Сравнение методов стеганографии в изображениях

Виталий Мартовицкий[1], Елизавета Кортяк[1]

1. Кафедра электронных вычислительных машин, Харьковский национальный университет радиоэлектроники, УКРАИНА, г. Харьков, пр. Науки, 14,
E-mail: vitalii.martovytskyi@nure.ua

1. Кафедра электронных вычислительных машин, Харьковский национальный университет радиоэлектроники, УКРАИНА, г. Харьков, пр. Науки, 14,
E-mail: yelyzaveta.kortiak@gmail.com

Steganography is a method of hiding information in other information of different format (container). There are many steganography techniques with various types of container. In the Internet, digital images are the most popular and frequently used containers. We consider main image steganography techniques and their advantages and disadvantages. We also identify the requirements of a good steganography algorithm and compare various such algorithms.

Ключевые слова – стеганорграфия, искажение данных, скрытый канал связи.

I. Введение

Назначение компьютерной безопасности состоит в защите информации от несанкционированного доступа, случайного или целенаправленного искажения данных без изменения основных свойств файлов. Криптография создавалась как методика для защиты систем связи методами кодирования и последующей расшифровки данных. Стеганография дополняет криптографию, скрывая сам факт наличия сообщения в передаваемом потоке данных. Стеганографию можно рассматривать как создание скрытого канала связи.

II. Стеганографические изображения

Скрытое сообщение можно инкапсулировать практически во все виды данных. Большинство инструментов стеганографии ориентируется на передачу сообщения в Интернете, где значительная часть информации передается в виде изображений. При обработке изображения- контейнера учитывают формат файла, в частности методы сжатия. От этого зависят как методы инкапсуляции, так и объем стеганограммы, которую можно вставить в файл. Сложность процедур стеганографии также зависит от формата контейнера.

III. Классификация методов стеганографии для изображений-контейнеров

В течение всего периода развития стеганографии было разработано множество методов, зависящих от форматов изображений и от применяемого аппаратного обеспечения. Методы стеганографии для изображений можно разделить на два класса: методы для временной области [1, 2] и методы для частотной области [1–3]. Для временной области основные процедуры инкапсулируют скрытое сообщение в младшие биты цифрового кода пикселов изображения. Для частотных процедур стеганограмма вставляется в частотную характеристику изображения. Временные процедуры включают следующие методы:

− внедрение цифрового кода сообщения в изображение;

− статистические методы замены: бит изображения заменяется по некоторому статистическому закону;

− частотные процедуры состоят в замене малозначащих частотных характеристик изображения.

IV. Сравнение стеганографических методов

Каждый стеганографичекий метод обладает как сильными, так и слабыми сторонами. Пользователю важно выбрать метод, который в наибольшей степени соответствует поставленной задаче. Все алгоритмы стеганографии должны удовлетворять нескольким основным требованиям. Наиболее важно, чтобы алгоритм давал малозаметное изменение изображения-контейнера. Рассмотрим критерии сравнения:

− *незаметность или уровень восприятия* (нез.). Это главное требование – стеганограмма не должна распознаваться глазом человека. Человек не должен видеть различие между исходным изображением и тем же изображением со вставленным сообщением;

− *вместимость* (вмест.). Это требование определяет размер вставляемого сообщения, который зависит от формата контейнера [2];

− *робастность*. Вставляемое сообщение не должно быть повреждено процессами обработки и передачи, присущими данному формату. Существует два типа робастности:

• *робастность для защиты от статистической атаки* (РПСА). Статистические тесты применяются для выявления наличия стеганограммы в контейнере, это методы статистической обработки данных, которые можно применять как во временной, так и в частотной области;

• *робастность для защиты от целенаправленного повреждения стеганограммы* (РПЦП). Этот вид робастности обусловлен тем, насколько скрытое сообщение зависит от контейнера;

− *способность к обнаружению или скрытность* (СОС). Этот критерий определяет успешность метода скрытия, при распознавании наличия сообщения он обусловливает сложность алгоритма распознавания;

− *вид области* (ВО). Этот параметр указывает на область, в которой применялась стеганография – временная (В) или частотная (Ч);

− *независимость от формата* (НФ). Следует использовать различные форматы файлов. Если партнеры постоянно используют один формат, то это может навести на мысль о тайной переписке [2, 4].

Основные критерий приведены на рис. 1:

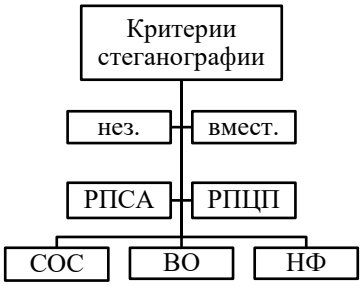

Рисунок 1 – Критерии стеганографии.

В идеальном случае стеганографический алгоритм должен удовлетворять высоким уровням всех критериев. Необходим взвешенный выбор стеганографического метода, который зависит от используемого пользователем приложения. Рассмотрим пригодность различных алгоритмов для форматов файлов:

LSB для BMP. Растровый формат BMP не использует сжатия, поэтому файлы этого формата имеют большой объем. Но для сокрытия сообщения в этих файлах необходим очень большой контейнер.

LSB для JPEG. Распространенный формат JPEG использует 8 битов на каждый цвет RGB. JPEG может скрыть сообщение большого объема.

LSB для цветовой палитры. Формат GIF кодирует пиксел 8 битами, изображение записывается в 256 цветах. Алгоритм LSB скрывает информацию с различными степенями успеха в зависимости от доли изменяемых бит. Необходимо искать равновесие между безопасностью и распознаваемостью

Псевдослучайные перестановки. Метод вставляет биты сообщения с изменением порядка их появления в сообщении, что затрудняет работу по обнаружению и расшифровке сообщения.

Метод с использованием патчей. Недостаток этого метода состоит в том, что в один патч инкапсулируется только один бит [4]. Преимущество этого метода состоит в том, что сообщение распределено по всему изображению, и если один из патчей будет поврежден, то это не принесет больших потерь и сообщение можно восстановить из других патчей.

Метод расширения спектра. Этот метод распределяет сообщение по всему изображению. Такую стеганограмму трудно распознать. Частотная характеристика сообщения обладает гораздо меньшей энергией, чем энергия контейнера. Этот метод имеет большую робастность против атак.

Дискретное косинус-преобразование. Методы области преобразования (частотной области) скрывают сообщение в значительной области изображения, что делает их более робастными по сравнению с методами во временной области, включая сжатие, обрезку и некоторые алгоритмы обработки изображений.

Дискретное вейвлет-преобразование. Инкапсуляция сообщения с помощью ДВП дает хорошие результаты, которые превосходят методы ДКП. Многомасштабный вейвлетный анализ разлагает сигнал в узкие частотные области, что позволяет скрыть сообщение в мелких деталях изображения.

Основные методы стеганографии приведены на рис. 2:

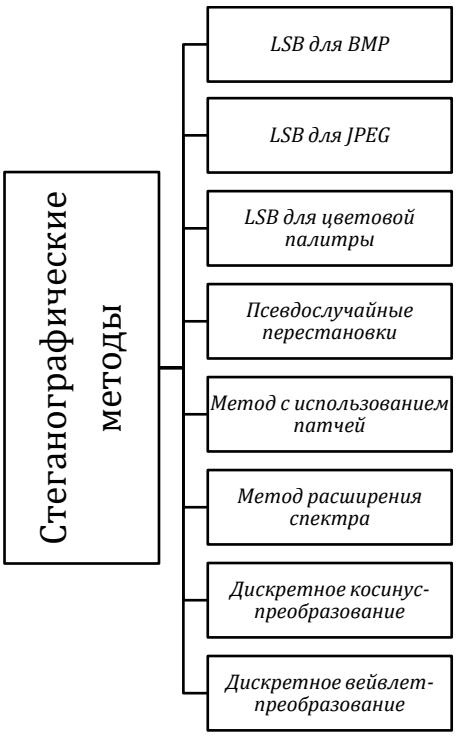

Рисунок 2 – Стеганографические методы.

Выводы

В статье были рассмотрены некоторые из основных методов стеганографии изображений. Все основные форматы графических файлов имеют различные методы сокрытия сообщений со своими сильными и слабыми сторонами. Выбор метода с большой надежностью противостоит методу с высокой скоростью обработки. Например, патч-подход имеет очень высокую устойчивость по отношению к большинству видов атак, но он может скрыть лишь очень небольшое количество информации. Поэтому более разумно скрывать информацию в дополнительных преобразованиях, а не в исходных файлах. Преобразование дискретными вейвлетами более надежно, потому что позволяет скрыть сообщение в области частот. Данная область менее подвержена зрению человека.

Литература

[1] Qiao, Mengyu, Andrew H. Sung, and Qingzhong Liu. "Predicting embedding strength in audio steganography." 9th IEEE International Conference on Cognitive Informatics (ICCI'10). IEEE, 2010.

[2] Ahsan, Kamran, and Deepa Kundur. "Practical data hiding in TCP/IP." Proc. Workshop on Multimedia Security at ACM Multimedia. Vol. 2. No. 7. 2002., p. 783.

[3] Maggi, Federico, Stefano Zanero, and Vincenzo Iozzo. "Seeing the invisible: forensic uses of anomaly detection and machine learning." ACM SIGOPS Operating systems review 42.3 (2008): p. 51-58.

[4] Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. "An overview of image steganography." ISSA. 2005.