УДК 004.932 **DOI:10.18413/2518-1092-2017-2-4-59-66**

Буханцов А.Д.[1]
Дружкова И.В.[1]
Кулешов С.И.[2]
Киселёв Ю.И.[1]

ИССЛЕДОВАНИЕ АЛГОРИТМОВ СКРЫТНОГО ВНЕДРЕНИЯ ИНФОРМАЦИИ В ПРОСТРАНСТВЕННЫЕ КОМПОНЕНТЫ МОНОХРОМНОГО ИЗОБРАЖЕНИЯ

[1)] Белгородский государственный национальный исследовательский университет, ул. Победы д. 85, г. Белгород, 308015, Россия
[2)] Администрация Губернатора Белгородской области, отдел информационной безопасности, пл. Соборная д. 4, г. Белгород, 308005, Россия

e-mail: bukhantsov@bsu.edu.ru, 984546@bsu.edu.ru, Kulechov27@mail.ru, 842884@bsu.edu.ru

Аннотация
Реальные изображения не являются случайным процессом с равномерным распределением, поэтому использование их как контейнеров в стенографическом кодировании является актуальной задачей. Для использования свойств изображений применяются неформатные методы кодирования. В данной статье предлагается рассмотреть следующий неформатный метод стеганографии: кодирование в субполосах изображения, где информация побитно кодируется в изображение, внося изменения в ограниченную субполосу стегоконтейнера, используя ограниченное количество её коэффициентов, выбор которых подчиняется реализованному алгоритму. Данный метод рассматривается в сравнение с распространённым методом скрытного внедрения информации в изображение с помощью расширения спектра, в котором информационное сообщение побитно модулируется путем умножения на ансамбль ортогональных сигналов.
Ключевые слова: оценка эффективности; мультимедийные данные; качество облуживания сети; качество восприятия.

UDC 004.932

Bukhantsov A.D.[1]
Druzhkova I.V.[1]
Kuleshov S.I.[2]
Kiselyov Y.I.[1]

RESEARCH OF ALGORITHMS CONCEALED INTRODUCTION OF DATA IN GRAYSCALE IMAGES SPATIAL DOMAIN

[1)] Belgorod State National Research University, 85 Pobedy St., Belgorod, 308015, Russia
[2)] Administration of the Gubernator of the Belgorod Region, Information Security Department, 4 Sobornaya Sq., Belgorod, 308005, Russia

e-mail: bukhantsov@bsu.edu.ru, 984546@bsu.edu.ru, Kulechov27@mail.ru, 842884@bsu.edu.ru

Abstract
Real images are not a random image with a uniform distribution, so using them as containers in steganography coding is an actual task. Non-formatting encoding methods use image properties. This article proposes to consider the following non-formatting method of steganography: encoding in sub-bands of an image where information is bit-coded in an image, including a limited sub-band of an image container, using a limited number of its coefficients, the choice of which obeys the implemented algorithm. This method is considered in a comparative analysis using the spread spectrum, in which the information message is bit by bit modulated by multiplying by an ensemble of orthogonal signals.
Keywords: steganography; image; subband analysis; spreading method.

В настоящее время задача надежной защиты информации от несанкционированного доступа посредством стеганографии является актуальной в связи с изменяемостью требований и ростом возможностей взлома. Пересекаясь с такой же актуальной задачей как сжатие информации, цель данной задачи не только в ограничении доступа к информации, но и в увеличении объема конфиденциальной информации в контейнере [5].

Таким образом, данные задачи привели к разработке новых стенографических методов, предназначенных для обеспечения безопасности передачи данных по каналам телекоммуникаций. Большинство исследований направлено на использование в качестве контейнеров стенографического кодирования изображений. Учитывая неточности устройств оцифровки и избыточность таких контейнеров, появляется возможность использовать пространственные компоненты изображений для внедрения информации.

В отличие от криптографии, которая скрывает содержимое тайного сообщения, стеганография скрывает сам факт его существования. То есть, преимущество стеганографии над чистой криптографией состоит в том, что сообщения не привлекают к себе внимания.

В данной статье сравниваются разработанный неформатный метод стеганографии: кодирование в субполосах изображения, который при преобразовании изображения используют его свойства, и такой же неформатный метод: метод расширения спектра. Неформатные методы – это методы, использующие непосредственно сами данные изображения [4]. Применение неформатных методов неизбежно приводит к появлению искажений, вносимых стеганографической системой, однако при этом они являются более стойкими к атакам как пассивных, так и активных противников.

В алгоритме стеганографического кодирования в субполосах изображения информационное сообщение побитно внедряется в субполосы стегоконтейнера.

Реальные изображения не являются случайным процессом с равномерным распределением. Известно, что большая часть энергии изображений сосредоточена в низкочастотной части спектра. Поэтому и необходимо декомпозировать изображения на субполосы. Низкочастотные субполосы содержат большую часть энергии изображения и, следовательно, носят шумовой характер. Высокочастотные субполосы наиболее подвержены воздействию со стороны различных алгоритмов обработки, будь то сжатие или НЧ фильтрация. Таким образом, для вложения сообщения наиболее подходящими кандидатами являются среднечастотные субполосы спектра изображения [1,6-10].

Вычисление энергетического спектра изображения позволяет получить представление о распределении его энергии по так называемым частотным интервалам. Известно, что алгоритмы, использующие преобразование Фурье и БПФ, не позволяют вычислять точные значения энергетических характеристик в заданных частотных интервалах. Умение точно определять долю энергии изображения в отдельном частотном диапазоне обеспечивает возможность более качественного выбора параметров различных преобразований визуальной информации. Это и обеспечивает субполосные преобразования [1].

Контейнер-изображение будет рассматриваться как массив данных C размерностью $M \cdot N$, разбитый на квадратные подблоки C_i размером $S = 64$. В качестве элементов массива C будут выступать несжатые растровые данные полутонового изображения.

Так как в данной работе будут использоваться квадратные подблоки, то необходимость в использовании второй субполосной матрицы по оси ординат не имеет смысла. Поэтому далее будет описываться алгоритм без учета построения второй субполосной матрицы.

Частотное пространство предлагается неравномерно разбить на субинтервалы каждый подблок стегоконтейнера в соответствии с выражениями [4]:

$$(2\mathrm{R}+1)\Omega_0 = \pi, \quad (1)$$

где R – количество частотных интервалов и $R = \frac{n-2}{4}$; Ω_0 – нулевой частотный интервал частотного пространства и $\Omega_0 = \frac{2\pi}{S}$.

Ширина остальных частотных интервалов, не считая нулевого, является вдвое большей и равна:

$$\Omega = \frac{4\pi}{S} \tag{2}$$

Для вычисления энергетического спектра изображения используется субполосная матрица $A = \{a_{ik}\}$ – симметричная матрица, элементы которой определяются:

$$a_{ik} = \begin{cases} \frac{\sin[\upsilon_2(i-k)] - \sin[\upsilon_1(i-k)]}{\pi(i-k)}, & i \neq k \\ \frac{\upsilon_2 - \upsilon_1}{\pi}, & i = k \end{cases} \tag{3}$$

Поскольку, матрица является симметрической, то данные матрицы можно представить, используя ее собственные числа и собственные векторы, в следующем виде:

$$A_r = Q^r L^r Q^{rT} \tag{4}$$

Так как матриц собственных векторов несколько, выбирается та матрица, у которой среднее значение энергии. Далее стеганографическое кодирование будет производится с помощью кодирования в знаки определенных коэффициентов матрицы q, полученной по следующей формуле:

$$q = Q^{rT} C_i Q^r \tag{5}$$

Выбор коэффициент был автоматизирован. Алгоритм будет рассмотрен ниже. В каждый найденный элемент внедряется информация по следующей формуле:

$$q_{ij} = q_{ij} \cdot e_k \tag{6}$$

где e_k – кодовое отображение двоичного бита контрольной информации, $e_k \in \{-1,1\}$, определяемое по формуле:

$$e_k = 2bit_k - 1, k = 1,..., K \tag{7}$$

где bit_k – бит информации в двоичной системе счисления, $bit_k \in \{0,1\}$; K – объем скрытно кодируемой информации.

Для процесса декодироваия вначале вычисляется обратное преобразование по формуле:

$$q = Q^r C_i Q^{rT} \tag{8}$$

Декодирование происходит аналогичным образом, то есть поиском определенных коэффициентов и извлечением из них знака:

$$\tilde{e}_k = sign(q_{ij}) \tag{9}$$

Решение о декодированном сигнале принимается в соответствии с выражением:

$$\tilde{b}it_k = \begin{cases} 0, \tilde{e}_k < 0 \\ 1, \tilde{e}_k > 0 \end{cases} \tag{10}$$

Выбор коэффициентов был автоматизирован с помощью следующего алгоритма:

1. Вычисляются абсолютные значения матрицы q.

2. Задается количество интервалов $100 \le I \le 500$ (оптимальные значения разбиения), на которые делится весь диапазон значений матрицы q.

3. Выбирается первый интервал, так как он всегда содержит наибольшее количество элементов.

4. Происходит поиск *nbit* (количество внедряемых бит в один подблок) элементов в матрице q по следующему алгоритму:

5. В каждый столбец кодируется не более $\frac{nbit}{S}$.

6. Происходит циклический поиск от диагонального элемента первых подходящих элементов, принадлежащих заданному интервалу.

7. В каждый найденный элемент внедряется информация по формуле (6-10).

В алгоритме стеганографического кодирования, основанного на методе расширения спектра, информационное сообщение побитно модулируется путем умножения на ансамбль ортогональных сигналов.

В данном случае разбиение контейнера на блоки может быть произвольным. Встраивание информационного сообщения осуществляется следующим образом: каждый бит сообщения сопоставляется с отдельным блоком контейнера-изображения [2].

Суть метода заключается в добавлении к изображению псевдослучайной последовательности (ПСП) в соответствии с выражением:

$$\tilde{C}_i = C_i + g \cdot e_k \cdot u, \tag{11}$$

где C_i – исходный подблок изображения; u – матрица размером $m \cdot n$, соответствующая ПСП; g – коэффициент, задающий энергию подблока изображения, куда встраивается бит; e_k – кодовое отображение двоичного бита внедряемой информации, определяемое по формуле (7).

Для уменьшения искажений в полученном стегоконтейнере, необходимо произвести фильтрацию на каждом подблоке:

$$\tilde{C}_i = \tilde{C}_i - \lambda \cdot u, \tag{12}$$

где λ – весовой коэффициент:

$$\lambda = \sum_{k=0}^{m-1} \sum_{j=0}^{n-1} \left(c_{kj} \cdot u_{kj} \right), \tag{13}$$

где c_{kj} – пиксель исходного подблока изображения $C_i = \{c_{kj}\}$, $k, j = 1, 2, .., S$.

Стоит отметить, что использование в качестве шума матрицы ПСП u, не обладающей взаимной энергией с данными, позволяет повысить помехоустойчивость стеганографически закодированной информации, а использование коэффициента проекции λ повышает скрытность информации.

На этапе извлечения данных нет необходимости владеть информацией о первичном контейнере. Операция декодирования заключается в восстановлении скрытого сообщения путем проецирования каждого блока, полученного стегоконтейнера, на все базисные функции. Поэтому для декодирования высчитывается только коэффициент λ, и далее аналогично применяются формулы (9) и (13=10).

Для исследования данных алгоритмов необходимо оценить их информационную скрытность и криптографическую стойкость.

Для оценки эффективности предоставленных алгоритмов предлагается использовать различные критерии оценок, каждый из которых обладает разной чувствительностью к различным изменениям. Существует множество таких критериев, наиболее известными из них являются: критерий минимума квадрата среднеквадратичного отклонения (MSE), пиковое отношение сигнала к шуму (PSNR), нормированная корреляция (NC). Ниже представлены эти формулы в соответствующем порядке:

$$MSE = \sqrt{\frac{\sum_{i=1}^{M}\sum_{k=1}^{N}\left(\tilde{f}_{ik} - f_{ik}\right)^2}{\sum_{i=1}^{M}\sum_{k=1}^{N} f_{ik}^{\ 2}}}, \quad (14)$$

где f_{ik} – пиксель исходного изображения $\Phi = \{f_{ik}\}$, $i = 1,2,..,M$, $k = 1,2,..,N$; $\tilde{\Phi}_{ik}$ – преобразованное изображение.

$$PSNR = 10\log_{10}\frac{MAX^2}{MSE}, \quad (15)$$

где MAX – это максимальное значение, принимаемое пикселем изображения. Когда пиксели имеют разрядность 8 бит, MAX = 255.

$$MSE = \frac{\sum_{i=1}^{M}\sum_{k=1}^{N}\tilde{f}_{ik}\cdot f_{ik}}{\sum_{i=1}^{M}\sum_{k=1}^{N} f_{ik}^{\ 2}} \quad (16)$$

Для сравнительного анализа производилось кодирование информации в изображения с помощью методов кодирования в субполосах и расширения спектра. Для вычислительного эксперимента были взяты аналогичные параметры для кодирования информации в изображении (табл. 1).

Таблица 1

Параметры кодирования

Table 1

Coding parameters

Параметры изображения	Значение	Параметры кодирования	Значение по методу кодирования в субполосах	Значение по методу расширения спектра
Размер изображения	512x512	Размер подблока изображения	64x64	8x8
Формат изображения	TIFF	Количество бит, кодируемое в одном подблоке	64	1
Глубина цвета	8 бит	Всего закодировано бит	4096	4096

При проведении эксперимента в изображения (рис. 1) были закодированы одинаковые последовательности бит, имеющие нормальный закон распределения.


Рис. 1. Шаблоны монохромного изображения: а) тестовое изображение «Lena» б) тестовое изображение «Cameraman»
Fig. 1. Patterns of grayscale image: a) test image «Lena» b) test image «Cameraman»

Таблица 2

Результаты оценки скрытности

Table 2

The results of assessment of stealthiness

Изображение	Метод	Оценки		
		MSE	PSNR	NC
№1	Субполосное кодирование	0.17838	55.61725	0.99999
	Расширение спектра	6.58521	39.94511	0.99987
№2	Субполосное кодирование	0.14879	56.40483	0.99999
	Расширение спектра	7.12655	39.60201	0.99983

С учетом функционального назначения стеганосистемы, вводятся следующие показатели эффективности для оценки ее стойкости:

Пропускная способность – отношение объема V встраиваемой в контейнер информации к общему объему $N \cdot M$ контейнера:

$$C = \frac{V}{N \cdot M} \tag{17}$$

Величина вносимых искажений как процентное отношение среднеарифметического всех абсолютных значений Δ-изменений данных контейнера к максимально возможному значению $\Delta_{\max}$:

$$I = \frac{100}{\Delta_{\max} \cdot N \cdot M} \cdot \sum_{i=1}^{N \cdot M} |\Delta_i|, \tag{18}$$

где Δ_i – Δ-изменения i-го элемента контейнера

Вероятность ошибочного извлечения информационных данных сообщения:

$$P_{ош} = \frac{V - V_{ош}}{N \cdot M}, \tag{19}$$

где $V_{ош}$ – объем ошибочно извлеченных данных.

В исследовании были использованы различные монохромные изображения, куда было закодировано 10^6 бит. Таким образом, полученные результаты по каждому изображению были усреднены.

Таблица 3

Результаты оценки стойкости

Table 3

The results of assessment of resistance

Показатель	Метод	
	Субполосное кодирование	Расширение спектра
Пропускная способность	до 0.04785	0.01563
Величина вносимых искажений	11.62646 %	18.70203 %
Вероятность ошибочного извлечения бита	0	0.00024

Кодирование в субполосах изображения и кодирование по методу расширения спектра позволяют осуществить встраивание информационных данных в неподвижные изображения для скрытной передачи и реализовать, таким образом, стеганографическую защиту информации.

Однако, свойства субполосных представлений позволяют говорить об их большей оптимальности для разработки алгоритмов стеганографического кодирования информации в изображении по сравнению с методом расширения спектра в связи с большей криптографической стойкостью и лучшими показателями скрытности.

Список литературы

1. Жиляков Е.Г., Веселых Н.К. Сжатие изображений на основе субполосного анализа/синтеза // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. 2014. №21-1 (192).

2. Жиляков Е. Г., Черноморец А.А., Лысенко И.В. Метод определения точных значений долей энергии изображений в заданных частотных интервалах // Вопросы радиоэлектроники. Сер. РЛТ. – 2007. – Вып. 4. – С. 115-123.

3. Жиляков Е.Г., Лихолоб П.Г., Медведева А.А. Исследование некоторых стеганографических алгоритмов // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. 2016. №2-1.

4. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – М.: МК-Пресс, 2006. – 288 с.

5. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М: Солон-Пресс, 2009. – 265 с.

6. Черноморец А. А., Голощапова В. А., Лысенко И. В., Болгова Е. В. О частотной концентрации энергии изображений // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. 2011. №1-1 (96).

7. Жиляков Е.Г., Черноморец А.А., Болгова Е.В., Гахова Н.Н. Исследование устойчивости стеганографии в изображениях // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. 2014. Т. 29. № 1-1 (172). С. 168-174.

8. Жиляков Е.Г., Черноморец А.А., Болгова Е.В., Гахова Н.Н. О субполосном внедрении информации в подобласти пространственных частот изображения-контейнера // Нейрокомпьютеры: разработка, применение. 2014. № 9. С. 85-87.

9. Жиляков Е.Г., Черноморец А.А., Болгова Е.В., Голощапова В.А. Оценка эффективности субполосного внедрения данных в изображени // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. 2014. Т. 30. № 8-1 (179). С. 200-206.

10. Жиляков Е.Г., Черноморец А.А., Болгова Е.В., Голощапова В.А. О субполосном внедрении в цветные изображения // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. 2015. Т. 33. № 1-1 (198). С. 158-162.

Reference

1. Zhilyakov E.G., Veselykh N.K. Image compression based on subband analysis / synthesis / Nauchnyye vedomosti Belgorodskogo gosudarstvennogo universiteta. Seriya: Ekonomika. Informatika. 2014. №21-1 (192).

2. Zhilyakov E.G., Chernomorets A.A., Lysenko I.V. The method of determining the exact values of the energy shares of images in given frequency intervals // Voprosy radioelektroniki. Ser. RLT. – 2007. – Vyp. 4. – S. 115-123.

4. Konakhovich GF, Puzyrenko A.Yu. Computer Steganography. Theory and practice. – Moscow: MK-Press, 2006. – 288 p.

5. Gribunin VG, Okov IN, Turintsev I.V. Digital steganography. – M: Solon-Press, 2009. – 265 p.

6. Chernomorets A. A., Goloshchapova V. A., Lysenko I. V., Bolgova Ye. V. About power concentration of images in spectral domain // Nauchnyye vedomosti Belgorodskogo gosudarstvennogo universiteta. Seriya: Ekonomika. Informatika. 2011. №1-1 (96).

7. Zhilyakov E.G., Chernomorets A.A., Bolgova E.V., Gakhova N.N. Investigation of steganography stability in images // Nauchnyye vedomosti Belgorodskogo gosudarstvennogo universiteta. Seriya: Ekonomika. Informatika. 2014. T. 29. № 1-1 (172). S. 168-174.

8. Zhilyakov E.G., Chernomorets A.A., Bolgova E.V., Gakhova N.N. On the subband introduction of information in the subregion of the spatial frequencies of the image container // Neyrokomp'yutery: razrabotka, primeneniye. 2014. № 9. S. 85-87.

9. Zhilyakov Ye.G., Chernomorets A.A., Bolgova E.V., Goloshchapova V.A. Estimation of the efficiency of subband introduction of data into images // Nauchnyye vedomosti Belgorodskogo gosudarstvennogo universiteta. Seriya: Ekonomika. Informatika. 2014. T. 30. № 8-1 (179). S. 200-206.

10. Zhilyakov E.G., Chernomorets A.A., Bolgova E.V., Goloshchapova V.A. On subband introduction in color images // Nauchnyye vedomosti Belgorodskogo gosudarstvennogo universiteta. Seriya: Ekonomika. Informatika. 2015. T. 33. № 1-1 (198). S. 158-162.

Буханцов Андрей Дмитриевич, кандидат технических наук, доцент, доцент кафедры информационно-телекоммуникационных систем и технологий

Дружкова Ирина Викторовна, студент кафедры информационно-телекоммуникационных систем и технологий

Киселёв Юрий Игоревич, магистр кафедры математического и программного обеспечения информационных систем

Кулешов Сергей Иванович, ведущий специалист-эксперт отдела информационной безопасности Администрации Губернатора Белгородской области г. Белгород

Bukhantsov Andrey Dmitrievich, candidate of technical sciences, associate professor, Department of information and telecommunication systems and technologies

Druzhkova Irina Viktorovna, student of the Department of Information and Telecommunication Systems and Technologies

Kiselev Yuri Igorevich, master of the Department of mathematical and software information systems

Kuleshov Sergey Ivanovich, leading expert-expert of the information security Department of the administration of the governor of the Belgorod Region, Belgorod