СТЕГАНОГРАФИЯ:
СИНТЕЗ И АНАЛИЗ СТЕГАНОГРАФИЧЕСКИ СКРЫТОЙ ИНФОРМАЦИИ

Термины, определения и сокращения

Стеганография – наука о скрытой передаче информации путем сохранения в тайне самого факта передачи.

Стеганографическая система (стегосистема) - это совокупность средств и методов, используемых для создания скрытого канала передачи информации.

Ключи в стегосистемах бывают двух типов: закрытые и открытые. Стегосистема, использующая закрытый ключ, должна обеспечивать создание ключа до начала обмена и передачу по защищенному каналу.

Сообщение – файл, произвольного типа, который предназначен для скрытия.

Контейнер – файл, который может быть использован для скрытия в нем сообщения.

Пустой контейнер – контейнер, который не содержит скрытой информации.

Стего (стегоконтейнер или заполненный контейнер) – контейнер, который содержит скрытую информацию.

Стегообъект – объект (файл), полученный в результате внедрения в объект сообщения.

Стегоключ (стеганографический ключ) – конкретное секретное состояние некоторых параметров алгоритма стеганографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

Стеганографический канал (стегоканал, канал передачи) – путь, по которому контейнер попадает от отправителя к получателю.

Злоумышленник (противник) – человек, пытающийся получить несанкционированный доступ к сообщению. Тот, кому данная информация не предназначена.

Исследование проблем разработки, совершенствования и применения методов защиты информации в процессе её хранения и передачи привлекает внимание множества исследователей, так как разработка новых и совершенствование имеющихся методов защиты имеет большое значение для развития инфокоммуникационных систем.

В современных системах защиты информации огромную роль играют не только методы криптографии, но и методы стеганографии. Если классическая задача криптографии состоит в том, чтобы скрыть от третьих лиц содержание сообщения, то классическая задача стеганографии – скрыть сам факт передачи сообщения. Стеганография, как метод защиты информации, появилась очень давно. Тем не менее данная наука не теряет совей актуальности и сейчас. В развивающемся мире высоких технологий задача сохранения информации обладателя в секрете остается первостепенной, поэтому стеганография тоже не стоит на месте.

Хотелось бы отметить, что в настоящее время информационная безопасность является мировой проблемой, и ежедневно на предприятиях происходят утечки информации, однако такие методы скрытия информации, как стеганография дают возможность защитить вашу информацию даже в таких непредвиденных случаях, поэтому нельзя недооценивать данный метод, как средство защиты важных сведений. Задача стеганографии решается посредством внедрения сообщений в безобидные на вид объекты данных, называемые *контейнерами*, передача которых является обычным делом и не вызывает подозрений. Ключевым понятием стеганографии является *стегосистема*, то есть совокупность средств и методов, используемых для организации скрытого канала передачи данных.

Существует и ряд других актуальных задач, которые принадлежат стеганографии, например, защита авторских прав, которая также базируется на внедрении в авторские цифровые документы скрытых сообщений, идентифицирующих автора или законных получателей.

Обратная задача стеганографии называется стегоанализом. В отличие от криптоанализа, основной целью которого является раскрытие содержания сообщения, стегоанализ, в первую очередь, направлен на раскрытие факта наличия связи, т. е. на выявление наличия скрытых сообщений.

Стеганография и стегоанализ неразрывно связаны между собой. Их методы постоянно конкурируют друг с другом и успехи в одной области, как правило, приводят к появлению новых результатов в другой. Так, невозможно качественно решить задачу стегоанализа, не рассматривая новейших методов внедрения скрытой информации.

Хотя рассматриваемые задачи известны издревле, на современном этапе проблемами стеганографии и стегоанализа занимаются многие российские и зарубежные ученые. Первые исследования в этой области включают работы М. Куттера (Kutter, M.), Ф. Джордана (Jordan, F.), Ф. Боссэна (Bossen, F.), Г. Лангелара (Langelaar, G.), Л. Марвела (Marvel, L.) и многих других.

Среди ныне действующих ученых большой вклад в развитие стеганографии внесли работы Р. Андерсона (Anderson, R.), К. Кашена (Cachin, C.), Н. Провоса (Provos N.), К. Салливана (Sullivan, K.), Х. Фарида (Farid, H.), Дж. Фридрич (Fridrich, J.), А. Кера (Ker, A.) и других исследователей.

В последние годы значительные успехи были также достигнуты представителями Российской Сибирской школы теории информации, возглавляемой проф. Б. Я. Рябко.

1.1 Основные положения стеганографии

Современная компьютерная стеганография основана на следующих положениях:

1. Методы скрытия должны обеспечивать аутентичность файла. Под аутентичностью понимают абсолютное совпадение скрываемого и восстановленного текста.
2. Предполагается, что эксперту 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. Если факт сокрытия сообщения стал известен эксперту, извлечение самого секретного сообщения должно представлять собой задачу, решение которой требует значительных затрат на создание и эксплуатацию программно-аппаратных средств дешифровки.

1.2 Основные задачи стеганографических систем

В настоящее время стеганографические системы активно используются для решения следующих основных задач:

1. Преодоление систем мониторинга и управления сетевыми ресурсами.

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

2. Защита авторского права на некоторые виды интеллектуальной собственности.

На графические изображения, представленные в цифровом виде, наносится специальная метка, которая остается невидимой для глаз, но распознается специальным программным обеспечением. Данное направление стеганографии получило широкое распространение для обработки

изображений, файлов с аудио- и видеоинформацией и призвано обеспечить защиту интеллектуальной собственности.

3. Защита конфиденциальной информации от несанкционированного доступа.

Это область использования КС является наиболее эффективной при решении проблемы защиты конфиденциальной информации.

1.3 Методы встраивания сообщений

Методы компьютерной стеганографии развиваются по двум основным направлениям:

1. Методы, использующие специальные свойства компьютерных форматов;

2. Методы, использующие избыточность аудио и визуальной информации. Основным направлением компьютерной стеганографии является использование избыточности аудио и визуальной информации.

Любая цифровая информация (фотографии, музыка, видео) представляется матрицами чисел, кодирующими интенсивность в дискретные моменты в пространстве и времени. Поскольку устройства оцифровки аналоговых сигналов не точны, то все числа, представленные в кодирующих матрицах, так же представлены не точно. Младшие разряды содержат минимальное количество информации о параметрах звука или графического файла. Заполнение этих разрядов не влияет в большинстве случаев на качество восприятия. Это свойство дает возможность для скрытия дополнительной информации.

1.4 Выбор контейнера

Надежность стегосистемы и возможность обнаружения факта передачи скрытого сообщения в большей степени зависит от используемого контейнера. При выборе типа информации для скрытия (звук, статические и динамические изображения) наиболее широкое применение получили статические изображения. Причиной этому может послужить наличие в большинстве изображений текстурных областей, имеющих шумовую текстуру. В связи с этим необходимо находить участи пригодных для встраивания дополнительной информации, слабой чувствительностью человеческого глаза к незначительным изменениям цветовых, яркостных и др. характеристик изображений, а также бурно развивающимися методами цифровой обработки информации.

Возможны следующие варианты контейнеров:

- Генерация контейнера производится самой стегосистемой. Такой подход называется конструирующей стеганографией.
- Выбор контейнера осуществляется из множества контейнеров. Для реализации этого варианта генерируется большое

число альтернативных контейнеров. После этого выбирается наиболее подходящий для сокрытия сообщения. Такой подход называется селектирующей стеганографией. Необходимо учитывать, что при выборе оптимального контейнера из множества сгенерированных важнейшим требованием является естественность контейнера.

- Генерация контейнера осуществляется вне стегосистемы. Недостатком этого случая является отсутствие возможности выбора контейнера. Назовем это безальтернативной стеганографией.

По протяженности контейнеры можно подразделить на два типа: непрерывные (потоковые) и ограниченные (фиксированной длины).

Потоковый контейнер характеризуется невозможностью определения его начала и конца.

Однако контейнер фиксированной длины тоже имеет свои недостатки. Например, он обладает ограниченным объемом. Преимуществом данного контейнера является то, что отправитель заранее знает размер файла и может выбрать скрывающие биты в подходящей псевдослучайной последовательности.

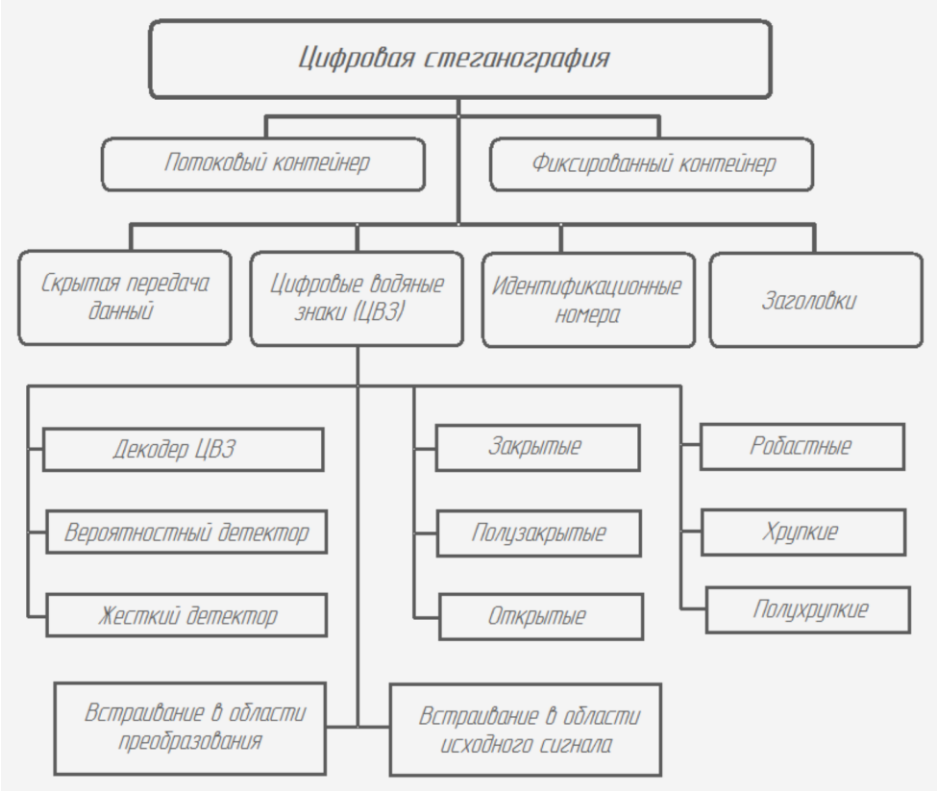

Рисунок 1 –

1.5 Методы использования специальных свойств компьютерных форматов

Современные методы компьютерной стеганографии развиваются в двух основных направлениях. Рассмотрим каждое из них.

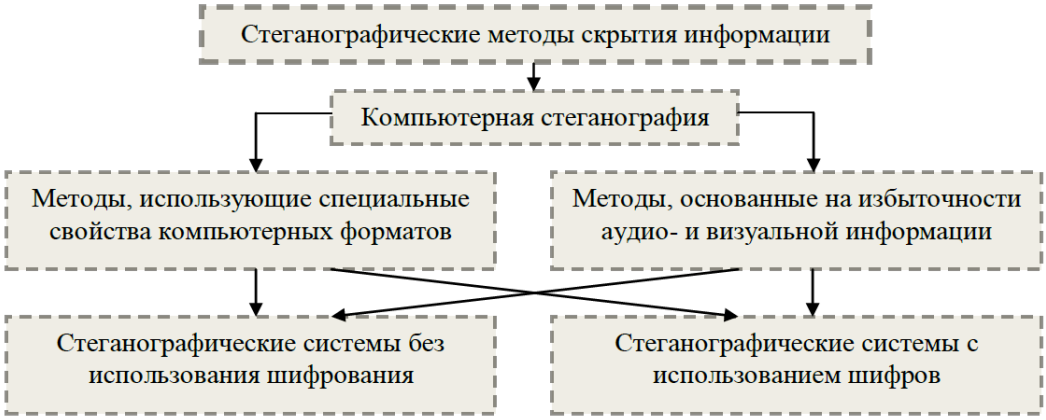

Рисунок 2 –

Это 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.

В зависимости от вида специальных свойств форматов различают такие стеганографические методы:

1. *Основанные на использовании зарезервированных для расширения полей компьютерных форматов файлов.* Поля для расширения имеются во многих мультимедийных форматах и предназначены для совершенствования, обновления и совместимости новых версий форматов со старыми. Как правило, эти поля заполняются нулевой информацией и не учитываются программами, и поэтому могут быть использованы для передачи дополнительной информации. Недостатком этих методов является низкая степень скрытности и передача небольших объемов скрываемой информации.

2. *Основанные на специальном форматировании текстовых файлов,* известны уже давно, использовались задолго до появления компьютерных технологий и включают в себя методы:

- использующие заранее известное смещение слов, предложений, абзацев в текстовом файле, основаны на изменение положения строк и расстановки слов в предложении, что производится вставкой дополнительных пробелов между словами, увеличений

промежутков незаметно визуально, но фактически передает скрываемую информацию;

- основанные на выборе определенных позиций букв (нулевой шифр). Например, выбор пятой буквы каждого последнего слова в строке в пределах одной страницы. Сюда же относятся художественные приемы тайнописи – акростих, хорошо известный знатокам поэзии, это такая организация стихотворного текста, при которой, например, начальные буквы каждой строки образуют скрываемое сообщение;
- использующие специальные свойства полей форматов, не отображаемых на экране. Например, использование черного шрифта на черном фоне ил специальных «невидимых», скрытых полей для организации сносок и ссылок.

3. *Основанные на скрытии в неиспользуемых местах гибких дисков.* Название этой группы говорит само за себя и имеет те же преимущества и недостатки, что и методы, основанные на использовании зарезервированных для расширения полей форматов.

4. *Основанные на имитирующих функциях (mimic*-function) – этот вид стеганографии основан на генерации текстов и является обобщением акростиха. Для заданного скрываемого сообщения генерируется осмысленный текст, который содержит скрываемое сообщение. При этом текст является грамматически и синтаксически правильным и статистически эквивалентным текстам на подобную тему. Такие тексты могут быть неподозрительны для систем мониторинга сети, но все же человек может быстро определить отсутствие всякого смысла в содержании текста.

5. *Основанные на использовании кодов, исправляющих ошибки;* скрытие данных в дополнительной информации, используемой помехозащищенными кодами при исправлении случайных ошибок и обеспечении точности передачи цифровой информации. Если информация спрятана, а на приемном конце код снят, то наблюдатель не будет даже знать, что было отправлено сообщение.

6. *Основанные на удалении идентифицирующего файл заголовка.*

В этом методе скрываемое сообщение шифруется и у результата удаляется идентифицирующий заголовок, оставляя только шифрованные данные, которые выдаются за случайную, возможно, искаженную информацию. Получатель заранее знает о передаче сообщения и имеет недостающий заголовок. При этом проблема скрытия решается только частично. Этот метод не является полностью стеганографическим, а служит скорее дополнением к ним. Хотя многие программные средства (WhiteNoiseStorm) обеспечивают эту дополнительную степень защиты с использованием алгоритма шифрования PGP.

Это лишь некоторые методы, иллюстрирующие эвристический подход в стеганографии.

Недостатками известных методов, основанных на использовании специальных свойств форматов файлов, являются:

- низкая степень скрытности (скрытность основывается на незнании противником самого алгоритма скрытия);
- передача небольших объемов скрываемой информации.

К достоинствам можно отнести простоту реализации. Следует заметить, что уже опубликован ряд программ, реализующих некоторые алгоритмы.

1.6 Методы использования избыточности аудио- и видеоинформации

Основным и наиболее перспективным направлением является использование избыточности звуковой и визуальной информации.

Цифровые фотографии, цифровая музыка, цифровое видео представляются матрицами чисел, которые кодируют интенсивность в специфические моменты в пространстве и/или времени. Цифровая фотография – это матрица чисел, представляющих интенсивность цветов в определенных точках кадра. Цифровой звук – это последовательность чисел, представляющая интенсивность звукового сигнала в идущие один за другим моменты времени.

Младшие разряды цифровых отсчетов содержат очень мало полезной информации о текущих параметрах звука и визуального образа. Существует мнение, что их заполнение ощутимо не влияет на качество восприятия, что и дает возможность скрытия дополнительной информации; указанный способ скрытия реализован в коммерческих программах.

Графические цветные файлы со схемой смешения RGB кодируют каждую точку рисунка тремя байтами. Каждая такая точка состоит из аддитивных составляющих: красного, зеленого, синего. Изменение каждого из трех наименее значимых бит приводит к изменению менее 1% интенсивности данной точки. Это позволяет размещать в стандартной графической картинке объемом 800 Кбайт около 100 Кбайт информации, что незаметно при просмотре изображения. Другой пример. Только одна секунда оцифрованного звука с частотой дискретизации 44100 Гц. уровнем отсчета 8 битов в стереорежиме позволяет скрыть за счет замены наименее значимых младших разрядов скрываемым сообщением около 10 Кбайт информации. При этом изменение значений отсчетов составляет менее 1%. Такое изменение практически не обнаруживается при прослушивании файла большинством людей.

Достоинствами этих методов являются:

- скрытие больших объемов данных (если не ставится задача скрытности от статистических методов контроля);
- относительная безопасность методов, т.е. невозможность определить факт скрытия, не выявив:

1) способ оцифровки сигнала;
2) природу сигнала;
3) статистические связи и зависимости для данного вида сигнала;
4) статистические отклонения исследуемого контейнера от исходного.

При этом в отличие от методов, основанных на использовании специальных свойств компьютерных форматов, методы использования избыточности предполагают, что заранее полностью известна стеганографическая система и детали ее реализации, неизвестным остается лишь правило размещения бит сообщения вдоль пути скрытия.

1.7 Задачи развития методов стеганографии

Рассмотрим актуальные задачи развития методов стеганографии. На сегодня методы компьютерной стеганографии предназначены для использования в следующих прикладных задачах:

1. Разведывательная деятельность.
2. Преодоление систем мониторинга и управления сетевыми ресурсами.
3. Камуфлирование математического обеспечения.
4. Защита авторского права на некоторые виды интеллектуальной собственности.
5. Медицинская безопасность.
6. Внедрение (включение) комментариев в мультимедийные файлы.
7. Возможность правдоподобного отрицания.
8. Автоматический контроль рекламных объявлений по радио.

Остановимся несколько подробнее на некоторых из перечисленных задач.

В первую задачу входит скрытая передача похищенной информации.

Стеганографические методы, направленные на противодействие системам мониторинга и управления сетевыми ресурсами, могут применяться в тех регионах мира, где регулируется или запрещается использование стойких криптографических методов. Стеганографические методы призваны противостоять попыткам контроля над информационным пространством при прохождении информации через серверы управления локальных и глобальных вычислительных сетей.

Другой важной задачей стеганографии является камуфлирование программного обеспечения. В тех случаях, когда использование программного обеспечения является нежелательным признаком, оно может быть закамуфлировано под стандартные универсальные программные продукты (например, текстовые редакторы) или скрыто в файлах мультимедиа (например, в звуковом сопровождении компьютерных игр). Заметим, что информация не передается от одного лица другому, а остается на магнитном диске. В этом случае стеганографические методы позволяют скрывать не факт передачи, а факт существования информации.

При обработке медицинских изображений (рентгеновских снимков, результатов ЭКГ и т.д.) необходима связь самого изображения и данных о пациенте (Ф.И.О., дата, лечащий врач). Использование методов внедрения характеризующей пациента информации в графический файл позволяет не только устранить случайную или преднамеренную подмену и потерю медицинских заключений, но и позволяет автоматически обрабатывать и

хранить результаты на ЭВМ. Кроме того, медицинская безопасность исследует способы психофизического воздействия на человека (например, использование 25-го кадра) и меры защиты от них.

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 программным обеспечением (ПО). Такое ПО уже используется в компьютерных версиях некоторых журналов. Это направление стеганографии предназначено не только для обработки изображений, но и для файлов с аудио- и видеоинформацией и призвано обеспечить защиту интеллектуальной собственности. Защита интеллектуальной собственности включает внедрение водяных знаков (watermarking) и «отпечатков пальцев» (fingerprinting), которые позволяют доказать незаконность использования авторского права. Водяные знаки – это метки авторского права, срытые в содержании. «Отпечатки пальцев» - это метки, вложенные в копии объекта, которые определяются для различны заказчиков (подобно скрытому регистрационному номеру). Это позволяет владельцу интеллектуальной собственности идентифицировать заказчиков, определять тех, кто нарушил лицензионное соглашение. Существует некоторое различие между классической формулировкой стеганографической проблемы, известной как «Проблема заключенных», и проблемой защиты авторских прав. В первой проблеме успешная атака на систему (взлом) состоит в обнаружении факта скрытия, во втором – наоборот, всем может быть известно о наличии внедренных меток. Так что успешная атака на систему состоит не в обнаружении меток, а в их удалении или внесении дополнительных меток. Предотвращение таких методов взлома системы скрытия может основываться на внедрении цифровой сигнатуры объекта или временных меток.

Увеличение объемов баз данных, содержащих видео- и аудиопродукцию, требует эффективной системы поиска и идентификации содержания файла. С этой целью в мультимедийные данные внедряется информация об авторе произведения, исполнителе, содержании, дате и т.п.

Еще одно направление стеганографии – возможность правдоподобного отрицания, основанная на стеганографической файловой системе. Стеганографическая система файлов является механизмом защиты, способным обеспечить высокую степень защиты от вынужденного разглашения информации. Этот механизм позволяет правдоподобным образом отрицать существование отдельных файлов. Даже если противник имеет полный доступ к ресурсам системы.

Методы стеганографии используются для автоматического контроля рекламы, передаваемой по радио, - это автоматизированные системы, предназначенные для проверки факта воспроизведения рекламного сообщения согласно заключенному договору.