УДК 004.056

О.О. ВОВК, А.А. АСТРАХАНЦЕВ, А.В. ДОРОЖАН

Харьковский национальный университет радиоэлектроники, Харьков

ИССЛЕДОВАНИЕ СТОЙКОСТИ МЕТОДОВ СКРЫТИЯ ИНФОРМАЦИИ В НЕПОДВИЖНЫХ ИЗОБРАЖЕНИЯХ

В последние годы стеганография является причиной многих дискуссий. Всё больший интерес к ней растёт именно как к эффективному методу сокрытия данных, что позволяет сохранять конфиденциальность информации. В работе проводилась оценка стойкости и надежности методов скрытия информации в пространственной области неподвижных изображений. С помощью качественных и количественных характеристик определялись оптимальные значения показателей для методов на основе замены наименее значащих бит изображения и метода Куттера-Джордана-Боссена. Устанавливалась целесообразность использования рассмотренных методов для различных стеганосистем.

Ключевые слова: *визуальные показатели искажения, метод замены наименее значащего бита, стеганосистема, метод Куттера-Джордана-Боссена, цифровой водяной знак.*

Введение

В последние годы стеганография является причиной многих дискуссий. Всё больший интерес к ней растёт именно как к эффективному методу сокрытия данных, что позволяет сохранять конфиденциальность информации.

Стеганография – в переводе с греческого дословно означает «тайнопись». Это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи. В современном мире – это цифровая стратегия сокрытия файла в мультимедийном формате, например: в графических, музыкальных, видео, текстовых и исполняемых файлах.

Как и большинство программных средств по обеспечению безопасности, у стеганографии есть свои достоинства и недостатки. Она может быть использована как для поддержания законных целей: водяные знаки, цифровые подписи – для обеспечения защиты авторских прав и прав собственности, или просто тайной передачи или хранения информации – в целях сохранения её целостности, предотвращения кражи или несанкционированного просмотра. Так и для незаконных, если методами стеганографии воспользуются злоумышленники, например для тайной переписки террористов или сокрытия украденных или неразрешённых файлов[1].

Большинство исследований [2,3] посвящено использованию изображений в качестве контейнера, это обусловлено существованием практической потребности защиты фотографий от незаконного тиражирования, а также заранее известными размерами контейнера и наличием текстурных областей, хорошо подходящих для встраивания информации. Наибольшее распространение на сегодняшний день получили методы скрытия на основе замены наименее значащего бита [2,3], поэтому актуальной задачей является сравнительный анализ методов на основе замены наименее значащего бита и альтернативного метода, обладающего априорно более высокой стойкостью к атакам – метода Куттера–Джордана–Боссена.

1. Обзор методов скрытия информации

Общий принцип методов скрытия данных в пространственной области заключается в замене избыточностей, малозначимой части изображения битами секретного сообщения. Их преимущества заключаются в том, что для встраивания нет необходимости выполнять вычислительно сложные и длительные преобразования изображений.

Метод замены наименее значащего бита (НЗБ, LSB – Least Significant Bit) наиболее распространен среди методов замены в пространственной области.

Младший значащий бит изображения несет в себе меньше всего информации. Известно, что человек в большинстве случаев не способен заметить изменений в этом бите. Фактически, НЗБ — это шум, поэтому его можно использовать для встраивания информации путем замены менее значащих битов пикселей изображения битами секретного сообщения. При этом, для изображения в градациях серого (каждый пиксель изображения кодируется одним байтом) объем встроенных данных может составлять 1/8 от общего объема контейнера.

Популярность данного метода обусловлена его простотой и тем, что он позволяет скрывать в относительно небольших файлах достаточно большие объемы информации (пропускная способность создаваемого скрытого канала связи составляет при

этом от 12,5 до 30%). Метод зачастую работает с растровыми изображениями, представленными в формате без компрессии (например, GIF и BMP).

Метод НЗБ имеет низкую стеганографическую стойкость к атакам пассивного и активного нарушителей. Основной его недостаток — высокая чувствительность к малейшим искажениям контейнера. Для ослабления этой чувствительности часто дополнительно применяют помехоустойчивое кодирование.

Метод Куттера–Джордана–Боссена. На сегодняшний день стойкость является одним из самых важных требований, предъявляемых алгоритмам встраивания информации. Более высокие характеристики в этом плане показывает метод Куттера–Джордана–Боссена, также использующий пространственную область для скрытия данных.

В алгоритме предложено использовать канал синего цвета изображения, которое имеет RGB-кодирование, для скрытия информации. Поскольку зрительная система человека является наименее восприимчивой к изменениям яркости именно синего цвета по сравнению с красным и зеленым.

Встраивание информации происходит таким способом – один i-й бит m_i сообщения в один псевдослучайный пиксель контейнера p = (x, y). Секретный ключ K_0 задает координаты пикселей, в которые будет встраиваться информация. При встраивания яркости красного и зеленого цветов остаются неизменными, а яркость синего – изменяется по следующей формуле:

$$B^*_{x,y} = \begin{cases} B_{x,y} + \upsilon \cdot \lambda_{x,y}, \text{при } m_i = 0; \\ B_{x,y} - \upsilon \cdot \lambda_{x,y}, \text{при } m_i = 1. \end{cases} \quad (1)$$

где $\lambda_{x,y} = 0{,}29890 \cdot R_{x,y} + 0{,}58662 \cdot G_{x,y} + 0{,}11448 \cdot B_{x,y}$ — яркость пикселя;

υ - коэффициент, задающий энергию встраиваемого бита данных (задается исходя из функционального назначения и особенностей стеганосистемы). Чем больше υ, тем выше робастность вложения, но и тем сильнее заметность.

Поскольку на принимающей стороне изображение-оригинал не известно, то нет возможности гарантированно узнать в какую сторону изменилась яркость синего цвета. Поэтому для извлечения прогнозируется значение яркости исходного синего цвета на основе его соседей:

$$\overline{B_{x,y}} = \frac{\sum_{i=1}^{\sigma} (B_{x,y+i} + B_{x,y-i} + B_{x+i,y} + B_{x-i,y})}{4\sigma}, \quad (2)$$

где $\sigma = 1 \div 3$ — размер области, по которой будет прогнозироваться яркость.

Пиксель в центре – это пиксель, яркость синего цвета которого прогнозируется на основе пикселей, которые выделены цветом.

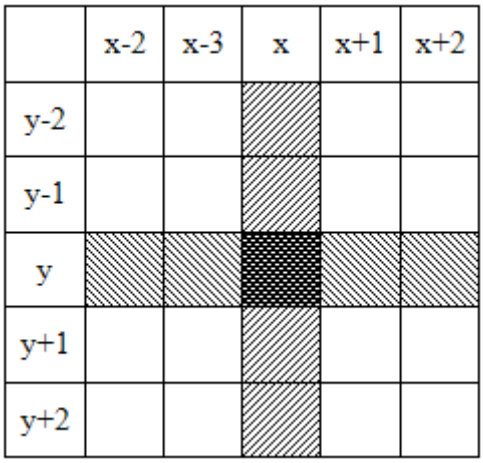


Рис. 1. Биты, используемые для прогнозирования, при $\sigma = 2$

При извлечении скрытого бита вычисляется разница δ между текущим ($B^*_{x,y}$) и спрогнозированным ($\overline{B^*_{x,y}}$) значениями интенсивности пикселя p = (x, y):

$$\delta = B^*_{x,y} - \overline{B^*_{x,y}}, \quad (3)$$

$$m_i = \begin{cases} 0, \text{если } \delta < 0; \\ 1, \text{если } \delta > 0. \end{cases}$$

Преимуществом этого метода является высокая пропускная способность, стойкость к несанкционированному ознакомлению, к частотному детектированию, а также к разрушению младшего бита контейнера и к атакам сжатия.

Недостатком является вероятностный характер извлечения сообщения. Для уменьшения вероятности ошибки рекомендуется использовать помехоустойчивое кодирование. Также можно в процессе встраивания каждый бит повторять несколько раз (многократное встраивание).

2. Характеристики методов встраивания

Основной целью стеганоанализа является моделирование стеганографических систем и исследование их характеристик для получения качественных и количественных оценок надежности использования стеганопреобразований.

Для сравнительного оценивания качества стеганографических средств разрабатываются разные показатели, дающие количественные оценки. Они оперируют с изображениями на уровне пикселей, хотя после надлежащей адаптации они могут быть применены и к другим способам описания изображения, а также к аудиоданным.

Наиболее популярным показателем при анализе уровня искажений, которые вносятся в контейнер

во время скрытия в нем информации, взятое из радиотехники соотношение "сигнал/шум" (SNR):

$$SNR = \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (C_{x,y})^2}{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (C_{x,y} - S_{x,y})^2}, \quad (4)$$

где $C_{x,y}$ – значение пикселя пустого контейнера с координатами (x, y);

$S_{x,y}$ – соответствующее значение пикселя заполненного контейнера;

rows (C) – количество строк в массиве C;

cols (C) – количество столбцов в массиве C.

Нормированная средняя абсолютная разница (NAD), указывающая степень отличия между исходным контейнером и контейнером со встроенным секретным файлом, рассчитывается таким способом:

$$NAD = \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} \left|C_{x,y} - S_{x,y}\right|}{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} \left|C_{x,y}\right|}. \quad (5)$$

Качество изображения (IF) является одной из основных оценочных характеристик для стеганоалгоритмов, работающих с изображениями. Потому что визуальная атака основана на способности зрительной системы человека анализировать визуальные образы и обнаруживать существенные расхождения в изображениях.

$$IF = 1 - \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (C_{x,y} - S_{x,y})^2}{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (C_{x,y})^2}. \quad (6)$$

Структурное содержание (SC) является еще одним показателем, который используется во время оценки искажений, которые вносит стеганосистема в изображение. Он рассчитывается по формуле:

$$SC = \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (C_{x,y})^2}{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (S_{x,y})^2}. \quad (7)$$

3. Результаты исследований

Функции встраивания и извлечения в методе Куттера-Джордана-Боссена не симметричные. Следовательно, хотя правильное распознавание бита сообщения является высоковероятным, но не является стопроцентным. Поэтому для уменьшения вероятности ошибок извлечения было предложено в процессе встраивания каждый бит повторять несколько раз. Поскольку при этом каждый бит был повторен τ раз, выходит τ оценок одного бита сообщения. Секретный бит извлекается по результатам усреднения разности между реальным и оценочными интенсивностями пикселя в полученном контейнере:

$$\delta = \tau^{-1} \cdot \sum_{i=1}^{\tau} (B^*_{x,y} - \overline{B^*_{x,y}}). \quad (8)$$

Как и в общем случае, знак усредненной разности δ будет определять значение встроенного бита.

Количество повторений встраивания одного и того же бита задается заранее. Проведем исследование вышеприведенных характеристик в зависимости от изменения кратности повторного встраивания каждого бита сообщения τ. Результаты полученных значений приведены в табл. 1, а также отображены графически на рис. 2 и рис.3.

Таблица 1

Показатели визуального искажения (ПВИ) в зависимости от τ

τ / ПВИ	1	3	8	10
SNR	$6{,}98 \cdot 10^5$	$2{,}63 \cdot 10^5$	$9{,}73 \cdot 10^4$	$7{,}59 \cdot 10^4$
NAD	$3{,}02 \cdot 10^{-5}$	$8{,}36 \cdot 10^{-5}$	$2{,}24 \cdot 10^{-4}$	$2{,}82 \cdot 10^{-4}$
τ / ПВИ	15	20	25	40
SNR	$5{,}1 \cdot 10^4$	$3{,}79 \cdot 10^4$	$2{,}97 \cdot 10^4$	$1{,}87 \cdot 10^4$
NAD	$4{,}22 \cdot 10^{-4}$	$5{,}66 \cdot 10^{-4}$	$7{,}16 \cdot 10^{-4}$	$1{,}14 \cdot 10^{-3}$

Очевидно, что увеличение количества повторений существенно уменьшит вероятность возникновения ошибок при извлечении скрытого сообщения, но как видно из графиков – это негативно влияет на статистику изображения.

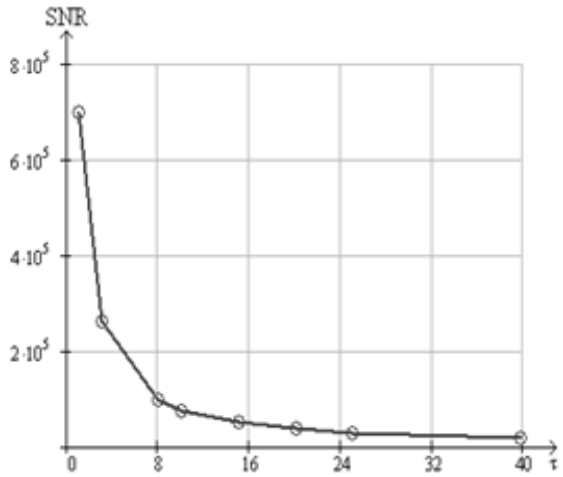


Рис. 2. График зависимости отношения "сигнал/шум" от количества повторного встраивания бита τ

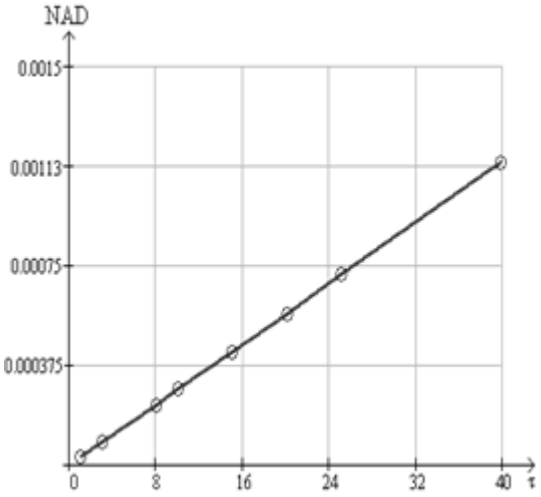


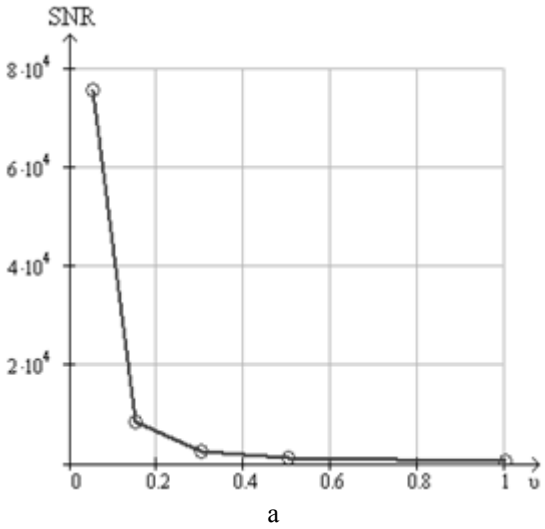
Рис. 3. График зависимости нормированной средней абсолютной разницы от количества повторного встраивания бита τ

Также заранее необходимо задать параметр *υ*, который определяет энергию встраиваемого сигнала. Чем меньше значение коэффициента υ, тем визуально менее заметен результат встраивания. Следовательно, исследуем влияние коэффициента υ на визуальные показатели искажения. Результаты полученных значений приведены в табл. 2, а также отображены графически на рис. 4 (а – г).

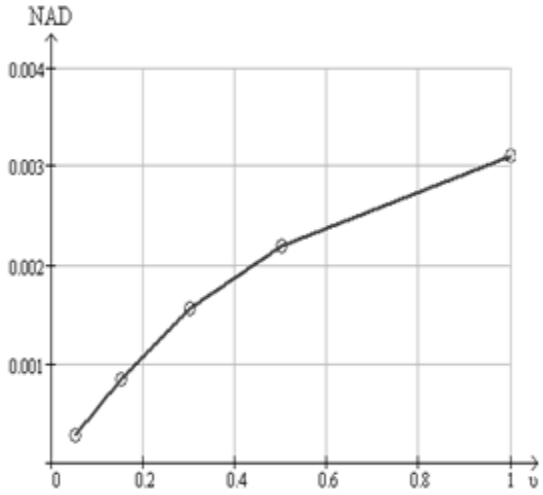
Таблица 2

Показатели визуального искажения (ПВИ) в зависимости от υ

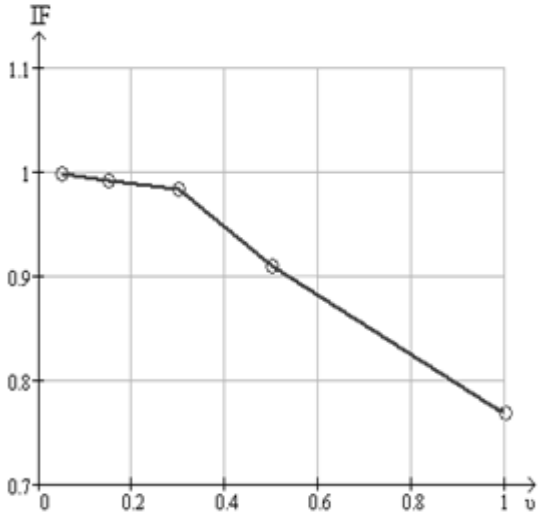
ПВИ \ υ	0,05	0,15	0,3	0,5	1
SNR	$7{,}5\cdot10^{4}$	$8{,}6\cdot10^{4}$	$2{,}4\cdot10^{3}$	$1{,}1\cdot10^{3}$	445,58
NAD	$2{,}8\cdot10^{-4}$	$8{,}3\cdot10^{-4}$	$1{,}6\cdot10^{-3}$	$2{,}2\cdot10^{-3}$	$3{,}1\cdot10^{-3}$
IF	0,999	0,992	0,984	0,91	0,766
SC	1,002	1	0,967	0,942	0,795



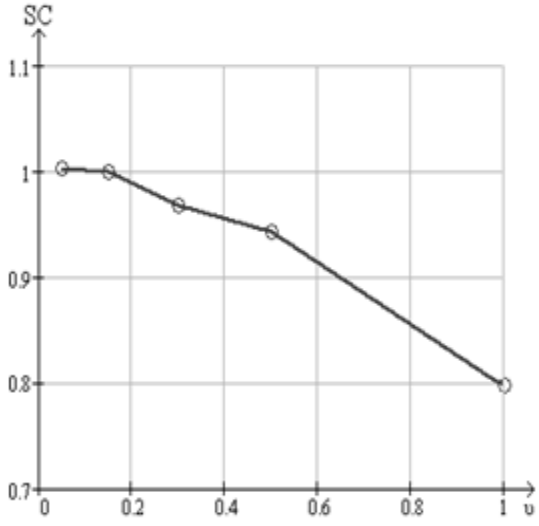
а



б



в



г

Рис. 4. Графики зависимости показателей искажения от энергии встраиваемого сигнала υ (а – отношение "сигнал/шум", б – нормированная средняя абсолютная разница, в – качество изображения, г – структурное содержание)

Согласно полученным результатам, было определено, что результат встраивания визуально незаметен при значениях $\upsilon < 0{,}05$. Но в этом случае для уменьшения количества ошибок при извлечении сообщения необходимо значительно повысить кратность повторного встраивания бита. А это также негативно влияет на характеристики контейнера со скрытым сообщением.

Следовательно, выбор таких характеристик, как энергия встраиваемого сигнала υ и количество повторений одного и того же бита τ в процессе скрытия, зависит от характеристик изображения, которое было выбрано в качестве контейнера, а также от назначения стеганосистемы. Анализируя полученные зависимости, можно сделать вывод, что оптимальными значениями являются $\upsilon \approx 0{,}1$ и $\tau < 10$.

Проведем сравнительный анализ характеристик, полученных для стеганосистем с встраиванием на основе метода НЗБ, модифицированного метода НЗБ, который использует для скрытия два младших бита и метода Куттера–Джордана–Боссена (табл. 3).

Таблица 3

Показатели визуального искажения (ПВИ) при встраивании секретного сообщения в разные биты изображения и методом Куттера–Джордана–Боссена

№ бит / ПВИ	1	2	3	**4**	5	6	7	8	1 і 2	**К-Д-Б**
SNR	$2{,}64\cdot10^{4}$	$6{,}61\cdot10^{3}$	$1{,}66\cdot10^{3}$	**415,4**	102,95	25,72	6,437	1,601	102,07	**540,367**
NAD	$4{,}67\cdot10^{-3}$	$9{,}14\cdot10^{-3}$	0,019	**0,037**	0,075	0,15	0,299	0,601	0,075	**0,018**
IF	1	1	0,999	**0,998**	0,99	0,961	0,845	0,375	0,99	**0,998**
NC	1	1	1	**1,001**	1,003	10,03	1,037	0,97	1,002	**0,998**
CQ	123,2	123,195	123,195	**123,33**	123,53	126,64	127,8	119,55	123,5	**123,001**
SC	1	1	0,999	**0,995**	0,985	0,913	0,813	0,639	0,985	**1,001**

Заключение

Полученные результаты показывают, что наименьший уровень визуальных искажений позволяет получить метод на основе замены НЗБ, однако он не обладает достаточной устойчивостью и не эффективен при внешних воздействиях на заполненный стегоконтейнер.

Система на основе замены нескольких НЗБ незначительно изменяет изображение визуально, характеристики метода, соответствуют встраиванию в 5 бит (табл.3, подчеркнутый текст) и существенно отличаются от характеристик контейнера-оригинала, что делает систему неустойчивой к обнаружению стеганограммы. Применение метода на основе замены нескольких младших бит целесообразно в случае необходимости удвоить пропускную способность стеганосистемы, но это приведет к ухудшению стойкости к обнаружению почти в 5 раз.

При использовании метода Куттера–Джордана–Боссена показатели искажения соответствуют показателям метода замены НЗБ при встраивании в 4-й бит (табл. 3, жирный текст), хотя за счет использования в методе особенностей человеческого зрения, при правильном выборе коэффициента энергии встраивания, вложение визуально не обнаруживается. В работе показано, что наилучшие характеристики по стойкости и минимальной разности с контейнером-оригиналом для данного метода можно получить при $\upsilon \approx 0{,}1\text{-}0{,}15$ и $\tau \in [3, 10]$.

Научная новизна полученных результатов заключается в том, что впервые получены характеристики модифицированного метода на основе замены НЗБ. Для метода Куттера-Джордана-Боссена оценены параметры, при которых метод обладает наименьшей уязвимостью к обнаружению стеганограммы.

Практическая значимость полученных результатов заключается в возможности их применения для скрытой передачи информации с высокой надежностью и стойкостью к обнаружению, а также для обеспечения защиты авторских прав на информацию, защиты от нелицензионного копирования и тиражирования.

Литература

1. Основи комп'ютерної стеганографії [Текст]: навчальний посібник для студентів і аспірантів / В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук. – Вінниця: ВДТУ, 2003. – 143 с.

2. Грибунин, В.Г. Цифровая стеганография [Текст] / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: Солон-Пресс, 2002. – 272с.

3. Конахович, Г.Ф. Компьютерная стеганография. Теория и практика [Текст] / Г.Ф. Конахович, А.Ю. Пузіренко. – К.: МК-Пресс, 2006. – 288 с.

4. Аграновский, А.В. Стеганография, цифровые водяные знаки и стеганоанализ [Текст]: учеб. пособие для вузов / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин. – М.: Вузовская книга, 2009. – 220 с.

5. Вовк, О.О. Дослідження та порівняльна характеристика методів вбудовування інформації для прихованої передачі у мережах зв'язку [Текст] / О.О. Вовк, А.А. Астраханцев // Всеукр. конкурс студентських наукових робіт з природничих, технічних та гуманітарних наук (галузь знань "Інформаційна безпека"): збірник тез доповідей – Львів,НУ «ЛП», 20-23 березня 2012. – С. 4.

Поступила в редакцию 11.06.2012

Рецензент: д-р техн. наук, проф., зав. кафедры "Приема, передачи и обработки сигналов" А.А. Зеленский, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

ДОСЛІДЖЕННЯ СТІЙКОСТІ МЕТОДІВ ПРИХОВУВАННЯ ІНФОРМАЦІЇ У НЕРУХОМИХ ЗОБРАЖЕННЯХ

О.О. Вовк, А.А. Астраханцев, О.В. Дорожан

Останні роки стеганографія є причиною багатьох дискусій. Все більший інтерес до неї зростає саме як до ефективного методу приховання даних, що дозволяє зберігати конфіденційність інформації. У роботі проводилася оцінка стійкості і надійності методів приховання інформації в просторовій області нерухомих зображень. За допомогою якісних і кількісних характеристик були визначені оптимальні значення показників для методів на основі заміни найменш значущих бітів зображення і методу Куттера-Джордана-Боссена. Встановлювалася доцільність використання розглянутих методів для різних стеганосистем.

Ключові слова: візуальні показники спотворення, метод НЗБ, метод Куттера-Джордана-Боссена, ЦВЗ, стеганосистема.

INVESTIGATION OF STABILITY OF INFORMATION HIDING METHODS IN STILL IMAGES

O.O. Vovk, A.A. Astrahancev, A.V. Dorozhan

Steganography is the cause of many discussions in recent years. Great interest to it increases exactly as to the effective method of hiding data, which allows maintaining the confidentiality of information. In this work estimation of stability and reliability of information hiding methods in the spatial area of still images was made. By means of qualitative and quantitative characteristics were determined optimal values for methods based on the replacement of the least significant bits of the image and Cutter-Jordan-Bossens method. Expediency of usefulness of the considered methods was determined for various stegosystems.

Keywords: visual indicators of distortion, method of LSB, Cutter-Jordan-Bossens method, digital watermark, steganosystem.

Вовк Олеся Олеговна – магистрант кафедры "Сети связи", Харьковский национальный университет радиоэлектроники**,** Харьков, Украина, e-mail: lisfo4ka@gmail.com.

Астраханцев Андрей Анатольевич – канд. техн. наук, доцент кафедры "Сети связи", Харьковский национальный университет радиоэлектроники**,** Харьков, Украина, e-mail: astrahkture@mail.ru.

Дорожан Алексей Валерьевич – аспирант кафедры "Телекоммуникационные системы", Харьковский национальный университет радиоэлектроники**,** Харьков, Украина, e-mail: aleksey.dorozhan@datagroup.ua.