sistemy zashhity informacii. Informacionnaja bezopasnost'. [Construction of steganographic systems for raster images based on information theoretic principles: abstract of the thesis for the degree of candidate of technical sciences, specialty 05.13.19 - Information security methods and systems. Information security.] Sibirskij gosudarstvennyj universitet telekommunikacij i informatiki [Siberian State University of Telecommunications and Informatics]. Novosibirsk, 2011. 16 p. (In Russian)
[28] Mazurkov M. I., Sokolov A. V., Barabanov N. A. Synthesis method for bent sequences in the Vilenkin-Chrestenson basis. Radioelectronics and Communications Systems, 2016. Vol. 59, No. 11. P. 510-517. doi: 10.3103/s0735272716110054
[29] Mazurkov M. I. Sistemy shirokopolosnoj radiosvjazi [Broadband radio systems]. Odessa : Nauka i Tehnika [Odessa: Science and Technology], 2010. 340 p. (In Russian)
[30] NRCS Photo Gallery // United States Department of Agriculture. URL: https://www.nrcs.usda.gov/wps/portal/nrcs/main/national/newsroom/multimedia/

Сведения об авторах.

Кобозева Алла Анатольевна. Национальный университет «Одесская политехника». Кафедра кибербезопасности и программного обеспечения, заведующая кафедрой, доктор технических наук, профессор. Область научных интересов: информационная безопасность, в частности, стеганография, экспертиза целостности информационного контента.
E-mail: alla_kobozeva@ukr.net

Соколов Артем Викторович. Национальный университет «Одесская политехника». Кафедра кибербезопасности и программного обеспечения, доцент, кандидат технических наук. Область научных интересов: методы защиты информации на основе совершенных алгебраических конструкций.
E-mail: radiosquid@gmail.com