ТЕХНИЧЕСКИЕ НАУКИ

УДК 004.056.5

Исследование стеганографии как одного из методов защиты информации

Ю.К. Булгакова, А.Р. Газизов
Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация

Аннотация
Рассмотрено состояние знаний о цифровой стеганографии и её отличиях от криптографии. Отмечена растущая роль стеганографии в IoT и защите конфиденциальности. Исследуется вопрос сравнительной эффективности методов LSB, KJB и ДКП по скрытности, устойчивости и ёмкости. Выполнен теоретический анализ и сопоставление характеристик методов, рассмотрены примеры применения и инциденты. Выявлено: LSB — высокая ёмкость, низкая устойчивость; KJB — баланс; ДКП — высокая скрытность и устойчивость, меньшая ёмкость. Сделан вывод о выборе метода в зависимости от требований системы. Результаты важны для разработки стего-решений в IoT и дальнейшего стегоанализа.

Ключевые слова: стеганография, LSB, KJB, ДКП, защита информации, цифровые водяные знаки, сокрытие данных, частотные преобразования, скрытые коммуникации

Для цитирования. Булгакова Ю.К., Газизов А.Р. Исследование стеганографии как одного из методов защиты информации. *Молодой исследователь Дона.* 2026;11(1):37–41.

Study on Steganography as One of the Information Security Methods

Yulia K. Bulgakova, Andrey R. Gazizov
Don State Technical University, Rostov-on-Don, Russian Federation

Abstract
The article studies the status-quo of knowledge referring to digital steganography and its differences from cryptography. The growing role of steganography in the IoT and privacy protection was emphasized. The efficiency of LSB, KJB, and DCT methods was compared by their secrecy, stability, and capacity. Theoretical analysis of these methods and comparative analysis of their properties were carried out. Cases of their application and incidents were also studied. It was found that LSB method is attributed with high capacity and low stability; KJB method offers a balanced approach; and DCT method possesses high secrecy and stability with lower capacity. A conclusion about choosing the method depending on system requirements was drawn. The results are important for development of the steganographic solutions for the IoT and further analysis of steganography.

Keywords: steganography, LSB, KJB, DCT, information security, digital watermarking, data hiding, frequency conversions, hidden communications

For Citation. Bulgakova YuK, Gazizov AR. Study on Steganography as One of the Information Security Methods. *Young Researcher of Don*. 2026;11(1):37–41.

Введение. В условиях цифровизации особое значение приобретает обеспечение конфиденциальности информации. Помимо криптографии всё большее внимание уделяется стеганографии как методу скрытой передачи данных, особенно в контексте «Интернета вещей» (IoT), где применяются встраивания данных в цифровые объекты [1]. Стеганография позволяет скрывать не только содержание, но и сам факт передачи данных, что делает её незаменимой в условиях ограничений на использование шифрования.

Цель настоящей работы — исследование и сравнительный анализ методов цифровой стеганографии: LSB, KJB и ДКП с точки зрения трёх критериев — скрытности, устойчивости и ёмкости, а также рассмотрение их применения в современных условиях.

Задачи исследования:

– изучить теоретические основы стеганографии;

– дать классификацию и характеристику современных методов;

– сравнить методы lsb, kjb и дкп;

– проанализировать практическое применение стеганографии.

Сущность и базовые понятия стеганографии

Стеганография — метод скрытого хранения и передачи информации, обеспечивающий конфиденциальность за счёт сокрытия самого факта передачи данных. Секретное сообщение внедряют в информационный объект — контейнер, который внешне не отличается от обычного файла. Встроенное сообщение называют стегосообщением (или секретным сообщением), а контейнер, содержащий скрытые данные, — стегоконтейнером. Для корректного внедрения и извлечения стегосообщения обычно применяется дополнительная секретная информация — стегоключ [1].

К основным терминам стеганографии относятся [2]:

– сообщение — секретные данные, предназначенные для скрытой передачи;

– контейнер — исходный объект (например, цифровое изображение, аудио или текст), используемый для внедрения сообщения;

– стегоконтейнер — контейнер, содержащий внедрённое стегосообщение;

– стегоканал — канал передачи стегоконтейнера;

– стегоключ — секретная информация, необходимая для внедрения и извлечения стегосообщения.

Ключевые требования к стеганографическим системам включают незаметность внедрённой информации, устойчивость к различным атакам и внешним воздействиям (например, шумам или искажениям), а также достаточную ёмкость для передачи данных [2].

Отличия и взаимосвязь стеганографии и криптографии

Хотя стеганография и криптография решают схожие задачи — защиту информации от несанкционированного доступа — между ними существуют принципиальные различия. Криптография превращает открытый текст в нечитаемую форму — шифротекст, то есть скрывает содержание данных, но сам факт наличия зашифрованного сообщения остаётся обнаружимым [3].

Стеганография, напротив, маскирует сообщение внутри обычного объекта, такого как изображение или звук, и тем самым скрывает сам факт передачи, — при этом данные могут быть предварительно зашифрованы для повышения безопасности. Такое комбинирование методов позволяет снизить вероятность привлечения внимания злоумышленника, поскольку внешний вид файла остаётся привычным [2].

В современных киберфизических системах и IoT-устройствах использование стеганографии позволяет скрыть сам факт наличия управляющих или идентификационных данных, что выгодно отличается от применения только криптографии [4].

На практике стеганография и криптография часто применяются совместно: сообщение сначала шифруют криптографическими алгоритмами, а затем скрывают внутри цифрового носителя стеганографическим методом. Такой подход существенно повышает общую безопасность и секретность передаваемых данных [3].

В таблице 1 представлено обобщённое сравнение стеганографии и криптографии по ключевым характеристикам.

Таблица 1

Сравнение стеганографии и криптографии

Характеристика	Стеганография	Криптография
Основная цель	Скрыть факт передачи данных	Скрыть содержание данных (шифрование)
Вид полученных данных	Обычные файлы, внешне неизменные	Зашифрованные файлы, нечитаемые без ключа
Выявляемость сообщения	Низкая (сложно выявить факт передачи)	Высокая (шифротекст привлекает внимание)
Использование ключей	Необязательно, но рекомендуется	Обязательно
Устойчивость к анализу	Высокая (при грамотном внедрении)	Зависит от стойкости шифра

Таким образом, стеганография дополняет криптографию, расширяя набор методов защиты информации и предлагая решения для случаев, когда требуется не только защитить содержание сообщения, но и скрыть сам факт его существования.

Классическая и компьютерная стеганография

Исторически методы стеганографии разделяются на классические и компьютерные. К классическим относятся приёмы, использующие физические носители и традиционные способы скрытого письма — симпатические чернила, микроточки, скрытые надписи, акростихи, решётки Кардано и иные литературные техники. Общее для них — отсутствие необходимости в применении вычислительной техники и цифровых технологий [1]. Компьютерная стеганография начала развиваться с распространением вычислительных систем. Она опирается на особенности цифровых сред, используя свойства форматов файлов, структуры данных, служебных полей и файловых систем для сокрытия сообщений. Несмотря на относительную простоту внедрения, такие методы часто характеризуются ограниченной ёмкостью и могут быть выявлены при специализированном анализе [2].

Цифровая стеганография — это быстро развивающаяся область, отличающаяся внедрением секретной информации прямо в цифровые объекты (изображения, аудио- и видеофайлы, цифровые документы и сетевой трафик). По подходам к внедрению разделяются пространственные и частотные методы [2].

Пространственные методы подразумевают непосредственное изменение значений отдельных элементов (например, пикселей) цифрового контейнера. Наиболее известен метод наименьших значащих битов (LSB), а также метод Куттера-Джордана-Боссена (KJB), применяющий адаптивный выбор мест для встраивания данных [3].

Частотные методы предполагают внесение информации в частотную область, в которую объект переводится с помощью математических преобразований, таких как дискретное косинусное преобразование (ДКП) или вейвлет-преобразование. Эти подходы обычно более устойчивы к внешним воздействиям, но требуют сложных вычислений и тщательного анализа [2].

Пространственные методы просты в реализации и обеспечивают большую ёмкость, однако их скрытность и устойчивость к атакам ограничены. Частотные методы требуют больше вычислительных ресурсов, но дают лучшую скрытность и стойкость к различным преобразованиям контейнера [3]. Методы на основе преобразований (в частности, ДКП) всё чаще применяются при защищённой передаче данных между компонентами IoT-систем [4].

Метод наименьших значащих битов (Least Significant Bit, LSB) — самый простой и широко распространённый пространственный метод цифровой стеганографии. Его идея заключается в замене наименее значимых битов байтов контейнера на биты скрываемого сообщения [1]. Чаще всего контейнерами служат изображения формата BMP, так как они не используют сжатие с потерями.

Ключевые особенности метода LSB:

– высокая ёмкость — до 1/8 от размера контейнера при замене одного бита в каждом байте;

– простота реализации — не требует значительных вычислительных затрат;

– недостаточная скрытность и устойчивость — метод легко выявляется статистическими методами стегоанализа, особенно при замещении более одного бита в каждом байте контейнера [1].

На практике LSB целесообразно применять в задачах, не связанных с жёсткими требованиями по устойчивости к внешним воздействиям, таким как сжатие или изменение формата файла.

Метод Куттера-Джордана-Боссена (KJB) — адаптивный пространственный подход, направленный на повышение скрытности и устойчивости по сравнению с LSB. Идея — адаптивно выбирать пиксели для встраивания, опираясь на локальные характеристики изображения: яркость и стандартное отклонение в соседних областях [2].

Этапы работы метода KJB:

– изображение делят на блоки, например 8×8 пикселей;

– в каждом блоке вычисляют стандартное отклонение яркости;

– блоки с отклонением выше заданного порога считаются пригодными для внедрения;

– в выбранных блоках корректируют яркость пикселей для встраивания битов скрытого сообщения;

– преимущества метода kjb:

– повышенная скрытность за счёт выбора областей, менее чувствительных к визуальным искажениям;

– средняя устойчивость к сжатию и иным искажениям [2].

Недостатки:

– сложность подбора оптимальных параметров — порога и размера блоков;

– чувствительность к геометрическим преобразованиям — масштабированию, вращению и т.д. [2].

Метод на основе дискретного косинусного преобразования (ДКП)

Частотные методы, в частности основанные на дискретном косинусном преобразовании (ДКП), предполагают предварительное преобразование изображения в частотную область и последующее встраивание данных в частотные коэффициенты, применяемые в стандартах сжатия изображений (например, JPEG) [2].

Основные шаги метода на основе ДКП:

– исходное изображение разбивается на блоки 8×8 пикселей;

– для каждого блока вычисляют дкп и получают набор частотных коэффициентов;

– секретные данные встраивают путём незначительных изменений коэффициентов средних частот — низкие частоты слишком заметны при изменениях, высокие частоты могут быть удалены при сжатии;

– выполняют обратное дкп для получения стегоконтейнера;

– преимущества метода дкп:

– высокая устойчивость к компрессии и цифровым преобразованиям;

– хорошая скрытность внедрения данных [2].

Недостатки:

– ограниченная ёмкость по сравнению с пространственными методами;

– вычислительная сложность, обусловленная частотными преобразованиями [2];

В таблице 2 представлено краткое сравнение рассмотренных методов.

Таблица 2

Сравнение методов LSB, KJB и ДКП

Критерий	LSB	KJB	ДКП
Скрытность	Низкая (легко обнаружить при статистическом анализе)	Средняя (зависит от подбора параметров)	Высокая (сложно выявить без знания преобразования)
Ёмкость	Высокая (до 1/8 объема)	Средняя (зависит от выбора областей внедрения)	Средняя-низкая (ограничена среднечастотной областью коэффициентов)
Устойчивость	Низкая (чувствительность к любым искажениям)	Средняя (устойчив к шумам и сжатию, но неустойчив к геометрическим преобразованиям)	Высокая (хорошо выдерживает сжатие и фильтрацию)
Сложность	Низкая	Средняя	Высокая

Цифровые водяные знаки и защита интеллектуальной собственности

Одной из наиболее распространённых областей применения цифровой стеганографии являются цифровые водяные знаки. Цифровой водяной знак — это скрытая метка, внедрённая в мультимедийный объект (изображение, аудиозапись, видео или текст), которая содержит сведения об авторских правах или о происхождении контента [1].

Цифровые водяные знаки применяются для следующих задач:

– подтверждение авторства и предотвращение нелегального копирования;

– отслеживание распространения мультимедийного контента;

– проверка целостности и подлинности цифровых документов.

Основные методы реализации водяных знаков — методы, основанные на дискретном косинусном преобразовании (ДКП), а также другие частотные подходы, которые обеспечивают высокую устойчивость к различным преобразованиям, таким как сжатие, редактирование и трансляция [2].

Скрытая передача информации

Другой значимой сферой применения стеганографии является скрытая передача информации. Это особенно важно в ситуациях, когда открытое использование криптографических инструментов ограничено или невозможно по соображениям безопасности.

Примеры практического использования стеганографии в этой области включают [3]:

– незаметный обмен конфиденциальной информацией в корпоративных и государственных структурах;

– обход цензуры и сетевых фильтров, используемых в некоторых странах для контроля информации;

– обеспечение безопасных каналов связи в чрезвычайных ситуациях.

Чаще всего для скрытой передачи используются методы пространственной стеганографии (LSB и KJB), обеспечивающие достаточную ёмкость и скрытность для небольших и средних объёмов информации.

Примеры применения и инциденты

Реальные случаи применения стеганографии демонстрируют её значимость в сфере информационной безопасности. В 2010 году был широко известен случай использования стеганографии иностранными разведками для скрытого обмена данными через едва заметно изменённые изображения, размещённые в сети Интернет [3]. В последние годы зафиксировано множество примеров, когда злоумышленники применяли стеганографические приёмы для сокрытия вредоносного кода в изображениях, что значительно осложняет его обнаружение антивирусными системами [3].

В современных IoT-сетях отмечены случаи применения стеганографических методов для сокрытия управляющих команд и передачи идентификационной информации между сенсорами и облачными шлюзами. Такие приёмы могут как повышать безопасность, так и становиться каналом для скрытых атак — это требует разработки адаптивных средств стегоанализа и мониторинга [4].

Эти инциденты подчёркивают необходимость дальнейшего развития методов стегоанализа, направленных на своевременное выявление и нейтрализацию скрытых каналов передачи данных.

Заключение. В статье рассмотрены ключевые вопросы современной цифровой стеганографии: проанализированы её теоретические основы и сопоставлены конкретные методы — наименьших значащих битов (LSB), Куттера-Джордана-Боссена (KJB) и метод, основанный на дискретном косинусном преобразовании (ДКП).

Показано, что стеганография остаётся эффективным инструментом защиты информации, особенно в ситуациях, когда традиционные криптографические средства ограничены или недостаточны. Анализ методов подтвердил, что выбор конкретного подхода определяется решаемыми задачами: метод LSB обеспечивает высокую ёмкость и простоту реализации, KJB представляет собой компромисс между скрытностью и ёмкостью, а метод ДКП характеризуется повышенной устойчивостью и незаметностью при относительно невысокой ёмкости.

Практическое применение цифровой стеганографии охватывает такие области, как защита авторских прав с помощью цифровых водяных знаков, скрытая передача конфиденциальной информации, а также противодействие атакам, использующим стеганографические каналы в информационной безопасности.

Перспективные направления дальнейших исследований включают разработку более устойчивых и незаметных стеганографических алгоритмов, совершенствование методов стегоанализа, а также изучение возможностей применения стеганографии в новых областях цифровой защиты.

Таким образом, цифровая стеганография остаётся актуальной и перспективной областью исследований и практики, способной значительно повысить уровень защищённости информации в современной цифровой среде.

Список литературы

1. Федосеев В.А., Митекин В.А. *Теоретические основы стеганографии и цифровых водяных знаков.* Учебное пособие. Самара: Изд-во Самарского ун-та; 2017. 132 с.

2. Грибунин В.Г., Оков И.Н., Туринцев И.В. *Цифровая стеганография.* Учебное пособие. Москва: Солон-Пресс, 2003. 264 с.

3. Грибунин В.Г., Костюков В.Е., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. *Стеганографические системы. Критерии и методическое обеспечение.* Учебно-методическое пособие. Грибунин В.Г (ред.). Саров: ФГУП «РФЯЦ-ВНИИЭФ»; 2016. 324с.

4. Евсютин О.О., Кокурина А.С. Обзор методов встраивания информации в цифровые объекты для обеспечения безопасности в «интернете вещей». *Компьютерная оптика*. 2019;43(1):137–154.

Об авторах:

Юлия Константиновна Булгакова, студент кафедры «Информационная безопасность в вычислительных системах и сетях» Донского государственного технического университета (344003, Российская Федерация, г. Ростов-на-Дону, пл. Гагарина, 1), trubachevayu@mail.ru

Андрей Равильевич Газизов, заведующий кафедрой «Информационная безопасность в вычислительных системах и сетях» Донского государственного технического университета (344003, Российская Федерация, г. Ростов-на-Дону, пл. Гагарина, 1), gazandre@yandex.ru

Конфликт интересов: **авторы заявляют об отсутствии конфликта интересов.**

Все авторы прочитали и одобрили окончательный вариант рукописи.

About the Authors:

Yulia K. Bulgakova, Student of the Department of Information Security in Computing Systems and Networks, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, Russian Federation), trubachevayu@mail.ru

Andrey R. Gazizov, Head of the Department of Information Security in Computing Systems and Networks, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, Russian Federation), gazandre@yandex.ru

Conflict of Interest Statement: **the authors declare no conflict of interest.**

All authors have read and approved the final manuscript.