1.1. Введение в стеганографию и цифровые водяные знаки

Материалы курса лекций "Цифровые водяные знаки и стеганография"

Федосеев В.А.

Самарский университет
Кафедра ГИиИБ

8 сентября 2023 г.

1.1.1. Понятие стеганографии. Классическая стеганография

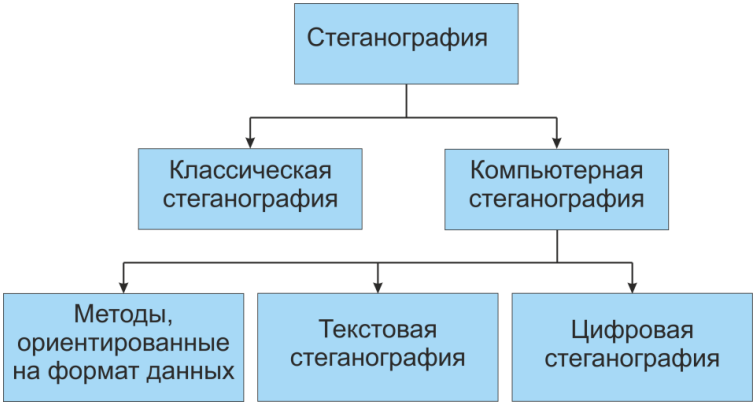
Понятие стеганографии

Стеганография – наука о защищённой передаче информации, осуществляемой путём сокрытия самого факта передачи информации.

В чём отличие от криптографии? Стеганографическая система (стегосистема) – совокупность методов и средств, предназначенных для создания канала защищённой передачи информации, осуществляемой путём сокрытия самого факта передачи информации.

1.1.1. Понятие стеганографии. Классическая стеганография

Основные направления стеганографии



1.1.1. Понятие стеганографии. Классическая стеганография

Примеры классической стеганографии

- Геродот (около 500 лет до н.э.): стеганография с головой раба
- Древний Китай и полоски шёлка
- Симпатические чернила
  - Китайский император Цин Шихуанди (III век до н.э.): Рисовый отвар / Раствор иода
  - Плиний Старший (около 50 г. н.э.): Сок растений
  - Филон Александрийский (I век н.э.): Сок чернильных орешков / Раствор железомедной соли
  - Чёрный передел (XIX век): Медный купорос / Нашатырный спирт
  - Ильич в тюрьме (XIX век): Молоко / Нагрев
- Иоганн Тритемий (около 1500 г.): стеганографический шифр по принципу акростиха

- «Алиса в Зазеркалье» Льюиса Кэрролла

В стихотворении в последней главе автор скрыл реального прототипа главной героини – девочку по имени Алиса Плэзнс Лидделл (Alice Pleasance Liddell)

Ах, какой был яркий день!
Лодка, солнце, блеск и тень,
И везде цвела сирень.
Сестры слушают рассказ,
А река уносит нас.
Плеск волны, сиянье глаз.
Летний день, увы, далёк.
Эхо смолкло. Свет поблёк.
Зимний ветер так жесток.
Но из глубины времён
Светлый возникает сон,
Легкий выплывает чёлн.
И опять я сердцем с ней —
Девочкой ушедших дней,
Давней радостью моей.
Если мир подлунный сам
Лишь во сне явился нам.
Люди, как не верить снам?
Перевод Нины Демуровой

- Подобие акростихов в разведке (т.н. нулевой шифр):

Сообщение, отправленное немецким шпионом в США во время Второй мировой войны

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.

Сообщение, сформированное по вторым буквам каждого слова

Pershing sails from NY June 1.

- Огюст Керкгоффс, 1883:

«Система защиты информации должна обеспечивать свои функции даже при полной информированности противника о её структуре и алгоритмах функционирования. Вся секретность системы защиты передаваемых сведений должна заключаться в секретном ключе, то есть в предварительно (как правило) разделенном между адресатами фрагменте информации».

- Позднее на смену классическим методам пришли методы компьютерной стеганографии.

1.1.2. Компьютерная стеганография и её виды

Компьютерная стеганография

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.

Основные положения современной компьютерной стеганографии:

1. Методы скрытия должны обеспечивать целостность файла
2. Предполагается, что противнику полностью известны возможные стеганографические методы (согласно принципу Керкгоффса)
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

1.1.2. Компьютерная стеганография и её виды

Стеганографические методы, ориентированные на формат данных

К методам, ориентированным на формат данных, будем относить методы, использующие для встраивания информации особенности определённых операционных, файловых систем, форматов файлов, физических носителей и пр.

Примеры:

1. Использование части зарезервированных полей компьютерных форматов файлов для записи данных
2. Скрытие информации в неиспользуемых местах физических носителей
3. Дописывание в остаточные кластеры файловой системы

Основные недостатки:

1. Физическое (на уровне областей памяти) разделение полезной информации и секретного сообщения, приводящее к тому, что последнее может быть легко обнаружено, прочитано или удалено
2. Эти методы не универсальны, а адаптированы под использование конкретных программно-аппаратных средств.

1.1.3. Текстовая стеганография

К текстовой стеганографии относятся методы, в которых встраивание секретной информации осуществляется в содержимое текстового файла.

Примеры:

1. Методы, использующие смещения слов, предложений, абзацев
   1. Один или два пробела между словами
   2. Изменение порядка следования маркеров конца строки CR/LF
   3. Добавление хвостовых пробелов
2. Метод выбора определенных позиций букв (нулевой шифр)
3. Использование символов другого языка, совпадающих по начертанию
4. Использование таблицы синонимов

Основные особенности: все методы достаточно просты, но обладают недостаточной защищённостью, а также низкой пропускной способностью

1.1.4. Цифровая стеганография. Цифровые водяные знаки

Цифровая стеганография и цифровые водяные знаки

В методах цифровой стеганографии встраивание секретного сообщения осуществляется в одномерные или многомерные цифровые сигналы (мультимедиа), имеющие физическую природу.

К таким сигналам мы будем относить цифровые изображения, звуковые файлы и видеофайлы.

Встраиванием ЦВЗ (Digital Watermarking) называется процесс внедрения в цифровой сигнал (как заметного, так и незаметного) информации, имеющей некоторое отношение к этому цифровому сигналу.

Цифровым водяным знаком называется собственно внедряемая информация.

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

1.1.4. Цифровая стеганография. Цифровые водяные знаки

Пример: видимые цифровые водяные знаки

1.1.5. Information Hiding

Понятие Information Hiding

- “Information Hiding” или “Data Hiding”, т.е. буквально *сокрытие информации* - более широкое понятие, покрывающее как методы стеганографии, так и методы встраивания ЦВЗ.
- Основной период развития - 1995 – 2010 гг. (Ingemar Cox, Jessica Fridrich, Mauro Barni, Franco Bartolini, Fabien Petitcolas, Stefan Katzenbeisser, Eric Cole, Birgit Pfitzmann).
- Мы будем использовать термин «встраивание информации» для оригинального “Information Hiding”.
- Под встраиванием информации (в узком смысле) будем понимать область знаний, охватывающую широкий круг проблем внедрения информации (называемой в различных ситуациях секретной информацией, секретным сообщением или цифровым водяным знаком) в содержимое другого информационного объекта (называемого открыто передаваемой информацией или контейнером).

	Сообщение связано с контейнером	Сообщение не связано с контейнером
Факт наличия сообщения сокрыт	Стеганографическое встраивание ЦВЗ (1)	Скрытая (стеганографическая) передача информации (2)
Факт наличия сообщения известен	Нестеганографическое встраивание ЦВЗ (3)	Открытая опосредованная передача информации (4)

Примеры

1. Утечка информации в кабинете министров при Маргарет Тэтчер
2. Скрытая коммуникация в рамках исполнения договора ОСВ-II
3. Яндекс.Карты
4. Сигнал времени в радиоэфире