ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ

УДК 004.056.5
DOI: 10.17586/0021-3454-2016-59-9-717-722

УВЕЛИЧЕНИЕ КОЛИЧЕСТВА ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ В СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЕ НА ОСНОВЕ МЕТОДА ПРЯМОГО РАСШИРЕНИЯ СПЕКТРА

Р. Х. Балтаев, И. В. Лунегов

Пермский государственный национальный исследовательский университет, 614990, Пермь, Россия
E-mail: rodion-baltaev@yandex.ru

Рассматривается стеганографическая система защиты информации, основанная на методе прямого расширения спектра. Исследуется возможность увеличения количества информации, передаваемой в данной системе, при использовании стеганографического метода. Выбирается критерий определения степени искажения изображения после введения скрываемого сообщения. Определяется эффективность применения перекрытия блоков при встраивании дополнительной информации при низкой степени искажения изображения.

Ключевые слова: *стеганография, прямое расширение спектра, двумерный процесс авторегрессии, перекрытие блоков, S-CIELAB, CIEDE2000*

Введение. Одним из современных средств защиты информации являются стеганографические системы, которые обеспечивают сохранение в тайне не только информационного содержания передаваемых данных, но и самого факта их передачи. Стеганографическая система — это совокупность средств и методов, используемых для создания скрытого канала передачи информации. Для встраивания данных в неподвижные изображения применяется стеганографический метод на основе прямого расширения спектра, в котором биты, составляющие сообщение, модулируются широкополосной псевдослучайной последовательностью (ПСП). Поскольку методы расширения спектра устойчивы к случайным и преднамеренным искажениям, применение широкополосной ПСП значительно затрудняет обнаружение и/или удаление встроенной дополнительной информации [1].

Основная характеристика стеганографических систем — количество передаваемой информации, которая может быть скрыта в контейнере таким образом, что наличие встроенной информации является незаметным для третьей стороны; здесь под контейнером понимается цветное цифровое изображение, в которое встраивается информация. Понятно, что чем больше информации может быть передано скрытно, тем лучше.

В настоящей статье исследуется возможность увеличения количества передаваемой информации в стеганографической системе, основанной на методе прямого расширения спектра. Увеличение количества передаваемой информации приводит к увеличению искажения изображения, поэтому для определения степени искажения выбран некоторый критерий.

Стеганографический метод на основе прямого расширения спектра. Согласно предложенному в работе [2] стеганографическому методу на основе прямого расширения спектра неподвижное изображение F разбивается на блоки $F_1, \ldots, F_L$, где L — количество блоков. Строится вектор C_i из всех элементов блока F_i, i=1...L, путем развертывания по столбцам

(строкам). На основе некоторого ключа генерируется широкополосная псевдослучайная последовательность Φ_j из некоторого набора ортогональных бинарных ПСП $\Phi=\{\Phi_1,...,\Phi_M\}$, где M — количество ПСП. Встраиваемое информационное сообщение m представляется бинарной последовательностью $m_i=\{-1,1\}$. Результирующий вектор S_i элементов блока изображения после встраивания одного бита сообщения m_i определяется по формуле

$$S_i = C_i + Gm_i\Phi_j, \quad i=1\ldots L, \quad \Phi_j \in \Phi, \tag{1}$$

где $G>0$ — параметр, задающий мощность встраиваемого бита.

Для извлечения бита m_i заполненное изображение разбивается на блоки, каждый блок развертывается по столбцам (строкам), по ключу генерируется ПСП $\Phi_k \in \Phi$, вычисляется их взаимная корреляция (схема коррелятора) и сравнивается с некоторым порогом. Однако предложенная в работе [2] схема является оптимальной только для аддитивного гауссова шума. В работе [3] извлечение встроенных данных из неподвижных изображений осуществлялся посредством одномерного авторегрессионного (АР) процесса. В данной статье для извлечения встроенных данных используется двумерный АР-процесс [4]:

$$\tilde{C}(m,n) = \sum_i \sum_{\mathrm{j}} \varphi(i,j)\tilde{C}(m-i,n-j) + a(m,n), \tag{2}$$

где $\varphi(i,j)$ — параметры двумерного АР-процесса; $a(m,n)$ — двумерный белый шум.

Для определения порядков p_1 и p_2 двумерного АР-процесса используется MDL-критерий [5].

Перекрытие блоков изображения. Для увеличения количества информации, передаваемой в одном изображении, целесообразно использовать перекрывающиеся блоки для встраивания скрываемых данных. Пример перекрытия блоков изображения размером 8×8 пкс представлен на рис. 1.

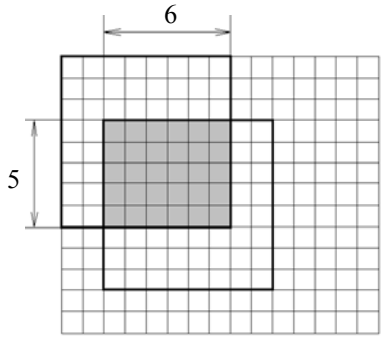

Рис. 1

Перекрытие блоков изображения возможно за счет того, что псевдослучайные последовательности обладают авто- и взаимокорреляционными функциями, близкими к аналогичным функциям белого шума.

Встраивание дополнительной информации в неподвижные изображения осуществляется следующим образом:

— выбирается блок изображения определенного размера и дополняется псевдослучайной последовательностью;

— осуществляется сдвиг на определенное количество пикселов по строкам и столбцам;

— выбирается блок изображения того же размера и дополняется псевдослучайной последовательностью и т.д.

Таким образом, в общих областях блоков изображений происходит аддитивное сложение псевдослучайных последовательностей. Поскольку используемые псевдослучайные последовательности обладают авто- и взаимокорреляционными функциями, близкими к авто-

и взаимокорреляционным функциям белого шума, то существенного уменьшения количества правильно извлеченных сообщений произойти не должно.

Критерий определения степени искажения изображения. Увеличение количества передаваемых скрытых данных обязательно приводит к увеличению искажения изображения. Поэтому для определения степени искажения изображения целесообразно выбрать некоторый критерий.

Наиболее распространенным показателем является пиковое отношение сигнал/шум [6]:

$$\mathrm{PSNR} = 10\log_{10}\frac{MN255^2}{\sum\limits_{x,y}(f_1(x,y)-f_2(x,y))^2},$$

где M, N — количество пикселов по высоте и горизонтали изображения соответственно; x, y — координаты пикселов; $f_1(x,y)$, $f_2(x,y)$ — пикселы исходного и измененного изображений соответственно.

Так как визуально наблюдаемое отличие изображений в показателе PSNR не отражено [6], необходим показатель, в котором будет учитываться информация о цвете изображения для определения его качества.

Согласно Международной комиссии по освещению (CIE) цветовая разница определяется метрикой ΔE_{12}. Значение $\Delta E_{12} \approx 2{,}3$ соответствует минимально различимому человеческим глазом отличию цветов [7].

Существует несколько стандартов, задающих цветовое различие, последним из которых является стандарт CIEDE2000, основанный на цветовом пространстве CIELAB [8]. Однако вместо цветового пространства CIELAB в ходе исследований использовалось цветовое пространство S-CIELAB, являющееся расширением CIELAB с добавлением цветового разделения и пространственной фильтрации. В настоящее время цветовое пространство S-CIELAB признано наиболее эффективной моделью для имитации восприятия цвета человеческим глазом [9].

Эксперимент. В качестве тестового было использовано цветное изображение “Lena” размером 512×512 пкс, взятое из базы данных изображений Института обработки сигналов и изображений Университета Южной Калифорнии [10].

В качестве набора бинарных псевдослучайных последовательностей использовались ПСП, формируемые генератором на основе блочного алгоритма шифрования AES.

Встраивание сообщения производилось в блоки размером 32×16 синего канала цветовой модели RGB с последующим определением количества правильно извлеченных бит данных при заданной вероятности α ложной тревоги. Такие блоки после развертывания по строкам (столбцам) соответствуют векторам длиной 512 бит.

Встраивание проводилось по формуле (1) при G=1. Поскольку генератор ПСП формирует двоичные последовательности, состоящие из 0 и 1, то каждый элемент ПСП преобразуется как

$$s_i = 2\varepsilon_i - 1,$$

где $\varepsilon_i \in \{0,1\}$ — элемент ПСП до преобразования.

Извлечение встроенных данных производилось с помощью инвариантных к дисперсии аддитивного шума правил принятия решения о наличии сигнала [11]:

$$\sum_{i=1}^{N} x_i s_i \ge t_\alpha \sqrt{\frac{\sum\limits_{i=1}^{N} x_i^2 - \left(\sum\limits_{i=1}^{N} x_i s_i\right)^2}{N-1}},$$

где t_α — процентная точка центрального распределения Стьюдента с N–1-й степенью свободы; N — длина вектора, s_i — проверяемый детерминированный сигнал при $\sum_{i=1}^{N} s_i^2 = 1$.

В качестве тестового принималось сообщение m, равное количеству используемых для встраивания блоков изображения, каждый элемент которого m_i=1.

На рис. 2 представлен график зависимости количества (Z) правильно извлеченных бит сообщения (в процентах) от количества перекрытых пикселов блоков изображения “Lena” по строкам и столбцам.

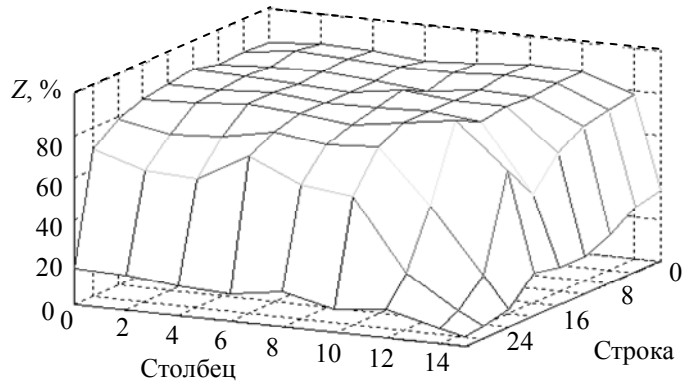

Рис. 2

Анализ рис. 2 показывает, что перекрытие в 20 пкс по строкам и 12 пкс по столбцам не приводит к существенному уменьшению количества правильно извлеченных бит сообщения, что позволяет передавать 5125 бит сообщения. Для сравнения, если использовать блоки без перекрытия, то максимально возможное количество бит — 512. Таким образом, использование перекрытия в данном случае дает 10-кратное увеличение количества передаваемых бит.

На рис. 3 представлен график зависимости количества (Y) цветовых искажений (в процентах), превышающих минимально различимое человеческим глазом отличие цветов, от количества перекрытых пикселов блоков изображения “Lena” по строкам и столбцам. Рис. 3 показывает существенное увеличение искажения изображения только при практически полном перекрытии блоков.

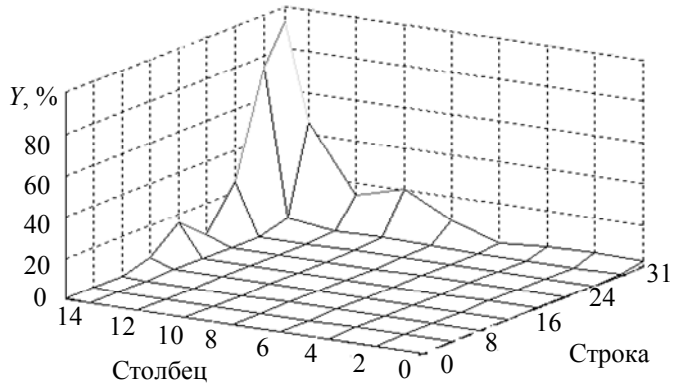

Рис. 3

Заключение. Предложен способ увеличения количества передаваемой в стеганографической системе информации с помощью перекрытия блоков изображения, в которое встраивается скрываемое сообщение. Применение перекрытия блоков изображения приводит к существенному увеличению количества передаваемых данных без уменьшения количества правильно извлеченных бит встроенной информации и без увеличения искажения изображения.

СПИСОК ЛИТЕРАТУРЫ

1. *Конахович Г. Ф., Пузыренко А. Ю.* Компьютерная стеганография. Теория и практика. Киев: МК-Пресс, 2006. 288 с.
2. *Smith J., Comiskey B.* Modulation and information hiding in image // Information Hiding: 1st Intern. Workshop "InfoHiding'96", Springer as Lecture Notes in Computing Science. 1996. Vol. 1174. P. 207—227.
3. *Балтаев Р. Х., Лунегов И. В.* Модель авторегрессии в стеганографическом методе на основе прямого расширения спектра // Вопросы защиты информации. 2015. № 3. С. 73—78.
4. *Марпл-мл. С. Л.* Цифровой спектральный анализ и его приложения: Пер. с англ. М.: Мир, 1990. 584 с.
5. *Aksasse B., Radouane L.* Two-dimensional autoregressive (2-D AR) model order estimation // IEEE Transact. on Signal Processing. 1999. Vol. 47, N 7. P. 2072—2077.
6. *Грибунин В. Г., Оков И. Н., Туринцев И. В.* Цифровая стеганография. М.: СОЛОН-ПРЕСС, 2009. 272 с.
7. *Sharma G.* Digital Color Imaging Handbook. N. Y.: CRC Press, 2003. 592 p.
8. *Sharma G., Wu W., Dalal E. N.* The CIEDE2000 color-difference formula: Implementation notes, supplementary test data, and mathematical observations // Color Research and Application. 2005. Vol. 30, N 1. P. 21—30.
9. *He L., Gao X., Lu W., Li X., Tao D.* Image quality assessment based on S-CIELAB model // Signal, Image and Video Processing. 2011. Vol. 5, N 3. P. 283—290.
10. The USC-SIPI Image Database [Электронный ресурс]: <http://sipi.usc.edu/database>.
11. *Левин Б. Р.* Теоретические основы статистической радиотехники. М.: Сов. радио, 1976. Кн. 3. 288 с.

Сведения об авторах

Родион Хамзаевич Балтаев — аспирант; ПГНИУ, кафедра радиоэлектроники и защиты информации; E-mail: rodion-baltaev@yandex.ru

Игорь Владимирович Лунегов — канд. физ.-мат. наук, доцент; ПГНИУ, кафедра радиоэлектроники и защиты информации; E-mail: lunegov@psu.ru

Рекомендована кафедрой радиоэлектроники и защиты информации

Поступила в редакцию 22.01.16 г.

Ссылка для цитирования: *Балтаев Р. Х., Лунегов И. В.* Увеличение количества передаваемой информации в стеганографической системе на основе метода прямого расширения спектра // Изв. вузов. Приборостроение. 2016. Т. 59, № 9. С. 717—722.

INCREASE IN THE VOLUME OF INFORMATION TRANSMITTED IN STEGANOGRAPHIC SYSTEM ON THE BASE OF THE DIRECT SPECTRUM EXTENSION METHOD

R. Kh. Baltaev, I. V. Lunegov

Perm State University, 614990, Perm, Russia
E-mail: rodion-baltaev@yandex.ru

A steganographic information protection system based on the direct spectrum extension method is considered. Possibility to increase the volume of information transmitted in the system is analyzed. A criterion is chosen for determining the degree of image distortion after introduction of the hidden message. Efficiency of application of block overlapping when embedding the additional information with a low degree of image distortion is determined.

Keywords: steganography, direct spectrum extension, two-dimensional autoregressive process, block overlapping, S-CIELAB, CIEDE2000

Data on authors

Rodion Kh. Baltaev — Post-Graduate Student; Perm State University, Department of Radioelectronics and Protection of Information; E-mail: rodion-baltaev@yandex.ru

Igor V. Lunegov — PhD, Associate Professor; Perm State University, Department of Radioelectronics and Protection of Information; Head of the Department; E-mail: lunegov@psu.ru

For citation: *Baltaev R. Kh., Lunegov I. V.* Increase in the volume of information transmitted in steganographic system on the base of the direct spectrum extension method // Izv. vuzov. Priborostroenie. 2016. Vol. 59, N 9. P. 717—722 (in Russian).

DOI: 10.17586/0021-3454-2016-59-9-717-722