Steganoanalytical Method Based on the Analysis of Singular Values of Digital Image Matrix Blocks

Kobozeva A.A.[1], Bobok I.I.[1], Batiene L.E.[2]
[1, 2] Odessa National Polytechnic University
[1] Odessa, Ukraine
[2] Ouagadougou, Burkina Faso

Abstract. The rapid development of digital steganography over the past decade involving numerous scientific publications in the open press, devoted to the new steganomethods and algorithms, have led to the possibility of wide use of the results obtained. At the same time, the organization of a steganographic channel can lead to various kinds and degrees of negative consequences both for individuals and for society as a whole. Because of this, the need and relevance of providing effective digital image steganalysis is currently increasing. One of the most widely used steganographic methods today is the LSB-method. The specific area of its application is in the organization of a hidden low bandwidth communication channel. Under these conditions, the existing steganalitic methods turn out to be ineffective. The aim of this paper is to increase the efficiency of image steganalysis in the conditions of low bandwidth of a covert channel organized by the LSB-method. Achieving this aim is carried out by developing a new method based on the analysis of the normalized separation of the maximum singular numbers of the image matrix blocks. The algorithmic implementation of the developed method is superior in efficiency when compared to the existing modern analogues, in terms of the covert channel for bandwidth values of less than 0.1 bpp. An important information component of the results of the proposed method is its ability to determine the cover-image quality factor of the primary lossy compression.
Keywords: steganalysis, digital image, least significant bit, low bandwidth, covert channel, cover, stego-message.
DOI: 10.5281/zenodo.2222384

O metodă stegano-analitică bazată pe analiza numerelor singulare ale blocurilor de matrice de imagini digitale

[1]Kobozeva A.A., [1]Bobok I.I., [2]Batiyene L.Ye.
[1, 2] Universitatea Politehnică Națională din Odessa
[1]Odessa, Ucraina, [2]Ouagadougou, Burkina Faso

Rezumat: Dezvoltarea rapidă a steganografiei digitale în ultimul deceniu, numeroase publicații științifice în presa deschisă, dedicate dezvoltării unor noi steganometode și algoritmi, au condus la posibilitatea utilizării pe scară largă a rezultatelor obținute. Relevanța furnizării de steganananaliză eficientă, a cărei sarcină principală este de a stabili prezența / absența informațiilor suplimentare în conținutul informațional, care este considerată o imagine digital se prezintă actuală. Una dintre cele mai utilizate metode steganografice se consideră metoda de modificare a celui mai nesemnificativ bit (metoda LSB). Deoarece există mulți algoritmi cvasi-analitice de a estima specificul utilizării canalului de comunicare ascuns, care constă în capacitatea redisă a lui de transmisie a informației se constată că metodele stegano-analitice existente se dovedesc a fi ineficiente sau de neconceput. Scopul lucrării constă în sporirea eficienței steganoanalizei imaginii în condiții de lățime redusă a bandei canalului de comunicare ascuns organizat de metoda LSB. Realizarea obiectivului se face prin dezvoltarea unei noi metode stegano-analitice pe baza analizei separării normalizate a numerelor maxime singulare ale blocurilor de matrice de imagini. Realizarea algoritmică a metodei depășește omologii moderni existenți în ceea ce privește lățimea bandei canalului de comunicare ascuns, mai mică de 0,1 biți / pixel. O componentă semnificativă a rezultatelor obținute constă în asigurarea posibilității determinării coeficientului calității comprimării primare cu pierderi a imaginii container. Metodele analogice moderne nu rezolvă această problemă, deși informația accesată din sursele disponibile poate fi utilă pentru determinarea / estimarea lățimii benzii canalului de comunicare ascuns.
Cuvinte-cheie: steganoanaliză, imagine, metodă de modificare a biților cel mai puțin semnificativ, lățime de bandă redusă a canalului de comunicare ascuns, container, mesaj stegano.

Стеганоаналитический метод, основанный на анализе сингулярных чисел блоков матрицы цифрового изображения

Кобозева А.А.[1], Бобок И.И.[1], Батиене Л.Е.[2]
[1, 2] Одесский национальный политехнический университет
[1] Одесса, Украина
[2] Уагадугу, Буркина-Фасо

Аннотация. Бурное развитие цифровой стеганографии за последнее десятилетие, многочисленные научные публикации в открытой печати, посвященные разработке новых стеганометодов и алгоритмов, привели к возможности широкого использования полученных результатов. При этом организация скрытого (стеганографического) канала связи может приводить к различного рода и степени негативным последствиям как для отдельно взятых личностей, так и для общества в целом при использовании такого канала с антигосударственными, противоправными, антигуманными целями. В силу этого в настоящий момент возрастает актуальность обеспечения эффективного стеганоанализа, основной задачей которого является установление факта наличия/отсутствия дополнительной информации в информационном контенте, в качестве которого в работе рассматривается цифровое изображение. Одним из наиболее широко используемых стеганографических методов остается сегодня метод модификации наименьшего значащего бита (LSB-метод). С учетом существования большого числа стеганоаналитических алгоритмов для его выявления спецификой его сегодняшнего использования является малая пропускная способность организуемого скрытого канала связи, в условиях которой существующие стеганоаналитические методы оказываются малоэффективными или вообще несостоятельными. Целью работы является повышение эффективности стеганоанализа изображений в условиях малой пропускной способности скрытого канала связи, организованного LSB-методом. Достижение цели осуществляется путем разработки нового стеганоаналитического метода, основанного на анализе нормированной отделенности максимальных сингулярных чисел блоков матрицы изображения. Алгоритмическая реализация разработанного метода превосходит по эффективности существующие современные аналоги в условиях пропускной способности скрытого канала связи, меньше 0.1 бит/пиксель. Важной информационной составляющей результатов работы предложенного метода является обеспечение им возможности определения коэффициента качества первичного сжатия с потерями изображения-контейнера. Такую задачу не решает в настоящий момент ни один из современных методов-аналогов, информация о которых доступна из открытых источников, хотя упомянутая информация может быть полезной для определения/оценки величины пропускной способности скрытого канала связи.

Ключевые слова: стеганоанализ, изображение, метод модификации наименьшего значащего бита, малая пропускная способность скрытого канала связи, контейнер, стеганосообщение.

ВВЕДЕНИЕ

Стремительное развитие цифровой стеганографии [1,2], происходящее в последние два десятилетия, привело к повышению актуальности обеспечения эффективного стеганоанализа [3], основной задачей которого является выявление в цифровом информационном контенте наличия некоторой дополнительной (скрытой) информации, существование которой не оглашается явно. Организация такого рода скрытых каналов коммуникации в каналах связи общего пользования могут приводить к различного рода и степени негативным последствиям как для отдельно взятых личностей, так и для общества в целом, если используются с антигосударственными, противоправными, антигуманными целями.

При организации скрытого (стеганографического) канала связи в настоящий момент в качестве контейнеров широко используются цифровые изображения (ЦИ) (рассматриваемые далее в настоящей работе), цифровые видео, аудио. Формирование стеганографической системы часто происходит при помощи метода модификации наименьшего значащего бита (LSB-метода) [1], распространенность которого привела к наличию большого количества стеганоаналитических разработок для его выявления [2, 4-6]. Наибольшее распространение получили на сегодняшний день статистические стеганоаналитические методы [7-9], основанные на оценке различий статистических параметров контейнера и стеганосообщения (СС), обладающие, тем не менее, очень существенными недостатками: во-первых, у стеганоаналитика, как правило, отсутствует оригинальный контейнер для сравнения, а сами статистические характеристики разных изображений могут отличаться очень сильно и зависят от специфики самого контейнера, во-вторых, при использовании LSB-метода в условиях малой пропускной способности организуемого при его помощи скрытого канала связи (или скрытой пропускной способности (СПС)) [1] различия в статистиках контейнера и стеганосообщения становятся практически нераспознаваемыми.

С учетом этого характерной особенностью сегодняшнего применения LSB-метода является его использование с малой СПС (не более 0.1 бит/пиксель). В таких условиях подавляющее большинство существующих стеганоаналитических методов оказываются несостоятельными, поскольку они, как правило, ориентированы на СПС более 0.1 бит/пиксель и в условиях меньшей СПС даже не тестируются [4,6]. И хотя разработки в этом направлении ведутся [5,10-12], задача выявления скрытого канала связи с малой пропускной способностью в условиях отсутствия у стеганоаналитика исходного незаполненного контейнера не является окончательно решенной, оставаясь актуальной.

Одним из наиболее эффективных существующих статистических стеганоаналитических подходов для выявления LSB-вложений является подход, использующий анализ «цветовых пар», нашедший свое отражение в методах, разработанных в [13,14], основанный на поиске закономерностей в вероятностях появления конкретных значений яркости в незаполненных контейнерах и стеганосообщениях с учетом, что при использовании метода LSB значения яркости цветовой составляющей ЦИ в результате стеганопреобразования возмущаются не более, чем на единицу. Предложенные разработки позиционируются авторами как эффективные, что подтверждается приведенными результатами вычислительных экспериментов, однако их тестирование осуществлялось лишь в условиях СПС>0.2 бит/пиксель, что подтверждает вышесказанное.

Подход, основанный на анализе статистики различных цветов ЦИ, нашел свое дальнейшее развитие в [5]. И хотя здесь сделан «шаг вперед» по сравнению с другими стеганоаналитическими разработками, основанными на той же идее анализа цветов, а именно, работоспособность разработанного метода обеспечена в условиях СПС=0.05 бит/пиксель, принцип, положенный в основу метода (анализ статистических отличий контейнера и стеганосообщения) не дает принципиальной возможности обеспечения его эффективности для значительно меньшей СПС.

Статистический стеганоанализ, основанный на анализе гистограмм результатов квантования значений коэффициентов дискретного косинусного преобразования матрицы ЦИ, представлен в [15-17]. Соответствующие разработки расчитаны на СПС>0.5 бит/пиксель и являются неэффективными в случае меньшей СПС. Такой результат является естественным следствием использованного математического аппарата. Отделение контейнера от стеганосообщения здесь делается в соответствии с устанавливаемым характером гладкости огибающей соответствующей гистограммы. Однако отличие в анализируемой гладкости упомянутых кривых для гистограмм контейнера и стеганосообщения при малой СПС становится практически недектируемым.

Один из наиболее многочисленных классов статистических методов – это методы классификации с обучением [18,19], которые предполагают формирование характеристических векторов анализируемых контентов, выбор и обучение классификатора.

В [18] предлагается стеганоаналитический метод, использующий характеристический вектор, учитывающий особенности гистограмм, построенных для коэффициентов дискретного косинусного преобразования анализируемого ЦИ. Разработанный метод обеспечивает возможность эффективного отделения контейнера от стеганосообщения лишь в условиях СПС>0.1 бит/пиксель. Аналогичным недостатком обладает и метод, предложенный в [19].

Все большее распространение приобретает на сегодняшний день обучение при помощи нейронных сетей [20-22], однако и здесь наблюдается невысокая эффективность при выявлении стеганосообщений, сформированных при малой СПС.

Таким образом, задача выявления результатов внедрения дополнительной информации в цифровые информационные контенты, в частности ЦИ, с малой СПС остается актуальной.

Очевидным здесь является следующий вывод: при выявлении стеганосообщения, сформированного в условиях малой СПС, когда возмущение контейнера в результате стеганопреобразования является незначительным, нецелесообразным является поиск отличий в статистиках контейнера и стеганосообщения: при СПС<0.05 бит/пиксель такие отличия практически не выявляемы. Для решения задачи стеганоанализа ЦИ в условиях малой СПС необходимо искать принципиально новые подходы, использовать новые математичские инструменты. Необходимо уйти от сравнения статистик матриц, исполь-

зовать характеристики контейнера и стеганосообщения, которые не определяются напрямую наличием/отсутствием дополнительной информации в анализируемом ЦИ.

Целью работы является повышение эффективности стеганоанализа ЦИ в условиях отсутствия контейнера в распоряжении стеганоаналитика и малой пропускной способности скрытого канала связи, организованного LSB-методом, путем разработки нового стеганоаналитического метода.

Под малой пропускной способностью скрытого канала связи в работе понимается СПС<=0.1 бит/пиксель.

I. МЕТОДЫ ИССЛЕДОВАНИЯ

Поскольку основной объем цифровой информации сегодня пересылается и хранится с потерями, то в качестве контейнера в настоящей работе используются ЦИ в формате с потерями. Не ограничивая общности рассуждений, в качестве такого формата рассматривается Jpeg с различными коэффициентами качества *QF*, значение которых выбирается в общем случае из множества $\{0,1,2,\ldots,100\}$. После стеганопреобразования контейнера, осуществляемого при помощи метода модификации наименьшего значащего бита, ЦИ-стеганосообщение, с учетом неустойчивости LSB-метода к атакам против встроенного сообщения, одной из которых является атака сжатием с потерями, сохраняется в формате без потерь (для определенности – Tif). Таким образом, при организации скрытого канала связи при помощи LSB-метода с использованием ЦИ с потерями форматы контейнера и стеганосообщения будут отличаться друг от друга наличием/отсутствием потерь, при этом беспотерийный формат стеганосообщения не является для соответствующего изображения оригинальным. Ключевым моментом такой ситуации является то, что она будет иметь место независимо от величины пропускной способности организуемого скрытого канала связи. Установление упомянутого факта, указывающего на нарушение целостности изображения, целесообразно использовать для выявления стеганосообщения.

При решении задач, связанных с выявлением нарушений целостности цифровых информационных контентов хорошо зарекомендовал себя подход, предложенный в [23], основанный на анализе полного набора формальных параметров ЦИ, состоящего из совокупности сингулярных чисел (СНЧ) и сингулярных векторов блоков матрицы изображения, полученных путем ее стандартного разбиения. В [24,25] были проведены дополнительные исследования свойств максимальных СНЧ 4×4-блоков ЦИ в форматах с потерями и без потерь, на основании которых в [26] был разработан метод отделения оригинального ЦИ в формате без потерь от ЦИ, пересохраненного без потерь из формата с потерями, и предложены две его алгоритмические реализации. Этот метод взят за основу при разработке нового стеганоаналитического метода в настоящей работе.

Не ограничивая общности рассуждения, в качестве формального представления ЦИ рассматривается одна $n\times m-$матрица F. Пусть матрица F ЦИ разбивается стандартным образом на непересекающиеся $4\times4-$блоки, B — 4×4-матрица блока,

$$\sigma_1(B)\geq\sigma_2(B)\geq\sigma_3(B)\geq\sigma_4(B)\geq0$$

— СНЧ B. Основным объектом исследования настоящей работы является нормированная отделеность максимального СНЧ (НОМСЧ) $\sigma_1(B)$ блока ЦИ $svdgap_n(1,B)$, окончательная формула для вычисления которой имеет следующий вид [24]:

$$svdgap_n(1,B)=(\sigma_1(B)-\sigma_2(B))/\|\sigma\|,$$

где $\sigma=(\sigma_1(B),\sigma_2(B),\sigma_3(B),\sigma_4(B))^T$, $\|\sigma\|$ — норма вектора σ.

Ранее установлено [24], что поведение параметра, далее обозначаемого *S*, определяемого количеством блоков, для которых НОМСЧ не изменяется при пересохранении ЦИ в формат с потерями с различными коэффициентами качества *QF*, выражаемого в процентах от общего количества блоков матрицы изображения, отличается для оригинальных ЦИ с потерями и без потерь. Так для оригинального ЦИ в формате без потерь количество упомянутых блоков практически не зависит от коэффициента *QF*, использованного при его пересохранении в формат с потерями с $QF\leq95$, чаще всего это количество не превосходят 1% общего количества блоков изображения; для оригинального ЦИ в формате с потерями (в отличие от изображения в формате без потерь) кривая, являющаяся гра-

фиком функции $y(x)$, $x \in [1,100]$, отражающей зависимость *S* от QF, имеет ярко выраженный локальный максимум при совпадении коэффициентов качества первичного и вторичного сжатия, иллюстрация чего для двух конкретных ЦИ приведена на рис.1.

В соответствии с [24-26] в качестве $y(x)$ рассматривается интерполяционный сплайн первой степени, построенный по точкам $(i, t_i), i = \overline{1,100}$, где t_i — количество блоков ЦИ, для которых нормированная отделенность максимального сингулярного числа не изменилась, при пересохранении изображения в формат JPEG с $QF = i$. С учетом вида функции $y(x)$ экстремумы она может достигать только в точках $x = i \in \mathrm{N}$, где N — множество натуральных чисел [24,25].

В соответствии с [25] локальный максимум в точке $x = \bar{i} \in \mathrm{N}$ функции $y(x)$ называется выраженным, если этот максимум определяется окрестностью $\delta(\bar{i}, r)$ с центром в точке $\bar{i} \in \mathrm{N}$ и радиусом $r \in \mathrm{N}$, представляющей из себя совокупность точек

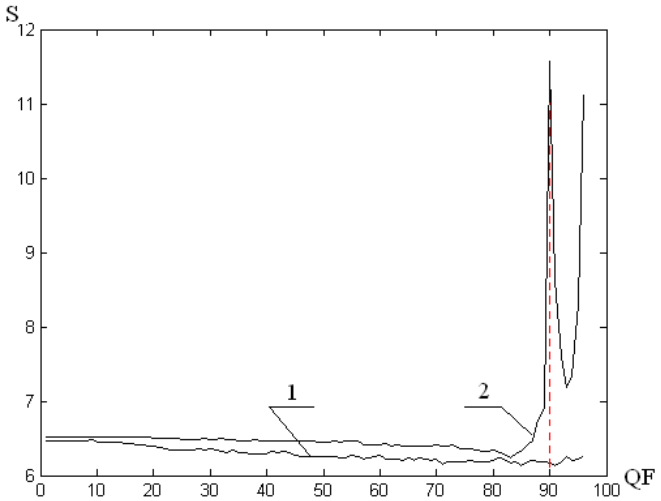
$$\bar{i} - r, \bar{i} - r + 1, \ldots, \bar{i} - 1, \bar{i}, \bar{i} + 1, \ldots, \bar{i} + r - 1, \bar{i} + r,$$

каждая из которых принадлежит сегменту $[1,100]$, где $r > 1$, и значение этого локального максимума $y(\bar{i})$ превосходит значения всех других локальных максимумов $y(x)$ на $[1,100]$, определяемых окрестностями того же радиуса $r > 1$, или если глубина локального максимума, вычисляемая в соответствии с формулой

$$\left(y(\bar{i}) - y(\bar{i} - r)\right) + \left(y(\bar{i}) - y(\bar{i} + r)\right) =$$

$$= 2y(\bar{i}) - y(\bar{i} - r) - y(\bar{i} + r),$$

имеет максимальное значение по сравнению со значением этого параметра для других локальных максимумов $y(x)$, определяемых окрестностями того же радиуса $r > 1$.



1 – оригинальное ЦИ в формате без потерь; 2 – оригинальное ЦИ в формате Jpeg с QF=90

Рис.1. Графики зависимости *S* от *QF* [1]

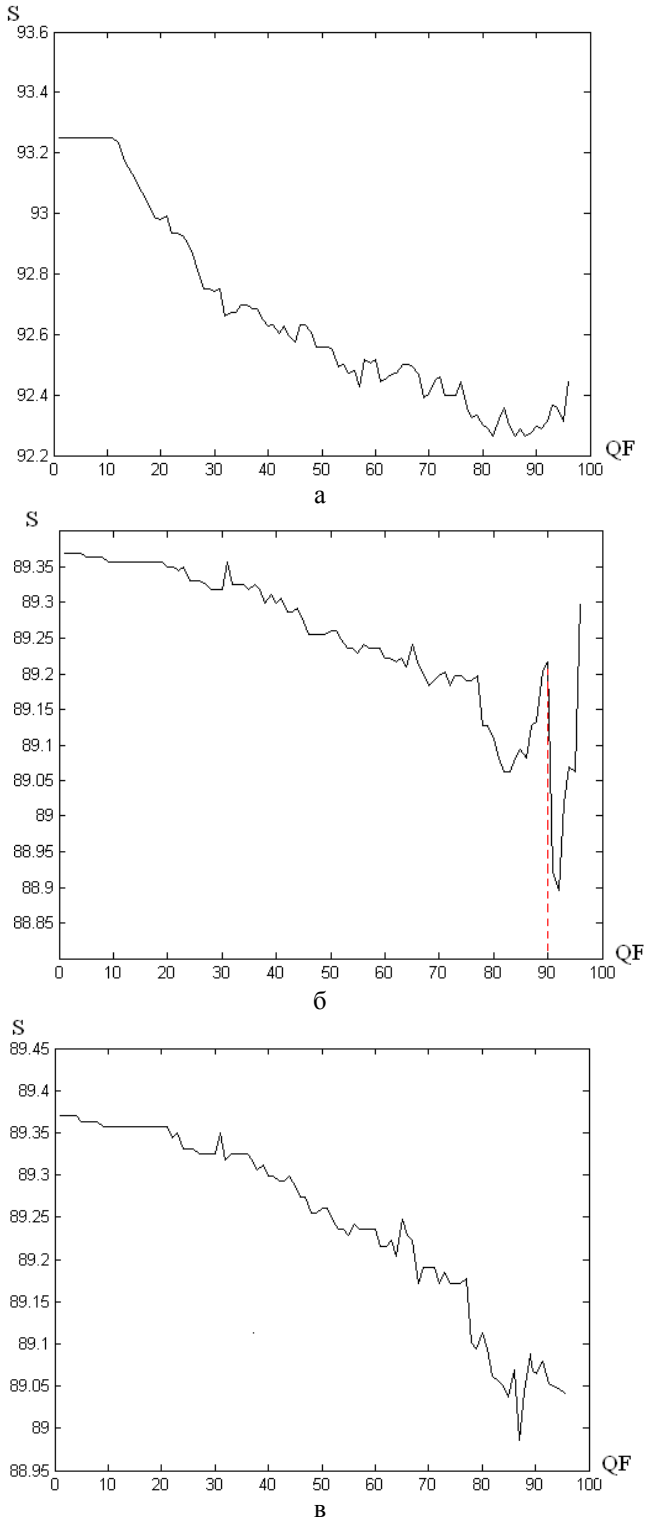
Метод отделения ЦИ, сохраненного первоначально в формате без потерь, от такого, которое было пересохранено без потерь из формата с потерями, разработанный в [26] и взятый за основу в настоящей работе для разработки стеганоаналитического метода, работающего в указанных выше условиях, требует существенной модификации, поскольку очевидно, что свойства оригинального ЦИ с потерями изменятся при его возмущении, являющемся результатом стеганопреобразования. В частности, глубина имеющего место выраженного локального максимума функции $y(x)$ может значительно уменьшится для ЦИ-стеганосообщения, по сравнению с глубиной соответствующего локального максимума $y(x)$ для ЦИ-контейнера, что может сделать этот локаль-

[1] Appendix 1

ный максимум не столь отличимым от имеющих место неярко выраженных максимумов для рассматриваемых кривых – графиков функции $y(x)$, $x \in [1,100]$, для стеганосообщений, т.е. привести к картине, качественно сравнимой с той, которая отвечает оригинальному ЦИ, и, как следствие, к ошибкам первого рода. Иллюстрация сказанному для конкретного ЦИ из базы 4cam_auth [27] приведена на рис.2.

Для возможности разработки стеганоаналитического метода были проведены дополнительные исследования свойств функции $y(x)$, $x \in [1,100]$, отражающей зависимость количества блоков изображения, для которых при пересохранении в формат с потерями не будет меняться НОМСЧ, от *QF*. Было установлено:

- если максимальное из значений количества блоков ЦИ, в которых не меняется НОМСЧ при пересохранении анализируемого изображения в формат Jpeg с каждым коэффициентом качества $QF \in \{1,2,...,100\}$, значительно (порядка 10 и выше (пороговое значение является параметром разработанного метода)), то это ЦИ является стеганосообщением, сформированным с СПС<=0.1 бит/пиксель;
- если разность между максимальным и минимальным из значений количества блоков ЦИ, в которых не меняется НОМСЧ при пересохранении анализируемого изображения в формат Jpeg с каждым $QF \in \{1,2,...,100\}$, значительна (порядка 10 и выше (пороговое значение является параметром разработанного метода)), то это ЦИ является стеганосообщением, сформированным с малой СПС;
- Наличие как и отсутствие для кривой, отражающей зависимость количества блоков ЦИ, для которых при пересохранении в формат с потерями с каждым $QF \in \{1,2,...,100\}$ не будет меняться НОМСЧ, от *QF*, выраженного локального максимума, определяемого по окрестности радиуса *r* как локального максимума максимальной глубины, может отвечать как стеганосообщению, так и контейнеру. Поэтому учет лишь наличия или отсутствия выраженного локального максимума является недостаточным (в отличие от метода, разработанного в [26]) для обеспечения возможности отделения стеганосообщения от контейнера, в силу чего в рассмотрение вводятся два дополнительных количественных параметра рассматриваемой кривой (графика функции $y(x)$, $x \in [1,100]$) – общее количество ее локальных максимумов, определяемых по окрестности радиуса *r*, а также разброс значений локальных максимумов – разность между максимальным и минимальным из значений локальных максимумов $y(x)$, определяемых по окрестности радиуса *r*;
- Для абсолютного большинства проанализированных ЦИ наличие выраженного локального максимума кривой, являющейся графиком функции $y(x)$, свидетельствует о том, что изображение является стеганосообщением, в случае, если разброс значений локальных максимумов $y(x)$ является значительным (пороговое значение разброса устанавливается экспериментально при разработке алгоритмической реализации стеганоаналитического метода);
- Наличие выраженного локального максимума функции $y(x)$, $x \in [1,100]$, при незначительном разбросе значений ее локальных максимумов указывает на стеганосообщение в случае, когда общее количество локальных максимумов незначительно (пороговое значение разброса устанавливается экспериментально при разработке алгоритмической реализации стеганоаналитического метода);
- Значительное количество локальных максимумов $y(x)$ при малом разбросе их значений отвечают ЦИ-контейнеру даже в случае наличия выраженного локального максимума.



а – оригинальное ЦИ в формате TIF; б – ЦИ-контейнер в формате JPEG (QF=90); в – ЦИ-стеганосообщение, сформированное на основе контейнера в формате JPEG (QF=90) методом LSB с СПС=0.1 бит/пиксель

Рис.2. Графики зависимости *S* от *QF* [1]

С учетом всего вышесказанного основные шаги разработанного стеганоаналитического метода следующие.

Шаг 1. Исходное ЦИ с матрицей F пересохранить в формат JPEG с каждым коэффициентом качества $QF \in \{1,2,3,\ldots,100\}$. Результат: ЦИ с матрицами F_i, $i = \overline{1,100}$, где i определяет значение соответствующего использованного *QF*.

[1] Appendix 1

Шаг 2. Для $i=\overline{1,100}$ делать:

2.1. Матрицы F и F_i разбить стандартным образом на непересекающиеся $4\times4-$блоки.

2.2. Сравнивая между собой соответствующие $4\times4-$блоки B и B_i матриц F и F_i определить количество t_i блоков, для которых НОМСЧ блока не изменилась при пересохранении с коэффициентом качества $QF=i$.

Шаг 3. Определить:

3.1. Максимальное количество блоков ЦИ, для которых не менялась НОМСЧ при пересохранении в формат Jpeg с каждым коэффициентом качества $QF\in\{1,2,3,...,100\}$:

$$M=\max_i t_i;$$

3.2. Разброс значений t_i, $i=\overline{1,100}$:

$$R=\max_i t_i-\min_i t_i.$$

Шаг 4.

Если

$$(M\le P_1)\vee(R\le P_2),$$

где P_1, P_2 — пороговые значения, устанавливаемые экспериментально,

то

исходное ЦИ является контейнером.

Переход на шаг 7.

Если

$$(M\ge P_3)\vee(R\ge P_4)$$

где P_3, P_4 — пороговые значения, устанавливаемые экспериментально,

то

исходное ЦИ с матрицей F является СС.

Переход на шаг 7

Шаг 5.

5.1. По точкам (i,t_i), $i=\overline{1,100}$, на сегменте $[1,100]$ построить интерполяционный сплайн $y(x)$ первой степени.

5.2. Определить радиус r окрестности $\delta(\bar{i},r)$, используемой при определении локальных максимумов функции $y(x)$.

5.3. Для полученной функции $y(x)$ найти локальные максимумы (они могут достигаться только в точках, являющихся узлами интерполяции), используя окрестность радиуса r.

Если

локальные максимумы не выявлены

то

если

$$(P_1\le M\le P_3)\&(P_2\le R\le P_4)$$

то

исходное ЦИ с матрицей F является контейнером

иначе

исходное ЦИ с матрицей F является стеганосообщением

иначе

5.3.1. Определить значения и глубины локальных максимумов $y(x)$.

5.3.2. Найти:

5.3.2.1. Наименьшее L_{min}, наибольшее L_{max} значения локальных максимумов функции $y(x)$;

5.3.2.2. Максимальную глубину G_{max} локальных максимумов – выраженный локальный максимум;

5.3.2.3. Количество k_{lok} локальных максимумов функции $y(x)$.

5.3.3. Вычислить разброс r_{lok} значений локальных максимумов функции $y(x)$:

$$r_{lok}=L_{max}-L_{min}.$$

5.3.4.

Если

$$r_{lok}>R_1$$

то

исходное ЦИ с матрицей F является стеганосообщением.

Если

$$(r_{lok}\le R_1)\&(k_{lok}>R_2)$$

то

исходное ЦИ с матрицей F является контейнером.

Если

$$\left(r_{lok} \le R_1\right) \& \left(k_{lok} \le R_2\right)$$

то

исходное ЦИ является СС

Шаг 6.

Если

исходное ЦИ является СС

то

найти тот локальный максимум функции $y(x)$, $x \in [1,100]$, глубина которого равна G_{max}. Пусть он достигается в точке $x = \bar{i}$, тогда считаем, что оригинальный контейнер был сохранен в формате с потерями с коэффициентом качества $QF = \bar{i}$.

Шаг 7. Конец экспертизы.

Очевидно, что предлагаемый стеганоаналитический метод осуществляет экспертизу цифрового изображения без наличия незаполненного контейнера, что выдвигалось авторами в качестве одного из основных требований.

II. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

При алгоритмической реализации метода использовались следующие значения параметров: $R_1 = 1$, $R_2 = 2$, $P_1 = P_2 = 1$, $P_3 = P_4 = 9$, установленные экспериментально. При определении локальных максимумов функции $y(x)$ использовались окрестности радиуса $r = 2$, поскольку увеличение радиуса окрестности приводило к значительному увеличению ошибок 1-го рода. Происходило это в силу следующих причин. Для некоторых ЦИ функция $y(x)$ в окрестности выраженного локального максимума имеет большую скорость изменения (определяемую при помощи $|y'(x)|$), или иначе является чувствительной к изменению значения *QF*. Следствием этого является резкое изменение значения функции $y(x)$ в окрестности локального максимума малого радиуса ($r \le 2$). Учет же окрестности радиуса $r > 2$ в таких ситуациях приводит к тому, что такие локальные максимумы могут быть утеряны, поскольку в границах окрестности $r > 2$ функция успевает поменять характер своей монотонности, что очевидно является нежелательным.

Для оценки эффективности алгоритмической реализации разработанного стеганоаналитического метода был проведен вычислительный эксперимент, в котором были задействованы: 150 ЦИ размером 500×500 пикселей (формат TIF) из базы 4cam_auth [27] (далее обозначается как множество M_1), 100 ЦИ размером 1000×1000 пикселей (формат TIF) из базы img_Nikon_D70s [28] (далее обозначается как множество M_2), 150 ЦИ размером 500×500 пикселей (формат TIF), сделанных непрофессиональными видеокамерами (далее обозначается как множество M_3), множества $M^{(i)}$, $i \in \{90,85,80,75,70,65\}$, полученные путем пересохранения ЦИ из $M_1 \bigcup M_2$ в формат JPEG с *QF=i*. Таким образом, в эксперименте принимали участие 400 ЦИ в формате без потерь и 1500 ЦИ в формате с потерями из множества $\bigcup_{i \in \{90,85,80,75,70,65\}} M^{(i)}$, используемые в качестве контейнеров.

Формирование стеганосообщений происходило LSB-методом при СПС 0.1, 0.05, 0.01 бит/пиксель, что привело к их общему количеству в эксперименте 4500 ЦИ.

Эффективность разработанного алгоритма оценивалась ошибками первого рода (когда стеганосообщение ошибочно определялось как контейнер), второго рода (когда незаполненный контейнер определялся как стеганосообщение). Результаты эксперимента, характеризуемые ошибками 1-го рода, представлены в табл.1. При сравнении полученных результатов с аналогичными показателями эффективности алгоритмической реализации метода, предложенного в [5], который, как уже отмечалось выше, является одним из наиболее эффективных (в том числе, при малой пропускной способности организуемого скрытого канала связи) современных стеганоаналитических методов, было установлено, что при СПС=0.05 бит/пиксель (наименьшее рассмотренное в [5] значение СПС при тестировании алгоритма) среднее значение ошибок первого рода здесь составило 7.6%, что значительно превосходит аналогичный показатель, полученный в аналогичных условиях при использовании алгоритмической

реализации метода, разработанного в настоящей работе.

Ошибки 2-го рода составили 4%.

Таблица 1 [1] –

Ошибки 1-го рода при тестировании разработанного стеганоаналитического алгоритма (%)

СПС (бит/пиксель)	QF ЦИ-контейнера						Среднее значение
	90	85	80	75	70	65	
0.1	1.6	2.4	2	0.4	10.4	11.6	4.7
0.05	1.6	5.2	1.6	1.2	6.8	11.6	4.6
0.01	2	5.2	1.2	0.8	4	10.4	3.9

Для удобства проведения более объемного и объективного сравнительного анализа эффективности, разработанного в работе стеганоаналитического метода с современными аналогами по полученным данным, были рассчитаны значения еще одного широко используемого показателя эффективности — точности выявления, далее обозначаемого *ACC* (табл.2):

$$ACC = \frac{TP + TN}{TP + FN + TN + FP}, \qquad (1)$$

где *TP* (*True Positive*) — число правильно выявленных стеганосообщений (истинноположительный результат); *TN* (*True Negative*) — число правильно выявленных контейнеров (истинноотрицательный результат); *FP* (*False Positive*) — число незаполненных контейнеров, ошибочно принятых за стеганосообщение (ложноположительный результат (ложная тревога) или ошибка второго рода); *FN* (*False Negative*) — число стегносообщений, ошибочно признанных контейнерами (ложноотрицательный результат или ошибка первого рода).

Для сравнительного анализа эффективности предложенного в работе алгоритма, оцениваемой при помощи коэффициента *ACC* (1), были выбраны современные аналоги, наиболее эффективные в условиях малой СПС, информация о которых доступна из открытых источников: S1 [10], S2 [11], S3 [12]. Результаты приведены в табл.3 (прочерки в таблице означают отсутствие в [10-12] результатов тестирования соответствующих алгоритмических реализаций методов при СПС=0.01 бит/пиксель, что может говорить лишь о несостоятельности их в этих условиях).

Результаты тестирования алгоритмической реализации разработанного метода по определению *QF* ЦИ-контейнера при различных значениях СПС организуемого скрытого канала связи, использованных при формировании стеганосообщения, представлены в табл.4. В тестировании были задействованы 4500 ЦИ-стеганосообщений, сформированных на основании 1500 ЦИ-контейнеров в формате Jpeg. Наименьшее количество ошибок было получены в случае, когда контейнер представлял из себя ЦИ в формате Jpeg с *QF*=75: при СПС=0.1 бит/пиксель ошибки составили 4%, при СПС=0.05 бит/пиксель – 5%, при СПС=0.01 бит/пиксель – 4%.

Пример результата экспертизы ЦИ-стеганосообщения, для которого в качестве контейнера использовалось оригинальное изображение в формате Jpeg с *QF*=70, проиллюстрирован на рис.3. Алгоритм безошибочно относит анализируемое изображение к стеганосообщениям, а также точно определяет коэффициент качества при сжатии ЦИ-контейнера за счет введения во множество анализируемых алгоритмом параметров общего количества локальных максимумов функции $y(x)$.

Таблица 2 [1] –

Средние по эксперименту (1500 ЦИ-стеганосообщений для каждого рассмотренного значения СПС) значения ACC для разработанного алгоритма в зависимости от значения пропускной способности организуемого скрытого канала связи

СПС (бит/пиксель)	0.1	0.05	0.01
ACC	0.9537	0.9543	0.9606

[1] Appendix 1

Таблица 3 [1] –

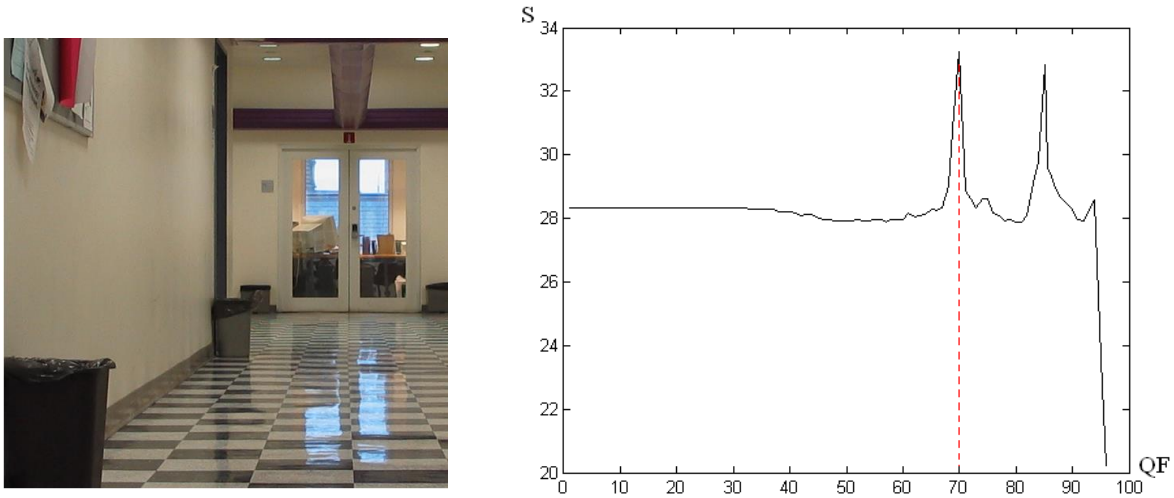
Сравнение эффективности, оцениваемой при помощи ACC, разработанного алгоритма с современными аналогами в условиях малой пропускной способности организуемого скрытого канала связи

СПС, бит/пиксель	S1	S2	S3	Разработанный алгоритм
0.1	0.9937	0.9924	0.970	0.9537
0.05	0.9319	0.9404	0.941	0.9543
0.01	—	—	—	0.9606

Таблица 4 [1] –

Количество ошибок при определении при помощи разработанного алгоритма коэффициента качества QF, использованного при сохранении в формате с потерями оригинального ЦИ-контейнера (%)

СПС (бит/пиксель)	0.1	0.05	0.01
Количество ЦИ-стеганосообщений, для которых *QF* контейнера был определен не верно (%)	13	12.9	12.4



а б

а – ЦИ-стеганосообщение, сформированное LSB-методом с СПС=0.05 бит/пиксель на основе ЦИ-контейнера (формат JPEG с QF=70); б – график функции $y(x)$

Рис.3. Пример результата экспертизы ЦИ разработанным стеганоаналитическим алгоритмом [1]

III. ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ

Приведенные результаты тестирования алгоритмической реализации разработанного стеганоаналитического метода говорят об имеющем место повышении эффективности стеганоанализа цифрового изображения в условиях малой пропускной способности скрытого канала связи, организованного LSB-методом: при СПС=0.05 бит/пиксель он превосходит наилучший из рассмотренных аналогов S3 по показателю *ACC* на 1.5%, с учетом ошибок первого рода превосходит разработку [5] 2017 года на 39.5%, оставаясь эффективным в условиях, когда аналоги вообще являются недееспособными (при СПС=0.01 бит/пиксель *ACC* превышает 0.96). При этом экспертиза ЦИ осуществляется без наличия незаполненного ЦИ-контейнера.

Значимым преимуществом разработанного стеганоаналитического метода является то, что эффективность его алгоритмической реализации практически не зависит от значения пропускной способности организуемого скрытого канала связи, оставаясь высокой при СПС <0.05 бит/пиксель.

Важной информационной составляющей результатов работы предложенного метода

[1] Appendix 1

является обеспечение им возможности определения коэффициента качества *QF* ЦИ-контейнера, участвовавшего в процессе стеганопреобразования, с которым это изображение было сохранено при создании в формате с потерями. Такую задачу не решает в настоящий момент ни один из современных методов-аналогов, информация о которых доступна из открытых источников. При этом такая информация может оказаться полезной для определения/оценки величины пропускной способности организованного скрытого канала связи.

APPENDIX 1 (ПРИЛОЖЕНИЕ 1)

Fig. 1. Plots of *S* versus *QF* (1 – lossless original image; 2 – original Jpeg image with *QF* = 90).

Fig. 2. Plots of *S* versus *QF* (a – original Tif image; b – Jpeg container (*QF* = 90); c – stego image generated by LSB-method with embedding rate 0.1 bpp).

Fig. 3. Examination of a specific image by the developed steganoanalysis algorithm (a – stego image generated by LSB-method with embedding rate 0.05 bpp (container – Jpeg image with *QF* = 70); b – plot of $y(x)$)

Table 1. Type I errors for the developed steganoanalysis algorithm (%).

Table 2. The average values of ACC for the developed algorithm depending on embedding rate (1500 stego image for each embedding rate).

Table 3. ACC comparison for the developed algorithm and modern analogs under conditions of the low communication channel capacity.

Table 4. The number of errors in determining the quality factor QF for Jpeg-container (%).

Литература (References)

[1] Altaay A., Sahib S., Zamani M. An introduction to image steganography techniques. *Proceedings of the 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT'12)*. Kuala Lumpur, 2012, pp. 122-126.

[2] Li B., He J., Huang J., Shi Y.Q. A survey on image steganography and steganalysis. *Journal of Information Hiding and Multimedia Signal Processing*, 2011, vol. 2, no. 2, pp. 142-172.

[3] Karampidis K., Kavallieratou E., Papadourakis G. A review of image steganalysis techniques for digital forensics. *Journal of Information Security and Applications*, 2018, vol. 40, pp.217-235.

[4] Chaeikar S.S., Zamani M., Manaf A., Zeki A.M. PSW statistical LSB image steganalysis. *Multimedia Tools and Applications*, 2018, vol. 77, no. 1, pp. 805-835.

[5] Akhmametieva A. Steganalysis of digital contents, based on the analysis of unique color triplets. Annales *Mathematicae et Informaticae*, 2017, No. 47, pp. 3-18.

[6] Juarez-Sandoval O., Cedillo-Hernandez M., Sanchez-Perez G., Toscano-Medina K., Perez-Meana H., Nakano-Miyatake M. Compact image steganalysis for LSB-matching steganography. *Proceedings of the 5th International Workshop on Biometrics and Forensics (IWBF 2017)*. Coventry, 2017, pp. 1-6.

[7] Chhikara R., Singh L. A review on digital image steganalysis techniques categorized by features extracted. *International Journal of Engineering and Innovative Technology*, 2013, vol. 3, no. 4, pp. 203-213.

[8] Fridrich J., Goljan M., Du R. Detecting LSB steganography in color and gray-scale images. *IEEE MultiMedia*, 2001, vol. 8, no. 4, pp. 22-28.

[9] Tan S., Li B. Targeted steganalysis of edge adaptive image steganography based on LSB Matching revisited using B-spline fitting. *IEEE Signal Processing Letters*, 2012, vol. 19, no. 6, pp. 336-339.

[10] Huang F., Huang J. Calibration based universal JPEG steganalysis. *Science in China Series F: Information Sciences*, 2009, vol. 52, no. 2, pp. 260-268.

[11] Pevny T., Bas P., Fridrich J. Steganalysis by subtractive pixel adjacency matrix. *IEEE Transactions on Information Forensics and Security*, 2010, vol. 5, no. 2, pp. 215-224,

[12] Lin Q., Liu J., Guo Z. Local ternary pattern based on path integral for steganalysis. *Proceedings of 2016 IEEE International Conference on Image Processing (ICIP)*. Phoenix, 2016, pp. 2737-2741.

[13] Geetha S., Sindhu S., Kamaraj N. Close color pair signature ensemble adaptive threshold based steganalysis for LSB embedding in digital images. *Transactions on Data Privacy*, 2008, vol. 1, no. 3, pp. 140-161.

[14] Mitra S., Roy T.K., Mazumdar D., Saha A.B. Steganalysis of LSB encoding in uncompressed images by close color pair analysis. *Proceedings of the IIT Kanpur Hacker's Workshop IITKHACK04*. Kanpur, 2004, pp. 20-22.

[15] Lou D.-C., Hu C.-H., Chiu C.-C. Steganalysis of histogram modification reversible data hiding scheme by histogram feature coding. *International Journal of Innovative Computing, Information and Control*, 2011, vol. 7, no. 11, pp. 6571-6583.

[16] Alimoradi D., Hasanzaden M. The effect of variance difference of dyadic quantized histograms on universal steganalysis. *International Journal of Computer Applications*, 2013, vol. 62, no. 8, pp. 19-24.

[17] Verma S., Sood S., Ranade S.K. Relevance of steganalysis using DIH on LSB steganography. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2014, vol. 4, no. 2, pp. 835-838.
[18] Ashu, Chhikara R. Performance evaluation of first and second order features for steganalysis. *International Journal of Computer Applications*, 2014, vol. 92, no. 16, pp. 17-22.
[19] Bera S., Sharma M. Blind JPEG steganalysis using statistical moment and second order statistics. *International Journal of Engineering Research and General Science*, 2015, vol. 3, no. 5, pp. 632-638.
[20] Rajendraprasad K., Narasimha V.B. Steganography image detection using different steganalysis techniques with Markov chain features. *International Journal of Applied Engineering Research*, 2016, vol. 11, no. 1, pp. 392-395.
[21] Nissar Arooj, Mir A.H. Texture based steganalysis of grayscale images using neural network. *Signal Processing Research*, 2013, vol. 2, no. 1, pp. 17-24.
[22] Sujatha P., Purushothaman S., Rajeswari P. Computational complexity evaluation of ANN algorithms for image steganalysis. *International Journal of Latest Trends in Engineering and Technology*, 2014, vol. 3, no. 3, pp. 229-233.
[23] Kobozeva A.A., Bobok I.I., Garbuz A.I. General principles of integrity checking of digital images and application for steganalysis. *Transport and Telecommunication*, 2016, vol. 17, no. 2, pp. 128-137.
[24] Bobok I.I., Kobozeva A.A. [Investigation of properties of singular numbers of matrix blocks of original digital images stored in formats with losses and without loss]. *Informatsiyna bezpeka* [Information Security], 2018, no. 4, pp. 134-145. (in Russian)
[25] Bobok I.I., Kobozeva A.A. [Development of theoretical basis of the method of separating digital image saved in a format without losses from image saved with losses]. *Suchasna spetsialna tekhnika* [Modern Special Equipment], 2018, no. 3, pp. 15-26. (in Ukrainian)
[26] Bobok I.I. [Development of the method of separating digital image saved in a format without losses from image saved with losses]. *Suchasna spetsialna tekhnika* [Modern Special Equipment], 2018, no. 4, pp. 28-36. (in Ukrainian).
[27] Hsu Y.-F., Chang S.-F. Detecting image splicing using geometry invariants and camera characteristics consistency. *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME'06)*. Toronto, 2006, pp. 549-552.
[28] Gloe T., Böhme R. (2010). The 'Dresden Image Database' for benchmarking digital image forensics. *Proceedings of the 25th Symposium on Applied Computing (ACM SAC 2010)*. Sierre, 2010, vol. 2, pp. 1585–1591.

Сведения об авторах.

Кобозева Алла Анатольевна – д.т.н., проф., заведующий кафедрой информатики и управления защитой информационных систем Одесского национального политехнического университета.
Email: alla_kobozeva@ukr.net

Бобок Иван Игоревич – к.т.н., старший преподаватель кафедры информатики и управления защитой информационных систем Одесского национального политехнического университета.
E-mail: onu_metal@ukr.net

Батиене Лаири Ератостенес (Буркина-Фасо) – магистр кафедры информатики и управления защитой информационных систем Одесского национального политехнического университета.
Email: eratos02@yahoo.fr