

УСТРОЙСТВО СОКРЫТИЯ ИНФОРМАЦИИ НА ОСНОВЕ СЖИМАЮЩИХ ОТОБРАЖЕНИЙ

М.В. Шакурский, В.К. Шакурский

Кафедра «Информационный и электронный сервис», кафедра электроснабжения и электротехники,
Поволжский государственный университет сервиса
Тольяттинский государственный университет
Тольятти, Российская Федерация
E-mail: m.shakurskiy@gmail.com, shakurskiy@mail.ru

Рассматривается способ и устройство встраивания полезной информации в маскирующий сигнал. Способ основан на сжимающих отображениях, которые разработаны для инвариантных преобразователей. Устройство реализует встраивание и извлечение информации с точностью, ограниченной разрядностью данных, при соотношении амплитуд полезного сигнала и маскирующего сигнала много меньше единицы. В работе рассматривается использование условия контрольной суммы.

ВВЕДЕНИЕ

В цифровой стеганографии [1, 2] рассматриваются вопросы встраивания полезной информации в маскирующий сигнал и образование стегоконтейнера. В рамках данной работы рассматривается встраивание полезного сигнала в маскирующий шумовой сигнал и образование двухкомпонентного стегоконтейнера. Маскирующий сигнал рассматривается как возмущающий, одинаковый для обоих компонент стегоконтейнера. Сжимающие отображения исключают возмущающий сигнал и восстанавливают полезную информацию [3]. В работе показан алгоритм и устройство встраивания и извлечения полезной информации.

I. ПОСТАНОВКА ЗАДАЧИ

Анализ полученных в [3] алгоритмов сжатия показывает, что использование метода контрольного значения позволяет исключать влияние возмущающих сигналов, амплитуда которых превосходит амплитуду полезного сигнала. Таким образом, формируя стегоконтейнер под соответствующий алгоритм сжатия, например, использующий условие контрольной суммы, можно строить теоретически устойчивую стегосистему. Особенностью данных стегосистем является необходимость формирования двух компонент передаваемой информации. Ниже приводятся результаты исследования разработанных стегосистем.

II. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СТЕГАНОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

Рассмотрим двухкомпонентную стегосистему, в которой реализуется условие контрольной суммы. В основу стеганографического преобразования положим следующие уравнения в функции текущего номера отсчёта значений встраиваемых данных и маскирующего сигнала [3]:

$$\begin{cases} u_1(n) = y_1(n) + \varphi_1[y_1(n), z(n)]; \\ u_2(n) = y_2(n) + \varphi_2[y_2(n), z(n)]. \end{cases} \quad (1)$$

где z - значения маскирующего сигнала; y - значения встраиваемых данных; φ - функция стеганографического преобразования.

Исследуем следующее стеганографическое преобразование:

$$\begin{cases} u_1(n) = y_1(n) + [k_1 + y_1(n)]z(n); \\ u_2(n) = y_2(n) + [k_2 + y_2(n)]z(n); \end{cases} \quad (2)$$

Выбор коэффициентов преобразования k произволен, но может повлиять на устойчивость стегосистемы. Значения встраиваемых данных формируются из исходных данных $y(n)$ следующим образом:

$$y_1(n) = 0.5 y(n), \quad y_2 = U - y_1(n). \quad (3)$$

Система уравнений (2) является математической моделью кодера. В обоих уравнениях (2) используются одни и те же отсчёты маскирующего сигнала. Передача двух сигналов осуществляется с помощью известных устройств передачи информации, например, устройств передачи стереофонического аудиосигнала, квадратурно-амплитудно модулированного сигнала и других устройств. Отличительной особенностью сформированного в соответствии с (2) контейнера является наличие двух сигналов, имеющих в своём составе общую маскирующую компоненту. Эта особенность позволяет использовать для вскрытия контейнера функциональные сжимающие отображения [3]. Рассмотрим эффективность маскировки скрываемого сигнала. Возьмём в качестве скрываемого сигнала гармоническое колебание, а в качестве маскирующего случайный сигнал с равномерным распределением плотности вероятности. Сформируем первый и второй сигналы. Вид сигналов приведён на рис. 1. Отношение значений встраиваемых данных к значениям маскирующих сигналов взято много меньше единицы.

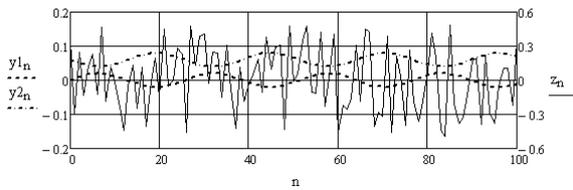


Рис. 1 – Входные сигналы стegosистемы

Сравним спектр полезного сигнала (рис. 2) и спектры первой (рис. 3) и второй (рис. 4) компонент сигнала после стеганографического преобразования. Спектр встраиваемого сигнала представляет собой одну составляющую с частотой, соответствующей номеру 40 нормированной шкалы частот. Видно, что гармоника скрываемого сигнала в спектре сигнала стегоконтейнера не выделяется.

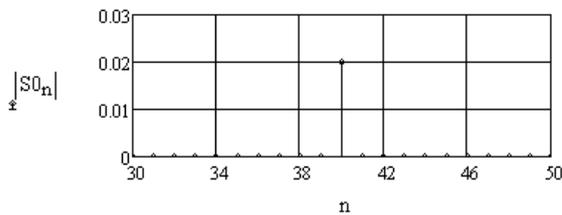


Рис. 2 – Спектр полезного сигнала

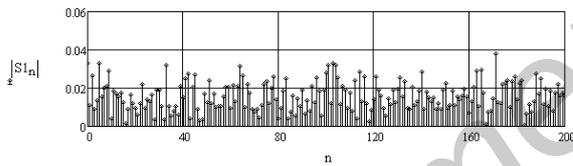


Рис. 3 – Спектр первой компоненты сигнала стegosистемы

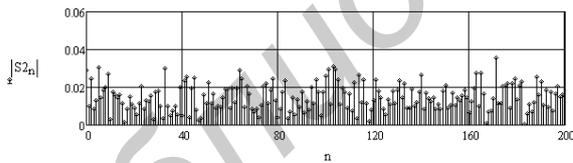


Рис. 4 – Спектр второй компоненты сигнала стegosистемы

Извлечение полезной информации из контейнеров (2) выполняется с помощью сжимающих преобразований, которые приводятся к виду:

$$y_{1C}(n) = \frac{u_1(n)(k_2 + U) + k_1(U - u_2(n))}{k_1 + k_2 + u_1(n) + u_2(n)}; \quad (4)$$

$$y_{2C}(n) = \frac{u_2(n)(k_1 + U) + k_2(U - u_1(n))}{k_1 + k_2 + u_1(n) + u_2(n)}. \quad (5)$$

Затем восстанавливаются исходные данные:

$$y_C(n) = y_{1C}(n) - y_{2C}(n) + U. \quad (6)$$

Таким образом, для вскрытия контейнера необходимо знать три константы, которые рассматриваются как ключи.

III. СТРУКТУРНАЯ СХЕМА СТЕГОСИСТЕМЫ

Рассмотрим структурную модель, реализующую прямое (2, 3) и обратное (4, 5, 6) стеганографические преобразования (рис. 5).

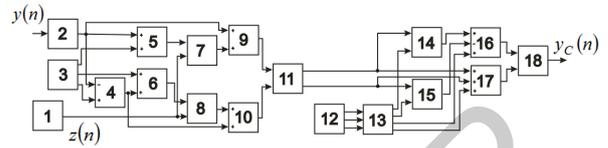


Рис. 5 – Структурная схема стegosистемы

Представленная на рис. 1 структурная схема содержит блок ослабления сигнала 2, первый и второй блоки памяти ключей 3 и 12, блок формирования маскирующего сигнала 1, блок вычитания 4, шесть блоков суммирования соответственно 5, 9, 6, 10, 17 и 16, четыре блока умножения соответственно 7, 8, 14 и 15, блок устройства передачи информации 11, блок формирования коэффициентов 13, блок деления 18. Блоки с первого по десятый представляют собой устройство встраивания полезной информации в контейнер в соответствии с выражениями (2, 3). В частности, в блоке 2 формируется сигнал $y_1(n)$, а в блоке 4 сигнал $y_2(n)$ в соответствии с выражением 3. На выходах блоков 9 и 10 в соответствии с выражениями (2) формируются сигналы $u_1(n)$ и $u_2(n)$. Блок 11 представляет собой устройство передачи информации. Блоки с 12 по 18 представляют собой устройство декодирования информации на основе выражений (4, 5, 6).

IV. ВЫВОДЫ

Разработанное устройство позволяет реализовать стеганографическое преобразование при достаточно малом соотношении амплитуд полезного сигнала и маскирующего сигнала. Помимо этого стegosистема инвариантна к маскирующему сигналу. Восстановление информации требует знания трёх ключей. Важным свойством является возможность восстановления информации с точностью, ограниченной разрядностью данных. Спектр маскирующего сигнала совпадает со спектром скрываемых данных, что не позволяет выделить скрытую информацию путём частотной фильтрации.

1. Сергиенко, А. Б. Цифровая обработка сигналов: учеб. пособие / А. Б. Сергиенко // Спб.: Питер, 2004. – 751 с.
2. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев // М.: Солон-Пресс, 2002. – 272 с.
3. Шакурский, В. К. Сжимающие отображения в инвариантных преобразователях и системах стеганографии / В. К. Шакурский, М. В. Шакурский // Самара.: СЦ РАН – 2014. – 159 с.