Стеганография

Стеганогра́фия (от греч. στεγανός — скрытый и греч. γράφω — пишу, буквально «тайнопись») — это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи.

В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает само его существование. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её.

Классификация стеганографии

В конце 90-х годов выделилось несколько направлений стеганографии:

- **Классическая стеганография**
- **Компьютерная стеганография**
- **Цифровая стеганография**

Классическая стеганография

Стеганография в Древнем мире

Существует версия[1] , что древние шумеры одними из первых использовали **стеганографию**, так как было найдено множество глиняных клинописных табличек, в которых одна запись покрывалась слоем глины, а на втором слое писалась другая. Однако противники этой версии считают, что это было вовсе не попыткой скрытия информации, а всего лишь практической потребностью.

В трудах древнегреческого историка Геродота встречается описание еще двух методов сокрытия информации: на обритую голову раба записывалось необходимое сообщение, а когда его волосы отрастали, он отправлялся к адресату, который вновь брил его голову и считывал доставленное сообщение. Второй способ заключался в следующем: сообщение наносилось на деревянную дощечку, а потом она покрывалась воском, и, тем самым, не вызывала никаких подозрений. Потом воск соскабливался, и сообщение становилось видимым.[2]

Симпатические чернила

Одним из наиболее распространенных методов **классической стеганографии** является использование симпатических (невидимых) чернил. Текст, записанный такими чернилами, проявляется только при определенных условиях (нагрев, освещение, химический проявитель и т. д.)[3] Изобретенные еще в I веке н. э. Филоном Александрийским[4] , они продолжали использоваться как в средневековье, так и в новейшее время, например, в письмах русских революционеров из тюрем. В советской школьной программе в курсе литературы изучался рассказ о том, как Владимир Ленин писал молоком на бумаге между строк, см. Рассказы о Ленине. Молоко проявлялось при нагреве над пламенем.

Существуют также чернила с химически нестабильным пигментом. Написанное этими чернилами выглядит как написанное обычной ручкой, но через определенное время нестабильный пигмент разлагается, и от текста не остается и следа. Хотя при использовании обычной шариковой ручки текст можно восстановить по деформации бумаги, этот недостаток можно устранить с помощью мягкого пишущего узла, наподобие фломастера.

Другие стеганографические методы

Во время Второй мировой войны активно использовались **микроточки —** микроскопические фотоснимки, вклеиваемые в текст писем, телеграмм.

Также существует ряд альтернативных методов сокрытия информации: [3]

- запись на боковой стороне колоды карт, расположенных в условленном порядке;
- запись внутри вареного яйца;
- «жаргонные шифры», где слова имеют другое обусловленное значение;
- трафареты, которые, будучи положенными на текст, оставляют видимыми только значащие буквы;
- узелки на нитках и т. д.

В настоящее время под **стеганографией** чаще всего понимают скрытие информации в текстовых, графических либо аудиофайлах путём использования специального программного обеспечения.

Стеганографические модели

Стеганографические модели — используются для общего описания стеганографических систем.

Основные понятия

В 1983 году Симмонс предложил т. н. «проблему заключенных». Её суть состоит в том, что есть человек на свободе (Алиса), в заключении (Боб) и охранник Вилли. Алиса хочет передавать сообщения Бобу без вмешательства охранника. В этой модели сделаны некоторые допущения: предполагается, что перед заключением Алиса и Боб договариваются о кодовом символе, который отделит одну часть текста письма от другой, в которой скрыто сообщение. Вилли же имеет право читать и изменять сообщения. В 1996 году на конференции Information Hiding: First Information Workshop была принята единая терминология:

- Стеганографическая система (стегосистема) — объединение методов и средств используемых для создания скрытого канала для передачи информации. При построении такой системы условились о том, что: 1) враг представляет работу стеганографической системы. Неизвестным для противника является ключ с помощью которого можно узнать о факте существования и содержания тайного сообщения. 2) При обнаружении противником наличия скрытого сообщения он не должен смочь извлечь сообщение до тех пор пока он не будет владеть ключом. 3) Противник не имеет технических и прочих преимуществ.
- Сообщение — это термин, используемый для общего названия передаваемой скрытой информации, будь то лист с надписями молоком, голова раба или цифровой файл.
- Контейнер — так называется любая информация, используемая для сокрытия тайного сообщения. Пустой контейнер — контейнер, не содержащий секретного послания. Заполненный контейнер (стегоконтейнер) — контейнер, содержащий секретное послание.
- Стеганографический канал (стегоканал) — канал передачи стегоконтейнера.
- Ключ (стегоключ) — секретный ключ, нужный для сокрытия стегоконтейнера. Ключи в стегосистемах бывают двух типов: секретные и открытые. Если стегосистема использует секретный ключ, то он должен быть создан или до начала обмена сообщениями, или передан по защищённому каналу. Стегосистема, использующая открытый ключ, должна быть устроена таким образом, чтобы было невозможно получить из него закрытый ключ. В этом случае открытый ключ мы можем передавать по незащищённому каналу.

Компьютерная стеганография

Компьютерная стеганография — направление классической стеганографии, основанное на особенностях компьютерной платформы. Примеры — стеганографическая файловая система StegFS для Linux, скрытие данных в неиспользуемых областях форматов файлов, подмена символов в названиях файлов, текстовая стеганография и т. д. Приведём некоторые примеры:

- Использование зарезервированных полей компьютерных форматов файлов — суть метода состоит в том, что часть поля расширений, не заполненная информацией о расширении, по умолчанию заполняется нулями. Соответственно мы можем использовать эту «нулевую» часть для записи своих данных. Недостатком этого метода является низкая степень скрытности и малый объем передаваемой информации.
- Метод скрытия информации в неиспользуемых местах гибких дисков — при использовании этого метода информация записывается в неиспользуемые части диска, к примеру, на нулевую дорожку. Недостатки: маленькая производительность, передача небольших по объему сообщений.
- Метод использования особых свойств полей форматов, которые не отображаются на экране — этот метод основан на специальных «невидимых» полях для получения сносок, указателей. К примеру, написание черным шрифтом на черном фоне. Недостатки: маленькая производительность, небольшой объём передаваемой информации.
- Использование особенностей файловых систем — при хранении на жестком диске файл всегда (не считая некоторых ФС, например, ReiserFS) занимает целое число кластеров (минимальных адресуемых объемов информации). К примеру, в ранее широко используемой файловой системе FAT32 (использовалась в Windows98/Me/2000) стандартный размер кластера — 4 Кб. Соответственно для хранения 1 Кб информации на диске выделяется 4 Кб информации, из которых 1Кб нужен для хранения сохраняемого файла, а остальные 3 ни на что не используются — соответственно их можно использовать для хранения информации. Недостаток данного метода: лёгкость обнаружения.

Цифровая стеганография

Цифровая стеганография — направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. Но, как правило, данные объекты являются мультимедиа-объектами (изображения, видео, аудио, текстуры 3D-объектов) и внесение искажений, которые находятся ниже порога чувствительности среднестатистического человека, не приводит к заметным изменениям этих объектов. Кроме того, в оцифрованных объектах, изначально имеющих аналоговую природу, всегда присутствует шум квантования; далее, при воспроизведении этих объектов появляется дополнительный аналоговый шум и нелинейные искажения аппаратуры, все это способствует большей незаметности сокрытой информации.

Применение цифровой стеганографии

Из рамок цифровой стеганографии вышло наиболее востребованное легальное направление — встраивание цифровых водяных знаков (ЦВЗ) (watermarking), являющееся основой для систем защиты авторских прав и DRM (Digital rights management) систем. Методы этого направления настроены на встраивание скрытых маркеров, устойчивых к различным преобразованиям контейнера (атакам).

Полухрупкие и хрупкие ЦВЗ используются в качестве аналоговой ЭЦП, обеспечивая хранение информации о передаваемой подписи и попытках нарушения целостности контейнера (канала передачи данных).

Например, разработки Digimarc в виде плагинов к редактору Adobe Photoshop позволяют встроить в само изображение информацию об авторе. Однако такая метка неустойчива, впрочем как и абсолютное их большинство. Программа Stirmark, разработчиком которой является ученый Fabien Petitcolas, с успехом атакует подобные системы, разрушая стеговложения.

Алгоритмы

Все алгоритмы встраивания скрытой информации можно разделить на несколько подгрупп:

- Работающие с самим цифровым сигналом. Например, метод LSB.
- «Впаивание» скрытой информации. В данном случае происходит наложение скрываемого изображения (звука, иногда текста) поверх оригинала. Часто используется для встраивания ЦВЗ.
- Использование особенностей форматов файлов. Сюда можно отнести запись информации в метаданные или в различные другие не используемые зарезервированные поля файла.

По способу встраивания информации стегоалгоритмы можно разделить на линейные (аддитивные), нелинейные и другие. Алгоритмы аддитивного внедрения информации заключаются в линейной модификации исходного изображения, а ее извлечение в декодере производится корреляционными методами. При этом ЦВЗ обычно складывается с изображением-контейнером, либо «вплавляется» (fusion) в него. В нелинейных методах встраивания информации используется скалярное либо векторное квантование. Среди других методов определенный интерес представляют методы, использующие идеи фрактального кодирования изображений. К аддитивным алгоритмам можно отнести:

- A17 (Cox)
- A18 (Barni)
- L18D (Lange)
- A21 (J. Kim).
- A25 (C. Podilchuk).

Метод LSB

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

Суть метода заключается в следующем: Допустим, имеется 8-битное изображение в градациях серого. 00h (00000000b) обозначает черный цвет, FFh (11111111b) — белый. Всего имеется 256 градаций (2^8). Также предположим, что сообщение состоит из 1 байта — например, 01101011b. При использовании 2 младших бит в описаниях пикселей, нам потребуется 4 пикселя. Допустим, они черного цвета. Тогда пиксели, содержащие скрытое сообщение, будут выглядеть следующим образом: 00000001 00000010 00000010 00000011. Тогда цвет пикселей изменится: первого — на 1/255, второго и третьего — на 2/255 и четвертого — на 3/255. Такие градации, мало того что незаметны для человека, могут вообще не отобразиться при использовании низкокачественных устройств вывода.

Методы LSB являются неустойчивыми ко всем видам атак и могут быть использованы только при отсутствии шума в канале передачи данных.

Обнаружение LSB-кодированного стего осуществляется по аномальным характеристикам распределения значений диапазона младших битов отсчётов цифрового сигнала.

Все методы LSB являются, как правило, аддитивными (A17, L18D).

Другие методы скрытия информации в графических файлах ориентированы на форматы файлов с потерей, к примеру, JPEG. В отличие от LSB они более устойчивы к геометрическим преобразованиям. Это получается за счёт варьирования в широком диапазоне качества изображения, что приводит к невозможности определения источника изображения.

Эхо-методы

Эхо-методы применяются в цифровой аудиостеганографии и используют неравномерные промежутки между эхо-сигналами для кодирования последовательности значений. При наложении ряда ограничений соблюдается условие незаметности для человеческого восприятия. Эхо характеризуется тремя параметрами: начальной амплитудой, степенью затухания, задержкой. При достижении некоего порога между сигналом и эхом они смешиваются. В этой точке человеческое ухо не может уже отличить эти два сигнала. Наличие этой точки сложно определить, и она зависит от качества исходной записи, слушателя. Чаще всего используется задержка около 1/1000, что вполне приемлемо для большинства записей и слушателей. Для обозначения логического нуля и единицы используется две различных задержки. Они обе должны быть меньше, чем порог чувствительности уха слушателя к получаемому эху.

Эхо-методы устойчивы к амплитудным и частотным атакам, но неустойчивы к атакам по времени.

Фазовое кодирование

Фазовое кодирование (phase coding, фазовое кодирование) — также применяется в цифровой аудиостеганографии. Происходит замена исходного звукового элемента на относительную фазу, которая и является секретным сообщением. Фаза подряд идущих элементов должна быть добавлена таким образом, чтобы сохранить относительную фазу между исходными элементами. Фазовое кодирование является одним из самых эффективных методов скрытия информации.

Метод расширенного спектра

Метод встраивания сообщения заключается в том, что специальная случайная последовательность встраивается в контейнер, затем, используя согласованный фильтр, данная последовательность детектируется. Данный метод позволяет встраивать большое количество сообщений в контейнер, и они не будут создавать помехи друг другу. Метод заимствован из широкополосной связи.

Атаки на стегосистемы

Под атакой на стегосистему понимается попытка обнаружить, извлечь, изменить скрытое стеганографическое сообщение. Такие атаки называются стегоанализом по аналогии с криптоанализом для криптографии. Наиболее простая атака — субъективная. Внимательно рассматривается изображение, прослушивается звукозапись в попытках найти признаки существования в нем скрытого сообщения. Такая атака имеет успех лишь для совсем незащищенных стегосистем. Обычно это первый этап при вскрытии стегосистемы. Выделяются следующие типы атак.[5]

- Атака по известному заполненному контейнеру;
- Атака по известному встроенному сообщению;
- Атака на основе выбранного скрытого сообщения;
- Адаптивная атака на основе выбранного скрытого сообщения;
- Атака на основе выбранного заполненного контейнера;
- Атака на основе известного пустого контейнера;
- Атака на основе выбранного пустого контейнера;
- Атака по известной математической модели контейнера.

Рассмотрим некоторые из них:

Атака по известному заполненному контейнеру — у взломщика имеется одно или несколько стего. В случае нескольких стего считается, что запись скрытой информации проводилось отправителем одинаковым способом. Задача взломщика заключается в обнаружении факта наличия стегоканала, а также доступа к нему или определения ключа. Имея ключ, можно раскрыть другие стегосообщения.

Атака по известной математической модели контейнера — взломщик определяет отличие подозрительного послания от известной ему модели. К примеру, пусть биты внутри отсчета изображения коррелированны. Тогда отсутствие корреляции может служить сигналом о наличии скрытого сообщения. При этом задача внедряющего сообщение состоит в том, чтобы не нарушить статистических закономерностей в контейнере.

Атака на основе известного пустого контейнера — если злоумышленнику известен пустой контейнер, то сравнивая его с предполагаемым стего можно установить наличие стегоканала. Несмотря на кажущуюся простоту метода, существует теоретическое обоснование эффективности этого метода. Особый интерес представляет случай, когда контейнер нам известен с некоторой погрешностью (такое возможно при добавлении к нему шума).

Стеганография и цифровые водяные знаки

Цифровые водяные знаки (ЦВЗ) используются для защиты от копирования, сохранения авторских прав. Невидимые водяные знаки считываются специальным устройством, которое может подтвердить либо опровергнуть корректность. ЦВЗ могут содержать различные данные: авторские права, идентификационный номер, управляющую информацию. Наиболее удобными для защиты с помощью ЦВЗ являются неподвижные изображения, аудио и видео файлы.

Технология записи идентификационных номеров производителей очень похожа на ЦВЗ, но отличие состоит в том, что на каждое изделие записывается свой индивидуальный номер (так называемые «отпечатки пальцев»), по которому можно вычислить дальнейшую судьбу изделия. Невидимое встраивание заголовков иногда используется, к примеру, для подписей медицинских снимков, нанесения пути на карту и т. п. Скорее всего, это единственное направление стеганографии, где нет нарушителя в явном виде.

Основные требования, предъявляемые к водяным знакам: надёжность и устойчивость к искажениям, незаметности, робастности к обработке сигналов (робастность — способность системы к восстановлению после воздействия на нее внешних/внутренних искажений, в том числе умышленных). ЦВЗ имеют небольшой объём, но для выполнения указанных выше требований, при их встраивании используются более сложные методы, чем для встраивания обычных заголовков или сообщений. Такие задачи выполняют специальные стегосистемы.

Перед помещением ЦВЗ в контейнер, водяной знак нужно преобразовать к подходящему виду. К примеру, если в качестве контейнера используется изображение, то и ЦВЗ должны быть представлена как двумерный битовый массив.

Для повышения устойчивости к искажениям часто применяют помехоустойчивое кодирование или используют широкополосные сигналы. Начальную обработку скрытого сообщения делает прекодер. Важная предварительная обработка ЦВЗ — вычисление его обобщенного Фурье-преобразования. Это повышает помехоустойчивость. Первичную обработку часто производят с использованием ключа — для повышения секретности. Потом водяной знак «укладывается» в контейнер (например, путем изменения младших значащих бит). Здесь используются особенности восприятия изображений человеком. Широко известно, что изображения имеют огромную психовизуальную избыточность. Глаза человека подобны низкочастотному фильтру, который пропускает мелкие элементы изображения. Наименее заметны искажения в высокочастотной области изображений. Внедрение ЦВЗ также должно учитывать свойства восприятия человека.

Во многих стегосистемах для записи и считывания ЦВЗ используется ключ. Он может предназначаться для ограниченного круга пользователей или же быть секретным. Например, ключ нужен в DVD-плейерах для возможности прочтения ими содержащихся на дисках ЦВЗ. Как известно, не существует таких стегосистем, в которых бы при считывании водяного знака требовалась другая информация, нежели при его записи. В стегодетекторе происходит обнаружение ЦВЗ в защищённом им файле, который, возможно, мог быть изменён.

Эти изменения могут быть связаны с воздействиями ошибок в канале связи, либо преднамеренными помехами. В большинстве моделей стегосистем сигнал-контейнер можно рассмотреть как аддитивный шум. При этом задача обнаружения и считывания стегосообщения уже не представляет сложности, но не учитывает двух факторов: неслучайности сигнала контейнера и запросов по сохранению его качества. Учет этих параметров позволит строить более качественные стегосистемы. Для обнаружения факта существования водяного знака и его считывания используются специальные устройства — стегодетекторы. Для вынесения решения о наличии или отсутствии водяного знака используют, к примеру, расстояние по Хэммингу, взаимокорреляцию между полученным сигналом и его оригиналом. В случае отсутствия исходного сигнала в дело вступают более изощренные статистические методы, которые основаны на построении моделей исследуемого класса сигналов.

Интересные факты

- Некоторые современные цветные принтеры используют методы стеганографии для затруднения использования их для печати денежных купюр. На каждой отпечатанной странице дополнительно в специальном порядке размещается группа точек, диаметром в доли миллиметра. Данная информация содержит модель принтера и его серийный номер. Таким образом, позже можно выявить на каком оборудовании была отпечатана конкретная банкнота и выявить его владельца. К примеру, принтеры HP и Xerox используют для этой цели группу точек бледно-желтого цвета, заметные лишь на синем фоне с использованием оптического увеличения.
- Скандально известный греческий миллионер Аристотель Онассис несколько раз использовал при подписании контрактов ручку с симпатическими чернилами.
- В фильме «Гений» главный герой — персонаж Александра Абдулова — обманывает милицию, написав признание симпатическими чернилами.

Ссылки

Программные реализации

- ImageSpyer Александра Мясникова [6] — бесплатная отечественная разработка, известная также как плагин StegoTC [7] для Total Commander. Реализуется вариант алгоритма LSB с возможностью установки произвольного порядка бит в сочетании с 40 симметричными криптографическими алгоритмами.
- DarkCryptTC [8] — бесплатный плагин для Total Commander с графической оболочкой DarkCrypt GUI [9], является продолжением разработок ImageSpyer и StegoTC и реализует алгоритм LSB, используя в качестве контейнера для зашифрованных архивов изображения PNG, BMP, TIFF, PSD, TGA, MGA, аудиофайлы WAVE, текстовые, XML и HTML файлы (текстовая стеганография, алгоритм замены символов).
- spammimic.com [10] превращает данное ему предложение в текст который для всех выглядит как спам.
- Страница Neil F. Johnson'a, с информацией о стеганографии [11]
- VSL: Virtual Steganographic Laboratory [12]

Статьи

- Обзор программ для поиска скрытых стеганографией материалов [13]
- Основы стегоанализа [14]
- Компьютерная стеганография вчера, сегодня, завтра [15]
- Стеганография [16]
- Методы текстовой стеганографии [17]

Прочее

- Мини-обзор средств криптографии и стеганографии [18]

Список использованной литературы

- Быков С. Ф. *Алгоритм сжатия JPEG с позиции компьютерной стеганографии* // Защита информации. Конфидент. — СПб.: 2000, № 3.
- Конахович Г. Ф., Пузыренко А. Ю. *Компьютерная стеганография. Теория и практика*. — К.: МК-Пресс, 2006. — 288 с, ил. описание [19]
- Грибунин В. Г., Оков И. Н., Туринцев И. В. *Цифровая стеганография*. — М.: Солон-Пресс, 2002. — 272 с, ил.

Примечания

[1] Криптология в Древнем мире (http://crypto.land.ru/history3.htm)
[2] Бабаш А. В., Материалы к лекции по теме «Криптография в древние времена»
[3] Громов В. И., Энциклопедия безопасности
[4] Вокруг Света | Вопрос-Ответ | Для чего нужны симпатические чернила? (http://www.vokrugsveta.ru/quiz/?item_id=70)
[5] :::::: НОУ ДПО 'Центр предпринимательских рисков' ::::: — Библиотека начальника СБ (http://www.cprspb.ru/bibl/computer/13.html)
[6] http://freesoft.ru/?id=80058
[7] http://wincmd.ru/plugring/stegotc.html
[8] http://wincmd.ru/plugring/darkcrypttc.html
[9] http://freesoft.ru/?id=675788
[10] http://www.spammimic.com
[11] http://www.jjtc.com/neil/
[12] http://vsl.sourceforge.net/
[13] http://www.xakep.ru/post/37769/default.asp
[14] http://www.cprspb.ru/bibl/computer/13.html
[15] http://st.ess.ru/publications/articles/steganos/steganos.htm
[16] http://www.kriptolog.net/blog/steganografija
[17] http://www.osp.ru/pcworld/2004/11/169154/
[18] http://void-runner.livejournal.com/12155.html
[19] http://www.my-shop.ru/shop/books/158345.html

Источники и основные авторы

Стеганография *Источник*: http://ru.wikipedia.org/w/index.php?oldid=34499863 *Редакторы*: Adultdreamer, Alexanderwdark, Andrey Case, Atr2006, Butko, Centurion198, Danik ik, Fractaler, Fuxx, Generous, Gr190ry, HugC12, Jaro.p, KleverI, Koliz, Lizz, Lvova, ManN, Maximaximax, Mind abuse, Monster adv, Nikolay Nikolaevich Fedotov, Noomorph, OckhamTheFox, Partyzan XXI, Pauk, Paul ls, Pianist, Raegdan, Roxis, Sergei, SidorovIlya, Tucvbif, Vem, Vemcaster, Vort, X-Storm, Yms, ВМНС, Веон, Чрьный человек, 81 анонимных правок

Лицензия