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](#_Toc135514435)

[**ОПРЕДЕЛЕНИЯ** 4](#_Toc135514436)

[**ОБОЗНАЧЕНИЯ И СООКРАЩЕНИЯ** 5](#_Toc135514437)

[**ВВЕДЕНИЕ** 6](#_Toc135514438)

[1 МЕТОДЫ ВНЕДРЕНИЯ СТЕГАНОГРАФИИ И СТЕГОНАЛИЗА 13](#_Toc135514439)

[1.1 Введение 13](#_Toc135514440)

[1.2 Обзор существующих методов внедрения данных в изображения 17](#_Toc135514441)

[1.2.1 LSB метод 18](#_Toc135514442)

[1.2.2 Алгоритм дискретного косинусного преобразования (DCT) 20](#_Toc135514443)

[1.2.3 Вейвлет –преобразование 22](#_Toc135514444)

[1.2.4 Практическое применение методов внедрения ЦВЗ 25](#_Toc135514445)

[1.3 Обзор известных методов стегоанализа 29](#_Toc135514446)

[1.3.1 RS – метод 31](#_Toc135514447)

[1.3.2 SPAM метод 33](#_Toc135514448)

[1.3.3 Метод Хи-квадрат 33](#_Toc135514449)

[1.4 Выводы по разделу 36](#_Toc135514450)

[2 ИНТЕРПОЛЯЦИЯ ИЗОБРАЖЕНИЯ 37](#_Toc135514451)

[2.1 Постановка задачи 37](#_Toc135514452)

[2.2 Понятие интерполяции 40](#_Toc135514453)

[2.3. Общие сведения об интерполяции Лагранжа 43](#_Toc135514454)

[2.4 Метод INMI 44](#_Toc135514455)

[2.3.5 Метод NMI 46](#_Toc135514456)

[2.6 Выводы по разделу 48](#_Toc135514457)

[3 РЕЗУЛЬТАТЫ И СРАВНЕНИЯ 49](#_Toc135514458)

[3.1 Кривая Безье 49](#_Toc135514459)

[3.2 52](#_Toc135514460)

[3.3 52](#_Toc135514461)

[3.4 Выводы по разделу 52](#_Toc135514462)

[4 ОПИСАНИЕ ПРОГРАММНЫХ СРЕДСТВ 53](#_Toc135514463)

[**СПИСОК ИСПОЛЬЗОВАННЫХ ЛИТЕРАТУР** 54](#_Toc135514464)

# **НОРМАТИВНЫЕ ССЫЛКИ**

В настоящей диссертации использованы нормативные ссылки на следующие стандарты:

# **ОПРЕДЕЛЕНИЯ**

В настоящем диссертации использованы следующие термины с соответствующими определениями:

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

Голограмма – объёмное изображение, воспроизведённое [интерференцией волн](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D0%B8%D1%8F_%D0%B2%D0%BE%D0%BB%D0%BD) 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.

Пустой контейнер - это контейнер без встроенного сообщения.

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.).

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

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

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

# **ОБОЗНАЧЕНИЯ И СООКРАЩЕНИЯ**

|  |  |
| --- | --- |
| DCT | Дискретное косинусное преобразование |
| INMI | Improved neighbor mean interpolation |
| LSB | Least Significant Bit (Наименее значимый бит) |
| NMI | Neighbor mean interpolation |
| RS | Regular–Singular (регулярно-сингулярный) |
| ЦВЗ | Цифровой водяной знак |
| SPAM | Statistic-based Pixel Adjacency Model |
| 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)) |

# **ВВЕДЕНИЕ**

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

Разработка стеганографических алгоритмов – это процесс создания методов, позволяющих скрыть информацию в изображениях таким образом, чтобы это не было заметно для человеческого восприятия. Основная задача при этом – обеспечить надежность сохранности скрытой информации при различных воздействиях, таких как сжатие, шумы 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 и скорость внедрения. Оценка и тестирование позволяют определить эффективность алгоритма и убедиться в том, что он может быть использован для скрытия информации в конкретных условиях.

Исследование стеганографических алгоритмов является важным направлением в области криптографии и информационной безопасности. 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: В.Г. Грибунин, 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:**

* **Daiyrbayeva E.N.,** Yerimbetova A.S., Murzin F.A., Lipskaya M.A. Processing of Images Using Orthogonal Matrixes // Bulletin of the National Engineering Academy of the Republic of Kazakhstan. – Almaty, 2020. – No. 3(2020). – P.103-112
* **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.,** Еримбетова А.С., Мурзин Ф.А., Липская М.А. Processing of Images Using Orthogonal Matrixes. Вестник НИА РК, №3 (2020). -стр. 103-112 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
* **Daiyrbayeva E.,** Yerimbetova A., Toigozhinova A. Comparative analysis of the results of image recovery based on the strip method using various matrices. "Вестник НАН РК", серия «Физ-мат". – Алматы: 2021. – №4, – С.29-34
* **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.** Восстановление изображений на основе стрип-метода. МНСК-2020 ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ Материа-лы 58-й Международной научной студенческой конференции, 10–13 апреля 2020 г., г. Новосибирск, РФ, стр.77
* **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
* Маратов Ж.С., **Дайырбаева Э.Н.**, Еримбетова А.С. Визуализация архитектуры вычислительной системы с помощью AUTOCAD ELECTRICAL // Материалы I Международной научно-практической конференции «Инновационные технологии на транспорте: образование, наука, практика». Алматы (АЛиТ), 2021. – С.113-114.
* **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 15 работ: 8 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); 6 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 «обложками» 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 [1-6].

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 [7-9].

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.

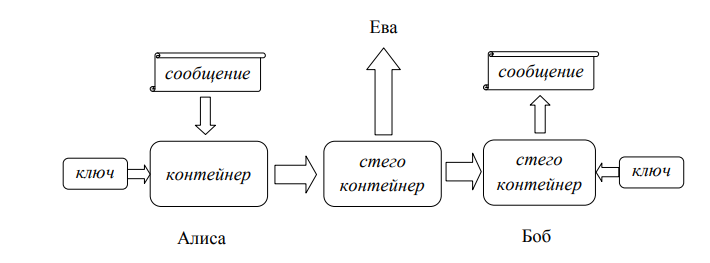


Рисунок 1.1 - Схема передачи секретного сообщения

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: В.Г. Грибунин, 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 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 [14-16].

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 [17] 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) [25] - 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 [21-22].
3. Masking and Filtering – 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 [24].
4. Phase Coding – 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) - 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) - этот метод использует дискретное косинусное преобразование для разложения изображения на компоненты частоты. Данные затем встраиваются в наименее значимые коэффициенты преобразования.
7. Вейвлет – преобразование – 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 [26-30].

# 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 [31].

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.

Для внедрения данных в изображение с помощью метода LSB используется битовая маска, которая позволяет выбирать определенный бит каждого пикселя. Затем выбранные биты заменяются на биты скрываемого сообщения.

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 [32-35], таких как внедрение водяных знаков, но для передачи большого объема данных лучше использовать более сложные методы стеганографии.

Авторы [36] 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 обложки 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.

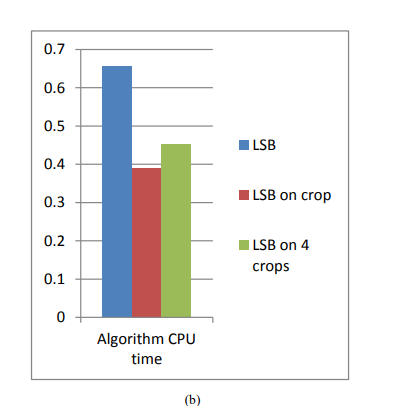
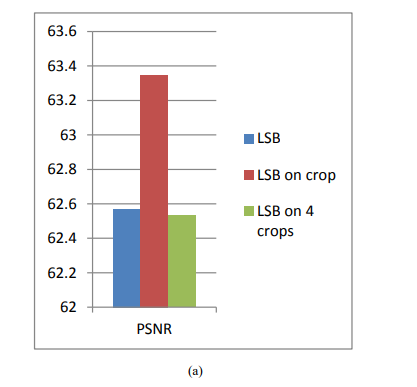


Рисунок 1.2 - (a) PSNR для изображения stego, (b) процессорное время в секундах.

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.

В статье [37] 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 рисунку 1.4, тогда можно увидеть что, предложенный подход авторами позволяет внедрить больше данных, чем существующий метод GLM.

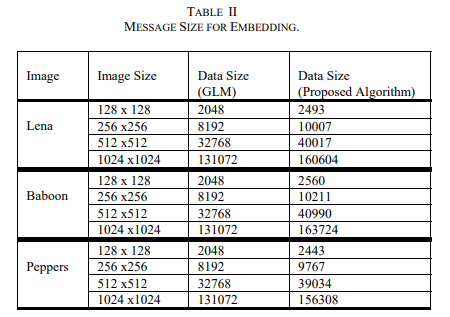


Рисунок 1.4 –Размеры сообщении для внедрения

Авторами PSNR был использован для оценки качества стего-изображения после встраивания секретного сообщения в «обложку». 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.1.5)

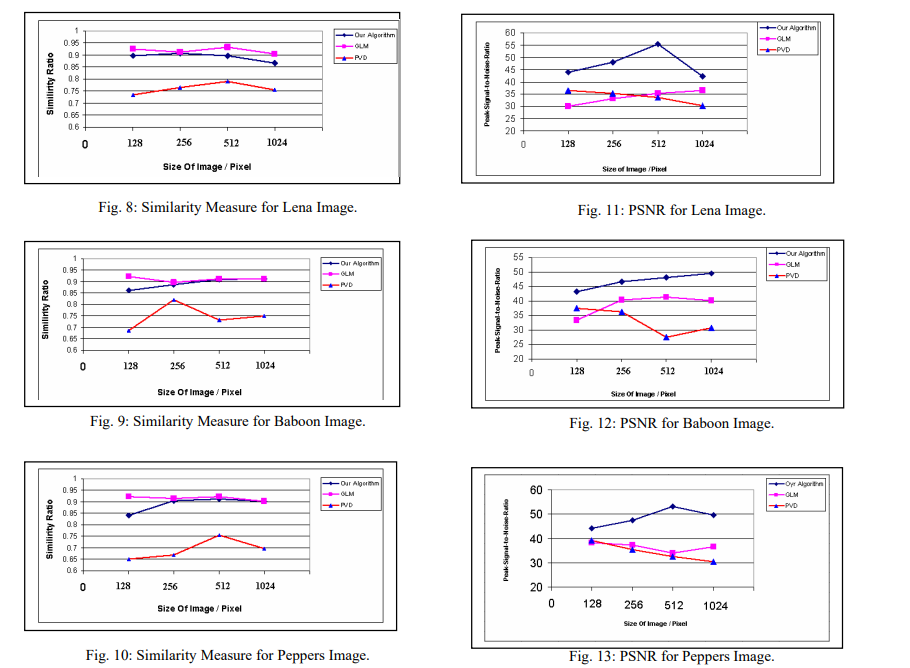


Рисунок 1.5 –Результаты эксперимента

В целом, [37] 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 [38] 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%. В предложенной статье схеме LSBMR-EA размер подблока составлял 4, а ключ поворота генерировался случайным образом. Протестированные коэффициенты скрытия составили 10%, 30%, 50% и 90% от возможности встраивания изображения на обложке. Экспериментальные результаты показывают, что предложенный метод устойчив не только к RS-атаке, но и к методам x2-детектирования.

Работа [39] 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 обложки для сокрытия зашифрованного секретного сообщения, пиковое отношение сигнал/шум (PSNR) линейно уменьшается, а качество изображения stego снижается.

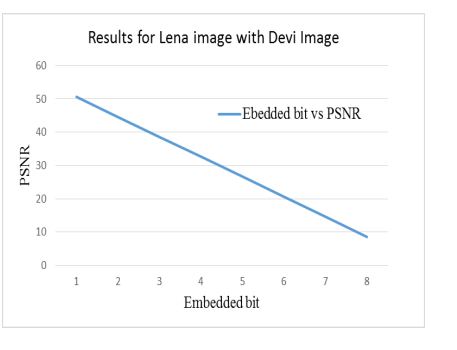


Рисунок 1.6 –Результаты эксперимента по картинке Lena

В работах [40-43] 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. Конец формы

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 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.

Стегаонографический 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 [44-52] 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 [53-62] 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 [63-65] 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 [67]. 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. 1.3

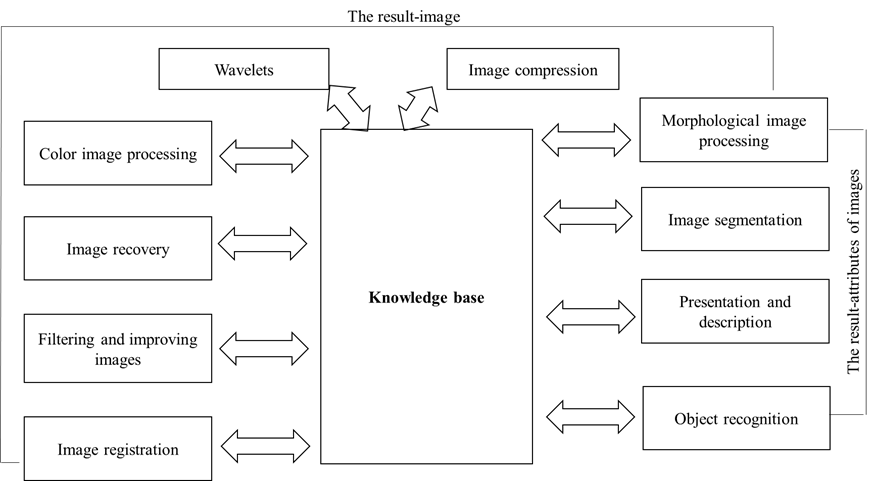


Рисунок 1.3 - Основные этапы обработки цифровых изображений

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 [68,69]. 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) - 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 [66].

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 [70-76].

# 1.2.4 Практическое применение методов внедрения ЦВЗ

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. Цифровые водяные знаки (ЦВЗ) используются для различных целей, таких как защита авторских прав, аутентификация, мониторинг и отслеживание [77].

Основной принцип работы цифровых водяных знаков заключается во встраивании некоторой информации в цифровое содержимое, которая не заметна для человеческого глаза или уха. Эта информация может быть извлечена только с помощью специальных алгоритмов обработки данных. Содержимое ЦВЗ может содержать паспортные данные автора контейнера и быть продемонстрированным в суде для установления авторства.

Существует множество исследований, посвященных разработке новых методов встраивания водяных знаков и анализу их эффективности [78].

В работе авторов [79] рассматривается теоретический анализ и исследование производительности репрезентативных систем водяных знаков в областях преобразования и геометрически инвариантных областях. Цифровые водяные знаки - это технология встраивания водяных знаков с правами интеллектуальной собственности в изображения, видео, аудио и другие мультимедийные данные по определенному алгоритму. Основными характеристиками цифрового водяного знака являются незаметность, пропускная способность, надежность и ложно-положительность алгоритма нанесения водяных знаков, а также безопасность места сокрытия. Более того, делается вывод о том, что для оценки систем нанесения водяных знаков используются различные операторы атак, что обеспечивает автоматизированный и объективный анализ существенных методов нанесения водяных знаков для выбранных областей применения.

В работе [80] авторы приходят к обычно неявному предположению, что цифровые водяные знаки имеют в качестве своей основной цели приложения для защиты авторских прав и копирования. Из этих целевых приложений делается очень много выводов о необходимой безопасности системы водяных знаков, и фактически значительная часть литературы по водяным знакам уделяет именно этой теме основное внимание. В данной работе авторы делают шаг назад и попытаються провести более тщательный анализ парадигмы «водяные знаки для приложений безопасности». Целью данной статьи являются: обсудить значение концепции безопасности в контексте водяных знаков и попытаться показать, что нужно быть осторожным при использовании аналогий из смежной области криптографии.

В [81] работе исследователи отмечают что, цифровые водяные знаки, традиционно моделируемые как связь со вспомогательной информацией, обычно считаются имеющими важные потенциальные применения в различных сценариях, таких как управление цифровыми правами. Однако в современной литературе основное внимание уделяется надежности, пропускной способности и незаметности. Отсутствует систематический формальный подход к решению проблем безопасности нанесения водяных знаков. В этой статье они рассматривают различные концепции и модели безопасности, использованные в предыдущим работе, и обсудили возможные направления будущих исследований.

В статье [82] авторами представлен безопасный (устойчивый к несанкционированному доступу) алгоритм нанесения водяных знаков на изображения и методология нанесения цифровых водяных знаков, которые могут быть обобщены на аудио, видео и мультимедийные данные. Авторы поддерживают такую идею, чтобы водяной знак был сконструирован как независимый и идентично распределенный гауссов случайный вектор, который незаметно вставляется в виде расширенного спектра в наиболее значимые для восприятия спектральные компоненты данных. На основе исследовании авторов можно предположить что, вставка водяного знака в этом режиме делает водяной знак устойчивым к операциям обработки сигналов (таким как сжатие с потерями, фильтрация, цифроаналоговое и аналого-цифровое преобразование, повторная обработка и т.д.) и обычным геометрическим преобразованиям (таким как обрезка, масштабирование, трансляция и поворот) при условии, что исходное изображение доступно и что его можно успешно зарегистрировать на преобразованном изображении с водяными знаками. В данной работе приведены экспериментальные результаты, подтверждающие эти утверждения, наряду с изложением нерешенных проблем.

В книге представлены [83] результаты исследования: цифровое нанесение водяных знаков охватывает важнейшие результаты исследований в этой области: в нем объясняются принципы, лежащие в основе технологий нанесения цифровых водяных знаков, описываются требования, которые привели к их появлению, и обсуждаются различные цели, для которых применяются эти технологии. В результате закладывается дополнительная основа для будущих разработок в этой области, помогающая читателю понять и предвидеть новые подходы и приложения.

В следующей статье [84] изучается нанесение водяных знаков на цифровые изображения. Авторами проанализированы типичные цифровые алгоритмы нанесения водяных знаков, основанные на пространственной области и области преобразования, а также ключевые достижения в алгоритмах нанесения водяных знаков, основанных на дискретном вейвлет-преобразовании. Авторы разработали улучшенный алгоритм нанесения водяных знаков вслепую и алгоритм нанесения водяных знаков на цветные изображения. В результате на основе двух улучшенных алгоритмов нанесения водяных знаков авторами разрабатывается алгоритм двойного нанесения водяных знаков. Оба они разделены, но связаны между собой. Он аутентифицирует двойные алгоритмы нанесения водяных знаков в дополнение к субъективной визуальной оценке, но также использует числовую объективную оценку и количественный анализ. Экспериментальные результаты данной работы показывают, что этот алгоритм двойного нанесения водяных знаков обладает хорошей надежностью и свойствами маскировки.

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.

# Обзор известных методов стегоанализа

Стегоанализ - это процесс обнаружения наличия стеганографического сообщения в носителе, то есть анализа изображений, аудио или видео файлов с целью обнаружения скрытой информации [85,86]. Некоторые известные методы стегоанализа включают в себя:

* Анализ статистических свойств: этот метод основывается на анализе статистических свойств носителя, таких как распределение пикселей, корреляция и энтропия. Изменения в этих свойствах могут указывать на наличие скрытой информации.
* Анализ на основе машинного обучения: этот метод использует алгоритмы машинного обучения для обнаружения скрытых сообщений. Алгоритмы машинного обучения могут использоваться для обнаружения изменений в паттернах или свойствах носителя, которые указывают на наличие стеганографического сообщения.
* Анализ на основе моделей: этот метод использует математические модели для анализа носителя и обнаружения скрытых сообщений. Модели могут основываться на знании о том, каким образом скрытая информация была внедрена в носитель.
* Анализ на основе спектральных свойств: этот метод основывается на анализе спектральных свойств носителя, 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:

1. Анализ на основе графов: одна из последних работ в этой области использует теорию графов для анализа стеганографических сообщений. Работа показывает, что использование графов может помочь улучшить точность обнаружения стеганографических сообщений.
2. Машинное обучение с глубокими нейронными сетями: новые исследования используют глубокие нейронные сети для стегоанализа изображений и видео. Эти сети могут обнаруживать изменения в пикселях и фреймах, которые указывают на наличие скрытой информации.
3. Анализ на основе многомерных статистических свойств: новые методы используют многомерные статистические свойства, такие как совместная энтропия, для обнаружения стеганографических сообщений. Эти методы могут быть особенно эффективны для обнаружения сообщений, внедренных с использованием более сложных алгоритмов стеганографии.
4. Анализ на основе моделей глубокого обучения: новые исследования используют модели глубокого обучения для анализа носителя и обнаружения стеганографических сообщений. Эти методы могут использовать знания о том, каким образом сообщение было внедрено в носитель, чтобы улучшить точность обнаружения.
5. Обнаружение сообщений с использованием машинного зрения: некоторые новые работы используют алгоритмы машинного зрения для обнаружения скрытой информации в изображениях. Эти методы могут обнаруживать изменения в текстуре, цветовых свойствах и других характеристиках изображения, которые указывают на наличие стеганографического сообщения.
6. Использование генетических алгоритмов: некоторые новые методы используют генетические алгоритмы для обнаружения скрытой информации в носителе. Эти методы могут использовать эволюционные алгоритмы для поиска оптимальных параметров для обнаружения стеганографического сообщения [87-89].

# 1.3.1 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. [90,91] 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. Для групп пикселов определяется функция регулярности . Под значением пикселов понимаем число от 0 до 255.

 (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:

 и  (2)

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

если  то ;

если  то ;

если  то .

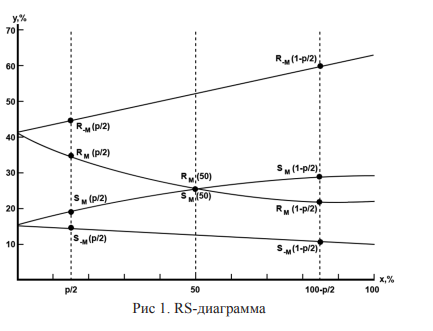
Метод RS может указать маленькую ненулевую длину сообщения из-за случайных отклонений даже для пустого контейнера. Это начальное ненулевое отклонение может быть, как положительным, так и отрицательным и накладывает ограничение на достижимую точность RS анализа.

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



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 пиксельной соседности 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, спрятанной внутри пакетов данных. Суть метода состоит в том, чтобы анализировать статистические свойства пакетов данных, таких как распределения IP-адресов и портов, структура заголовков пакетов и другие факторы. Если в данных присутствует скрытая информация, то статистические свойства пакетов могут измениться в тех областях, где скрытая информация была внедрена. Кроме того, SPAM может обнаружить небольшие изменения в данных, которые могут оставаться незамеченными другими методами [93,94].

При использовании SPAM для стегоанализа следует иметь в виду, что этот метод может быть ограничен в случае, если скрытая информация была внедрена в абсолютен новые или необычные области данных, которые не могут быть анализированы статистически. Также, метод может быть более требовательным к вычислительным мощностям, нежели другие методы стегоанализа, особенно при анализе больших объемов данных.

В работах авторов [95,96] 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 пиксельной соседности для обнаружения скрытых сообщений в JPEG изображениях.

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) - 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 данных. Если наблюдаемое распределение отличается от ожидаемого распределения, 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 ложноположительные результаты, если наблюдаемое распределение данных не отличается от ожидаемого распределения случайным образом. 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 ранних работ в этой области является статья "A Statistical Approach to Detection of LSB Steganography in Grayscale Images" (2002) авторов Нейла Ф. Джонса и Джессины Ф. Абрамс. В этой статье авторы использовали метод Хи-квадрат для обнаружения скрытых сообщений, встроенных с использованием метода младшего значащего бита (LSB) в оттенках серого изображений.

В работе "Steganalysis of Spread Spectrum Data Hiding Using a Subspace Approach" (2005) авторы Эндрю Кер и Герберт К. Ли использовали метод Хи-квадрат в сочетании с методом анализа подпространства, чтобы обнаружить скрытые сообщения в данных, которые были встроены с использованием метода распространения спектра.

В статье "LSB Matching and Its Generalization in Spatio-Temporal Steganography" (2011) авторы Кейхидзи Огава и Мидори Китагава использовали метод Хи-квадрат для обнаружения скрытых сообщений в мультимедийных данных, которые были встроены с использованием метода LSB Matching.

В работе "A Novel Approach to Detecting JSteg Steganography in Images" (2012) авторы Мингченг Чен и Кун Шэнь использовали метод Хи-квадрат в сочетании с методом анализа текстуры для обнаружения скрытых сообщений в изображениях, которые были встроены с использованием метода JSteg.

Другие исследования используют метод Хи-квадрат для оценки эффективности различных методов стеганографии. Например, в статье "Comparative Study of Various Image Steganography Techniques: A Review" (2015) авторы Ибрагим Абдуллаев и Абу Бакр Билял использовали метод Хи-квадрат для сравнения эффективности различных методов встраивания скрытых сообщений в изображения.

В целом, метод Хи-квадрат остается важным инструментом в стегоанализе, и его применение может быть расширено и улучшено с помощью дальнейших исследований в этой области. Одно из ранних исследований, проведенное Кривсаном (Krivic et al., 2005), показало, что метод Хи-квадрат может использоваться для обнаружения сообщений, встроенных с помощью методов стеганографии на основе замены младших битов. Исследование также показало, что этот метод может обнаружить сообщения, встроенные с помощью методов, использующих прямое изменение значений пикселей.

В более поздних исследованиях Хо и Шу (Ho and Shu, 2009) было продемонстрировано, что метод Хи-квадрат может быть эффективно использован для обнаружения сообщений, встроенных с помощью методов стеганографии на основе изменения переходов, методов на основе замены пикселей и методов на основе изменения порядка пикселей. Они также провели исследование влияния размера сообщения на эффективность обнаружения с помощью метода Хи-квадрат.

Большинство исследований, проведенных в последнее время, используют метод Хи-квадрат в сочетании с другими методами стегоанализа, такими как методы машинного обучения и методы анализа текстур. Например, Чен и др. (Chen et al., 2015) использовали метод Хи-квадрат и метод анализа текстур Габора для обнаружения скрытых сообщений, встроенных с помощью методов стеганографии на основе изменения переходов и методов на основе замены пикселей.

Недавнее исследование Кханг и Хо (Khang and Ho, 2021) показало, что метод Хи-квадрат может быть эффективно использован для обнаружения скрытых сообщений, встроенных с помощью методов стеганографии, которые используют множественные уровни интенсивности пикселей.

Например, некоторые исследования 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.

Некоторые работы также исследуют применение метода Хи-квадрат в комбинации с другими методами стегоанализа, такими как методы машинного обучения или методы анализа текстур, чтобы улучшить точность обнаружения скрытых сообщений. Так же некоторые исследования также исследуют применение метода Хи-квадрат в сочетании с другими методами стеганографии, чтобы создать более эффективные методы встраивания скрытых сообщений.

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. Выводы по разделу

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

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

Оценка эффективности алгоритма внедрения оценивается объемом данных, которое встраивается в контейнер при котором вероятность выявления мала.

В стегоанализе эффективными методами считаются:

* RS анализ;
* SPAM.

В целом, выше представленные методы продолжают оставаться важным инструментом в стегоанализе, и их применение может быть расширено и улучшено с помощью дальнейших исследований в этой области. Эффективность стегоанализа оценивается по вероятности выявления и отсутствии ошибочных срабатываний на пустых контейнерах.

# **СПИСОК ИСПОЛЬЗОВАННЫХ ЛИТЕРАТУР**

1. Китани М. Методы и системы сокрытия информации. – М.: Техносфера, 2003. – 336 с.
2. Дэвид Н., Форсайт Дж. Стеганография и цифровые водяные знаки. – М.: Издательский дом «Вильямс», 2002. – 344 с.
3. Кори Б., Буррес С. Методы и системы сокрытия информации: основы теории и применения. – М.: Техносфера, 2013. – 400 с.
4. Лэй Х., Уайт М. Information Hiding - A Survey // Proceedings of the IEEE. – 1998. – Т. 86. – №. 6. – С. 1062-1078.
5. Кэмпбелл М. Стеганография: техника сокрытия информации // Журнал «Хакер». – 2003. – №. 56. – С. 30-37.
6. Фридрихс Дж., Свенсон А. Методы стеганографии // Наука и жизнь. – 2001. – №. 6. – С. 42-47.
7. 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
8. Колчин А.А. Методы и алгоритмы стеганографии // Информационно-измерительные и управляющие системы. – 2005. – №. 4. – С. 20-25.
9. Китани М. Методы и системы сокрытия информации. – М.: Техносфера, 2003. – 336 с.
10. Дэвид Н., Форсайт Дж. Стеганография и цифровые водяные знаки. – М.: Издательский дом «Вильямс», 2002. – 344 с.
11. Кори Б., Буррес С. Методы и системы сокрытия информации: основы теории и применения. – М.: Техносфера, 2013. – 400 с.
12. Лэй Х., Уайт М. Information Hiding - A Survey // Proceedings of the IEEE. – 1998. – Т. 86. – №. 6. – С. 1062-1078.
13. Кэмпбелл М. Стеганография: техника сокрытия информации // Журнал «Хакер». – 2003. – №. 56. – С. 30-37.
14. Фридрихс Дж., Свенсон А. Методы стеганографии // Наука и жизнь. – 2001. – №. 6. – С. 42-47.
15. Колчин А.А. Методы и алгоритмы стеганографии // Информационно-измерительные и управляющие системы. – 2005. – №. 4. – С. 20-25.
16. Китани М. Техника сокрытия данных на основе LSB метода // Информационные технологии. – 2004. – №. 10. – С. 56-61.
17. Китани М. Методы и системы сокрытия информации. – М.: Техносфера, 2003. – 336 с.
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. Кэмпбелл М. Стеганография: техника сокрытия информации // Журнал «Хакер». – 2003. – №. 56. – С. 30-37.
22. Фридрихс Дж., Свенсон А. Методы стеганографии // Наука и жизнь. – 2001. – №. 6. – С. 42-47.
23. Колчин А.А. Методы и алгоритмы стеганографии // Информационно-измерительные и управляющие системы. – 2005. – №. 4. – С. 20-25.
24. Китани М. Техника сокрытия данных на основе LSB метода // Информационные технологии. – 2004. – №. 10. – С. 56-61.
25. 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.
26. 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.
27. 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.
28. 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.
29. Китани М. Техника сокрытия данных на основе LSB метода // Информационные технологии. – 2004. – №. 10. – С. 56-61.
30. 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.
31. 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.
32. Китани М. Методы и системы сокрытия информации. – М.: Техносфера, 2003. – 336 с.
33. Кори Б., Буррес С. Методы и системы сокрытия информации: основы теории и применения. – М.: Техносфера, 2013. – 400 с.
34. Янг У. Реализация алгоритма стеганографии на основе LSB метода // Труды Международной конференции по компьютерной безопасности и криптографии. – 2012. – С. 143-147.
35. Ань Л., Жан Ч., Пай Ж. Обзор и анализ методов стеганографии // Информационные технологии. – 2016. – №. 5. – С. 11-16.
36. F. Petitcolas, R. Anderson and M. Kuhn, "Information hiding-a survey," in Proceedings of the IEEE, vol. 87, no. 7, pp. 1062-1078, July 1999, doi: 10.1109/5.771065.
37. 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.
38. 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.
39. Deshmukh P.U., Pattewar T.M. A novel approach for edge adaptive steganography on LSB insertion technique (2015) 2014 International Conference on Information Communication and Embedded Systems, ICICES 2014, DOI: 10.1109/ICICES.2014.7033807
40. Arora, Himanshu & Bansal, Cheshta & Dagar, Sunny. (2018). Comparative study of image steganography techniques. 982-985. DOI:10.1109/ICACCCN.2018.8748451
41. 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>
42. Chengqing Li, Jiashu Zhang, and Xiaoxiao 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>
43. Ritu Kaur, Pawan 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>
44. "Performance Comparison of DCT-Based Steganography Techniques Using LSB and PN Sequence" by K. M. Habib and M. A. Karim.
45. "A Comparative Study of DCT-Based Steganography Techniques" by H. R. Nagarahalli and S. P. Raju.
46. "Performance Evaluation of Various DCT-Based Steganography Techniques" by G. V. K. Durga and S. Koppula.
47. "An Empirical Study on the Performance Analysis of DCT-Based Steganography Techniques" by M. Arthavathi and S. S. Kumar.
48. "Performance Evaluation of DCT-Based Steganography Techniques Using Different Cover Images" by M. A. Karim and K. M. Habib.
49. "A Comparative Analysis of DCT-Based Steganography Techniques" by R. S. Reddy and K. S. Rao.
50. "Performance Analysis of DCT-Based Steganography Techniques in Different Color Spaces" by M. R. Chandran and V. Mathivanan.
51. "A Comparative Study of DCT-Based Steganography Techniques using Digital Images" by S. V. Ramesh and M. Venkatesan.
52. "Performance Analysis of DCT-Based Steganography Techniques using Different Embedding Techniques" by N. M. Solanki and V. K. Srivastava.
53. "A new approach to steganography based on DCT and discrete wavelet transform" by J. Li and S. Li.
54. "An efficient image steganography algorithm based on DCT and quantization" by Berna Gökmenoğlu and İsmail Avcı.
55. "Robust image steganography using DCT and LSB substitution" by S. K. S. Sivaiah and M. Rajesh Kumar.
56. "A novel secure data hiding technique in medical images based on DCT and LSB substitution" by K. Revathi and D. Sridharan.
57. "A novel steganographic technique based on DCT and multiple LSB substitution" by Manju Khari and Anjana Jain.
58. "A robust and efficient steganography technique using DCT and secret key encryption" by Ravinder Kumar and Manoj Kumar.
59. "A novel reversible data hiding technique based on DCT and histogram shifting" by Yong Xie and Jun Zhang.
60. "A new perceptually based image steganography technique based on DCT and visual masking" by S. S. Lakshmi and R. S. Rajesh.
61. "A new approach to robust steganography based on DCT and basis functions" by Zhihua Xia and Guoping Qiu.
62. "A new steganographic technique based on DCT and random walk" by M. C. Gupta and S. K. Singh.
63. Yuqing Li., Zebiao Guan., Chi Xu. Digital Image Self Restoration Based on Information Hiding. 2018 37th Chinese Control Conference (CCC)
64. Jun Xiao., Bin Qin., Yusheng Sun., Xiao Xu. Research of multi-direction transition probability matrices algorithm for JPEG steganalysis. 2012 - 24th Chinese Control and Decision Conference (CCDC)
65. 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 Processing10 September 2020Volume 179
66. 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>
67. 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.
68. 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.
69. 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.
70. R. Zheng, C. Wang, and Y. Miao, "A robust steganographic method based on wavelet transform," International Conference on Cyber Security, pp. 18-24, 2013.
71. 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.
72. 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.
73. 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.
74. 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.
75. 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.
76. M.S. Ali, A.R. Ansari, and S.K. 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.
77. Ingemar Cox, Matthew Miller, and Jeffrey Bloom. Digital Watermarking and Steganography, 2nd Edition. -Morgan Kaufmann Publishers Publication date: December 2007
78. Xiaolong Li and Shuyuan Yang (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 Volume: 8 Issue: 2 Pages: 71-80
79. (2014) Robust Image Watermarking Theories and Techniques: A Review. Journal of Applied Research and Technology. JART. Vol. 12. Issue 1.pages 122-138. DOI: 10.1016/S1665-6423(14)71612-8
80. T. Kalker, "Considerations on watermarking security," 2001 IEEE Fourth Workshop on Multimedia Signal Processing (Cat. No.01TH8564), Cannes, France, 2001, pp. 201-206, DOI:10.1109/MMSP.2001.962734
81. Li, Q., Memon, N. (2007). Security Models of Digital Watermarking. In: Sebe, N., Liu, Y., Zhuang, Y., Huang, T.S. (eds) Multimedia Content Analysis and Mining. MCAM 2007. Lecture Notes in Computer Science, vol 4577. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-73417-8\_12
82. I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia," in IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, Dec. 1997, DOI:10.1109/83.650120
83. Ingemar Cox, Matthew Miller, Jeffrey Bloom, Mathew Miller. Digital Watermarking. eBook ISBN: 9780080504599
84. Fang Y., Han B., Zhang Y., Tian L. A novel dual watermarking algorithm for digital images. (2016) International Journal of Simulation: Systems, Science and Technology, 17 (44), pp. 34.1-34.8. DOI: 10.5013/IJSSST.a.17.44.34
85. 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
86. 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
87. 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.
88. 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
89. Fhf
90. Fridrich J., Golja M., Du R. . Reliable Detection of LSB Steganogra-phy in Color and Grayscale Images. Proceedings of the 2001 workshop on Multimedia and security: new challenges. 2001 -pp.27–30. URL: https://doi.org/10.1145/1232454.1232466
91. Vil'khovskiy D.E. Algoritmy steganograficheskogo analiza izobrazheniy s nizkim zapolneniyem stegokonteynera:diss….kand. tekh. nauk: 05.13.19 — Omsk: Omskiy gosudar-stvennyy universitet im. F.M. Dostoyevskogo,2021-p.135 URL: https://www.ugatu.su/media/uploads/MainSite/Science/dissovet/07/2020/vilkhovsky-de/dissert\_vilkhovsky-de.pdf
92. Daiyrbayeva, E., Yerimbetova, A., Nechta, I., Merzlyakova, E., Toigozhinova, A., & Turganbayev, A. (2022). A Study of the Information Embedding Method into Raster Image Based on Interpolation. Journal of Imaging, 8(10), 288.
93. 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>
94. 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
95. Гонсалес-Артеага Л.В., Паредес-Пенуэла Р., Рейес-Гарсия Э. "A Study of Steganalysis Based on SPAM Features and Boosting Algorithms", 2009.
96. Li, H., Huang, W., & Fu, J. (2011). Steganalysis of JPEG Images Using Rich Models.
97. 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