ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ
INFOCOMMUNICATION TECHNOLOGIES

УДК 004.932
DOI: 10.18413/2411-3808-2018-45-2-385-393

ИССЛЕДОВАНИЕ МОДИЦИФИЦИРОВАННОГО МЕТОДА КОДИРОВАНИЯ В СУБПОЛОСЫ МОНОХРОМНОГО ИЗОБРАЖЕНИЯ

RESEARCH OF MODIFIED METHOD OF CODING IN SUB-BANDS OF MONOCHROME IMAGE

А.Д. Буханцов, И.В. Дружкова
A.D. Bukhantsov, I.V. Druzhkova

Белгородский государственный национальный исследовательский университет,
Россия, 308015, г. Белгород, ул. Победы, 85

Belgorod State National Research University, 85 Pobeda St., Belgorod, 308015, Russia

E-mail: bukhantsov@bsu.edu.ru, 984546@bsu.edu.ru

Аннотация
В настоящее время задача надежной защиты информации от несанкционированного обращения посредством стеганографии является актуальной в связи с изменяемостью требований и ростом возможностей взлома. Использование изображений как контейнеров в стенографическом кодировании обусловлено избыточностью таких контейнеров. Для использования свойств изображений применяются неформатные методы кодирования. Применение неформатных методов неизбежно приводит к появлению искажений, вносимых стеганографической системой, однако при этом они являются более стойкими. В данной статье предлагается рассмотреть модификацию неформатного метода 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. Данная реализация метода рассматривается в сравнении с распространённым методом скрытного внедрения информации в изображение с помощью расширения спектра, в котором информационное сообщение побитно модулируется путем умножения на ансамбль ортогональных сигналов.

Abstract
Currently, the task of reliable protection of information from unauthorized access through steganography is relevant in connection with the variability of requirements and the growth of opportunities for hacking. The use of images as containers in stenographic coding is due to the redundancy of such containers. Non-formatting encoding methodsuse image properties and its use inevitably leads to distortions introduced by steganographic system, but at the same time they are more resistant. In this article, we consider the modification of non-formatting method of steganography: the encoding in the sub-bands of the image, where the information is bit-coded in the image, including the limited sub-band of the stack container, using a limited number of its coefficients, the choice of which obeys the implemented algorithm. This implementation of the research method in comparison with the method of the spread spectrum, in which the information message is bit by bit modulated by multiplying by an ensemble of orthogonal signals.

Ключевые слова: стеганография, изображение, субполосный анализ, метод расширения спектра.
Keywords: steganography, image, subband analysis, spreading method.

Теоретический анализ

Задача надежной защиты информации от несанкционированного обращения 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 обращения к информации, но и в увеличении объема конфиденциальной информации в контейнере [Грибунин и др., 2009].

Стеганография – это метод сокрытия сообщения в выбранный контейнер, так что никто, кроме получателей, не знает о его существовании [Provos, Honeyman, 2003]. Стеганографическая система является устойчивой к активным атакам, если встроенная информация не может быть заменена без значительных изменений контейнера [Хорошко и др., 2003]. При этом битовый состав стего-контейнера отличается от битового состава исходного контейнера, и это не должно обнаруживаться при помощи человеческих органов чувств и оказывать существенного влияния на работу телекоммуникационной системы [Жарких и др., 2009].

Большинство исследований направлено на использование контейнеров-изображений при стеганографическом кодировании. Это обусловлено рядом причин:

– в настоящий момент существует значимая с практической точки зрения задача защиты картин и фотографий от незаконного распространения и использования;

– современные форматы позволяют хранить изображения в хорошем качестве, для этого необходимо хранить большой объем информации об изображении и, следовательно, существует возможность встраивания сообщений большого объема [Alwan et al., 2005];

– размер контейнера заранее известен, встраивание не ограничено требованиями встраивания в режиме реального времени [Cox, 1997];

– в большинстве реальных изображений присутствуют области, имеющие шумовую структуру и хорошо подходящие для встраивания информации [Smith, Comiskey, 1996, Morkel, Eloff, 2005];

– система человеческого зрения слабо чувствительна к незначительным изменениям цветов изображения, яркости, контрастности, искажениям вблизи контуров и содержанию шумов;

– методы цифровой обработки изображений в настоящее время хорошо разработаны [Раткин, 2006].

Почти все цифровые форматы файлов могут использоваться для стеганографии, но более подходящие форматы – это те, которые имеют высокую степень избыточности [Sravanthi et al., 2012, Meghanathan, Nayak, 2010].

В данной статье исследуются неформатные методы стеганографии. Неформатные методы – это методы, использующие непосредственно сами данные, которыми изображение представлено в этом формате [Конахович, Пузыренко, 2006]. 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 [Жиляков и др., 2014, Черноморец и др., 2006].

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 [Жиляков, Веселых, 2014, Жиляков и др., 2016].

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 [Жиляков и др., 2014, Жиляков и др., 2015]:

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

где R – количество частотных интервалов и $\mathrm{R} = \frac{n-2}{4}$; 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:

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

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 декодирования вначале вычисляется обратное преобразование по формуле:

$$q = Q^r C_i Q^{rT} \quad (8)$$

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

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

Решение о декодированном сигнале принимается в соответствии с выражением:

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

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).

Для сравнительного анализа используется метод расширения спектра. В алгоритме стеганографического кодирования, основанного на методе расширения спектра, информационное сообщение побитно модулируется путем умножения на ансамбль ортогональных сигналов [Жиляков, Лихолоб, 2016].

Основное преимущество метода расширения спектра сравнительно высокая стойкость, поскольку скрываемая информация распределена в широкой полосе частот и ее трудно удалить без полного разрушения контейнера [Шелухин, Канаев, 2016].

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 [Жиляков, Черноморец, 2007].

Суть метода заключается в добавлении к изображению псевдослучайной последовательности (ПСП).

Исследование и его результаты

Для оценки эффективности предоставленного алгоритма предлагается оценить его скрытность и стойкость.

Для оценки скрытности существует множество критериев, наиболее известными из них являются: критерий минимума квадрата среднеквадратичного отклонения (MSE), пиковое отношение сигнала к шуму (PSNR), нормированная корреляция (NC).

$$MSE = \sqrt{\frac{\sum_{i=1}^{M}\sum_{k=1}^{N}\left(\tilde{f}_{ik} - f_{ik}\right)^2}{\sum_{i=1}^{M}\sum_{k=1}^{N} f_{ik}^{\ 2}}}, \quad (11)$$

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

$$PSNR = 10\log_{10}\frac{MAX^2}{MSE}, \tag{12}$$

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

$$MSE = \frac{\sum_{i=1}^{M}\sum_{k=1}^{N}\tilde{f}_{ik}\cdot f_{ik}}{\sum_{i=1}^{M}\sum_{k=1}^{N}f_{ik}^{\ 2}} \tag{13}$$

Для оценки скрытности было произведено кодирование информации в изображения с помощью метода кодирования в субполосах при параметрах, отраженных в таблице 1.

В качестве изображений для исследования были взяты стандартные тестовые изображения, широко используемого в научных работах для проверки и иллюстрации алгоритмов обработки изображений.

Таблица 1
Table 1

Параметры кодирования
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 100 различных монохромных изображений были закодированы одинаковые последовательности бит, имеющие нормальный закон распределения.

Для оценки скрытности использовались критерий минимума квадрата среднеквадратичного отклонения (MSE), пиковое отношение сигнала к шуму (PSNR) и нормированная корреляция (NC).

Результаты полученных оценок были усреднены и округлены, и представлены в таблице 2.

Таблица 2
Table 2

Результаты оценки скрытности
The results of assessment of stealthiness

Метод	Оценки		
	MSE	PSNR	NC
Субполосное кодирование	0.18973	57.61725	0.99998
Расширение спектра	7.01271	39.74581	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:

$$C = \frac{V}{N \cdot M} \tag{14}$$

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

$$I = \frac{100}{\Delta_{\max} \cdot N \cdot M} \cdot \sum_{i=1}^{N \cdot M} |\Delta_i|, \tag{15}$$

где Δ_i – Δ-изменения i-го элемента контейнера

Вероятность ошибочного извлечения информационных данных сообщения:

$$P_{ош} = \frac{V - V_{ош}}{N \cdot M}, \tag{16}$$

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

При проведении эксперимента в 100 различных монохромных изображений были закодированы одинаковые последовательности бит, имеющие нормальный закон распределения.

Результаты полученных оценок были усреднены и округлены, и представлены в таблице 3.

Таблица 3
Table 3

Результаты оценки стойкости в монохромном изображении
The results of assessment of resistance in a monochrome image

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

В модифицированном методе субполосного кодирования есть возможность настройки такого параметра как количество бит, кодируемое в одном подблоке. При изменении этого параметра было получено оптимальное значениене более 128 бит. Результаты отражены в таблице 4.

Таблица 4
Table 4

Зависимость оценок метода субполосного кодирования при увеличении количества зашифрованных бит
Dependence of sub-band encoding estimates with increasing number of encrypted bits

Количество бит в одном подблоке	**Оценки**		
	MSE	**PSNR**	**NC**
16	0.04926	61.20544	0.99999
64	0.14879	56.40483	0.99999
128	0.36624	52.49304	0.99999
192	2.10812	44.89184	0.99994
256	7.55459	39.34869	0.99978

Результаты

По результатам исследования можно представить следующие выводы и рекомендации по кодированию в субполосах изображения:

1. Кодирование в субполосах изображения позволяет осуществить встраивание информационных данных в неподвижные изображения для скрытной передачи и реализовать, таким образом, стеганографическую защиту информации.

2. Метод кодирования в субполосах изображения учитывает неточности устройств оцифровки и избыточность изображений и позволяет более эффективно скрыть информацию.

3. 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.

4. Субполосный метод отлично справляется с кодированием до 128 битов в одном подблоке, что для изображения размером 512x512 составляет общее количество в 8192 бита (для ASCII кодировки приравнивается кодированию 1024 символов).

Список литературы
References

1. Жиляков Е.Г., Веселых Н.К. 2014. Сжатие изображений на основе субполосного анализа/синтеза. Научные ведомости БелГУ. Сер. История. Политология. Экономика. Информатика. 21(192): 202–212.

Zhilyakov E.G., Veselykh N.K. 2014. Image compression based on subband analysis/synthesis. Nauchnye vedomosti BelGU. Istoriya. Politologiya. Ekonomika. Informatika. [Belgorod State University Scientific Bulletin. History Political science Economics Information technologies]. 21(192): 202–212.

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

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

3. Жиляков Е.Г., Лихолоб П.Г., Медведева А.А. 2016. Исследование некоторых стеганографических алгоритмов. Научный результат. Информационные технологии. 1(2): 9–15.

Zhilyakov E.G., Liholob P.G., Medvedeva A.A. 2016. Research of some steganographic algorithms. Research Result. Information technologies 1(2): 9–15.

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

Konakhovich G.F., Puzyrenko A.Yu. 2006. Computer Steganography. Theory and practice. MK-Press: 288.

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

Gribunin V.G., Okov I.N., Turintsev I.V. 2009. Digital steganography. Solon-Press, 265.

6. Черноморец А.А., Голощапова В.А., Лысенко И.В., Болгова Е.В. 2011 О частотной концентрации энергии изображений. Научные ведомости БелГУ. Сер. История. Политология. Экономика. Информатика. 1(96): 146–151.

Chernomorets A.A., Goloschapova V.A., Lysenko I.V., Bolgova E.V. 2011. On frequency concentration of image energy. Nauchnye vedomosti BelGU. Istoriya. Politologiya. Ekonomika. Informatika. [Belgorod State University Scientific Bulletin. History Political science Economics Information technologies]. 1(96): 146–151.

7. Жиляков Е.Г., Черноморец А.А., Болгова Е.В., Гахова Н.Н. 2014. Исследование устойчивости стеганографии в изображениях. Научные ведомости БелГУ. Сер. История. Политология. Экономика. Информатика. 1(172): 168–174.

Zhilyakov E.G., Chernomorets A.A., Bolgova E.V., Gakhova N.N. 2014. Investigation of steganography stability in images. Nauchnye vedomosti BelGU. Istoriya. Politologiya. Ekonomika. Informatika. [Belgorod State University Scientific Bulletin. History Political science Economics Information technologies]. 1(172): 168–174.

8. Жиляков Е.Г., Черноморец А.А., Болгова Е.В., Гахова Н.Н. 2014. О субполосном внедрении информации в подобласти пространственных частот изображения-контейнера. Нейрокомпьютеры: разработка, применение. 9: 85–87.

Zhilyakov E.G., Chernomorets A.A., Bolgova E.V., Gakhova N.N. 2014. On the subband introduction of information in the subregion of the spatial frequencies of the image container. Neyrokomp'yutery: razrabotka, primeneniye. 9: 85–87.

9. Жиляков Е.Г., Черноморец А.А., Болгова Е.В., Голощапова В.А. 2014. Оценка эффективности субполосного внедрения данных в изображение. Научные ведомости БелГУ. Сер. История. Политология. Экономика. Информатика. 8(179): 200–206.

Zhilyakov Ye.G., Chernomorets A.A., Bolgova E.V., Goloshchapova V.A. 2014. Assessment of efficiency of subband embedding of data in the image. Nauchnye vedomosti BelGU. Istoriya. Politologiya. Ekonomika. Informatika. [Belgorod State University Scientific Bulletin. History Political science Economics Information technologies]. 8(179): 200–206.

10. Жиляков Е.Г., Черноморец А.А., Болгова Е.В., Голощапова В.А. 2015. О субполосном внедрении в цветные изображения. Научные ведомости БелГУ. Сер. История. Политология. Экономика. Информатика. 1(198): 158–162.

Zhilyakov E.G., Chernomorets A.A., Bolgova E.V., Goloshchapova V.A. 2015. About subband embedding in colored images. Nauchnye vedomosti BelGU. Istoriya. Politologiya. Ekonomika. Informatika. [Belgorod State University Scientific Bulletin. History Political science Economics Information technologies]. 1(198): 158–162.

11. N. Provos, P. Honeyman. 2003. Hide and seek: An introduction to steganography. IEEE Security and Privacy, 1(3): 32–44.

12. I.J. Cox, J. Kilian, F.T. Leighton and T. Shamoon. 1997. Secure Spread Spectrum Watermarking for Multimedia. IEEE Trans. On Image Processing, 6 (12): 1673–1687.

13. Smith J., Comiskey B. 1996. Modulation and information hiding in image. Springer as Lecture Notes in Computing Science. 117: 207–227.

14. Хорошко В.О., Азаров О.Д., Шелест М.С., Яремчук Ю.С. 2003. Основы компьютерной стеганографии: Учебное пособие для студентов и аспирантов. Винница: ВДТУ: 143

Khoroshko V.O., Azarov O.D., Shelest M.S., Yaremchuk YU.S. 2003. Fundamentals of computer steganography: A manual for students and graduate students. Vinnitsa: VDTU: 143

15. Шелухин О. И., Канаев С. Д. 2016. Алгоритм скрытия водяных знаков на основе 2D дискретного вейвлет-преобразования. Спецтехника и связь. 2: 33–37.

Shelukhin O. I., Kanayev S. D. 2016. Algorithm for hiding watermarks based on 2D discrete wavelet transform. Spetstekhnika i svyaz'. 2: 33–37.

16. Sravanthi G.S. et al. 2012. A spatial domain image steganography technique based on plane bit substitution method.Global Journal of Computer Science and Technology Graphics & Vision. 12(15): 176–179.

17. R.H. Alwan, F. J. Kadhim, A. T. Al-Taani. 2005. Data embedding based on better use of bits in image pixels. International Journal of Signal Processing, 2(1): 104–107

18. Жарких А.А., Гурин А.В., Пластунов В.Ю. 2009. Метод стеганографии на основе прямого расширения спектра сигнала. Материалы VII Международной научно-технической конференции, 4: 78–83.

Zharkikh A.A., Gurin A.V., Plastunov V.Y. 2009. Steganography Method based on the Direct Spread Spectrum Signal. Materials of the VII International Science and Technology Conference, 4: 78–83.

19. Meghanathan N., Nayak L. 2010. Steganalysis algorithms for detecting the hidden information in image, audio and video cover media.international journal of Network Security & Its application (IJNSA). 2(1): 43–55.

20. Раткин Л.С. 2006. О некоторых аспектах применения стеганографии для защиты информационных систем. Вопросы защиты информации. 4: 12–15.

Ratkin L.S. 2006. About some shouts of the use of steganography for the protection of information systems. Voprosy zashchity informatsii. 4: 12–15.