УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 2, pp. 179-189

СТЕГАНОАНАЛИЗ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ, ХРАНЯЩИХСЯ В ПРОИЗВОЛЬНЫХ ФОРМАТАХ

И.А. Узун

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: uzun.illya@gmail.com

Работа посвящена разработке стеганоаналитического алгоритма выявления наличия секретного сообщения, погруженного в цифровое изображение методом модификации наименьшего значащего бита. Алгоритм основан на анализе пар цветов, применим для контейнера-изображения, хранимого в произвольном формате.

Ключевые слова: стеганография, стеганоанализ, близкие пары цветов, уникальные цвета, сокрытие информации

Введение

Компьютеризация и информатизация, всевозрастающая роль знаний и технологий приводят к становлению информационного общества. Одними из характерных черт такого общества является активное использование цифровых технологий, развитие информационной экономики, электронного государства и электронных социальных сетей. Важная роль в информационном обществе возложена на информационное пространство. Информационное пространство должно обеспечивать эффективное информационное взаимодействие людей, их доступ к мировым информационным ресурсам, удовлетворять потребности людей в информационных продуктах и услугах. Большую значимость в информационном пространстве приобретает проблема обеспечения конфиденциальности и конфиденциальной информации. Данную проблему, проблему предотвращения разглашения какой-либо информации, способна решить как криптография, так и стеганография [1, 2].

Целью криптографии является модификация секретного конфиденциального сообщения, чтобы его в зашифрованном виде было невозможно прочесть перехватчику. При этом криптография не заботится о том, что зашифрованное сообщение может привлекать к себе внимание. Стеганография же, в отличие от криптографии, скрывает передаваемую информацию внутри контейнера или основного сообщения (ОС), который сам по себе не вызывает никаких подозрений и, соответственно, в тайне остается сам факт передачи. Таким образом, преимущество стеганографических методов и алгоритмов состоит в том, что они предоставляют возможность скрытно передать дополнительную информацию (ДИ) – конфиденциальное сообщение, одновременно с ОС – открытой информацией. В качестве ОС может быть выбран любой мультимедиа объект – цифровое изображение (ЦИ), видео или аудио (в настоящей работе как контейнер используется ЦИ). В результате погружения ДИ в ОС не должно происходить заметных изменений контейнера. Данный процесс будем называть стеганопреобразованием (СП), а его результат – стеганосообщением (СС).

Использование СП часто позволяет избежать прямых атак на ДИ, поскольку неизвестно, присутствует ли она в информационном потоке. ДИ, вносимая в контейнер, может быть предварительно зашифрована, чтобы усложнить основную задачу

стегоанализа (СА) [1, 2] – установление факта присутствия в контейнере скрытой информации.

Большое количество программных средств (*Steganos*, *StegHide*, *S-tools* и др.) как платных, так и бесплатных, свободно распространяемых через Интернет, сделали стеганографию очень популярным средством для сокрытия информации. Совсем недавно Эдвардом Сноуденом была разглашена закрытая секретная информация [3, 4] о существовании программ компьютерного слежения PRISM (США) и Tempora (Великобритания), прослушивающих телефонные разговоры и Интернет-трафик в максимально возможных объемах. PRISM позволяет просматривать электронную почту (Microsoft Hotmail, Google Mail, Yahoo), прослушивать голосовые и видео-чаты, просматривать фотографии, видео, отслеживать пересылаемые файлы и узнавать любые другие подробности из социальных сетей (Facebook, YouTube, Skype). Очевидно, что в свете подобных обстоятельств, к использованию стеганографии прибегнет еще большее число людей, использующих упомянутые сервисы электронной почты и социальные сети, чтобы сохранить конфиденциальность своей информации, не привлекая при этом внимания, как если бы это были зашифрованные файлы.

Известно, что посредством стеганографии между собой общаются как секретные государственные службы, шпионы [5], так и криминальные структуры, и террористы [6–8]. (Упомянутые выше программы PRISM, Tempora как раз и были созданы для борьбы с терроризмом, хоть и нарушая при этом права и свободы честных людей.) Стеганография также может быть использована как способ организации утечки ценной информации из компаний и т.д. Поэтому развитие методов СА на сегодняшний день является чрезвычайно *актуальной* задачей.

СА осуществляет поиск и анализ определенных характеристик и признаков в исследуемом цифровом объекте, установление факта наличия или отсутствия которых позволяет получить ответ на вопрос, является ли анализируемый объект СС или же он не подвергался СП.

Как говорилось ранее, уже создано достаточное количество стеганографических средств, применяемых для различных цифровых контейнеров. Большинство таких продуктов применяет различные модификации LSB-метода, или метода модификации наименьшего значащего бита, основной идеей которого является использование одного или нескольких младших двоичных разрядов интенсивности цветовых компонент отдельных пикселей для внедрения ДИ. Популярность данного метода обусловлена его простотой и тем, что он позволяет скрывать в относительно небольших файлах достаточно большие объемы информации [9]. Визуально изображение при этом не изменяется, особенно если в качестве ОС выбрано многоцветное изображение с большим количеством деталей, то есть информационно нагруженное. Если, например, взять ЦИ цветовой модели RGB, на каждую компоненту цвета R, G и B которого отводится 8 бит, и изменить значения наименьших значащих бит (НЗБ) – то подобное искажение будет неуловимо для человеческого восприятия [10]. Это в значительной степени осложняет работу стегоаналитика, если он не обладает специальными средствами СА. В качестве таких средств могут выступать программы, реализующие методы и алгоритмы стегоанализа.

Хорошо зарекомендовали себя при выявлении LSB-метода стеганоаналитические алгоритмы, основанные на анализе пар цветов [11–15]. Однако, они не лишены существенных недостатков, что осложняет их использование. Так существующие алгоритмы нацелены на работу с конкретными форматами хранения анализируемых изображений. При этом алгоритмы, работающие с форматами без потерь, прибегают к дополнительной категоризации ЦИ [11, 13] с последующим определением пороговых значений для каждой категории. Однако предложенная классификация является неполной и неубедительной, базируется на субъективном мнении исследователей. Для алгоритмов, работающих с ЦИ, хранимыми в форматах с потерями [14], существует

ограничение относительно количества уникальных цветов в ЦИ. Область их применимости – ЦИ, количество уникальных пикселей в которых не превышает половину общего числа пикселей. Данное условие значительно сужает область применимости предлагаемых стеганоаналитических алгоритмов даже для сжатых с потерями изображений.

В силу вышесказанного, создание нового стеганоаналитического метода выявления наличия секретной информации, погруженной при помощи LSB-метода, основанного на анализе пар цветов цифрового изображения, свободного от перечисленных выше недостатков, не зависящего от формата хранения анализируемого ЦИ, является *актуальной* задачей.

Цель и постановка исследований

Целью статьи является разработка стеганоаналитического алгоритма (САА), основанного на анализе количества близких пар цветов и уникальных цветов, применимого для ЦИ, хранимых в произвольном формате (с потерями, без потерь).

Для достижения поставленной цели необходимо решить следующие *задачи*:

1) Определить статистические характеристики ОС и СС, анализ которых, позволит отделить ЦИ, подвергавшиеся СП, от ЦИ, не содержащих ДИ;

2) Выявить характерные особенности и отличия ЦИ, не подвергавшихся СП, от СС, полученных после внедрения ДИ в ходе СП посредством модификации НЗБ;

3) Выявить характерные особенности и отличия изображений, уже подвергавшихся СП посредством модификации НЗБ, от СС, полученных после повторного СП;

4) Исходя из результатов решения предыдущих задач, разработать САА для выявления СС, полученных путем использования метода LSB;

5) Провести анализ эффективности разработанного САА;

6) На основании результатов, полученных при анализе эффективности разработанного САА, определить пороговое значение используемого алгоритмом параметра, при котором ошибки первого и второго рода будут минимальными.

Основная часть

Введем необходимые обозначения и определения. Под цветом в дальнейшем будем понимать тройку компонент (R,G,B) или пиксель, который также подразумевается как триплет значений (R,G,B), где R — красная, G — зеленая и B — синяя компонента в цветовой модели RGB [10].

В качестве статистических характеристик для анализа выбраны коэффициенты близких пар цветов и уникальных цветов.

Пусть P — число близких пар цветов в изображении. Согласно определению, данному в [12] (для ЦИ, хранимых в форматах без потерь), под близкой парой понимают два цвета (R_1,G_1,B_1) и (R_2,G_2,B_2), если для них справедливо следующее соотношение:

$$\begin{cases} |R_1-R_2|\le 1, \\ |G_1-G_2|\le 1, \\ |B_1-B_2|\le 1 \end{cases} \Leftrightarrow \quad (R_1-R_2)^2+(G_1-G_2)^2+(B_1-B_2)^2\le 3. \qquad (1)$$

Для изображений, хранимых в формате с потерями, в [16] было введено следующее определение для соотношения цветов близкой пары:

$$\begin{cases} |R_1 - R_2| \le 2, \\ |G_1 - G_2| \le 2, \\ |B_1 - B_2| \le 2 \end{cases} \Leftrightarrow \quad (R_1 - R_2)^2 + (G_1 - G_2)^2 + (B_1 - B_2)^2 \le 12. \qquad (2)$$

Выбор того, что разность соответствующих цветовых компонент двух пикселей не должна превышать по модулю 2 в соотношении (2) было обусловлено тем, что в процессе сохранения ЦИ в JPEG (с потерями) происходит обнуление высокочастотных (и, возможно, некоторых среднечастотных) коэффициентов дискретного косинусного преобразования (ДКП) 8×8-блоков, полученных после стандартного разбиения матрицы исходного изображения. Исключение высоких (и, возможно, средних) частот в JPEG ЦИ никак не восполнится при его пересохранении в формате TIF, поэтому матрица изображения, сохраненного в TIF первоначально и сохраненного в TIF после JPEG-сжатия должны качественно отличаться друг от друга по своим характеристикам [17]. Таким образом, соотношение (1), как проверено в ходе представительного вычислительного эксперимента, является «нерабочим» для контейнеров с потерями, поскольку в результате квантования частотных коэффициентов ЦИ, происходящего в процессе сжатия, количество цветов снижается. Именно эта принципиальная проблема не позволяла до сих пор использовать САА, основанный на анализе пар цветов для ОС с потерями [11, 13, 15].

Согласно определению уникального цвета в [11, 13] для ЦИ в форматах без потерь, два цвета (R_1, G_1, B_1) и (R_2, G_2, B_2) будем называть уникальными, если выполняется, хотя бы одно из условий:

$$\begin{aligned} |R_1 - R_2| &\le 1, \\ |G_1 - G_2| &\le 1, \\ |B_1 - B_2| &\le 1. \end{aligned}$$

Согласно причине изложенной выше, по которой было введено соотношение (2), в [16] было введено определение уникальных цветов в ЦИ, хранимых в формате с потерями. Так, два цвета (R_1, G_1, B_1) и (R_2, G_2, B_2) называются уникальными, если выполняется, хотя бы одно из условий:

$$\begin{aligned} |R_1 - R_2| &\le 2, \\ |G_1 - G_2| &\le 2, \\ |B_1 - B_2| &\le 2. \end{aligned} \qquad (3)$$

Пусть R — отношение количества близких пар цветов P к количеству уникальных цветов U, определяемых согласно (2), (3) соответственно:

$$R = \frac{P}{U}. \qquad (4)$$

Коэффициент R играет ключевую роль при отделении ОС от СС в разработанном САА. Как уже говорилось ранее, процесс стеганоанализа в предлагаемом алгоритме включает в себя операции внедрения ДИ в анализируемый контейнер. Было замечено,

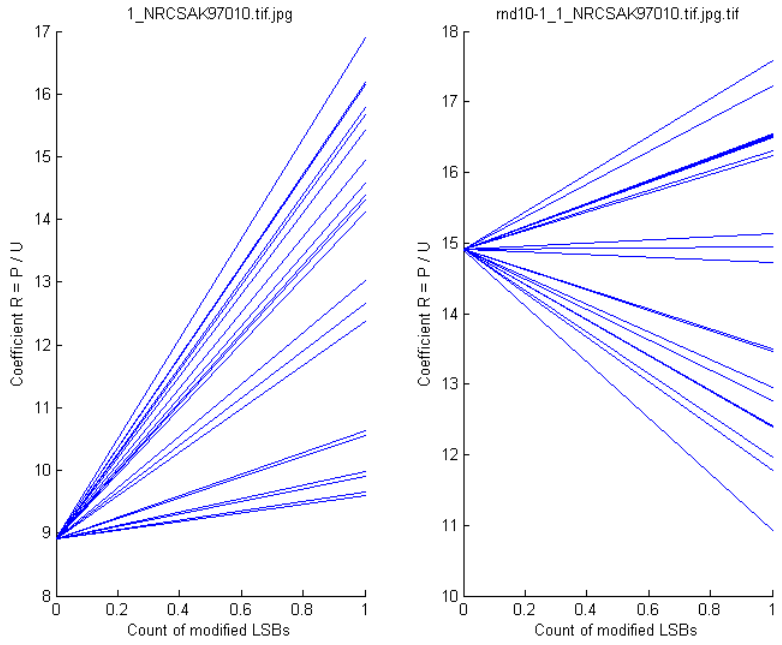
что для точности детектирования целесообразно выполнять не одно, а n СП, которые отличаются лишь внедряемой ДИ.

В [18] был предложен общий математический подход к анализу состояния и технологии функционирования информационных систем, в частности – систем защиты информации. Данный подход основан на теории возмущений и матричном анализе. Процесс получения СС при внедрении ДИ в контейнер посредством LSB-метода, согласно [18], можно представить, как результат воздействия на матрицу контейнера F матрицей возмущения ΔF:

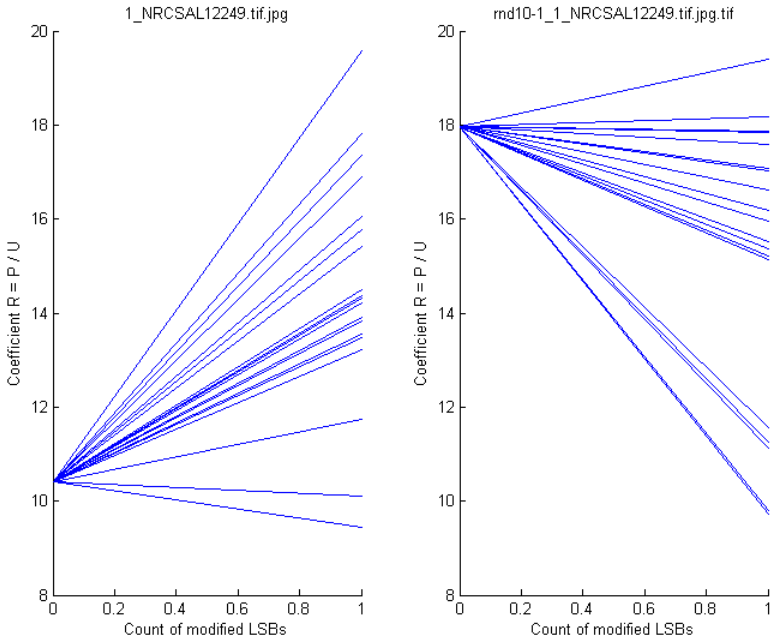
$$\overline{F} = F + \Delta F,$$

где $\overline{F}$ — матрица СС, ΔF — матрица возмущения или ДИ, и F — матрица ОС. Матрица возмущения ΔF, исходя из смысла метода модификации НЗБ, содержит лишь элементы из множества $\{-1,0,1\}$. Для того, чтобы произвести n СП над F, случайным образом осуществляется генерирование n матриц ΔF. Говоря об объеме погружаемой ДИ в процентах, следует понимать, что именно такой процент ненулевых элементов будет содержать матрица ΔF. В основу предлагаемого САА, выполняющего детектирование СС и ОС, было принято положить анализ коэффициентов R и R' из (4). Коэффициент R определяется для матрицы F, а значения R' — для каждой из n матриц ΔF. При работе с ЦИ, хранящимися в формате с потерями, используется соотношение (2), а для ЦИ, не подвергавшихся сжатию, соответственно — (1). На основании сравнения показателей R и R', с использованием при этом порогового значения, делается вывод о наличии либо отсутствии ДИ в анализируемом ЦИ.

На рис. 1, как на примере анализа двух разных изображений, хранимых изначально в формате с потерями, показано, как изменяется отношение близких пар цветов к уникальным цветам (коэффициент R, R') при проведении СП над контейнерами (рис. 1(а)), не содержащими ДИ изначально, и над СС (рис. 1(б)). Ось ординат – значения R и R', ось абсцисс – это количество изменяемых НЗБ. Каждый из графиков состоит из n отрезков. Ордината точки, из которой исходят отрезки – соответствует коэффициенту R, конечные точки отрезков – это n коэффициентов R'.



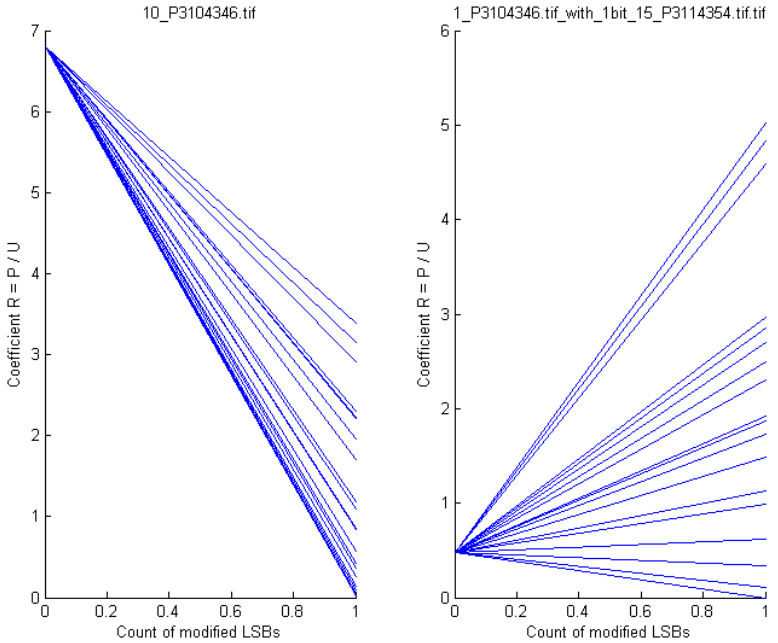
а



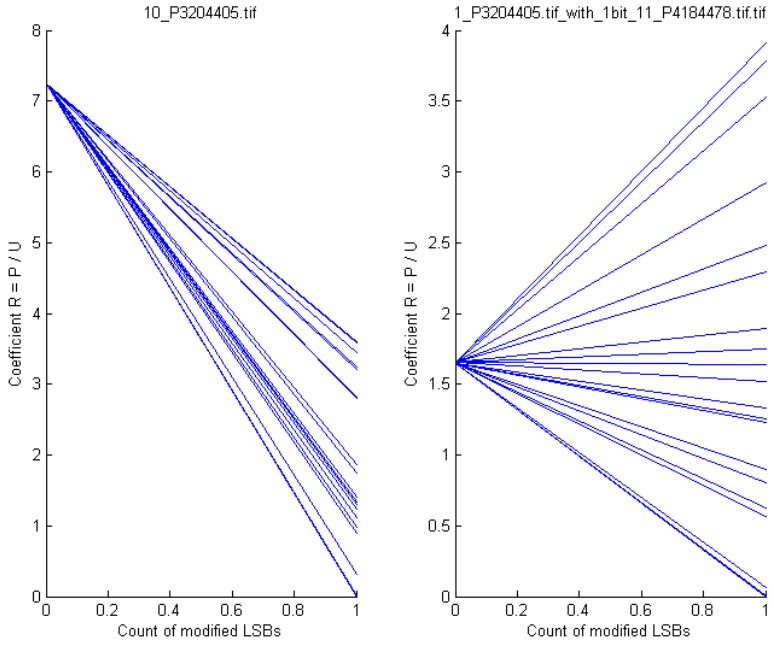
б

Рис. 1. Графики изменения коэффициентов R и R' при СП хранимых в формате JPEG: а – в ЦИ, не содержащих ДИ; б – в СС

Аналогичные графики для изображений, хранившихся изначально в формате без потерь, представлены на рис. 2:



а



б

Рис. 2. Графики изменения коэффициентов R и R' при СП хранимых в формате TIFF: а – в ЦИ, не содержащих ДИ; б – в СС

Как видно из рисунков 1 и 2, характер изменения отношений близких пар цветов к уникальным цветам значительно отличается в зависимости от того, в каком формате изначально хранилось ЦИ. В первую очередь данная особенность объясняется в силу выкладок, изложенных для введения соотношения (2).

Однако данный факт не мешает ввести различные условия для анализируемых контейнеров, в зависимости от того, в каком формате (с потерями или без потерь) изначально хранилось ЦИ.

Для детектирования СС и ОС в ЦИ, хранившихся в формате с потерями, в качестве оцениваемого значения предложена величина $(R - \min(R'))$, а для ЦИ, хранившихся в формате без потерь $(R - \max(R'))$.

Обозначим через T_1, T_2 — величины пороговых значений, минимизирующих ошибки первого и второго рода, для изображений хранимых с потерями и без потерь соответственно.

Тогда, для ЦИ, хранившихся в JPEG (в формате с потерями), будем считать, что матрица F не подвергалась возмущению ΔF, если выполняется условие:

$$R - \min(R') < T_1,$$

иначе считаем анализируемый контейнер СС.

Для ЦИ, хранившихся в TIFF (в формате без потерь), будем считать, что матрица F не подвергалась возмущению ΔF, если выполняется условие:

$$R - \max(R') > T_2,$$

иначе считаем анализируемый контейнер СС.

Предложенный алгоритм был протестирован на выборке из 300 ЦИ, хранимых в формате JPEG, размером 500×500 пикселей, загруженных из базы изображений NRCS [19]. В ходе экспериментов, отдельно анализировались контейнеры, а также СС. Для

оценки эффективности САА были получены специально выборки из СС, в которых были модифицированы все 3 цветовых канала, отдельно только два канала и только один канал. При этом для каждого из этих вариантов были также получены наборы СС в зависимости от объема внедренной ДИ, который был выбран на уровне 20, 35 и 50%. В результате данного анализа была определена оптимальная величина T_1, значение которой составило $T_1 = 1.23$. Ошибки первого и второго рода составили порядка 0.5%. Данные результаты проиллюстрированы на рис. 3:

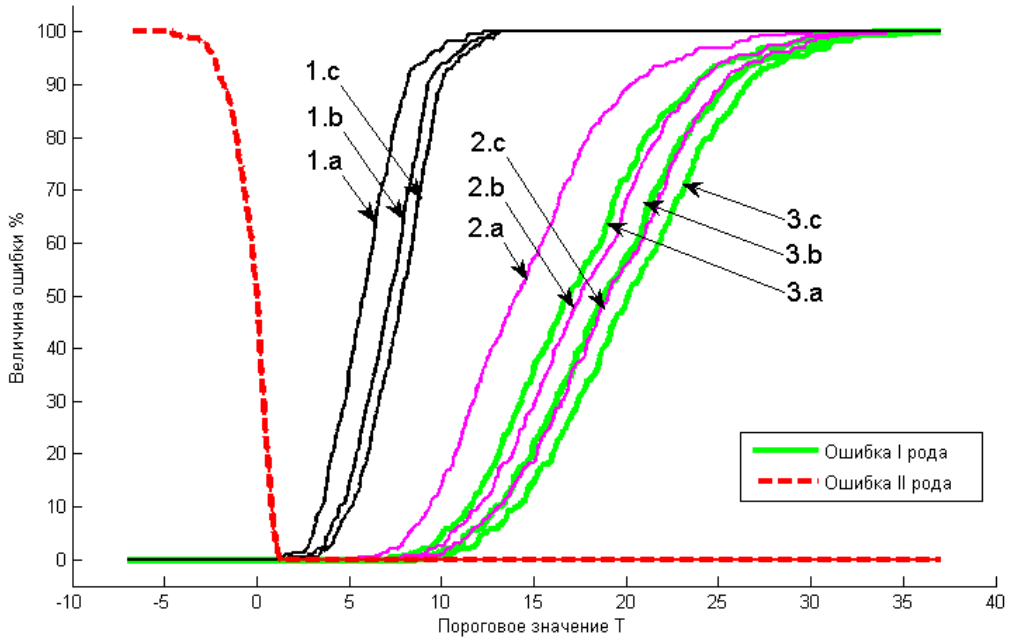


Рис. 3. График зависимости ошибок I и II рода от выбора порогового значения в ЦИ, хранившихся в формате с потерями: 1.a, 1.b, 1.c – в СС изменялся один цветовой канал с объемом ДИ 20, 35 и 50% соответственно; 2.a, 2.b, 2.c – в СС изменялось два цветовых канала с объемом ДИ 20, 35 и 50% соответственно; 3.a, 3.b, 3.c – в СС изменялось три цветовых канала с объемом ДИ 20, 35 и 50% соответственно

Ось ординат на рис. 3 – это величина ошибок первого, либо второго рода. Ось абсцисс – это значение выбираемого порогового значения T_1. Пунктиром изображен график зависимости ошибки второго рода от T_1. Сплошными изображены графики зависимости ошибки первого рода, соответствующие разным наборам СС относительно объема внедренной ДИ. Самый левый график, таким образом, соответствует набору СС, в которые был внедрен наибольший объем ДИ.

Для тестирования САА на изображениях, хранимых в формате без потерь, была использована собственная база из 100 TIFF изображений размером 500×500 пикселей. Была создана выборка из контейнеров, а также выборка из СС, полученных путем замены НЗБ ОС битовой плоскостью случайного ЦИ. Объем внедренной ДИ при этом мог составить порядка 1 бита на пиксель в худшем случае. В результате данного эксперимента величина порогового значения была определена на уровне $T_2 = 0.28$, а ошибка первого и второго рода составила 1% (рис. 4).

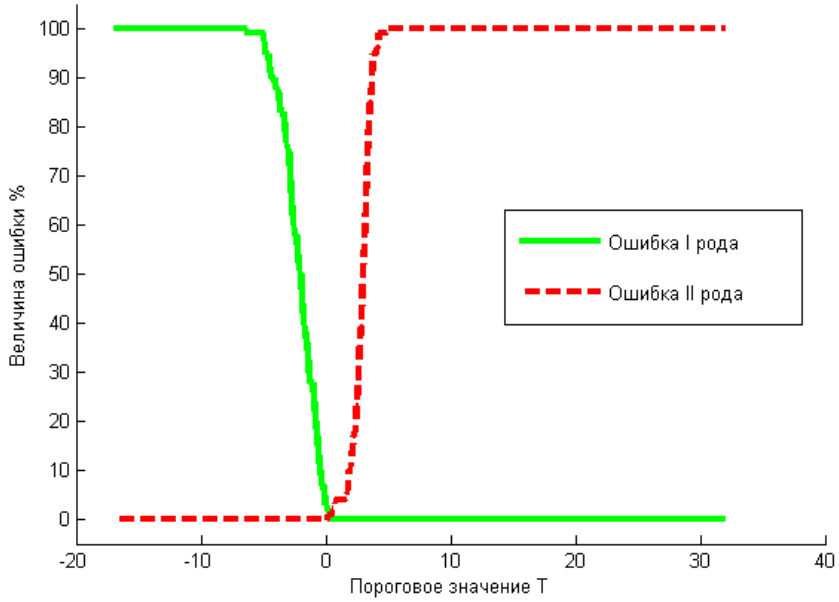


Рис. 4. График зависимости ошибок I и II рода от выбора порогового значения в ЦИ, хранившихся в формате без потерь

Заключение

Результаты вычислительного эксперимента, проведенного с целью проверки эффективности работы нового САА, представлены в таблице 1.

Таблица 1.

Результаты работы предложенного САА

	Порог	Ошибки I рода, %	Ошибки II рода, %	Объем внедренной информации, бит/пиксель
ОС формата с потерями	$T_1 = 1.23$	0.5	0.5	0.2
ОС формата без потерь	$T_2 = 0.28$	1	1	1

В настоящий момент основные усилия автора направлены на увеличение эффективности САА при уменьшении объема внедряемой ДИ для контейнеров, хранимых в формате без потерь.

Список литературы

1. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с.
2. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.
3. O'Harrow Jr, R. U.S., company officials: Internet surveillance does not indiscriminately mine data *[Электронный ресурс]* / R. O'Harrow Jr., E. Nakashima and B. Gellman // The Washington Post.

Washington, USA. Режим доступа: http://articles.washingtonpost.com/2013-06-08/world/39834622_1_prism-clapper-jr-fisa-court (Дата обращения: 08.06.2013).
4. Greenwald, G. NSA Prism program taps in to user data of Apple, Google and others *[Электронный ресурс]* / G. Greenwald, E. MacAskill // The Guardian. London, UK. Режим доступа: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (Дата обращения: 26.05.2013).
5. Fox, S. FBI: Russian Spies Hid Codes in Online Photos *[Электронный ресурс]* // NBC News. New York, USA. Режим доступа: http://www.nbcnews.com/id/38028696/ns/technology_and_science-science/t/fbi-russian-spies-hid-codes-online-photos/ (Дата обращения: 26.05.2013).
6. Бобок, И.И. Стеганоанализ, как частный случай анализа информационной системы / И.И. Бобок, А.А. Кобозева // Сучасна спеціальна техніка. — 2011. — № 2. — С. 21–34.
7. Gul, G. SVD-Based Universal Spatial Domain Image Steganalysis / G. Gul, F. Kurugollu // IEEE Transactions on Information Forensics and Security. — 2010. — Vol. 5, No. 2. — PP. 349–353.
8. Kelley, J. Terrorist instructions hidden online *[Электронный ресурс]* // USA Today. Tysons Corner, Virginia, USA. Режим доступа: http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen-side.htm (Дата обращения: 26.05.2013).
9. Швидченко, И.В. Анализ криптостеганографических алгоритмов / И.В. Швидченко // Проблемы управления и информатики. — 2007. — № 4. — С. 149–155.
10. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. — М. : Техносфера, 2006. — 1070 с.
11. Geetha, S. Close color pair signature ensemble adaptive threshold based steganalysis for LSB embedding in digital images / S. Geetha, S. Sindhu, and N. Kamaraj // Transactions on Data Privacy. — 2008. — Vol. 1, Iss. 3. — PP. 140–161.
12. Johnson, N.F. Exploring Steganography: Seeing the Unseen / N.F. Johnson, S.Jajodia // IEEE Computer. — 1998. — Vol. 31, No. 2. — PP. 26−34.
13. Mitra, S. Steganalysis of LSB Encoding in Uncompressed Images by Close Color Pair Analysis / S. Mitra, T. Roy, D. Mazumdar and A.B. Saha // IIT Kanpur Hackers' Workshop 2004 (IITKHACK04), 23–24 Feb 2004. — 2004. — PP. 23–24.
14. Fridrich, J. Steganalysis of LSB Encoding in Color Image / J. Fridrich, R. Du, M. Long // IEEE International Conference on Multimedia and Expo. — 2000. — Vol.3. — PP. 1279–1282.
15. Seymer, P. Performance Optimization of Close-Color Pair Steganalysis / P. Seymer, G. Dimitoglou // Proceedings of the 2007 International Conference on Security & Management, Las Vegas, USA. — 2007. — PP. 123–127.
16. Рудницкий, В.Н. Стеганоаналитический алгоритм для изображений, подвергавшихся операции сжатия с потерями / В.Н. Рудницкий, И.А. Узун // Захист інформації. — 2013. — Том 15, № 2. — С. 122–127.
17. Бобок, И.И. Стеганоаналитический алгоритм для основного сообщения, хранимого в форматах с потерями / И.И. Бобок // Вісник Національного технічного університету «ХПІ». — 2012. — №29. — С. 41–49.
18. Кобозєва, А.А. Аналіз захищеності інформаційних систем [Текст] : підруч. для студ. вищ. навч. закл., які навч. за напр. «Інформаційна безпека» та «Системні науки та кібернетика» / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко ; М-во трансп. та зв'язку України, Держ. ун-т інформ.-комунікац. технологій. — К. : ДУІКТ, 2010. — 316 с.
19. NRCS Photo Gallery: *[Электронный ресурс]* // United States Department of Agriculture. Washington, USA. Режим доступа: http://photogallery.nrcs.usda.gov (Дата обращения: 26.07.2012).

СТЕГАНОАНАЛІЗ ЦИФРОВИХ ЗОБРАЖЕНЬ, ЩО ЗБЕРІГАЮТЬСЯ У ДОВІЛЬНИХ ФОРМАТАХ

І.А. Узун

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; email: uzun.illya@gmail.com

Робота присвячена розробці стеганоаналітичного алгоритму визначення наявності секретного повідомлення, вбудованого в цифрове зображення. Запропонований алгоритм не залежить від формату зберігання зображення. Алгоритм заснований на аналізі пар кольорів з використанням методу модифікації найменшого значущого біту.

Ключові слова: стеганографія, стеганоаналіз, близькі пари кольорів, унікальні пари кольорів, приховування інформації

STEGANALYSIS OF DIGITAL IMAGES THAT SAVED IN RANDOM FILE FORMATS

Illya A. Uzun

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; email: uzun.illya@gmail.com

This paper is devoted to steganalysis algorithm determining presence a secret message embedded into digital image which is stored in compressed or uncompressed form. The algorithm is based on the analysis of pairs of colors and uses the method of modifying the least significant bit.

Keywords: steganography, steganalysis, close-color pairs, unique colors, information hiding