ПРИНЦИП ИНВАРИАНТНОСТИ В СИСТЕМАХ СТЕГАНОРАФИИ

М. В. Шакурский, В. К. Шакурский
Кафедра информационного и электронного сервиса, кафедра электроснабжения и электротехники,
Поволжский государственный университет сервиса, Тольяттинский государственный университет
Тольятти, Российская Федерация
E-mail: m.shakurskiy@gmail.com, shakurskiy@mail.ru

Рассматривается общий вопрос использования инвариантных преобразований для построения стеганографических систем. В основе принципа лежит использование преобразований, как функции полезного и маскирующего сигналов, при том, что обратное преобразование не зависит от маскирующего сигнала. При этом защищённость системы обеспечивается наличием ключей, или коэффициентов, обспечивающих невозможность корректной реализации обратного преобразования. Показан как общий подход к реализации таких преобразований, так и пример частных решений.

Введение

В цифровой стеганографии [1] рассматриваются вопросы встраивания полезной информации в маскирующий сигнал и её последующего извлечения. Одним из перспективных направлений развития стеганографии является использование хаотического сигнала в качестве маскирующего. При этом возникает задача извлечения сигнала. Эффективным способом решения данной задачи является использование инвариантных алгоритмов, позволяющих реализовать извлечение полезного сигнала не зная маскирующий сигнал. В данной статье приведён общий подход к формированию инвариантных алгоритмов на примере метода контрольного значения.

I. Постановка задачи

Получение алгоритма извлечения полезной информации из стего-контейнера без знания маскирующего сигнала возможно осуществить как на основе статистического анализа данных, так и на основе информационной изюыточности. Статистические методы не всегда дают точный результат, ы то время, как инвариантные алгоритмы позволяют получить точное восстановление сигнала. В основе инвариантных структур лежит принцип двухканальности Б.Н. Петрова, положенный в основу работы [2]. Таким образом реализация инвариантного стеганографического преобразования может быть реализована в двухканальной системе, обладающей информационной избыточностью.

II. Общий подход к формированию инваринтного преобразования

Формирование двухканальной стеганографической системы можно описать, в общем случае в виде системы уравнений:

$$\begin{cases} u_1(n) = f_1(y(n), z(n), k_1(n), ..., k_m(n)); \\ u_2(n) = f_2(y(n), z(n), k_1(n), ..., k_m(n)). \end{cases} \quad (1)$$

где y - значения отсчётов встраиваемых данных; z -значения отсчётов маскирующего сигнала; k - значения отсчётов ключей; f - функции стеганографического преобразования.

Рассмотрим систему уравнений (1) подробнее. Функции u_1 и u_1 представляют собой две компоненты стеганографического контейнера, которые могут интерпретироваться как элементы двухканальной системы или как элементы одноканальной системы, при обеспечении их корректного получения принимающей стороной. При этом декодирование информации происходит в соответствии со следующим выражением:

$$y(n) = f(u_1(n), u_2(n), k_1(n), ..., k_m(n)); \quad (2)$$

Для того, чтобы выражение (2) был реализуемо, необходимо, чтобы система уравнений (1) имела не более двух неизвестных. Одна из неизвестных это величина $z(n)$, вторая - $y(n)$. Основная задача преобразования заключается в обеспечении заданного уровня сокрытия, выражающегося в устойчивости к различного вида атакам и потенциальной вероятности обнаружения наличия скрытого сигнала.

Очевидно, что возможных вариантов систем уравнений, соответствующих выражениям (1) и (2) может быть много. Условие инвариантности позволяет использовать в качестве маскирующего сигнала практически любой сигнал, а разность амплитуд между маскирующим и маскируемым сигналом ограичивается только разрядной сеткой. Таким образом эффективным решением задачи сокрытия сигнала на основе преобразований (1) и (2) является использование хаотического маскирующего сигнала. Обеспечивая достаточное соотношение амплитуд маскирующего и маскируемого сигналов можно получить достаточно устойчивую систему сокрытия информации. Устойчивость стеганографической системы к обнаружению обеспечивается наличием ключей k в преобразованиях.

Так как формируемая на основе выражения (1) система имеет два отсчёта, каждый из которых является функцией маскирующего и маскируемого сигналов, использование линейных преобразований приведёт к значительному сходству

характера изменения двух сигналов. Поэтому в основе формирования инвариантных преобразований должен лежать принцип их нелинейности. Другим важным аспектом должно быть сходство сигналов в плане плотности распределения и в плане занимаемой ими полосы частот. Отсюда следует условие эффективности преобразования вида (1) - формируемые компоненты стеганографического преобразования должны занимать одинаковые полосы частот, иметь сходный характер плотности распределения и иметь разный характер изменения в зависимости от маскирующегои маскируемого сигналов.

Одним из возможных решений поставленной задачи является метод контрольного значения. Рассмотрим пример реализации инвариантнго преобразования на основе метода контрольного значения.

III. Метод контрольнго значения

В основе метода контрольного значения является помещение в первое и второе уравнения системы (1) не сигнала $y(n)$, а сигналов $y_1(n)$ и $y_2(n)$ связанных контрольным значением k_1 знание которого принимающей стороной является обязательным условием для корректного вскрытия стего-контейнера. Важно отметить, что контрольное значение также может являться функцией отсчёта $k_1(n)$, что позволит сформировать разный характер изменения одного из аргументов выражения (1).

Стоит отметить что значения переменных $y_1(n)$ и $y_2(n)$ могут быть связаны со значением $y(n)$ с помощью различных преобразований. К простейшим можно отнести контрольную сумму:

$$y_1(n) = 0.5\ y(n), \quad y_2 = k_1(n) - y_1(n). \qquad (3)$$

Контрольную разность:

$$y_1(n) = 0.5\ y(n), \quad y_2 = y_1(n) - k_1(n). \qquad (4)$$

Контрольное отношение:

$$y_1(n) = y(n), \quad y_2 = \frac{y_1(n)}{k_1(n)}. \qquad (5)$$

Каждое из приведённых преобразований влияет на свойства стеганографической системы и может быть использовано при формировании инваринтного стеганографического преобразования на основе системы уравнений вида (1). Представленные выше соотношения на основе метода контрольного значения являются простейшими и могут иметь более сложный вид.

IV. Стеганографическое преобразование на основе метода сжимающих отображений

Одним из эффективных способов формирования инвариантных преобразований для стеганографических систем является метод сжимающих отображений, подробно рассмотренный в работе [2]. Сжимающие отображения хорошо согласуются с инвариантными преобразованиями, если считать, что информационное пространство определяется всеми маскирующими отклонениями, которые являются решениями или неподвижными точками. таким образом, на основе итеративных процедур могут быть синтезированы инвариантные преобразования для систем стеганографии. В частности, в работах [5] и [6] описаны способ и устройство сокрытия информации на основе метода сжимающих отображений для условия контрольной суммы (3).

Заключение

В работе рассмотрен общий подход к формированию стеганографических преобразований, инвариантных к маскирующему сигналу. Описаны условия, соблюдение которых является необходимым для обеспечения устойчивости двухкомпонентных, или, в частном случае, двухканальных стеганографических систем с информационной избыточностью к стегоанализу. На основе проведённых исследований, сделан вывод, что использование сжимающих отображений является эффективным средством синтеза стеганоррафических преобразований. Обосновано использование метода контрольной суммы в двухкомпонентных стеганографических преобразованиях.

1. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков , И. В. Туринцев // М.:Солон-Пресс,2002. – 272 с.
2. Шакурский, В.К. Сжимающие отображения в инвариантных преобразователях и системах стеганографии / В. К. Шакурский, М. В. Шакурский // Самара.:СНЦ РАН – 2014.- 159 с.
3. Шакурский, В.К. Стеганографическая система на основе сжимающих отображений / В. К. Шакурский, М. В. Шакурский // Научно-практический журнал «Вопросы защиты информации», №2 – 2015.- С. 74-78.
4. Шакурский, М.В. Формирование контейнера для стеганографической системы на основе сжимающих отображений / М. В. Шакурский // Международный научно-технический журнал «Радиотехника», №2 – 2015.- С. 134-139.
5. 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.
6. 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.