**1) Стеганография ( Steganography)**

Определение стеганографии: Стего – скрытый, графо – пишу, буквально «тайнопись» мы будем называть науку о защищённой передаче информации, осуществляемой путём сокрытия самого факта передачи информации.

В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает сам факт существования канала передачи информации.

Стеганографическая система – совокупность методов и средств, предназначенных для создания канала защищённой передачи информации, осуществляемой путём сокрытия самого факта передачи информации.

О классификации, стеганография может быть разделиться как на рис. 1.

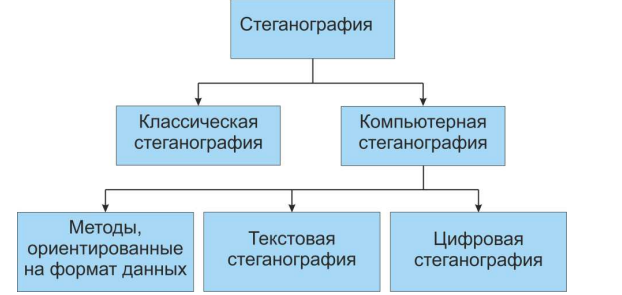


Рисунок 1 – Основные направления стеганографии

Классическая стеганография относится к методам скрытия информации, которые использовались до появления современных цифровых технологий. Эти методы включали различные техники, направленные на скрытие сообщений в физических объектах или текстах.

Компьютерная стеганография – Это раздел стеганографии, изучающий системы скрытой передачи информации, в которых в качестве контейнера и сообщения выступают аппаратное или программное обеспечение компьютера или цифровые данные, которые он хранит и обрабатывает.

К текстовой стеганографии принято относить все методы, в котоых встраивание секретной информации осуществляется в содержимое текстового файла.

В методах цифровой стеганографии встраивание секретного сообщения осуществляется в одномерные или многомерные цифровые сигналы, имеющие физическую природу. К таким сигналам мы будем относить цифровые изображения, звуковые файлы и видеофайлы. Отличием от методов, ориентированных на формат данных, является то, что они не используют особенностей конкресного формата представления информации, поскольку втсраивание осуществляется за счёт изменения содержимого сигнала, а не каких-либо специальных полей. При встраивании информации учитываются особенности человеского зрения и слуха, за счёт чего может бытт достигнута незаметность встроенной информации.

**2) Цифровой водяной знак (ЦВЗ)**

В тесной связи с цифровой стеганографией находятся вопросы, связанные с так называемыми цифровыми водяными знаками (ЦВЗ).

Встраивание ЦВЗ (Digital Watermarking) называется процесс внедрения в цифровой сигнал информции, имеющей некоторое отношение к этому цифровому сигналу. Цифровым водяным знаком называется собственно внедряемая информация. Примером такой информации может быть идентификатор автора, предназначеный для защиты авторских прав на аудиовизуальное произведение, или электронная цифровая подпись, подтверждающая аутентичность цифровой мультимедийной информации.

Системой встраивания ЦВЗ будем называть совокупность методов и средств, предназначенных для внедрения в цифровой сигнал информации, имеющей некоторое отношение к этому цифровому сигналу.

**3) Какие существуют методы встраивания скрытой информации в контейнер**

Под встраиванием информации (в узком мысле) будем понимать область знаний, охватывающую широкий круг проблем внедрения информации (секретная информация) в содержимое другого информационного объекта (называемого открыто передаваемой информацией или контейнером).

В современное времени есть несколько методов встраивания скрытой информации в контейнер. По зависимости от факта наличия сообщения, если факт наличия сообщения сокрыт то используем стеганографическое встраивание ЦВЗ, а если факт наличия сообщения известен используем нестеганографическое втраивание ЦВЗ. Кроме того, можно упомянуть:

* + Метод наименее значимого бита (LSB): Встраивание информации в наименее значимые биты пикселей изображения или аудио сэмплов.
  + Методы пространственной области: Встраивание информации напрямую в пиксели изображения.
  + Методы трансформной области: Встраивание информации в коэффициенты, полученные после преобразования изображения (например, дискретное косинусное преобразование (DCT), дискретное вейвлет-преобразование (DWT)).
  + Методы амплитудной и фазовой модуляции: Встраивание информации в амплитуду или фазу аудио сигналов.
  + Методы на основе спектрального анализа: Встраивание информации в частотные компоненты данных.
  + Методы на основе статистических свойств: Изменение статистических характеристик контейнера для встраивания информации.

**4) Как работает метод встраивания в наименее значимую битовую плоскость (Least Significant Bit, НЗБ, LSB)**

Встраивание информации в наименее значимые биты контейнера (или сокращённо НЗБ-встраивание) – исторически один из первых, и пожалуй, наиболее известный широкой публике подход, который может применяться как для стеганографии, так и для защиты сигналов цифровыми водяными знаками. НЗБ-встраивание вполне подходит для задач, в которых отсутствуют жёсткие требования по стойкости к отдельным видам атак.

Основная идея метода заключается в том, что любое полутоновое изображение может быть представлено в виде совокупности битовых плоскостей. Так, контейнер будет иметь вид:

*,* (1)

где – битовые плоскости, – номер битовой плоскости, К = 8 – их количество

Наименее и наиболее значащими битовыми плоскостями являются соответственно С1 и С8; если изменить значения бита С1, то яркость изменится на единицу; если же изменить значение бита С8, то яркость изменится на 128. Мы можем встраивовать информации в одну *р-ю* битовую плоскость, тогда носитель информации будет иметь вид:

, (2)

где для всех .

Метод LSB является одним из наиболее простых и часто используемых методов стеганографии для встраивания скрытой информации в цифровые изображения. Основной принцип метода заключается в замене наименее значимых битов (обычно последние биты каждого цветового канала пикселя) контейнера (например, изображения) битами скрытого сообщения. Метод LSB (Least Significant Bit) работает следующим образом:

* Извлечение LSB: В стандартном изображении RGB каждый пиксель представлен тремя байтами (красный, зелёный, синий), и каждый байт состоит из 8 бит. Наименее значимый бит — это последний (самый правый) бит каждого байта.
* Замена LSB: Чтобы встроить сообщение, каждый наименее значимый бит каждого пикселя заменяется битом из сообщения.
* Пример: Допустим, у нас есть пиксель с цветом, представленным байтами (10100110, 11010011, 01101101). Если мы хотим встроить битовую последовательность "101", мы заменим наименее значимые биты каждого байта: (10100111, 11010010, 01101100).

Из-за изменений только наименее значимого бита, визуальные изменения в изображении практически незаметны для человеческого глаза.

**5) Какие существуют методы стегоанализа.**

Под стегоанализом обычно понимается атака на стеганографические системы, целью которой является обнаружение канала скрытой перадачи информации. Существуют различные методы стегоанализа, которые можно разделить на следующие категории:

* Статистические методы: Эти методы основаны на анализе статистических свойств контейнера (изображения, аудио или видео файла). Они включают:
  + Анализ гистограмм: Исследование распределения значений пикселей или частот.
  + Расчет энтропии: Оценка уровня случайности данных.
  + Метод χ² (хи-квадрат): Проверка соответствия распределения значений теоретическому распределению.
* Методы анализа целостности: Основаны на выявлении нарушений целостности контейнера, которые могли произойти из-за встраивания скрытого сообщения.
* Анализ временных и пространственных зависимостей: Включает изучение изменений в пространственных и временных зависимостях данных, что может указывать на присутствие скрытой информации.
* Методы машинного обучения: Использование алгоритмов машинного обучения для классификации данных как содержащих или не содержащих скрытую информацию. Включает обучение моделей на метках данных с известным присутствием или отсутствием стеганографической информации.
* Просты признаки для НЗБ-систем: Методы стегоанализа могут использовать простые признаки для обнаружения встраивания информации в наименее значимые биты (НЗБ, LSB). Эти признаки включают:
* Изменение гистограммы: При встраивании информации в НЗБ гистограмма распределения значений пикселей может изменяться. Если гистограмма равномерного изображения становится более равномерной или показывает характерные пики, это может указывать на наличие стеганографии
* Анализ последовательности битов: Изменения в наименее значимых битах могут нарушать нормальную структуру данных. Например, последовательность LSB в изображении обычно не является случайной, но после встраивания данных может стать ближе к случайной.
* Сравнение соседних пикселей: В LSB стеганографии значения соседних пикселей могут показывать аномальные изменения. Это особенно заметно при анализе корреляции между пикселями.
* -встраивание: Метод ±1-встраивания (±1 embedding) является модификацией традиционного метода LSB. Вместо замены наименее значимого бита значение пикселя изменяется на ±1 для встраивания бита скрытой информации.
* Метод гистограм пар значений: один из самых простоых и наиболее известных методов целенаправленного стегоанализа НЗБ-встраивания. Использует расчёт статистики хи-квардрат для проверки гипотезы о виде распределения яркости контейнера.

Применение различных методов стегоанализа позволяет эффективно обнаруживать и противодействовать использованию стеганографии для скрытия информации в цифровых данных.