

2. Нисон С. Японские свечи: графический анализ финансовых рынков: Пер. с англ. М., 1998. - 217 с.
3. Швагер Дж. Технический анализ. Полный курс. М., 2001. - 69 с.
4. Колби Р. В., Мейерс Т. А. Энциклопедия технических индикаторов рынка. М., 1998. - 179 с.
5. Элдер А. Практическое пособие дилеру биржевых и внебиржевых рынков. М., 1995. - 234 с.

Исаєва Н.В.

Анализ современных стеганографических методов

Одной из важнейших проблем современности является проблема защиты информации секретных сообщений на цифровых изображениях. Это древнейшая задача, которая остаётся проблематичной и не решённой и на данный момент.

Методы и способы скрытия секретных сообщений были известны с давних времён и эта сфера получила название стеганография. Это слово в переводе с греческого означает "тайнопись" (steganos - секрет, тайна ; graphy - запись). К. Шеннон дал нам общую теорию тайнописи, которая является базисом стеганографии как науки. В современной компьютерной стеганографии существует два основных типа файлов: сообщение - файл, который предназначен для скрытия, и контейнер - файл, который может быть использован для скрытия в нём сообщения. Стеганографические методы позволяют передавать секретные сообщения, встроенные в контейнер, так что невозможно обнаружить даже сам факт передачи.

В такой области занимаются многие учёные и исследователи такие, как FaridH. в своей работе «Exposingdigitalforgeriesfromjpegghosts», JunfengHe, ZhouchenLin, LiefengWang, XiaouTang в работе «DetectingdoctoredJPEGimagesviaDCTCoefficientanalysis». Однако эта область ещё до конца неисследована и её потенциал не раскрыт.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Рассмотреть стеганографические методы позволяющие передавать секретные сообщения в цифровое изображение (ЦИ), в частности метод LSB (Least Significant Bit).

2. Исследовать чувствительность метода LSB к повороту стегосообщения, который является одним из самых распространенных геометрических преобразований.

На сегодняшний день методы компьютерной стеганографии развиваются по двум основным направлениям:

1. Методы, которые основаны на использовании специальных свойств компьютерных форматов;

2. Методы, которые основаны на избыточности аудио и визуальной информации.

В настоящее время наиболее распространённым, но наименее стойким является метод замены наименьших значащих битов или LSB - метод.

LSB(Least Significant Bit, наименьший значащий бит) - суть этого метода заключается в замене последних значащих битов в контейнере (изображение, аудио или видеозаписи) на биты скрываемого сообщения[1]. Разница между пустым и заполненным контейнерами должна быть неощутима для органов восприятия человека.

Этот метод использует скрытие данных с искажением контейнера, основанное на особенностях человеческого восприятия. Идея метода заключается в следующем: если взять картинку в формате BMP в 24-х битном формате и заменить младшие значащие биты цвета, то на глаз это будет незаметно. Именно в этом формате существует не мало важный фактор - контейнер, по которому определяется сколько всего можно вставить в картинку, пока это не станет явным для человеческого зрения. Чем больше контейнер, тем больше можно вставить.

Для добавления секретного сообщения нужно выполнить следующее:

- предварительно подготовить нужное нам сообщение: шифруя его и архивируя. Этим мы достигаем сразу две цели- повышение КПД(коэффициент полезного действия) и увеличение стойкости системы;
- далее берем контейнер и внедряем обработанное в предыдущем шаге сообщение в младшие его биты любым удобным для нас способом. А именно: раскрываем упакованное сообщение в битовую последовательность и заменяем избыточные биты контейнера битами сообщения. Надежность такого внедрения сильно зависит от характера распределения Наименьшего Значащего Бита в контейнере и в сообщении. В подавляющем большинстве случаев эти распределения оказываются разными. А на картинках, которые построены из одних младших битов, такое внедрение будет явно заметно на глаз(поэтому к выбору самого контейнера нужно подходить ответственней).

Относительно использования метода LSB можно дать еще несколько простых советов, которые позволяют обойти стеганографический контроль:

- не следует использовать для хранения сообщения более трех битов каждого байта контейнера, а лучше ограничиться двумя, разбив большое сообщение на несколько мелких или подобрав более емкий файл-носитель. Кроме того, не стоит забивать контейнер пользовательскими данными «под завязку» — чем меньше будет доля важной информации в общем объеме передаваемого файла, тем сложнее обнаружить факт закладки. На практике обычно рекомендуют скрывать сообщения так, чтобы их размер составлял не более 10% размера контейнера;
- не рекомендуется использовать в стеганографических целях искусственно созданные изображения или фотографии, на которых присутствуют значительные участки однотонной заливки (например, голубое небо). Большое количество мелких пестрых деталей, наоборот, повысит надежность сокрытия;
- неудачным контейнером для сообщения будут общедоступные, широко известные мультимедийные файлы, поскольку простое сравнение файла с оригиналом сразу обнаружит стеганограмму. Для этих целей лучше использовать собственноручно сделанное цифровое изображение — с помощью цифрового фотоаппарата или сканера[1].

Главной целью любой атаки на стегосистему является обнаружение стеганографического канала. Максимально достижимым результатом при реализации атаки - получение полной информации о стеганографической системе.

Устойчивость к геометрическим искажениям является непременным требованием, которое предъявляется к стегосистемам. Однако не все существующие на сегодняшний день системы выдерживают такого рода атаки. Например, нерешенным остается вопрос модификации с целью повышения устойчивости к геометрическим преобразованиям вообще и к повороту стегосообщения в частности. Так как иногда поворот контейнера-изображения даже на незначительный угол может привести к потере некоторой части информации.

В среде разработки Matlab был проведен вычислительный эксперимент с привлечением 50 цифровых изображений (ЦИ). Каждое изображение использовалось, как контейнер для встраивания секретного сообщения в биты разных порядков[2]. После этого встраивания сообщение ЦИ поворачивалось на некоторый угол, сохранялось и поворачивалось назад, после чего происходило восстановление секретного сообщения. Повороты ЦИ проводились на разные углы поворота стегосообщения, а именно от 1 до 15 градусов . При проведении эксперимента анализировался процент верно восстановленного секретного сообщения.

Более характерные результаты эксперимента приведены в таблице 1.

Табл. 1 – Восстановление секретного сообщения в зависимости от угла поворота.

Угол поворота ЦИ, °	%Восстановленного секретного сообщения
1	97
2	86
3	83
4	78
5	74
6	70
7	67
8	64
9	61
10	58
11	56
12	53
13	50
14	46
15	42

При проведении такого эксперимента делается вывод, что процент верно восстановленного секретного сообщения после поворота цифрового стегосообщения больше зависит от угла, на который был произведен поворот, чем от порядка значащего бита, в который происходило погружение. Этим было доказано, что целостность важной информации при каком-либо повороте стегосообщения очень сильно зависит.

Модификация чувствительности метода LSB к повороту стегосообщения для возможности его использования в реальных условиях анализа ЦИ является дальнейшей работой автора.

Литература:

1. В.Н. Кустов, А.А. Федчук, Методы встраивания скрытых сообщений//*Задачи информатики*, 2000.
2. FaridH. Exposingdigitalforgeriesfromjpegghosts / H.Farid // IEEE Transactions on Information Forensics and Security. — v1,i4. — P.154—160.
3. Городецкий В.И., Самойлов В.В., Стеганография на основе цифровых изображений // Информационные технологии и вычислительные системы, №2/3, 2001, с. 51-64.

Козина М. А.

Стеганографический метод, основанный на нормированном преобразовании хотеллинга. недостатки практической реализации.

Надежная защита информации от несанкционированного доступа является актуальной, но не решенной в полном объеме проблемой. Одно из перспективных направлений защиты информации сформировали современные методы стеганографии [1,2], хотя область ее приложения не ограничивается безопасностью информации (Рис.1).

Защита от копирования Электронная коммерция, контроль за копированием (DVD), распространение мультимедийной информации (видео по запросу)	Скрытая аннотация документов Медицинские снимки, картография, мультимедийные базы данных	Аутентификация Системы видеонаблюдения, электронной коммерции, голосовой почты, электронное конфиденциальное делопроизводство	Скрытая связь Военные и разведывательные приложения, а также применение в случаях, когда

Рис.1 – Потенциальные области применения стеганографии