

Внимание:

1. Этого листа в вашем отчет быть не должно (удалить).
2. Оформляем в соответствии с **СТО Самарского университета**
3. Если у вас есть приложения, то так оформляем как требует стандарт.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение высшего образования
«Самарский национальный исследовательский университет имени академика С.П. Королева»
(Самарский университет)

Институт информатики и кибернетики
Кафедра геоинформатики и информационной безопасности

ОТЧЕТ ПО ПРАКТИКЕ

Вид практики: учебная
(учебная, производственная)

Тип практики: Экспериментально-исследовательская практика

Сроки прохождения практики: с 01.07.2024 г. по 13.07.2024 г.
по направлению подготовки 10.05.03 Информационная безопасность
автоматизированных систем
(уровень академического специалитета)
направленность (профиль) «Безопасность открытых информационных систем»

Обучающийся группы	<u>№ 6313-100503D Ле Лок Тхо</u>
Руководитель практики от университета	<u>профессор, д.т.н. Сергеев В.В.</u>

Дата сдачи 13.07.2024 г.
Дата защиты 13.07.2024 г.

Оценка _____

Самара 2024

СОДЕРЖАНИЕ

ОТЧЕТ ПО ПРАКТИКЕ	2
Планируемые результаты освоения образовательной программы (компетенции)	4
Выполнение определенных видов работ, связанных с будущей профессиональной деятельностью (сбор и анализ данных и материалов, проведение исследований)	4
Результаты практики	4
ВЫПОЛНЕНИЕ ЗАДАНИЯ.....	7
1. Теоретические основы встраивания информации	7
1.1. Введение в стеганографию и цифровые водяные знаки	7
1.2. Методы стегоанализа	9
1.3. Методы встраивания скрытой информации в контейнер	10
1.4. Метод встраивания в наименее значимую битовую плоскость (Least Significant Bit, НЗБ, LSB)	11
2. Описание программной реализации	17
2.1. Модуль «process.py»	17
2.2. Модуль «lsb_embedding.py»	17
2.3. Модуль «extraction.py»	18
2.4. Модуль «analysis.py»	18
3. Результаты реализации программы	19
ЗАКЛЮЧЕНИЕ	22
ОТЗЫВ О ПРОХОЖДЕНИИ ПРАКТИКИ.....	23

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение высшего образования
«Самарский национальный исследовательский университет имени академика С.П. Королева»
(Самарский университет)

Институт информатики и кибернетики
Кафедра геоинформатики и информационной безопасности

Индивидуальное задание на практику

Студенту группы № 6313-100503D Ле Лок Тхо

Направление на практику оформлено приказом по университету от 348 от 28.06.24 г. на кафедру геоинформатики и информационной безопасности Самарского университета

(наименование профильной организации или структурного подразделения университета)

Планируемые результаты освоения образовательной программы (компетенции)	Выполнение определенных видов работ, связанных с будущей профессиональной деятельностью (сбор и анализ данных и материалов, проведение исследований)	Результаты практики
ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	Ознакомиться с техникой сокрытия информации «Стеганография» и методами сокрытия.
ОПК-2	Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности	Работы включал разработку и внедрение программного обеспечения для обработки аудиофайлов, где были использованы Python-библиотеки для работы с аудиоданными и математическими расчетами.
ОПК-3	Способен использовать математические методы, необходимые для решения задач профессиональной деятельности	Использовался метод наименьших значащих битов (LSB) для встраивания секретных данных в аудиофайлы, требующий применения операций побитового И (AND) и исключающего ИЛИ (XOR). Для анализа изменений были построены и сравнены гистограммы аудиосэмплов, что позволило оценить влияние модификаций на качество аудио.
ОПК-4	Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	Исследовались методы скрытого встраивания данных, включая изменения на уровне цифровых аудиосэмплов, что потребовало понимания свойств сигналов и их взаимодействий. Основные физические законы и модели использовались для оценки и минимизации искажений аудиосигналов при встраивании данных.

ОПК-9	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	Задачи по встраиванию и извлечению данных из аудиофайлов с учетом современных тенденций развития информационных технологий и средств технической защиты информации. Использовались передовые методы обработки цифровых сигналов и стеганографии для безопасной передачи информации.
ОПК-14	Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	Проводилась разработка и внедрение автоматизированной системы для встраивания и извлечения данных из аудиофайлов с использованием методов стеганографии. Работа включала подготовку исходных данных и анализ требований по защите информации, что позволило разработать систему, обеспечивающую высокий уровень безопасности.
ОПК-15	Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	Выполнены задачи по администрированию и контролю функционирования системы стеганографии для защиты информации в аудиофайлах.
ОПК-16	Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма	Во время практики был выполнен анализ исторического развития технологий защиты информации в России и их влияния на современные методы обеспечения безопасности данных. Изучение эволюции отечественных систем защиты информации позволило лучше понять текущие тенденции и разработать более эффективные методы стеганографии, учитывая исторический контекст и достижения российской науки и техники.

Срок предоставления на кафедру отчета о практике:

13.07.2024 г.

Руководитель практики от
университета, д.т.н., профессор

В.В.Сергеев

(подпись)

Руководитель практики
от профильной организации

А.И. Максимов

(подпись)

Задание принял к исполнению
обучающийся группы № 6313-
100503D

Ле Лок Тхо

(подпись)

О Т Ч Е Т

о выполнении индивидуального задания
по экспериментально-исследовательской практике

ВВЕДЕНИЕ

Цель: исследование «Стеганографии», реализация программного обеспечения для встраивания и извлечения цифровых водяных знаков с использованием метода встраивания наименее значимой битовой плоскости.

При прохождении практики, руководителем были поставлены следующие задачи:

- Изучение предметной области практики
- Реализация модуля встраивания и извлечения цифрового водяного знака
- Реализация модуля визуализация гистограмм

Задания необходимо было выполнять последовательно в течение всего времени практики, предоставляя руководителю промежуточные отчеты.

ВЫПОЛНЕНИЕ ЗАДАНИЯ

1. Теоретические основы встраивания информации

1.1. Введение в стеганографию и цифровые водяные знаки

Термин «стеганография» происходит от греческих слов «στεγανός» («скрытый») и «γράφω» («пишу»).

Стеганография – это способ скрытия информации внутри другой информации или физического объекта так, чтобы она была не обнаружена. С использованием техники стеганографии можно скрыть практически любой цифровой контент, включая текстовые файлы, изображения, аудио и видео. И когда скрытая информация доходит до получателя, она может быть извлечена

Стеганографию иногда сравнивают с криптографией, так как обе являются методами секретной коммуникации. Однако между ними есть разница, так как в случае со стеганографией данные не шифруются при отправке и для их получения не требуется ключ дешифрования.

Основные направления стеганографии:



Цифровой водяной знак (ЦВЗ) - это технология для предотвращения похищения или использования цифровых изображений, аудио и видео без разрешения владельца. ЦВЗ представляет собой внедрение цифровой подписи в данные. Существует два класса цифровых водяных знаков - видимые и невидимые.

Видимый водяной знак лучше всего использовать для данных, зрительный образ которых не портится при добавлении цифровой подписи. Преимуществом таких водяных знаков является то, что данные защищены авторским правом и их полноценное использование становится невозможным без удаления цифрового водяного знака. Подобные меры защиты значительно упрощают споры по авторскому праву, поскольку наличие или факт удаления водяных знаков можно легко обнаружить.

Невидимый водяной знак используется, когда внешний вид данных не может быть изменен. Невидимый ЦВЗ – это специальная метка, встраиваемая в цифровой контент, называемый контейнером, с целью защиты авторских прав и подтверждения целостности документа. Преимущество такого типа водяных знаков состоит в том, что их нельзя легко обнаружить. Потенциальные нарушители могут использовать данные, не подозревая, что они содержат маркировку владельца.

В настоящее время при формировании ЦВЗ применяется принцип встраивания метки, которая представляет собой узкополосный сигнал, в широком диапазоне частот маркируемого изображения. Этот метод реализуется посредством двух различных алгоритмов. В одном алгоритме информация передается посредством фазовой модуляции «несущей», представляющей собой псевдослучайную последовательность чисел. В другом – весь диапазон частот делится на несколько субдиапазонов и передача производится между этими субдиапазонами. В отношении маркируемого изображения метку можно рассматривать как некоторый дополнительный шум. Но так как в изображении всегда присутствует шум, то его незначительное возрастание за счет добавления

метки не приводит к заметному для зрения увеличению искажений. Кроме того, сигнал, представляющий метку, распространяется по всему изображению, благодаря чему достигается устойчивость к обрезке изображения. Параллельный алгоритм обучения нейронной сети с машиной опорных векторов в качестве выходного слоя позволяет автоматизировать процедуру формирования тренировочных наборов при создании систем распознавания изображений.

Важнейшее применение ЦВЗ нашли в системах защиты от копирования, которые стремятся предотвратить или удержать от несанкционированного копирования цифровых данных. Применяют ЦВЗ в стеганографии (способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи или хранения), когда стороны обмениваются секретными сообщениями, внедрёнными в цифровой сигнал. Используется как средство защиты документов с фотографиями — паспортов, водительских удостоверений, кредитных карт с фотографиями. Хотя некоторые форматы цифровых данных могут также нести в себе дополнительную информацию, называемую метаданными, ЦВЗ отличаются тем, что информация «зашифрована» прямо в сигнал. Объекты мультимедиа в этом случае будут представлять собой контейнеры (носители) данных. Основное преимущество состоит в наличии условной зависимости между событием подмены объекта идентификации и наличии элемента защиты — скрытого водяного знака. Подмена объекта идентификации приведёт к выводу о подделке всего документа.

1.2. Методы стегоанализа

Статистический анализ:

- Гистограммы: Анализ распределения цветовых значений или значений аудиосигналов для выявления аномалий
- Анализ частотного спектра: Выявление изменений в частотных компонентах аудиофайлов или изображений, которые могут указывать на скрытую информацию.

Анализ наименее значимых битов (LSB):

- Chi-квадрат тест (χ^2 -тест): Проверка равномерности распределения значений LSB для выявления аномалий.
- Анализ последовательностей битов: Поиск неестественных последовательностей в наименее значимых битах.

Методы на основе машинного обучения:

- Классификация: Обучение моделей для распознавания изображений или аудио с встраиванием и без встраивания скрытой информации.
- Кластеризация: Группировка медиафайлов на основе схожих характеристик, чтобы выявить потенциальные аномалии.

Анализ визуальных артефактов:

- Сравнительный анализ: Сравнение оригинальных и подозреваемых файлов на наличие визуальных артефактов, вызванных встраиванием.
- Анализ остаточных сигналов: Выявление следов, оставленных стеганографическими алгоритмами.

Анализ метаданных:

- Изучение заголовков и метаданных файлов: Поиск нестандартных или необычных записей, которые могут указывать на наличие скрытой информации.

Методы на основе измененной корреляции:

- Проверка корреляции пикселей: Анализ корреляции между соседними пикселями для выявления нарушений, вызванных встраиванием данных.

1.3. Методы встраивания скрытой информации в контейнер

Метод наименее значимого бита (LSB): 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.

Спектральное встраивание: Изменение спектральных компонентов аудио или видео сигналов. Например, модификация коэффициентов дискретного косинусного преобразования (DCT) в изображениях JPEG.

Метод маскировки и фильтрации: Используется в аудиостеганографии, где скрытая информация добавляется к аудиофайлу на частотах, которые меньше всего воспринимаются человеческим ухом.

Разрезание и смешивание: Разделение скрываемой информации на части и встраивание их в различные участки контейнера.

Стеганография на основе разности: Изменение разности между парами пикселей или аудиосэмплов таким образом, чтобы внедрить скрытую информацию.

Форматно-специфическое встраивание: Использование особенностей конкретных форматов данных, например, заголовков файлов или метаданных для скрытия информации.

1.4. Метод встраивания в наименее значимую битовую плоскость (Least Significant Bit, НЗБ, LSB)

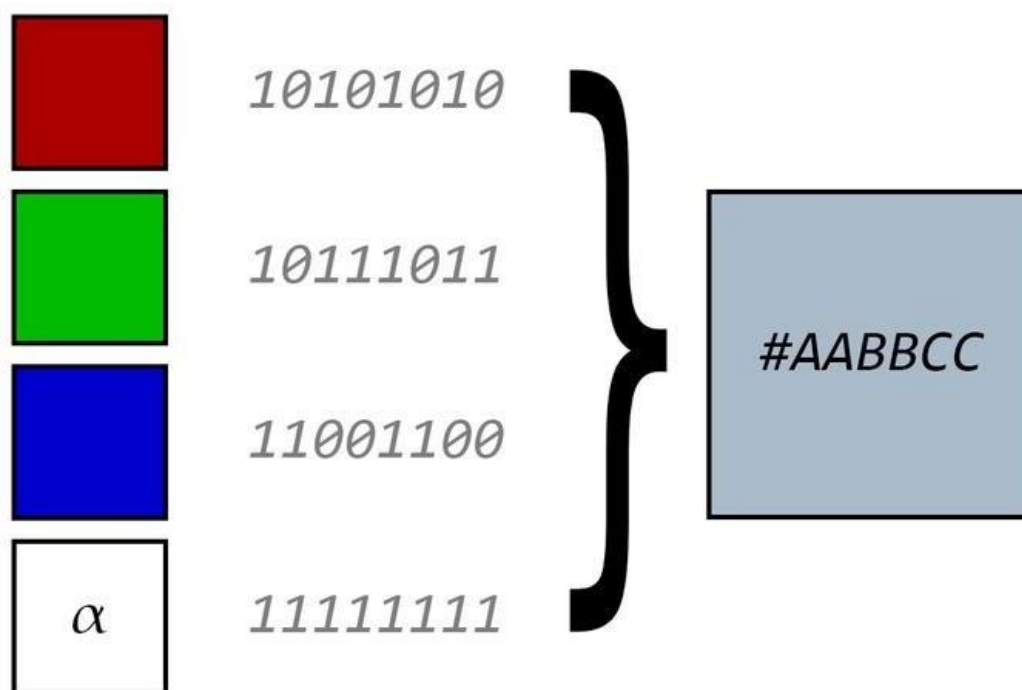
Метод LSB (англ. Least Significant Bit — Наименее значимый бит) относится к пространственным методам цифровой стеганографии в изображениях. То есть, в рамках данного метода мы будем «прятать» информацию в каждом пикселе или группе пикселей какого-либо изображения, изменяя при этом младший бит каждого цветового канала.

Данный метод заключается в выделении наименее значимых бит изображения- контейнера с последующей их заменой на биты сообщения. Поскольку замене подвергаются лишь наименее значимые биты, разница между исходным изображением- контейнером и контейнером, содержащим скрытые данные невелика и обычно незаметна для человеческого глаза.

Метод LSB применим лишь к изображениям в форматах без сжатия или со сжатием без потерь, так как для хранения скрытого сообщения используются наименее значимые биты значений пикселей, при сжатии с потерями эта информация может быть утеряна.

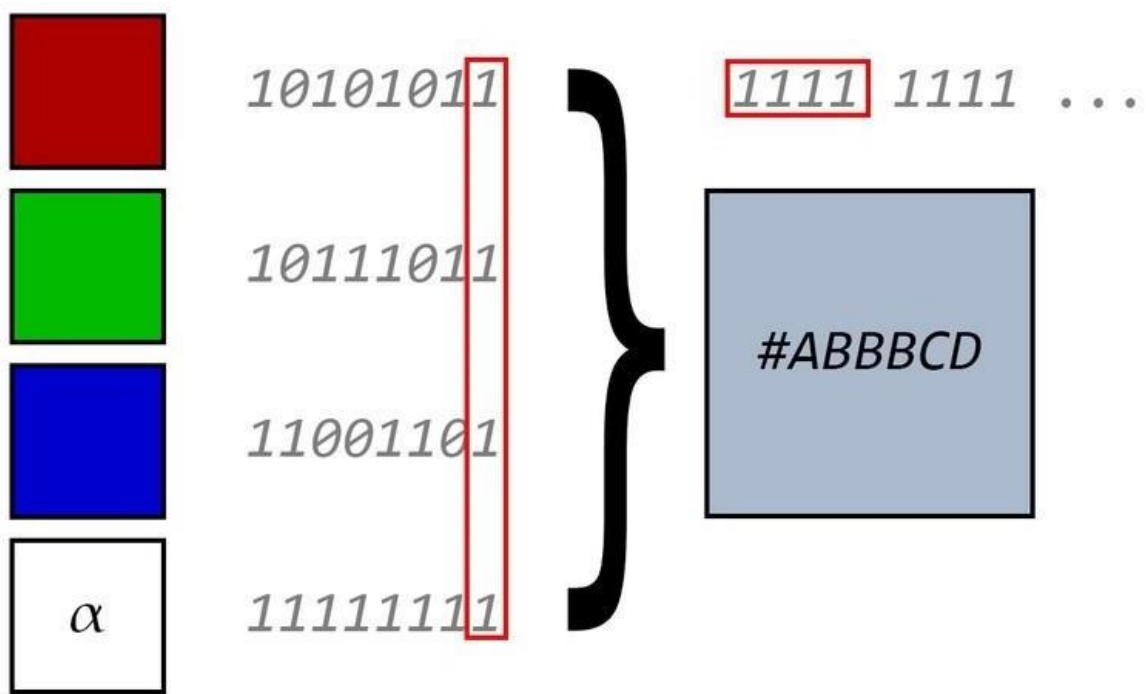
Встраивание

Как известно, в цифровом изображении каждый цвет кодируется при помощи нескольких основополагающих цветов, иногда с использованием дополнительных каналов. В зависимости от конечного применения это могут быть модели RGB (красный, зеленый, синий), RGBA (красный, зеленый, синий, альфа-канал) или, например, CMYK (циан, маджента, желтый, черный). Каждый цвет можно представить в виде последовательности чисел, где для каждого канала-цвета определено свое числовое значение.



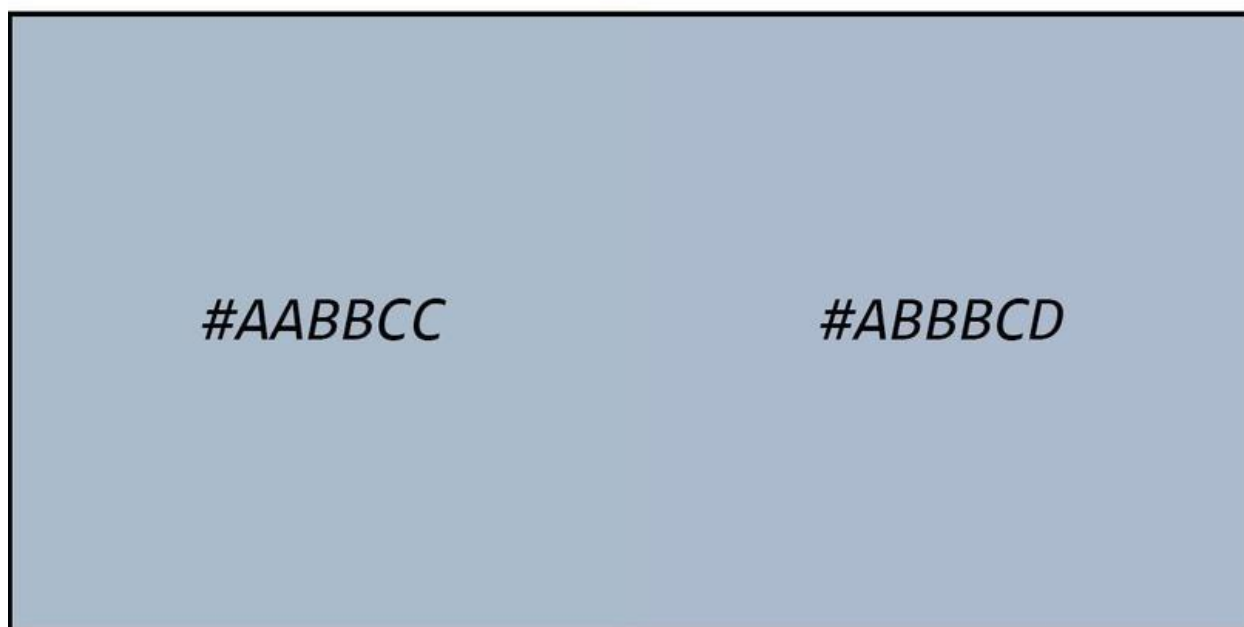
Кодирование одного цвета в формате RGBA (8 бит).

Для «упаковки» секретного сообщения в пиксели изображения необходима некоторая подготовка: сообщение преобразуется в битовую цепочку и делится «порциями» по n бит, где n — количество каналов, кодирующих итоговое изображение. Например, при «упаковке» сообщения в кодировке UTF-8 в изображение вида RGBA для записи одного символа текста понадобится 2 пикселя (т.к. 1 символ «весит» 1 байт, а цветовых канала мы имеем 4).



«Упаковка» сообщения в пиксель в формате RGBA (8 бит).

Вполне очевидно, что при таком незначительном изменении цветов отличить один пиксель от другого «на глаз» не представляется возможным.



Видите разницу? А она есть!

Поскольку крайне редко секретное сообщение имеет тот размер, который идеально вписывается в изображение, то нам необходимо записать некоторый «шум» в неиспользованные пиксели. В качестве «шума» подойдет любая цепочка бит, например, можно повторно записать секретное сообщение.

Извлечение

Для извлечения секретного сообщения следует знать следующие данные:

- Количество младших бит, используемых для «упаковки» сообщения.
- Исходная кодировка сообщения.
- Порядок кодирования бит сообщения по каналам (если каналов больше одного).
- Порядок кодирования пикселей (например, слева направо, сверху вниз).
- Длина сообщения либо любая последовательность, указывающая на конец сообщения (для предотвращения попытки извлечь данные из случайного шума).

Само извлечение происходит следующим образом:

1. Из каждого цветового канала каждого пикселя извлекается значение младших бит и склеивается в одну цепочку.
2. Цепочка бит декодируется в сообщение при помощи используемой отправителем сообщения кодировки.
3. В случае, если имеются данные о длине сообщения, то извлечение заканчивается в момент получения сообщения известной длины. Если же для указания окончания используется парольная фраза, то извлечение заканчивается в тот момент, когда последние n символов извлеченного сообщения соответствуют парольной фразе.

НЗБ для аудио

Метод встраивания в наименее значимую битовую плоскость (Least Significant Bit, НЗБ, LSB) для внедрения информации в аудио заключается в

замене наименее значимых битов в сэмплах аудиосигнала на биты скрываемого сообщения. Этот метод широко используется из-за своей простоты и способности скрывать значительные объемы данных без заметного изменения исходного аудиофайла. Существует несколько вариаций алгоритма НЗБ, которые можно реализовать для улучшения устойчивости и скрытности встраиваемых данных.

Основные этапы метода LSB для аудио

1. Преобразование аудиосигнала:

- Аудиосигнал сначала преобразуется в цифровую форму, если он еще не находится в этом формате. Цифровой аудиосигнал состоит из последовательности сэмплов, каждый из которых представляет амплитуду звука в определенный момент времени.

2. Методы замены битов:

- *Непосредственная замена битовой плоскости контейнера битами цифрового водяного знака:* В этом методе наименее значимые биты каждого сэмпла заменяются битами скрываемого сообщения. Например, если сэмпл состоит из 16 бит, то изменения происходят в последнем бите каждого сэмпла.

- *Побитовое сложение битовой плоскости контейнера и битов цифрового знака:* В этом методе выполняется операция побитового сложения (XOR) между наименее значимыми битами сэмплов и битами скрываемого сообщения. Это позволяет скрыть информацию таким образом, что для её извлечения необходимо знать исходное состояние битов контейнера.

- *Отрицание побитового сложения битовой плоскости контейнера и битов цифрового знака:* В этом методе выполняется операция побитового сложения (XOR) между наименее значимыми битами сэмплов и битами скрываемого сообщения, а затем результат инвертируется. Этот метод добавляет дополнительный уровень сложности для потенциальных злоумышленников, пытающихся извлечь скрытую информацию.

3. Сохранение изменений:

- После применения одного из методов замены битов аудиофайл сохраняется в новом формате, содержащем скрытую информацию. Изменения в амплитуде звука, вызванные заменой наименее значимых битов, настолько малы, что человеческое ухо обычно не способно их заметить.

Преимущества метода LSB для аудио

1. Незаметность:

- Человеческое ухо обычно не может различить изменения в наименее значимых битах, что делает метод LSB особенно эффективным для скрытия информации в аудио.

2. Простота:

- Метод LSB прост в реализации и не требует сложных вычислений или алгоритмов, что делает его доступным для широкого использования.

3. Емкость:

- В аудиофайлах можно скрывать значительные объемы информации, поскольку каждый сэмпл содержит наименее значимый бит, который можно заменить.

Недостатки метода LSB для аудио

1. Чувствительность к искажениям:

- Метод LSB чувствителен к различным видам обработки аудиофайлов, таким как сжатие или фильтрация, что может привести к потере скрытой информации.

2. Низкая стойкость:

- Поскольку метод LSB заменяет наименее значимые биты, скрытая информация может быть легко обнаружена и изменена, если злоумышленник знает о её наличии.

Метод встраивания в наименее значимую битовую плоскость (LSB) является мощным инструментом для скрытия информации в аудиофайлах благодаря своей простоте и эффективности. Тем не менее, его чувствительность к

искажениям требует тщательного подхода к использованию и защите скрытой информации.

2. Описание программной реализации

2.1. Модуль «process.py»

Модуль «process.py» предназначен для работы с аудиофайлами в формате WAV. В нем реализованы функции для преобразования стерео аудиофайлов в моно и для чтения аудиоданных из файла. Ниже приведено описание каждой функции, включая их параметры и назначение.

Импортируемые библиотеки

- wave: Стандартная библиотека Python для работы с аудиофайлами в формате WAV.
- numpy: Библиотека для работы с массивами и числовыми данными.
- logging: Библиотека для ведения логов.
- typing: Библиотека для типизации данных.

Функции модуля

1. *convert_to_mono(input_file: str, output_file: str) -> None*

Эта функция преобразует стерео аудиофайл в моно. Она считывает стерео данные, усредняет левый и правый каналы, и сохраняет результат в новый моно файл.

2. *read_audio(file: str) -> Optional[Tuple[np.ndarray, wave._wave_params]]*

Эта функция считывает аудиоданные из файла WAV и возвращает их в виде массива numpy, а также параметры WAV файла.

2.2. Модуль «lsb_embedding.py»

Модуль «lsb_embedding.py» предназначен для встраивания секретной информации в аудиофайлы с использованием метода наименее значимого бита (LSB). В модуле реализованы функции для чтения аудиоданных, генерации секретных битов, внедрения этих битов в аудиоданные и сохранения модифицированного аудиофайла. Также реализован класс EmbeddingLSB,

который управляет всем процессом встраивания. Ниже приведено подробное описание каждой части модуля.

Класс «EmbeddingLSB» - Этот класс отвечает за весь процесс встраивания секретных битов в аудиофайл.

Методы класса

1. *generate_secret_bits*: Генерирует случайную последовательность битов на основе секретного ключа.

2. *get_embedding_function*: Возвращает функцию для встраивания битов в зависимости от выбранного алгоритма.

3. *embed_bits*: Встраивает секретные биты в аудиоданные.

4. *save_audio*: Сохраняет модифицированные аудиоданные в новый файл.

2.3. Модуль «*extraction.py*»

Модуль «*extraction.py*» предназначен для извлечения скрытых битов информации из аудиофайлов, в которых была применена техника наименее значимого бита (LSB). В модуле реализован класс ExtractorLSB, который управляет процессом извлечения из ранее аудиофайла встраивания. Ниже приведено подробное описание каждой части модуля.

Класс «ExtractorLSB» - Этот класс отвечает за извлечение скрытых битов из аудиофайлов.

Методы класса

1. *extract_lsb*: Извлекает скрытые биты из аудиоданных в зависимости от выбранного метода.

2. *extract_watermark*: Вспомогательный метод, проверяющий наличие аудиоданных и вызывающий метод *extract_lsb*.

2.4. Модуль «*analysis.py*»

Модуль «*analysis.py*» предназначен для анализа и визуализации изменений в аудиофайлах, которые подверглись стеганографическому встраиванию информации с использованием различных методов на основе наименее значимого бита (LSB). Этот модуль включает функции для построения гистограмм

аудиосэмплов и сравнения гистограмм оригинального и модифицированных аудиофайлов.

Функции модуля

1. plot_histogram(file: str, ax: plt.Axes, title: str) -> None

Эта функция преобразует стерео аудиофайл в моно. Она считывает стерео данные, усредняет левый и правый каналы, и сохраняет результат в новый моно файл. Считывает аудиосэмплы из файла и строит их гистограмму на заданной оси. Если не удастся прочитать файл, выводит сообщение об ошибке.

2. compare_histograms(original_file: str, stego_files: List[str], stego_titles: List[str]) -> None

Сравнивает гистограммы оригинального аудиофайла и нескольких модифицированных аудиофайлов. Создает подграфики для оригинального и каждого модифицированного аудиофайла, строит их гистограммы и отображает их.

3. plot_histogram_difference(original_hist: np.ndarray, stego_hist: np.ndarray, bins: np.ndarray, ax: plt.Axes, title: str) -> None



Строит разницу между гистограммами оригинального и модифицированного аудиофайлов. Вычисляет разницу между гистограммами и строит график этой разницы.

4. compare_histogram_differences(original_file: str, stego_files: List[str], stego_titles: List[str]) -> None

Сравнивает разницы гистограмм между оригинальным аудиофайлом и несколькими модифицированными аудиофайлами. Создает подграфики для каждой разницы гистограмм и отображает их.

3. Результаты реализации программы




При получении входного аудиофайла «input_audio.wav» через функцию *convert_to_mono*, он будет преобразован в моно аудиофайл и сохранен аудиофайл после преобразования с именем «mono_audio.wav».

 input_audio	05.07.2024 15:40	WAV File
 mono_audio	08.07.2024 16:21	WAV File

Теперь вся последующая работа будет производиться в аудиофайле «mono_audio.wav».

Через модуль «lsb_embedding.py» для встраивания секретной информации в файл «mono_audio.wav», в частности, секретная информация представляет собой строку битов, автоматически генерируемую методом *generate_secret_bits*.

Затем методом НЗБ с 3-мя алгоритмами изменения битов: "replace", "XOR" и "Negative XOR" получаем 3 новых аудиофайла и сохраняем их с соответствующими именами "output_replace.wav", "output_xor.wav" и "output_negate_xor.wav"

 output_negate_xor	08.07.2024 16:44	WAV File
 output_replace	08.07.2024 16:44	WAV File
 output_xor	08.07.2024 16:44	WAV File

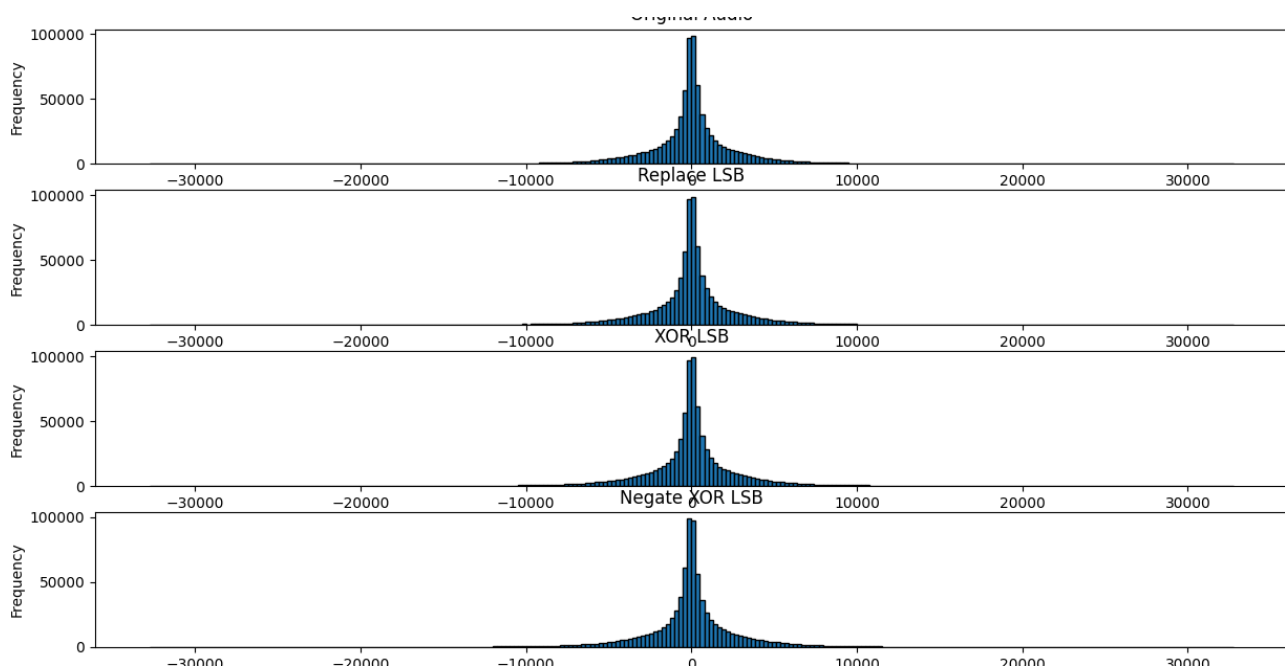
Через модуль «extraction.py» извлечь секретную информацию из файла «output_replace.wav», "output_xor.wav", "output_negate_xor.wav" и вывести строку секретных битов на экран. В частности, секретная информация — это битовая строка, автоматически создаваемая методом *gener_secret_bits* в модуле «lsb_embedding.py».

```

extraction x
"C:\Users\ASUS_ZENBOOK\PycharmProjects\practice2024\venv\Scripts\python.exe" "C:/Users/ASUS_ZENBOOK/PycharmProjects/practice2024/extraction.py"
Extracted watermark (replace): 10101011101111001000011000010101000100100001011101100001010011111100111001111110101
Extracted watermark (xor): 10101011101111001000011000010101000100100001011101100001010011111100111001111110101
Extracted watermark (negate_xor): 10101011101111001000011000010101000100100001011101100001010011111100111001111110101
Process finished with exit code 0

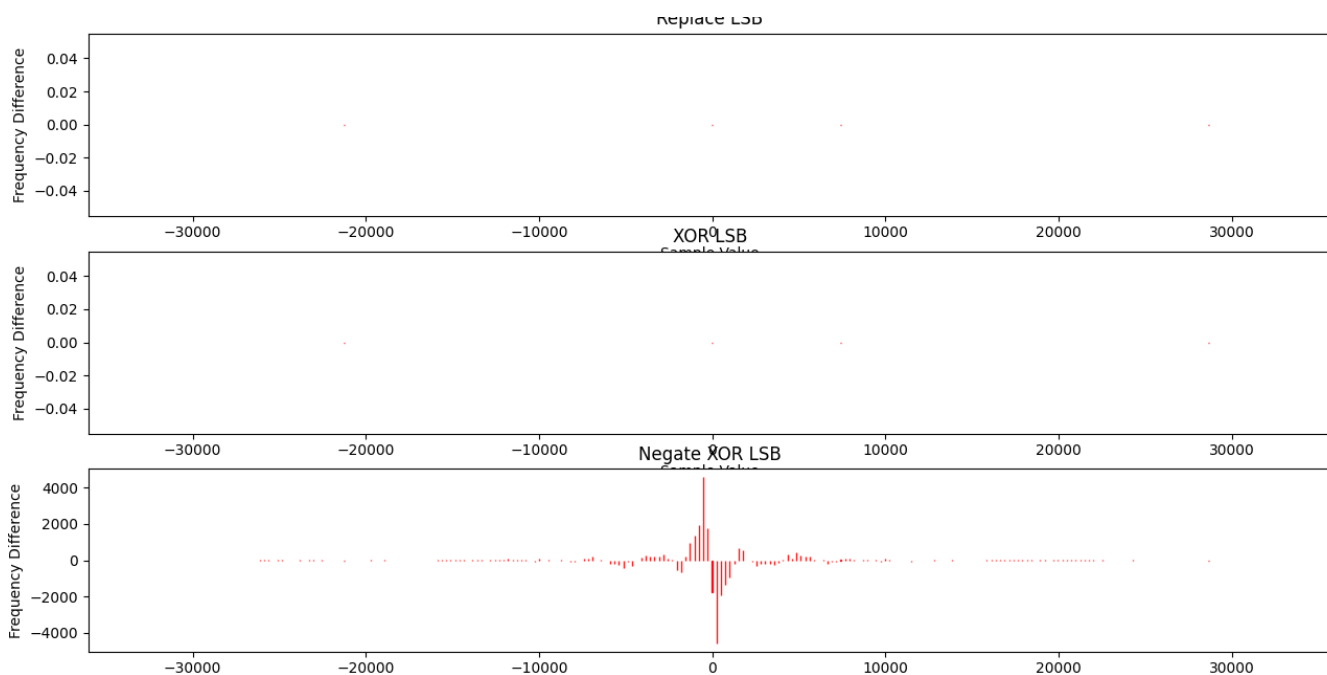
```

Выполнять анализ изменений в исходном файле и файлах после внедрения информации через модуль «analysis.py». Там программа рисует графики частоты исходного аудиофайла и аудиофайла после встраивания.



Из диаграммы видно, что между исходными аудиофайлами и аудиофайлами после встраивания особых изменений нет, поскольку метод НЗБ не меняет слишком много исходных файлов.

Чтобы увидеть изменение, программа вычитала каждую соответствующую звуковую диаграммы битовых изменений из исходной звуковой диаграммы. И получите следующий результат.



В методах изменения битов «replace» и «XOR» изменений не так уж много, но в методе «Negative_XOR» изменения в диаграмме заметны.

ЗАКЛЮЧЕНИЕ

В течение практики по получению профессиональных умений и опыта профессиональной деятельности были успешно выполнены поставленные задачи: проанализированы Стеганография в сфере информационной безопасности. Узнайте больше о методах сокрытия информации с помощью встраивания информации, особенно метод встраивания в наименее значимую битовую плоскость (НЗБ), о том, как развертывать алгоритмы и анализировать их. Благодаря этому вы сможете лучше понять, как безопасно защитить информацию.

За время прохождения практики освоены необходимые компетенции, в частности попыталась освоить базовые знания по сокрытию информации, извлечению информации, а также сильные и слабые стороны этих методов решения, из которых можно получить понимание, чтобы лучше обеспечивать информационную безопасность.

ОТЗЫВ О ПРОХОЖДЕНИИ ПРАКТИКИ

Вид практики _____ учебная практика
(учебная, производственная, преддипломная)

Тип практики _____ Экспериментально-исследовательская практика
(учебная, производственная, преддипломная)

Сроки прохождения практики: с 01.07.2024 г. по 13.07.2024 г.
по направлению подготовки 10.05.03 Информационная безопасность
автоматизированных систем (уровень академического специалитета)
направленность (профиль) «Безопасность открытых информационных систем»
студентом группы № 6313-100503D Ле Лок Тхо

№ п/п	Критерии оценки	Оценка (по 5-балльной шкале)
1.	Общая систематичность и ответственность работы в ходе практики	
2.	Степень личного участия и самостоятельности практиканта в представляемой работе	
3.	Выполнение поставленных целей и задач	
4.	Корректность в сборе, анализе и интерпретации представляемых данных	
5.	Качество оформления отчетной документации	
ИТОГОВАЯ ОЦЕНКА*		

Руководитель практики
от профильной организации _____ А.И. Максимов
(подпись)

* Итоговая оценка выставляется как средняя арифметическая оценок по пяти критериям оценки