Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

«Исследование стеганографии и метода LSB»

Выполнил:

студент 3 курса 8 группы

специальности ПОИБМС

Руденя Д.В.

Минск 2020

1. **Теоретические сведения**

Стеганография — способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи (хранения).

В отличие от криптографии, которая скрывает содержимое тайного сообщения, стеганография скрывает сам факт его существования. Как правило, сообщение будет выглядеть как что-либо иное, например, как изображение, статья, список покупок, письмо или судоку. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её.

Преимущество стеганографии над чистой криптографией состоит в том, что сообщения не привлекают к себе внимания. Сообщения, факт шифрования которых не скрыт, вызывают подозрение и могут быть сами по себе уличающими в тех странах, в которых запрещена криптография. Таким образом, криптография защищает содержание сообщения, а стеганография защищает сам факт наличия каких-либо скрытых посланий.

В конце 1990-х годов выделилось несколько направлений стеганографии:

* классическая,
* компьютерная,
* цифровая.

Одним из наиболее распространённых методов классической стеганографии является использование симпатических (невидимых) чернил. Текст, записанный такими чернилами, проявляется только при определённых условиях (нагрев, освещение, химический проявитель и т. д.).

Также существует ряд альтернативных методов сокрытия информации:

* запись на боковой стороне колоды карт, расположенных в условленном порядке;
* запись внутри варёного яйца;
* «жаргонные шифры», где слова имеют другое обусловленное значение;
* трафареты, которые, будучи положенными на текст, оставляют видимыми только значащие буквы;
* геометрическая форма — метод, в котором отправитель старается скрыть ценную информацию, поместив её в сообщение так, чтобы важные слова расположились в нужных местах или в узлах пересечения геометрического рисунка;
* семаграммы — секретные сообщения, в которых в качестве шифра используются различные знаки, за исключением букв и цифр;
* узелки на нитках и т. д.

Компьютерная стеганография — направление классической стеганографии, основанное на особенностях компьютерной платформы. Примеры — стеганографическая файловая система StegFS для Linux, скрытие данных в неиспользуемых областях форматов файлов, подмена символов в названиях файлов, текстовая стеганография и т. д. Приведём некоторые примеры:

* Использование зарезервированных полей компьютерных форматов файлов — суть метода состоит в том, что часть поля расширений, не заполненная информацией о расширении, по умолчанию заполняется нулями. Соответственно мы можем использовать эту «нулевую» часть для записи своих данных. Недостатком этого метода является низкая степень скрытности и малый объём передаваемой информации.
* Метод скрытия информации в неиспользуемых местах гибких дисков — при использовании этого метода информация записывается в неиспользуемые части диска, к примеру, на нулевую дорожку. Недостатки: маленькая производительность, передача небольших по объёму сообщений.
* Метод использования особых свойств полей форматов, которые не отображаются на экране — этот метод основан на специальных «невидимых» полях для получения сносок, указателей. К примеру, написание чёрным шрифтом на чёрном фоне. Недостатки: маленькая производительность, небольшой объём передаваемой информации.
* Использование особенностей файловых систем — при хранении на жёстком диске файл всегда (не считая некоторых ФС, например, ReiserFS) занимает целое число кластеров (минимальных адресуемых объёмов информации). К примеру, в ранее широко используемой файловой системе FAT32 (использовалась в Windows98/Me/2000) стандартный размер кластера — 4 КБ. Соответственно для хранения 1 КБ информации на диске выделяется 4 КБ памяти, из которых 1 КБ нужен для хранения сохраняемого файла, а остальные 3 ни на что не используются — соответственно их можно использовать для хранения информации. Недостаток данного метода: лёгкость обнаружения.

Цифровая стеганография — направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. Но, как правило, данные объекты являются мультимедиа-объектами (изображения, видео, аудио, текстуры 3D-объектов) и внесение искажений, которые находятся ниже порога чувствительности среднестатистического человека, не приводит к заметным изменениям этих объектов. Кроме того, в оцифрованных объектах, изначально имеющих аналоговую природу, всегда присутствует шум квантования; далее, при воспроизведении этих объектов появляется дополнительный аналоговый шум и нелинейные искажения аппаратуры, все это способствует большей незаметности сокрытой информации.

Все алгоритмы встраивания скрытой информации можно разделить на несколько подгрупп:

* работающие с самим цифровым сигналом. Например, метод LSB.
* «впаивание» скрытой информации. В данном случае происходит наложение скрываемого изображения (звука, иногда текста) поверх оригинала. Часто используется для встраивания цифровых водяных знаков (ЦВЗ).
* использование особенностей форматов файлов. Сюда можно отнести запись информации в метаданные или в различные другие не используемые зарезервированные поля файла.

**Метод LSB**

LSB (Least Significant Bit, наименьший значащий бит (НЗБ)) — суть этого метода заключается в замене последних значащих битов в контейнере (изображения, аудио или видеозаписи) на биты скрываемого сообщения. Разница между пустым и заполненным контейнерами должна быть не ощутима для органов восприятия человека.

Суть метода заключается в следующем: допустим, имеется 8-битное изображение в градациях серого. 00h (00000000b) обозначает чёрный цвет, FFh (11111111b) — белый. Всего имеется 256 градаций (28). Также предположим, что сообщение состоит из 1 байта — например, 01101011b. При использовании 2 младших бит в описаниях пикселей, нам потребуется 4 пикселя. Допустим, они чёрного цвета. Тогда пиксели, содержащие скрытое сообщение, будут выглядеть следующим образом: 00000001 00000010 00000010 00000011. Тогда цвет пикселей изменится: первого — на 1/255, второго и третьего — на 2/255 и четвёртого — на 3/255. Такие градации, мало того, что незаметны для человека, могут вообще не отобразиться при использовании низкокачественных устройств вывода.

Методы LSB являются неустойчивыми ко всем видам атак и могут быть использованы только при отсутствии шума в канале передачи данных.

Обнаружение LSB-кодированного стего осуществляется по аномальным характеристикам распределения значений диапазона младших битов отсчётов цифрового сигнала.

Все методы LSB являются, как правило, аддитивными (А17 (Cox), L18D (Lange)).

Другие методы скрытия информации в графических файлах ориентированы на форматы файлов с потерей, к примеру, JPEG. В отличие от LSB, они более устойчивы к геометрическим преобразованиям. Это получается за счёт варьирования в широком диапазоне качества изображения, что приводит к невозможности определения источника изображения.

Для стеганографических систем принято определять необнаруживаемость — вероятность пропуска (то есть отсутствием обнаружения стегосистемы, когда она была представлена для анализа), и вероятность ложного обнаружения (когда стегосистема ложно обнаруживается при её действительном отсутствии). Практические подходы оценки стойкости стегосистем основаны на их устойчивости к обнаружению посредством разработанных к настоящему времени алгоритмов стегоанализа. Все они построены на том, что все алгоритмы встраивания так или иначе вносят в стегограммы искажения относительно использованных контейнеров.

Под атакой на стегосистему понимается попытка обнаружить, извлечь, изменить скрытое стеганографическое сообщение. Такие атаки называются стегоанализом по аналогии с криптоанализом для криптографии. Способность стеганографической системы противостоять атакам называется стеганографической стойкостью.

Многие атаки на стегосистемы аналогичны атакам на криптосистемы:

* атака на основании известного заполненного контейнера;
* атака на основании известного встроенного сообщения;
* атака на основании выбранного встроенного сообщения;
* адаптивная атака на основании выбранного встроенного сообщения (частный случай атаки на основе выбранного скрытого сообщения, когда аналитик имеет возможность выбирать сообщения, исходя из результатов анализа предыдущих контейнеров);
* атака на основании выбранного заполненного контейнера.

Некоторые же не имеют аналогов в криптографии:

* атака на основании известного пустого контейнера;
* атака на основании выбранного пустого контейнера;
* атака на основании известной математической модели контейнера или его части.

Стеганография используется в некоторых современных принтерах. При печати на каждую страницу добавляются маленькие точки, содержащие информацию о времени и дате печати, а также серийный номер принтера.

Из рамок цифровой стеганографии вышло наиболее востребованное легальное направление — встраивание цифровых водяных знаков (ЦВЗ) (watermarking), являющееся основой для систем защиты авторских прав и DRM (Digital rights management) систем. Методы этого направления настроены на встраивание скрытых маркеров, устойчивых к различным преобразованиям контейнера (атакам).

Полухрупкие и хрупкие ЦВЗ используются в качестве аналоговой ЭЦП, обеспечивая хранение информации о передаваемой подписи и попытках нарушения целостности контейнера (канала передачи данных).

1. **Практическая часть**

В данной лабораторной работе необходимо было разработать приложения, которое зашифровывает и расшифровывает тайное сообщение в картинке с помощью метода LSB.

Файл условно можно разбить на 4 части: заголовок файла, заголовок изображения, палитру и само изображение. Для наших целей надо знать только то, что записано в заголовке.

Первые два байта заголовка – это сигнатура BM, далее в двойном слове записан размер файла в байтах, следующие 4 байта зарезервированы и должны содержать нули и, наконец, в ещё одном двойном слове записано смещение от начала файла, до собственно байтов изображения. В 24-битном bmp-файле каждый пиксел кодируются тремя байтами BGR.

Для этого нам и пригодится метод LSB. Суть метода заключается в следующем: мы заменяем младшие биты в байтах, отвечающих за кодирование цвета. Допустим, если очередной байт нашего секретного сообщения – 11001011, а байты в изображении –…11101100 01001110 01111100 0101100111…, то кодирование будет выглядеть так. Мы разобьём байт секретного сообщения на 4 двухбитовые части: 11, 00, 10, 11, и заменим полученными фрагментами младшие биты изображения: …11101111 01001100 01111110 0101100111…. Такая замена в общем случае не заметна человеческому глазу. Более того, многие старые устройства вывода, даже не смогут отобразить такие незначительные перемены.

Понятно, что можно менять не только 2 младших бита, но и любое их количество. Тут есть следующая закономерность: чем большее количество бит мы меняем, тем больший объём информации мы можем спрятать, и тем большие помехи в исходном изображении это вызовет.

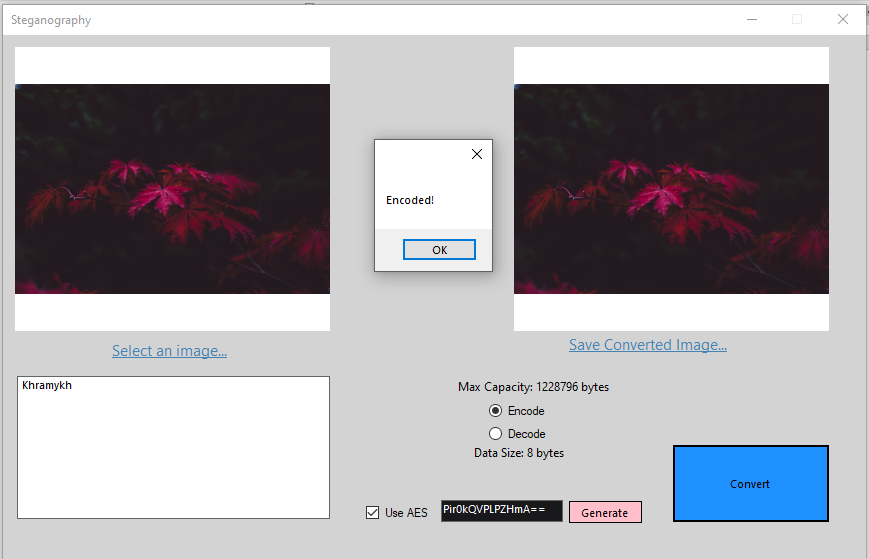


Рисунок 2.1 – получение результата генерации/верификации ЭЦП.

На следующем рисунке показан результат выполнения дешифрования секретного сообщения:

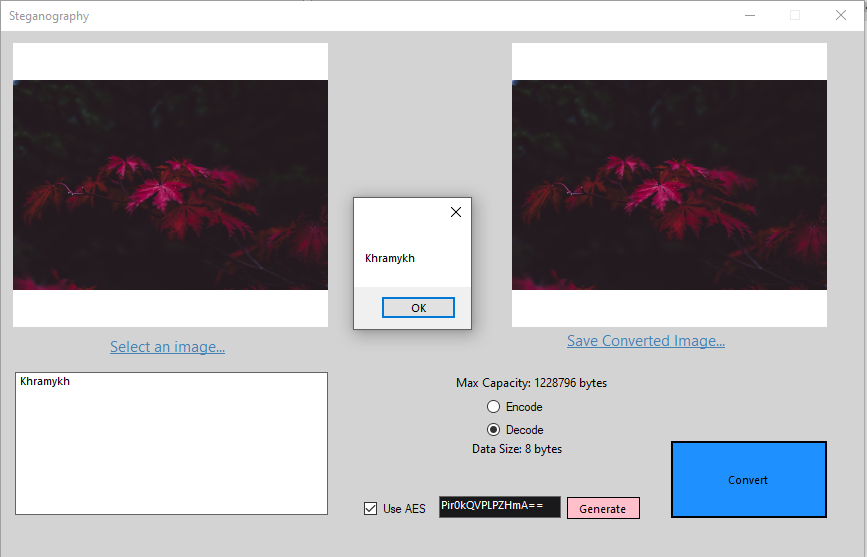


Рисунок 2.2 – получение зашифрованного сообщения

Вывод: в данной лабораторной работе я изучил и приобрел практические навыки разработки и использования приложений для реализации стеганографии и метода LSB.