**МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ**

**ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ**

**«СРЕДНЯЯ ПОЛИТЕХНИЧЕСКАЯ ШКОЛА №33»**

**ИНДИВИДУАЛЬНЫЙ ИТОГОВЫЙ ПРОЕКТ**

**«Стеганография как метод шифрования»**

**Выполнила:** Гизатуллина Олеся Сергеевна*,*

9-г класс

**Руководитель:** Хаустова Светлана Александровна, учитель информатики

Старый Оскол

2025

**СОДЕРЖАНИЕ**

**ВВЕДЕНИЕ**…………………………………………………………………..........3

**ТЕОРЕТИЧЕСКАЯ ЧАСТЬ**……………………………………………….........5

1.1. История стеганографии .................................…………………………...........5

1.2. Основные задачи стеганографии......................................…......…………......6

1.3. Структура стеганографической системы ……................................................7

1.4 Скрытие данных в частотной области изображения.......................................8

**ПРАКТИЧЕСКАЯ ЧАСТЬ**…………………………………………………......9

2. Алгоритм .................................…………………………......................................9

2.1.-2.2 Инициализация и создания ключа......................................…......…….....9

2.3.-2.5 Шифрование и дешифрования текста …….............................................10

2.6.-2.7 Операция XOR, сохранение и восстановление изображения................11

**ЗАКЛЮЧЕНИЕ**………………………………………………………….............12

**ИНФОРМАЦИОНННЫЕ ИСТОЧНИКИ**……………………………............13

### **Введение**

#### **Актуальность**

В современном мире, где объемы передаваемой информации растут экспоненциально, а киберугрозы становятся все более изощренными, защита данных приобретает критически важное значение. Стеганография, как метод скрытой передачи информации, позволяет обеспечить конфиденциальность данных, маскируя их в обычных на первый взгляд файлах, таких как изображения, аудио или видео. Это особенно актуально в условиях, когда традиционные методы шифрования могут привлекать внимание злоумышленников. Стеганография позволяет скрыть сам факт передачи информации, что делает ее важным инструментом в арсенале защиты данных.

#### **Объект и предмет исследования**

* **Объект исследования**: методы стеганографии, которые используются для скрытой передачи информации.
* **Предмет исследования**: алгоритмы скрытой передачи данных через изображения, их эффективность, устойчивость к обнаружению и применимость в различных сферах.

#### **Цель исследования**

Целью работы является разработка и анализ алгоритма стеганографии, который позволит скрытно передавать информацию через изображения, обеспечивая высокую устойчивость к обнаружению и сохранение качества исходного изображения.

#### **Задачи исследования**

1. Изучить существующие методы стеганографии, их преимущества и недостатки.
2. Разработать алгоритм скрытой передачи данных через изображения, учитывая требования к скрытности и устойчивости.
3. Провести анализ разработанного алгоритма, оценить его применимость в различных условиях.

#### **Гипотеза**

Предполагается, что разработанный алгоритм стеганографии будет обладать высокой степенью скрытности, что сделает его пригодным для передачи конфиденциальных данных. Алгоритм будет устойчив к попыткам обнаружения и извлечения скрытой информации, сохраняя при этом качество исходного изображения.

#### **Методы исследования**

* **Теоретические методы**:
  + Анализ научной литературы и существующих методов стеганографии.
  + Моделирование алгоритма и его теоретическое обоснование.
* **Практические методы**:
  + Разработка программного обеспечения для реализации алгоритма.
  + Проведение экспериментов для оценки скрытности, устойчивости и производительности алгоритма.

#### **Практическая значимость**

Разработанный алгоритм и программа могут быть использованы в различных сферах, таких как:

* **Защита информации**: для передачи конфиденциальных данных без привлечения внимания.
* **Криминалистика**: для скрытой передачи данных между правоохранительными органами.
* **Образование**: в качестве учебного пособия для изучения методов стеганографии и защиты информации.

#### **Продукт исследования**

Основным продуктом исследования станет программа, позволяющая скрыто передавать данные через изображения. Программа будет включать следующие функции:

1. **Встраивание информации**: пользователь сможет скрывать текстовые данные или файлы в изображениях.
2. **Извлечение информации**: возможность извлечения скрытых данных из изображений.
3. **Оценка качества**: анализ изменений в изображении после встраивания данных.

**ТЕОРЕТИЧЕСКАЯ ЧАСТЬ**

**1.1.История стеганографии**

История стеганографии тесно связана с защитой информации, хотя её задачи отличаются от криптографии. Криптография делает содержание сообщения недоступным для посторонних, а стеганография скрывает сам факт передачи. Эти методы могут использоваться как вместе, так и по отдельности. Термин «стеганография» (от греч. «скрытый» и «пишу») введён в 1499 году Иоганном Тритемием. Хотя стеганография зародилась раньше криптографии, она долгое время оставалась в тени, пока в XX веке интерес к ней не возродился благодаря развитию технологий.

Основная идея стеганографии — встраивание сообщения в незаметный контейнер, например, изображение, аудиофайл или текст. Получатель извлекает скрытое сообщение, которое может быть как открытым, так и зашифрованным. Исторически стеганография использовалась в различных формах: симпатические чернила, микрофотоснимки, типографские эффекты (опечатки, изменения шрифтов). Например, в фильме «Семнадцать мгновений весны» открытка с цветами служила кодом.

С развитием цифровых технологий стеганография перешла на новый уровень. Современные методы позволяют скрывать данные в цифровых контейнерах (изображения, аудио, видео) благодаря избыточности данных. Цифровая стеганография активно развивается для обхода ограничений на криптографию, защиты авторских прав (водяные знаки) и обеспечения приватности в условиях массовой цифровизации.

Государства и спецслужбы всегда уделяли внимание методам противодействия скрытой передаче информации. Например, во время Второй мировой войны США ввели ограничения на пересылку газетных вырезок, шахматных партий и цветов. В СССР подобные методы также применялись, хотя подробности остаются засекреченными.

Стеганография прошла долгий путь от древних методов до современных технологий. Её значение продолжает расти в условиях цифровизации и ужесточения контроля. В будущем она станет ещё более сложной и эффективной, оставаясь ключевым инструментом защиты информации.

**1.2.Основные задачи стеганографии**

Основные задачи стеганографии, несмотря на её древнее происхождение, в цифровом формате стали активно изучаться лишь в последние десятилетия. Цифровая стеганография — относительно молодая наука, основные понятия которой были согласованы на Первой Международной конференции по сокрытию данных в 1996 году. В работе В.Г. Грибунина и других авторов выделяются ключевые направления: скрытая передача информации, встраивание цифровых водяных знаков (ЦВЗ), идентификационных номеров и заголовков. Эти направления составляют теоретическую основу стеганографии, но на практике её методы решают более конкретные задачи.

Одной из главных задач является защита конфиденциальной информации и создание скрытых каналов передачи данных. Совместное использование криптографии и стеганографии повышает уровень защиты: криптография шифрует содержание, а стеганография скрывает факт передачи. Это значительно усложняет задачу для злоумышленников.

Другой важной задачей является защита авторских прав. С развитием цифровых технологий проблема незаконного копирования и распространения контента стала особенно актуальной. Для её решения используются ЦВЗ и идентификационные номера. ЦВЗ, в отличие от видимых аналогов, остаются невидимыми и содержат информацию о правообладателе или код аутентификации. Метод «fingerprinting» позволяет внедрять уникальные идентификаторы в каждую копию объекта, что помогает отслеживать распространение и бороться с пиратством.

Третья задача — преодоление систем мониторинга и управления сетевыми ресурсами. Злоумышленники могут использовать стеганографию для скрытого встраивания запрещённого контента в разрешённые файлы, обходя корпоративные ограничения. Это создаёт угрозы для информационной безопасности.

Следует отметить, что не все задачи стеганографии законны. Например, создание скрытых каналов для утечки данных или обход систем контроля могут использоваться в преступных целях. Однако изучение таких методов необходимо для успешного противодействия.

Таким образом, стеганография играет важную роль в защите информации, авторских прав и противодействии сетевым угрозам. Её методы продолжают развиваться, адаптируясь к новым вызовам, что делает её незаменимым инструментом в современном мире цифровых коммуникаций.

**1.3.Структура стеганографической системы**

Стеганографическая система скрывает сообщение в контейнере — несекретных данных, передаваемых открыто. Сообщение — это информация, которую нужно скрыть, а контейнер — это носитель, например, изображение, аудио или текст. Пустой контейнер не содержит скрытой информации, а заполненный — результат внедрения сообщения. Основное требование: контейнер-результат должен быть неотличим от оригинала для человеческого восприятия.

Контейнеры бывают избранными (подобранными для повышения скрытности), навязанными (предоставленными для предотвращения скрытой передачи) или случайными. Для сокрытия сообщения требуется контейнер, размер которого в несколько раз превышает размер сообщения. Чем больше это соотношение, тем выше скрытность.

На стороне отправителя процесс начинается с анализатора формата, который выбирает подходящий контейнер. Сообщение может быть предварительно обработано в прекодере: зашифровано, преобразовано для устойчивости к искажениям или защищено помехоустойчивым кодированием. В стеганокодере сообщение упаковывается в контейнер с использованием стеганографических методов. Ключ, хотя и не обязателен, повышает секретность.

На стороне получателя стеганодетектор определяет наличие скрытого сообщения. Если оно обнаружено, стеганодекодер извлекает его. Если на стороне отправителя использовался прекодер, извлечённое сообщение может быть обработано во вторичном декодере для восстановления исходного вида.

Стеганографическая система может использоваться не только для передачи, но и для хранения конфиденциальной информации. Основная задача — сокрытие сообщения — выполняется стеганокодером, где реализуются ключевые алгоритмы и методы. Правильный выбор контейнера и предварительная обработка сообщения играют важную роль, но именно стеганокодер является центральным элементом системы.

**1.4.Скрытие данных в частотной области изображения**

Скрытие данных в изображениях может осуществляться как в пространственной, так и в частотной областях. В первом случае изменения вносятся в значения отдельных пикселей, что делает метод уязвимым к сжатию, особенно с потерями, как в JPEG. Более надежным способом является внедрение данных в частотную область изображения с использованием дискретных преобразований, таких как дискретное косинусное преобразование (ДКП), дискретное преобразование Фурье (ДПФ) или вейвлет-преобразование.

При использовании частотного подхода информация внедряется в коэффициенты преобразования, что позволяет минимально изменять визуальные характеристики изображения. Этот метод более устойчив к компрессии, если он учитывает используемый алгоритм. Например, стеганография на основе ДКП будет более надежной при последующей JPEG-компрессии, а для JPEG2000, использующего вейвлет-преобразование, предпочтителен аналогичный метод.

Разработка универсального стеганографического метода, независимого от алгоритма компрессии, остается актуальной задачей. Исследования показывают, что большая часть энергии сосредоточена в низкочастотных областях спектра, которые менее подвержены искажению, но могут содержать шум. Высокочастотные компоненты более уязвимы к искажению, что делает их менее подходящими для встраивания данных. Оптимальными для стеганографии являются среднечастотные поддиапазоны, обеспечивающие баланс между устойчивостью к сжатию и незаметностью изменений.

При разработке стеганографического метода для конкретного канала передачи важно учитывать выбор алгоритма сжатия. Алгоритмы с максимальным сжатием уменьшают емкость контейнера для скрытых данных, удаляя избыточную информацию. Менее агрессивные методы компрессии позволяют внедрить больше скрытых данных, увеличивая пропускную способность стеганоалгоритма. Таким образом, выбор компрессии зависит от приоритетов – скрытности или пропускной способности канала.

**ПРАКТИЧЕСКАЯ ЧАСТЬ**

**2.Алгоритм**

Алгоритм, реализует простую схему стеганографии, где текст шифруется и дешифруется с использованием изображения в качестве ключа. Основная идея заключается в том, что текст кодируется в байты UTF-8, а затем эти байты "скрываются" в зеленом канале пикселей изображения с помощью операции XOR. Давайте разберем алгоритм по шагам:

### **2.1. Инициализация и загрузка изображения**

* Элементы DOM:
  + encrypt и decrypt — кнопки для шифрования и дешифрования.
  + text — поле ввода текста.
  + result — поле для вывода результата.
  + canvas — холст для работы с изображением.
  + imageInput — поле для загрузки изображения (не используется в текущем коде).
* Загрузка изображения:
  + Изображение загружается из файла img/orig.webp.
  + После загрузки изображения (img.onload) оно отрисовывается на холсте.
  + Изображение анализируется, и извлекаются данные о каждом пикселе (ширина, высота, общее количество пикселей, данные о цвете).

### **2.2. Создание ключа**

* Для каждого пикселя изображения извлекается значение зеленого канала (g).
* Эти значения сохраняются в массиве key вместе с координатами пикселя (x, y).
* Массив key используется как ключ для шифрования и дешифрования.

### **2.3. Преобразование текста в байты UTF-8**

* Функция textToUTF8Bytes преобразует текст в массив байтов UTF-8.
  + Каждый символ текста кодируется в один или несколько байтов в зависимости от его Unicode-кода.
  + Например:
    - Символы ASCII (0-127) кодируются одним байтом.
    - Символы из других диапазонов (например, кириллица) кодируются двумя или тремя байтами.

### **2.4. Шифрование текста**

* При нажатии на кнопку encrypt:
  + Текст из поля ввода преобразуется в массив байтов UTF-8.
  + Для каждого байта текста:
    - Извлекается значение зеленого канала соответствующего пикселя.
    - Байт текста и значение зеленого канала преобразуются в двоичные строки.
    - Выполняется операция XOR между битами байта текста и битами зеленого канала.
    - Результат XOR записывается обратно в зеленый канал пикселя.
  + Изображение с измененными пикселями сохраняется в формате PNG.

### **2.5. Дешифрование текста**

* При нажатии на кнопку decrypt:
  + Для каждого пикселя изображения:
    - Извлекается текущее значение зеленого канала.
    - Извлекается оригинальное значение зеленого канала из массива key.
    - Выполняется операция XOR между текущим и оригинальным значением зеленого канала.
    - Результат XOR преобразуется в байт.
  + Полученные байты объединяются и декодируются обратно в текст с помощью функции utf8BytesToText.
  + Расшифрованный текст выводится в поле result.

### **2.6. Операция XOR**

* Операция XOR (исключающее ИЛИ) является ключевой в этом алгоритме.
  + Она обратима: A XOR B = C, затем C XOR B = A.
  + Это позволяет использовать одно и то же значение зеленого канала для шифрования и дешифрования.

### **2.7. Сохранение и восстановление изображения**

* После шифрования измененное изображение сохраняется в формате PNG.
* Для дешифрования используется это же изображение, но с учетом оригинального ключа (значений зеленого канала до шифрования).

### **Пример работы алгоритма**

1. Шифрование:
   1. Ввод текста: "Hello".
   2. Текст преобразуется в байты: [72, 101, 108, 108, 111].
   3. Байты шифруются с использованием зеленого канала пикселей.
   4. Изображение сохраняется.
2. Дешифрование:
   1. Загружается измененное изображение.
   2. Для каждого пикселя выполняется XOR между текущим и оригинальным значением зеленого канала.
   3. Полученные байты декодируются в текст: "Hello".

**Заключение**

Главный вывод, который я сделала: стеганография на основе изменения частотных характеристик изображения позволяет скрывать информацию более надежно, чем методы, использующие пространственную область, особенно при последующей компрессии.

В ходе проведённого исследования было установлено, что эффективность сокрытия данных зависит от выбора метода преобразования, соответствующего алгоритму сжатия изображения. Кроме того, было подтверждено, что использование среднечастотных областей спектра изображения обеспечивает баланс между устойчивостью к сжатию и незаметностью изменений.

Этот метод позволяет скрывать информацию внутри изображения и позже извлекать её почти без видимых изменений изображения для человеческого глаза.

Результаты исследования могут быть использованы учителями при подготовке уроков по информатике, кибербезопасности и цифровым технологиям, а также для проведения конкурсов и викторин по этим темам.

Кроме того, данное исследование может быть полезно для дальнейших разработок в области безопасной передачи данных, создания методов защиты информации и изучения уязвимостей существующих алгоритмов.

Своей работой я хотела привлечь внимание одноклассников к проблеме защиты информации в цифровом мире и показать, как можно скрывать и расшифровывать данные с помощью изображений.

**ИНФОРМАЦИОННЫЕ РЕСУРСЫ**

1. Основные положения стенографии. <http://www.i2r.ru/static/567/out_19447.shtml>

2. Dallas system. О стеганографии кратко, ДКП, Встраивание ЦВЗ <https://codeby.net/threads/o-steganografii-kratko-dkp-vstraivanie-cvz.72975/>

3. NTA. Стеганография. Методы сокрытия сообщения в контейнере изображения <https://vc.ru/dev/248478-steganografiya-metody-sokrytiya-soobshcheniya-v-konteynere-izobrazheniya>

4. Основы JavaScript <https://learn.javascript.ru/>

5. Учебники CSS, HTML, JavaScript <https://developer.mozilla.org/ru/docs/Web/Tutorials>

6. Вёрстка <https://uiverse.io/>

7. Методы компьютерной стеганографии https://www.vsavm.by/knigi/ kniga3/1740.html

8. Стеганография kaspersky <https://kids.kaspersky.ru/files/steganography/%D0%9C%D0%B0%D1%82%D0%B5%D1%80%D0%B8%D0%B0%D0%BB%20%D0%B4%D0%BB%D1%8F%20%D1%83%D1%87%D0%B8%D1%82%D0%B5%D0%BB%D1%8F.pdf>

9. В.Г. Грибунин и др. «Цифровая стеганография»

10. Жельников В. Криптография от папируса до компьютера. М., 1996.

|  |  |
| --- | --- |
| Название проекта | Стеганография как метод шифрования |
| Проблема, которую решает проект (его актуальность) | В современном мире, где объемы передаваемой информации растут экспоненциально, а киберугрозы становятся все более изощренными, защита данных приобретает критически важное значение. Стеганография, как метод скрытой передачи информации, позволяет обеспечить конфиденциальность данных, маскируя их в обычных на первый взгляд файлах, таких как изображения, аудио или видео. Это особенно актуально в условиях, когда традиционные методы шифрования могут привлекать внимание злоумышленников. Стеганография позволяет скрыть сам факт передачи информации, что делает ее важным инструментом в арсенале защиты данных. |
| Цель проекта | Целью работы является разработка и анализ алгоритма стеганографии, который позволит скрытно передавать информацию через изображения, обеспечивая высокую устойчивость к обнаружению и сохранение качества исходного изображения. |
| Способы решения проблемы | Программа, позволяющая скрыто передавать данные через изображения |
| Выводы | Главный вывод, который я сделала: стеганография на основе изменения частотных характеристик изображения позволяет скрывать информацию более надежно, чем методы, использующие пространственную область, особенно при последующей компрессии.  В ходе проведённого исследования было установлено, что эффективность сокрытия данных зависит от выбора метода преобразования, соответствующего алгоритму сжатия изображения. Кроме того, было подтверждено, что использование среднечастотных областей спектра изображения обеспечивает баланс между устойчивостью к сжатию и незаметностью изменений. |
| Демонстрация продукта проекта | <https://olesyacone.github.io/Steganography/> |
| Практическое применение продукта проекта | **1)Защита информации**: для передачи конфиденциальных данных без привлечения внимания.  **2)Криминалистика**: для скрытой передачи данных между правоохранительными органами.  **3)Образование**: в качестве учебного пособия для изучения методов стеганографии и защиты информации. |