ВЕСТНИК ПЕРМСКОГО УНИВЕРСИТЕТА

2016 **Серия: Физика** **Вып. 1 (32)**

УДК 004.056.5
PACS 01.20.+x

Вложение дополнительной информации в неподвижные изображения методом прямого расширения спектра

Р. Х. Балтаев[a], **И. В. Лунегов**[b]

Пермский государственный национальный исследовательский университет
614990, Пермь, ул. Букирева, 15
[a] email: rodion-baltaev@yandex.ru
[b] email: lunegov@psu.ru

В работе описывается общий принцип действия метода стеганографии на основе прямого расширения спектра: модуляция информационных сигналов, встраивание модулированного сигнала в контейнер-изображение, извлечение информационных данных. Рассматриваются основные недостатки данного метода. Предлагаются основные способы увеличения эффективности извлечения дополнительной информации из неподвижных изображений.

Ключевые слова: стеганография; расширение спектра; извлечение встроенных данных

Поступила в редакцию 28.12.2015; принята к опубликованию 25.03.2016

Adding additional information to images by direct spread spectrum

R. Kh. Baltaev[a], **I. V. Lunegov**[b]

Perm State University
Bukireva St. 15, 614990, Perm
[a] email: rodion-baltaev@yandex.ru
[b] email: lunegov@psu.ru

The paper deals with the general principle of the method of steganography by direct spread spectrum: modulation of information signals, insertion of a modulated signal in an image, extracting data. The main disadvantages of this method are considered. The main ways of increase in efficiency of extraction of additional information from images are offered.

Keywords: steganography; spread spectrum; extracting embedded data

Received 28.12.2015; accepted 25.03.2016

doi: 10.17072/1994-3598-2016-1-51-54

1. Введение

Метод прямого расширения спектра является одним из методов стеганографии. Стеганография скрывает сам факт передачи сообщения в отличие от криптографии, которая скрывает только содержимое сообщения.

Изначально методы расширения спектра (SS – Spread Spectrum) использовались при разработке военных систем управления и связи. Во время Второй мировой войны расширение спектра использовалось в радиолокации для борьбы с намеренными помехами [1].

Система связи является системой с расширенным спектром в следующих случаях [2]:

– расширение спектра выполняется с помощью расширяющего (или кодового) сигнала, который не зависит от передаваемой информации;

– восстановление первичной информации осуществляется путем сопоставления.

В радиосвязи используются три основных способа расширения спектра[1]:

– с помощью прямой псевдослучайной последовательностью (РСПП);

– с помощью скачкообразного перестраивания частот;

– с помощью компрессии с использованием линейной частотной модуляции (ЛЧМ).

При расширении спектра прямой последовательностью информационный сигнал модулируется функцией, которая принимает псевдослучайные значения. Данный псевдослучайный сигнал содержит составляющие на всех частотах, которые моделируют энергию сигнала в широком диапазоне.

В методе расширения спектра с помощью скачкообразного перестраивания частот передатчик мгновенно изменяет одну частоту несущего сигнала на другую. Секретным ключом при этом является псевдослучайный закон изменения частот.

При компрессии с использованием ЛЧМ сигнал модулируется функцией, частота которой изменяется во времени.

В данной работе рассмотрен вариант реализации метода стеганографии на основе расширения спектра прямой псевдослучайной последовательностью, авторами которого являются Смит (J. R. Smith) и Комиски (B. O. Comiskey) [3]. Определены теоретические предпосылки дальнейших исследований для уменьшения ошибок извлечения встроенных в изображения данных.

2. Модуляция информационных сигналов

Сначала введем условные обозначения и математические соотношения. Информационное сообщение, подлежащее встраиванию в контейнер-изображение, представим в виде блоков m_i равной длины, т.е. $m = (m_0, m_1, \ldots, m_{N-1})$, где N – количество блоков. Каждый блок m_i – последовательность из M бит, т.е. $m_i = (m_{i0}, m_{i1}, \ldots, m_{iM-1})$.

Контейнер-изображение рассматриваем как массив данных размерностью K·L, разбитый на подблоки размером $k \cdot l = n$, где n – длина псевдослучайной последовательности (ПСП).

Секретными ключевыми данными является набор слабокоррелированных друг с другом псевдослучайных последовательностей:

$$\Phi = \{\Phi_1, \ldots, \Phi_M\},$$

где M – количество ПСП, $\Phi_i \in \{-1;1\}$.

В качестве набора псевдослучайных последовательностей используется ансамбль ортогональных дискретных последовательностей Уолша–Адамара [3].

Встраивание информационного сообщения осуществляется следующим образом. Каждый блок сообщения сопоставляется с отдельным блоком контейнера-изображения. Каждый информационный бит блока m_{ij}, где $j = 0,\ldots, M–1$, представляется в виде информационного сигнала $m_{ij}(t) = \{-1; 1\}$.

Для каждого информационного блока формируется модулированный информационный сигнал:

$$E_i(t) = \sum_{j=0}^{M-1} m_{ij}(t)\Phi_j. \qquad (2.1)$$

Полученный блок сообщения (2.1) попиксельно суммируется с подблоком контейнера.

3. Встраивание и извлечение информационных данных

Стеганограмма (заполненный контейнер) S_i элементов блока изображения после встраивания одного бита сообщения:

$$S_i = C_i + GE_i, \qquad (3.1)$$

где $G > 0$ – коэффициент усиления расширяющего сигнала, задающий «энергию» встраиваемых бит информационной последовательности.

На этапе извлечения данных нет необходимости владеть информацией о первичном контейнере C.

Каждый блок представляется в форме вектора $S_i = (S_{i0}, S_{i1}, \ldots, S_{in-1})$, где $i = 0,\ldots,N–1$.

Чтобы извлечь j-й бит сообщения из i–го блока стеганоизображения, необходимо вычислить коэффициент корреляции между Φ_j и принятым блоком S_i (представленного в виде вектора):

$$\rho\left(S_i,\Phi_j\right)=\frac{1}{n}\sum_{z=0}^{n-1}S_{iz}\Phi_{jz} \tag{3.2}$$

или (3.2) в развернутом виде:

$$\rho\left(S_i,\Phi_j\right)=G\frac{1}{n}\sum_{z=0}^{n-1}E_{iz}\Phi_{jz}+\frac{1}{n}\sum_{z=0}^{n-1}C_{iz}\Phi_{jz}, \tag{3.3}$$

где C_i – блок контейнера, представленный в форме вектора.

Предположим, что массив имеет случайную статистическую структуру, т.е. положим, что второе слагаемое в правой части выражения (3.3) близко к нулю и им можно пренебречь. В результате имеем

$$\rho\left(S_i,\Phi_j\right)\approx G\sum_{l=0}^{M-1}m_{il}(t)\frac{1}{n}\sum_{z=0}^{n-1}\Phi_{lz}\Phi_{jz}. \tag{3.4}$$

Все последовательности из множества Φ слабокоррелированы, т.е. при $l\neq j$ имеем $\rho\left(\Phi_l,\Phi_j\right)\approx 0$. Следовательно, всеми слагаемыми в правой части равенства (3.4) при $l\neq j$ можно пренебречь. Отсюда имеем

$$\rho\left(S_i,\Phi_j\right)\approx Gm_{ij}(t). \tag{3.5}$$

Поскольку $G > 0$, то знак $\rho\left(S_i,\Phi_j\right)$ зависит только от знака $m_{ij}(t)$.

4. Величина вносимых искажений в контейнере-изображении

Для оценки величины вносимых искажений воспользуемся выражением (3.1). Второе слагаемое в правой части (3.1) определяет величину Δ – изменений элементов данных контейнера. Сомножитель E_i в выражении (2.1) формируется в результате суммирования M дискретных сигналов (принимающих значения ±1). Следовательно, все элементы будут принимать значения из диапазона $[-M,\ldots,+M]$, а соответствующие Δ-изменения элементов контейнера не будут превышать

$$\left|\Delta_i\right|\le MG. \tag{4.1}$$

Таким образом, исходя из выражения (4.1), для уменьшения величины вносимых искажений в контейнере-изображении необходимо уменьшать коэффициент усиления расширяющего сигнала при заданном количестве встраиваемых бит в подблок контейнера-изображения.

5. Ошибочное извлечение информационного сообщения

Ошибка извлечения произойдет при изменении знака коэффициента корреляции $\rho\left(S_i,\Phi_j\right)$ в выражении (3.5).

Представим коэффициент $\rho\left(S_i,\Phi_j\right)$ в виде

$$\rho\left(S_i,\Phi_j\right)=\rho\left(C_i,\Phi_j\right)+\rho\left(GE_i,\Phi_j\right). \tag{5.1}$$

Ошибка извлечения информационного бита сообщения произойдет при наступлении события:

$$\left|\rho\left(C_i,\Phi_j\right)\right|>\left|\rho\left(GE_i,\Phi_j\right)\right|=G. \tag{5.2}$$

То есть ошибочное извлечение информационного сообщения произойдет, когда абсолютное значение коэффициента корреляции дискретного сигнала Φ_j с блоком контейнера C_i, в который встраивается бит, превзойдет коэффициент усиления G.

Встраивание информации производилось во все не пересекающиеся блоки размером 8x8 пикселей синего канала изображения “Sailboat on lake” (рис. 1) с помощью формулы (3.1) при $G = 1$.

Рис. 1. *Изображение “Sailboat on lake” (цветное только в электронной версии)*

Для извлечения встроенных данных использовалась формула (3.2), коэффициент 1/n опущен. В качестве порога принятия решения k о присутствии сигнала использовалось следующее выражение [4]:

$$k=\sigma^2\ln c+\frac{1}{2}\sum_{i=0}^{n-1}S_i^2, \tag{5.3}$$

где введена оценка дисперсии контейнера

$$\sigma^2=\frac{1}{n-1}\sum_{i=0}^{n-1}\left(C_i-\bar{C}\right)^2.$$

Константа c из (5.3) находится с помощью критерия Неймана–Пирсона, согласно которому задается вероятность ложной тревоги α и определяется константа c из следующей формулы [4]:

$$\alpha=1-F\left(\frac{\sigma^2\ln c+\frac{1}{2}\sum_{i=0}^{n-1}S_i^2}{\sigma\sqrt{\sum_{i=0}^{n-1}S_i^2}}\right). \tag{5.4}$$

На рис. 2 представлен график зависимости коэффициента битовых ошибок BER от вероятности ложного обнаружения α. Коэффициент битовых ошибок BER – отношение числа ошибочно принятых бит к общему числу переданных бит. Изображение “Sailboat on lake” после встраивания информации не приводится в силу отсутствия визуального различия.

Рис. 2 показывает довольно большую ошибку извлечения данных.

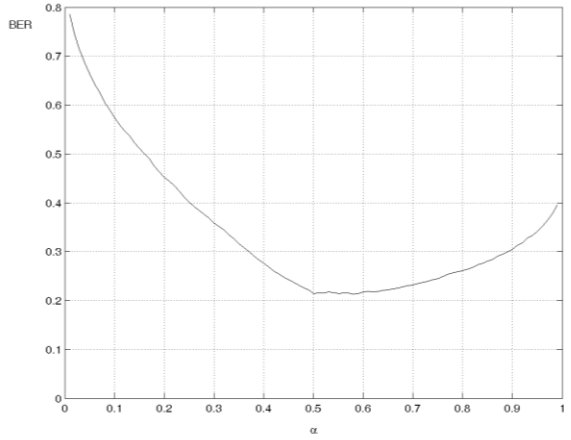

Рис. 2. *График зависимости коэффициента битовых ошибок BER от вероятности ложного обнаружения α для изображения “Sailboat on lake”*

Таким образом, исходя из вышесказанного, для уменьшения величины вносимых искажений необходимо уменьшать коэффициент усиления G при заданном количестве встраиваемых бит в подблок контейнера-изображения, а для безошибочного извлечения информационного сообщения следует увеличивать коэффициент усиления G.

6. Увеличение эффективности вложения дополнительной информации в неподвижные изображения методом прямого расширения спектра

Для увеличения эффективности этого метода необходимо выполнить следующие условия:

– использование помехоустойчивого кодирования для уменьшения вероятности ошибочного извлечения информационного сообщения;

– адаптивный выбор псевдослучайных последовательностей для уменьшения коэффициента корреляции этих последовательностей с блоком контейнера;

– использование фильтрации. Если посмотреть на выражение (3.1), то можно принять, что слагаемое C_i в правой части этого выражения есть аддитивный шум.

Список литературы

1. *Конахович Г. Ф., Пузыренко А. Ю.* Компьютерная стеганография. Теория и практика. М.: МК-Пресс, 2006. 288 с.
2. *Скляр Б.* Цифровая связь: теоретические основы и практическое применение. М.: Вильямс, 2003. 1104 с.
3. *Smith J., Comiskey B.* Modulation and information hiding in image // Information hiding: First Int. Workshop “InfoHiding’96”. Springer as Lecture Notes in Computing Science. 1996. Vol. 1174. P. 207–227.
4. *Левин Б. Р.* Теоретические основы статистической радиотехники. Кн. 2. М.: Советское радио, 1975. 392 с.

References

1. Konahovich G. F., Puzyrenko A. Yu. *Kompyuternaya steganografiya. Teoriya i praktika*. (Computer steganography. Theory and practice). Moscow: MK- Press, 2006. 288 p. (In Russian).
2. Sklyar B. *Digital Communications: Fundamentals and Applications*. Upper Saddle River, New Jersey: Prentice Hall, 2001. 1104 p.
3. Smith J., Comiskey B. Modulation and Information hiding in image. Information hiding. *First International Workshop “InfoHiding’96”*. Springer as Lecture Notes in Computing Science, 1996, vol. 1174, pp. 207–227.
4. Levin B. R. *Teoreticheskie osnovy statisticheskojradiotekhniki*. (Theoretical foundations of statistical radio engineering). Vol. 2. Moscow: Sovetskoe radio, 1975. 392 p. (In Russian).

Просьба ссылаться на эту статью в русскоязычных источниках следующим образом:
Балтаев Р. Х., Лунегов И. В. Вложение дополнительной информации в неподвижные изображения методом прямого расширения спектра // Вестник Пермского университета. Серия: Физика. 2016. № 1 (32). С. 51–54. doi: 10.17072/1994-3598-2016-1-51-54

Please cite this article in English as:
Baltaev R. Kh., Lunegov I. V. Adding additional information to images by direct spread spectrum // Bulletin of Perm University. Series: Physics, 2016, no. 1 (32), pp. 51–54. doi: 10.17072/1994-3598-2016-1-51-54