Эссе по курсу "Защита информации",
кафедра радиотехники,

Московский физико-технический институт
(ГУ МФТИ),

http://www.re.mipt.ru/infsec

Компьютерная стеганография

Юников А. Л. 314гр.

Долгопрудный

2007 г

Стеганография - метод передачи информации, который скрывает само факт самой передачи информации. Главное отличие стеганографии от криптографии, где криптограф точно может определить является ли передаваемое сообщение зашифрованным текстом, заключается в возможности встраивать секретные сообщения в открытые сообщения так, чтобы невозможно было заподозрить существование встроенного тайного послания.

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

Бурное развитие вычислительной техники и новых каналов передачи информации способствует появлению новых стеганографических методов, в основе которых лежат особенности представления информации в компьютерных файлах, вычислительных сетях и т. п. Поэтому в последнее время появилось новое направление стеганографии - компьютерная стеганография.

1.Основные термины и определения

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

Основные принципы построения стегосистем:

1. криптоаналитик имеет полное представление о стеганографической системе и деталях ее реализации. Единственной информацией, которая остается неизвестной криптоаналитику, является ключ, с помощью которого только его держатель может установить факт присутствия и содержание скрытого сообщения;
2. если криптоаналитик 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;
3. криптоаналитик 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: текстовое сообщение, изображение, видео- или аудио-файл, и т. п.

Далее будем использовать слово "сообщение", так как сообщением может быть как текст или изображение, так и, например, аудиоданные. 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 (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.

Как и в криптографии, 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 к построению стегосистемы

Стегосистема должна отвечать следующим требованиям:

1. 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.
2. 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.
3. Для сохранения целостности встраиваемого сообщения необходимо использование кода с исправлением ошибки.
4. Для повышения надежности встраиваемое сообщение должно быть продублировано.

Основные приложения

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

Сокрытие внедряемых данных, передача вместе с контейнером скрытых данных 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.

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

В зависимости от назначения приложений стеганографии тредъявляются различные требования к соотношению 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 обратная зависимость надежности системы от объема встраиваемых данных.

Данная зависимость говорит о том, 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.

2. Основные принципы компьютерной стеганографии и области её применения

Основными положениями современной компьютерной стеганографии являются следующие:

1. Методы скрытия должны обеспечивать **аутентичность и целостность** файла.

2. Предполагается, что криптографу полностью известны возможные стеганографические методы.

3. Безопасность методов основывается на **сохранении** стеганографическим преобразованием основных **свойств** открыто передаваемого файла при внесении в него секретного сообщения и некоторой неизвестной противнику информации — ключа.

4. Даже если факт скрытия сообщения стал известен противнику через сообщника, извлечение самого секретного сообщения представляет сложную вычислительную задачу.

В связи с возрастанием роли глобальных компьютерных сетей становится все более важным значение стеганографии. В настоящее время стеганографические системы активно используются для решения следующих основных задач:

1. Защита конфиденциальной информации от несанкционированного доступа;
2. Преодоление систем мониторинга и управления сетевыми ресурсами;
3. Камуфлирования программного обеспечения;
4. Защита авторского права на некоторые виды интеллектуальной собственности.

Рассмотрим подробнее каждую из перечисленных задач.

Защита конфиденциальной информации от несанкционированного доступа

Это область использования КС является наиболее эффективной при решении проблемы защиты конфиденциальной информации. Так, например, только одна секунда оцифрованного звука с частотой дискретизации 44100 Гц и уровнем отсчета 8 бит в стерео режиме позволяет скрыть за счет замены наименее значимых младших разрядов на скрываемое сообщение около 10 Кбайт информации. При этом, изменение значений отсчетов составляет менее 1 %. Такое изменение практически не обнаруживается при прослушивании файла большинством людей.

Преодоление систем мониторинга и управления сетевыми ресурсами

Стеганографические методы, направленные на противодействие системам мониторинга и управления сетевыми ресурсами промышленного шпионажа, позволяют противостоять попыткам контроля над информационным пространством при прохождении информации через серверы управления локальных и глобальных вычислительных сетей.

Камуфлирование программного обеспечения (ПО)

Другой важной задачей стеганографии является камуфлирование ПО. В тех случаях, когда использование ПО незарегистрированными пользователями является нежелательным, оно может быть закамуфлировано под стандартные универсальные программные продукты (например, текстовые редакторы) или скрыто в файлах мультимедиа (например, в звуковом сопровождении компьютерных игр).

Защита авторских прав

Еще одной областью использования стеганографии является защита авторского права от пиратства. На компьютерные графические изображения наносится специальная метка, которая остается невидимой для глаз, но распознается специальным ПО. Такое программное обеспечение уже используется в компьютерных версиях некоторых

журналов. Данное направление стеганографии предназначено не только для обработки изображений, но и для файлов с аудио- и видеоинформацией и призвано обеспечить защиту интеллектуальной собственности.

2.2. Обзор известных стеганографических методов.

Основные направления развития приложений стеганографии:

1. Методы, основанные на использовании специальных свойств компьютерных форматов;
2. Методы, основанные на избыточности аудио и визуальной информации.

Сравнительные характеристики существующих стеганографических методов приведены в табл. 1.

Таблица 1. Сравнительные характеристики стеганографических методов

Стеганографические методы	**Краткая характеристика методов**	**Недостатки**	**Преимущества**
1. Методы использования специальных свойств компьютерных форматов данных			
1.1. Методы использования зарезервированных для расширения полей компьютерных форматов данных	Поля расширения имеются во многих мультимедийных форматах, они заполняются нулевой информацией и не учитываются программой	Низкая степень скрытности, передача небольших ограниченных объемов информации	Простота использования
1.2. Методы специального форматирования текстовых файлов:			
1.2.1. Методы использования известного смещения слов, предложений, абзацев	Методы основаны на изменении положения строк и расстановки слов в предложении, что обеспечивается вставкой дополнительных пробелов между словами	1. Слабая производительность метода,передача небольших объемов информации 2. Низкая степень скрытности	Простота использования. Имеется опубликованное программное обеспечение реализации данного метода
1.2.2. Методы выбора определенных позиций букв (нулевой шифр)	Акростих - частный случай этого метода (например, начальные буквы каждой строки образуют сообщение)		
1.2.3. Методы использования специальных свойств полей форматов, не отображаемых на экране	Методы основаны на использовании специальных "невидимых", скрытых полей для организации сносок и ссылок (например, использование черного шрифта на черном фоне)		
1.3. Методы скрытия в неиспользуемых местах гибких дисков	Информация записывается в обычно неиспользуемых местах ГМД (например, в нулевой	1. Слабая производительность метода, передача небольших объемов информации 2. Низкая степень скрытности	Простота использования. Имеется опубликованное программное обеспечение

	дорожке)		реализации данного метода
1.4. Методы использования имитирующих функций (mimic-function)	Метод основан на генерации текстов и является обобщением акростиха. Для тайного сообщения генерируется осмысленный текст, скрывающий само сообщение	1. Слабая производительность метода, передача небольших объемов информации 2. Низкая степень скрытности	Результирующий текст не является подозрительным для систем мониторинга сети
1.5. Методы удаления идентифицирующего файл заголовка	Скрываемое сообщение шифруется и у результата удаляется идентифицирующий заголовок,оставляя только шифрованные данные. Получатель заранее знает о передаче сообщения и имеет недостающий заголовок	Проблема скрытия решается только частично. Необходимо заранее передать часть информации получателю	Простота реализации. Многие средства (White Noise Storm, S-Tools), обеспечивают реализацию этого метода с PGP шифроалгоритмом
2. Методы использования избыточности аудио и визуальной информации			
2.1. Методы использования избыточности цифровых фотографии, цифрового звука и цифрового видео	Младшие разряды цифровых отсчетов содержат очень мало полезной информации. Их заполнение дополнительной информацией практически не влияет на качество восприятия, что и дает возможность скрытия конфиденциальной информации	За счет введения дополнительной информации искажаются статистические характеристики цифровых потоков. Для снижения компрометирующих признаков требуется коррекция статистических характеристик	Возможность скрытой передачи большого объема информации. Возможность защиты авторского права, скрытого изображения товарной марки, регистрационных номеров и т.п.

Как видно из табл. 1, первое направление основано на использовании специальных свойств компьютерных форматов представления данных, а не на избыточности самих данных. Специальные свойства форматов выбираются с учетом защиты скрываемого сообщения от непосредственного прослушивания, просмотра или прочтения. На основании анализа материалов табл. 1 можно сделать вывод, что основным направлением компьютерной стеганографии является использование избыточности аудио и визуальной информации. Цифровые фотографии, цифровая музыка, цифровое видео — представляются матрицами чисел, которые кодируют интенсивность в дискретные моменты в пространстве и/или во времени. Цифровая фотография — это матрица чисел, представляющих интенсивность света в определенный момент времени. Цифровой звук — это матрица чисел, представляющая интенсивность звукового сигнала в последовательно идущие моменты времени. Все эти числа не точны, т.к. не точны устройства оцифровки аналоговых сигналов, имеются шумы квантования. Младшие разряды цифровых отсчетов содержат очень мало полезной информации о текущих параметрах звука и визуальнного образа. Их заполнение ощутимо не влияет на качество восприятия, что и дает возможность для скрытия дополнительной информации.

Источники :

http://www.citforum.ru/internet/securities/stegano.shtml

http://www.securitylab.ru/analytics/216270.php
http://st.ess.ru/publications/articles/steganos/steganos.htm