УДК 621.396

А.А. Смирнов

Кировоградский национальный технический университет, Кировоград

СТЕГАНОГРАФИЧЕСКОЕ ВСТРАИВАНИЕ ДАННЫХ В НЕПОДВИЖНЫЕ ИЗОБРАЖЕНИЯ МЕТОДОМ ПРЯМОГО РАСШИРЕНИЯ СПЕКТРА

Рассматриваются стеганографические методы встраивания данных в контейнеры-изображения на основе использования сложных дискретных сигналов. Показано, что применение технологии прямого расширения спектра в стеганографических системах позволяет реализовать стеганографическую защиту информации и обеспечить высокую пропускную способность организуемого стеганоканала. Предлагается дальнейшее развитие методов встраивания информации в неподвижные контейнеры-изображения на основе использования больших ансамблей слабокоррелированных (квазиортогональных) дискретных сигналов.

Ключевые слова: *стеганография, сложные дискретные сигналы, прямое расширение спектра.*

Постановка проблемы в общем виде и анализ литературы

Одним из перспективных направлений в развитии современной стеганографии являются методы встраивания данных в контейнеры-изображения на основе использования сложных дискретных сигналов [1 – 4]. Так, в работе [2] показано, что применение ортогональных последовательностей позволяет реализовать стеганографическое преобразование для встраивания информации в неподвижные контейнеры-изображения. В работе [3] исследована эффективность такой стеганографической защиты, показано, что применение ортогональных сигналов не всегда позволяет обеспечить высокую пропускную способность организовываемого стеганоканала. В данной работе предлагается дальнейшее развитие методов встраивания информации в неподвижные контейнеры-изображения на основе использования больших ансамблей слабокоррелированных (квазиортогональных) дискретных сигналов.

Стеганографическое преобразование на основе прямого расширения спектра

Целью стеганографической защиты информации является скрытное встраивание информационных сообщений в передаваемые контейнеры (цифровые данные, обладающие высоким уровнем естественной избыточности). При передаче контейнеров по открытым каналам связи скрывается сам факт передачи информационных сообщений, чем и обеспечивается секретность организуемого стеганографического канала [1 – 4].

В работах [1 – 3] показано, что применение технологии прямого расширения спектра в стеганографических целях позволяет, используя развитый математический аппарат цифровой обработки сигналов, реализовать стеганографическое встраивание информации в неподвижные контейнеры-изображения. При этом, каждый блок m_i информационного сообщения сопоставляется с отдельным блоком контейнера-изображения C_i.

В результате, для каждого информационного блока m_i формируется модулированный информационный сигнал:

$$E_i(t) = \sum_{j=0}^{M-1} m_{i_j}(t)\Phi_j, \qquad (1)$$

где $m_{i_j}(t)$ – информационный сигнал, соответствующий j-му биту i-му блоку информационного сообщения,

$$m_{i_j}(t) = \begin{cases} +1, m_{i_j} = 1; \\ -1, m_{i_j} = 0; \end{cases}$$

$\Phi_j = \left(\varphi_{j0}, \varphi_{j1}, ..., \varphi_{jn-1}\right)$ – расширяющий кодовый сигнал длины n из ансамбля (множества) слабокоррелированных друг с другом псевдослучайных последовательностей (ПСП) $\Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\}$,

$$\varphi_{i_z} = \begin{cases} +1 \\ -1 \end{cases}, \; z = 0, ..., n-1,$$

M – число бит в одном блоке информационного сообщения, т.е. число информационных бит, встраиваемых в отдельный блок контейнера-изображения C_i. Величина M характеризует, таким образом, пропускную способность $Q = M/N$ организовываемого стеганоканала передачи информационных сообщений, где N – объем блока контейнера-изображения C_i.

Выражение (1) описывает процесс модуляции информационных сигналов $m_{i_j}(t)$ расширяющими сигналами Φ_j, традиционно используемый в широкополосной системе связи с прямым расширением спектра. Поскольку кодовый сигнал по своим стати-

стическим свойствам подобен шуму, то полученный расширенный (широкополосный) сигнал $E_i(t)$ слабо отличим от шумов в канале связи, что и позволяет осуществить скрытую передачу. Таким образом, передаваемые сообщения приобретают вид шумоподобных последовательностей, а за счет большой мощности ансамбля Φ и прямого расширения частотного спектра обеспечивается высокая скрытность организовываемых каналов связи [5 – 7].

Для встраивания информационного сообщения в контейнер сформированный сигнал $E_i(t)$ попиксельно суммируется с подблоком контейнера C_i:

$$S_i = C_i + E_i \cdot G,$$

где $G > 0$ – коэффициент усиления расширяющего сигнала, задающий «энергию» встраиваемых бит $m_{i_j}, j = 0,...,n-1$ информационной последовательности. Стеганограмма (заполненный контейнер) S формируется посредством объединения отдельных блоков S_i.

При извлечении информационных данных первичный контейнер C и его отдельные блоки C_i на приемной стороне не требуются. Операция декодирования заключается в восстановлении скрытого сообщения путем проецирования каждого блока S_i полученной стеганограммы S на все $\Phi_j \in \Phi$. Чтобы извлечь j-й бит сообщения из i-го блока стеганоизображения S_i необходимо вычислить коэффициент корреляции между Φ_j и принятым блоком S_i:

$$\begin{aligned}\rho(S_i, \Phi_j) &= \frac{1}{n}\sum_{z=0}^{n-1} S_{i_z}\Phi_{j_z} = \\ &= G \cdot \frac{1}{n}\sum_{z=0}^{n-1} E_{i_z}\Phi_{j_z} + \frac{1}{n}\sum_{z=0}^{n-1} C_{i_z}\Phi_{j_z}.\end{aligned} \quad (2)$$

Если массив C_i сформирован некотором случайным и равновероятным процессом, тогда второе слагаемое в правой части выражения (2) близко к нулю и им можно пренебречь. Следовательно имеем:

$$\begin{aligned}\rho(S_i, \Phi_j) &\approx G \cdot E_i \cdot \Phi_j = G \cdot \sum_{l=0}^{M-1} m_{i_l}(t)\Phi_l\Phi_j = \\ &= G \cdot \sum_{l=0}^{M-1} m_{i_l}(t)\sum_{z=0}^{n-1}\Phi_{l_z}\Phi_{j_z}.\end{aligned} \quad (3)$$

Все последовательности из множества Φ по определению слабокоррелированы, т.е. при $l \neq j$ имеем $\rho(\Phi_i, \Phi_j) \approx 0$. Следовательно, всеми слагаемыми в правой части равенства (3) при $l \neq j$ можно пренебречь. Отсюда имеем:

$$\rho(S_i, \Phi_j) \approx G \cdot m_{i_j}(t) \cdot \frac{1}{n}\sum_{z=0}^{n-1}\left(\Phi_{j_z}\right)^2 = G \cdot m_{i_j}(t).$$

Тогда значения $m_{i_j}(t)$ могут быть легко восстановлены с помощью выражения:

$$m_{i_j}(t) = \begin{cases} +1, \text{при } \rho(S_i, \Phi_j) \approx G, \\ -1, \text{при } \rho(S_i, \Phi_j) \approx -G; \end{cases}$$

где знак «$\approx$» предполагает наличие незначительной статистической взаимосвязи отдельных элементов множества Φ и C_i.

Рассмотренная стеганосистема наследует все преимущества широкополосных систем связи с прямым расширением спектра: устойчивость к несанкционированному извлечению встроенных сообщений соответствует скрытности в системе связи, устойчивость к разрушению или модификации встроенных сообщений – помехозащищенности, устойчивость к навязыванию ложных сообщений – имитостойкости в системе связи.

Таким образом, использование технологии прямого расширения спектра в стеганографических целях позволяет осуществить встраивание информационных данных в неподвижные изображения для скрытной передачи и реализовать, таким образом, стеганографическую защиту информации.

В работах [1 – 2] при встраивании информационных сообщений в качестве ансамблей расширяющих ПСП $\Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\}$ использовались ортогональные дискретные сигналы Уолша-Адамара. Проведем исследования эффективности построенных таким образом стеганографических систем, обоснуем возможные направления их дальнейшего совершенствования.

Стеганосистемы с ортогональными сигналами Уолша-Адамара

Ортогональные дискретные сигналы Уолша-Адамара образуются из строк матрицы H_i, формируемой по рекуррентному правилу:

$$H_i = \begin{bmatrix} H_{i-1} & H_{i-1} \\ H_{i-1} & -H_{i-1} \end{bmatrix}, \; H_0 = [1]. \quad (4)$$

Многократное повторение правила (4) позволяет сформировать матрицу Адамара H_i любого размера, кратного четырем. Строки сформированных матриц взаимноортогональны, т.е. их скалярное произведение равно нулю. Эти строки и составляют ансамбль $\Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\}$ ортогональных дискретных сигналов Уолша-Адамара $\Phi_i = (\varphi_{i_0}, \varphi_{i_1}, ..., \varphi_{i_{n-1}})$, где n – размерность сформированной матрицы H_i.

При проведении экспериментальных исследований эффективности стеганографической системы с использованием ортогональных дискретных сигналов Уолша-Адамара выбраны следующие исход-

ные данные: $n = 256$, $M = 4$ (т.е. использовалось лишь 4 из 256 сигналов из Φ), $N = 256$, $Q = 1/64 \approx 0{,}02$.

Исследовались следующие зависимости: зависимости усредненной величины вносимых искажений от коэффициента усиления $I(G)$ $I(G)$; частота ошибок извлечения от коэффициента усиления $P^*_{ош}(G)$. Исследования проводились при встраивании информационных данных в растровые данные изображения (цветовая модель R,G,B) с 8 битным кодированием каждого цвета.

Полученные эмпирические зависимости приведены на рис. 1 – 2.

Приведенные графики показывают, что увеличение коэффициента усиления G приводит к резкому снижению вероятности ошибочного извлечения и одновременному повышению величины вносимых искажений. При $G = 4$ обеспечивается безошибочное извлечение информационных данных, доля вносимых искажений в среднем лежит ниже порога зрительной чувствительности человека. Тем не менее, использование при встраивании данных ортогональных дискретных сигналов Уолша-Адамара не всегда оправдано, поскольку на отдельных участках эти ПСП имеют вид детерминированных последовательностей. Как следствие, отдельные пиксели или группа пикселей могут быть значительно искажены, а доля вносимых искажений для этих фрагментов изображения может существенно превышать рассчитанное усредненное значение $I(G)$. Для примера на рис. 3, 4 приведены: контейнер S, заполненный с показателями: $M = 128$, $G = 1$ (рис. 2); исходный контейнер (рис. 3).

Кроме того, пропускная способность организуемых стеганоканалов ограничена невысокой мощностью ансамблей ортогональных сигналов. Альтернативой использования ортогональных сигналов Уолша-Адамара являются квазиортогональные дискретные последовательности, обладающие псевдослучайной структурой и не содержащие (в идеальном случае) детерминированные участки.

Стеганосистемы с квазиортогональными дискретными сигналами

Для качественного совершенствования рассмотренных стеганографических систем предлагается использовать квазиртогональные дискретные сигналы. Обладая хорошими корреляционными и анасмблевыми свойствами квазиортогональные дискретные сигналы позволяют существенно повысить пропускную способность организуемого стеганоканала.

В ходе исследований разработана программная реализация стеганографической системы с использованием квазиортогональных дискретных сигналов в качестве ансамбля расширяющих последовательностей ансамбль $\Phi = \{\Phi_0, \Phi_1, \ldots \Phi_{M-1}\}$. Для формирования отдельных элементов квазиортогональных последовательностей использован программный генератор ПСП. При проведении исследований использованы следующие исходные данные: $n = 256$, $M = 10$, $N = 256$, $Q = 10/256 \approx 0{,}04$. Полученные в результате экспериментальных исследований эмпирические зависимости приведены на рис. 5, 6.

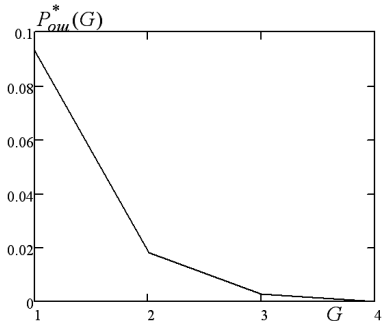

Рис. 1. Зависимость $P^*_{ош}(G)$

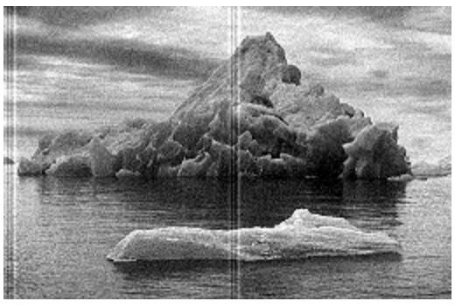

Рис. 3. Пример заполненного контейнера

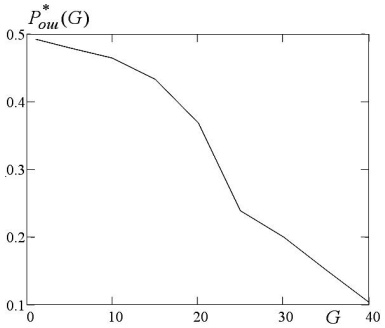

Рис. 5. Зависимость $P^*_{ош}(G)$

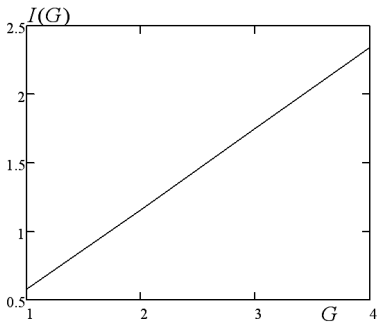

Рис. 2. Зависимость $I(G)$

Рис. 4. Пример пустого контейнера

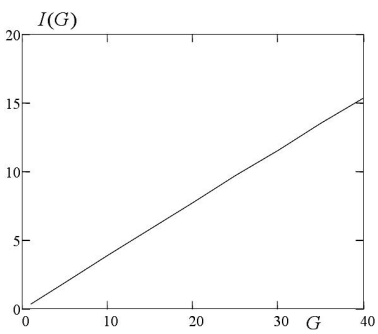

Рис. 6. Зависимость $I(G)$

Полученные эмпирические зависимости показывают, что повышение коэффициента усиления G приводит к резкому снижению вероятности ошибочного извлечения информационных бит сообщения (частоты ошибок извлечения). Однако это также ведет к увеличению вносимых искажений в контейнер-изображение. По сравнению с использованием ортогональных дискретных сигналов (рис. 1, 2) применение квазиортогональных сигналов приводит к меньшему искажению контейнера. Так, например, при встраивании M = 4 бит сообщения в один фрагмент контейнера с использованием ортогональных дискретных сигналов при коэффициенте усиления G = 4 величина вносимых искажений составляет более 2,33%.

При большем числе вносимых бит данных (M = 10 бит в один фрагмент контейнера), а следовательно и при более чем в два раза большей пропускной способности стеганографического канала передачи данных применение квазиортогональных дискретных сигналов даже с большим значением коэффициента усиления (G = 5) приводит к меньшим искажениям контейнера, величина вносимых искажений не превосходит 2%.

Таким образом, применение квазиортогональных дискретных сигналов позволяет существенно повысить пропускную способность стеганоканалов при меньшей величине вносимых искажений. В то же время, использование квазиортогональных дискретных сигналов существенно повышает вероятность ошибочного извлечения бит сообщения (за счет сильной коррелированности с отдельными фрагментами контейнера-изображения). Избавиться от этого негативного фактора возможно за счет адаптивного формирования квазиортогональных дискретных сигналов с учетом особенностей используемого контейнера-изображения.

Выводы

Проведенные исследования показали, что использование больших ансамблей квазиортогональных дискретных сигналов при построении стеганографических систем защиты информации позволяет существенно повысить пропускную способность стеганоканалов. В то же время, величина вносимых искажений в контейнеры-изображения остается высокой. ***Перспективным направлением исследований*** является использование адаптивно формируемых ансамблей дискретных сигналов, что за счет учета статистических свойств контейнеров-изображений позволит существенно снизить вносимые искажения при стеганографическом преобразовании данных.

Список литературы

1. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с., ил.

2. Smith J. Modulation and Information hiding in Image / J. Smith, B. Comiskey // Information hiding: First Int. Workshop "InfoHiding'96", Springer as Lecture Notes in Computing Science. – 1996. – Vol. 1174. – P. 207-227.

3. Кузнецов А.А. Встраивание информационных данных в неподвижные изображения с использованием прямого расширения спектра / А.А. Кузнецов, А.М. Ботнов, П.А. Лаптий // Прикладная радиоэлектроника: науч.-техн. журн. – Х.: Харьк. нац. ун-т радиоэлектроники.– Т.9, № 3. – С. 470-478.

4. Kuznetsov A. Use of Complex Discrete Signals for Steganographic Information Security / A. Kuznetsov, R. Serhiienko, V. Kovtun, A. Botnov // Statistical Methods of Signal and Data Processing (SMSDP-2010): Proceedings. – K.: National Aviation University "NAU-Druk" Publishung House. – 2010. – P. 143-146.

5. Голомба С. Цифровые методы в космической связи / С. Голомба. – М.: Связь, 1969. – 272 с.

6. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – М.: Вильямс, 2003. – 1104 с.

7. Горбенко И.Д. Анализ производных ортогональных систем сигналов / И.Д. Горбенко, Ю.В. Стасев // Радиотехника. – 1989. – № 9. – С. 16-18.

Поступила в редколлегию 26.09.2011

Рецензент: д-р техн. наук проф. А.А. Кузнецов, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

СТЕГАНОГРАФІЧНЕ ВБУДОВУВАННЯ ДАНИХ У НЕРУХЛИВІ ЗОБРАЖЕННЯ МЕТОДОМ ПРЯМОГО РОЗШИРЕННЯ СПЕКТРА

О.А. Смірнов

Розглядаються стеганографічні методи вбудовування даних у контейнери-зображення на основі використання складних дискретних сигналів. Показано, що застосування технології прямого розширення спектра в стеганографічних системах дозволяє реалізувати стеганографічний захист інформації й забезпечити високу пропускну здатність стеганоканалу, що організується. Пропонується подальший розвиток методів вбудовування інформації в нерухливі контейнери-зображення на основі використання великих ансамблів слабокорельованих (квазіортогональних) дискретних сигналів.

Ключові слова: *стеганографія, складні дискретні сигнали, пряме розширення спектра.*

STEGANOGRAPHIC VSTRAIVANIE GIVEN IN STILL IMAGE BY METHOD OF THE DIRECT EXPANSION OF THE SPECTRUM

A.A. Smirnov

Are considered steganographic methods embed given in containers-images on base of the use complex discrete signal. It is shown that using to technologies of the direct expansion of the spectrum in steganographic system allows to realize steganographic protection to information and provide high reception capacity organized steganochannell. It is offered the most further development of the methods to embed information in still containers-images on base of the use the greater ensembles weakly correlated (the quasi-orthogona) discrete signal.

Keywords: *steganographic, difficult discrete signals, direct expansion of spectrum.*