МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №14 НА ТЕМУ:**

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

Выполнила студентка 3 курса 4 группы

Решетилова Антонина

Минск 2023

**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

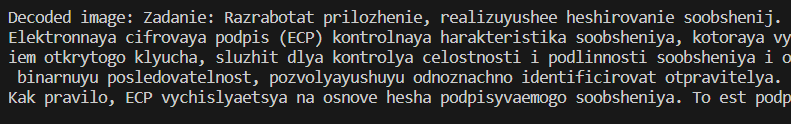


Рисунок 1.3 – Отрывок декодированного сообщения

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.

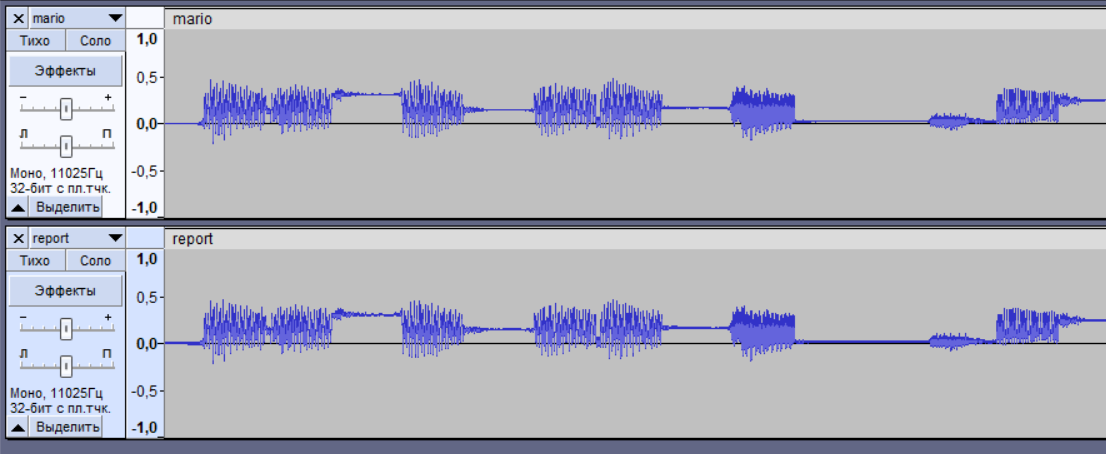


Рисунок 1.4 – Звуковые дорожки контейнеров

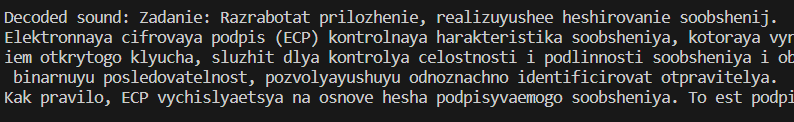


Рисунок 1.5 – Фрагмент декодированного сообщения из аудиофайла

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

**Контрольные вопросы:**

**1. Охарактеризовать цели, задачи и области применения стеганографии.**

Целью стеганографии являетсясокрытие самого факта существования секретного сообщения. Задача стеганографии – это разработка методов скрытой передачи информации, обеспечивающих сохранность передаваемой информации и ее невидимость для посторонних. Область применения стеганографии – это информационная безопасность и криптография, когда скрытая информация может быть использована для хранения секретных данных, обеспечения безопасности сети или транспортировки сообщений в условиях, когда прямая передача информации затруднена или нежелательна.

**2. В чем состоят сходства и различия между стеганографией и криптографией.**

Целью криптографии является преобразование информации в такой вид, при котором её сложно прочитать, не имея ключевой информации и понимания работы криптографического алгоритма. Целью же стеганографии является сокрытие факта передачи информации.

**3. Дать определение стеганографической системы. Охарактеризовать составные части стеганосистемы и их взаимосвязь?**

**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.

**4.** **Основные классификационные критерии методов стеганографии.**

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

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

**5. Пояснить сущность основных атак на стеганосистемы?**

1. Атака по известному заполненному контейнеру: злоумышленник знает, какой файл используется в качестве контейнера и пытается извлечь скрытую информацию без знания ключа.

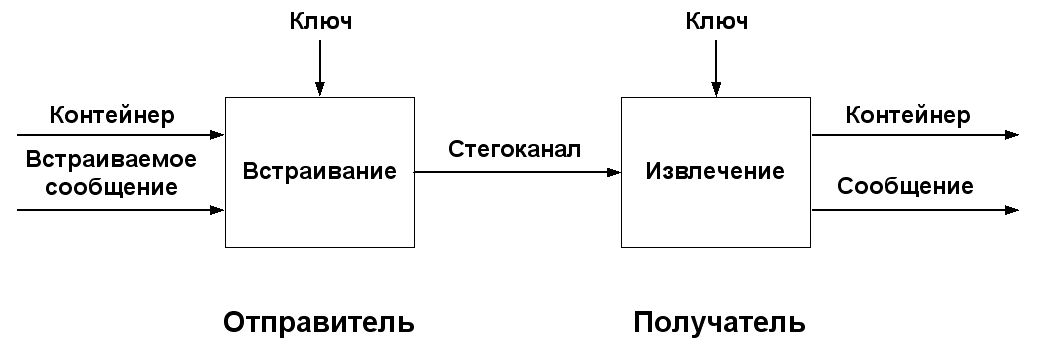
2. Атака на основе выбранного заполненного контейнера: злоумышленник выбирает заполненный контейнер и пытается извлечь скрытую информацию без знания ключа.

3. Атака на основе известного пустого контейнера: злоумышленник знает, что контейнер пуст, и пытается найти скрытую информацию, если она есть.

4. Атака на основе выбранного пустого контейнера: злоумышленник выбирает пустой контейнер и пытается встроить в него скрытое сообщение.

5. Атака по известной математической модели контейнера: злоумышленник знает, как устроена математическая модель контейнера, и пытается использовать эту информацию для извлечения скрытой информации.

**6. Изобразить структурную схему стеганографической системы.**



**7. Сущность метода НЗБ. Области его применении?**

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. Области применения НЗБ включают защиту авторских прав, защиту информации, восстановление информации, хранение метаданных и тд.

**8. Изобразить алгоритмы встраивания и извлечения сообщений на основе метода НЗБ при передаче этих сообщений.**

Алгоритм встраивания:

1. Перевести сообщение в бинарный вид;

2. Перевести контейнер в бинарный вид и разбить его на сегменты по n бит;

3. Заменять младшие биты каждого сегмента битами сообщения, пока сообщение не закончится. Заменять можно от 1 до n-1 младших бит сегмента;

4. Перевести бинарный вид контейнера к изначальному формату.

Алгоритм извлечения:

1. Перевести контейнер в бинарный вид и разбить его на сегменты по n бит;

2. Извлечь из каждого сегмента от 1 до n-1 младших бит (число извлекаемых является заранее известным);

3. Сконкатенировать извлечённые биты;

4. Привести полученную бинарную последовательность к изначальному формату сообщения.