# Стеганоанализ графических изображений на основе вейвлет-анализа

Лобач С.В.
Белорусский государственный университет
г. Минск, Республика Беларусь
e-mail: sergey_lobach@mail.ru

***Аннотация*—Рассматривается применение вейвлет- преобразовния к встраиванию и обнаружению скрытых ссбщений в изображениях.**

***Ключевые слова:* вейвлет-преобразование, стеганоанализ, растровое изображениех.**

## Введение

В настоящее время стеганография стремительно развивается [1,2,3]. Статистические проблемы стеганографии недостаточно разработаны, поэтому актуальной задачей является проблема построения новых и анализа существующих методов стегано анализа. Большинство исследований в области стеганографии посвящено использованию в качестве стеганоконтейнеров цифровых изображений. Это обусловлено следующими причинами: 1) относительно большим объемом цифрового представления, что позволяет внедрять сообщение большого объема либо повышать скрытность внедрения, 2) наличием в большинстве реальных изображений текстурных областей, имеющих шумовую структуру и хорошо подходящих для встраивания информации, 3) слабой чувствительностью человеческого глаза к незначительным изменениям цветов изображений, его яркости, контрастности, содержанию в нем шума, искажения вблизи контуров, 4) хорошо разработанными в последнее время методами цифровой обработки изображений. Надо отметить, что последняя причина вызывает значительные трудности в обеспечении скрытости секретных сообщений: чем более совершенными становятся методы сжа тия, тем меньше остается возможностей для встраивания посторонней информации. Для скрытия информации в частотной области наиболее часто применяется дискретное вейвлет-преобразование, которое может применяться либо ко всему изображению, либо к его отдельным частям.

## I. Методы скрытия, использующие изображения

Данные могут быть скрыты цветным изображением. Переведенные в цифровую форму изображения состоят из пикселей (элемент картинки), в котором обычно каждый пиксель использует 24 бита (три байта). Каждый байт представляет представляет один из первичных оттенков цвета (красный, зеленый, синий). Поэтому можно взять 28 различных оттенков каждого цвета. В методе, названном LSB (Last Signification Bit), самый младший бит каждого байта установлен на нуль. От этого изображение становится немного светлее в некоторых областях. Теперь мы можем скрыть двоичные данные в изображении, сохраняя или изменяя самый младший бит. Если наша двоичная цифра 0, то мы сохраняем бит, если это 1, то мы изменяем бит на 1. Этим способом мы можем скрыть символ (восемь битов ASCII) в трех пикселях. Такой метод применяется к растровым изображениям, представленным в формате без компрессии. Одним из таких форматов является BMP. Положительной стороной BMP является высокое качество изображения, а также простота формата, что делает его популярным для применения в качестве контейнера.

Еще один метод стеганографического преобразования информации основан на использовании особенностей файлов, сжатых с потерей данных. При скрытии в JPEG-файлы информация прячется не в значения цветовых составляющих отдельных пикселей, а в биты квантованных дискретных коэффициентов. Возможны другие варианты для изменения битов, в байтах, например, определенных некоторым ключом. Секретное сообщение может быть, например, закрыто аудио- (звук и музыка) и видеоинформацией. И аудио, и видео сегодня подвергаются сжатию. Секретные данные могут быть внесены в информацию в процессе и перед сжатием. При встраивании сообщения в контейнер следует учитывать следующие проблемы.

Искажения, вносимые скрытыми сообщениями должны быть неощутимо малы..

Система встраивания разрабатывается так, чтобы она удовлетворяла определенным условиям шума. Встроенные данные могут подвергаться большому числу различных атак, так что реальный шум может быть сильно изменен. Консервативная установка на условии сильного шума ведет к снижению пропускной способности, в то время как агрессивная установка на легкий шум может привести к искажению встроенных битов.

Неодинаковое распределение способности к встраиванию, количество данных, которые могут быть встроены, сильно меняется от области к области изображения или видео. Это вызывает большие трудности для встраивания с большей пропускной способностью.

Базовой операцией для любой системы встраивания является встраивание одного бита. Все подходы встраивания базируются на одном из двух основных механизмов. В первом механизме вторичные данные добавляются к чистому сигналу. Сложение может производиться на специфической области или на специфических признаках. При встраивании одного бита $b$ разница между помеченными данными и чистым сигналом есть функция от $b$ : $I_1 - I_0 = f(b)$ . При обнаружении $I_0$ может быть основным источником шума. Пример

использования первого механизма — аддитивное спектральное встраивание с растяжением. Пространство сигнала делится на подмножества, каждое из которых отображается некоторой функцией на множестве значений, определенных вторичными данными.. Для минимизации заметных искажений, $I_1$ должен быть по возможности близок к $I_0$. Примером использования второго механизма является четно-нечетное встраивание, при котором ближайшее четное число используется для кодирования “0”, а ближайшее нечетное- “1”. Применение механизма второго типа не требует знаний $I_0$ для извлечения скрытого сообщения.

## II. Методы стеганоанализа контейнеров-изображений

Анализ существующих методов стеганоанализа показал, что в зависимости от используемых исходных данных их можно разделить на две основные группы: 1) методы, предназначенные для работы с конкретными заранее известными стеганографическими алгоритмами, 2) методы, предназначенные для любых алгоритмов стеганографии, поэтому стеганоанализ этими методами не требует знания использованного стеганографического алгоритма, алгоритмы шифрования, ключа и длины сообщения. Известные методы этой группы обычно построены на алгоритмах, требующих предварительного "обучения" на сериях из заполненных и пустых контейнеров. Методы обеих групп построены с учетом предположении о недоступности пустого контейнера, который был использован для внедрения информации в исследуемый стеганоконтйнер. К первой группе относится сигнатурные и схемные методы анализа. Во вторую группу входят визуальные и статистические методы [ ]. Статистические критерии обнаружения факта встраивания информации в графические изображения базируются на понятии “естественного” контейнера. Идея методов заключается в оценивании вероятности существования стеганографического вложения с неизвестной стеганосистемой на основе критерия оценки близости исследуемого контейнера к “естественному”. К достоинствам статистических методов относится неограниченная область применения, что довольно существенно как при проверке гипотезы о наличии стеганографического вложения с неизвестной стеганосистемой, так и при разработке схемных методов стеганоанализа. Метод анализа распределения пар значений основан на критерии $\chi^2$. В этом методе используется анализ гистограммы, полученной по элементам изображения и оценка распределения пар значений этой гистограммы. Для GIF-файлов пары значений формируются значениями пикселей изображения. Младшие биты изображений не являются случайным. Частоты двух соседних элементов контейнера должны находиться далеко от значения частоты среднего арифметического этих элементов. В пустом изображении ситуация, когда частоты элементов со значениями $2N$ и $2N+1$ близки по значению, встречается редко. При встраивании сообщения данные частоты сближаются или становятся равными. Идея атаки $\chi^2$ заключается в поиске этих близких значений и подсчете вероятности встраивания на основе того, как близко располагаются значения частот четных и нечетных элементов анализируемого контейнера. Для применения данного метода необходимо знать, каким образом вычисляется значение статистики $\chi^2$ с одной степенью свободы. Делается это по формуле:

$$\chi^2 = \sum \frac{(h-m)^2}{m},$$

где h- число нулей в наименьших значащих битах стеганографического контейнера, m- число единиц.

## III. Методы оценки частот появления К-битовых серий в потоке элементов контейнера

В данной работе рассматривается один из наиболее популярных статистических методов стеганоанализа- метод оценки частот появления К-битовых серии в потоке элементов изображений, только он применяется не к самому стеганоконтейнеру, а его образу, полученному путем его сжатия с помощью вейвлета Хаара.

Метод позволяет оценить равномерность распределения элементов в исследуемой последовательности на основе анализа частоты появления нулей и единиц, и серии, состоящей из К бит. В битовом представлении исследуемой последовательности x(t) подсчитывается, сколько раз встречаются нули и единицы (0,1, к = 1), серии-двойки (00, 01, 10, 11 : к = 2), серии- тройки (000, 001,010, 011, 100, 101, 110, 111 : к = 3) и т.д. На основе результатов строится гистограмма. Для сжатия изображений гистограмма строится по значениям частот появления битовых серии в потоке вейвлет-коэффициентов.

Оказалось, что для незаполненных изображений не является характерным, чтобы значения частот всех комбинации были одинаковыми, при внедрении информации значения частот серии становятся приблизительно равными. Результаты работы алгоритма зависят от стеганографического преобразования, используемого для встраивания скрываемых данных, а также от их объема. Результаты численного моделирования показали, что выявление факта скрытия осуществимо при заполнении обычного контейнера на 60% и выше, а для сжатого – на 50% и выше.


[1] Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: Солон Пресс, 2002.

[2] Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Киев: Мн-Пресс, 2006.

[3] Барсуков В.С., Романцев А.П. Компьютерная стеганография вчера, сегодня, завтра. –Специалная техника, №4-5, 1998.

[4] Добеши И. Десять лекций по вейвлетам. Ижевск: “Регулярная и хаотическая динамика”, 2001