УДК 004.056

А.А. Смирнов[1], С.А. Смирнов[1], Е.В. Мелешко[1], А.А. Кузнецов[2]

[1] *Кировоградский национальный технический университет, Кировоград*
[2] *Институт информационных технологий, Харьков*

ПРОТОКОЛ ОБМЕНА КЛЮЧАМИ И ПЕРЕДАЧИ ДАННЫХ В ЗАКРЫТОЙ СТЕГАНОСИСТЕМЕ С ИСПОЛЬЗОВАНИЕМ АДАПТИВНО ФОРМИРУЕМЫХ ДИСКРЕТНЫХ СИГНАЛОВ

Рассмотрена стеганосистема с использованием технологии прямого расширения спектра. Для ее практического применения в телекоммуникационных системах и сетях предложен протокол обмена ключами и передачи данных в закрытой стеганосистеме с использованием адаптивно формируемых дискретных сигналов.

Ключевые слова: *стеганография, расширение спектра, адаптивно формируемые дискретные сигналы*

Введение

Постановка проблемы в общем виде и анализ литературы. Перспективным направлением в обеспечении безопасности информации в современных телекоммуникационных системах и сетях является цифровая (компьютерная) стеганография, основные средства которой, должны реализовывать требуемые услуги безопасности и обеспечивать предоставление соответствующих информационных сервисов в современных телекоммуникационных системах и сетях [1 – 3]. В тоже время, в связи с бурным развитием современных компьютерных технологий, повышением объемов передаваемой и обрабатываемой информации в телекоммуникационных системах и сетях, появлением новых информационных услуг и сервисов, существующий на сегодняшний день математический аппарат стеганографической защиты информации, не позволяет реализовать обеспечение повышенных требований.

Проведенные исследования и сравнительный анализ известных методов скрытного встраивания и извлечения информации показали, что одним из перспективных направлений в развитии методов стеганографической защиты является использование математического аппарата сложных дискретных сигналов и технологии прямого расширения спектра [1 – 8]. Этот подход позволяет обеспечить высокие показатели безопасности стеганосистем, организуемые стеганографические каналы обладают всеми преимуществами широкополосных систем связи, а именно высокой безопасностью и достоверностью передачи данных, устойчивостью к несанкционированному ознакомлению (извлечению) и детектированию [4 – 8].

Однако в существующей литературе не приведены алгоритмы или протоколы распределения ключей и обмена скрытыми сообщениями для практической реализации стеганографии с использованием сложных дискретных сигналов и технологии прямого расширения спектра. **Целью статьи** является разработка именно такого протокола.

Изложение основного материала

Описание стеганосистемы с использованием сложных дискретных сигналов и технологии 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 [4 – 8] 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 (ИС) 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 ИС;

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

$\Phi_j = (\varphi_{j_0}, \varphi_{j_1}, ..., \varphi_{j_{n-1}})$ – расширяющий кодовый сигнал длины n из ансамбля (множества) слабокоррелированных друг с другом псевдослучайных последовательностей (ПСП) $\Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\}$;

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

где 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 статистическим 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:

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

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:

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

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:

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

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.

При этом, проведенные исследования [4 – 8] показали, что применение элементов теории конечных полей позволяет синтезировать дискретные сигналы с особыми корреляционными свойствами. Мощность ансамбля формируемых дискретных сигналов и величины боковых выбросов функций корреляции определяются свойствами используемых примитивных многочленов.

Описание закрытой стеганосистемы

В стеганографической системе, информационное сообщение после предварительного кодирования, утаивается в цифровом контейнере с помощью полученных анализатором данных. Стеганограмма передается на приёмную сторону и декодируется стеганодекодером. Основным элементом, предна-

значенным для установления факта наличия сообщения в полученном контейнере, является детектор, который и определяет решение относительно принятого сообщения.

Согласно данным, которые требует для своей работы детектор, принята следующая общая классификация стеганосистем: открытые, полузакрытые, закрытые и сверхзакрытые (табл. 1).

Таблица 1

Общая классификация стеганосистем

Классификация стеганосистем	Защищенность / практичность	Вход детектора		Выход детектора	
		Пустой контейнер	Скрываемая информация	Да/Нет	Скрываемая информация
Сверх закрытые	+++/–	+	+	+	–
Закрытые	++/+	+	–	–	+
Полузакрытые	+/++	–	+	+	–
Открытые	-/+++	–	–	–	+

Наиболее практичными считаются открытые системы, так как для функционирования стеганодетектора, в них не нужно ни какой дополнительной информации. Но, с точки зрения обеспечиваемой безопасности, такие системы являются наихудшими.

Наивысшую стойкость, к атакам злоумышленника, имеют сверх закрытые стеганосистемы. Но с точки зрения практической реализации, они требуют чрезвычайно много усилий, так как детектор на приемной стороне требует наличие как пустого контейнера так и встроенного сообщения.

Наибольшее развитие, в последнее время, приобрели закрытые и полузакрытые стеганосистемы. Это некоторое компромиссное решение с точки зрения потенциальной безопасности и практичности при реализации процедур сокрытия и извлечения данных. В дальнейшем, будут преимущественно рассматриваться именно закрытые стеганосистемы, соответствующие процедуры стеганокодирования/декодирования будут разрабатываться именно для них.

Разработка протокола обмена ключами и передачи данных в закрытой стеганосистеме с использованием адаптивно формируемых дискретных сигналов

Для практического применения разработанных стеганографических систем защиты информации в телекоммуникационных системах и сетях, предлагается протокол обмена ключами и передачи данных.

Разрабатываемая стеганосистема относится к классу закрытых, то есть, на приемной стороне, получатель, в качестве общесистемных параметров, должен владеть пустым контейнером. Следовательно, протокол обмена ключами и передачи данных должен предполагать обмен и согласования целого спектра общесистемных параметров, устанавливающих как сам пустой контейнер, так и правила формирования и отбора дискретных последовательностей.

Для повышения защищенности информации и реализации обмена сообщениями в условиях взаимного недоверия абонентов предлагается применять несимметричные криптопреобразования. Схема организации обмена в предлагаемых стеганосистемах приведена на рис. 1.

На рис. 1 использованы следующие обозначения:

- $К_{АО}$ – открытый криптоключ пользователя А;
- $К_{АЗ}$ – закрытый криптоключ пользователя А;
- $К_{ВО}$ – открытый криптоключ пользователя В;
- $К_{ВЗ}$ – закрытый криптоключ пользователя В;
- ПП – порождающий полином;
- G – коэффициент усиления.

Предлагаемый протокол обмена ключами и передачи данными состоит в следующем.

На первом этапе происходит генерация сторонами информационного обмена открытых и секретных ключей, после чего осуществляется обмен открытыми ключами.

На втором этапе отправитель формирует общесистемные параметры, в частности, устанавливает правило формирования дискретных последовательностей по полученному, от получателя, пустому контейнера.

На третьем этапе производится стеганокодирование информации, т.е. заполнение контейнера зашифрованными информационными данными, полученная стеганограмма отправляется получателю.

На четвертом этапе происходит извлечение встроенного сообщения на приемной стороне, и, при необходимости, его дешифрование.

Выводы

Таким образом, с использованием предлагаемого протокола обмена ключами и передачи данных реализуется стеганографическое кодирование и декодирование. Организовываемая стеганосистема относится к классу закрытых, робастных или хрупких стеганосистем.

Список литературы

1. Аграновский А.В. Стеганография, цифровые водяные знаки и стеганоанализ / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин. – М.: Вузовская книга, 2009. – 220 с.

2. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – СПб.: Солон-Пресс, 2002. – 272 с.

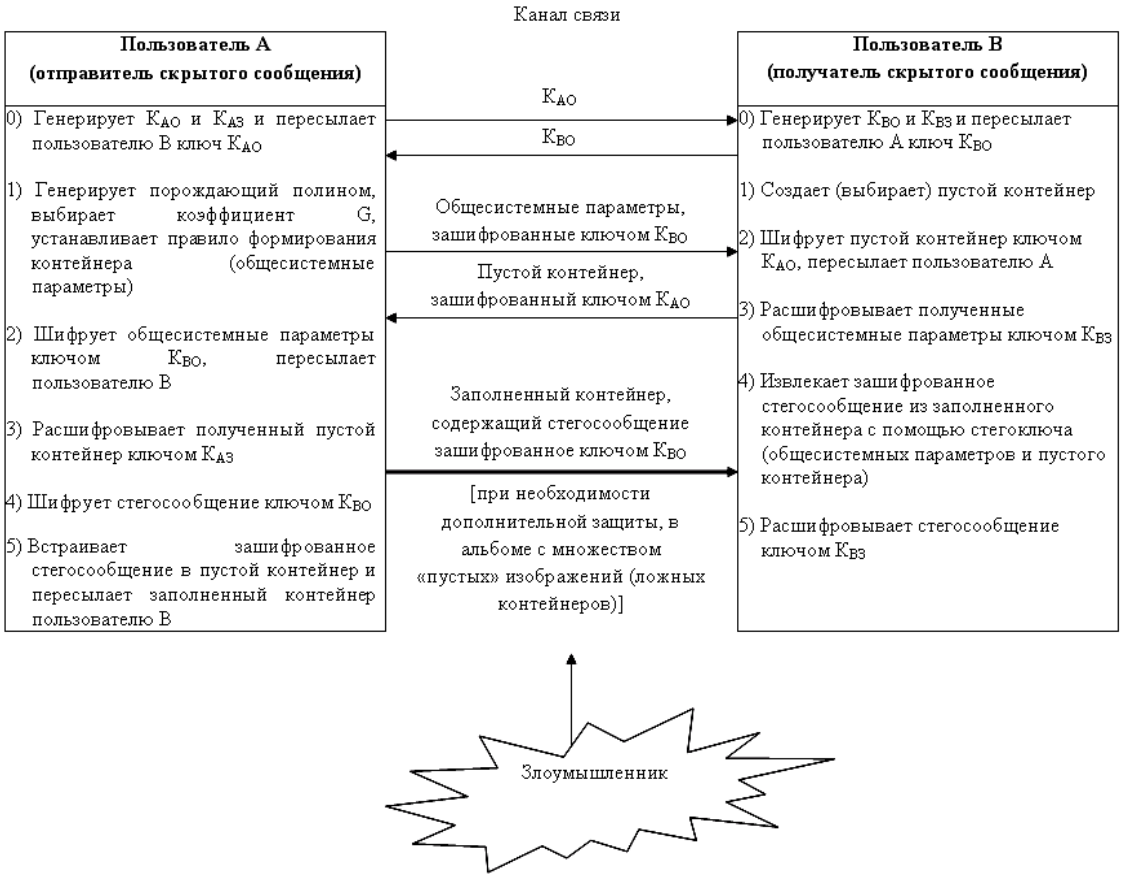

Рис. 1. Протокол организации обмена в предлагаемых стеганосистемах

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

4. Кузнєцов А.А. Встраивание данных в контейнеры-изображения с использованием сложных дискретных сигналов / А.А. Кузнецов, А.А. Смирнов // Радиотехника: Всеукраинский межведомственный научно-технический сборник. Тематический выпуск «Информационная безопасность». – Х.: ХНУРЭ. – 2011. – Вып. 166. – С. 134-141.

5. Kuznetsov A.A. Use of Complex Discrete Signals for Steganographic Information Security / A.A. Kuznetsov, A.A. Smirnov // International Journal of Engineering Practical Education. – USA, Indiana, Riley: Science and Engineering Publishing Company. – 2012. – Vol. 1. – Issue 1. – PP. 21-25.

6. Смирнов А.А. Методы и средства компьютерной стеганографии с применением сложных дискретных сигналов для защиты информации в компьютерных системах и сетях: монографія / А.А. Смирнов. – К.: КОД, 2012. – 350 с.

7. Смирнов А.А. Стеганографическое встраивание данных в неподвижные изображения методом прямого расширения спектра / А.А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – Х.: ХУПС, 2011. – Вип. 2 (6). – С. 126-129.

8. Смирнов А.А. Метод стеганографического встраивания информации в неподвижные изображения с использованием сложных дискретных сигналов и прямого расширения спектра / А.А. Смирнов // Захист інформації. – К.: НАУ, 2011. – Вип. 4 (53). – С. 64-70.

Поступила в редколлегию 4.02.2014

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

ПРОТОКОЛ ОБМІНУ КЛЮЧАМИ І ПЕРЕДАЧІ ДАНИХ У ЗАКРИТІЙ СТЕГАНОСИСТЕМІ З ВИКОРИСТАННЯМ АДАПТИВНО ФОРМОВАНИХ ДИСКРЕТНИХ СИГНАЛІВ

О.А. Смірнов, С.А. Смірнов, Є.В. Мелешко, О.О. Кузнецов

Розглянуто стеганосістему з використанням технології прямого розширення спектра. Для її практичного застосування в телекомунікаційних системах та мережах запропонований протокол обміну ключами і передачі даних в закритій стеганосистемі з використанням адаптивно сформованих дискретних сигналів.

Ключові слова: *стеганографія, розширення спектру, адаптивно формовані дискретні сигнали.*

KEY EXCHANGE PROTOCOL AND DATA TRANSMISSION IN CLOSED STEGANOGRAPHY SYSTEM USING ADAPTIVE DISCRETE SIGNALS FORMED

A.A. Smirnov, S.A. Smirnov, E.V. Meleshko, A.A. Kuznetsov

Considered steganographic system using the technology of direct spreading. For its practical application in telecommunication systems and networks are proposed key exchange protocol and transmitting data in a closed system using steganographic adaptively formed discrete signals.

Keywords: *steganography, spread spectrum, adaptively formed discrete signals.*