Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №12**

**«ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ»**

Выполнил:

Cтудент 3 курса 1 группы

Парибок И. А.

Вариант 5

**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.

**Задачи:**

1. Закрепить теоретические знания из области стеганографического преобразования информации, моделирования стеганосистем, классификации и сущности методов цифровой стеганографии.

2. Изучить алгоритм встраивания/извлечения тайной информации на основе метода НЗБ (LSB – Least Significant Bit), получить опыт практической реализации метода.

3. Разработать приложение для реализации алгоритма встраивания/извлечения тайной информации с использованием электронного файла-контейнера на основе метода НЗБ.

4. Познакомиться с методиками оценки стеганографической стойкости метода НЗБ.

5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Теоретические сведения**

Определение 1. Стеганографическая система (stegosystem, стегосистема или стеганосистема – в русскоязычной тематической литературе используются оба сокращения) – 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).

Определение 2. Абстрактно стеганографическая система обычно определяется как некоторое множество отображений одного пространства (множества возможных сообщений М) в другое пространство (множество возможных стеганосообщений S), и наоборот.

Основные компоненты стеганосистемы:

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

• тайное сообщение М, осаждаемое в контейнер для передачи или хранения (например, с целью доказательства или защиты авторских прав на документ-контейнер; здесь речь может идти о невидимых цифровых водяных знаках (ЦВЗ));

• 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 (например, на основе помехоустойчивого кодирования, сжатия или зашифрования) и т. д.;

• контейнер со встроенным сообщением, или стеганоконтейнер, S, который передается по открытому каналу, также являющемуся важным компонентом анализируемой системы; стеганоконтейнер будем именовать также стеганосообщением;

• для полноты упомянем также субъектов системы: отправителя и получателя.

В зависимости от формата документа-контейнера цифровую (или компьютерную) стеганографию подразделяют на классы:

• аудиостеганография;

• видеостеганография;

• графическая стеганография;

• текстовая стеганография;

• и др.

Определение 3. Стеганографической системой *∑* будем называть совокупность сообщений *M*, контейнеров *C*, ключей *K*, стеганосообщений (заполненных контейнеров) *S* и преобразований (прямого *F* и обратного *F*–1), которые их связывают:



Как видим, сущностью рассматриваемой системы является тайное хранение или передача одной информации в другой информации, которая является открытой.

Таким образом, при построении стеганосистемы должны учитываться следующие основные положения:

• свойства контейнера должны быть модифицированы так, чтобы изменение невозможно было выявить при визуальном контроле; это требование определяет качество сокрытия внедряемого сообщения: для обеспечения беспрепятственного прохождения стеганосообщения по каналу связи оно никоим образом не должно привлечь внимание атакующего;

• противник (интруз) имеет полное представление о стеганографической системе и деталях ее реализации; единственной информацией, которая остается ему неизвестной, является ключ, с помощью которого только его держатель может установить факт присутствия и содержание скрытого сообщения;

• если противник каким-то образом узнает о факте существования скрытого сообщения, это не должно позволить ему извлечь подобные сообщения до тех пор, пока ключ хранится в тайне;

• потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений.

*Метод НЗБ и особенности его реализации*

Большинство исследований в предметной области посвящено использованию в качестве стеганоконтейнеров изображений (текст также можно рассматривать как изображение). Это обусловлено следующими причинами:

• относительно большим объемом цифрового представления изображений, что позволяет внедрять большой объем данных;

• заранее известным размером контейнера, отсутствием ограничений, накладываемых требованиями реального времени;

• наличием в большинстве реальных изображений текстурных областей, имеющих шумовую структуру и хорошо подходящих для встраивания информации;

• слабой чувствительностью человеческого глаза к незначительным изменениям цветов изображения, его яркости, контрастности, содержанию в нем шума, искажениям вблизи контуров;

• хорошо разработанными в последнее время методами цифровой обработки изображений.

Метод НЗБ основывается на ограниченных способностях зрения или слуха человека, вследствие чего людям тяжело различать незначительные вариации цвета или звука. Рассмотрим это на примере 24-битного растрового RGB-изображения. Как известно, каждая точка кодируется тремя байтами. Каждый байт определяет интенсивность красного (Red), зеленого (Green) и синего (Blue) цветов. Совокупность интенсивностей цвета в каждом из трех каналов определяет оттенок пикселя.

Представим пиксель тремя байтами в битовом виде, как это показано на рис. 1:

Изображение выглядит как текст, снимок экрана, линия, число

Автоматически созданное описание

Рисунок 1 – Пример, показывающий принцип реализации метода LSB

Младшие биты (выделены бледным, справа) дают незначительный «вклад» в изображение по сравнению со старшими.

Замена одного или даже нескольких младших битов для человеческого глаза будет почти незаметна, поскольку реально человек может различать около полторы сотни цветовых оттенков.

**Ход работы**

На рисунке 2 представлено основное окно с работой приложения. С окном для просмотра контейнера. Окнами для просмотра разницы до и после осадки. Выбор режима осадки и кнопками с осадком и извлечением сообщений.

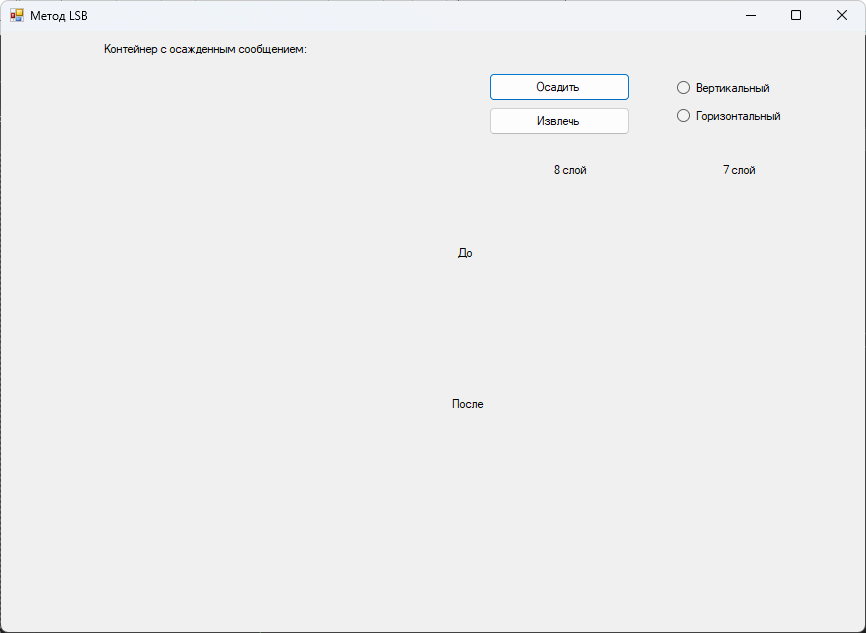


Рисунок 2 – Общий вил приложения

Для осадки необходимо нажать «Осадить» выбрать файл для осадки (рис. 3), файл с сообщением и путь сохранения контейнера. После чего на главном экране появится контейнер с осажденным сообщением и разницей до и после осаждения (рис. 4).

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рис 3 – Выбор контейнера

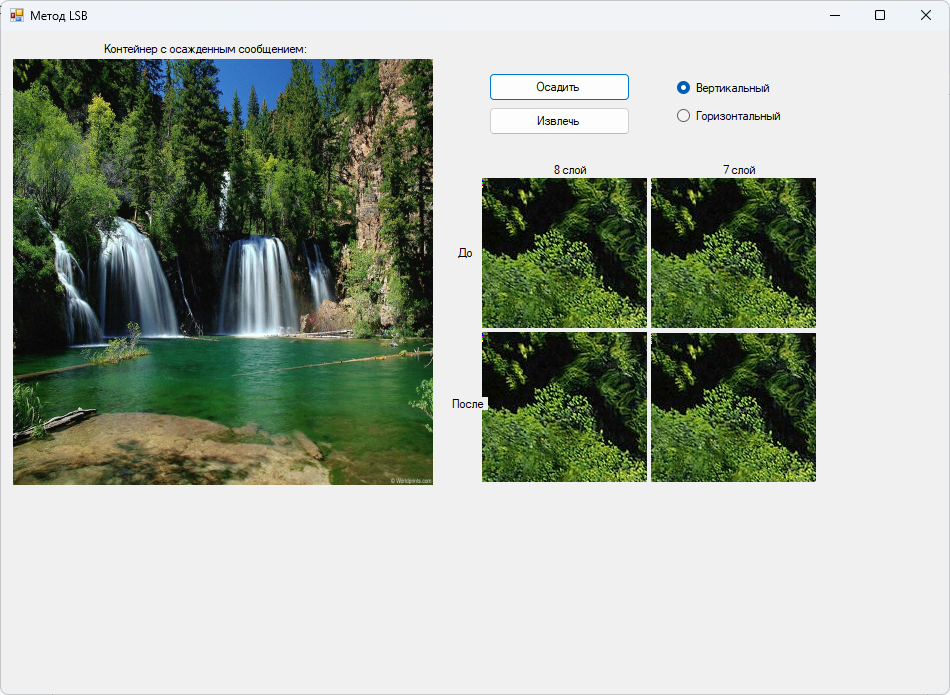


Рисунок 4 - Вид приложения после сокрытия информации

При нажатии на кнопку "Извлечь", появится окно файловой системы, в с выбором изображение, содержащее скрытую информацию. Появится окно для экспорта текстового документа, в котором будет содержаться извлеченная информация (рис 5.).

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Автоматически созданное описание

Рисунок 5 – Извлеченное сообщение

**Вывод:**

В процессе выполнения лабораторной работы был исследован метод стеганографии, основанный на использовании наименее значащих битов. Этот метод позволяет скрытно внедрять дополнительную информацию в целевой файл, используя малозначимые биты, и прост в реализации. Было установлено, что данный метод является эффективным и может быть применен к различным типам файлов. Он может использоваться в областях, связанных с конфиденциальностью данных и скрытой коммуникацией.

Тем не менее, следует учитывать потенциальные ограничения этого метода, например, возможную потерю качества целевого файла при внедрении большого объема скрытой информации. Поэтому важно подбирать оптимальные параметры внедрения, чтобы достичь баланса между емкостью для стенографической информации и сохранением качества целевого файла.

**Контрольные вопросы**

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

Стеганография — это наука о скрытой передаче информации, которая заключается в внедрении секретных данных в незаметные носители, такие как изображения, звуковые файлы, видео или текстовые документы. Цели, задачи и области применения стеганографии могут быть разнообразными.

Цели стеганографии:

Скрытая передача информации: Основная цель стеганографии - передать информацию между отправителем и получателем, не вызывая подозрений третьих лиц.

Конфиденциальность: Стеганография обеспечивает конфиденциальность, поскольку скрытые данные остаются незамеченными для наблюдателей.

Безопасность: Скрытая передача информации может помочь обеспечить безопасность данных от несанкционированного доступа и атак.

Задачи стеганографии:

Внедрение данных: Задача стеганографии - эффективно внедрить секретные данные в выбранный носитель, используя различные методы и алгоритмы.

Скрытность: Задача стеганографии - сделать внедренные данные незаметными для наблюдателей и статистического анализа.

Устойчивость: Задача стеганографии - обеспечить стойкость к различным атакам, включая атаки на внедрение данных, изменение данных или удаление данных.

Области применения стеганографии:

Коммерческая безопасность: Стеганография может использоваться для безопасной передачи коммерческой информации, такой как финансовые данные, планы проектов, секретные соглашения и т. д.

Криминалистика: В области криминалистики стеганография может использоваться для скрытой передачи доказательств, информации о преступлениях или тайных сообщениях между преступниками.

Компьютерная безопасность: Стеганография может быть применена для скрытого хранения и передачи аутентификационных данных, ключей шифрования или другой критической информации.

Журналистика и активизм: Журналисты и активисты могут использовать стеганографию для скрытой передачи чувствительной информации, например, о нарушениях прав человека или коррупции, чтобы защитить источник информации.

Компьютерные игры: Стеганография может быть использована в компьютерных играх для скрытой передачи информации между игроками или для внедрения дополнительных элементов в игровые ресурсы.

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

Сходства:

Цель безопасности: как стеганография, так и криптография стремятся обеспечить безопасность информации и защитить ее от несанкционированного доступа или изменений.

Использование методов и алгоритмов: Обе области полагаются на использование различных методов и алгоритмов для достижения своих целей безопасности. В криптографии это может быть шифрование и дешифрование с использованием ключей, а в стеганографии - внедрение и извлечение скрытой информации.

Защита конфиденциальности: Обе области имеют цель обеспечить конфиденциальность передаваемых данных, чтобы третьи лица не могли прочитать или распознать содержимое информации.

Различия:

Цель и подход: Криптография фокусируется на шифровании информации для сокрытия содержимого от несанкционированного доступа. Стеганография, с другой стороны, стремится скрыть сам факт наличия информации в носителе, делая ее незаметной.

Форма защиты: В криптографии информация обычно защищается путем преобразования ее в нечитаемую форму (шифрование), а затем обратного преобразования (дешифрование) с использованием ключа. В стеганографии информация внедряется в другой носитель, такой как изображение или звуковой файл.

Видимость: Криптография может быть видна для наблюдателей, но зашифрованное содержимое должно оставаться непонятным без доступа к ключу. Стеганография, напротив, стремится быть незаметной, чтобы наблюдатели не могли определить наличие скрытой информации.

Устойчивость: Криптографические методы зависят от прочности используемого шифра и безопасности ключа. В стеганографии, помимо вопросов криптографической стойкости, важным является и стойкость к атакам на сам факт скрытой передачи информации.

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

Стеганографическая система — это система, предназначенная для скрытой передачи информации путем внедрения секретных данных в носитель без вызывающих подозрений изменений в его внешнем виде или свойствах.

Составные части стеганосистемы и их взаимосвязь:

Информация: это секретные данные или сообщение, которое требуется передать скрытно.

Носитель (Carrier): это файл или данные, в которые будет внедрена информация. Носитель может быть изображением, звуковым файлом, видео или текстовым документом.

Метод внедрения (Embedding Method): это алгоритм или методика, которая определяет способ внедрения информации в носитель. Метод внедрения определяет, какие биты или части носителя будут использоваться для хранения информации.

Ключ (Key): В некоторых стеганографических системах используется ключ для обеспечения дополнительной безопасности и контроля доступа к скрытой информации. Ключ может использоваться для определения места внедрения информации или параметров внедрения.

Извлечение (Extraction): это процесс извлечения скрытой информации из носителя. Извлечение может быть осуществлено с помощью соответствующего алгоритма, использующего знание о методе внедрения и, при необходимости, ключа.

Оценка стойкости (Steganalysis): это процесс анализа носителя с целью обнаружения или определения наличия скрытой информации. Оценка стойкости может быть проведена для оценки эффективности стеганографической системы и ее устойчивости к различным атакам.

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

Методы стеганографии могут быть классифицированы по различным критериям. Вот некоторые основные классификационные критерии методов стеганографии:

Вид носителя:

Визуальная стеганография: использует визуальные носители, такие как изображения, для внедрения информации.

Аудио стеганография: использует звуковые носители, такие как аудиофайлы, для внедрения информации.

Видео стеганография: использует видеоносители для внедрения информации.

Метод внедрения:

Метод замены: заменяет определенные части носителя битами скрытой информации.

Метод перестановки: меняет порядок битов в носителе для хранения информации.

Метод частотного спектра: Внедрение информации в частотную область носителя.

Метод распределения ошибок: использует ошибки внутри носителя для внедрения информации.

Вместимость:

Методы с низкой вместимостью: Внедрение небольшого количества информации, обычно менее значимых битов носителя.

Методы с высокой вместимостью: Внедрение большого количества информации, включая использование всех доступных битов носителя.

Стеганографическая стойкость:

Слабая стойкость: Методы, которые легко обнаружить или извлечь скрытую информацию.

Сильная стойкость: Методы, которые сложно обнаружить или извлечь скрытую информацию даже с использованием стеганографического анализа.

Ключевые особенности:

Симметричные методы: используют один и тот же ключ для внедрения и извлечения информации.

Асимметричные методы: используют разные ключи для внедрения и извлечения информации.

Классификация методов стеганографии может быть более детализированной и зависит от конкретных аспектов исследования. Эти критерии помогают организовать и классифицировать методы стеганографии в соответствии с их основными характеристиками и применениями.

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

Основные атаки на стеганосистемы направлены на обнаружение скрытой информации или нарушение целостности стеганографического процесса. Вот некоторые из них:

Стеганализ (Steganalysis): это атака на стеганосистему с целью обнаружения наличия скрытой информации или извлечения самой информации. Стеганализ включает различные методы и алгоритмы для анализа стеганографического носителя с целью обнаружения аномалий, статистических распределений или характерных признаков, которые могут указывать на наличие скрытой информации. Стеганализ может использоваться для определения типа стеганографии, метода внедрения или даже извлечения скрытой информации.

Атака на ключ (Key Attack): это атака, направленная на получение или компрометацию ключа, используемого в стеганосистеме. Если злоумышленник получает доступ к ключу, он может легко извлечь скрытую информацию или внести изменения в стеганографический процесс.

Атака на носитель (Cover Attack): это атака на сам носитель, в котором внедрена скрытая информация. Например, злоумышленник может попытаться анализировать исходный носитель, чтобы обнаружить наличие изменений или артефактов, свидетельствующих о наличии скрытой информации.

Целенаправленное нарушение стеганографии (Targeted Steganography Attack): Это атака, при которой злоумышленник специально настраивает свою стеганосистему для обнаружения или нарушения стеганографии, используемой другими лицами. Например, злоумышленник может использовать методы стеганализа для обнаружения и извлечения информации, переданной в стеганографическом сообщении, или может попытаться внести изменения в стеганографический процесс для повреждения или искажения скрытой информации.

Социальная инженерия: это атака, которая основывается на манипуляции или обмане людей, работающих с стеганосистемой. Например, злоумышленник может попытаться получить доступ к ключам или информации, используя методы социальной инженерии, такие как фишинг, подмена личности или обман.

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

Входные данные:

Информация, которую необходимо скрыть (скрытая информация).

Носитель, который будет использован для внедрения скрытой информации.

Процесс внедрения информации:

Метод внедрения: определяет алгоритм или методику внедрения скрытой информации в носитель. Метод внедрения может варьироваться в зависимости от выбранного подхода и используемого носителя.

Ключ: в некоторых случаях для внедрения информации может использоваться ключ, который обеспечивает дополнительную безопасность и контроль доступа к скрытой информации.

Стеганографический носитель:

Носитель: это файл или данные, в которые будет внедрена скрытая информация. Носитель может быть изображением, аудиофайлом, видео или другими типами данных.

Процесс извлечения информации:

Извлечение метода: определяет алгоритм и методику извлечения скрытой информации из носителя. Для успешного извлечения информации требуется знание метода внедрения и, при необходимости, ключа.

Выходные данные:

Скрытая информация: Полученная скрытая информация, которая была извлечена из носителя.

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

Метод наименее значащих битов (НЗБ) является одним из методов стеганографии, который использует младшие (наименее значащие) биты носителя для внедрения скрытой информации. Основная сущность метода НЗБ состоит в замене младших битов пикселей или символов носителя на биты скрытой информации без заметного изменения визуального или акустического восприятия носителя.

Метод НЗБ часто применяется в следующих областях:

Стеганография изображений: Метод НЗБ широко используется для внедрения скрытой информации в изображения. Он может быть применен к различным форматам изображений, таким как JPEG, PNG, BMP и др.

Стеганография аудио: Метод НЗБ может быть использован для внедрения скрытой информации в аудиофайлы. Замена младших битов аудио сэмплов позволяет скрыть информацию в звуковом сигнале.

Стеганография видео: Метод НЗБ может быть применен к видеофайлам для внедрения скрытой информации. Замена младших битов пикселей видеокадров позволяет скрыть информацию в видеопотоке.

Защита авторских прав: Метод НЗБ может использоваться для помещения водяных знаков или метаданных в носители, такие как изображения или аудиофайлы, для защиты авторских прав и идентификации владельца.

Скрытая коммуникация: Метод НЗБ может быть применен для скрытой передачи информации между сторонами, не привлекая внимание наблюдателей. Это может быть полезно для конфиденциальной передачи сообщений или обмена информацией в чувствительных ситуациях.

Криминалистика: Метод НЗБ может использоваться в криминалистике для скрытого внедрения информации в цифровые доказательства, такие как изображения или видео, для их аутентификации или маркировки.

Метод НЗБ имеет свои преимущества и ограничения, и его эффективность зависит от выбранного носителя, методики внедрения и методов анализа стеганографической информации.

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

Входные данные:

Носитель: Изображение, аудиофайл или другой подходящий носитель, в котором будет внедряться скрытое сообщение.

Сообщение: Текстовое сообщение или другой тип данных, которое будет скрыто в носителе.

Процесс встраивания:

Разделение сообщения на биты: Каждый символ или байт сообщения разбивается на биты.

Обход пикселей/сэмплов носителя: проходимся по пикселям или сэмплам носителя, начиная с начального пикселя/сэмпла.

Замена младших битов: Младшие биты каждого пикселя/сэмпла заменяются на следующий бит из сообщения.

Продолжение процесса: переходим к следующему пикселю/сэмплу носителя и следующему биту сообщения.

Завершение: когда все биты сообщения были внедрены, завершаем процесс встраивания.

Выходные данные:

Стеганографический носитель: Носитель с внедренным скрытым сообщением.

Алгоритм извлечения сообщений на основе метода НЗБ:

Входные данные:

Стеганографический носитель: Носитель, содержащий внедренное скрытое сообщение.

Процесс извлечения:

Начало извлечения: устанавливаем начальный пиксель/сэмпл для извлечения сообщения.

Извлечение младших битов: извлекаем младшие биты каждого пикселя/сэмпла носителя.

Сбор извлеченных битов: собираем извлеченные младшие биты, формируя последовательность бит сообщения.

Продолжение процесса: переходим к следующему пикселю/сэмплу носителя и извлекаем младшие биты.

Завершение: когда все биты сообщения извлечены, завершаем процесс извлечения.

Выходные данные:

Извлеченное сообщение: Сообщение, которое было скрыто в стеганографическом носителе.

**9. Изобразить алгоритмы встраивания и извлечения сообщений на основе метода НЗБ при решении задачи защиты прав интеллектуальной собственности на электронный контент.**

Алгоритм встраивания сообщений на основе метода НЗБ в задаче защиты прав интеллектуальной собственности на электронный контент:

Входные данные:

Носитель: Электронный контент, такой как изображение, аудиофайл или видеофайл, который содержит информацию, подлежащую защите.

Сообщение: Информация об авторском праве или другая метаданных, которую необходимо скрыть в носителе.

Процесс встраивания:

Кодирование сообщения: Сообщение кодируется в битовую последовательность, используя определенный стандарт или формат.

Обход пикселей/сэмплов носителя: проходимся по пикселям или сэмплам носителя, начиная с начального пикселя/сэмпла.

Замена младших битов: Младшие биты каждого пикселя/сэмпла заменяются на следующий бит из сообщения.

Продолжение процесса: переходим к следующему пикселю/сэмплу носителя и следующему биту сообщения.

Завершение: когда все биты сообщения были внедрены, завершаем процесс встраивания.

Выходные данные:

Стеганографический носитель: Электронный контент с внедренной информацией об авторском праве или метаданными.

Алгоритм извлечения сообщений на основе метода НЗБ в задаче защиты прав интеллектуальной собственности на электронный контент:

Входные данные:

Стеганографический носитель: Электронный контент, содержащий внедренную информацию об авторском праве или метаданные.

Процесс извлечения:

Начало извлечения: устанавливаем начальный пиксель/сэмпл для извлечения сообщения.

Извлечение младших битов: извлекаем младшие биты каждого пикселя/сэмпла носителя.

Сбор извлеченных битов: собираем извлеченные младшие биты, формируя последовательность бит сообщения.

Декодирование сообщения: Извлеченная битовая последовательность декодируется в исходное сообщение об авторском праве или метаданные.

Завершение: когда все биты сообщения извлечены и декодированы, завершаем процесс извлечения.

Выходные данные:

Извлеченное сообщение: Информация об авторском праве или метаданные, которые были внедрены и извлечены из стеганографического носителя.