МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №13 НА ТЕМУ:**

**Исследование стеганографического метода на основе преобразования наименее значащих битов**

Выполнил студент 3 курса 6 группы

Подобед Владислав

Минск 2024

**Цель:** изучение стеганографического метода встраивания / извлечения тайной информации с использованием электронного файла-контейнера на основе преобразования наименее значащих битов (НЗБ), приобретение практических навыков программной реализации данного метода.

**Теоретические сведения**

**Стеганографическая система** – совокупность средств и методов, которые используются для формирования скрытого канала передачи (или хранения) информации. При этом скрытый канал организуется на базе и внутри открытого канала с использованием особенностей восприятия информации. «Скрытость» канала передачи тайной информации отличает стеганографию от криптографии: в первом случае тайной является сам факт наличия канала (передачи информации).

**Основные компоненты стеганосистемы:**

1. **Контейнер** С (файл-контейнер или электронный документ произвольного формата), в котором размещается (осаждается, скрывается) тайное сообщение М; именно контейнер является упомянутым скрытым каналом;

2. **Тайное сообщение** М, осаждаемое в контейнер для передачи или хранения;

3. **Ключи**, или ключевая информация, K системы, выполняющие ту же функцию, что и криптографические ключи; ключей может быть несколько, в соответствии с этим современные стеганосистемы характеризуют как многоключевые: один ключ отождествляется с методом встраивания/извлечения тайной информации, другой – с выбором элементов (например, битов) контейнера для его модификации при осаждении тайной информации, третий – для предварительного (перед встраиванием) преобразования тайной информации;

4. **Контейнер со встроенным сообщением**, или **стеганоконтейнер**, S, который передается по открытому каналу, также являющемуся важным компонентом анализируемой системы; стеганоконтейнер будем именовать также стеганосообщением.

В зависимости от формата документа-контейнера компьютерную стеганографию разделяют на классы:

* Аудиостеганография;
* Видеостеганография;
* Графическая стеганография;
* Текстовая стеганография.

**Метод наименее значимых битов (НЗБ)**

Метод НЗБ основывается на ограниченных способностях зрения или слуха человека, вследствие чего людям тяжело различать незначительные вариации цвета или звука. Например, если в качестве контейнера используется изображение, каждый его пиксель колируется тремя байтами, представляющими цвета RGB-модели. Так как младшие биты этих байтов крайне слабы влияют на итоговый цвет пикселя, в них можно записать скрываемую информацию. Стоит отметить, что в таком случае с вероятность 50% значение исходного бита и бита сообщения могут совпадать, что ещё сильнее сглаживает изменение цвета пикселя. Данный метод может также применяться для видео и аудиофайлов.

**Практическая часть**

Для разработки стеганографического приложения, позволяющего скрывать сообщения в изображениях и аудиофайлах методом НЗБ был использован язык программирования Python с дополнительными модулями Pillow (для работы с изображениями) и wave (для работы с аудиофайлами в формате wav).

Для начала рассмотрим результат скрытия информации в изображении. Исходное изображение представлено на рисунке 1.1.



Рисунок 1.1 – Исходное изображение

Для скрытия был взять транслитерированный отрывок из отчёта по 10 лабораторной работе. Каждый восьмой бит пиксельного канала изображения заменяется на бит сообщения. Изображение со скрытым сообщением представлено на рисунке 1.2. Визуальный анализ показал, что человеческий глаз не может определить различия между пустым контейнером и контейнером с сообщением.



Рисунок 1.2 – Изображение со скрытым сообщением

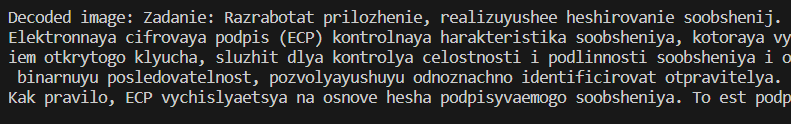


Рисунок 1.3 – Отрывок декодированного сообщения

При скрытии сообщения в аудиофайле (разработанное приложение используется файлы в формате wav), последний разбивается на сегменты по 8 байт. Каждый последний бит сегмента заменяется на бит сообщения. При этом при прослушивании аудиофайла с сообщением слышны высокочастотные шумы. Для просмотра звуковых дорожек контейнеров можно воспользоваться программой Audacity. Звуковые дорожки аудиофайлов представлены на рисунке 1.4.

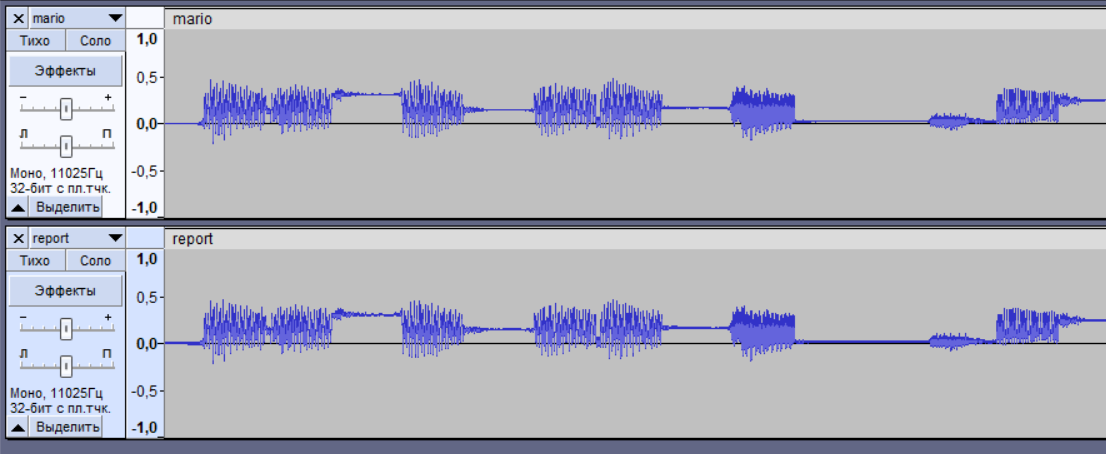


Рисунок 1.4 – Звуковые дорожки контейнеров

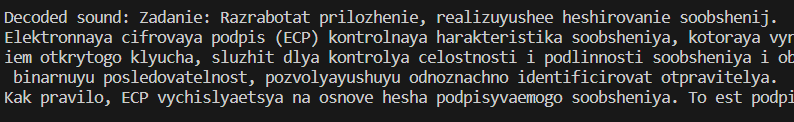


Рисунок 1.5 – Фрагмент декодированного сообщения из аудиофайла

**Вывод:** В ходе лабораторной работы было разработано приложение, позволяющее скрывать сообщения с помощью метода преобразования наименее значащих битов в изображениях и аудиофайлах.