УДК 004.056.5

О.В. Костырка,
аспирант Академии пожарной безопасности
им. Героев Чернобыля,
М.А. Мельник,
В.Н. Рудницкий,
доктор технических наук, профессор

СТЕГАНОПРЕОБРАЗОВАНИЕ ПРОСТРАНСТВЕННОЙ ОБЛАСТИ ИЗОБРАЖЕНИЯ-КОНТЕЙНЕРА, УСТОЙЧИВОЕ К СЖАТИЮ

В работе разработан стеганографический алгоритм, реализующий стеганометод, предложенный авторами ранее. Этот алгоритм, осуществляя погружение дополнительной информации в пространственной области контейнера-изображения, является устойчивым к атаке однократным и двукратным сжатием, обеспечивает приемлемое качество стеганосообщения, имеет малую вычислительную сложность: является полиномиальным степени 2. Характеристики алгоритма не зависят от формата используемого изображения-контейнера.

За счет отсутствия необходимости перехода в область преобразования контейнера при организации погружения/декодирования дополнительной информации повышена эффективность разработанного стеганоалгоритма, по сравнению с аналогом, осуществляющим погружение конфиденциальной информации в области сингулярного разложения матрицы основного сообщения.

***Ключевые слова**: стеганопреобразование, атака сжатием, контейнер-изображение, пространственная область изображения, сингулярное число.*

У роботі розроблений стеганографічний алгоритм, що реалізує стеганометод, запропонований авторами раніше. Цей алгоритм, здійснюючи вбудову додаткової інформації в просторовій області контейнера-зображення, є стійким до атаки одноразовим і дворазовим стиском, забезпечує прийнятну якість стеганоповідомлення, має малу обчислювальну складність: є поліноміальним ступеня 2. Характеристики алгоритму не залежать від формату використовуваного зображення-контейнера.

За рахунок відсутності необхідності переходу в область перетворення контейнера при організації вбудови/декодування додаткової інформації підвищена ефективність розробленого стеганоалгоритма, у порівнянні з аналогом, що здійснює вбудову конфіденційної інформації в області сингулярного розкладання матриці основного повідомлення.

***Ключові слова**: стеганоперетворення, атака стиском, контейнер-зображення, просторова область зображення, сингулярне число.*

The paper is devoted to the development of a new steganographic algorithm, based on the previous developed method. Developed method embeds an additional information in spatial domain of cover-image. This algorithm is robust against compression attacks and enforces the reliability perception of stegano message, and is a polynomial of degree 2. Characteristics of the algorithm does not depend on the image format.

***Keywords**: stegano transformation, compression attack, cover-image, spatial domain, singular value.*

Введение

Современное развитие информационных технологий привело к повышению актуальности вопроса информационной безопасности. Сегодня решение этого вопроса немыслимо без создания комплексных систем защиты информации [1], которые наряду с законодательными, морально-этическими, физическими, административными, техническими, программными мерами, включают в себя меры криптографические и стеганографические [2]. Единая концепция защиты, основанная на комплексном применении всех имеющихся методов и средств [3], определяет основные требования к комплексным системам защиты информации, среди которых:

- использование комплекса программно-технических средств и организационных мер;
- надежность, производительность, конфигурируемость;
- экономическая целесообразность;
- возможность совершенствования;
- обеспечение разграничения доступа к конфиденциальной информации с отвлечением нарушителя на ложную информацию;
- взаимодействие с незащищенными компьютерными сетями по установленным для этого правилам разграничения доступа;
- обеспечение проведения учета и расследования случаев нарушения безопасности информации в компьютерных сетях и т.д.

Дальнейшее совершенствование теории защиты информации очевидно связано с учетом новых обстоятельств, характерных для современного периода развития, среди которых повышенное внимание к развитию методов стеганографии.

В качестве контейнеров в современной компьютерной стеганографии часто используются цифровые изображения (ЦИ), что сделано и в настоящей работе, а также цифровые видео и аудио файлы, целесообразность чего подробно обсуждается в [4; 5].

В процессе стеганопреобразования (СП) дополнительная информация (ДИ) погружается в контейнер, или основное сообщение (ОС), при этом может использоваться как пространственная область (ПО) ЦИ-контейнера, так и его области преобразования (ОП). В [6] показано, что пространственная область ОС обладает рядом преимуществ при организации СП. Однако существовавшее долгое время мнение о том, что для обеспечения устойчивости стеганоалгоритма к возмущающим воздействиям СП целесообразно проводить в области преобразования контейнера, в частности, в частотной, незаслуженно отодвигало пространственную область на “непризовые” места при разработке упомянутых алгоритмов [4; 7].

Цель статьи и постановка заданий

В [8] был разработан новый стеганографический метод, устойчивый к возмущающим воздействиям, осуществляющий погружение дополнительной информации в пространственной области изображения-контейнера, основанный на достаточном условии такой устойчивости, полученном в [9]. Достаточное условие сводится к обеспечению устойчивости за счет организации СП путем корректировки яркости пикселей каждого $l \times l$-блока B ЦИ-контейнера, полученного путем стандартного разбиения его матрицы на значение Δb, которое удовлетворяет следующему условию:

$$|\Delta b| = \left| \frac{\Delta \sigma_1}{l} \right| > \frac{\left\| \Delta \overline{B} \right\|_2}{l}, \qquad (1)$$

где $\Delta \sigma_1$ – возмущение максимального сингулярного числа блока B при СП, а $\left\| \Delta \overline{B} \right\|_2$ – спектральная норма матрицы предполагаемого возмущения блока СС.

Обеспечение устойчивости стеганоалгоритма к конкретным возмущающим воздействиям будет определяться конкретным выбором значения Δb, для чего необходима оценка величины $\left\| \Delta \overline{B} \right\|_2$.

В настоящей работе в качестве возмущающего воздействия рассматривается атака сжатием на СС. Эта атака является очень распространенной в настоящий момент в силу широкого использования форматов с потерями для хранения и передачи информации.

Целью настоящей работы является разработка полиномиального стеганоалгоритма, реализующего предложенный в [8] метод, устойчивого к атаке сжатием, обеспечивающего надежность восприятия СС.

Для достижения поставленной цели работы необходимо решить следующие *задачи*:

1. определить размер блоков l, на которые целесообразно разбивать матрицу ОС при СП;
2. получить оценку $\left\| \Delta \overline{B} \right\|_2$ для атаки сжатием с различными коэффициентами качества QF;
3. определить конкретное значение Δb с учетом выбранного размера блока l и полученной оценки возмущения блока $\left\| \Delta \overline{B} \right\|_2$;
4. разработать стеганоалгоритм, реализующий метод из [8];
5. исследовать эффективность разработанного стеганоалгоритма в условиях сжатия с различными коэффициентами качества QF;
6. исследовать эффективность разработанного стеганоалгоритма в условиях повторного сжатия;
7. провести сравнение эффективности разработанного алгоритма с современными аналогами.

Основная часть

Пусть F, $\overline{F}$ – $m \times m$-матрицы ОС, СС соответственно, $b_1, b_2, ..., b_t$; $\overline{b}_1, \overline{b}_2, ..., \overline{b}_t$ – соответственно погруженная и извлеченная ДИ, представляющая из себя бинарную последовательность.

В [10] было получено достаточное условие устойчивости стеганоалгоритма к сжатию (к возмущающим воздействиям), на основании которого в [11] был разработан устойчивый стеганоалгоритм, осуществляющий погружение ДИ в области преобразования контейнера − области сингулярного разложения матриц блоков ОС, полученных путем стандартного разбиения. СП осуществлялось при помощи возмущения максимальных сингулярных чисел блоков.

Результаты, полученные в [10], явились основой для достаточного условия устойчивости стеганоалгоритма, полученного в [9], реализуемые в пространственной области ЦИ-контейнера, а алгоритм, предложенный в настоящей работе, является усовершенствованием алгоритма из [11]. Основная идея ожидаемого повышения эффективности декодирования ДИ разрабатываемым алгоритмом, называемым ниже *SS_J*, заключается в отсутствии необходимости осуществления перехода:

$$ПО \rightarrow ОП \rightarrow ПО \qquad (2)$$

в процессе погружения/декодирования ДИ, что уменьшает вычислительную погрешность стеганографического процесса в целом (кроме того, уменьшает и вычислительную сложность на $\underline{O}\left(m^2\right)$ операций при организации процесса СП поблоково).

Величина размера блока l является существенной при организации СП рассматриваемым методом. Поскольку разрабатываемый алгоритм нацелен на устойчивость к сжатию, а наиболее распространенным форматом с потерями на сегодняшний день является Jpeg, который в процессе сжатия разбивает ЦИ на 8×8-блоки, то для возможности наиболее тщательного контроля и анализа происходящих в процессе сжатия СС изменений яркости пикселей, положим l=8.

В [10] была получена оценка величины возмущающего воздействия блока при сжатии ЦИ с коэффициентами качества $QF \geq 60$: $\left\|\Delta\overline{B}\right\|_2 < 72$. Использование этого результата с учетом (1) определяет значение $\Delta b = 9$, которое должно гарантировать высокую эффективность разрабатываемого алгоритма для $QF \geq 60$.

Обозначим матрицу размерами 8×8, имеющую вид:

$$\Delta B = \begin{pmatrix} \Delta b & \Delta b & \dots & \Delta b \\ \Delta b & \Delta b & \dots & \Delta b \\ \dots & \dots & \dots & \dots \\ \Delta b & \Delta b & \dots & \Delta b \end{pmatrix}.$$

Основные шаги алгоритма *SS_J* выглядят следующим образом.

Стеганопреобразование.

1. $m \times m$ − матрица ЦИ-контейнера F разбивается на $K = \left[\frac{m}{8}\right] \times \left[\frac{m}{8}\right] 8\times 8$ − блоков, где $[\bullet]$ − целая часть аргумента.

2. Пусть B − очередной блок ОС, используемый для СП, а b_i − очередной бит ДИ, $\overline{B}$ − соответствующий блок стеганосообщения.

Если

$$b_i = 1,$$

то

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

иначе

$$\overline{\overline{B}} = B - \Delta B.$$

Извлечение ДИ

1. Матрицы F контейнера и $\overline{\overline{F}}$ возможно возмущенного СС разбиваются на 8×8 − блоки. Каждый блок СС используется для извлечения 1 бита ДИ.

2. Пусть $\overline{\overline{B}}$ − очередной блок СС, из которого извлекается бит $\overline{b}_i$ ДИ, а B − соответствующий ему блок ОС.

2.1. Определить:

$$\Delta B = \overline{\overline{B}} - B.$$

2.2. Определить количество положительных k_p и отрицательных k_n элементов в матрице ΔB.

если

$$k_p > k_n,$$

то

$$\overline{b}_i = 1,$$

иначе

$$\overline{b}_i = 0.$$

Вычислительная сложность *SS_J* определяется количеством 8×8 − блоков, на которые разбивается $m \times m$ − матрица контейнера/стеганосообщения, и составляет $\left\lceil \frac{m}{8} \right\rceil \left\lceil \frac{m}{8} \right\rceil = \underline{O}\left(m^2\right)$ операций.

Для проверки эффективности разработанного стеганоалгоритма в среде Matlab был проведен вычислительный эксперимент, в котором были задействованы 250 ЦИ размером 1000×1000 пикселей (цветовая схема RGB) в форматах как с потерями (Jpeg), так и без потерь (Tif) из базы NRCS [12], а также полученные непрофессиональными фотографами. В качестве матрицы F при СП использовалась синяя составляющая изображения-контейнера. После погружения ДИ стеганосообщение сохранялось сначала в формате без потерь (Tif), после чего определялась характеристика визуального искажения ЦИ в результате СП. Это происходило стандартным образом при помощи определения *PSNR* − пикового отношения "сигнал-шум", получаемого в децибелах (dB) [7]:

$$PSNR = 10 \cdot \log_{10}\left(255^2 \Big/ \left(\frac{1}{m^2} \sum_{i,j}^{m} \left(f_{ij} - \overline{f}_{ij} \right)^2 \right) \right), \qquad (3)$$

где f_{ij}, $\overline{f}_{ij}$, $i, j = \overline{1,m}$, – элементы матриц F и $\overline{F}$ соответственно (предварительно ЦИ из цветовой схемы RGB переводилось в цветовую схему YCbCr, после чего в (3) анализировалась Y – матрица яркости [13]). *PSNR*, отражающий искажение ОС в процессе СП, равнялся здесь в среднем 49 dB, независимо от формата контейнера, что рассматривается в литературных источниках как значение, характеризующее приемлемое качество ЦИ [7].

Следующий этап вычислительного эксперимента состоял в моделировании атаки сжатием на СС путем его пересохранения в формат с потерями (Jpeg, Jpeg2000) с разными коэффициентами качества $QF \in \{30,40,50,60,70,80,90\}$. Визуальные искажения, которые претерпевали СС в процессе атак, оценивались при помощи *PSNR*, вычисляемого по матрицам исходного (формат Tif) и возмущенного (формат Jpeg) СС. Результаты эксперимента, говорящие о высокой абсолютной эффективности *SS_J*, которая оценивалась стандартным образом по значению коэффициента корреляции (*NC*) [14]: $NC = \left(\sum_{i=1}^{t} b_i' \times \overline{b}_i' \right) \Big/ t$, где $b_i' = 1, \overline{b}_i' = 1$, если $b_i = 1, \overline{b}_i = 1$, и $b_i' = -1, \overline{b}_i' = -1$, если $b_i = 0, \overline{b}_i = 0$, приведены в табл. 1, 2. Результаты, представленные на рис. 1, наглядно показывают, что основным параметром, от которого зависит эффективность декодирования ДИ разработанным алгоритмом в условиях сжатия с потерями, является величина возмущающего воздействия (оцениваемая по значению *PSNR*), которое претерпевает СС в процессе атаки. Действительно, значения *NC* при близких значениях *PSNR* также близки для обоих вариантов проведения атаки (сохранение СС в Jpeg, Jpeg2000), несмотря на различные математические основы этих сжатий – дискретное косинусное преобразование (Jpeg), дискретное вейвлет-преобразование (Jpeg2000).

Таблица 1

Результаты декодирования ДИ алгоритмом в условиях атаки сжатием на СС путем пересохранения в формат Jpeg

QF	30	40	50	60	70	80	90
NC	0.946	0.969	0.981	0.987	0.988	0.989	0.991
PSNR	35	37	38	39	41	43	45

Таблица 2

Результаты декодирования ДИ алгоритмом в условиях атаки сжатием на СС путем пересохранения в формат Jpeg2000

QF	40	60	70	80	90
NC	0.782	0.947	0.980	0.990	0.992
PSNR	33	36	39	43	44

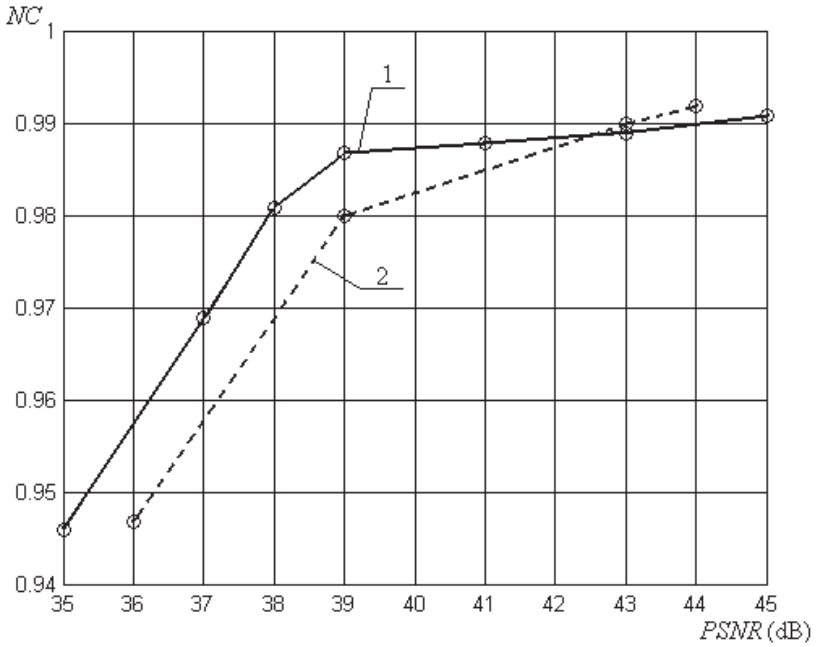


Рис. 1. Зависимость эффективности декодирования алгоритма *SS_J* в условиях атаки сжатием путем сохранения СС в формат с потерями: 1 – Jpeg; 2 – Jpeg2000

Для сравнительной оценки эффективности разработанного алгоритма использовался стеганоалгоритм *A*1 [11]. Результаты отражены на рис. 2, из которых видно, что разработанный алгоритм действительно превосходит свой аналог, взятый за основу, по эффективности, что и предполагалось выше. Причиной этому, очевидно, является использование пространственной области контейнера для погружения ДИ, что повлекло за собой уменьшение накопления вычислительной погрешности.

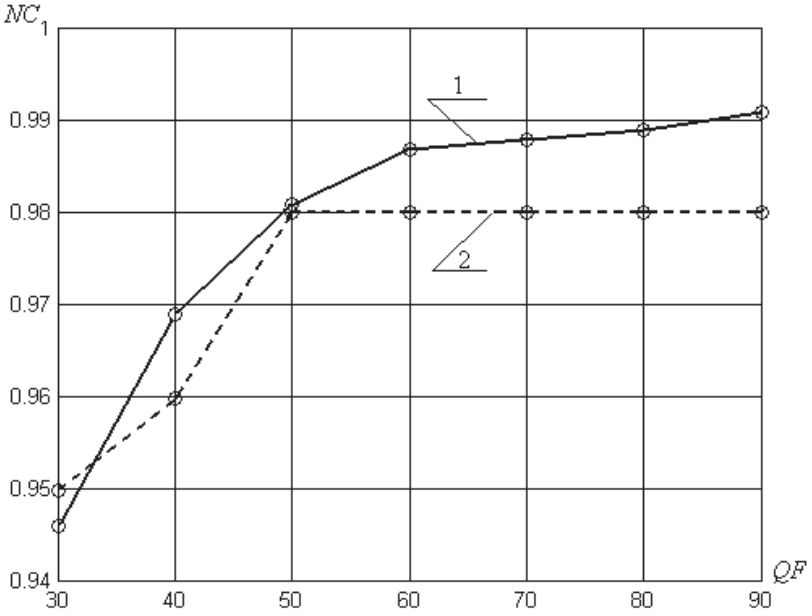
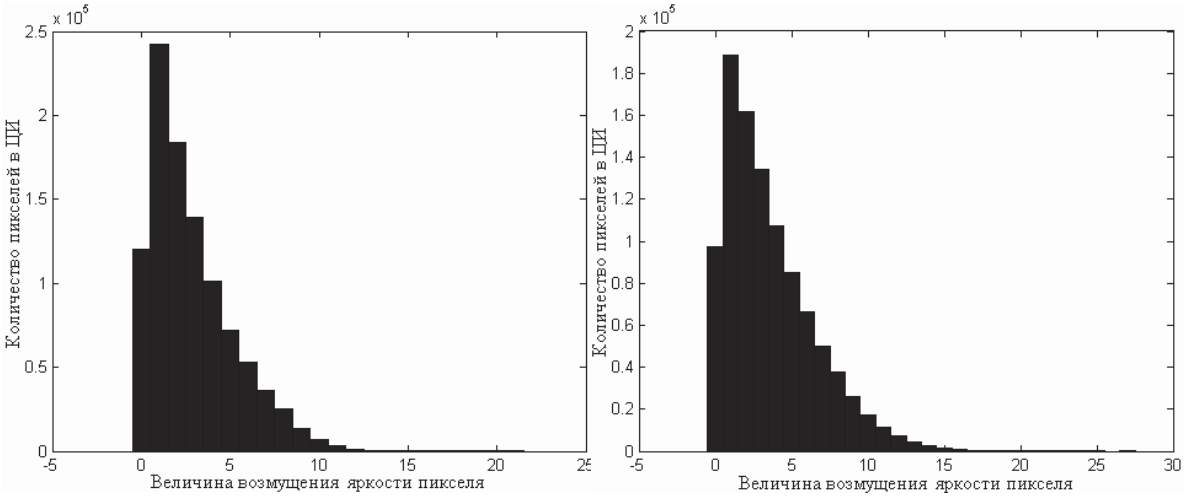


Рис. 2. Результаты декодирования ДИ в зависимости от коэффициента качества сжатия СС: 1 – стеганоалгоритмом *SS_J*; 2 – стеганоалгоритмом *A*1

По результатам проведенного эксперимента очевидной есть высокая эффективность разработанного стеганографического алгоритма *SS_J*, оцениваемая при помощи коэффициента *NC*.

В настоящий момент передача информации, в том числе ЦИ, по каналам коммуникаций происходит, как правило, в сжатом виде. Поэтому сама передача ЦИ в форматах без потерь в большей или меньшей мере привлекает к себе внимание. Это говорит о том, что СС еще на стадии его формирования для увеличения вероятности нераскрытия стеганографического канала связи имеет смысл сохранять в формат с потерями (Jpeg), т.е. для СП сегодня целесообразно всегда использовать стеганоалгоритмы, устойчивые к сжатию, каким является алгоритм *SS_J*, разработанный в настоящей работе. Чаще всего ЦИ сохраняются в Jpeg с QF = 80,90, что соответствует хорошему визуальному качеству изображения и отвечает сравнительно малому объему памяти для хранения. Если предположить в такой ситуации атаку сжатием на СС, проводимую противником, то для исходного СС (сохраненного без потерь) это сжатие будет повторным, поэтому используемый стеганоалгоритм должен быть устойчивым не только к первичному, но и к повторному сжатию. Проверим, на сколько возмущаются пиксели ЦИ (значения яркости в цветовой матрице синего цвета (схема RGB)) при сжатии с QF = 80,90. Как показывает вычислительный эксперимент для подавляющего большинства пикселей их возмущения не превосходят 4, и лишь малая часть пикселей претерпевает возмущения, величина которых больше 9, что с учетом выбранного значения $\Delta b = 9$ говорит о том, что даже после первичного сжатия СС, сформированное *SS_J* остается малочувствительным ко вторичному, поскольку для подавляющего большинства пикселей ЦИ знак их возмущений, произошедших в ходе СП, при первичном сжатии измениться не мог. Типичные картины количественного распределения различных значений возмущений яркости пикселей для QF = 80,90 соответственно представлены на рис. 3.



а б

Рис. 3. Типичный пример гистограмм значений возмущений яркости пикселей изображения при сжатии: а – QF = 90; б – QF = 80

Таким образом, проведенный вычислительный эксперимент дает возможность предположить высокую эффективность разработанного стеганоалгоритма в

условиях повторного сжатия СС противником. Для практического подтверждения этой гипотезы в среде Matlab был проведен вычислительный эксперимент, где СС (первоначально сохраненные в формате без потерь) подвергались сначала первичному сжатию с $QF = 80,90$, а затем вторичному с $QF = 50,70,90$. Результаты, полностью подтверждающие высокую эффективность алгоритма *SS_J* в условиях двукратного сжатия, приведены в табл. 3.

Таблица 3

Результаты декодирования ДИ (значение *NC*) разработанным стеганоалгоритмом *SS_J* в условиях повторного сжатия СС

Вторичное сжатие / Первичное сжатие	$QF = 50$	$QF = 70$	$QF = 90$
$QF = 90$	0.967	0.984	0.988
$QF = 80$	0.964	0.984	0.986

Заключение

В работе разработан новый стеганографический алгоритм *SS_J*, реализующий стеганометод, предложенный в [8]. Разработанный алгоритм, осуществляя погружение ДИ в пространственной области контейнера-изображения, является устойчивым к атаке сжатием, в том числе двукратным, обеспечивает приемлемое качество СС (в результате СП $PSNR \approx 49\ dB$ независимо от формата контейнера), является полиномиальным степени 2.

За счет отсутствия необходимости перехода (2) при организации погружения/декодирования ДИ эффективность разработанного алгоритма выше, чем у его “ближайшего” аналога – алгоритма, обеспечивающего нечувствительность СС в области сингулярного разложения соответствующих матриц контейнера, основной математический принцип работы которого был взят за основу при разработке метода в [8].

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Ленков С.В.* Методы и средства защиты информации : в 2 т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – К. : Арий, 2008. – Т. 2 : Информационная безопасность. – 344 с.

2. *Хорошко В.А.* Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – К. : Юниор, 2003. – 501 с.

3. *Хорев П.Б.* Методы и средства защиты информации в компьютерных системах / П.Б. Хорев. – Изд-во “Академия”, 2005. – 256 с.

4. *Грибунин В.Г.* Цифровая стеганография : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М. : СОЛОН-Пресс, 2002. – 272 с.

5. Стеганография, цифровые водяные знаки и стеганоанализ : монография / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. – М. : Вузовская книга, 2009. – 220 с.

6. *Костырка О.В.* Анализ преимуществ пространственной области цифрового изображения-контейнера для стеганопреобразования / О.В. Костырка // Інформатика та математичні методи в моделюванні. – 2013. – Т. 3, № 3. – С. 220–227.

7. *Конахович Г.Ф.* Компьютерная стеганография: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – К. : МК-Пресс, 2006. – 288 с.

8. *Рудницький В.М.* Стійке стеганоперетворення в просторовій області зображення-контейнера / В.М. Рудницький, О.В. Костирка // Інформатика та математичні методи в моделюванні. – 2013. – Т. 3, № 4. – С. 320–327.

9. *Кобозева А.А.* Условия обеспечения устойчивости стеганоалгоритма при организации стеганопреобразования в пространственной области контейнера-изображения / А.А. Кобозева, О.В. Костырка // Інформаційна безпека. – 2013. – № 4. – С. 57–65.

10. *Кобозева А.А.* Формальные условия обеспечения устойчивости стеганометода к сжатию / А.А. Кобозева, М.А. Мельник // Сучасна спеціальна техніка. – 2012. – № 4 (31). – С. 60–69.

11. *Мельник М.А.* Стеганоалгоритм, устойчивый к сжатию / М.А. Мельник // Інформаційна безпека. – 2012. – № 2 (8). – С. 99–106.

12. NRCS Photo Gallery : United States Department of Agriculture. Washington, USA [Электронный ресурс]. – Режим доступа : http : // photogallery.nrcs.usda.gov.

13. PSNR : MathWorks. Documentation Center. The MathWorks, Inc. USA [Электронный ресурс]. – Режим доступа : http : // www.mathworks.com/help/vision/ref/psnr.html.

14. *Lin W.-H.* A blind watermarking method using maximum wavelet coefficient quantization / W.-H. Lin et al. // Expert Systems with Applications. – 2009. – Vol. 36, Iss. 9. – PP. 11509–11516.

Отримано 28.01.2014