Академия логистики и транспорта

УДК На правах рукописи

**ДАЙЫРБАЕВА ЭЛЬМИРА НУРБЕККЫЗЫ**

**Разработка и исследование стеганографических алгоритмов, ориентированных на внедрение скрытой информации в изображения**

8D06254-Радиотехника, электроника и телекоммуникации

Диссертация на соискание степени

доктора философии (PhD)

Научный консультант:

PhD, ассоц. проф.

Тойгожинова А.Ж.

PhD, ассоц. проф.

Еримбетова А.С.

Зарубежный консультант:

д.т.н., доцент

Нечта И.В.

(г. Новосибирск, РФ)

Алматы -2023

**СОДЕРЖАНИЕ**

[**НОРМАТИВНЫЕ ССЫЛКИ** 3](#_Toc136042092)

[**ОПРЕДЕЛЕНИЯ** 4](#_Toc136042093)

[**ОБОЗНАЧЕНИЯ И СООКРАЩЕНИЯ** 6](#_Toc136042094)

[**ВВЕДЕНИЕ** 7](#_Toc136042095)

[1 МЕТОДЫ ВНЕДРЕНИЯ СТЕГАНОГРАФИИ И СТЕГОНАЛИЗА 14](#_Toc136042096)

[1.1 Обзор предметной области 14](#_Toc136042097)

[1.2 Обзор существующих методов внедрения данных в изображения 17](#_Toc136042098)

[1.2.1 LSB метод 18](#_Toc136042099)

[1.2.2 Алгоритм дискретного косинусного преобразования (DCT) 23](#_Toc136042100)

[1.2.3 Вейвлет –преобразование 25](#_Toc136042101)

[1.3 Практическое применение методов стеганографии 27](#_Toc136042102)

[1.4 Обзор известных методов стегоанализа 32](#_Toc136042103)

[1.4.1 RS – метод 34](#_Toc136042104)

[1.3.2 SPAM метод 36](#_Toc136042105)

[1.3.3 Метод Хи-квадрат 36](#_Toc136042106)

[1.5 Выводы по разделу 39](#_Toc136042107)

[**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ** 41](#_Toc136042108)

# **НОРМАТИВНЫЕ ССЫЛКИ**

В настоящей диссертации использованы нормативные ссылки на следующие стандарты:

# **ОПРЕДЕЛЕНИЯ**

В настоящем диссертации использованы следующие термины с соответствующими определениями:

Boosting - (усиление) [ансамблевый](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D1%81%D0%B0%D0%BC%D0%B1%D0%BB%D0%B5%D0%B2%D0%BE%D0%B5_%D0%BE%D0%B1%D1%83%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) [машинного обучения](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%88%D0%B8%D0%BD%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D1%83%D1%87%D0%B5%D0%BD%D0%B8%D0%B5), применяется главным образом для уменьшения [смещения](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D0%BB%D0%B5%D0%BC%D0%BC%D0%B0_%D1%81%D0%BC%D0%B5%D1%89%D0%B5%D0%BD%D0%B8%D1%8F%E2%80%93%D0%B4%D0%B8%D1%81%D0%BF%D0%B5%D1%80%D1%81%D0%B8%D0%B8) (погрешности оценки), а также дисперсии в [*обучении с учителем*](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%83%D1%87%D0%B5%D0%BD%D0%B8%D0%B5_%D1%81_%D1%83%D1%87%D0%B8%D1%82%D0%B5%D0%BB%D0%B5%D0%BC).

DCT - это один из наиболее распространенных методов внедрения информации в изображения.

RS – анализ основан на применении двойной статистики, полученной из пространственных корреляций в изображениях.

SPAM (Statistic-based Pixel Adjacency Model) - это метод стегоанализа, который использует статистическую модель соседних пикселей для обнаружения скрытых сообщений в мультимедийных данных.

Вейвлет (от wavelet - малая волна, пульсация, также всплеск, часто - вейвлет) - математическая функция, которая анализирует различные частотные составляющие данных.

Встроенное (скрытое) сообщение – это сообщение, встроенное в контейнер.

Гауссовский шум — это [статистический шум](https://ru.wikipedia.org/w/index.php?title=%D0%A1%D1%82%D0%B0%D1%82%D0%B8%D1%81%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D1%88%D1%83%D0%BC&action=edit&redlink=1), имеющий [плотность вероятности](https://ru.wikipedia.org/wiki/%D0%9F%D0%BB%D0%BE%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B2%D0%B5%D1%80%D0%BE%D1%8F%D1%82%D0%BD%D0%BE%D1%81%D1%82%D0%B8), равную плотности вероятности [нормального распределения](https://ru.wikipedia.org/wiki/%D0%9D%D0%BE%D1%80%D0%BC%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B5_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5), также известного как [Гауссовское](https://ru.wikipedia.org/wiki/%D0%93%D0%B0%D1%83%D1%81%D1%81%D0%BE%D0%B2%D1%81%D0%BA%D0%BE%D0%B5_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5" \o "Гауссовское распределение).

Голограмма – объёмное изображение, воспроизведённое интерференцией волн с некоторой поверхности.

Заполненный контейнер – содержащий встроенную информацию.

Интерполяция — в вычислительной математике нахождение неизвестных промежуточных значений некоторой функции, по имеющемуся дискретному набору её известных значений, определенным способом.

Контейнер – это любая информация, предназначенная для сокрытия сообщения.

Ошибка второго рода (β-ошибка, ложноотрицательное заключение) — ситуация, когда принята неверная нулевая гипотеза.

Ошибка первого рода (𝛼-ошибка, ложноположительное заключение) — ситуация, когда отвергнута верная нулевая гипотеза (об отсутствии связи между явлениями или искомого эффекта).

Пустой контейнер - это контейнер без встроенного сообщения.

[Случайный вектор](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D1%87%D0%B0%D0%B9%D0%BD%D1%8B%D0%B9_%D0%B2%D0%B5%D0%BA%D1%82%D0%BE%D1%80), имеющий многомерное нормальное распределение, называется гауссовским вектором.

Сообщение – это любая информация, подлежащая скрытой передаче. В качестве сообщения может использоваться любой вид информации: изображение, текст, аудиосигнал.

Стеганографическая система или стегосистема – это совокупность средств и методов, которые используются для формирования скрытого канала передачи информации.

Стеганография – это наука, изучающая методы секретного сообщения.

Стегоанализ – раздел стеганографии; наука о выявлении факта передачи скрытой информации в анализируемом сообщении.

Стегоконтейнер – контейнер, содержащий секретное сообщение.

Текстовый контейнер представляет собой текстовый файл, подготовленный к печати на принтере, в котором для встраивания сообщений используются небольшие изменения стандартов печати (расстояния между буквами, словами и строками, размеры букв, строк и др.).

Хи-квадрат (χ²) - это статистический метод, который используется для анализа распределения данных.

Цифровой водяной знак (Digital Watermark) — это невидимая информация, встроенная в цифровое изображение, видео или звуковой файл.

# **ОБОЗНАЧЕНИЯ И СООКРАЩЕНИЯ**

|  |  |
| --- | --- |
| DCT | Дискретное косинусное преобразование |
| GLM | Gray Level Modification (Изменение уровня серого) |
| INMI | Improved neighbor mean interpolation |
| LIBC5 | Lagrange interpolation Bezier curve 5 |
| LSB | Least Significant Bit (Наименее значимый бит) |
| NMI | Neighbor mean interpolation |
| PSNR | Peak signal-to-noise ratio (Пиковое [отношение сигнала к шуму](https://ru.wikipedia.org/wiki/%D0%9E%D1%82%D0%BD%D0%BE%D1%88%D0%B5%D0%BD%D0%B8%D0%B5_%D1%81%D0%B8%D0%B3%D0%BD%D0%B0%D0%BB/%D1%88%D1%83%D0%BC)) |
| PVD | Pixel value differencing (Разница в значениях пикселей) |
| RS | Regular–Singular (регулярно-сингулярный) |
| SPAM | Statistic-based Pixel Adjacency Model |
| АЦП | Аналого-цифровое преобразование |
| ЦАП | Цифро – аналоговый преобразование |
| ЦВЗ | Цифровой водяной знак |

# **ВВЕДЕНИЕ**

**Общая характеристика работы.** Диссертационная работа посвящена разработке эффективных методов внедрения и обнаружения скрытых данных в изображениях.

Разработка стеганографических алгоритмов – это процесс создания методов, позволяющих организовывать тайный канал связи. В качестве среды передачи используют, например, файлы, передаваемые по сети Интернет. Требуется, чтобы сам факт существования такого канала был трудно обнаружим. Одним из требований к подобным алгоритмам часто выдвигают обеспечение устойчивости к искажению обрабатываемого третьим лицом сетевого трафика, например, для изображения это масштабирование, добавление шумов и другие формы обработки изображения.

Существует множество методов и алгоритмов, используемых в стеганографии, которые основаны на различных подходах и принципах. Некоторые из них ориентированы на скрытие информации в определенных типах изображений, например, в изображениях с высоким разрешением или в видеопоследовательностях. Другие методы используют разные способы внедрения информации в изображения, например, изменение цветовых компонентов пикселей или использование маскировки.

Одним из ключевых аспектов в разработке стеганографических алгоритмов является их оценка и тестирование. Для этого используются различные критерии качества, такие как устойчивость, емкость, незаметность (скрытность) и трудоемкость внедрения. Оценка и тестирование позволяют определить эффективность алгоритма и убедиться в том, что он может быть использован для скрытия информации в конкретных практических условиях.

Исследование стеганографических алгоритмов является важным направлением в области информационной безопасности телекоммуникационных систем. Разработка новых алгоритмов и их исследование позволяют улучшить качество стеганографических методов, сделать их более надежными и защищенными от различных атак.

**Актуальность темы.**

Развитие инфокоммуникационных технологий, процессы внедрения новейших телекоммуникационных систем, формирование и развитие современного информационного сообщества определяет важность понятии стеганографии.

Тема разработки и исследования стеганографических алгоритмов, ориентированных на внедрение скрытой информации в изображения, остается актуальной и востребованной в современном информационном мире. С каждым годом объем данных, которые мы создаем и обрабатываем, становится все больше, и возрастает необходимость в защите информации от несанкционированного доступа. Стеганография является одним из инструментов для обеспечения безопасности данных, позволяя скрыть секретную информацию в ненавязчивой форме, такой как изображение.

Существующие стеганографические алгоритмы имеют свои преимущества и недостатки, и постоянно требуют доработок и совершенствований, чтобы сохранять свою эффективность и защищенность от атак. Кроме того, с развитием технологий и появлением новых методов анализа данных необходимо постоянно адаптировать стеганографические алгоритмы к новым условиям и требованиям.

Таким образом, разработка и исследование новых стеганографических алгоритмов, способных эффективно и безопасно встраивать секретную информацию в изображения, является актуальной задачей, которая имеет практическое применение в различных областях, таких как защита данных, криптография, медицина, телекоммуникации и другие.

«Стеганография» – это слово греческого происхождения, которое означает «скрытое письмо», способ передачи или хранения [информации](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F) с учётом сохранения в тайне самого факта такой передачи. Слово стеганография делится на две части: стеганография, что означает «секретный или скрытый» (где вы хотите скрыть секретные сообщения), и графика, которая означает “написание” (текст).

Главная цель стеганографии заключается в том, чтобы скрыть сам факт наличия связи с помощью встраивания сообщений в безобидные на вид объекты, которые называют контейнерами. Как правило, сообщение будет выглядеть как что-либо иное, например, как изображение, звук, текст. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её. Преимущество стеганографии над чистой криптографией состоит в том, что сообщения не привлекают к себе внимания. Сообщения, факт шифрования которых не скрыт, вызывают подозрение. Таким образом, криптография защищает содержание сообщения, а стеганография защищает сам факт наличия каких-либо скрытых посланий.

Для обеспечения безопасности канала связи, передаваемые между двумя абонентами сообщения, преобразуют так, чтобы их перехват третьим лицом был бесполезным. Обычно такие задачи решаются при помощи методов криптографии. В общем случае криптографическое преобразование сообщения происходит с участием некоторого секретного ключа, доступного только отправителю и получателю. Получение исходного сообщения из преобразованного практически невозможна без знания секретного ключа. Соответственно анализ данных, передаваемых по открытому каналу связи, не позволяет третьему лицу свободно прочитать исходное сообщение.

Когда сообщение получено, то проблема его дальнейшей защиты также является актуальной. Так, графический файл, созданный одним лицом, может быть скопирован другим лицом или незначительно изменен и далее неправомерно выдаваться как авторская собственность. Тогда возникает необходимость создавать средства, позволяющие однозначно идентифицировать автора, когда речь идет об авторском праве, или идентифицировать конечного пользователя, когда речь идет о поиске источника нелицензионных копий файла. Подобные средства разрабатываются и исследуются в рамках науки стеганографии. Стеганография изучает методы создания тайного канала связи, посредством встраивания секретных сообщений в цифровые объекты данных, называемые контейнеры. В криптографии доступ к сообщению ограничивается, если неизвестен секретный ключ, а в стеганографии скрывается сам факт существования секретного сообщения.

В сети Интернет передается огромное количество медиа контента. Большая часть этих данных является источником дохода его создателя и рассматривается как объект защиты авторского права. Учитывая легкость и нулевую стоимость воспроизводства (создания копии) любого файла, возникает потребность отслеживать траекторию его пути (от создателя до конечного потребителя, в том числе нелицензионного). Одним из самых эффективных решений данной проблемы является применение методов стеганографии, которые используют секретные сообщения, встраиваемые в файл. Такие сообщения могут либо идентифицировать автора (цифровые водяные знаки), либо конечного потребителя (цифровой отпечаток пальца).

В научных публикациях встречаются работы, направленные на создание новых методов внедрения и на создание новых методов обнаружения (стегоанализа). Последние используются для выявления фактов утечки информации, например, через служебную переписку. Таким образом, возникает острая необходимость анализа существующих методов внедрения и создания новых и эффективных методов внедрения скрытых сообщений.

Учитывая, то наиболее распространенным типом файлов, передаваемом в сети Интернет, является картинки, то в настоящее исследование ориентированного на внедрение скрытой информации в изображения. Так один из современных подходов стеганографии базируется на методах интерполяции. В частности, исследуется применение методов интерполяции для внедрения сообщения, которая, в некотором смысле, является дискретным аналогом голограммы, и обычно применяется для восстановления сигналов и изображений, подвергшихся воздействиям и приведшим к большой потере информации.

В настоящее время проводится множество исследований, по проблемам информационной безопасности. С каждым годом растет число публикаций, посвященных методам стеганографии и стегоанализа. В этом направлении науки работают многие российские и зарубежные ученые: И.Н. Оков, Б.Я. Рябко, И.В. Туринцев, А.Н. Фионов, И.В. Нечта, Р. Бергмар (R. Bergmar), К. Кашен (C. Cachin), М. Чапман (M. Chapman), Ц. Чень (J. Chen), Дж. Фридрич (J. Fridrich), и др. Автором диссертации был проведен анализ основных отечественных и зарубежных источников за более чем 10 последних лет. Список этих источников отражен в тексте диссертации. Основные работы, с которыми производилось сопоставление результатов диссертации, принадлежат таким специалистам как Ц. Чень (J. Chen), Дж. Ю (Z. Yu), Мерзлякова Е.Ю., Евсютин О.

**Данная диссертационная работа** **направлена** на создание научно-технического задела в области информационно-коммуникационных технологий и на получение новых знаний, позволяющих осуществлять анализ и эффективно работать в области стеганографии с применением интерполяции.

**Целью диссертационной работы** является создание новых и эффективных методов внедрения и обнаружения скрытых данных в изображении. Для достижения этой цели необходимо решить следующие **задачи**:

1. Изучение существующих методов стеганографии и анализ их преимуществ и недостатков. Эта задача включает в себя обзор литературы по теме, изучение основных методов стеганографии и оценку их преимуществ и недостатков.
2. Разработка новых стеганографических алгоритмов, ориентированных на внедрение секретной информации в изображения, с учетом современных требований к безопасности и эффективности. Для решения этой задачи необходимо провести теоретический анализ и выбрать оптимальный подход к разработке новых стеганографических алгоритмов, затем реализовать эти алгоритмы и провести их тестирование.
3. Исследование разработанных алгоритмов на устойчивость к атакам, а также на возможность обнаружения скрытой информации. Для решения этой задачи необходимо провести тестирование разработанных алгоритмов на различных датасетах и оценить их устойчивость к атакам, таким как изменение размера изображения, сжатие, фильтрация и другие. Также необходимо провести анализ возможности обнаружения скрытой информации с помощью стеганализа.
4. Оценка эффективности разработанных алгоритмов по сравнению с существующими методами стеганографии. Для решения этой задачи необходимо провести сравнительный анализ разработанных алгоритмов с существующими методами стеганографии и оценить их эффективность по таким критериям, как скорость внедрения, скрытность информации, устойчивость к атакам и другие.
5. Разработка программной реализации новых стеганографических алгоритмов и создание пользовательского интерфейса. Для решения этой задачи необходимо разработать программную реализацию разработанных алгоритмов, которая будет позволять пользователям внедрять секретную информацию в изображения. Также необходимо разработать удобный и интуитивно понятный пользовательский интерфейс для работы с программой.
6. Проведение экспериментальных исследований и анализ полученных результатов

**Объектом исследования** являются методы сокрытия информации в контейнерах, представляющие собой цифровые изображения, а также методы выявления наличия скрытой в таких контейнерах информации.

**Предмет исследования** являются методы оценки стойкости стеганографических систем, основанные на перестановках элементов пространства сокрытия, различные характеристики стегоконтейнеров.

**Методы исследования** – в процессе проведения исследований были использованы методы стеганографии и алгоритмы сжатия.

**Новизна работы**. Новизна и оригинальность работы заключается в том, что в ней впервые:

* Проведен обзор существующих, актуальных методов встраивания и обнаружения скрытых данных в изображения. В настоящее время нет исследований, анализирующих устойчивость подобных алгоритмов к анализу;
* Проведен стегоанализ методов INMI и базирующихся на кривой Безье, и выявлены их уязвимости.
* Разработан новый метод встраивания секретных сообщении в изображения используя кривую Безье – LIBC5 (по пяти точкам), являющийся устойчивым к лучшим современным алгоритмам стегоанализа;
* Впервые проведен сравнительный анализ алгоритмов внедрения NMI и INMI, в котором выявлена уязвимость обоих алгоритмов к RS анализу.

**Положения, выносимые на защиту**

1. Метод на основе кривой Безье является устойчивым к анализу RS и сопоставим по стойкости и ёмкости со стегосистемой способа перестановок для растровых изображений;
2. Метод INMI и базирующийся на кривой Безье являются уязвимыми к RS и SPAM анализу.
3. Метода внедрения LIBC5 является устойчивым к RS анализу.
4. Для рассматриваемых INMI и базирующийся на кривой увеличение объема встроенной информации повышает вероятность успешного стегоанализа.
5. Методы NMI и INMI уязвимы к RS анализу.

**Научно-практическая значимость работы.**

Принимая во внимание то, что наиболее распространенным типом файлов, передаваемых в сети Интернет, являются картинки, то настоящее исследование ориентировано на внедрение скрытой информации в изображения. Полученные результаты могут быть использованы в системах скрытой передачи данных по каналам связи. Предложенные алгоритмы стегоанализа могут быть реализованы на аппаратном уровне в телекоммуникационном оборудовании. Предложенные методы внедрения сообщений не увеличивают объем передаваемого трафика в сети.

**Личный вклад автора** заключается в том, что основные результаты экспериментов были получены соискателем. Постановка задач и обсуждение результатов проводились совместно с научными консультантами.

**Достоверность и обоснованность полученных результатов** подтверждаются наличием публикаций в журналах дальнего зарубежья с импакт – фактором и в изданиях, рекомендованных Комитетом по обеспечению качества в сфере образования и науки МНВО РК, и в трудах международных научных конференции ближнего и дальнего зарубежья. Экспериментальные данные, полученные в процессе выполнения работы хорошо согласуется с данными, полученными на основе нового предложенного метода.

**Апробация диссертационной работы.** Результаты, полученные в диссертационной работе опубликованы, докладывались и обсуждались:

**Публикации с импакт-фактором по базе данных Thomson Reuters или в изданиях, входящих в международную научную базу данных Scopus:**

* **Daiyrbayeva, E.;** Yerimbetova, A.; Nechta, I.; Merzlyakova, E.; Toigozhinova, A.; Turganbayev, A. A Study of the Information Embedding Method into Raster Image Based on Interpolation. J. Imaging 2022, 8, 288. <https://doi.org/10.3390/jimaging8100288>
* **Daiyrbayeva E.,** Yerimbetova A., Toigozhinova A., Maratov Z., Sambetbayeva M. Learning steganography with a strip transform. 6th International Conference on Computer Science and Engineering.UBMK-2021, 15-17.09.2021, Ankara-Turkey/ IEEE Xplore. -P.209-212.

**Публикации в изданиях, рекомендованных КОКСОНВО РК:**

* **Дайырбаева Э.Н.,** Мурзин Ф.А., Липская М.А. Скрытие информации в изображениях. Вестник КазАТК им. М. Тынышпаева №1 (112), 2020. -Б.283-290, РК, г. Алматы
* **Дайырбаева Э.Н.,** Липская М.А., Тойгожинова А.Ж. Суреттерді өңдеуде стрип-әдісті пайданалу жолдары мен нәтижелері. Вестник КазНИТУ, №5 (2020). –Б. 279-284, РК, г.Алматы
* **Дайырбаева Э.Н.,** Липская М.А., Тойгожинова А.Ж, Нугуманов Ш.Е. Сандық және компьютерлік стеганографиялардың сипаттамалары мен мүмкіншіліктеріне шолу. Вестник КазАТК №3 (114) 2020. -Б. 246-252, РК,г.Алматы
* **Дайырбаева Э.Н.,** Еримбетова А.С., Тұрғанбаев А.Ж., Тойгожинова А.Ж., Нурланбек А.Д. Интерполяция арқылы ақпараттарды жасыру жолдарына талдау. – ҚазККА хабаршысы, 2022. – №3. – С. 376-383.
* Yerimbetova A., **Daiyrbayeva E.,** Cherikbayeva L. Embedding hidden information in images based on bicubic interpolation. -Известия НАН РК. Серия информатики, (1),2023-P. 50-63

**Публикации в сборниках тезисов и докладов:**

* **Daiyrbayeva E.,** Yerimbetova A., Toigozhinova A., Maratov Z., Sambetbayeva M. Learning steganography with a strip transform. 6th International Conference on Computer Science and Engineering.UBMK-2021, 15-17.09.2021, Ankara –Turkey/ IEEE Xplore (Scopus). - P.209-212.
* **Дайырбаева Э.Н**., Еримбетова А.С. Роль метрики в обработке изображений // МНСК-2021 ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ Материалы 59-й Международной научной студенческой конференции, 12–23 апреля 2021 г., Новосибирск, РФ, - С.53
* **Дайырбаева Э.Н.** Использование RS анализа в стеганографии // МНСК-2022 ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ Материалы 60-ой Международной научной студенческой конференции. – Новосибирск, РФ, 2022. – С.9
* **Дайырбаева Э.Н.**, Еримбетова А.С. Исследование и внедрение встраивания скрытой информации в изображения на основе интерполяции // Российская конференция с международным участием РАСПРЕДЕЛЕННЫЕ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫЕ РЕСУРСЫ (DICR-2022) Сборник трудов Россия, г. Новосибирск, 5 – 8 декабря 2022 г. – С. 45-48.

Диссертационная работа частично выполнена в соответствии с планами научно-исследовательской работы (НИР): «Разработка методов и алгоритмов для многомерных данных в задачах обработки изображений и компьютерной лингвистике» 2020-2022 гг., ГФ АР 08857179.

**Публикации.** По материалам диссертационной работы опубликовано 10 работ: 5 в журналах из перечня КОКСОНВО РК для опубликования основных результатов диссертации на соискание ученой степени PhD и 1 статья в журнале дальнего зарубежья с импакт-фактором, входящих в международные информационные ресурсы Web of Science (Clarivate Analitycs, США) и Scopus (Elesiver, Нидерланды); 4 работ в материалах Международных научных конференций.

**Объем и структура диссертации.** Диссертационная работа состоит из введения, 4 разделов, заключения и списка использованных источников из ХХХ наименовании, содержит 120 страниц основного компьютерного текста, включая ХХ рисунков, ХХХ формул и ХХ таблиц.

**Свидетельства о внесении записи в Государственный реестр прав на объекты авторского права.**

* + Еримбетова А.С., **Дайырбаева Э.Н.,** Маратов Ж.С. Программа для передачи срытых данных с помощью объекта изображения. Авторское свидетельство. № 20614 от 30.09.2021 г.
  + **Дайырбаева Э.Н.,** Еримбетова А.С., Маратов Ж.С., Турганбаев А.Ж. Программа встраивания информации в цифровые изображения с применением интерполяции. Авторское свидетельство № 25573 от 28.04. 2022 г.
  + **Дайырбаева Э.Н.,** Еримбетова А.С., Турганбаев А.Ж. Программа встраивания информации в цифровые изображения с применением кривой Безье. Авторское свидетельство № 34297 от 04.04. 2023 г.

# 1 МЕТОДЫ ВНЕДРЕНИЯ СТЕГАНОГРАФИИ И СТЕГОНАЛИЗА

* 1. Обзор предметной области

Стеганография – это наука, изучающая методы скрытой передачи информации. Она включает в себя различные методы и подходы для передачи конфиденциальной информации таким образом, чтобы факт её передачи оставался незамеченным для посторонних. Для достижения этой цели стеганография использует различные техники, такие как внедрение сообщения в изображения, звуковые файлы, видео, текстовые документы, и т.д.

В современном мире, в связи с бурным резким увеличением передаваемого трафика в сети Интернет и развитием компьютерной техники невидимые чернила и бумага были заменены гораздо более универсальными и практичными контейнерами для сокрытия сообщений: цифровыми документами, изображениями, видео- и аудиофайлами. До тех пор, пока электронный документ содержит не относящуюся к восприятию или избыточную информацию, он может использоваться в качестве “прикрытия”, чтобы скрыть секретные сообщения [1-10].

Классическая задача стеганографии формулируется следующим образом. Пусть имеется два заключенных, сидящих в различных ячейках камеры: Алиса и Боб, их задача обсудить детали плана побега, но так чтобы охранник Ева не заподозрила о готовящемся побеге. Алиса может отправлять Бобу любые невинные сообщения (контейнеры) по открытому каналу связи. Ева способна проводить анализ этого контейнера. При помощи методов стеганографии Алиса встраивает секретное послание в контейнер и отправляет его Бобу. Например, она может скрыть сообщение внутри изображения, используя методы, такие как замена наименее значимых битов (LSB) или метод альфа-канала (alpha channel).

Когда Боб получает это изображение, он может использовать те же методы, чтобы извлечь и расшифровать скрытое сообщение. Ева не обладает некоторыми секретными параметрами алгоритма, что не дает ей возможности получить секретное сообщение. Даже проведя статистический анализ, Ева не способна однозначно утверждать о наличии внедрения. Таким образом, Алиса и Боб могут обмениваться секретными сообщениями без вызова подозрений у третьих лиц.

Чтобы защитить свою переписку от Евы, Алиса и Боб могут использовать различные меры. Например, они могут использовать шифрование для защиты своих сообщений перед тем, как спрятать их в данных, а затем использовать стеганографию, чтобы скрыть зашифрованные сообщения в изображении или других данных [11-15].

На рис. 1.1, изображена схема передачи секретных сообщений, описанная выше. С помощью специального алгоритма Алиса встраивает секретное сообщение в контейнер, получая стегоконтейнер, и передает его Бобу. Благодаря особенностям алгоритма стеганографии, Ева, перехватив контейнер, не сможет однозначно утверждать о наличии факта внедрения. Боб без труда извлечет и прочитает секретное сообщение. Таким образом, задача сокрытия факта передачи секретного сообщения от третьих лиц будет выполнена.

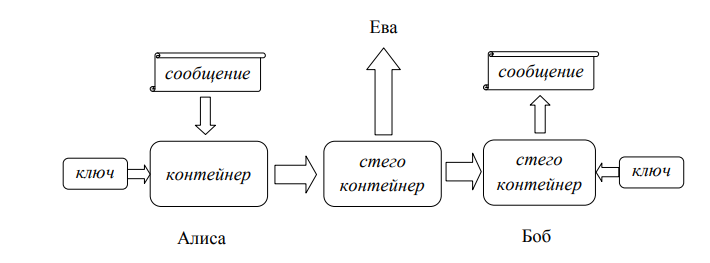


Рисунок 1.1 - Схема передачи секретного сообщения

Метод стеганографии должен предусматривать этап предварительной обработки сообщения: сжатия или шифрования, непосредственно этап внедрения и этап извлечения секретного сообщения. Согласно принципу Керкгофса стегоаналитик (Ева) заранее знает о том какой алгоритм внедрения может быть применен. Это допущение справедливо, так как большинство программ внедрения общедоступны и могут быть скачаны из Интернета. Тем не менее свойства алгоритмов таковы, что внедренное сообщение не меняет статистические свойства контейнера и Ева не может проводить стегоанализ эффективнее чем простое угадывание. В ряде случаем допускается, что Ева обладает неограниченными вычислительными возможностями. Следует отметить, что используемый контейнер не должен быть общедоступным. Например, любое изменение текста Библии будет очевидно вызывать подозрение. Таким образом в качестве контейнера возможно применение личных фотографий, которые могут иметь различное качество сжатия. Причем шумы изображения будут помогать маскировать присутствие секретного сообщения.

В настоящее время проводится множество исследований, по проблемам информационной безопасности. С каждым годом растет число публикаций, посвященных методам стеганографии и стегоанализа. В этом направлении науки работают многие российские и зарубежные ученые: И.Н. Оков, Б.Я. Рябко, И.В. Туринцев, А.Н. Фионов, И.В. Нечта, Р. Бергмар (R. Bergmar), К. Кашен (C. Cachin), М. Чапман (M. Chapman), Ц. Чень (J. Chen), Дж. Фридрич (J. Fridrich), и др.

При работе с стеганографическими системами [16-17] будут использоваться следующие основные понятия.

*Стеганографическая система* или стегосистема – это совокупность средств и методов, которые используются для формирования скрытого канала передачи информации.

*Сообщение* – это любая информация, подлежащая скрытой передаче. В качестве сообщения может использоваться любой вид информации: изображение, текст, аудиосигнал.

*Встроенное (скрытое) сообщение* – это сообщение, встроенное в контейнер.

*Контейнер* – это любая информация, предназначенная для сокрытия сообщения.

Под пустым контейнером будем понимать контейнер без встроенного сообщения. Заполненный контейнер – содержащий встроенную информацию. При выборе вида контейнера нужно обратить внимание на надёжность стегосистемы и возможность обнаружения факта передачи скрытого сообщения. По размеру (протяжённости) *контейнеры* можно разделить на два типа: потоковые и ограниченной длины.

Отличительной характеристикой потокового контейнера является то, что невозможно определить его начало и конец. В таком контейнере биты информации, используемые для скрытия сообщения, включаются в общий поток в реальном масштабе времени и выбираются с помощью специального генератора, задающего расстояния между ними. Также в этом виде контейнера самая большая трудность для получателя – определить, когда начинается скрытое сообщение.

При использовании второго вида контейнера, т.е. ограниченной длины отправитель заранее знает размер файла и может выбрать скрывающие биты в подходящей псевдослучайной последовательности. С другой стороны, такие контейнеры имеют ограниченный объём, и встраиваемое сообщение иногда может не поместиться в файл-контейнер. Другой недостаток заключается в том, что расстояния между скрывающими битами равномерно распределены между наиболее короткими и наиболее длинными заданными расстояниями, в то время как истинный случайный шум будет иметь экспоненциальное распределение длин интервала. На практике чаще всего используются контейнеры ограниченной длины как наиболее распространённые и доступные [18-20].

В зависимости от вида информации, используемой для встраивания сообщений, контейнеры могут быть визуальные, звуковые и текстовые. Визуальный контейнер представляет собой картинку или фотографию, в которой для встраивания сообщений используются небольшие изменения яркости заранее определённых точек растра изображения.

Звуковой контейнер представляет собой речевой или музыкальный сигнал, в котором для встраивания сообщений используются замена младших бит аудиосигнала на секретное сообщение, что практически не отражается на качестве звука.

Текстовый контейнер представляет собой текстовый файл, подготовленный к печати на принтере, в котором для встраивания сообщений используются небольшие изменения стандартов печати (расстояния между буквами, словами и строками, размеры букв, строк и др.).

При выборе того или иного вида контейнера необходимо иметь в виду, что при увеличении объёма встраиваемого сообщения снижается надёжность стегосистемы (при неизменном размере контейнера). Таким образом, используемый в стегосистеме контейнер накладывает ограничения на размер встраиваемого сообщения.

Задача стегоанализа [21] заключается в обнаружении факта внедрения в контейнер и оценке параметров внедрения (объём, позиция и др.). Так как внедряемое сообщение предварительно шифруют, то встраиваемое сообщение выглядит как псеводослучайная двоичная последовательность (по свойству шифра).

В настоящей работе рассматриваются существующие и новые методы внедрения и производится оценка их эффективности при помощи известных методов стегоанализа.

# 1.2 Обзор существующих методов внедрения данных в изображения

Наиболее часто передаваемым файлом по сети Интернет является изображение и видеофайлы. Видеофайл может в свою очередь рассматриваться как набор чередующихся картинок. Изображения в подавляющем числе случаев представлены в виде Jpg файла, использующим сжатие данных с потерями.

В общем случае изображение на мониторе представляет собой матрицу цветных пикселей. Цвет пикселя представлен в памяти компьютера в виде числа. Незначительно искажение такого цвета (числа) не заметно для глаза наблюдателя, что используется при внедрении. Изменение цвета может проводиться для одиночного пиксела либо для целой группы пикселей, путем снижения яркости. В первом случае возникает статистическая неоднородность (шум) картинки, которая бывает и в обычной фотографии. Во втором случае группа пикселей понижает свою яркость равномерно и создается впечатление естественной игры освещения.

Обычно информацию встраивают не в каждый возможный пиксел, а в некоторые случайно выбранные (например, не более 5% от общего числа). Такое требование возникает потому, что последние сообщение статистические выглядит случайным, а любые извлечения из картинки статистически взаимосвязаны. Поэтому выбирают случайные пикселы и встраивают туда информацию, что внешне похоже на тепловой шум матрицы фотоаппарата.

Рассмотрим наиболее распространенные методы внедрения, встречающиеся в научной литературе.

1. Least Significant Bit (LSB) [22] - один из самых простых методов стеганографии. Данные встраиваются в наименее значимый бит каждого пикселя изображения. Этот метод очень уязвим для стеганализа, так как изменение наименее значимого бита не сильно влияет на качество изображения.
2. Методы на основе стеганографических алгоритмов: Эти методы используют различные стеганографические алгоритмы для внедрения данных в изображения. Они более безопасны, чем методы, основанные на изменении младших битов, и обладают более высокой устойчивостью к атакам [23-25].
3. Masking and Filtering [26] – этот метод использует маскирование и фильтрацию, чтобы встроить данные в изображение. Изображение разбивается на блоки, и данные встраиваются в эти блоки, используя маскирование и фильтрацию.
4. Phase Coding [27] – этот метод использует фазовый кодировщик для встраивания данных в изображение. Фаза каждого пикселя изменяется на определенную величину, что позволяет внедрить данные.
5. Алгоритм разность – модификации (DM) [28] - этот метод основан на изменении значений пикселей изображения. Вместо внедрения данных в наименее значимый бит пикселя, он изменяет значения пикселей, чтобы встроить данные.
6. Алгоритм дискретного косинусного преобразования (DCT) [29]- этот метод использует дискретное косинусное преобразование для разложения изображения на компоненты частоты. Данные затем встраиваются в наименее значимые коэффициенты преобразования.
7. Вейвлет – преобразование [30] – этот метод использует вейвлет-преобразование для разложения изображения на компоненты частоты. Данные затем встраиваются в наименее значимые коэффициенты преобразования.
8. Методы на основе стеганографических алгоритмов: Эти методы используют различные стеганографические алгоритмы для внедрения данных в изображения. Они более безопасны, чем методы, основанные на изменении младших битов, и обладают более высокой устойчивостью к атакам.

Это лишь некоторые из методов внедрения данных в изображения. Каждый метод имеет свои преимущества и недостатки, и выбор метода зависит от конкретных требований [31-33].

# 1.2.1 LSB метод

Одним из самых распространенных и широко используемых методов стеганографии является метод встраивания в младшие биты (LSB). На сегодняшний день его продолжают применять для встраивания скрытых данных в цифровые изображения, фильмы и аудиозаписи [34].

Согласно алгоритму, каждый пиксель в изображении представлен битами, которые определяют цвет или яркость этого пикселя. Наименее значимый бит (LSB) содержит наименее значащую информацию и обычно не влияет на качество изображения. Именно поэтому метод LSB можно использовать для внедрения дополнительной информации, не заметной для глаза.

Внедрение данным методом может производиться в каждый канал RGB изображения. Причем все каналы равнозначны по объему и устойчивости к анализу. По этой причине исследователи в своих статьях рассматривают только черно-белые изображения (т.н. gray scale). В таком случае, во-первых, изображения становятся меньше по размеру, что упрощает обработку, и, во-вторых, делает метод внедрения универсальным: без привязки к конкретному цветовому слою.

Недостатком метода LSB является то, что он уязвим для атак стеганализа. Для обнаружения скрытых данных в изображении, необходимо проанализировать наличие изменений в наименее значимых битах. Также внедрение большого количества данных может привести к существенному снижению качества изображения.

В целом, метод LSB прост в использовании и может быть эффективным для внедрения небольшого объема данных в изображение. Он широко используется в различных приложениях [35-45], таких как внедрение водяных знаков, но для передачи большого объема данных лучше использовать более сложные методы стеганографии.

Авторы [46] представили метод LSB и предложили надежный подход к сокрытию данных с высоким уровнем безопасности, использующий обрезку изображений и стеганографию по наименьшему значащему биту (LSB). Новый подход, предложенный авторами основан на разделении секретного текстового сообщения на четыре части и извлечении четырех фрагментов из цветного изображения контейнер с определенными секретными координатами. Каждая часть сообщения встраивается в обрезку изображения с использованием предопределенной секретной последовательности. При проведении эксперимента был использован PSNR и трудоемкость, представленную в относительных единицах для сравнения с другими существующими результатами при известных методах.

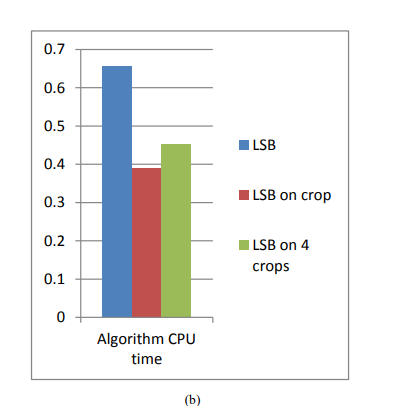
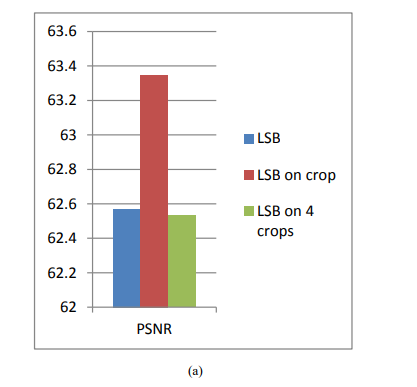


Рисунок 1.2 - (a) PSNR для изображения stego, (b) процессорное время в секундах [46]

По результатам исследований можно увидеть, что предлагаемый подход PSNR и трудоемкость находятся в пределах того же диапазона, что и другие аналогичные подходы, однако он оказался более безопасным (рис.1.2).

В статье [47] исследователи также предложили эффективный подход к стеганографии для сокрытия информации в изображении в серой шкале. Авторы в своих исследованиях сравнили новый метод с двумя более известными методами PVD и GLM. Если сравнить по количеству внедрение данных согласно таблице 1.1, тогда можно увидеть, что предложенный подход авторами позволяет внедрить больше данных, чем существующий метод GLM.

Таблица 1.1 – Размеры сообщения для внедрения [47]

|  |  |  |  |
| --- | --- | --- | --- |
| **Изображение** | **Размер изображения** | **Объем внедряемых данных** | |
| **GLM** | **PVD** |
| Lena | 128 x128 | 2048 | 2493 |
| 256 x256 | 8192 | 10007 |
| 512x512 | 32768 | 40017 |
| 1024x1024 | 131072 | 160604 |
| Baboon | 128 x128 | 2048 | 2560 |
| 256 x256 | 8192 | 10211 |
| 512x512 | 32768 | 40990 |
| 1024x1024 | 131072 | 163724 |
| Peppers | 128 x128 | 2048 | 2443 |
| 256 x256 | 8192 | 9767 |
| 512x512 | 32768 | 39034 |
| 1024x1024 | 131072 | 156308 |

Авторами PSNR был использован для оценки качества стего-изображения после встраивания секретного сообщения в контейнер. Также был применен формула для вычисления сходства методов и результатов. Экспериментальные результаты показали эффективность предложенного метода по сравнению с другими методами. С точки зрения объема данных метод PVD был лучшим после предложенного метода, а метод GLM был последним. Измерения сходства показали, что метод GLM был лучшим. Предложенный метод дал результаты, близкие к GLM, но метод PVD дал худшие результаты (рис.1.3 –рис.1.6)

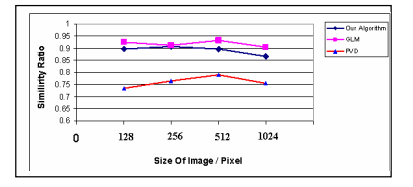


Рисунок 1.3 – Меры сходства для изображения Lena [47]

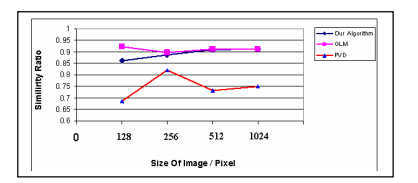


Рисунок 1.4 – Меры сходства для изображения Baboon Image [47]

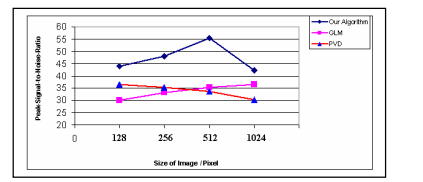


Рисунок 1.5 - PSNR для изображения Lena [47]

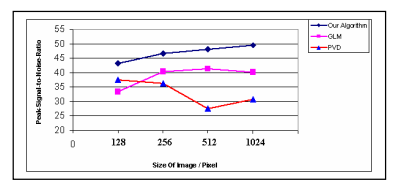


Рисунок 1.6 - PSNR для изображения Baboon Image [47]

В целом, [47] является важным вкладом в область стеганографии и может быть полезной для разработчиков, исследователей и всех, кто интересуется безопасностью и скрытым хранением информации в изображениях.

В статье [48] авторы применяют для определения и оценки длины встроенного сообщения два метода стегоанализа: RS и Хи-квадрат. Для секретной связи устойчивость стеганографии к стеганоанализу очень важна с точки зрения информационной безопасности. Также исследователями предлагается стеганографический метод обратимого преобразования гистограммы, основанный на функции LSB, для противодействия статистическому стегоанализу. Большинство начальных значений RS-атаки находятся в пределах ±6%, но некоторые начальные значения обнаружения x2 превышают 10%.

Работа [49] является одной из первых, посвященных методам внедрения данных в изображения с использованием LSB-метода. В ней описывается метод внедрения данных в изображения, по мере того, как пользователь увеличивает позицию встраиваемого бита в изображение контейнер для сокрытия зашифрованного секретного сообщения, пиковое отношение сигнал/шум (PSNR) линейно уменьшается, а качество изображения stego снижается (рис.1.7).

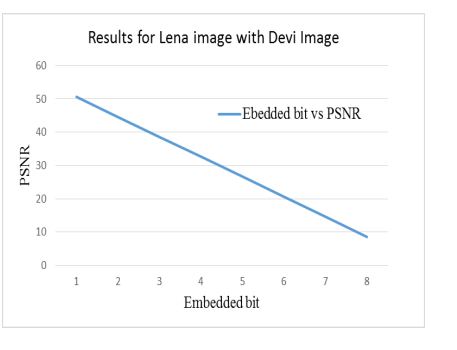


Рисунок 1.7 –Результаты эксперимента по картинке Lena [49]

В работах [50-53] представляет обзор и сравнение различных методов внедрения данных в изображения с использованием LSB – метода. В работах рассмотрены различные подходы, включая методы изменения младших битов, методы на основе стеганографических алгоритмов и методы на основе преобразования вейвлетов. Авторы демонстрируют, что предложенный метод улучшает устойчивость и безопасность метода внедрения данных.

В целом, метод LSB остается одним из наиболее популярных и широко используемых методов стеганографии, и его применение и анализ продолжаются и в настоящее время. Сделав обзор существующих работ по методу LSB можно сделать следующие выводы:

1) более ранние стеганографические схемы, которые использовали метод LSB, фокусировались на внедрении информации с помощью изменений цветов пикселей исходного изображения. Очевидно, что чем меньше внедряется информация, тем будет меньше статистических искажений контейнера и тем более безопасной (устойчивой к анализу) становится стеганографическая схема.

2) современные возможности в стегоанализе четко показывают, что внедрение информации в младшие биты с последовательным либо случайным размещением сообщения успешно обнаруживается даже для коротких сообщений (более 5% от допустимого объема внедрения).

# 1.2.2 Алгоритм дискретного косинусного преобразования (DCT)

Одним из перспективных методов стеганографии является внедрение информации в jpg изображения. Известно, что формат jpg хранит изображение как запись пространственной волны периодического сигнала. Оси абсциссы и ординаты соответствуют позиции пикселя на мониторе, а значение по оси аппликат соответствует цвету изображения. Вся картинка представляет собой набор квадратов мелких изображений 8х8. Сигнал записывается в виде коэффициентов ряда Фурье. Так как ряд Фурье бесконечный для конечных сигналов (картинок), то сохраняют только первые 64 коэффициента этого ряда.

Стеганографический метод внедрения, базирующийся на дискретном косинусном преобразовании (DCT) — это один из наиболее распространенных методов внедрения информации в изображения. Алгоритм DCT основан на расчете косинусных функций для частотных компонент изображения и преобразовании их в векторы коэффициентов, которые представляют изображения. Данные коэффициенты хранятся в матрице, которая представляет изображение.

Для внедрения информации в изображение с использованием алгоритма DCT, сначала выбирается некоторое количество коэффициентов из матрицы DCT и изменяется в соответствии с информацией, которую мы хотим скрыть. Затем производится обратное DCT-преобразование, в результате которого мы получаем измененную версию исходного изображения.

Из множества обзоров литературы за последние 10 лет, которые были проанализированы в рамках исследования, можно выделить несколько ключевых направлений и достижений, которые были получены в DCT стеганографии.

Первая группа статей [54-62] фокусировалась на исследовании производительности методов стеганографии на основе DCT. Некоторые исследователи сравнивали эффективность методов, основанных на DCT с другими методами, такими как wavelet-перобразование или descrete Fourier transform. Другие исследования включали анализ устойчивости методов на основе DCT к атакам и исследование скрытости информации.

Вторая группа статей [63-72] фокусировалась на разработке новых алгоритмов стеганографии на основе DCT. Например, некоторые исследователи предложили использовать двойное DCT для скрытия информации, что улучшило качество стеганографии по сравнению с обычным DCT. Другие исследования предложили использовать кластеризацию для определения наиболее эффективных коэффициентов DCT для скрытия информации.

Третья группа статей [73-75] была посвящена разработке алгоритмов извлечения скрытой информации на основе DCT. Некоторые исследования предложили использовать машинное обучение, чтобы повысить эффективность извлечения информации, а другие предложили использовать алгоритмы восстановления изображений для улучшения качества извлекаемой информации.

В целом, исследования за последние 10 лет показывают, что DCT продолжает быть важным инструментом в стеганографии, и его эффективность может быть улучшена с помощью новых разработок и усовершенствований. Данный метод обладает рядом преимуществ, среди которых высокая эффективность внедрения информации, низкий уровень потерь изображения и простота реализации. Однако, он также обладает и недостатками, связанными с тем, что в ряде случаев просто заметить изменения в матрице DCT, что позволяет с обнаружить скрытую информацию.

Таким образом, метод внедрения информации в изображения с использованием алгоритма DCT имеет свои преимущества и недостатки и может использоваться в рамках стеганографии для скрытой передачи информации в изображениях.

# 1.2.3 Вейвлет –преобразование

Цифровая обработка изображений продолжает развиваться и сегодня. Во многих промышленных и научно-прикладных областях существуют различные задачи цифровой обработки изображений. Многие вопросы имеют полное решение. Это относится к задачам фильтрации, сегментации, распознавания объектов на изображениях, обработки мультимедийной информации и оценки цифрового телевизионного сигнала [76,77]. Чтобы выполнить цифровую обработку изображений, необходимо преобразовать непрерывный (аналоговый) сигнал изображения в цифровую матрицу.

Это преобразование включает в себя выполнение двух преобразований. Первое преобразование — это замена реального непрерывного изображения набором выборок в дискретные моменты времени, такое преобразование называется выборкой. Второй — это преобразование непрерывного набора значений сигнала изображения в набор квантованных значений, такое преобразование называется квантованием. Основные этапы цифровой обработки изображений показаны на рис. 1.8:

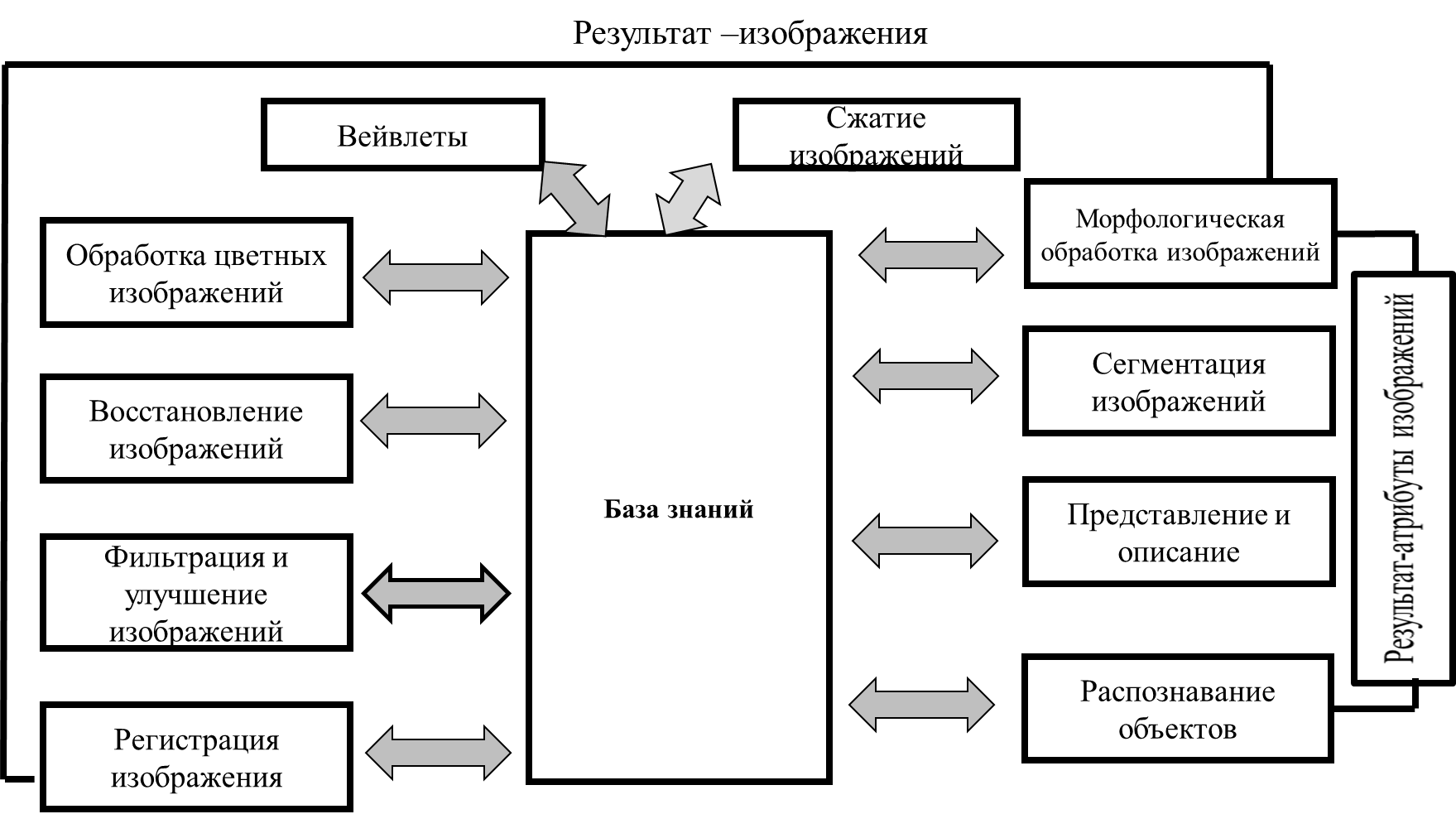


Рисунок 1.8 - Основные этапы обработки цифровых изображений

Анализируя литературу в этой области, можно выделить следующее: практически полное отсутствие методов встраивания устойчивых к сжатию мультимедийных данных. Одним из преобразований, допускающих такое встраивание, является дискретное вейвлет-преобразование [78,79]. Как известно, набор вейвлетов в их временном или частотном представлении может аппроксимировать сложный сигнал или Вейвлет-преобразование является одним из методов внедрения информации в стеганографии. Оно используется для разложения изображений на различные частотные компоненты, которые затем могут быть использованы для внедрения секретной информации.

Новые эффективные методы обработки изображений стали возможны с развитием теории вейвлетов, которые, по сравнению с преобразованием Фурье, позволяют нам с гораздо большей точностью представлять мельчайшие особенности функций, изображений и сигналов, вплоть до разрывов первого рода (скачков), с их привязкой ко времени или пространственные координаты. Термин "вейвлет" был введен Алексом Гроссманом и Жаном Морле в середине 1980-х годов в связи с анализом сейсмических и акустических сигналов. В настоящее время вейвлеты используются в задачах распознавания изображений, при обработке и синтезе различных сигналов, при анализе изображений различной природы, для сжатия больших объемов информации.

Вейвлет (от wavelet - малая волна, пульсация, также всплеск, часто - вейвлет) [80] - математическая функция, которая анализирует различные частотные составляющие данных. График функции выглядит как волнообразные колебания с амплитудой, уменьшающейся до нуля вдали от начала координат. Идеи теории вейвлетов возникли, когда появилось достаточное количество рядов экспериментальных данных, обработка которых стандартным и хорошо разработанным методом преобразования Фурье показала свои ограничения для нахождения в них закономерностей. Стремительное развитие компьютерных технологий также сыграло свою роль, что позволило численно решать такие задачи, которые раньше были просто недоступны. Практически важные вейвлеты традиционно определяются как функции одной действительной переменной с действительными значениями. В зависимости от математической модели (структуры, объема, структурирующего поля возможных значений и преобразований) различают дискретные и непрерывные вейвлеты. Поскольку разложение сигналов в вейвлет-базисе осуществляется с использованием арифметики с плавающей запятой, возникают ошибки, величина которых зависит от степени аппроксимации сигнала.

Рассмотрим пример внедрения информации в коэффициенты дискретного вейвлет-преобразования изображения. Для этого сначала производится разложение изображения на коэффициенты дискретного вейвлет-преобразования. Затем происходит выбор коэффициентов, в которые будет внедрена секретная информация.

Внедрение информации происходит путем изменения выбранных коэффициентов на небольшую величину в зависимости от значения битов секретной информации. Это изменение незначительно для человеческого глаза, но позволяет внести секретную информацию в изображение без заметных с точки зрения восприятия искажений человеческим глазом.

После внедрения информации необходимо произвести обратное вейвлет-преобразование для получения измененного изображения. Важно заметить, что при этом происходит некоторое сжатие изображения, что может привести к потере качества. Поэтому при выборе метода стеганографии необходимо учитывать не только стойкость информации, но и ее визуальное качество [81-86].

# 1.3 Практическое применение методов стеганографии

Применение стеганографии имеет мирное и полезное применение – встраивание цифровых водяных знаков. Цифровой водяной знак (Digital Watermark) — это невидимая информация, встроенная в цифровое изображение, видео или звуковой файл для различных целей, таких как: защита авторских прав, аутентификация, мониторинг и отслеживание [87]. Например, автор встраивает свои идентификационные данные в каждую продаваемую копию программы, изображения или иного файла. Если будет перехвачен аналогичный файл под авторством третьего лица, то истинный автор может извлечь внедренный ЦВЗ и доказать свое авторство в судебном порядке. Стеганографические алгоритмы позволяют свободно встраивать и извлекать ЦВЗ.

Существует множество исследований, посвященных разработке новых методов встраивания водяных знаков и анализу их эффективности [88]. К требованиям ЦВЗ относят устойчивость – свойство, позволяющее сохранять информацию даже после графических преобразований контейнера, например, масштабирования или сохранения в другом формате файла.

В работе авторов [89] для оценки систем водяных знаков были применены различные методы атак (атаки на удаление, атаки с шумоподавлением и сжатием с потерями, модуляционные атаки, атаки на усреднение и геометрические атаки), что обеспечивает автоматизированный и объективный анализ существенных методов водяных знаков для выбранных области применения. Ключевыми моментами исследований были алгоритмы нанесения водяных знаков, которые устойчивые к геометрическим искажениям.

В работе [90] исследователи продемонстрировали универсальную модель водяных знаков для приложений с цифровыми изображениями (с графическим интерфейсом). В представленном модели определили набор возможных входов, выходов и функций компонентов, изучив схемы нанесения водяных знаков, предложенные для различных приложений для обработки изображений (рис.1.8):

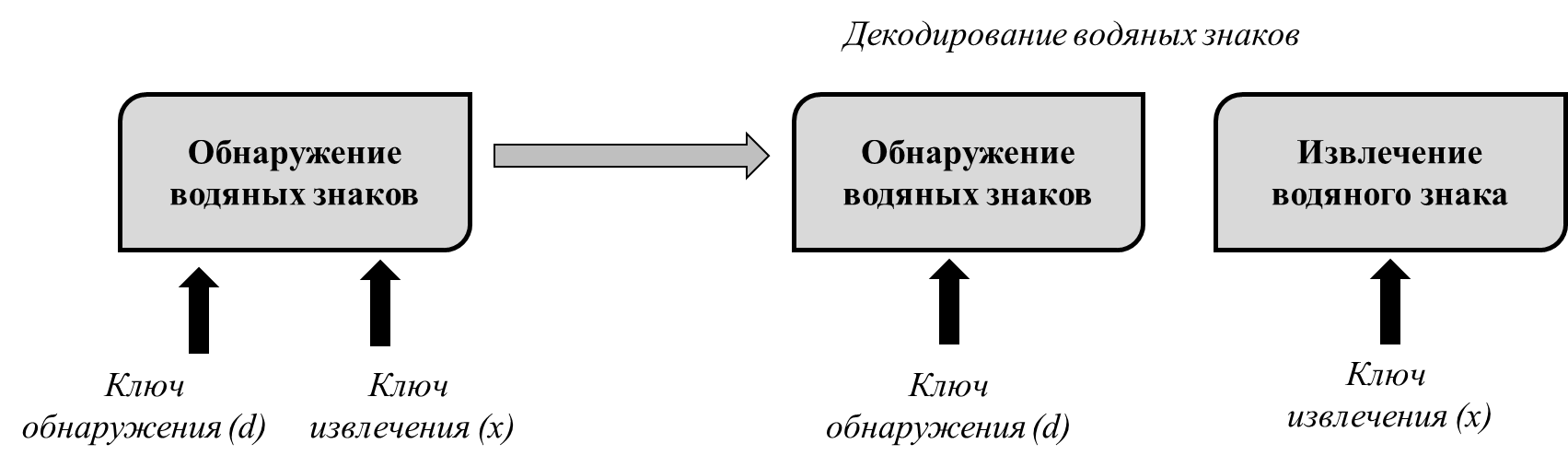


Рисунок 1.9 - Развертывание ключей в функции обнаружения базовой модели [90]

Применяя предложенную модель с подходящими входами, выходами и функциональными свойствами, можно охарактеризовать и описать все возможные варианты схем нанесения водяных знаков на цифровые изображения (например, для проведения необходимого вычислительного анализа). В данной статье авторами был прописан четкие описания предложенной модели в виде таблицы 1.2:

Таблица 1.2 - Нанесение водяных знаков на цифровые изображения: его формальная модель, фундаментальные свойства и возможные атаки [90]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Используемая модель** | **Цели** | **Входы и выходы** | **Функции компонентов** | **Теория** | **Ограничения** |
| Предложенный | Обеспечить средства для систематического развития и, таким образом, разработать единую и более реалистичную теорию нанесения водяных знаков на цифровые изображения | Изображение-данные (с различными свойствами, например, оригинал, с водяными знаками и т.д.,) | Генератор ключей | Цифровая обработка изображений и сигналов | Может не подходить для изучения схем стеганографии |
|  |  | Водяной знак | Генерация водяных знаков | Криптография |  |
|  |  | Сообщение | Встраивание водяного знака |  |  |
|  |  | Ключ (для каждой функции) | Обнаружение водяного знака |  |  |
|  |  |  | Извлечение водяного знака |  |  |

Предложенная модель позволяет унифицировать обработку всех практически значимых вариантов нанесения водяных знаков на цифровые изображения

В исследовании [91] предлагается новый метод создания водяных знаков на изображениях, основанный на инвариантных областях изображения. Понятие инвариантные области понимается, как самоадаптивные участки изображения, которые деформируются при геометрических преобразованиях. Авторы для разработки водяных знаков рассмотрели три различных метода определения инвариантной области, основанные на масштабно-пространственном представлении изображения. В каждую инвариантную область водяной знак встраивается после геометрической нормализации в соответствии с формой области; путем привязки водяных знаков с помощью инвариантных областей можно легко получить устойчивость к геометрическим преобразованиям.

В экспериментах был использован шаблон водяного знака длиной 1024 и только 50 инвариантных областей из 50 при обнаружении водяного знака. Экспериментальные результаты показывают, что предложенный метод устойчив к различным этапам обработки изображений, включая геометрические преобразования, обрезку, фильтрацию и сжатие в формате JPEG.

В работе [92] предлагается защищенный алгоритм создания водяных знаков на изображениях, устойчивых к атаки коалиции. Так группа пользователей может объединиться и сравнить свои копии защищенных файлов. Поскольку ЦВЗ в каждой копии отличается, то все найденные различия могут быть искажены. Тем не менее предлагается встраивать такой знак, который будет устойчив к подобной атаке.

Водяной знак создавался как независимый и идентично распределенный гауссовский случайный вектор, который незаметно вставляется в виде расширенного спектра в наиболее значимые с точки зрения восприятия спектральные компоненты данных. По мнению авторов, вставка водяного знака в этом режиме делает водяной знак устойчивым к операции обработки сигналов (такие как сжатие с потерями, фильтрация, ЦАП и АЦП, повторная обработка и т.д.) и обычные геометрические преобразования при условии, что исходное изображение доступно и что его можно успешно сопоставить с преобразованным водяным знаком изображение. В этих случаях детектор водяных знаков однозначно идентифицирует владельца.

Авторы также отмечают что, использование гауссовского шума обеспечивает высокую устойчивость к атакам с несколькими документами или сговору. В статье даны экспериментальные результаты: применение этого метода к цветным изображениям с точки зрения авторов несложно. Наиболее распространенным преобразованием цветного изображения является преобразование его в черно-белое. Однако устойчивость к определенному цветовому изображению следует изучить процедуры обработки.

В книге представлены [93] обзор форматов хранения различных типов носителей, сжатия данных, а также механизмов и методов защиты этих типов носителей. Материалы, представленные в этой книге, дают всесторонний обзор различных аспектов управление медиа-активами и цифровыми правами. Целью книги являются: изложить соответствующие теоретические основы и последние результаты исследований в этой области.

В следующей статье [94] исследованы ситуаций, в которых требуется встроить в изображение несколько водяных знаков. Авторы в своем исследовании предлагают эффективный подход к внедрению двойных водяных знаков путем расширения алгоритмов создания одиночных водяных знаков для нанесения водяных знаков с цифрами и логотипом соответственно. Идея алгоритма заключается в том, если потребители хотят достичь нескольких целей, например, защитить авторские права на один продукт у нескольких владельцев на разных этапах или проверить целостность контента и защитить авторские права одновременно, то они должны использовать множественные водяные знаки, то есть встраивать более одного водяного знака в одно и то же мультимедийное изображение. Авторы в своих исследованиях применяли три схемы для встраивания двойного водяного знака, как показано на рис. 1.10-1.11.

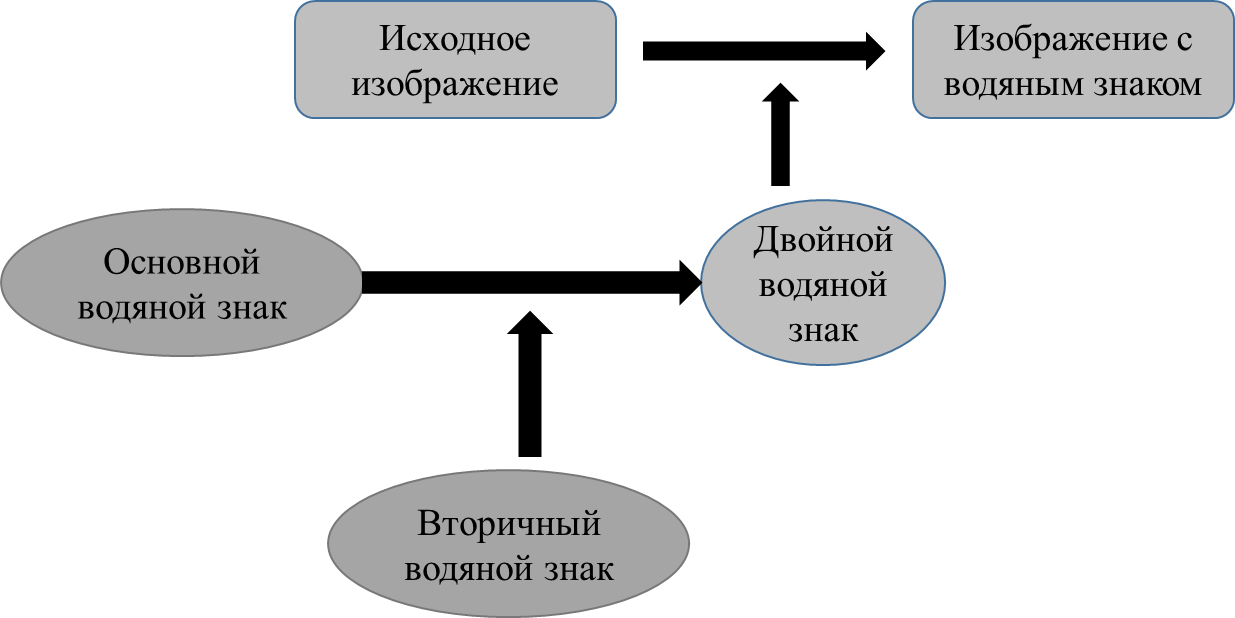


Рисунок 1.10 - Схема встраивания двойного водяного знака [94]

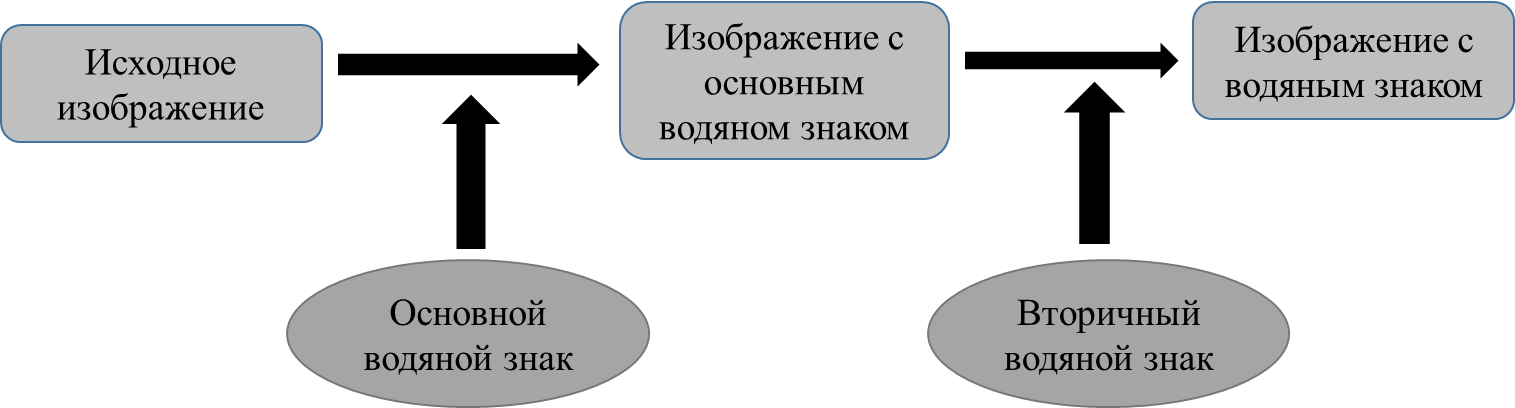


Рисунок 1.11 – Вторая схема встраивания двойного водяного знака [94]

Предлагаемые в данных работах схемы внедрения ЦВЗ не конфликтуют и дополняют друг друга.

Таблица 1.3- Сравнение PSNR с алгоритмом Chemak (Чемак) и новым алгоритмом [94]

|  |  |  |
| --- | --- | --- |
| Тип искажения | PSNR (Chemak) | PSNR (новый) |
| Среднее смещение | 24.6090 | 28.5274 |
| Контрастное растяжение | 24.6003 | 28.5127 |
| Импульсивный шум соли и бумаги | 24.6499 | 28.8416 |
| Мультипликативный спекл-шум | 24.6186 | 28.6741 |
| Aддитивный гауссовский шум | 24.5906 | 28.4598 |
| Cжатие в формате jpeg | 24.7849 | 30.1737 |

Экспериментальный результаты (табл.઎1.3) показывают, что результирующие алгоритмы двойного нанесения водяных знаков имеют значительно более высокую PSNR по сравнению с существующими алгоритмами создания двойных водяных знаков, а также сохраняют ту же надежность и более высокую чувствительность, чем исходные алгоритмы создания одиночных водяных знаков, на которых они основаны.

Эти работы показывают, что цифровые водяные знаки остаются активной областью исследований, и что различные методы могут быть использованы для создания более эффективных и устойчивых водяных знаков.

# 1.4 Обзор известных методов стегоанализа

Стегоанализ — это процесс обнаружения наличия стеганографического сообщения в контейнере, то есть анализа изображений, аудио или видео файлов с целью обнаружения скрытой информации [95,96]. Строго говоря, задача обнаружения эквивалентна задачи классификации. Имеется два класса: пустых и заполненных контейнеров. Известны статистические свойства данного классов. Необходимо определить принадлежность произвольного контейнера к одному из этих классов. Отличие методов стегоанализа между собой заключается только в наборе анализируемой статистики или характеристик контейнера. Некоторые известные методы стегоанализа включают в себя:

* Анализ статистических свойств: этот метод основывается на анализе статистики контейнера, таких как распределение цветов пикселей, их взаимная корреляция и энтропия. Изменения в этих свойствах могут указывать на наличие скрытой информации.
* Алгоритмы машинного обучения могут использоваться для обнаружения изменений в паттернах или свойствах носителя, которые указывают на наличие стеганографического сообщения.
* Анализ на основе спектральных свойств: этот метод основывается на анализе спектральных свойств контейнер, таких как частоты и фазы, чтобы обнаружить изменения, которые могут указывать на наличие стеганографического сообщения.
* Анализ на основе артефактов: этот метод основывается на обнаружении артефактов, которые обычно появляются при внедрении стеганографического сообщения, таких как изменения насыщенности цветов, блоковый эффект и т.д.
* Анализ на основе сравнения: этот метод сравнивает оригинальный носитель с возможными стеганографическими версиями, чтобы найти отличия, которые могут указывать на наличие скрытого сообщения.

Это лишь некоторые известные методы стегоанализа, и исследователи продолжают разрабатывать новые методы и улучшать существующие для более эффективного обнаружения стеганографических сообщений.

Некоторые из новых работ по известным методам стегоанализа включают в себя [97-99]:

1. Анализ на основе графов:Идея подхода заключается в использовании теории графов для анализа стеганографических сообщений в целях повышения точности их обнаружения. Данная методика позволяет отображать взаимосвязи между различными элементами стеганографического сообщения в виде графа, что позволяет выявлять скрытые связи между этими элементами и обнаруживать скрытые сообщения. Этот подход может быть использован для различных целей, например, для обнаружения наличия стеганографического сообщения в файле, для определения его типа, для обнаружения и анализа сокрытой информации. В целом, использование этого подхода может помочь в повышении эффективности и точности анализа стеганографических сообщений.
2. Машинное обучение с глубокими нейронными сетями: Идея подхода заключается в использовании глубоких нейронных сетей для анализа изображений и видео с целью обнаружения скрытой информации. С помощью алгоритмов обработки большого объема данных модели глубоких нейронных сетей позволяют корректно определять изменения в пикселях и фреймах изображений и видео, которые могут указывать на наличие стеганографической информации. Такой подход может быть использован для обеспечения безопасности данных и защиты от нежелательных утечек информации.
3. Анализ на основе многомерных статистических свойств: Идея данного подхода заключается в использовании многомерных статистических свойств для обнаружения стеганографических сообщений, которые были внедрены с помощью более сложных алгоритмов стеганографии. Данный подход использует совместную энтропию для анализа изображений и обнаружения скрытых сообщений. Такой подход может быть эффективен для обнаружения стеганографических сообщений, которые меньше зависят от изменений окружающей среды.
4. Анализ на основе моделей глубокого обучения: Идея данного подхода заключается в использовании моделей глубокого обучения для повышения точности обнаружения стеганографических сообщений. В рамках подхода используется анализ носителя и знания о том, как сообщение было внедрено, что позволяет улучшить результаты анализа. Такой подход может быть эффективным в обнаружении скрытой информации и защите от кибератак.
5. Обнаружение сообщений с использованием машинного зрения: Идея подхода заключается в использовании алгоритмов машинного зрения для обнаружения скрытых сообщений в изображениях. Эти методы основаны на обнаружении изменений в текстуре, цветовых свойствах и других характеристиках изображения, которые могут указывать на наличие стеганографического сообщения. Это позволяет эффективно обнаруживать скрытые сообщения, которые могут быть использованы в криминальной или шпионской деятельности.

# 1.4.1 RS – метод

RS – анализ основан на применении двойной статистики, полученной из пространственных корреляций в изображениях. На данный момент не имеется каких-либо исследований по анализу скрытности внедрения данных алгоритмов при помощи методов стегоанализа. Одним из основных методов статистического стегоанализа является метод RS, который был разработан Фридрич и др. [100-102] в 2001 году. Сокращение в названии расшифровывается как Regular–Singular, то есть «регулярно-сингулярный».

RS — это метод стегоанализа, который основан на анализе остаточной информации, оставленной при встраивании сообщения в изображение или другой мультимедийный контент. Основная идея RS состоит в том, чтобы определить изменения, произведенные в остаточной информации после встраивания сообщения, и использовать эти изменения для обнаружения скрытой информации. Остаточная информация — это разница между оригинальным и измененным контентом после встраивания сообщения.

RS использует статистические методы для анализа остаточной информации и определения ее характеристик, таких как среднее значение, дисперсия и ковариация. Затем эти характеристики используются для построения модели, которая может определять, содержит ли контент скрытую информацию. Одним из преимуществ RS является его способность обнаруживать скрытую информацию, встроенную с помощью различных методов стеганографии, в том числе и более сложных методов. Однако этот метод также может давать ложноположительные результаты, если остаточная информация изменена, например, в результате сжатия изображения или другого контента.

Суть метода состоит в следующем: все изображение разбивается на группы по пикселов где четно (1.1). Для групп пикселов определяется функция регулярности . Под значением пикселов понимаем число от 0 до 255 .

 (1.1)

Функция называется флиппингом и имеет свойство . Определяют две функции флиппинга – , соответствующую инверсии младшего бита пиксела, и  представляющую собой инверсию с переносом в старший бит (1.2-1.3):

 (1.2)

 (1.3)

При применении флиппинга к группе получают преобразованную группу пикселов. Далее делят все группы пикселов на классы следующим образом:

если  то ;

если  то ;

если  то .

Метод RS может указать маленькую ненулевую длину сообщения из-за случайных отклонений даже для пустого контейнера. Это начальное ненулевое отклонение может быть, как положительным, так и отрицательным и накладывает ограничение на достижимую точность RS анализа.

Для каждой группы флиппинг производится два раза: с прямой и с инвертированной маской. После проведения операций классификации для всех групп выполняется подсчет ряда количественных характеристик:

* количество обычных групп для маски ;
* количество необычных групп для маски ;
* количество обычных групп для инверсной маски ;
* количество необычных групп для инверсной маски .

RS анализ показывает более точные результаты для сообщений, которые рассеянно распределены по картинке, по сравнению с анализом сообщений, которые сконцентрированы в определенной области изображения.

На рис.1.12 представлен типичный вид RS-диаграммы – графиков значений  в зависимости от количества пикселей с инвертированными LSB в изображении [92]:

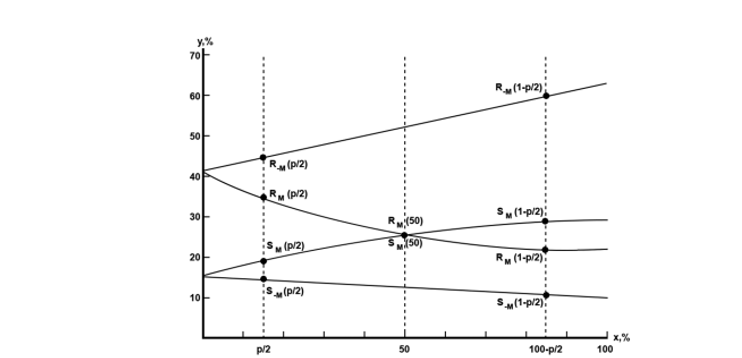


Рисунок 1.12 – RS диаграмма

Ключевая особенность RS – метод состоит с том, что он анализирует количественные характеристики небольших групп пикселей. В связи с чем он, хотя и не способен декодировать область потенциального встраивания, может обнаружить скрытие, произведенное в случайные биты, а не последовательно.

# 1.3.2 SPAM метод

SPAM (Statistic-based Pixel Adjacency Model) - это метод стегоанализа, который использует статистическую модель соседних пикселей для обнаружения скрытых сообщений в мультимедийных данных. Однако, по сравнению с другими методами, такими как паритетная проверка или анализ используемого алгоритма сжатия, SPAM предлагает более точное и эффективное обнаружение скрытой информации. Если в данных присутствует скрытая информация, то статистические свойства контейнера может измениться в тех областях, где скрытая информация была внедрена. Кроме того, SPAM может обнаружить небольшие изменения в данных, которые могут оставаться незамеченными другими методами [103, 104].

При использовании SPAM для стегоанализа следует иметь в виду, что этот метод может быть ограничен в случае, если скрытая информация была внедрена в необычные (шумные) области данных, нарушения в которых не входит за границы известной дисперсии статистики. Также, метод может быть более требовательным к вычислительным мощностям, нежели другие методы стегоанализа, особенно при анализе больших объемов данных.

В работах авторов [105-108] использованы метод SPAM в сочетании с алгоритмами усиления (boosting) для улучшения обнаружения скрытых сообщений в мультимедийных данных, которые были встроены с использованием различных методов стеганографии и с более сложными моделями взаимосвязи соседних пикселов, например, групповое понижение яркости цвета соседних пикселов.

В целом, метод SPAM продолжает оставаться важным инструментом в стегоанализе, и его применение может быть расширено и улучшено с помощью дальнейших исследований в этой области.

# 1.3.3 Метод Хи-квадрат

Хи-квадрат (χ²) [109] - это статистический метод, который используется для анализа распределения данных. В контексте стегоанализа, Хи-квадрат может быть использован для обнаружения скрытых сообщений в изображениях или других мультимедийных данных. Метод Хи-квадрат основывается на сравнении ожидаемого распределения данных с наблюдаемым распределением. Если наблюдаемое распределение отличается от ожидаемого, это может указывать на наличие скрытой информации. В контексте стегоанализа, Хи-квадрат может быть использован для анализа частоты появления пикселей в изображении или других мультимедийных данных. Используя этот метод, можно определить, являются ли эти частоты случайными или сформированы определенным образом. Если частоты появления пикселей не соответствуют ожидаемому распределению, это может указывать на наличие скрытой информации.

Одним из преимуществ метода Хи-квадрат является его универсальность, то есть возможность использовать его для обнаружения скрытых сообщений, встроенных с помощью различных методов стеганографии. Однако, этот метод также может давать ошибочные результаты:

* ошибка первого рода – случай, когда заполненный контейнер признается пустым.
* ошибка второго рода – случай, когда пустой контейнер признается заполненным.

Метод Хи-квадрат широко используется в области стегоанализа для обнаружения скрытых сообщений в различных типах мультимедийных данных, включая изображения, аудио и видео.

Существует множество исследований, которые используют этот метод для анализа качества различных методов стеганографии, а также для разработки новых методов обнаружения скрытых сообщений. Одной из работ в этой области является статья [110]. В этой статье авторы использовали метод Хи-квадрат (рис.1.13) для обнаружения скрытых сообщений, встроенных с использованием метода младшего значащего бита (LSB, НЗБ):

а) при последовательной записи в НЗБ дискретных коэффициентов;

б) при псевдослучайной записи в НЗБ дискретных коэффициентов.

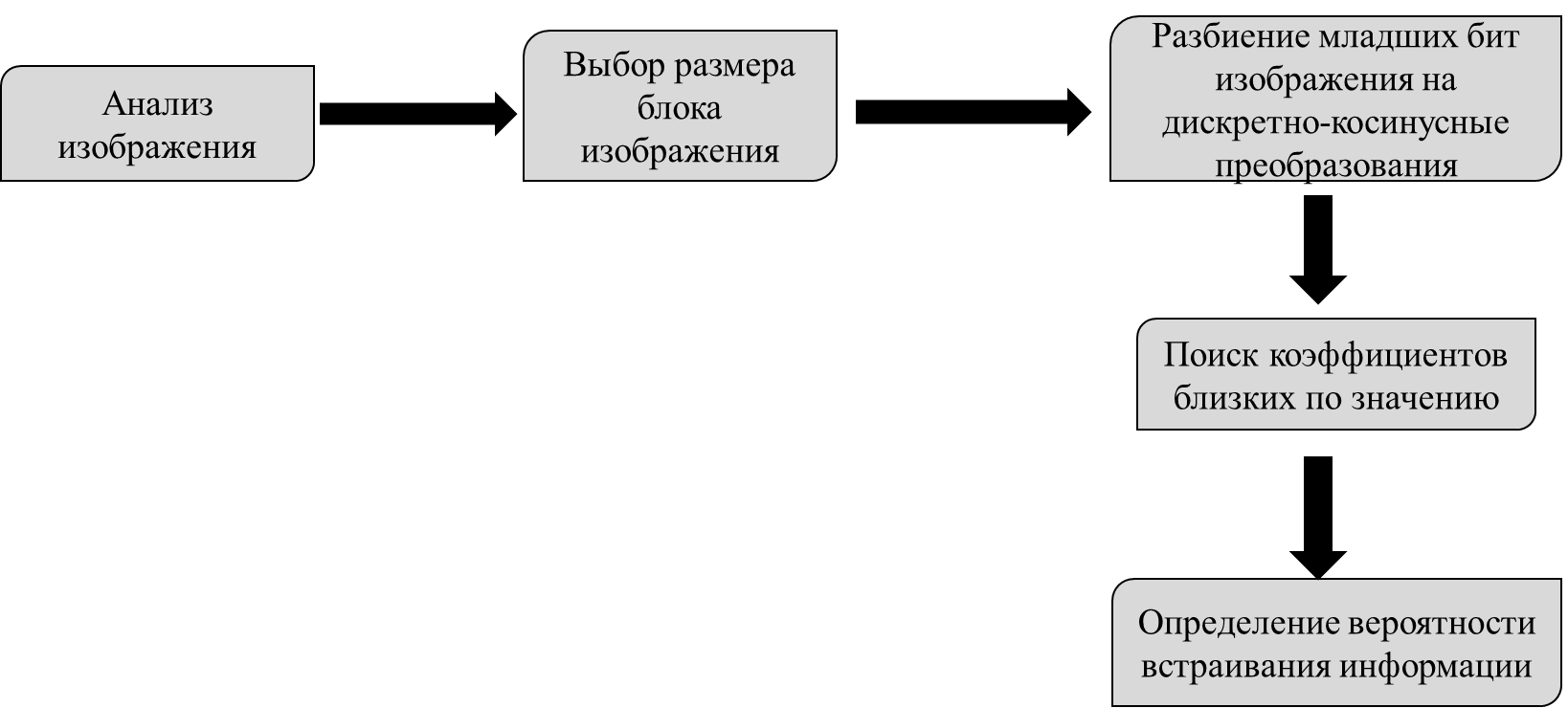


Рисунок 1.13- Алгоритм работы метода Хи-квадрат [110]

Для сравнительной характеристики вероятности обнаружения внедренных данных авторы использовали следующие методы стегоанализа: RS-анализ, метод анализа гистограмм, хи-квадрат, сигнатурный метод (Рис.1.14):

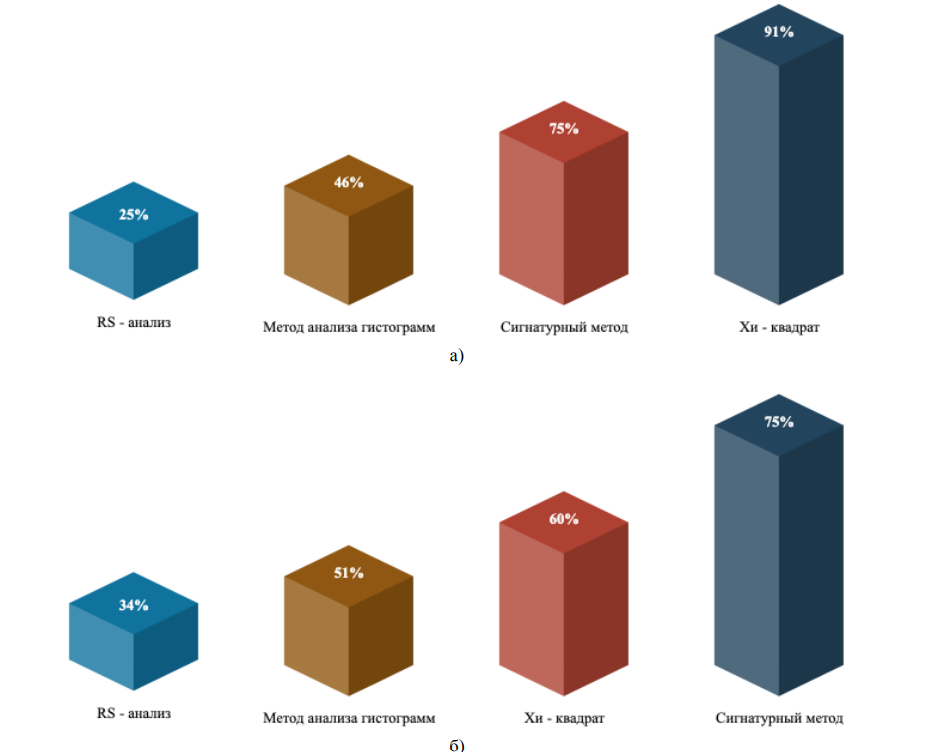


Рисунок 1.14 –Сравнительная статистика вероятности обнаружения скрытой информации: а) при последовательной записи в НЗБ дискретных коэффициентов; б) при псевдослучайной записи в НЗБ дискретных коэффициентов [110]

Согласно результатам эксперимента и утверждениям авторов с точки зрения защищенности информации предложенная методика обеспечивает стойкость и быстродействие выявления и предотвращения стеганографии.

В разработке [111] исследован принцип работы методов стегоанализа сообщений, внедренных с помощью метода замены LSB. В качестве контейнера применяли изображение. Показаны реализации следующих методов стегонализа: хи-квадрат и метод RS. Авторами проанализированы математические реализации данных методов и наглядно представлены результаты их работы в виде графиков (рис.1.15).

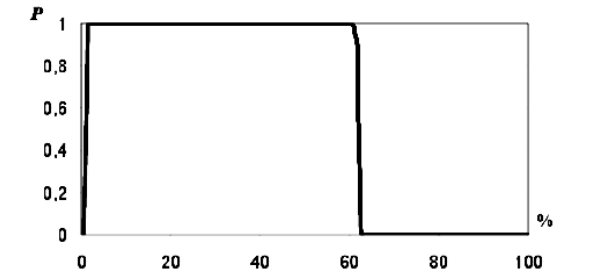


Рисунок 1.15- Вероятность встраивания по критерию Хи –квадрат при анализе стегоконтейнера, полученного методом последовательной замены [111]

Согласно результатам эксперимента, можно увидеть, что метод RS является достаточно эффективным методом стегоанализа, основанным на анализе соотношения между группами в цифровом изображении. Данный метод позволяет избежать недостатков, присущих методу анализа на основе Хи–квадрат, так как он не зависит от метода встраивания информации в пространственные области изображений.

Например, некоторые исследования [112-114] используют метод Хи-квадрат для обнаружения скрытых сообщений, встроенных в различные типы мультимедийных данных, такие как изображения, аудио и видео. Другие работы используют метод Хи-квадрат для оценки качества стеганографических методов, путем сравнения их эффективности в обходе методов стегоанализа.

Кроме того, существует также исследования, которые расширяют метод Хи-квадрат для обнаружения скрытых сообщений в более сложных сценариях, таких как мультимедийные данные с шумом или изменениями размера. В целом, метод Хи-квадрат является важным инструментом в стегоанализе, и его применение может быть расширено и улучшено с помощью последних исследований в этой области.

1.5 Выводы по разделу

В этой главе был приведен обзор существующих и известных методов стеганографии и стегоанализа. Наиболее популярными методами стеганографии являются:

* LSB метод;
* DCT;
* Вейвлет - преобразование.

В стегоанализе изображений наиболее эффективными методами считаются:

* RS анализ;
* Хи-квадрат;
* SPAM.

Было показано, что методы стеганографии имеют широкое применение в области защиты авторских прав и отслеживания траектории распространения цифрового объекта. Оценка эффективности алгоритма внедрения определяется объемом данных, которое встраивается в контейнер, при котором вероятность успешного стегоанализа мала.

Применение стегоанализа может быть найдено в области обеспечения безопасности объектов критической телекоммуникационной инфраструктуры в части контроля за передачей конфиденциальных данных.

# **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Рябко Б.Я., Фионов А.Н., Шокин Ю.И. Криптография и стеганография в информационных технологиях. Новосибирск: Наука, 2015. 240 с.
2. Дайырбаева Э.Н., Мурзин Ф.А., Липская М.А. Скрытие информации в изображениях. Вестник КазАТК им. М. Тынышпаева №1 (112), 2020. -С.283-290.
3. Кори Б., Буррес С. Методы и системы сокрытия информации: основы теории и применения. – М.: Техносфера, 2013. – 400 с.
4. Дайырбаева Э.Н., Липская М.А., Тойгожинова А.Ж. Суреттерді өңдеуде стрип-әдісті пайданалу жолдары мен нәтижелері. Вестник КазНИТУ, №5 (2020). –Б. 279-284.
5. Дайырбаева Э.Н., Липская М.А., Тойгожинова А.Ж, Нугуманов Ш.Е. Сандық және компьютерлік стеганографиялардың сипаттамалары мен мүмкіншіліктеріне шолу. Вестник КазАТК №3 (114) 2020. -Б. 246-252.
6. Фридрихс Дж., Свенсон А. Методы стеганографии // Наука и жизнь. – 2001. – №. 6. – С. 42-47.
7. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии. - М.: Горячая линия – Телеком, (грант РФФИ 10-07-07010-д). - 2010. - 232 с. - ISBN 978-5-9912-0150-6.
8. Рябко Б.Я., Фионов А.Н., Шокин Ю.И. Криптография и стеганография в информационных технологиях. - 500 экз. - Новосибирск: Наука. - 2015. - 240 с. - ISBN 978-5-02-019206-5.
9. Нечта И. В. Новый метод стеганографии в социальных сетях //Современные проблемы телекоммуникаций. – 2017. – С. 86-90.
10. Абазина Е. С., Ерунов А. А. Цифровая стеганография: состояние и перспективы //Системы управления, связи и безопасности. – 2016. – №. 2. – С. 182-201.
11. Gustavus J. Simmons. The Prisoners' Problem and the Subliminal Channel. Problems of Control and Information Theory - 1984. Том 13, выпуск 4, стр. 297-304. DOI: 10.1016/S0167-6911(84)80025-3
12. Колчин А.А. Методы и алгоритмы стеганографии // Информационно-измерительные и управляющие системы. – 2005. – №. 4. – С. 20-25.
13. Китани М. Методы и системы сокрытия информации. – М.: Техносфера, 2003. – 336 с.
14. Нечта И. В. Метод внедрения скрытых сообщений в исполняемые файлы //Вестник СибГУТИ. – 2011. – №. 2. – С. 3-10.
15. Галан Ф., Кабатянский Г. А. Покрытия, центрированные коды и комбинаторная стеганография //Проблемы передачи информации. – 2009. – Т. 45. – №. 3. – С. 106-111.
16. Рябко Б. Я., Фионов А. Н. Идеальные стенографические системы //Доклады Томского государственного университета систем управления и радиоэлектроники. – 2008. – №. 2-1 (18). – С. 61-62.
17. Рябко Б. Я., Фионов А. Н. Алгоритмы кодирования для идеальных стеганографических систем //Вестник Новосибирского государственного университета. Серия: Информационные технологии. – 2008. – Т. 6. – №. 2. – С. 88-93.
18. Дэвид Н., Форсайт Дж. Стеганография и цифровые водяные знаки. – М.: Издательский дом «Вильямс», 2002. – 344 с.
19. Кори Б., Буррес С. Методы и системы сокрытия информации: основы теории и применения. – М.: Техносфера, 2013. – 400 с.
20. Лэй Х., Уайт М. Information Hiding - A Survey // Proceedings of the IEEE. – 1998. – Т. 86. – №. 6. – С. 1062-1078.
21. Нечта И. В. Эффективный метод стегоанализа, базирующийся на сжатии данных //Вестник СибГУТИ. – 2010. – №. 1. – С. 50-55.
22. Евсютин О. О. Модификация стеганографического метода lsb, основанная на использовании //Информатика и системы управления. – 2014. – №. 1. – С. 15-22.
23. Boris Ryabko and Daniil Ryabko, Constructing perfect steganographic systems. Information and Computation, v. 209 (2011), pp. 1223 – 1230
24. Китани М. Техника сокрытия данных на основе LSB метода // Информационные технологии. – 2004. – №. 10. – С. 56-61.
25. Китани М. Методы и системы сокрытия информации. – М.: Техносфера, 2003. – 336 с.
26. Пашин А. А., Кудрина М. А. Исследование методов стеганографии изображений. – 2022.
27. Stepanov P. I. Development and testing of the decision-making unit for the control system of the technical condition of electromechanical equipment //Южно-Сибирский научный вестник. – 2018. – С. 113.
28. Пастушков А. В., Калайда В. Т. Методы и алгоритмы поиска объекта на видеопотоке //Сборник научных трудов SWorld. – 2013. – Т. 6. – №. 3. – С. 38-42.
29. Чучкалова А. С. и др. Алгоритм стеганографии на основе дискретного косинусного преобразования. – 2023.
30. Грибунин В. Г. Вейвлеты в стеганографии //Статья. СПб. – 2009.
31. Кэмпбелл М. Стеганография: техника сокрытия информации // Журнал «Хакер». – 2003. – №. 56. – С. 30-37.
32. Фридрихс Дж., Свенсон А. Методы стеганографии // Наука и жизнь. – 2001. – №. 6. – С. 42-47.
33. Колчин А.А. Методы и алгоритмы стеганографии // Информационно-измерительные и управляющие системы. – 2005. – №. 4. – С. 20-25.
34. Китани М. Техника сокрытия данных на основе LSB метода // Информационные технологии. – 2004. – №. 10. – С. 56-61.
35. Кумар Р., Лалит Н., Ананд М. LSB Steganography: A Review // International Journal of Advanced Research in Computer and Communication Engineering. – 2014. – Т. 3. – №. 4. – С. 4641-4646.
36. Гуарини М., Баринотто М. LSB-Based Steganography and Steganalysis: Recent Advances and Future Perspectives // Journal of Information Hiding and Multimedia Signal Processing. – 2010. – Т. 1. – №. 1. – С. 142-172.
37. Кумар Р., Лалит Н., Ананд М. LSB Steganography: A Review // International Journal of Advanced Research in Computer and Communication Engineering. – 2014. – Т. 3. – №. 4. – С. 4641-4646.
38. Гуарини М., Баринотто М. LSB-Based Steganography and Steganalysis: Recent Advances and Future Perspectives // Journal of Information Hiding and Multimedia Signal Processing. – 2010. – Т. 1. – №. 1. – С. 142-172.
39. Китани М. Техника сокрытия данных на основе LSB метода // Информационные технологии. – 2004. – №. 10. – С. 56-61.
40. Кумар Р., Лалит Н., Ананд М. LSB Steganography: A Review // International Journal of Advanced Research in Computer and Communication Engineering. – 2014. – Т. 3. – №. 4. – С. 4641-4646.
41. Гуарини М., Баринотто М. LSB-Based Steganography and Steganalysis: Recent Advances and Future Perspectives // Journal of Information Hiding and Multimedia Signal Processing. – 2010. – Т. 1. – №. 1. – С. 142-172.
42. Кори Б., Буррес С. Методы и системы сокрытия информации: основы теории и применения. – М.: Техносфера, 2013. – 400 с.
43. Дайырбаева Э.Н., Еримбетова А.С. Роль метрики в обработке изображений // МНСК-2021 ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ Материалы 59-й Международной научной студенческой конференции, 12–23 апреля 2021 г., Новосибирск, РФ, - С.53
44. Янг У. Реализация алгоритма стеганографии на основе LSB метода // Труды Международной конференции по компьютерной безопасности и криптографии. – 2012. – С. 143-147.
45. Ань Л., Жан Ч., Пай Ж. Обзор и анализ методов стеганографии // Информационные технологии. – 2016. – №. 5. – С. 11-16.
46. Al-Afandy K. A. et al. High security data hiding using image cropping and LSB least significant bit steganography //2016 4th IEEE International Colloquium on Information Science and Technology (CiSt). – IEEE, 2016. – С. 400-404.
47. Al-Taani, A. T., & Al-Issa, A. M. (2009). A novel steganographic method for gray-level images. International Journal of Computer, Information, and Systems Science, and Engineering, 3(3), 574-579.
48. Lou D. C., Hu C. H. LSB steganographic method based on reversible histogram transformation function for resisting statistical steganalysis //Information Sciences. – 2012. – Т. 188. – С. 346-358.
49. Deshmukh P.U., Pattewar T.M. A novel approach for edge adaptive steganography on LSB insertion technique (2015). International Conference on Information Communication and Embedded Systems, ICICES 2014, DOI: 10.1109/ICICES.2014.7033807
50. Arora, Himanshu & Bansal, Cheshta & Dagar, Sunny. (2018). Comparative study of image steganography techniques. 982-985. DOI:10.1109/ICACCCN.2018.8748451
51. Saru Kumari, Manoj Diwakar, and Amit Kumar Singh. A hybrid LSB-DE algorithm for secure color image steganography. Journal of Ambient Intelligence and Humanized Computing, Volume 9, pages 1523–1533 (2018) DOI: <https://doi.org/10.1007/s12652-017-0516-7>
52. Ch. Li, J. Zhang, X. Liu. A novel LSB-based image steganography algorithm using chaotic map. Multimedia Tools and Applications, Volume 77, pages 21685–21700 (2018) DOI: <https://doi.org/10.1007/s11042-018-5901-7>
53. R. Kaur, P. Kumar. A novel approach for color image steganography using LSB and pixel value differencing. International Journal of Computer Applications, Volume 120, Issue 5, pages 27-32 (2015) DOI: <https://doi.org/10.5120/21285-1414>
54. Najih M. N. M. et al. An improved secure image hiding technique using PN-sequence based on DCT-OTP //2017 1st International Conference on Informatics and Computational Sciences (ICICoS). – IEEE, 2017. – С. 47-52.
55. El\_Rahman S.A. A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information //Computers & Electrical Engineering. – 2018. – Т. 70. – С. 380-399.
56. Walia E., Jain P., Navdeep N. An analysis of LSB & DCT based steganography //Global Journal of Computer Science and Technology. – 2010. – Т. 10. – №. 1. – С. 4-8.
57. Emam A. M., Ouf M. M. Performance evaluation of different universal steganalysis techniques in jpg files //Annales Universitatis Mariae Curie-Skłodowska. Sectio AI, Informatica. – 2012. – Т. 12. – №. 3.
58. Goel S., Rana A., Kaur M. A review of comparison techniques of image steganography //Global Journal of Computer Science and Technology. – 2013.
59. Walia E., Jain P., Navdeep N. An analysis of LSB & DCT based steganography //Global Journal of Computer Science and Technology. – 2010. – Т. 10. – №. 1. – С. 4-8.
60. Poljicak A. et al. Portable real-time DCT-based steganography using OpenCL //Journal of Real-Time Image Processing. – 2018. – Т. 14. – С. 87-99.
61. Singla D., Syal R. Data security using LSB & DCT steganography in images //Int. J. Of Computational Engineering Research. – 2012. – Т. 2. – №. 2. – С. 359-364.
62. Fateh M., Rezvani M., Irani Y. A new method of coding for steganography based on LSB matching revisited //Security and Communication Networks. – 2021. – Т. 2021. – С. 1-15.
63. Maheswari S. U., Hemanth D. J. Different methodology for image steganography-based data hiding //International Journal of Information and Communication Technology. – 2015. – Т. 7. – №. 4-5. – С. 521-536.
64. Thai T. H., Cogranne R., Retraint F. Steganalysis of Jsteg algorithm based on a novel statistical model of quantized DCT coefficients //2013 IEEE International Conference on Image Processing. – IEEE, 2013. – С. 4427-4431.
65. Goel S., Rana A., Kaur M. A review of comparison techniques of image steganography //Global Journal of Computer Science and Technology. – 2013.
66. Abdel-Aziz M. M., Hosny K. M., Lashin N. A. Improved data hiding method for securing color images //Multimedia Tools and Applications. – 2021. – Т. 80. – С. 12641-12670.
67. Muhuri P. K., Ashraf Z., Goel S. A novel image steganographic method based on integer wavelet transformation and particle swarm optimization //Applied Soft Computing. – 2020. – Т. 92. – С. 106257.
68. Chu R. et al. A DCT-based image steganographic method resisting statistical attacks //2004 IEEE International Conference on Acoustics, Speech, and Signal Processing. – IEEE, 2004. – Т. 5. – С. V-953.
69. Hou D. et al. Reversible data hiding in JPEG image based on DCT frequency and block selection //Signal Processing. – 2018. – Т. 148. – С. 41-47
70. Muhuri P. K., Ashraf Z., Goel S. A novel image steganographic method based on integer wavelet transformation and particle swarm optimization //Applied Soft Computing. – 2020. – Т. 92. – С. 106257.
71. Zhang T., Ping X. A new approach to reliable detection of LSB steganography in natural images //Signal processing. – 2003. – Т. 83. – №. 10. – С. 2085-2093.
72. Abd EL-Latif A.A., Abd-El-Atty B., Venegas-Andraca S.E. A novel image steganography technique based on quantum substitution boxes //Optics & Laser Technology. – 2019. – Т. 116. – С. 92-102.
73. Li Y., Guan Z., Xu C. Digital image self restoration based on information hiding //2018 37th Chinese Control Conference (CCC). – IEEE, 2018. – С. 4368-4372.
74. Xiao J. et al. Research of multi-direction transition probability matrices algorithm for JPEG steganalysis //2012 24th Chinese Control and Decision Conference (CCDC). – IEEE, 2012. – С. 3907-3912.
75. Evsutin O., Melman A., Meshcheryakov R. Algorithm of error-free information embedding into the DCT domain of digital images based on the QIM method using adaptive masking of distortions //Signal Processing. – 2021. – Т. 179. – С. 107811.
76. Daiyrbayeva, E., Murzin, F., Yerimbetova, A., Toigozhinovа A. (2020). Using wavelet transform in image processing. Advanced technologies and computer science, (2), 15–20. <https://atcs.iict.kz/index.php/atcs/article/view/25>
77. D.J. Evans, N.F. Johnson, and S. Roe, "Wavelet-based steganography," IEEE Transactions on Information Forensics and Security, vol. 1, no. 1, pp. 142-154, 2006.
78. F. Liu, J. Li, and G. Xie. A new steganographic method based on wavelet transform. IEEE International Conference on Fuzzy Systems and Knowledge Discovery, vol. 2, pp. 1452-1456, 2009.
79. S. Wu, R. Lu, and X. Sun. A new steganographic method based on wavelet transform and matrix embedding. Journal of Computers, vol. 6, no. 7, pp. 1486-1493, 2011.
80. R. Zheng, C. Wang, and Y. Miao. A robust steganographic method based on wavelet transform. International Conference on Cyber Security, pp. 18-24, 2013.
81. V. Devi and V. Seetha Lakshmi. A novel wavelet based steganographic technique for hiding image into image. International Conference on Applied Soft Computing and Communication Networks, pp. 399-404, 2015.
82. K. Murugan and S. Neelavathi. Wavelet based multimedia steganography using adaptive threshold. International Journal of Applied Engineering Research, vol. 10, no. 55, pp. 39305-39311, 2015.
83. P. Gajjar and V. Prajapati. A review on steganography techniques using wavelet transform," International Journal of Advance Research, vol. 5, no. 10, pp. 3177-3182, 2017.
84. S.Kumar and P. Singh. A comparative study on wavelet based image steganography techniques. International Journal of Computer Applications, vol. 178, no. 11, pp. 10-14, November 2018.
85. F. Zhou, L. Wang, and Y. Qin. A new image steganography scheme based on wavelet transform and high-dimensional chaotic map. Multimedia Tools and Applications, vol. 77, no. 11, pp. 13195-13216, 2018.
86. M.Ali, A. Ansari, S. Chaudhuri. A novel color image steganography scheme using DWT and IWT. International Journal of Image, Graphics and Signal Processing, vol. 10, no. 8, pp. 114-122, 2018.
87. I. Cox, M. Miller, J. Bloom. Digital Watermarking and Steganography, 2nd Edition. -Morgan Kaufmann Publishers Publication date: December 2007
88. Xiaolong Li., Shuyuan Y. (2014). A Secure and Robust Digital Watermarking Scheme for Color Images based on Discrete Wavelet Transform and Singular Value Decomposition. International Journal of Security and Its Applications V.: 8 Issue: 2 Pages: 71-80
89. Tao H. et al. Robust image watermarking theories and techniques: A review //Journal of applied research and technology. – 2014. – Т. 12. – №. 1. – С. 122-138.
90. Nyeem H., Boles W., Boyd C. Digital image watermarking: its formal model, fundamental properties and possible attacks //EURASIP Journal on Advances in Signal Processing. – 2014. – Т. 2014. – №. 1. – С. 1-22.
91. Seo J. S., Yoo C. D. Image watermarking based on invariant regions of scale-space representation //IEEE Transactions on Signal Processing. – 2006. – Т. 54. – №. 4. – С. 1537-1549.
92. Cox I.J. et al. Secure spread spectrum watermarking for multimedia //IEEE transactions on image processing. – 1997. – Т. 6. – №. 12. – С. 1673-1687.
93. Seitz J. Digital watermarking for digital media. – IGI Global, 2005. eBook ISBN: 1-59140-520-3
94. Shen H., Chen B. From single watermark to dual watermark: a new approach for image watermarking //Computers & Electrical Engineering. – 2012. – Т. 38. – №. 5. – С. 1310-1324.
95. M. Goljan and R. Du, Reliable Detection of LSB Steganography in Grayscale and Color Images. Proc. of the ACM Workshop on Multimedia and Security, Ottawa, Canada, October 5, 2001, pp. 27-30. PDF
96. M. Goljan. Practical Steganalysis - State of the Art. Proc. SPIE Photonics West, Vol. 4675, Electronic Imaging 2002, Security and Watermarking of Multimedia Contents, San Jose, California, January, 2002, pp. 1-13. PDF
97. Thanikaiselvan V, Arulmozhivarman P, Subashanthini S, Amirtharajan R. A graph theory practice on transformed image: a random image steganography. Scientific World Journal. Dec 22;2013. doi: 10.1155/2013/464107.
98. Li F., Tang H., ZouY., Huang Y., Feng Y., Peng L. Research on information security in text emotional steganography based on machine learning. Enterprise Information Systems, V.15, (7), pp. 984-1001, 2021. Doi:10.1080/17517575.2020.1720827
99. Chaumont M. Deep learning in steganography and steganalysis // Digital Media Steganography, Academic Press. 2020. P. 321–349
100. Fridrich J., Golja M., Du R. Reliable Detection of LSB Steganography in Color and Grayscale Images. Proceedings of the 2001 workshop on Multimedia and security: new challenges. -pp.27–30. URL: https://doi.org/10.1145/1232454.1232466
101. Xu G., Wu H.Z., Shi Y.Q. Structural design of convolutional neural networks for steganalysis // IEEE Signal Process. Lett. 2016. V. 23, No. 5. P. 708–712. 39.
102. Дайырбаева Э.Н. Использование RS анализа в стеганографии // МНСК-2022 Информационные технологии Материалы 60-ой Международной научной студенческой конференции. – Новосибирск, РФ, 2022. – С.9
103. Ye J., Ni J., Yi Y. Deep learning hierarchical representations for image steganalysis // IEEE Trans Inf Forensics Secur. 2017. V. 12, No. 11. P. 2545-–255
104. Chhikara S., Kumar R. Information theoretic steganalysis of processed image LSB steganography //Multimedia Tools and Applications. – 2023. – Т. 82. – №. 9. – С. 13595-13615.
105. Chiesa V. An approach for detecting global image manipulations. – 2014.
106. Zhang, H., Ping, X., Xu, M. *et al.* Steganalysis by subtractive pixel adjacency matrix and dimensionality reduction. *Sci. China Inf. Sci.* 57, 1–7 (2014). <https://doi.org/10.1007/s11432-013-4793-x>
107. Hassan Farsi and Amir Shahi. Steganalysis of images based on spatial domain and two-dimensional JPEG array. (2014) Journal of the Chinese Institute of Engineers, V. 37, (8). pp. 1055-1063. doi = 10.1080/02533839.2014.929711
108. Гонсалес-Артеага Л.В., Паредес-Пенуэла Р., Рейес-Гарсия Э. A Study of Steganalysis Based on SPAM Features and Boosting Algorithms, 2009.
109. Грачев Я.Л., Сидоренко В.Г. Стегоанализ методов скрытия информации в графических контейнерах. Надежность. 2021;21(3):39-46. https://doi.org/10.21683/1729-2646-2021-21-3-39-46
110. Частикова В. А., Аббасов Т. О., Аббасова С. С. Методика распознавания скрытой информации в изображениях на основе алгоритмов стеганографии //Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2020. – №. 3 (266). – С. 40-45.
111. Назаренко Ю.Л. Стегоанализ метода сокрытия информации в изображении замены наименьшего значащего бита (LSB) //European science. – 2018. – №. 3 (35). – С. 23-27.
112. Киселева А. В., Кудрина М. А. Стеганография и методы стегоанализа //Перспективные информационные технологии (ПИТ 2017). – 2017. – С. 226-229.
113. Курс К. С., Сабирзянова Э. И., Кротова Е. Л. LSB-стеганография //Автоматизированные системы управления и информационные технологии. – 2020. – С. 465-472.
114. Кириченко А. А., Боровых Н. Е. Оценка ёмкости контейнеров для графематического метода текстовой стеганографии //Актуальные проблемы технических наук в России и за рубежом. – 2017. – С. 46-48.