Московский Физико-Технический Институт (ГУ)

Факультет Радиотехники и Кибернетики

«Стеганография в Интернете и сотовой связи»

Эссе по курсу «Защита информации»

Иванов Егор. 316 гр.

Москва, 2007 г.

Во многих случаях, наряду с шифрованием конфиденциальной информации, возникает потребность сделать незаметным сам факт передачи или хранения данных. Актуальность задачи напрямую связана с ростом конкурентной борьбы, промышленным шпионажем, возрастающим контролем государственных структур над электронными средствами связи, проникновением хакеров в базы данных.

Одним из наиболее эффективных способов противодействия такому вмешательству является сокрытие данных (**стеганография**) в массиве цифрового изображения. Изображение в этом случае будет представлять собой контейнер (носитель) для передачи или хранения секретных данных. При этом, доступ для просмотра изображения может быть отрытым и не вызывать подозрений. Для хранения данных, в этом случае, могут использоваться не только центры данных (Data Center), но и обычные HTTP серверы.

Термины и определения

Стеганография - это метод организации связи, который собственно скрывает само наличие связи. В отличие от криптографии, где неприятель точно может определить является ли передаваемое сообщение зашифрованным текстом, методы стеганографии позволяют встраивать секретные сообщения в безобидные послания так, чтобы невозможно было заподозрить существование встроенного тайного послания.

Слово "стеганография" в переводе с греческого буквально означает "тайнопись" (steganos - секрет, тайна; graphy - запись). К ней относится огромное множество секретных средств связи, таких как невидимые чернила, микрофотоснимки, условное расположение знаков, тайные каналы и средства связи на плавающих частотах и т. д.

Стеганография занимает свою нишу в обеспечении безопасности: она не заменяет, а дополняет криптографию. Сокрытие сообщения методами стеганографии значительно снижает вероятность обнаружения самого факта передачи сообщения. А если это сообщение к тому же зашифровано, то оно имеет еще один, дополнительный, уровень защиты.

В настоящее время в связи с бурным развитием вычислительной техники и новых каналов передачи информации появились новые стеганографические методы, в основе которых лежат особенности представления информации в компьютерных файлах, вычислительных сетях и т. п. Это дает нам возможность говорить о становлении нового направления - компьютерной стеганографии.

Несмотря на то, что стеганография как способ сокрытия секретных данных известна уже на протяжении тысячелетий, компьютерная стеганография - молодое и развивающееся направление. Как и любое новое направление, компьютерная стеганография, несмотря на большое количество открытых публикаций и ежегодные конференции, долгое время не имела единой терминологии.

Стеганографическая система или стегосистема - совокупность средств и методов, которые используются для формирования скрытого канала передачи информации.

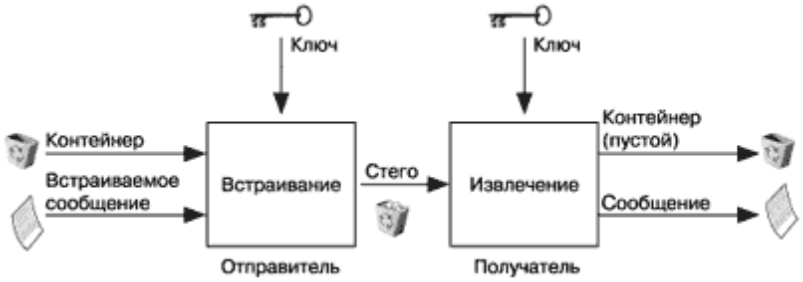
При построении стегосистемы должны учитываться следующие положения:

- противник имеет полное представление о стеганографической системе и деталях ее реализации. Единственной информацией, которая остается неизвестной потенциальному противнику, является ключ, с помощью которого только его держатель может установить факт присутствия и содержание скрытого сообщения;

- если противник каким-то образом узнает о факте существования скрытого сообщения, это не должно позволить ему извлечь подобные сообщения в других данных до тех пор, пока ключ хранится в тайне;

- потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений.

Обобщенная модель стегосистемы представлена на рис. 1.



В качестве данных может использоваться любая информация: текст, сообщение, изображение и т. п. В общем же случае целесообразно использовать слово "сообщение", так как сообщением может быть как текст или изображение, так и, например, аудиоданные. Далее для обозначения скрываемой информации, будем использовать именно термин сообщение.

Контейнер - любая информация, предназначенная для сокрытия тайных сообщений.

Пустой контейнер - контейнер без встроенного сообщения; заполненный контейнер или стего - контейнер, содержащий встроенную информацию.

Встроенное (скрытое) сообщение - сообщение, встраиваемое в контейнер.

Стеганографический канал или просто стегоканал - канал передачи стего.

Стегоключ или просто ключ - секретный ключ, необходимый для сокрытия информации. В зависимости от количества уровней защиты (например, встраивание предварительно зашифрованного сообщения) в стегосистеме может быть один или несколько стегоключей.

По аналогии с криптографией, по типу стегоключа стегосистемы можно подразделить на два типа:

- с секретным ключом;
- с открытым ключом.

В стегосистеме с секретным ключом используется один ключ, который должен быть определен либо до начала обмена секретными сообщениями, либо передан по защищенному каналу.

В стегосистеме с открытым ключом для встраивания и извлечения сообщения используются разные ключи, которые различаются таким образом, что с помощью вычислений невозможно вывести один ключ из другого. Поэтому один ключ (открытый) может передаваться свободно по незащищенному каналу связи. Кроме того, данная схема хорошо работает и при взаимном недоверии отправителя и получателя.

Требования

Любая стегосистема должна отвечать следующим требованиям:

- Свойства контейнера должны быть модифицированы, чтобы изменение невозможно было выявить при визуальном контроле. Это требование определяет качество сокрытия внедряемого сообщения: для обеспечения беспрепятственного прохождения стегосообщения по каналу связи оно никоим образом не должно привлечь внимание атакующего.
- Стегосообщение должно быть устойчиво к искажениям, в том числе и злонамеренным. В процессе передачи изображение (звук или другой контейнер) может претерпевать различные трансформации: уменьшаться или увеличиваться, преобразовываться в другой формат и т. д. Кроме того, оно может быть сжато, в том числе и с использованием алгоритмов сжатия с потерей данных.
- Для сохранения целостности встраиваемого сообщения необходимо использование кода с исправлением ошибки.
- Для повышения надежности встраиваемое сообщение должно быть продублировано.

Приложения

В настоящее время можно выделить три тесно связанных между собой и имеющих одни корни направления приложения стеганографии: сокрытие данных (сообщений), цифровые водяные знаки и заголовки.

Сокрытие внедряемых данных, которые в большинстве случаев имеют большой объем, предъявляет серьезные требования к контейнеру: размер контейнера в несколько раз должен превышать размер встраиваемых данных.

Цифровые водяные знаки используются для защиты авторских или имущественных прав на цифровые изображения, фотографии или другие оцифрованные произведения искусства. Основными требованиями, которые предъявляются к таким встроенным данным, являются надежность и устойчивость к искажениям.

Цифровые водяные знаки имеют небольшой объем, однако, с учетом указанных выше требований, для их встраивания используются более сложные методы, чем для встраивания просто сообщений или заголовков.

Третье приложение, заголовки, используется в основном для маркирования изображений в больших электронных хранилищах (библиотеках) цифровых изображений, аудио- и видеофайлов.

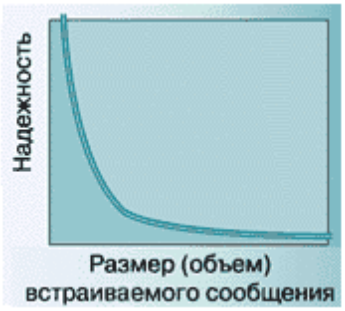
В данном случае стеганографические методы используются не только для внедрения идентифицирующего заголовка, но и иных индивидуальных признаков файла.

Внедряемые заголовки имеют небольшой объем, а предъявляемые к ним требования минимальны: заголовки должны вносить незначительные искажения и быть устойчивы к основным геометрическим преобразованиям.

Ограничения

Каждое из перечисленных выше приложений требует определенного соотношения между устойчивостью встроенного сообщения к внешним воздействиям (в том числе и стегоанализу) и размером самого встраиваемого сообщения.

Для большинства современных методов, используемых для сокрытия сообщения в цифровых контейнерах, имеет место следующая зависимость надежности системы от объема встраиваемых данных.



Данная зависимость показывает, что при увеличении объема встраиваемых данных снижается надежность системы (при неизменности размера контейнера). Таким образом, используемый в стегосистеме контейнер накладывает ограничения на размер встраиваемых данных.

Контейнеры

Существенное влияние на надежность стегосистемы и возможность обнаружения факта передачи скрытого сообщения оказывает выбор контейнера.

Например, опытный глаз цензора с художественным образованием легко обнаружит изменение цветовой гаммы при внедрении сообщения в репродукцию "Мадонны" Рафаэля или "Черного квадрата" Малевича.

По протяженности контейнеры можно подразделить на два типа: непрерывные (потоковые) и ограниченной (фиксированной) длины. Особенностью потокового контейнера является то, что невозможно определить его начало или конец. Более того, нет возможности узнать заранее, какими будут последующие шумовые биты, что приводит к необходимости включать скрывающие сообщение биты в поток в реальном масштабе времени, а сами скрывающие биты выбираются с помощью специального генератора, задающего расстояние между последовательными битами в потоке.

В непрерывном потоке данных самая большая трудность для получателя - определить, когда начинается скрытое сообщение. При наличии в потоковом контейнере сигналов синхронизации или границ пакета, скрытое сообщение начинается сразу после одного из них. В свою очередь, для отправителя возможны проблемы, если он не уверен в том, что поток контейнера будет достаточно долгим для размещения целого тайного сообщения.

При использовании контейнеров фиксированной длины отправитель заранее знает размер файла и может выбрать скрывающие биты в подходящей псевдослучайной последовательности. С другой стороны, контейнеры фиксированной длины, как это уже отмечалось выше, имеют ограниченный объем и иногда встраиваемое сообщение может не поместиться в файл-контейнер.

Другой недостаток заключается в том, что расстояния между скрывающими битами равномерно распределены между наиболее коротким и наиболее длинным заданными расстояниями, в то время как истинный случайный шум будет иметь экспоненциальное распределение длин интервала. Конечно, можно породить псевдослучайные экспоненциально распределенные числа, но этот путь обычно слишком трудоемок. Однако на практике чаще всего используются именно контейнеры фиксированной длины, как наиболее распространенные и доступные.

Возможны следующие варианты контейнеров:

- Контейнер генерируется самой стегосистемой. Примером может служить программа MandelSteg, в которой в качестве контейнера для встраивания сообщения генерируется фрактал Мандельброта. Такой подход можно назвать конструирующей стеганографией.
- Контейнер выбирается из некоторого множества контейнеров. В этом случае генерируется большое число альтернативных контейнеров, чтобы затем выбрать наиболее подходящий для сокрытия сообщения. Такой подход можно назвать селектирующей стеганографией. В данном случае при выборе оптимального контейнера из множества сгенерированных важнейшим требованием является естественность контейнера. Единственной же проблемой остается то, что даже оптимально организованный контейнер позволяет спрятать незначительное количество данных при очень большом объеме самого контейнера.
- Контейнер поступает извне. В данном случае отсутствует возможность выбора контейнера и для сокрытия сообщения берется первый попавшийся контейнер, не всегда подходящий к встраиваемому сообщению. Назовем это безальтернативной стеганографией.

Методы сокрытия информации

В настоящее время наиболее распространенным, но наименее стойким является метод замены наименьших значащих битов или LSB-метод. Он заключается в использовании погрешности дискретизации, которая всегда существует в оцифрованных изображениях или аудио- и видеофайлах. Данная погрешность равна наименьшему значащему разряду числа, определяющему величину цветовой составляющей элемента изображения (пикселя). Поэтому модификация младших битов в большинстве случаев не вызывает значительной трансформации изображения и не обнаруживается визуально. Алгоритм встраивания основывается на свойствах визуального восприятия, и выполняется таким образом, чтобы внедряемые биты оставались бы незаметными при визуальном рассмотрении цифрового изображения. Объем **Q** встраиваемых данных можно подсчитать по формуле: **Q=P*W*H/B** символов, где **P** - число битовых плоскостей, используемых для встраивания, **W** и **H** - ширина и высота изображения в пикселах, соответственно, **B** - число бит на символ. Основное преимущество способа - простота реализации. Основной недостаток этого способа обусловлен

ограниченным количеством битовых плоскостей и как следствие, детерминированностью встраивания. Последнее обстоятельство можно компенсировать путем перемешивания битовых плоскостей в зависимости от значений яркости изображения-контейнера.

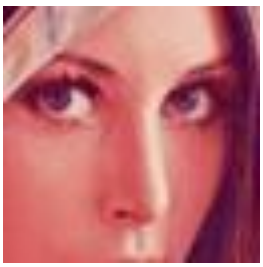


Рис. 1.

Рис. 2.

На **рис. 1** и **рис. 2** представлены примеры встраивания данных в битовые плоскости. В первом случае, для встраивания используется только одна плоскость нулевого разряда, а во втором - битовые плоскости четырех младших разрядов. Из сравнения изображений видно, что чем больше битовых плоскостей заминают встраиваемые данные, тем выше степень искажений, видимых глазу. Применение текстурных изображений, в качестве контейнеров, позволяет минимизировать визуальные искажения

Другим популярным методом встраивания сообщений является использование особенностей форматов данных, использующих сжатие с потерей данных (например JPEG). Этот метод (в отличии от LSB) более стоек к геометрическим преобразованиям и обнаружению канала передачи, так как имеется возможность в широком диапазоне варьировать качество сжатого изображения, что делает невозможным определение происхождения искажения.

Еще один способ основан на принципах цифровой голографии. В изображение-контейнер страиваются не непосредственно секретные данные, а их голограмма. Этот способ создает условную зависимость между видеоданными контейнера и встраиваемыми секретными данными и обладает наилучшей защищенностью к взлому. Применение голографического подхода, позволяет осуществлять встраивание срытых данных в обычные фотографии на бумажной или пластиковой основе. Для обнаружения и восстановления секретных данных требуется знание параметров создания голограммы. Основной недостаток этого способа связан с ограниченным объемом встраиваемых данных.

Рис. 3а.

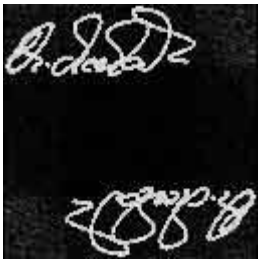


Рис. 3б.

Рис. 4а.

Рис. 4б.

Наиболее целесообразно применять этот способ для сокрытия небольших изображений, восстановление которых допускает некоторую потерю (подобно JPEG) качества: образцы подписей, образцы отпечатков пальцев и т.п. На **рис. 3б** представлен контейнер со встроенным факсимильным образцом подписи, а на **рис. 3а** показан результат восстановления. Аналогичный вариант для сокрытия дактилоскопического отпечатка иллюстрируется **рис. 4б** и **рис. 4а.** На **рис. 3а** и **рис. 4а**, восстановленные образцы имеют зеркальное отображение, что обусловлено появлением вещественного и мнимого изображения при восстановлении голограммы

Опасные картинки

Если вы получили почтовое вложение, будьте начеку. Не открывайте файлы, которые выглядят подозрительно!

Благодаря публичному обсуждению проблем информационной безопасности пользователи, похоже, усвоили эти нехитрые правила защиты от вирусов. И все же сугубая осторожность не помешает, поскольку некоторые из прописных истин, гласящих, к примеру, что вирус всегда является исполняемым файлом или что графические и текстовые файлы безвредны по своей природе, не вполне верны. Недавно открытая уязвимость при работе ряда программ для просмотра рисунков заставила вспомнить о том, что хакеры в состоянии внедрить вредоносный код даже в файлы JPEG! Впрочем, поддаваться панике не стоит: пока атаки, вызываемые файлами данного типа, немногочисленны. Но и с учетом этого бдительность терять нельзя. Приведем несколько примеров атак, связанных с JPEG-файлами, и поговорим о мерах предосторожности.

Perrun

О вирусе Perrun, появившемся в 2002 г., писали немало. При всей своей безобидности он остается первым примером вирусного кода, способного поражать JPEG-файлы. Как и подобные ему, Perrun скрывает вирусный код во внешне безвредном файле, в данном случае в рисунках JPEG. Но, в отличие от прочих, Perrun не может самостоятельно запускаться или рассылать многочисленные копии другим получателям. Для извлечения и исполнения вирусного кода, скрытого в JPEG-файле, требуется «троянский» компонент. Появление Perrun доказало: файлы изображений тоже могут быть атакованы. После этого «вирусописатели» пошли дальше и стали разрабатывать комбинации «JPEG + троян», что может привести к созданию куда более опасных вирусов.

Не JPEG, а вирус!

Хакеры нередко пользуются тем, что файлы JPEG выглядят безобидно и широко распространены. По Интернету гуляют зараженные сообщения, предлагающие полюбоваться на Дженнифер Лопес или взглянуть на снимки футбольного матча. Многие ни о чем не подозревающие пользователи уже попались в эту ловушку. Оказывается, вредоносный код скрывается в ложном JPEG-файле. Инфицированный файл выглядит как графический, но в действительности имеет двойное расширение и представляет собой исполняемый код. Не так давно похожий способ завлечения жертвы был применен в «червях» Bropia.F и Bobax.H. В файле Bropia на первый взгляд содержались эротические фотографии, а Bobax обещал фото мертвого Саддама Хуссейна, но те интернет-пользователи, которые поверили, что открывают файлы изображений, заразили свои компьютеры. Чтобы избежать этой ловушки, рекомендуется с помощью своевременно обновляемой антивирусной программы проверять перед открытием каждый вложенный файл.

В файле JPEG может прятаться троян

В сентябре 2004 г. на некоторых интернет-форумах в изобилии появились порнографические фотографии-ловушки: попытка открыть или просмотреть изображение грозила пользователю «троянской» атакой. Механизм ловушки основывался на одной ошибке в программном обеспечении Microsoft, предназначенном для просмотра изображений. Заметим, кстати, что эта ошибка была устранена в тот же день, когда появился вирус. Но, как всегда, большая часть пользователей не обновила вовремя программное обеспечение и, следовательно, попала в «группу риска». Другие фотографии-ловушки с грудастыми красотками рассылались через службу мгновенных сообщений AOL. Каким же образом просмотр изображения может спровоцировать вирусную инфекцию? Дело в том, что вирус эффективно использовал уязвимость графического интерфейса устройств (Microsoft Graphics Device Interface Plus, GDI+). В раздел примечаний программы хакеры поместили код, вызывающий переполнение буфера памяти. Это в свою очередь приводило к проникновению троянов. Чтобы защитить пользователей Интернета от подобных угроз, Symantec предлагает в составе своего антивирусного пакета служебную программу, проверяющую подлинность изображений JPEG.

Winamp — жертва «скинов»

В заключение упомянем еще пример вирусного кода, скрытого в графических файлах и использующего ошибку в проигрывателе Winamp. Так называемые «скины» (файлы, с помощью которых изменяется внешний вид программного обеспечения) для этого проигрывателя в действительности могут служить средством передачи вирусной инфекции. Данная ошибка была устранена в августе 2004 г., но сам факт еще раз напомнил об уязвимости таких, казалось бы, безвредных файлов, как файлы изображений

Литература:

1. www.confident.ru/magazine
2. http://www.osp.ru/
3. http://www.compdoc.ru/secur