|  |  |
| --- | --- |
|  | **Российский государственный социальный университет** |

**Итоговое практическое задание № 1.**

**по дисциплине «Информационная безопасность»**

**на тему «Методы компьютерной стеганографии. LSB-метод»**

|  |  |
| --- | --- |
| **ФИО студента** | Салов Артём Владимирович |
| **Направление подготовки** | Программная инженерия |
| **Группа** | ПИН-Б-О-Д-2021-1 |

**Москва 2023**

Оглавление

[Введение. 3](#_Toc153726551)

[Стенография и LSB-метод. 4](#_Toc153726552)

[Что такое стеганография. 4](#_Toc153726553)

[LSB-метод. 5](#_Toc153726554)

[Плюсы и минусы LSB-метода. 5](#_Toc153726555)

[Способы стегоанализа и защиты от него. 6](#_Toc153726556)

[Способы стегоанализа. 6](#_Toc153726557)

[Способы защиты от стегоанализа. 7](#_Toc153726558)

[Заключение 8](#_Toc153726559)

# Введение.

В эпоху цифровых технологий, в которой информационный обмен стал неотъемлемой частью нашей повседневной жизни, вопросы безопасности данных приобретают особенное значение. Угрозы кибер-безопасности, перехват конфиденциальных данных и несанкционированный доступ к информации заставляют нас постоянно совершенствовать методы обеспечения безопасности. Одним из инновационных и недооцененных средств обеспечения конфиденциальности информации является компьютерная стеганография.

Методы компьютерной стеганографии предоставляют механизмы для незаметного внедрения информации в различные типы файлов, сохраняя при этом внешний вид носителя. Этот подход открывает новые перспективы для защиты конфиденциальности данных и обеспечения безопасности информационных потоков.

Цель данного доклада — более глубокое понимание LSB-метода в компьютерной стеганографии. Мы рассмотрим основные принципы этой техники, рассмотрим ее применение в различных сферах, а также обсудим потенциальные угрозы и методы обнаружения стеганографии. Проанализировав технические аспекты метода, мы сможем оценить его возможности и ограничения, а также более глубоко вникнуть в современные вопросы безопасности и защиты данных в цифровом мире.

# Стенография и LSB-метод.

## Что такое стеганография.

*Стеганография* — это область информационной безопасности, посвященная скрытой передаче данных с минимизацией заметности факта их существования. В отличие от криптографии, которая фокусируется на шифровании данных для защиты от несанкционированного доступа, стеганография стремится сохранить конфиденциальность, скрывая сам факт наличия информации.

Слово "стеганография" происходит от греческих слов "steganos" (скрытый) и "graphia" (письмо), что подчеркивает суть этой техники — скрытая передача информации. Основной задачей стеганографии является внедрение скрытого контента в носитель (например, изображение, аудиофайл или текст), при этом изменения должны быть невидимыми или незаметными для человеческого восприятия.

Сегодня стеганография находит применение в различных сферах, включая кибер-безопасность, медицину, цифровую форензику, и даже в военных операциях. Однако, вместе с ее потенциальными пользами, возникают и риски, такие как скрытая передача вредоносных данных или нарушение авторских прав. Развитие методов стеганографии и стеганализа становится неотъемлемой частью борьбы за безопасность и контроль над цифровой информацией.

Методы стеганографии разнообразны и эволюционируют вместе с развитием технологий. Они направлены на скрытое внедрение информации в различные типы данных, при этом минимизируя заметность изменений. Ниже приведены основные методы стеганографии:

1. Frequency Domain Steganography:

Этот метод использует преобразование Фурье для внедрения информации в частотной области сигнала. Применяется к изображениям, аудиофайлам и видео. Методы, такие как изменение амплитуды или фазы в определенных частотных компонентах, могут быть использованы для внедрения данных.

1. Spread Spectrum Steganography:

Этот метод аналогичен принципу работы спред-спектра в коммуникационных системах. Информация распределяется по всему спектру сигнала, что делает ее менее заметной. В контексте стеганографии, это может включать в себя изменение фазы, частоты или амплитуды.

1. Transform Domain Steganography:

Этот метод внедрения информации в основном применяется к изображениям и аудиофайлам. Он основан на изменении коэффициентов преобразования (например, вейвлет-преобразования) сигнала. Это позволяет эффективно скрывать данные, используя особенности в различных областях сигнала.

1. Text Steganography:

Скрытая передача информации может также происходить в текстовых данных. Это может включать в себя изменение форматирования, шрифта, размера или даже внедрение скрытого текста в невидимую область текстового документа.

1. Network Steganography:

В данном случае, стеганография применяется к передаче данных через сетевые протоколы. Это может включать в себя изменение размера пакетов, времени задержки и других параметров для скрытой передачи информации.

1. Artificial Intelligence (AI) Steganography:

С использованием методов машинного обучения и искусственного интеллекта, разрабатываются более сложные методы стеганографии, способные адаптироваться и обходить методы стеганализа.

## LSB-метод.

*LSB-метод* в стеганографии представляет собой эффективную технику внедрения скрытой информации в цифровые носители, такие как изображения, аудиофайлы или видео, путем модификации наименее значащих битов этих данных. Акроним "LSB" расшифровывается как "Least Significant Bit" (наименее значащий бит). Этот метод основан на простой, но мощной идее: заменять наименее значащие биты в бинарном представлении пикселей (в случае изображений) или отсчетов (в случае аудиофайлов) на биты скрытого сообщения.

Одной из главных привлекательных черт LSB-метода является его незаметность для человеческого восприятия. Изменения в наименее значащих битах обычно незаметны для человеческого глаза или уха, что позволяет сохранить визуальное или звуковое качество оригинальных данных. Таким образом, LSB-стеганография обеспечивает деликатный баланс между сокрытием информации и сохранением естественного вида или звучания.

Применение LSB-метода может быть широким: от обеспечения конфиденциальности данных и водяных знаков в изображениях до скрытой передачи метаданных или даже хранения дополнительной информации в цифровых файлах. Тем не менее, с увеличением возможностей стеганографии возрастают и риски, связанные с ее злоупотреблением в киберпространстве.

Важно отметить, что LSB-метод, несмотря на свою эффективность, не является безупречным, и существуют методы стеганализа, направленные на обнаружение скрытых данных. Следовательно, постоянное развитие и совершенствование методов стеганографии и стеганализа остаются ключевыми аспектами в обеспечении цифровой безопасности и контроле за передачей информации в современном информационном обществе.

## Плюсы и минусы LSB-метода.

Плюсы LSB-метода в стеганографии:

1. Невидимость для человеческого восприятия: Изменения, внесенные в наименее значащие биты, обычно не заметны для человеческого глаза или уха, что обеспечивает высокую степень незаметности внедрения скрытой информации.
2. Простота реализации: LSB-метод является относительно простым в реализации, что делает его доступным и понятным для широкого круга пользователей.
3. Универсальность: Метод применим к различным типам данных, включая изображения, аудиофайлы и видео, что расширяет его область применения.
4. Отсутствие необходимости в дополнительных ключах: В отличие от некоторых криптографических методов, LSB-стеганография не требует дополнительных ключей для внедрения и извлечения скрытой информации.

Минусы LSB-метода в стеганографии:

1. Низкая устойчивость к стеганализу: LSB-метод является относительно уязвимым для методов стеганализа, направленных на обнаружение скрытых данных. Атакующие могут использовать статистические методы для выявления изменений в наименее значащих битах.
2. Ограниченная вместимость данных: Поскольку информация встраивается в младшие биты, объем доступного места для скрытых данных ограничен. Это может быть недостаточным для встраивания больших объемов информации.
3. Чувствительность к сжатию: Процессы сжатия данных, такие как алгоритмы JPEG для изображений, могут повлиять на наименее значащие биты и стереть скрытую информацию.
4. Не устойчив к некоторым видам атак: Например, при применении атаки сжатия и последующего повторного встраивания информации, может произойти потеря данных и ухудшение качества стеганографического изображения.
5. Неэффективность при работе с текстом: В случае текстовых данных встраивание информации в наименее значащие биты может привести к видимым изменениям в тексте и его структуре.
6. Ограниченность в контексте видео- и аудиостеганографии: В случае видео и аудиофайлов, изменения в наименее значащих битах могут быть заметны при проигрывании контента, особенно при использовании высококачественного оборудования.

# Способы стеганоанализа и защиты от него.

## Способы стеганоанализа.

LSB-метод, несмотря на свою популярность и широкое использование, подвержен риску взлома различными методами стеганализа. Вот несколько методов, которые могут использоваться для взлома LSB-метода:

1. *Статистический анализ* – это анализ статистических характеристик изображения, таких как распределение битов или гистограмма, может выявить аномалии, связанные с внедрением скрытой информации. Если изменения в LSB-битах не соответствуют естественной статистике изображения, это может стать признаком наличия стеганографии.
2. Анализ фрактальной размерности: Изменения, внесенные LSB-методом, могут влиять на фрактальную размерность изображения. Сравнение этой размерности с ожидаемой может выявить скрытые данные.
3. Атаки на сжатие: Алгоритмы сжатия, такие как JPEG, могут изменять LSB-биты при обработке изображения. Процессы сжатия могут привести к потере данных и ухудшению качества стеганографического изображения. Атаки, направленные на такие изменения, могут выявить наличие скрытой информации.
4. Частотный анализ: Анализ частотных компонент изображения может выявить изменения в LSB-битах. Атакующие могут использовать методы фурье-анализа для выделения изменений, связанных с внедрением данных.
5. Атаки на размер файла: Если ожидается, что файл имеет определенный размер, а размер увеличивается из-за внедрения скрытой информации, это может быть признаком стеганографии.
6. Анализ энтропии: Изменения в LSB-битах могут влиять на энтропию изображения. Несоответствие ожидаемой энтропии может быть использовано для обнаружения стеганографии.
7. Особенности формата: Некоторые форматы изображений имеют структуру, которая может быть использована для выявления изменений, связанных с внедрением данных. Например, в BMP-изображениях изменения в заголовках могут выдать стеганографию.
8. Атаки на повторное встраивание: Повторное внедрение данных в стеганографическое изображение может привести к потере части информации. Атаки, направленные на повторное встраивание, могут раскрывать наличие стеганографии.

## Способы защиты от стегоанализа.

Защита от стегоанализа в контексте LSB-метода в стеганографии требует внимательности и использования дополнительных методов для сокрытия внедрения данных. Вот несколько способов защиты от стегоанализа в рамках LSB-метода:

1. Использование случайного выбора битов: Вместо внедрения информации только в наименее значащие биты каждого компонента, можно использовать случайный выбор битов для внедрения. Это делает статистический анализ более сложным, поскольку изменения распределены более случайным образом.
2. Использование адаптивного подхода: Адаптивные методы изменения количества встраиваемых бит в зависимости от конкретных характеристик изображения или звукового файла могут сделать стегоанализ более сложным.
3. Добавление шума: Добавление случайного шума к наименее значащим битам может затруднить стегоанализ. Однако, важно контролировать уровень шума, чтобы сохранить незаметность изменений.
4. Использование дополнительных слоев шифрования: Внедрение дополнительных слоев шифрования поверх LSB-метода может усложнить анализ и обеспечить дополнительный уровень защиты.
5. Смешивание с данными: Перед встраиванием данных можно применить методы, которые смешивают стеганографические изменения с естественными данными, чтобы сделать их менее заметными.
6. Избегание равномерного распределения: Избегание равномерного распределения изменений по всему изображению может снизить эффективность статистических методов стегоанализа.
7. Использование различных каналов: Вмешивание информации в различные цветовые каналы (RGB, YUV и т. д.) может сделать стегоанализ более сложным, поскольку изменения будут распределены по различным компонентам.
8. Динамическая адаптация параметров: Изменение параметров внедрения, таких как количество изменяемых битов, в зависимости от свойств изображения, может сделать анализ более трудным.

# Заключение

В итоге, проведенный анализ методов компьютерной стеганографии, с фокусом на LSB-методе, позволяет сделать несколько важных выводов. LSB-метод, основанный на замене младших битов пикселей изображения, представляет собой эффективный и относительно простой способ внедрения скрытой информации. Его применение широко распространено в различных областях, включая передачу данных в цифровых изображениях, аудиофайлах и видео.

Однако, несмотря на свою популярность, LSB-метод не лишен определенных недостатков. В первую очередь, его уязвимость к атакам, направленным на выявление и извлечение скрытой информации. Существующие методы анализа LSB-стеганографии могут поддаваться современным методам криптоанализа, что подчеркивает важность дополнительных механизмов защиты и усовершенствования техник стеганографии.

В свете растущих угроз безопасности данных и прогрессирующих технологий, изучение методов компьютерной стеганографии, включая LSB-метод, является ключевым элементом в обеспечении информационной безопасности. Перспективы развития данной области связаны с поиском новых методов стеганографии, способных устойчиво сокрыть информацию и предоставить высокий уровень защиты данных от несанкционированного доступа.

Таким образом, дальнейшие исследования в области компьютерной стеганографии, в том числе с учетом LSB-метода, могут способствовать созданию более совершенных и безопасных методов передачи и хранения конфиденциальной информации в цифровой среде.

*Список источников:*

1. Скрывать не скрывая. Еще раз о LSB-стеганографии, хи-квадрате и… сингулярности? – URL: <https://habr.com/ru/articles/422593/>
2. Что такое стеганография? Определение и описание - <https://www.kaspersky.ru/resource-center/definitions/what-is-steganography>
3. Стеганография – URL: <https://ru.wikipedia.org/wiki/Стеганография>
4. Стегоанализ метода сокрытия информации в изображении замены наименьшего значащего бита (LSB) – URL: <https://cyberleninka.ru/article/n/stegoanaliz-metoda-sokrytiya-informatsii-v-izobrazhenii-zameny-naimenshego-znachaschego-bita-lsb>
5. Стеганография в цифровых изображениях – URL: <https://ru.wikipedia.org/wiki/Стеганография_в_цифровых_изображениях>
6. Применение LSB в информационной безопасности – URL: <https://uralchip.ru/faq/lsb-cto-eto-znacit-i-kak-eto-rabotaet>