Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ «Робототехника и комплексная автоматизация»

КАФЕДРА «Системы автоматизированного проектирования»

РАСЧЕТНО-ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ

НА ТЕМУ:

Разработка устойчивого метода стеганографии изображений для скрытой передачи данных в социальных сетях

Студент	РК6-41М (Группа)	_____ (Подпись, дата)	А.А. Жидков (И.О.Фамилия)
Руководитель ВКР		_____ (Подпись, дата)	Т.М. Волосатова (И.О.Фамилия)
Консультант		_____ (Подпись, дата)	_____ (И.О.Фамилия)
Консультант		_____ (Подпись, дата)	_____ (И.О.Фамилия)
Нормоконтролер		_____ (Подпись, дата)	С.В. Грошев (И.О.Фамилия)

2025 г.

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

УТВЕРЖДАЮ
Заведующий кафедрой РК6
(Индекс)
А.П. Карпенко
(И.О.Фамилия)
«» _____ 202_ г.

З А Д А Н И Е

на выполнение выпускной квалификационной работы бакалавра

Студент группы РК6-41М

Жидков Антон Алексеевич
(фамилия, имя, отчество)

Тема квалификационной работы Разработка устойчивого метода стеганографии изображений для скрытой передачи данных в социальных сетях

Источник тематики (НИР кафедры, заказ организации и т.п.)

НИР кафедры

Тема квалификационной работы утверждена распоряжением по факультету

_____ № _____от «___» _____ 20__ г.

Часть 1. Исследовательская

Исследовать методы защиты информации. Рассмотреть методы стеганографии, современных методов шифрования. Рассмотреть методы текстовой стеганографии и методов стеганографии изображений, изучить реализацию методов стеганографии изображений. Изучить методы, применяемые при стегоанализе, устойчивость методов стеганографии к стегоанализу, применение систем искусственного интеллекта в стегоанализе и стеганографии.

Часть 2. Конструкторская

Часть 3.

Оформление квалификационной работы:

Расчетно-пояснительная записка на 88 листах формата А4.

Перечень графического (иллюстративного) материала (чертежи, плакаты, слайды и т.п.)

Титульный слайд, слайд целей работы, слайд постановки задачи, слайд влияния разброса начальной скорости, слайд определения начальной скорости по временным отчётам, слайд определения начальной скорости по двум временным отчётам, слайд модели магнитного поля одиночного магнита, слайд модели магнитного поля кольца магнитов, слайд исследования зависимости напряжения датчика Холла, слайд магнитного поля кольца магнитов, слайд модели показаний датчика Холла, слайд исследования алгоритма определения начальной скорости, слайд разработки схемы электрической структурной слайд схемы электрической принципиальной, слайд чертежа платы, слайд сборочного чертежа, слайд заключения

Дата выдачи задания « 23 » ноября 2022 г.

В соответствии с учебным планом выпускную квалификационную работу выполнить в полном объеме в срок до « 08 » июня 2023 г.

Руководитель квалификационной работы _____ Т.М Волосатова
(Подпись, дата) (И.О.Фамилия)

Студент _____ А.А Жидков
(Подпись, дата) (И.О.Фамилия)

Примечание:

1. Задание оформляется в двух экземплярах: один выдается студенту, второй хранится на кафедре.

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ РК УТВЕРЖДАЮ

КАФЕДРА РК6 Заведующий кафедрой РК6
(Индекс)

ГРУППА РК6-41М А. П. Карпенко
(И.О.Фамилия)

« » ___ 202_ г.

КАЛЕНДАРНЫЙ ПЛАН
выполнения выпускной квалификационной работы

студента: Жидкова Антона Алексеевича
(фамилия, имя, отчество)

Тема квалификационной работы: дистанционная автономная информационная управляющая система с корректировкой времени

№ п/п	Наименование этапов выпускной квалификационной работы	Сроки выполнения этапов		Отметка о выполнении	
		план	факт	Должность	ФИО, подпись
1.	Задание на выполнение работы. Формулирование проблемы, цели и задач работы	23.11.22г. Планируемая дата		Руководитель ВКР	Волосатова Т.М.
2.	1 часть. Исследовательская	10.05.23г. Планируемая дата		Руководитель ВКР	Волосатова Т.М.
3.	Утверждение окончательных формулировок решаемой проблемы, цели работы и перечня задач	01.05.23г. Планируемая дата		Заведующий кафедрой	Карпенко А.П.
4.	2 часть. Конструкторская	15.05.23г. Планируемая дата		Руководитель ВКР	Волосатова Т.М.
5.	3 часть _____	_____ Планируемая дата		Руководитель ВКР	Волосатова Т.М.
6.	1-я редакция работы	20.05.23г. Планируемая дата		Руководитель ВКР	Волосатова Т.М.
7.	Подготовка доклада и презентации	25.05.23г. Планируемая дата			
8.	Заключение руководителя	28.05.23г. Планируемая дата		Руководитель ВКР	Волосатова Т.М.
9.	Допуск работы к защите на ГЭК (нормоконтроль)	08.06.23г. Планируемая дата		Нормоконтролер	Грошев С.В.
10.	Внешняя рецензия	_____ Планируемая дата			
11.	Защита работы на ГЭК	20.06.23г. Планируемая дата			

Студент _____ _____
(подпись, дата)

Руководитель работы _____
(подпись, дата)

РЕФЕРАТ

Расчетно-пояснительная записка содержит 88 с., 48 рис., 4 табл., 10 источников, 4 приложения.

СТЕГАНОГРАФИЯ, СОЦИАЛЬНЫЕ СЕТИ, КОНФИДЕНЦИАЛЬНАЯ СВЯЗЬ, СТЕГОАНАЛИЗ, ГЛУБОКОЕ ОБУЧЕНИЕ, ЗАЩИТА ДАННЫХ.

Объект исследования – стеганографические методы передачи информации через изображения в условиях цензуры и ограничений интернета.

Цель выпускной квалификационной работы – разработка и анализ методов стеганографии изображений для обеспечения конфиденциальной связи в цифровых каналах передачи информации.

Методы проведения исследования – анализ существующих алгоритмов стеганографии, моделирование процессов внедрения и извлечения скрытых данных, тестирование устойчивости к сжатию изображений в социальных сетях, применение методов машинного обучения для выявления скрытой информации (стегоанализ).

Основные результаты выпускной квалификационной работы:

а) проведен обзор существующих методов стеганографии и их применимость в условиях социальных сетей;
б) исследована эффективность методов стеганографии в условиях потерь при компрессии изображений (JPEG, WebP);
в) разработан и протестирован алгоритм стеганографии, устойчивый к обработке в социальных сетях;
г) проведен анализ устойчивости разработанного метода к стегоанализу, включая машинное обучение;
д) предложены рекомендации по защите скрытых данных от автоматического обнаружения алгоритмами социальных платформ;
е) разработан программный модуль для автоматизированного внедрения и извлечения скрытых сообщений из изображений.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность работы

В современных условиях цифрового контроля и цензуры пользователи сталкиваются с ограничениями при передаче конфиденциальной информации. Традиционные методы шифрования, такие как PGP и VPN, могут привлекать внимание систем мониторинга трафика, что делает их неэффективными в условиях жестких ограничений. В этом контексте стеганография изображений предоставляет уникальный способ скрытой передачи данных, маскируя информацию внутри цифровых изображений. Особенно актуальной является передача скрытых сообщений через социальные сети, поскольку изображения являются распространенным типом контента, подвергающимся компрессии и обработке. Разработка устойчивых к таким изменениям методов стеганографии является важной задачей для обеспечения конфиденциальности цифровой коммуникации.

Цель работы – разработать устойчивый метод стеганографии изображений для скрытой передачи сообщений через социальные сети, сохраняющий скрытые данные после компрессии и обработки изображений.

Задачи, решаемые в работе:

а) исследовать существующие методы стеганографии изображений и их применимость в условиях социальных сетей;
б) разработать алгоритм внедрения данных, устойчивый к сжатию и обработке изображений;
в) провести анализ устойчивости метода к стегоанализу, включая машинное обучение;
г) протестировать работоспособность метода на различных платформах социальных сетей;
д) разработать программный модуль для автоматизированного внедрения и извлечения скрытых данных из изображений.

Объект исследования – методы стеганографии изображений и их применимость для передачи скрытых сообщений в условиях цензуры и сетевых ограничений.

Предмет исследования – алгоритмы встраивания и извлечения скрытых данных, устойчивых к компрессии и детектированию в социальных сетях.

Научная новизна

Разработан новый алгоритм стеганографии изображений, устойчивый к компрессии и алгоритмам обработки в социальных сетях. Проведено исследование устойчивости метода к современным методам стегоанализа, включая машинное обучение. Предложены методы защиты скрытых данных от обнаружения.

Практическая значимость

Разработанный метод может быть использован для защиты информации в условиях жесткой цензуры, а также для безопасного обмена конфиденциальными данными в цифровых платформах. Полученные результаты могут применяться в кибербезопасности, журналистике и защите прав человека.

Методы исследования:

1. Исследовательская часть

1.1. Исследование проблем и методов защиты данных.

Защита данных обеспечивает их безопасность, целостность и доступность, охватывая комплекс мер по сохранению информации и поддержанию стабильности операций. Основные технологии в этой сфере направлены на обеспечение непрерывного доступа к данным, а также на оптимизацию их администрирования. Гарантированная доступность данных позволяет бизнес-процессам функционировать даже в условиях деградации инфраструктуры или потери информации.

Эффективная защита данных основывается на управлении их жизненным циклом, что включает автоматизацию процессов передачи, резервного копирования и восстановления данных, а также защиту от сбоев, вредоносного ПО, кибератак и отказов оборудования. В условиях цифровой трансформации обеспечение конфиденциальности и безопасности информации становится критически важной задачей как для частных лиц, так и для организаций. Однако в данной области существует ряд вызовов, требующих особого внимания.

1. Рост частоты утечек и кибератак.

   Несанкционированный доступ к данным приводит к краже личной информации, финансовым потерям и репутационному ущербу. Современные методы кибератак постоянно совершенствуются, что требует от организаций внедрения передовых средств защиты.

2. Соблюдение законодательства.

   Компании обязаны соответствовать требованиям нормативных актов, таких как GDPR (General Data Protection Regulation) (1) в ЕС, HIPAA (Health Insurance Portability and Accountability Act) в США и других законодательных норм по защите персональных данных.

3. Сложности минимизации данных.

Современные организации собирают большие объемы данных, что требует тщательной оценки их обработки в соответствии с законодательными и этическими нормами.

4. Риски, связанные с использованием облачных сервисов.

   Внешние провайдеры облачных услуг и подрядчики увеличивают потенциальные угрозы безопасности. Организациям необходимо внедрять надежные механизмы защиты данных при взаимодействии с третьими сторонами.

5. Права пользователей на управление своими данными.

   Компании должны обеспечивать пользователям возможность контролировать обработку их данных, в том числе давать согласие или отзывать его, что влечет за собой сложности в реализации эффективных механизмов управления доступом.

6. Методы защиты персональных данных.

   Основными методами обеспечения безопасности являются анонимизация, псевдонимизация и криптографические техники шифрования, препятствующие повторной идентификации персональных данных.

7. Необходимость обучения сотрудников.

   Человеческий фактор остается одной из главных уязвимостей. Инвестиции в обучение персонала способствуют снижению количества ошибок, связанных с обработкой данных, и повышению общего уровня информационной безопасности.

8. Использование шифрования.

   Шифрование данных предотвращает их несанкционированное прочтение путем преобразования в зашифрованный формат с использованием криптографических алгоритмов. Оно также обеспечивает целостность информации, позволяя обнаруживать любые попытки изменения данных.

9. Стеганография как средство защиты данных.

   Стеганография позволяет скрывать информацию внутри цифровых объектов, снижая вероятность ее обнаружения злоумышленниками. Эта технология широко применяется в военной сфере, цифровой криминалистике и системах кибербезопасности.

Стеганография — это скрытая связь: Техники стеганографии позволяют скрытую передачу конфиденциальной информации, снижая подозрения и обеспечивая конфиденциальность за счет минимизации обнаружения непредназначенными получателями или подслушивающими. Защита через окклюзию: Стеганография усиливает безопасность, скрывая информацию, делая ее необнаружимой при перехвате, тем самым защищая от несанкционированного вторжения. Техники стеганографии критически важны для сохранения безопасности информации, защиты чувствительных данных и конфиденциальности, и используются в военных коммуникациях, кибербезопасности, цифровой криминалистике и повседневной цифровой связи.

Криптографические алгоритмы кодируют и декодируют данные, преобразуя открытый текст в зашифрованный текст с помощью ключа. Различные способы шифрования показаны на рисунке 1.

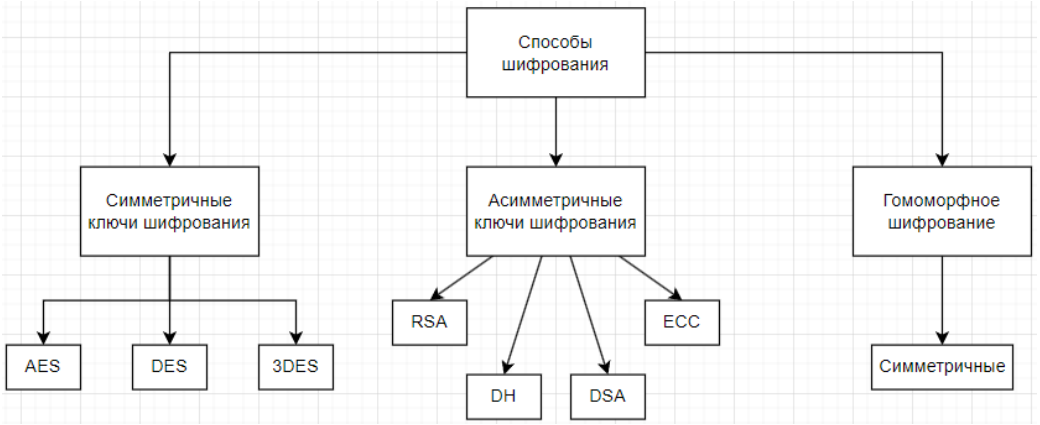

Рисунок 1 – способы шифрования

1.1.1 Симметричные ключи шифрования.

Существует множество типов симметричного шифрования, которые показаны ниже. Алгоритмы симметричного ключа — это методы шифрования, которые используют один и тот же секретный ключ как для шифрования, так и для дешифрования (2).

1. Расширенный стандарт шифрования (AES): Правительство США стандартизировало AES в 2001 году, технологию шифрования блочного шифра с размерами ключей 128, 192 и 256 бит, известную своей высокой безопасностью шифрования данных (3).

2. Стандарт шифрования данных (DES), популярный метод шифрования блочного шифра 1970-х и 1980-х годов, использует 64-битные блоки и 56-битный ключ, но сейчас менее рекомендуемый из-за небольшого размера ключа (4).

3. Стандарт тройного шифрования данных (3DES), улучшенная версия DES, в которой используется три последовательных шифрования с разными ключами, что повышает безопасность. Несмотря на это, 3DES все еще используется в устаревших системах и постепенно вытесняется более современными алгоритмами (5).

4. Метод шифрования Twofish, блочный шифр, заменяющий алгоритм Blowfish, поддерживает размеры ключей до 256 бит, сохраняя при этом

фиксированный размер блока в 128 бит, предлагая надежные меры безопасности (6).

5. Симметричное шифрование, ключ к выявлению сильных и слабых сторон. Широко используемый метод симметричного шифрования ключа заключается в использовании одного и того же ключа для операций шифрования и дешифрования, с сильными и слабыми сторонами.

Сильные стороны:

1. Процесс шифрования с симметричным ключом, как правило, быстрее, чем процесс шифрования с асимметричным ключом, поскольку он использует один ключ для шифрования и дешифрования.
2. Шифрование с симметричным ключом является одним из самых простых в использовании типов шифрования из-за простоты его реализации и управления, используя один ключ как для операций дешифрования, так и для операций шифрования.
3. Метод шифрования с симметричным ключом более эффективен из-за его расширенного использования вычислительной эффективности и ресурсов по сравнению с шифрованием с асимметричным ключом.
4. Шифрование с симметричным ключом является надежным способом защиты конфиденциальной информации в области безопасности данных, но только при условии, что оно используется эффективно, разумно и с надежным и сильным ключом.

Слабые стороны:

1. Крайне важно распределять ключи для безопасной связи в процессе шифрования с симметричным ключом, потому что непрерывность связи эффективно поддерживается с помощью небезопасных средств, и это может создавать проблемы.

2. Поддержание безопасности ключей очень важно для шифрования с симметричным ключом, поскольку стало возможным, что скомпрометированный ключ может поставить под угрозу безопасность зашифрованных данных.
3. Ограничения шифрования с симметричным ключом включают невозможность отказа, что затрудняет определение отправителя сообщения.
4. Процесс расширения шифрования с симметричным ключом из-за сложности управления им ограничен, и распространение многих ключей также ограничено, и это может создавать проблемы при разработке системы для включения более крупных и более широких сетей или систем.

Симметричная криптография с ключом — это эффективный, быстрый, простой и подходящий метод управления ключами и их распределения, но он не подходит в случаях безотказности или масштабируемости.

1.1.2 Шифрование асимметричным ключом

Алгоритмы с открытым ключом, также известные как алгоритмы с асимметричным ключом, используют два различных ключа для расшифровки и шифрования и широко используются в различных областях.

1. RSA, разработанный Шамиром, Ривестом и Адлеманом в 1977 году, является известным методом криптографии с открытым ключом, который использует большие простые числа для создания пар ключей и поддерживает размеры ключей до 4096 бит (7).
2. Криптография на эллиптических кривых (ECC) — это современный метод шифрования с открытым ключом, который отличается высокой эффективностью и скоростью. Благодаря использованию более коротких длин ключей, ECC особенно популярен в мобильных и встроенных устройствах (8).

3. Протокол Диффи-Хеллмана (DH) является безопасным криптографическим методом, используемым для обмена ключами между сторонами, позволяющим взаимно согласованные секретные ключи без физического обмена (4).

4. Алгоритм цифровой подписи (DSA) — это схема шифрования с открытым ключом, используемая для генерации цифровых подписей, обеспечивающая двойную функциональность шифрования и генерацию цифровой подписи наряду с другими методами (9).

Популярные алгоритмы асимметричного ключа учитывают безопасность, размер, скорость, совместимость и проблемы управления и распределения ключей при выборе, обеспечении безопасности, совместимости с существующими системами и скорости.

Сильные и слабые стороны асимметричного шифрования. Асимметричное шифровани, также известное как шифрование с открытым ключом, является широко используемым методом, который использует два различных ключа для шифрования и расшифровки.

Сильные стороны:

1. Асимметричное шифрование ключа упрощает проблемы распределения ключей, используя открытый ключ каждой стороны, участвующей в шифровании, и закрытый ключ для расшифровки.

2. Использование асимметричного ключа шифрования облегчает достижение безотказности, следовательно, упрощая процесс установления личности отправителя сообщения.

3. Шифрование с асимметричным ключом обеспечивает масштабируемость, что делает его идеальным для юридических контекстов, поскольку не требует множественного распределения ключей.

4. Использование шифрования с асимметричным ключом может обеспечить высокую степень безопасности для защищенной информации, если оно реализовано правильно и с продуманными, надежными ключами.

Слабые стороны:

1. Шифрование с асимметричным ключом медленнее, чем шифрование с симметричным ключом. Это связано с тем, что для шифрования и дешифрования используются два отдельных ключа.
2. Из-за использования двух разных ключей и необходимости управления ключами шифрование с асимметричным ключом становится более сложным (10).
3. Поддержание безопасности ключей требует шифрования с асимметричным ключом в виде точных ключей. Если закрытый ключ утерян или украден, безопасность зашифрованных данных также будет скомпрометирована.
4. Требует больших размеров ключей, чем шифрование с симметричным ключом, что затрудняет его использование на маломощных устройствах.

Преимущества шифрования с асимметричным ключом заключаются в распределении ключей, безотказности и масштабируемости, а недостатки в том, что оно может стать более сложным и медленным, и требует тщательного управления ключами для обеспечения безопасности.

1.1.3 Гомоморфное шифрование

Симметричное шифрование основано на базовых концепциях, которые позволяют выполнять математические операции над зашифрованными данными без необходимости их расшифровки. Это свойство, известное как гомоморфное шифрование, позволяет производить вычисления над шифротекстом, получая

результат, эквивалентный тому, что был бы получен при работе с открытым текстом (11).

- Симметричный алгоритм используется для шифрования данных, делая шифротекст нечитаемым без ключа расшифровки. Это обеспечивает высокий уровень конфиденциальности данных.
- Вторым основным элементом является вычисление, которое выполняет математические операции над зашифрованными данными без необходимости их расшифровки. Это сохраняет шифрование и приводит к зашифрованным результатам.
- Третий и последний принцип симметричного шифрования — расшифровка, которая позволяет расшифровать зашифрованный результат с использованием ключа расшифровки, чтобы получить тот же результат, что и открытый текст.

Одной из характеристик симметричного шифрования является то, что он обеспечивает надежную конфиденциальность и безопасность данных, позволяя выполнять вычисления над конфиденциальными данными, хранящимися в облаке и в защищенных приложениях обмена сообщениями, и это работает для обеспечения конфиденциальности и конфиденциальности данных без раскрытия информации.

Гомоморфное шифрование — это безопасный метод, который позволяет выполнять математические операции над зашифрованными данными без необходимости предварительной расшифровки, при этом подчеркивая различные приложения и ограничения.

1. Облачные вычисления используют методы гомоморфного шифрования для безопасной обработки конфиденциальных данных, обеспечивая конфиденциальность и предоставляя финансовые выгоды отдельным лицам и организациям.

2. Гомоморфное шифрование позволяет выполнять вычисления над зашифрованными данными, позволяя проверять конфиденциальную информацию, сохраняя конфиденциальность данных.
3. Гомоморфное шифрование используется в безопасных приложениях обмена сообщениями для выполнения вычислений над зашифрованными сообщениями, сохраняя содержимое нераскрытым только предполагаемому получателю.

Гомоморфное шифрование выгодно в финансовых приложениях, особенно в онлайн-банкинге, поскольку оно позволяет выполнять вычисления над зашифрованными данными, защищая их от несанкционированного доступа или раскрытия.

Ограничения:

1. Вычислительная сложность гомоморфного шифрования может привести к увеличению времени обработки зашифрованных данных, что потенциально создает ограничения в сценариях реального времени.
2. Безопасность гомоморфного шифрования основана на тщательной практике управления ключами, но может быть скомпрометирована, если закрытый ключ получен незаконным путем.
3. Гомоморфное шифрование, относительно новая технология, в настоящее время имеет ограничения в своей полезности по сравнению с традиционными методами шифрования.
4. Гомоморфное шифрование, в отличие от стандартных методов, требует больших размеров ключей, что может создавать проблемы, особенно при работе с маломощными устройствами.

Гомоморфное шифрование — это надежный метод шифрования с потенциальными приложениями в секторах целостности данных и

конфиденциальности, но его реализация требует учета его ограничений и недостатков (12).

1.2. Исследование методов стеганографии.

Стеганография Стеганография — это метод сокрытия информации внутри другого сообщения или элемента, такого как текст, изображения, видео или аудио, чтобы избежать обнаружения. Скрытая информация может быть извлечена только в предполагаемом месте назначения. Различные методы стеганографии проиллюстрированы на рисунке 2.

Рисунок 2 – методы стеганографии

1.2.1 Замена LSB (наименьшего значимого бита).

Основная концепция метода LSB (Least Significant Bit) заключается в замене наименее значимых битов изображения-носителя на биты конфиденциальной информации. Этот подход широко используется благодаря своей простоте и эффективности (13).

Стеганография на основе расширенного спектра — это метод, используемый для сокрытия конфиденциальной информации путем ее распределения в широком диапазоне частот, как правило, в аудио-, графических или видеофайлах с помощью модуляции.

1. Модуляция с расширенным спектром — это использует псевдослучайный шаблон шума для распределения энергии сигнала в

широком диапазоне частот, что обеспечивает высокий уровень конфиденциальности.

2. Расширение спектра прямой последовательности (DSSS) — расширяет полосу пропускания сигнала, умножая его на псевдослучайную шумовую последовательность, что делает сигнал более устойчивым к помехам.

3. Стеганография с расширенным спектром со скачкообразной перестройкой частоты (FHSS) на основе спектра изменяет сигнал таким образом, что он выглядит как псевдослучайная последовательность. Это затрудняет взлом, делает его безопасны.

4. Ограничения спектральной стеганографии включают необходимость высокого отношения сигнал/шум, использование секретного ключа и ограниченная возможность скрывать данные в носителях с высокой степенью защиты.

Стеганография на основе расширенного спектра обеспечивает высокий уровень безопасности, но имеет свои ограничения, которые необходимо учитывать при её реализации.

Эффективность:

1. Благодаря широкому распространению и сложности обнаружения спектральная стеганография обеспечивает высокую безопасность, что затрудняет для злоумышленников различение защитных носителей и стеганографических данных (10).

2. Стеганография устойчива к таким атакам, как сжатие, визуальный осмотр и статистический анализ, благодаря сложности обнаружения скрытых данных.

3. Из-за широкой полосы пропускания стеганография на основе расширенного спектра имеет низкую вероятность обнаружения, что

затрудняет для злоумышленников обнаружение наличия скрытых данных (10).

Ограничения:

1. В стеганографии если секретный ключ скомпрометирован, безопасность скрытых данных также будет скомпрометирована. Обусловлено использованием секретного ключа для генерации псевдослучайной последовательности, которая используется для распространения секретных данных по носителе-обложке.
2. Для того чтобы стеганография на основе спектра была эффективной, необходимо высокое отношение сигнал/шум. Если отношение сигнал/шум недостаточно, извлечение данных становится затруднительным.
3. Способность скрывать информацию в обложке ограничена.
4. Стеганография на основе расширенного спектра уязвима для методов обработки сигналов, таких как повторная выборка, сжатие и фильтрация, которые могут изменить псевдослучайную последовательность, используемую для распространения секретных данных.

Стеганография на основе расширенного спектра обеспечивает высокую безопасность и устойчивость к атакам, но имеет такие ограничения, как требование секретного ключа, высокое отношение сигнал/шум и ограниченная емкость данных.

1.2.2 Метод расширенного спектра

Стеганография на основе расширенного спектра использует метод модуляции расширенного спектра для сокрытия конфиденциальной информации в носителе, таком как аудио, изображение или видеофайл, в широкой полосе пропускания.

1. Использование псевдослучайной шумовой последовательности. Энергия сигнала распределяется по широкой полосе пропускания с

помощью псевдослучайной последовательности, что делает сигнал менее заметным и более устойчивым к помехам (14).

2. Модуляция расширенного спектра. Метод включает расширение спектра в прямой последовательности (DSSS), где псевдослучайная последовательность используется для модуляции сигнала и его распределения по широкой полосе пропускания (15).
3. Модуляция расширенного спектра использует псевдослучайный шум для распределения энергии сигнала по широкой полосе пропускания, в то время как секретный ключ генерирует псевдослучайную последовательность для распределения конфиденциальных данных (16).
4. Расширение спектра в прямой последовательности (DSSS). В этом методе псевдослучайная последовательность модулирует сигнал, который затем распределяется по широкой полосе пропускания, что делает его устойчивым к помехам и сложным для обнаружения (17).
5. Скачкообразная перестройка частоты (FHSS). В этом методе частота сигнала изменяется в соответствии с псевдослучайной последовательностью, что обеспечивает высокую безопасность, устойчивость к атакам и низкий риск обнаружения (18).

Стеганография на основе спектра с расширением — это безопасный способ скрыть конфиденциальную информацию, распределяя ее по разным частотам, но у нее есть ограничения, которые требуют тщательного рассмотрения.

Преимущества:

1. Технологии с расширением спектра обеспечивают расширенную безопасность, распределяя сигналы по большому диапазону частот, что затрудняет их глушение или обнаружение (11).

2. Демонстрирует устойчивость к различным формам помех, таким как преднамеренные помехи, многолучевые помехи и частотно-селективное замирание.
3. Методы расширения спектра оптимизируют использование полосы пропускания, позволяя нескольким сигналам сосуществовать в одной полосе частот без помех.
4. Методы расширения спектра могут улучшить качество сигнала за счет снижения помех и воздействия шума.

Недостатки:

1. Методы расширения спектра сложнее обычных методов модуляции, требуют дополнительного оборудования и программного обеспечения.
2. Стоимость системы может увеличиться из-за дополнительного оборудования и программного обеспечения, необходимых для развертывания методов расширения спектра.
3. Методы расширения спектра потребляют больше энергии по сравнению с традиционными методами модуляции, что может быть проблемой для устройств с батарейным питанием.
4. По сравнению с некоторыми другими методами модуляции, методы расширения спектра имеют ограниченную пропускную способность для передачи данных.

Методы расширенного спектра обеспечивают высокую безопасность и помехоустойчивость, но они сложны, дороги и требуют больше энергии, что может повлиять на устройства с батарейным питанием и емкость данных.

1.2.3 Методы преобразования домена

Стеганография на основе домена преобразования использует математические методы, такие как дискретное косинусное преобразование (DCT) и дискретное вейвлет-преобразование (DWT), для сокрытия

конфиденциальной информации в носителях, таких как изображения, аудио- или видеофайлы. Эти методы преобразуют данные в частотную область, что позволяет скрывать информацию с высокой степенью безопасности и устойчивости к обработке сигналов (14).

1. Дискретное вейвлет-преобразование (DWT) является широко используемым преобразованием в стеганографии и обработке сигналов, используемым для сокрытия данных путем незаметного изменения коэффициентов носителя прикрытия (16).
2. Дискретное косинусное преобразование (DCT) — это популярный метод, используемый в стеганографии и сжатии изображений. Он эффективно скрывает данные, но уязвим к атакам статистического анализа и методам обработки сигналов, таким как обрезка или масштабирование.
3. Дискретное преобразование Фурье (DFT). DFT анализирует частотные компоненты сигналов, обеспечивая повышенную конфиденциальность и устойчивость. Однако его применение ограничено по сравнению с DCT и DWT из-за меньшей ёмкости сокрытия данных (2).
4. Модуляция индекса квантования (QIM) — это популярный метод, используемый в стеганографии на основе DCT и DWT. Он кодирует конфиденциальную информацию, обеспечивая высокую безопасность, но уязвим к атакам статистического анализа (19).

Стеганография использует методы преобразования домена, такие как DCT, DWT и DFT, причем DCT является широко используемым преобразованием в фото, видео и стеганографии.

1. DCT в стеганографии эффективно скрывает данные, но уязвимо для атак статистического анализа и методов обработки сигналов, таких как обрезка или масштабирование.

2. Дискретное вейвлет-преобразование (DWT) является широко используемым методом стеганографии и обработки сигналов, обеспечивающим безопасность и надежность при сжатии и фильтрации, но более сложным в реализации и менее эффективным при сокрытии данных.

3. Анализ DFT частотных подкомпонентов сигналов обеспечивает повышенную конфиденциальность и устойчивость, но его внедрение ограничено по сравнению с методами стеганографии на основе DCT или DWT, которые предлагают меньшие возможности сокрытия информации.

4. Методы стеганографии на основе DWT и DCT используют модуляцию индекса квантования для кодирования конфиденциальной информации, обеспечивая надежную безопасность, но уязвимы для атак статистического анализа из-за ограничений в сокрытии данных.

Стеганография использует преобразования DCT, DWT и DFT, при этом модуляция индекса квантования (QIM) является популярным методом, но подвержена атакам статистического анализа.

1.3. Исследование передовых методов шифрования

Симметричное шифрование — это метод, который использует один ключ как для шифрования, так и для дешифрования защищенных данных. Данные подвергаются многократным итерациям подстановки, транспозиции и смешивания для повышения их устойчивости к компрометации, а не шифруются только один раз.

1.3.1 Квантовое распределение ключей (QKD)

Квантовое распределение ключей (QKD) — это безопасный метод связи, использующий фотоны для представления двоичных чисел. Он позволяет двум сторонам (например, Алисе и Бобу) создавать секретный ключ, даже если

злоумышленник пытается перехватить данные. Это возможно благодаря способности обнаруживать вмешательство в квантовые состояния фотонов

Квантовое распределение ключей (QKD) обеспечивает улучшенную защиту данных и безопасность связи благодаря различным факторам, что делает его многообещающим решением для защиты данных.

1. Квантовое распределение ключей (QKD) обеспечивает надежную безопасность благодаря законам квантовой физики, гарантируя немедленное обнаружение потенциального перехвата связи, делая ее неуязвимой для различных атак.
2. QKD позволяет генерировать случайные криптографические ключи, которые периодически обновляются, что предотвращает несанкционированный доступ и повышает безопасность связи.
3. Квантовое распределение ключей (QKD) обеспечивает периодическое обновление секретного ключа, предотвращая несанкционированный доступ и делая его неэффективным для будущих целей связи.
4. Квантовое распределение ключей (QKD) имеет решающее значение в таких областях, как банковское дело, армия и здравоохранение для защиты целостности данных.

Однако существуют некоторые ограничения QKD, которые необходимо учитывать:

1. Стоимость технологии квантового распределения ключей (QKD) остается относительно высокой по сравнению с обычными методами шифрования, что создает потенциальное препятствие для ее широкого внедрения.
2. Развертывание QKD требует специализированной инфраструктуры, что создает трудности с точки зрения создания и обслуживания.

3. Одним из недостатков квантового распределения ключей (QKD) являются его ограничения по расстоянию, поскольку расстояние связи ограничивается потерями, возникающими в среде передачи.
4. Квантовое распределение ключей (QKD) — это сложная технология, которая представляет несколько технических препятствий, которые необходимо устранить. Эти проблемы в основном связаны с повышением эффективности и надежности систем QKD.

Квантовое распределение ключей (QKD) обеспечивает повышенную безопасность данных и связи, но сталкивается с финансовыми, инфраструктурными и географическими ограничениями. Несмотря на это, данная технология имеет потенциал для дальнейшего развития.

1.3.2 Полностью гомоморфное шифрование (FHE)

Полностью гомоморфное шифрование (FHE) — это криптографический метод, который позволяет выполнять вычисления над зашифрованными данными без необходимости их расшифровки. Этот подход потенциально революционизирует безопасность данных и конфиденциальность, особенно в таких областях, как облачные вычисления и машинное обучение.

FHE использует решетчатую криптографию для шифрования данных с помощью открытого ключа. Гомоморфные операции позволяют выполнять вычисления над зашифрованными данными, а результат может быть расшифрован с использованием закрытого ключа. Это обеспечивает высокий уровень безопасности, так как данные остаются зашифрованными на всех этапах обработки.

Федеративное обучение гетерогенных ансамблей (FHE) демонстрирует многочисленные возможные приложения, которые охватывают:

1. Облачные вычисления. FHE позволяет выполнять вычисления над зашифрованными данными в облаке, обеспечивая конфиденциальность и безопасность конфиденциальной информации.

2. Безопасный обмен данными. FHE обеспечивает защищённый обмен данными между несколькими сторонами, сохраняя конфиденциальность ключевой информации.

3. Машинное обучение. FHE может использоваться для выполнения математических операций над зашифрованными данными в моделях машинного обучения, что открывает новые возможности для анализа данных без ущерба для конфиденциальности.

Гомоморфное шифрование (FHE) предполагает ряд технических трудностей:

1. Вычислительные операции над зашифрованными данными, как правило, медленные и требуют ресурсов. Производительность полностью гомоморфного шифрования (FHE) требует больших вычислительных затрат.

2. Реализация полностью гомоморфного шифрования (FHE) требует глубоких знаний в области криптографии и специализированных навыков для внедрения (20).

3. Управление ключами является критически важным аспектом реализации полностью симметричного шифрования (FHE).

4. В процессе вычислений в зашифрованных данных накапливается шум, что может ухудшить их качество. Для решения этой проблемы используются методы самонастройки и оптимизации

Полностью гомоморфное шифрование (FHE) предлагает потенциал для шифрования, но проблемы сохраняются. Препятствия и прорывы в реализации FHE для широкого внедрения.

1. Благодаря достижениям в алгоритмах и методах реализации производительность полностью гомоморфного шифрования (FHE), таких как оптимизация параллельных вычислений и инструкции SIMD,

была улучшена для снижения вычислительных затрат, времени и нагрузки на ресурсы.

2. Реализация полностью гомоморфного шифрования (FHE) требует специальных знаний из-за его сложности. Был достигнут прогресс, при этом высокоуровневые API и управление ключами стали важнейшими аспектами, повышающими простоту использования для разработчиков.

3. Системы управления ключами для полностью гомоморфного шифрования (FHE) достигли значительного прогресса, используя методологии ротации ключей для безопасного администрирования криптографических ключей в течение заданного периода.

4. Полностью гомоморфное шифрование (FHE) вносит шум в зашифрованные данные, потенциально ухудшая их качество. Однако достижения в алгоритмах FHE, такие как методологии самонастройки, эффективно смягчили накопление шума, улучшив качество данных.

5. Внедрение полностью гомоморфного шифрования (FHE) является молодой технологией с ограниченными ресурсами и навыками. Консорциум по стандартизации гомоморфного шифрования (HESC) стремится установить стандартизированные руководящие принципы и протоколы для внедрения FHE.

Подводя итог, внедрение полностью гомоморфного шифрования (FHE) сталкивается с такими проблемами, как производительность, сложность и накопление шума. Однако прогресс был достигнут за счет усовершенствованных алгоритмов, методологий и стратегий управления, что привело к повышению производительности и удобства использования.

1.4. Исследование методов текстовой стеганографии

Текстовая стеганография может варьироваться от изменения форматирования существующего текста до изменения слов внутри текста и создания нового текста. Для создания понятных текстов используются

случайные последовательности символов или контекстно-свободные грамматики.

Из-за отсутствия избыточной информации, содержащейся в файлах изображений, аудио или видео, текстовая стеганография считается самой сложной. Структура текстовых документов идентична тому, что мы видим, тогда как структура других видов документов, таких как изображения, отличается от того, что мы видим. В результате мы можем скрыть информацию в таких документах, изменив структуру документа, не влияя на вывод.

Изображение или аудиофайл можно изменить способами, которые невозможно обнаружить; однако случайный читатель может пометить текстовый файл дополнительной буквой или знаком препинания. Текстовые файлы требуют меньше памяти для хранения, и они быстрее и проще в передаче, чем другие формы стеганографических технологий.

Текстовую стеганографию можно разделить на три категории: лингвистические подходы, случайная и статистическая генерация на основе формата. На рисунке 3 показан механизм текстовой стеганографии.

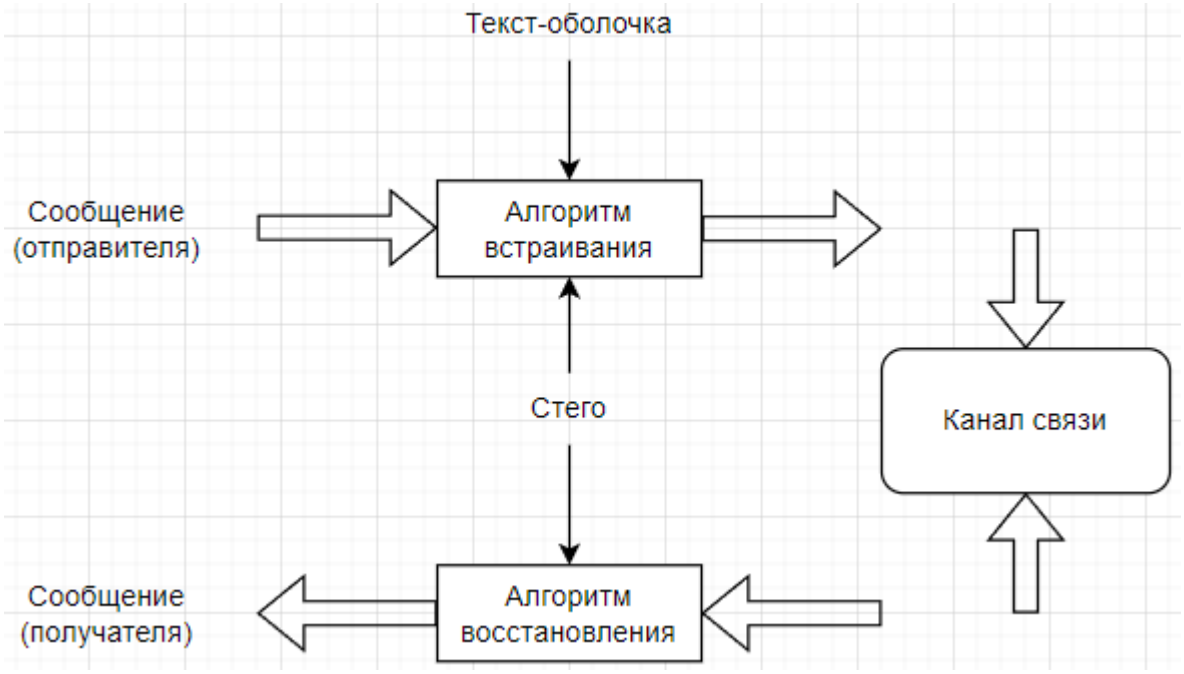

Рисунок 3 – Механизм текстовой стеганографии

1.4.1 Правописание слов

Мы используем этот процесс для сокрытия информации на английском языке. В этих процессах написание слов в американском (США) языке объясняется иначе, чем в британском (Великобритания). Приведем пример: у Organize есть другие варианты написания в Великобритании (Organise) и США (Organize). Этот процесс подходит для области, где редко используются как американские, так и британские термины. В этом процессе, если кто-то не знает метода обоих написаний, но легко обнаруживает, то наши данные скрыты.

Есть небольшая разница между написанием слов в американском и британском языках, например, в американском языке (Color) и в британском языке (Colour), небольшие изменения только в «u», которые легко обнаружить. Метод New Synonym Text является более конфиденциальным процессом, чем этот метод, поскольку в методе New Synonym мы используем различные слова, такие как (Soccer) в американском языке и (Football) в британском языке. Очевидно, что те, кто использует эти два слова как синонимы, не смогут легко понять.

1.4.2 Семантический метод

Этот процесс такой же, как и процесс написания слов. Хотя небольшое отличие заключается в том, что в этой технике мы можем использовать слова, которые являются синонимами слов, поэтому используются специальные слова, которые скрывают информацию в тексте. Это также защищенные данные (OCR) в случае применения или использования программы идентификации. У нас есть много преимуществ. Поэтому нужна самая надежная техника, потому что если у кого-то есть много приказов или команд на его языке, он может легко обнаружить скрытые данные.

1.4.3 Метод смещения строк

В этом методе строки текста перемещаются на разную величину (например, каждая строка перемещается на 1/300 дюйма вверх и вниз), и путем обнаружения идентичной формы текста информация скрывается.

Это устройство для измерения расстояния и обязательная модификация будут инициированы для устранения скрытой информации. Кроме того, если используется программа распознавания символов (OCR), напечатанные данные повреждаются. Этот метод полезен для печатного текста, поскольку OCR не используется в печатных тестах.

1.4.4 Метод сдвига слов

В этом методе конфиденциальное сообщение скрывается путем преобразования слов по горизонтали, так что справа или справа не будет отображаться небольшой 0 и 1 соответственно, а в тексте данные скрываются путем изменения расстояния между словами. Эта практика подходит для текстов, где интервал между словами не одинаков. Этот процесс можно недооценить, так как обычно интервал между словами изменяется для заполнения строки. Но если кто-то знает об алгоритмах, связанных с методом сдвига слов, он легко получит скрытые данные.

1.4.5 Синтаксический процесс

В этом процессе, изменяя некоторые знаки препинания, такие как запятая (,), точка (.), точка с запятой (;), кавычки (“) в соответствующем положении, любой может скрыть данные в текстовом файле. Требования этого процесса — идентификация соответствующих мест или вкладов. Преимущество этого метода в том, что для защиты данных практически не требуется информации. Например: в любом стихотворении или абзаце мы определяем точку (.) как 0, а запятую (,) как 1 для защиты данных в нем и отправки их пользователям.

1.4.6 Новый метод синонимического текста

В этом процессе некоторые слова с их синонимами используются для защиты секретного сообщения в текстовом файле. В методе правописания слов написание меняется очень мало, но в новой синонимической технике для одного и того же числа используются различные типы слов. Некоторые слова в английском языке имеют разные термины в Соединенных Штатах (US) и Соединенном Королевстве (UK). Например, «Movie» имеет другой термин в Великобритании как (Flim) и в США как (Movie).

Этот процесс более полезен, чем метод правописания слова, потому что в этой технике используются различные типы слов, которые нелегко понять. В технике правописания используются различные типы написания слов, например, в США (faculty) и в Великобритании (staff).

Недостатком этого метода является то, что он занимает немного времени, поскольку нам приходится искать синонимы слов и заменять их, пока не получим соответствующие результаты [4]. На рис. 3 показано несколько приемов сокрытия сообщения.

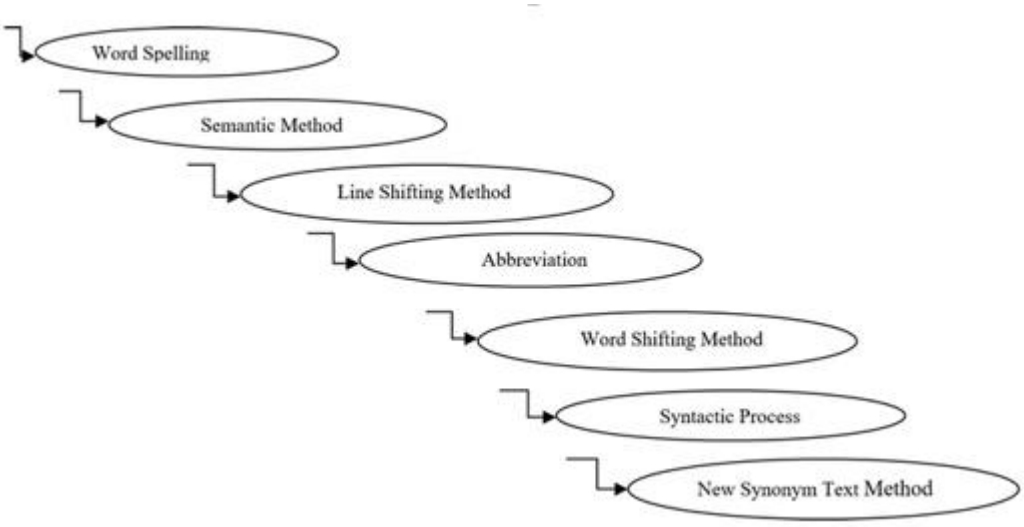

Рисунок 4

1.4.7 Механизм сокрытия текста

Поскольку читать может каждый, шифрование текста в беспристрастных предложениях вряд ли будет эффективным. В предыдущем предложении, если вы возьмете первую букву каждого слова, вы увидите, что это не невозможно и очень просто.

Существует много способов защитить информацию в текстовом файле. Алгоритм первой буквы, используемый здесь, очень ненадежен, потому что знание используемой системы автоматически раскрывает вам секрет. Недостатком является то, что существует много распространенных методов сохранения секретов в простом тексте.

Многие методы включают такие правила, как изменение порядка текста, использование каждого девятого символа или изменение количества пробелов после строк или между словами. Успешно использовался последний метод, и даже после печати и копирования текста на бумаге десять раз зашифрованное сообщение можно восстановить.

Другой эффективный способ шифрования текста — использовать общедоступный источник обложки, книгу или газету и использовать код, который содержит, например, номер строки, номер страницы, букву и номер

включения. Таким образом, никакая информация, скрытая внутри сервера, не приведет к скрытому сообщению.

Его обнаружение полностью зависит от получения знаний о секретном ключе. Сосредоточение на методе внедрения, используемом для сокрытия конфиденциальной информации в тексте обложки. Существует три основные категории текстовой стеганографии, которые являются методами на основе формата, случайной и статистической генерацией и лингвистическими методами.

1.4.8 Методы на основе формата

Физическое форматирование текста способами на основе формата используется как место для сокрытия данных. Методы на основе формата обычно редактируют существующий текст, чтобы скрыть стеганографический текст. Метод стеганографии текста на основе формата также известен как метод открытого пространства.

Взаимодействующие пробелы или невидимые символы, преднамеренное прописывание всего распределения текста и изменение размера шрифтов — вот некоторые из многих методов форматирования, используемых в текстовой стеганографии.

Некоторые из этих процессов, такие как преднамеренные орфографические ошибки и интервалы, иногда могут обмануть читателей-людей, которые игнорируют неправильные толкования, но часто могут быть легко обнаружены машиной.

1.4.9 Случайные и статистические методы

Чтобы избежать сравнения с известным простым текстом, стенографисты всегда поддерживают подготовку собственных текстов сокрытия. Хотя это часто решает проблему атаки на известное ядро, особенности подготовленного текста все еще могут вызывать подозрения, что текст является незаконным.

Такая генерация обычно пытается имитировать некоторые особенности общего текста, приближаясь к некоторым статистическим разделениям, обнаруженным в исходном тексте.

Текст может скрывать информацию от стенографии до точки зрения, которая случайным образом показывает ряд символов. Конечно, эта настройка далека от случайной как для отправителя, так и для получателя сообщения, но она должна быть случайной для всех, кто перехватывает сообщение.

Однако она не только должна быть известна случайным образом, но поскольку нас также беспокоит тот факт, что это стенографическая фраза, она не выглядит подозрительной. Случайные наборы символов, которые все попадают в один и тот же набор символов, но не имеют четкого значения, могут действительно вызвать предупреждение.

1.4.10 Кодирование признаков

Кодирование признаков имеет дело с изменением признаков текста таким образом, что значимое сообщение скрывается для создания текста-обложки. Такие признаки, как высота текста, цвет текста, шрифт текста, являются некоторыми из способов, которые используются. Большой объем информации скрывается с помощью кодирования признаков.

Когда признаки текста изменяются, то только отправитель и предполагаемый получатель обнаруживают скрытое сообщение. Третья сторона не привлекает внимание к чему-то скрытому внутри текста. Методы OCR и перепечатка ответственны за изменение признаков текста и повреждение сообщения.

1.4.11 Текстовая стеганография в языке разметки

Язык разметки — это современная система для аннотирования документа таким образом, чтобы он был синтаксически отличим от текста. Языки разметки, нечувствительные к регистру, можно легко использовать для создания скрытых смыслов. Для этой цели используется HTML. Теги html не поддерживают чувствительность к регистру. Теги, такие как
 и
, дают одинаковый

вывод, независимо от регистра, в котором они написаны. Другие теги, такие как <b>,<u> и т. д., могут использоваться для того, чтобы было больше возможностей для стеганографии в HTML. XML является чувствительным к регистру языком. Это означает, что теги, написанные в XML, зависят от заглавных букв алфавита. Для целей стеганографии в основном используется HTML. Он увеличивает диапазон, в котором отправитель использует функциональность создания секретного сообщения.

1.4.12 Последовательности слов

Проблема, возникающая в том, что обнаружение текста обложки в обычном тексте иногда не так уж и сложно. Могут быть обнаружены различные нелексические последовательности, и мощность стеганографии уменьшается. Для решения этой проблемы фактические элементы обнаружения могут использоваться для кодирования одного или нескольких бит информации на слово. Сопоставление между лексическими последовательностями и последовательностями битов может потребовать кодовой книги. Это связано с тем, что биты в текстах используются для кодирования лексического сообщения. Этот метод также имеет несколько проблем, заключающихся в том, что и человек, и компьютер могут обнаружить строку слов без семантической структуры. Аномальное поведение может привлечь злоумышленников и разрушить суть стеганографии.

1.4.13 Последовательности символов

В тексте есть несколько символов. Прелесть текстовой стеганографии заключается в том, что символы языков могут быть использованы для создания текста обложки. В методе последовательности символов генерация символов заключается в учете свойств длины слова и частоты букв для создания слов. Это придает внешнему виду те же статистические свойства, что и фактические слова в данном языке.

1.4.14 Лингвистические методы

Фактические, оригинальные элементы словаря могут использоваться для кодирования одного или нескольких битов информации в каждом слове, чтобы решить проблему идентификации небуквальной непрерывности.

Это может включать в себя кодовую книгу карты между лексическими объектами и битовыми конфигурациями или словами (длинами, буквами и т. д.), кодирующими скрытую информацию. Однако в обоих случаях есть проблема. Строка слов, не имеющая семантической диаграммы и понятной семантической связи. И люди, и компьютеры могут знать одно и то же. Этот метод требует правильной идентификации мест, куда могут быть вставлены знаки. Другой метод лингвистической стеганографии — семантический метод. В этом методе используются синонимы слов для некоторых предварительно выбранных. Слова заменяются их синонимами, чтобы скрыть в них информацию. На рисунке 5 показана классификация текстовой стеганографии.

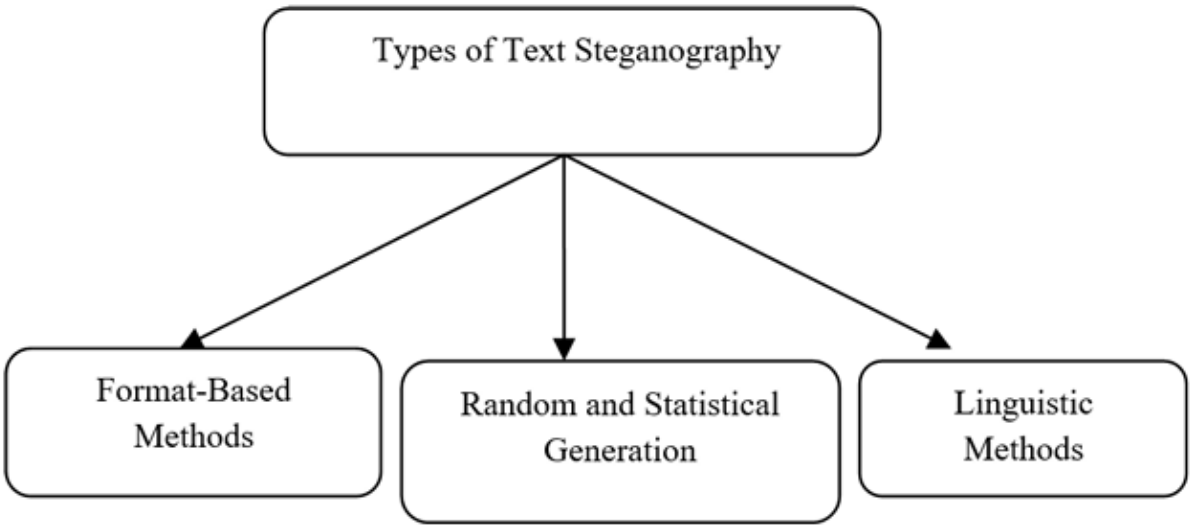

Рисунок 5 – Классификация текстовой стеганографии

1.5. Исследование методов стеганографии изображений

В стеганографии изображений используется несколько методов, каждый из которых имеет свои собственные сильные стороны и ограничения. От базовых методов, таких как замена наименее значимого бита (LSB), до более

продвинутых подходов, таких как преобразования частотной области, стеганография предлагает разнообразный набор инструментов для сокрытия информации в изображениях. Эти методы манипулируют значениями пикселей, изменяют цветовую информацию или преобразуют изображения способами, которые незаметны для наблюдателей-людей. Ограниченная чувствительность человеческого глаза к тонким изменениям делает его мощным инструментом в различных приложениях, начиная от защищенной связи и заканчивая цифровыми.

Стеганография изображений имеет несколько преимуществ по сравнению с другими формами стеганографии, что делает ее предпочтительным подходом в определенных сценариях:

a. Незаметность:

Внедрение информации в пиксели изображения, особенно с использованием методов замены LSB или частотной области, обеспечивает высокий уровень незаметности. Вносимые изменения часто незначительны и не видны при обычном визуальном осмотре.

b. Широкая применимость:

Изображения повсеместно используются в цифровой коммуникации, и стеганография изображений может применяться в различных форматах, таких как JPEG, PNG и GIF. Эта универсальность делает ее универсальным выбором для сокрытия информации.

c. Устойчивость к восприятию человеком:

Зрительная система человека менее чувствительна к небольшим изменениям в изображениях, особенно когда эти изменения происходят в менее важных компонентах, таких как наименее значимые биты или определенные частотные области. Эта устойчивость обеспечивает эффективное сокрытие.

d. Надежность:

Методы стеганографии изображений могут быть устойчивы к обычным операциям обработки изображений, сжатию и другим преобразованиям. Скрытая информация часто переживает эти процессы, сохраняя свою целостность.

e. Правдоподобное отрицание:

Поскольку изменения, внесенные в изображение-носитель, являются тонкими, злоумышленникам становится сложно доказать существование скрытой информации. Это правдоподобное отрицание является ценной функцией в сценариях, где секретность имеет решающее значение.

Подводя итог, стеганография изображений выделяется как эффективный и универсальный подход к скрытой коммуникации. Ее способность бесшовно интегрировать скрытую информацию в визуальное содержимое изображений в сочетании с ограниченной чувствительностью человеческого глаза к тонким изменениям делает ее мощным инструментом в различных приложениях, начиная от защищенной коммуникации и заканчивая цифровыми водяными знаками.

1.6. Повышение безопасности с помощью стеганографии изображений

Стеганография изображений служит инновационным и скрытым инструментом для усиления мер безопасности в цифровой связи. Благодаря бесшовному сокрытию конфиденциальной информации в, казалось бы, безобидных изображениях, этот метод обеспечивает дополнительный уровень защиты от несанкционированного доступа и обнаружения. Одно из ключевых преимуществ использования стеганографии изображений для обеспечения безопасности заключается в ее способности скрывать существование скрытых данных. В отличие от традиционных методов шифрования, которые могут привлекать внимание из-за использования определенных алгоритмов или шаблонов, стеганография действует скрытно в визуальных компонентах изображения. Эта скрытая интеграция помогает поддерживать низкий профиль

и снижает вероятность перехвата. Более того, незаметный характер стеганографически внедренных данных повышает общую безопасность, используя ограниченные способности восприятия человеческого глаза. Изменения, вносимые в изображение-носитель, часто являются тонкими и находятся в менее заметных аспектах, таких как наименее значимые биты или определенные частотные домены. Это гарантирует, что даже тщательный визуальный осмотр не выявит наличие скрытой информации. Универсальность стеганографии изображений также способствует ее роли в обеспечении безопасности. Поскольку изображения являются обычным явлением в цифровой коммуникации, этот метод может применяться на различных платформах и в различных форматах файлов, что делает его практичным и гибким вариантом для защиты различных типов данных. Кроме того, устойчивость стеганографии изображений к распространенным операциям обработки изображений, сжатию и преобразованиям повышает ее надежность как меры безопасности. Скрытая информация остается нетронутой в ходе этих процессов, сохраняя свою конфиденциальность даже в динамических цифровых средах. По сути, безопасность с помощью стеганографии изображений заключается в использовании сокрытия данных в визуальной структуре изображений для предотвращения потенциальных угроз и несанкционированного доступа. Ее сдержанный характер в сочетании со способностью легко интегрироваться в повседневную цифровую коммуникацию позиционирует стеганографию изображений как актив в повышении безопасности конфиденциальной информации. Независимо от того, применяется ли она в скрытом обмене сообщениями или для защиты цифровых активов, эта техника предлагает уникальный и эффективный подход к укреплению.

Методы стеганографии изображений.

1. Наименее значимый бит (LSB).

LSB — один из самых ранних и простых методов стеганографии. Он изменяет наименее значимые биты значений пикселей на изображении, чтобы

скрыть секретное сообщение. Простота этого метода делает его широко распространенным; однако его уязвимость к атакам и сжатию изображений ограничивает его эффективность в приложениях с высоким уровнем безопасности (Wang et al., 2012). Были предложены различные усовершенствования LSB, такие как использование случайного выбора пикселей и объединение LSB с методами шифрования для повышения безопасности (Bandyopadhyay et al., 2016).

2. Разница значений пикселей (PVD)

PVD улучшает LSB, внедряя данные на основе разницы между двумя последовательными значениями пикселей. Этот метод допускает переменную емкость внедрения данных, что делает его более устойчивым к статистическим атакам (Nguyen et al., 2015). Методы PVD были дополнительно усовершенствованы для улучшения визуального качества и емкости данных при сохранении высокого уровня безопасности (Ghosh & Ranjan, 2017).

3. Дискретное косинусное преобразование (DCT)

Стеганография DCT работает в частотной области и особенно эффективна для изображений, сжатых с помощью JPEG. Внедряя данные в частотные коэффициенты, методы DCT могут поддерживать качество изображения даже после сжатия, тем самым обеспечивая более высокую надежность (Zhang & Wang, 2018). Последние достижения в области стеганографии DCT сосредоточены на выборе оптимальных коэффициентов для внедрения данных, балансировки емкости и качества восприятия (Hussain et al., 2019).

4. Маскирование и фильтрация

Этот метод использует характеристики зрительной системы человека для сокрытия данных в сложных узорах изображения. Манипулируя пикселями таким образом, чтобы они оставались визуально незаметными, маскирование и фильтрация обеспечивают высокую емкость и точность восприятия (Peterson et

al., 2020). Однако его сложность и чувствительность к деградации изображения создают проблемы для практической реализации.

5. Методы преобразования домена

Помимо DCT, другие методы преобразования домена, такие как дискретное вейвлет-преобразование (DWT) и разложение сингулярных значений (SVD), привлекли внимание в стеганографии.

DWT особенно полезен для анализа с множественным разрешением, позволяя внедрять данные на различных уровнях детализации (Wang et al., 2021). SVD предлагает надежные возможности сокрытия данных и менее чувствителен к манипуляциям с изображениями (Huang et al., 2021).

6. Расширенный спектр (SS)

Стеганография SS встраивает данные в широком диапазоне частот, что затрудняет обнаружение скрытого сообщения злоумышленниками. Эта техника особенно эффективна в аудио- и видеофайлах и была исследована для ее применения в защищенных коммуникациях (Tavakkol et al., 2020).

7. Адаптивная стеганография

Адаптивные методы динамически корректируют процесс внедрения на основе характеристик изображения обложки, что приводит к улучшению невидимости и безопасности. Эти методы показали себя многообещающими в различных приложениях, включая защищенные цифровые водяные знаки и скрытую связь (Zhao et al., 2020).

1.7. Техники реализации стеганографии изображений

A. Наименее значимый бит (LSB)

Техника LSB работает путем изменения наименее значимого бита каждого пикселя в изображении обложки для внедрения секретных данных. Процесс выглядит следующим образом:

1. Подготовка данных: Преобразуйте секретное сообщение в двоичный формат, гарантируя, что размер сообщения не превышает емкость изображения обложки.
2. Процесс внедрения: Для каждого пикселя в изображении обложки:
   - Извлеките наименее значимый бит (LSB).
   - Замените LSB соответствующим битом секретного сообщения.
   - Сохраните измененные значения пикселей в новом изображении.
3. Процесс извлечения: Для извлечения скрытого сообщения:
   - Пройдите по пикселям стегоизображения.
   - Извлеките LSB и восстановите двоичные данные секретного сообщения.

B. Разность значений пикселей (PVD)

PVD предназначен для повышения надежности внедрения данных путем использования различий между значениями пикселей.

Включаются следующие шаги:

1. Подготовка данных: преобразование секретного сообщения в двоичный формат.
2. Процесс встраивания:
   - Вычислите абсолютную разницу между соседними парами пикселей. На основе значения разницы определите, сколько бит секретного сообщения может быть встроено:

- ▪ Для небольших различий встраивайте больше бит.
- ▪ Для больших различий встраивайте меньше бит, чтобы минимизировать искажение восприятия.

- Измените значения пикселей соответствующим образом, чтобы включить секретные биты.

3. Процесс извлечения: для извлечения скрытого сообщения:

- Проанализируйте различия между парами пикселей в стегоизображении.
- Извлеките встроенные биты на основе измененных значений пикселей.

C. Дискретное косинусное преобразование (DCT)

DCT работает в частотной области и обеспечивает надежный метод встраивания данных, особенно в сжатые изображения. Методология включает:

1. Подготовка данных: преобразование секретного сообщения в двоичный формат.
2. Процесс встраивания:

- Разделение изображения обложки на неперекрывающиеся блоки (например, 8x8 пикселей).
- Применение DCT к каждому блоку для преобразования значений пикселей в частотные коэффициенты.
- Встраивание секретного сообщения путем изменения определенных коэффициентов DCT, обеспечивающих минимальное искажение.
- Выполнение обратного DCT для реконструкции стегоизображения.

3. Процесс извлечения: для извлечения скрытого сообщения:

- Применение DCT к блокам стегоизображения.
- Извлечение измененных коэффициентов и реконструкция из них секретного сообщения.

D. Маскирование и фильтрация

Маскирование и фильтрация используют характеристики человеческого зрения для незаметного встраивания данных в изображение. Шаги:

1. Подготовка данных: преобразование секретного сообщения в двоичный формат.
2. Процесс встраивания:

- Анализ изображения обложки для определения областей, подходящих для встраивания данных на основе интенсивности и сложности пикселей.
- Измените значения пикселей в этих областях, чтобы включить секретные биты, гарантируя, что изменения останутся незаметными для человеческого глаза.

3. Процесс извлечения: для извлечения скрытого сообщения:

- Анализируйте интересующие области в стегоизображении.
- Извлекайте скрытые биты на основе изменений, внесенных в процессе встраивания.

2. Конструкторская часть

ЗАКЛЮЧЕНИЕ

Список литературы

1. **General Data Protection Regulation. [В Интернете] [Цитировано: 13 03 2025 г.] https://gdpr-info.eu/.**

2. Stallings, William. *Cryptography and Network Security: Principles and Practice.* б.м. : Pearson, 2022.

3. Daemen, J., & Rijmen, V. Probability distributions of correlation and differentials in block ciphers. *Journal of Mathematical Cryptology.* 2007 г.

4. W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory.* 1976 г., Т. 22, 6, стр. 644-654.

5. Schneier, Bruce. *Applied cryptography : protocols, algorithms, and source code in C.* б.м. : Wiley, 1996.

6. Niels Ferguson, Bruce Schneier, Tadayoshi Kohno. *Cryptography Engineering: Design Principles and Practical Applications.* б.м. : John Wiley & Sons, 2011.

7. *A method for obtaining digital signatures and public-key cryptosystems.* R. L. Rivest, A. Shamir, and L. Adleman. 2, б.м. : Association for Computing Machinery, 1978 г., Т. 21.

8. Hankerson, D. and Menezes, A.J. and Vanstone, S. *Guide to Elliptic Curve Cryptography.* б.м. : Springer New York, 2004.

9. National Institute of Standards and Technology. *Digital Signature Standard (DSS).* 2023.

10. Makhdoom, Imran & Abolhasan, Mehran & Lipman, Justin. A Comprehensive Survey of Covert Communication Techniques, Limitations and Future Challenges. *Techniques, Limitations and Future Challenges. Computers & Security. 120. 102784. 10.1016/j.cose.2022.102784.* 2022 г.

11. Rohit,Saluja, Deepak and Kumar, Suman Singh. Spread Spectrum Coded Radar for R2R Interference Mitigation in Autonomous Vehicles. *IEEE Transactions on Intelligent Transportation Systems.* 2022 г., Т. 23.

12. Yuan,Zhao, Yongli ets Cao. The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet. *IEEE Communications Reviews and Tutorials.* 2022 г., Т. 24.

13. Johnson, Neil F. and Jajodia, Sushil. Exploring steganography: Seeing the unseen. *IEEE Computer.* 1998 г., Т. 31, 2, стр. 26-34.

14. Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker. *Digital Watermarking and Steganography.* б.м. : Morgan Kaufmann, 2007.

15. Proakis, John G. *Digital Communications.* б.м. : McGraw-Hill Higher Education, 2008.

16. Fridrich, Jessica. *Steganography in Digital Media: Principles, Algorithms, and Applications.* б.м. : Cambridge University Press, 2010.

17. Torrieri, Don. *Principles of Spread-Spectrum Communication Systems.* б.м. : Springer, 2018.

18. Roger L. Peterson, Rodger E. Ziemer, David E. Borth. *Introduction to Spread-spectrum Communications.* б.м. : Prentice Hall, 1995.

19. *Cyber warfare.* Wang, H., Wang, S. 2004 г., Communications of the ACM, стр. 76-82.

20. *A new synonym text steganography.* Shirali-Shahreza, M. H., & Shirali-Shahreza, M. б.м. : International conference on intelligent information hiding and multimedia signal processing IEEE, 2008. стр. 1524-1526.