Стеганография и существующие носители.
Steganography in current cover-medium.

Стеганография.

Стеганография дословно значит «скрытое письмо» - это искусство скрытой передачи информации, причем скрывается не только содержание сообщения, но и сам факт передачи. Цель стеганографии – не вызвать подозрений к передаче сообщений. Стеганализ - это искусство находить и уничтожать такие сообщения.

«сообщение» - информация, которую нужно скрыть.
«обложка» - графика, видео или любой другой информационный поток, используемый для скрытия сообщения.
«носитель» = «обложка» + «сообщение» + возможно «ключ», необходимый для извлечения скрытой информации.

Введение.

Стеганография включает в себя методы сокрытия секретных сообщений внутри «обложки». Как правило, сокрытие информации с использованием электронных носителей требует модификации свойств обложки, что в свою очередь может вызвать деградацию. Например, в случае компьютерной графики возможна деградация изображения, заметная глазом, что может указывать на специфические методы, использованные для скрытия сообщения, а также может нейтрализовать саму цель стеганографии – скрыть существование сообщения.

Двумя аспектами стеганализа являются обнаружение и уничтожение скрытого сообщения. Любой файл может быть обработан, с целью уничтожить потенциальное скрытое сообщение, вне зависимости от его наличия, но предварительное обнаружение сэкономит время на этапе уничтожения.

Частным случаем стеганографии является встраивание *«водяных знаков»* или *подписи* в обложку. Главное отличие состоит в целях применения методов: стеганография прячет сообщение (оно и является объектом сообщения), а «водяные знаки» дают дополнительную информацию о владельце авторских прав (в то время как объектом является сама обложка), не смотря на то, что методы могут в отдельных случаях совпадать. Технологии «водяных знаков», как правило, более устойчивы к атакам типа сжатие, обрезка, обработка с уничтожением младших битов информации.

Классификация методов:

Все инструменты для стеганографии можно разделить на две категории, работающие в области изображения (Image Domain) или в области преобразований (Transform Domain).

1. Инструмены области изображения манипулируют младшим значащим битом (LSB) или шумом в изображении. Такой подход типичен для стеганографии, и считается «простой системой» [limits]. Обычно используются форматы без потерь, данные могут быть напрямую восстановлены. Вместе с масками и обьектами изображения, к которым применяются «водяные знаки», инструменты этого типа в определенном смысле не зависят от формата «изображения», которым может являться не только двумерная картинка, а звук, видео, или любой битовый поток, в котором допустима манипуляция младшими битами (LSB) без видимых повреждений «обложки».

2. Инструменты области преобразований манипулируют алгоритмами и преобразованиями изображения, такими как DCT (Дискретное косинусное преобразование), используемое в JPEG, или широкополосным (импульсным, wavelet) преобразованием. Эти методы более тесно интегрированы с форматом обложки и алгоритмом сжатия, используемым, для уменьшения избыточности обложки (JPEG, MPEG-video, MP3-audio) – такие алгоритмы дают результат, находящийся ниже порога восприятия человека, но выше уровня, где начинается «избыточность», отбрасываемая алгоритмами сжатия (могут использоваться модели основанные на особенностях восприятия человека – например, в течение некоторого времени после громкого звука мы не можем услышать тихий звук, играющий фоном). Эти методы скрывают информацию в более значительных обьемах (или площадях) «обложки» и могут затрагивать статистические свойства «изображения», такие как яркость, громкость и т.п. Как правило, эти методы являются более устойчивами, чем битовые технологии, тем не менее существует выбор между количеством скрытой информации и достигаемой устойчивостью. Многие методы этой группы могут устоять при переводе из форматов без потерь в форматы с потерями, при записи на аналоговые носители (для звука и видео).

Методы и носители:

В качестве «обложки» могут использоваться любые «безобидные» данные (графика, звук, видео, текст, программы или любой другой осмысленный код), не вызывающие подозрений при передаче. Они будут нести скрытую информацию - это может быть открытый текст, шифротекст и т.д. Вместе, обложка и сообщение, дают «стего-носитель». Кроме того, может потребоваться дополнительная информация – ключ, для извлечения информации из стего-носителя.

Для каждого вида обложки придумано множество разнообразных способов встроить сообщение. Иногда берется произвольная обложка, иногда встраивание сообщения сопряжено с генерацией «псевдо-настоящей» обложки, которая удовлетворяет всем статистическим свойствам «настоящей» обложки.

1. Текст – довольно своеобразная обложка. Методы обычно связаны с расстановкой дополнительных пробелов (между слов и в конце строки), запятых, или заменой слов по словарю синонимов, а также генерации «псевдо-осмысленного» текста на основе словарей. Примерами могут быть:
   - Nicetext (http://www.ctgi.net/nicetext/) – создает текст из любого бинарного файла, возможно применения словарей и эмуляция авторского стиля.
   - Snow (http://www.darkside.com.au/snow/) – добавляет пробелы в конце строки
   - Stegonosaurus (http://www.fourmilab.ch/stego/) – генерирует бессмысленный текст, который по статистическим параметрам сходен со словарем.
2. Графика представляет собой прекрасный носитель для скрытой информации, поэтому было придумано множество различных технологий (см. литературу).
   a. Инструменты области изображения включают: StegoDos, S-Tools, Mandelsteg, EzSteg, Hide-and-Seek, Hide4PGP, White Noise Storm, Steganos.

   Как правило, методы состоят в дублировании цветов в палитре и использовании младших бит как носителя информации: для 24bit используются до 3 младших бит в каждом цвете, что дает возможность сохранять значительные объемы, но и объем обложки тоже велик. Неустойчивы против большинства атак.

b. Примерами области преобразований являются Jpeg-Jsteg, PictureMarc, JK-PGS, SysCop, SureSign.

Отдельно остановимся на Jpeg-Jsteg:

JPEG использует DCT для получения сжатия изображений. Сжатые данные хранятся как целые числа, тем не менее, вычисления производятся с плавающей точкой, после чего округляются. Ошибки округления определяют степень потерь при сжатии. Jpeg-Jsteg использует уровни округления DCT-коэффициентов для скрытия данных. Нахождение такого рода скрытой информации кажется очень сложным – особенностью DCT по отношению к другим преобразованиям является то, что оно минимизирует «блочность» получаемого изображения – когда границы между блоками 8x8 становятся видимыми.

Некоторые технологии используют характеристики инструментов области изображений и области преобразований. Это может включать в себя «мозаику», широкополосные методы и маскирование изображений, что добавляет избыточность к сохраненной информации. Эти методы могут устоять против некоторой обработки, например поворот или обрезка. «Мозаика» выбирает несколько областей изображения для маркировки – если одна область повреждена, то остальные могут уцелеть. Маски могут быть добавлены как в область изображения, так и как преобразование свойств изображения (при установке водяных знаков «подписывается» не всё изображение, а только часть, или несколько частей, что позволяет с большей избыточностью встроить меньший обьем информации в обложку, параллельно могут применяться широкополосные методы, которые распределяют ошибки, вызванные добавлением информации по всему изображению).

3. Звук

Поскольку несжатый звук, представляет собой довольно избыточный битовый поток, то в простом случае используют несколько младших бит для передачи сообщений. Более интересным является скрытие сообщений в сжатом звуке, например MP3, поскольку этот формат сегодня очень широко распространен в интернете.

- StegonoWav (работает с 16-bit WAV, прячет данные с использованием широкополосных методов)
- MP3Stego (http://www.petitcolas.net/fabien/steganography/mp3stego/index.html) (использует особенности сжатия Mpeg Layer 3)

4. Видео

Видео имеет самый большой по избыточности поток, т.е. открывает широкие возможности для создания инструментов стеганографии, но, в то же время, видео – это тот неразработанный участок, который сейчас осваивают производители цифровых фильмов. С помощью широкополосных методов возможно встроить водяные знаки так, что даже экранная съемка при наличии оригинала и времени для анализа даст информацию о владельце прав на данный видеоматериал. Кроме того, система должна обеспечивать стойкость в случае обьединения нескольких «пользователей» лицензионного материала с целью удаления подписи [dcinema].

Варианты атак

Стеганография имеет много общего с криптографией: как аналитик применяет криптоанализ к шифротексту, чтобы расшифровать сообщение, так он применяет стеганализ к стего-носителю чтобы определить наличие скрытого сообщения. В криптографии сравнение производится по известному открытому тексту (которого может и не быть) или шифротексту, в стеганографии – между обложкой, носителем и, возможно,

фрагментами сообщения. В стеганографии сообщение может быть дополнительно зашифровано, в этом случае после извлечения применяются технологии криптоанализа.

Варианты атак в криптографии: по известному шифротексту, по известному открытому тексту, по выбранному открытому тексту, и по выбранному шифротексту. В стеганографии методы во многом похожи: по известному носителю, по известной обложке, по известному сообщению, по известному алгоритму, и по выбранному сообщению.

1) по известному носителю – то же самое, что и по известному шифротексту в криптографии – для анализа доступен только носитель;
2) если оригинальная «обложка» доступна вместе с «носителем» - атака «по известной обложке»;
3) по «известному сообщению» - данная атака очень сложна, и, как правило, эквивалентна первому случаю;
4) по «известному алгоритму» - известны носитель и алгоритм, ищем ключ и текст;
5) по «выбранному сообщению» - аналитик получает носитель с помощью некоторого алгоритма из известного сообщения с целью уловить закономерности в форме носителя, указывающие на конкретный алгоритм или программу.

Если не известно, какой инструмент был использован для встраивания информации и ключ (если нужно), определение факта сообщения может быть очень сложным. Тем не менее, некоторые инструменты создают изображения с характеристиками, которые указывают на метод или инструмент, которые были использованы, например, для простых систем – это наличие или, наоборот, отсутствие определенных статистических шаблонов в младших битах носителя. Такие особенности, как дублирование цветов в палитре сразу могут вызвать подозрение. Более сложные методы дают повышенный шум, изменение характеристик, например яркости, цветового диапазона, но такого рода изменения сложно отследить, не имея в наличии исходного варианта обложки до внедрения скрытой информации. Определение наличия сообщения также сильно зависит от модели «средней обложки», ее статистических свойств, которые могут изменяться при встраивании сообщения.

Однако, активный наблюдатель, может проводить атаки, направленные на уничтожение скрытой информации: размытие по гауссу, обрезка, перестановка похожих строк или солбцов изображения, создание эха с малым временем задержки, нелинейными искажениями картинки (например, небольшая сферизация), срыв синхронизации перестановкой кадров или удаление и повтор аудио-сэмплов и т.п.

Специально для тестирования методов встраивания водяных знаков в изображения был создан набор стандартных тестов, дающий представление о неустойчивости современных методов. StirMark (http://www.petitcolas.net/fabien/watermarking/stirmark/index.html). Также разрабатывается AudioStirMark.

Теоретическая точка зрения

Интересно узнать, какой максимальный объем информацмм можно скрыть в исходной обложке, так, чтобы вероятность опознавания была меньше δ, или в случае активного наблюдателя – существует ли возможность установить канал без ошибок, если активный наблюдатель изменяет некоторое количество бит в передаваемом сообщении.

1. В случае наличия пассивного наблюдателя (passive warden) – мы всегда можем создать защищенный канал, не смотря на то, насколько мало возможное искажение обложки,

которое заметит наблюдатель (от него зависит только время требуемое на передачу нужного количества информации).

2. В случае активного наблюдателя, который может модифицировать передаваемую информацию, задача усложняется (active warden).

Основная идея стеганографии состоит в преобразовании обложки с изменением бит, которые на данный момент избыточны. Избыточны - в понимании, что некоторый нетривиальный набор бит определенного размера может быть изменен так, что это не будет замечено наблюдателем, или вообще замечено, если не известно, какие именно биты выбраны. Очевидно, что таким образом стеганография не ожидает найти широкополосные каналы передачи сообщений, т.к. большая избыточность была бы устранена по экономическим причинам с помощью сжатия. В свою очередь, сжатие тоже ограничено экономическими причинами – сколько процессорного времени мы готовы потратить, чтобы сжать сообщение? Таким образом, потратив чуть больше усилий, чем «обычный» пользователь, мы сможем получить некоторую дополнительную «избыточность», которую можно затем использовать для скрытия сообщений. Но, допустим, существует подслушивающая сторона, которой доступны много большие ресурсы – тогда наша «избыточность» попадает в ту область, которую можно смоделировать.

Пусть алгоритм сокрытия известен подслушивающему, тогда устойчивость алгоритма обеспечивается ключем. Используем ключ для генерации псевдослучайной последовательности для выбора избыточных бит из потока для восстановления сообщения. Тогда наблюдатель, не зная ключа, может изменить часть бит, с целью уничтожить сообщение. Тогда, согласно теореме Шеннона для канала с ошибками: $C=\max(H-H_{noise})$, поскольку изменения вносимые наблюдателем тоже должны быть незаметны, то их энтропия не превысит энтропию канала, образованного избыточностью информации, тогда при наличии соответствующего корректирующего кода у получателя сообщения, передача сообщения всё-таки возможна. (Prisoner Problem with active warden) [limits]

Literature

[Fabien] Fabien A. P. Petitcolas – The information hiding homepage

[Neil] Neil F. Johnson and Sushil Jajodia - Steganalysis of Images Created Using Current Steganography Software. Center for Secure Information Systems. George Mason University, Fairfax, Virginia. http://www.jjtc.com/ihws98/jjgmu.html

[infohiding] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn. Information hiding – a survey. *Proceedings of the I.E.E.E.*, 87(7):1062–1078, July 1999.

[limits] Ross J. Anderson and Fabien A. P. Petitcolas. On the limits of steganography. *I.E.E.E. Journal of Selected Areas in Communications*, 16(4):474-481, May 1998. Special Issue on Copyright & Privacy Protection. ISSN 0733-8716.

[dcinema] Darko Kirovski, Marcus Peinado and Fabien A. P. Petitcolas. Digital rights management for digital cinema. Invited paper. *Security in Imaging: Theory and Applications, International Symposium on Optical Science and Technology*. San Diego, U.S.A., July 2001.