ДВУХКАНАЛЬНАЯ СТЕГАНОГРАФИЧЕСКАЯ СИСТЕМА НА ОСНОВЕ МЕТОДА КОНТРОЛЬНОЙ РАЗНОСТИ

М. В. Шакурский
Кафедра теоретической и общей электротехники, Самарский государственный технический университет
Самара, Российская Федерация
E-mail: m.shakurskiy@gmail.com

Рассматривается задача синтеза стеганографической системы на основе метода контрольной разности. Данная система является частным случаем системы на основе контрольной суммы для коэффициентов с изменённым знаком. Реализация такой системы позволяет увеличить устойчивость ко взлому за счёт изменённого алгоритма декодирования. В статье рассмотрена математическая модель такой системы и приведена структурная схема реализации стеганографического кодера и декодера.

Введение

Построение стеганографических систем на основе метода контрольного значения рассмотрено в работе [1]. Основной идеей таких систем является использование информационной избыточности в двух компонентах передаваемого стегоконтейнера, для реализации алгоритма декодирования при неизвестном маскирующем сигнале. Основным достоинством такой системы является возможность использования хаотического маскирующего сигнала, с амплитудой в разы больше амплитуды маскируемого полезного сигнала [2, 3, 4]. Согласно [5] такие системы можно отнести к абсолютно устойчивым.

I. Математическая модель

При формировании стеганографического контейнера для каждой из компонент формируется преобразованный информационный сигнал:

$$u_1(n) = 0.5u(n) \tag{1}$$

где $u(n)$ - передаваемый полезный сигнал; $u_1(n)$ - преобразованный информационный сигнал первого канала.

Заметим, что коэффициент 0,5 не является необходимым для преобразования. Его наличие позволяет повысить устойчивость к коэффициентам преобразования. Сигнал второго канала связан с сигналом первого канала через контрольное значение [6, 7]. При этом воспользуемся контрольной разностью:

$$u_2(n) = u_1(n) - K_1 \tag{2}$$

где K_1 - значение первого ключа (контрольное значение).

Общий вид стеганографического преобразования [1, 8] описывается следующими выражениями:

$$\begin{cases} y_1(n) = u_1(n) + \phi[u_1(n), z(n)]; \\ y_2(n) = u_2(n) + \phi[u_2(n), z(n)]. \end{cases} \tag{3}$$

где z – отсчёты маскирующего сигнала; u – отсчёты скрываемых данных; ϕ – функция стеганографического преобразования.

Устройство реализует линейную модель стеганографического преобразования. Функция стеганографического преобразования имеет следующий вид:

$$\begin{array}{l} \phi_1(n) = u_1(n) + (K_2 + u_1(n))z(n); \\ \phi_2(n) = u_2(n) + (K_3 + u_2(n))z(n). \end{array} \tag{5}$$

Система уравнений (5) является математической моделью кодера. В обоих уравнениях (5) используются одни и те же отсчёты маскирующего сигнала. Передача двух сигналов осуществляется с помощью известных устройств передачи информации, например, устройств передачи стереофонического аудио-сигнала, квадратурно-амплитудно модулированного сигнала и других устройств.

Отношение значений встраиваемых данных к значениям маскирующих сигналов может быть много меньше единицы [7, 8]. Полученные сигналы (5) являются заполненным стегоконтейнером. Отличительной особенностью сформированного в соответствии с (5) контейнера является наличие двух компонент, имеющих в своём составе общую маскирующую составляющую z. Эта особенность позволяет использовать для вскрытия контейнера функциональные сжимающие отображения [1].

Сигналы после преобразования попадают в систему передачи информации, включающую в себя устройства преобразования сигнала, передающие и приёмные устройства, и линию передачи информации. В качестве примера системы передачи информации, реализующей одновременную передачу двух сигналов по одному каналу связи можно рассмотреть систему передачи стерео аудио-сигнала.

Извлечение скрываемого сигнала выполняется с помощью обратного стеганографического преобразования. Для извлечения скрываемого сигнала принимающей стороной необходимо знать значения ключей K_1 , K_2 и K_3 . Извлечение скрываемой информации из контейнера (5) выполняется с помощью сжимающих преобразований. Восстановление двух сигналов (1) и (2) из контейнера выполняется с помощью следующих

выражений [3]:

$$\begin{array}{l} u_{1C}(n) = \frac{y_1(n)(K_1-K_3)+K_2(K_1+y_2(n))}{K_2-K_3+y_1(n)-y_2(n)} \\ u_{2C}(n) = \frac{y_2(n)(K_1+K_2)+K_3(K_1-y_1(n))}{K_2-K_3+y_1(n)-y_2(n)} \end{array} \quad (6)$$

Затем восстанавливается скрытый сигнал:

$$u_C(n) = u_{1C}(n) + u_{2C}(n) + K_1 \quad (7)$$

Объединяя выражения (6) и (7) получим:

$$u_C(n) = \frac{y_1(n)k_1 + y_2(n)k_2 + k_3}{k_4 + y_1(n) - y_2(n)} \quad (8)$$

где коэффициенты k формируются из значений ключей K следующим образом:

$$\begin{array}{l} k_1 = 2(K_1 - K_3); k_2 = 2K_2; \\ k_3 = 2K_1K_2; k_4 = K_2 - K_3. \end{array} \quad (9)$$

Выражение (8) является математической моделью декодера.

II. Структурная модель

Сформируем на основании математической модели стего-кодера (5) и математической модели стего-декодера (8), с учётом выражений формирования коэффициентов (1, 2, 9) структурную модель стеганографической системы на основе метода контрольной разности (рис. 1).

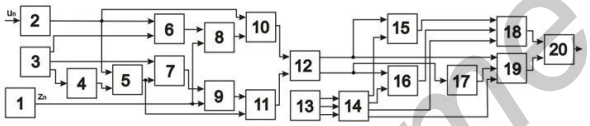

Рис. 1 – Структурная модель стегосистемы

Устройство (рис. 1) содержит блок формирования маскирующего сигнала 1, блок ослабления сигнала 2, первый и второй блоки памяти ключей 3 и 13, два блока инверторов 4 и 17, семь блоков суммирования соответственно 6, 10, 7, 11, 19, 18 и 5, четыре блока умножения соответственно 8, 9, 15 и 16, блок устройства передачи информации 12, блок формирования коэффициентов 14, блок деления 20. Блоки 1 – 11 формируют устройство стего-кодера. В соответствии с выражениями (1), (2) и (5). Блок 12 является блоком передачи информации и может содержать в себе любую известную систему передачи информации, обеспечивающую неискаженную передачу информации. Блоки 13 - 20 представляют собой структурную модель стего-декодера, построенную в соответствии с выражениями (8) и (9).

III. Выводы

Разработанная стеганграфическая система является частным случаем стеганографической системы, использующей, в качестве контрольного значения - контрольную сумму. Использование представленной системы позволяет расширить количество модификаций системы и, при сходных свойствах осложнить стегоанализ. Отметим, что выражение (8) представляет собой отношение и, как следствие, обладает точками разрыва. Наибольшая чувствительность системы наблюдается вблизи точек разрыва данной функции. Однако, в этом случае аддитивный шум в канале может привести к разрыву функции и, как следствие, к значительной ошибке восстановления сигнала. Таким образом, реализация данной системы защиты информации подразумевает точную передачу информации по телекоммуникационным каналам. В частности, с использованием сетевых протоколов, обеспечивающих передачу информации без потери и искажений.

Список литературы

1. Шакурский, М.В. Сжимающие отображения в инвариантных преобразователях и системах стеганографии / В.К. Шакурский, М.В. Шакурский // Монография. Издательство СНЦ РАН, Самара 2014., 159 с.
2. Пат. 2546307 Российская федерация, МПК H03L 9/00, H03K 3/00 Устройство сокрытия информации / М.В. Шакурский, В.К. Шакурский; Опубл. 10.04.2015 Бюл. 10.
3. Пат. 2546306 Российская федерация, МПК H03L 9/00, H03K 3/00 Способ скрытой передачи информации / М.В. Шакурский, В.К. Шакурский; Опубл. 10.04.2015 Бюл. 10.
4. Обработка и преобразование сигналов в радиотехнических и инфоком-муникационных системах : монография / под ред. В. И. Воловача. – М. : Радио и связь, 2014. – 448 с. : ил.
5. J. Fridrich Steganography in digital media. Principles, Algorithms and applications. Cambridge university press, New York, 2010.
6. Шакурский, М.В. Формирование контейнера для стеганографической системы на основе сжимающих отображений / М.В. Шакурский // Международный научно-технический журнал «Радиотехника». – 2015. – №2. –С. 134-139.
7. Shakurskiy, M.V. Two-channel real-time steganographic system / M.V. Shakurskiy, V.K. Shakurskiy, V.I. Volovach // Proceedings of IEEE East-West Design and Test Symposium (EWDTS 2014) / KNURE, Kharkov 2014 p. 309-311.
8. Шакурский, М.В. Стеганографическая система на основе сжимающих отображений [Текст] / М.В. Шакурский, В.К. Шакурский // Научно-практический журнал «Вопросы защиты информации». – 2015. – №2. –С. 74-78.