# Введение

В современном мире, благодаря активному развитию технологий, передача и дублирование данных осуществляется достаточно просто. В связи с этим остро стоит вопрос о защите интеллектуальной собственности . Нередко возникают ситуации незаконного копирования и использования произведений интеллектуальной собственности. В таких случаях автор вынужден обращаться в суд и доказывать свое исключительное право на собственное произведение. Но как это сделать?

Существует такое понятие, как презумпция авторства, которое означает, что лицо, указанное в качестве автора на оригинале или экземпляре произведения считается его автором, если не доказано иное. Однако в случае с цифровым контентом это можно легко подделать. Можно назначить экспертизу по установлению авторства, но это долгая, сложная, а главное, дорогая процедура.

Каждый автор желает защитить свои произведения. К сожалению, в наше стране нет такого понятия, как государственная регистрация авторского права, поэтому люди прибегают к различным способам «собственной» регистрации. Например, рукописи можно отправить по почте самому себе и сохранить, не вскрывая конверта, на котором будет зарегистрирована дата отправления. Тогда в случае необходимости доказать свое авторство, достаточно распечатать конверт. Многие интернет-магазины по продаже стоковых фотографий во избежание копирования и незаконного использования накладывают поверх полупрозрачную надпись с названием магазина размером почти во всю фотографию. Это эффективно, но визуально портит продукт.

Что если «подписывать» фотографию таким образом, чтобы это не было заметно глазу, но при этом было очень сложно удалить, не прибегая к сильным искажениям фотографии? Эту проблему решает один из способов цифровой современной стеганографии – цифровой водяной знак (ЦВЗ). Существует множество различных схем по встраиванию ЦВЗ, заточенных под определенные нужды.

В данной работе будут рассмотрены основные виды ЦВЗ и возможные способы их реализации. Также будет описан один из алгоритмов по встраиванию ЦВЗ в изображения с целью защиты авторских прав и его программная реализация. В основе алгоритма лежит вейвлет-анализ, который является на сегодняшний день одной из самых перспективных технологий анализа данных. Его инструменты находят применение в самых различных сферах интеллектуальной деятельности, таких как фильтрация и предварительная обработка данных, анализ состояния и прогнозирования ситуации на фондовых рынках, распознавание образов. Также он используется при обработке и синтезе различных сигналов, например речевых, медицинских, для решения задач сжатия и обработки изображений, при обучении нейросетей и во многих других случаях.

# 1. Стеганография

Стеганография (от греч. στεγανός «скрытый» + γράφω «пишу»; букв. «тайнопись») — способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи (хранения).

В отличие от криптографии, которая скрывает содержимое тайного сообщения, стеганография скрывает сам факт его существования. Преимущество стеганографии над чистой криптографией состоит в том, что сообщения не привлекают к себе внимания. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её.

Первая запись об использовании стеганографии встречается в трактате Геродота «История», относящегося к 440 году до н. э. В трактате были описаны два метода скрытия информации. Демарат, царь Спарты в 515—491 годах до н.э., отправил предупреждение o предстоящем нападении на Грецию, записав его на деревянную подложку восковой таблички до нанесения воска. Второй способ заключался в следующем: на обритую голову раба записывалось необходимое сообщение, а когда его волосы отрастали, он отправлялся к адресату, который вновь брил его голову и считывал доставленное сообщение.

Существует версия, что древние шумеры одними из первых использовали стеганографию, так как было найдено множество глиняных клинописных табличек, в которых одна запись покрывалась слоем глины, а на втором слое писалась другая. Однако противники этой версии считают, что это было вовсе не попыткой скрытия информации, а всего лишь практической потребностью.

## Виды стеганографии

В настоящее время выделяют три вида стеганографии: классическая, компьютерная и цифровая. Рассмотрим каждый из них подробнее.

### Классическая стеганография

Одним из наиболее распространённых методов классической стеганографии является использование симпатических (невидимых) чернил. Текст, записанный такими чернилами, проявляется только при определённых условиях (нагрев, освещение, химический проявитель и т. д.). Изобретённые ещё в I веке н. э. Филоном Александрийским, они продолжали использоваться как в средневековье, так и в новейшее время, например, в письмах русских революционеров из тюрем.

Существуют также чернила с химически нестабильным пигментом. Текст, написанный этими чернилами, выглядит как текст, написанный обычной ручкой, но через определённое время нестабильный пигмент разлагается, и от текста не остаётся и следа. Хотя при использовании обычной шариковой ручки текст можно восстановить по деформации бумаги, этот недостаток можно устранить с помощью мягкого пишущего узла, наподобие фломастера.

Во время Второй мировой войны активно использовались микроточки микроскопические фотоснимки, вклеиваемые в текст писем.

**Другие примеры классической стеганографии:**

* запись на боковой стороне колоды карт, расположенных в условленном порядке;
* запись внутри варёного яйца;
* «жаргонные шифры», где слова имеют другое обусловленное значение;
* трафареты, которые, будучи положенными на текст, оставляют видимыми только значащие буквы;
* геометрическая форма — метод, в котором отправитель старается скрыть ценную информацию, поместив её в сообщение так, чтобы важные слова расположились в нужных местах или в узлах пересечения геометрического рисунка;
* семаграммы — секретные сообщения, в которых в качестве шифра используются различные знаки, за исключением букв и цифр;
* узелки на нитках и т. д.

### Компьютерная стеганография

Компьютерная стеганография — направление классической стеганографии, основанное на особенностях компьютерной платформы. Приведём некоторые примеры:

* *Использование зарезервированных полей компьютерных форматов файлов.* Суть метода состоит в том, что часть поля расширений, не заполненная информацией о расширении, по умолчанию заполняется нулями. Соответственно мы можем использовать эту «нулевую» часть для записи своих данных. Недостатком этого метода является низкая степень скрытности и малый объём передаваемой информации.
* *Сокрытие информации в неиспользуемых местах гибких дисков*. При использовании этого метода информация записывается в неиспользуемые части диска, к примеру, на нулевую дорожку. Недостатки: маленькая производительность, передача небольших по объёму сообщений.
* *Использование особых свойств полей форматов, которые не отображаются на экране*. Этот метод основан на специальных «невидимых» полях для получения сносок, указателей. К примеру, написание чёрным шрифтом на чёрном фоне. Недостатки: маленькая производительность, небольшой объём передаваемой информации.
* *Использование особенностей файловых систем*. При хранении на жёстком диске файл всегда (не считая некоторых файловых систем, например, ReiserFS) занимает целое число кластеров (минимальных адресуемых объёмов информации). К примеру, в ранее широко используемой файловой системе FAT32 (использовалась в Windows98/Me/2000) стандартный размер кластера — 4 КБ. Соответственно для хранения 1 КБ информации на диске выделяется 4 КБ памяти, из которых 1 КБ нужен для хранения сохраняемого файла, а остальные 3 ни на что не используются — соответственно их можно использовать для хранения информации. Недостаток данного метода: лёгкость обнаружения.

В последнее время приобрели популярность методы, когда скрытая информация передаётся через компьютерные сети с использованием особенностей работы протоколов передачи данных. Эта разновидность компьютерной стеганографии получила название «**сетевая стеганография**». Типичные методы сетевой стеганографии включают изменение свойств одного из сетевых протоколов. Кроме того, может использоваться взаимосвязь между двумя или более различными протоколами с целью более надёжного сокрытия передачи секретного сообщения. Сетевая стеганография охватывает широкий спектр методов, в частности:

* *WLAN-стеганография* основывается на методах, которые используются для передачи стеганограмм в беспроводных сетях (Wireless Local Area Networks). Практический пример WLAN-стеганографии — система HICCUPS (Hidden Communication System for Corrupted Networks).
* *LACK-стеганография* — скрытие сообщений во время разговоров с использованием IP-телефонии. Например: использование пакетов, которые задерживаются или намеренно повреждаются и игнорируются приемником (этот метод называют LACK — Lost Audio Packets Steganography) или сокрытие информации в полях заголовка, которые не используются.

Принцип функционирования LACK выглядит следующим образом. Передатчик выбирает один из пакетов голосового потока, и его полезная нагрузка заменяется битами секретного сообщения — стеганограммой, которая встраивается в один из пакетов. Затем выбранный пакет намеренно задерживается. Каждый раз, когда чрезмерно задержанный пакет достигает получателя, незнакомого со стеганографической процедурой, он отбрасывается. Однако, если получатель знает о скрытой связи, то вместо удаления полученных RTP-пакетов он извлекает скрытую информацию.

### Цифровая стеганография

Цифровая стеганография — направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. Но, как правило, данные объекты являются мультимедиа-объектами (изображения, видео, аудио, текстуры 3D-объектов) и внесение искажений, которые находятся ниже порога чувствительности среднестатистического человека, не приводит к заметным изменениям этих объектов. Кроме того, в оцифрованных объектах, изначально имеющих аналоговую природу, всегда присутствует шум квантования; далее, при воспроизведении этих объектов появляется дополнительный аналоговый шум и нелинейные искажения аппаратуры, все это способствует большей незаметности сокрытой информации.

В связи со спецификой данной работы, наибольший интерес представляет цифровая стеганография, а именно сокрытие данных в изображениях. Но прежде чем рассмотреть подробно технологию сокрытия данных в изображении, стоит сказать несколько слов о различных применениях цифровой стеганографии.

## Задачи цифровой стеганографии

Рассмотрим основные задачи, решаемые современной цифровой стеганографией.

1. **Защита конфиденциальной информации от несанкционированного доступа.** Это область использования цифровой стеганографии является наиболее эффективной при решении проблем защиты конфиденциальной информации. Встраивание скрытой информации происходит в общедоступную мультимедийную информацию. Так, например, объем секретного сообщения в звуковых и графических файлах может составлять до 25 - 30 % от размера файла. Причем, аудиовизуальные изменения таковы, что не обнаруживаются при прослушивании и просмотре файлов большинством людей, даже если факт сокрытия известен.Такой способ сокрытия секретной информации используется в военной сфере, а также в случаях, когда нельзя использовать криптографию.
2. **Преодоление систем мониторинга и управления сетевыми ресурсами.** Стеганографические методы позволяют противостоять попыткам контроля над информационным пространством при прохождении информации через серверы управления локальных и глобальных вычислительных сетей.

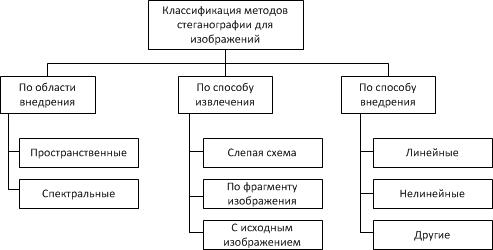
Например, существует утилита Camera/Shy, которая работает на основе браузера Internet Explorer, не оставляя в нем истории деятельности. Используя стеганографическую технику LSB и алгоритм шифрования AES с 256-разрядным ключом, функционирует очень быстро и позволяет скрывать сообщения в gif-файлах. Кроме того, эта программа способна также автоматически сканировать HTML-страницы на наличие графических изображений со скрытой информацией. По заявлению авторов, эта программа была создана “для обхода национальных межсетевых экранов, что дает возможность безопасно обмениваться любым цифровым контентом через Интернет”.

1. **Камуфлирование программного обеспечения (ПО).** Применяется в тех случаях, когда использование ПО незарегистрированными пользователями является нежелательным. ПО может быть закамуфлировано под стандартные универсальные программные продукты (например, текстовые редакторы) или скрыто в файлах мультимедиа и использоваться только лицами, имеющими на это права. Таким образом, обеспечивается многоуровневый санкционированный доступ к ПО.
2. **Защита авторских прав.** Одним из наиболее перспективных направлений компьютерной стеганографии является технология использования цифровых водяных знаков ЦВЗ (digital watermarking) – в данном случае, создание невидимых глазу знаков защиты авторских прав на графические и аудио файлы. Такие ЦВЗ, помещенные в файл, могут быть распознаны специальными программами, которые извлекут из файла много полезной информации: когда создан файл, кто владеет авторскими правами, как вступить в контакт с автором и т.д.

Данная дипломная работа посвящена исследованию способов сокрытия данных в изображении с целью защиты авторских прав. Введем несколько необходимых понятий, рассмотрим возможные способы сокрытия данных в изображении и существующие атаки на них.

## Встраивание информации в изображения

### Основные понятия



Современные компьютерные системы обеспечивают доступность и простоту дублирования фото, аудио, видео и других типов данных. При этом сами данные могут являться цифровой формой представления художественного, литературного, музыкального или иного произведения, на которое распространяется авторское право. В этом случае, для защиты авторского права, наносится специальная метка, которая остается невидимой для глаз, но распознается специальным программным обеспечением (ПО). Такой меткой могут быть цифровой водяной знак и цифровой отпечаток пальца.

**Цифровой водяной знак (ЦВЗ)** – невидимая информация, маркирующая изображение со специальной целью. В частности, ЦВЗ может играть роль метки авторского права, которая вставляется для фиксации владельца изображения, цифровой подписи и др.

**Стойкий (робастный) цифровой водяной знак**  – ЦВЗ, который нельзя удалить или модифицировать даже автору без заметного искажения изображения-носителя.

**Цифровой отпечаток пальца, или идентификационный номер,** – метка, подобная серийному номеру, цель которого идентифицировать случаи нарушения лицензионный соглашений.

**Слепое встраивание информации** – встраивание информации, которое не требует наличия ни исходного изображения, ни самого ЦВЗ для извлечения на стороне получателя.

Схемы встраивания ЦВЗ основаны на том, что зрение человека не чувствительно к малым амплитудным изменениям, а также к малым изменениям во временной или в частотной областях.

В качестве входных данных в любой схеме встраивания ЦВЗ выступают оригинальное изображение (контейнер), встраиваемая информация (ЦВЗ) и, опционально, секретный ключ, ограничивающий доступ к скрытой информации. Встраиваемая информация может быть представлена в виде бинарной последовательности, текста, двумерного объекта, цифрового изображения.

Выходным результатом будет маркированное изображение (стеганоконтейнер), иначе говоря, модифицированное исходное изображение.

Встраиваемые ЦВЗ могут быть трех типов:

* робастные,
* хрупкие,
* полухрупкие.

Под робастностью, как уже было сказано выше, понимается устойчивость ЦВЗ к различных воздействиям на стеганоконтейнер. Робастные ЦВЗ могут быть трех типов. Это ЦВЗ, которые могут быть обнаружены всеми желающими, обнаружены хотя бы одной стороной, либо это могут быть ЦВЗ, которые трудно модифицировать или извлечь из контента (контейнера).

**Хрупкие ЦВЗ** разрушаются при незначительной модификации заполненного контейнера и применяются для аутентификации сигналов (изображений). Отличие от средств электронной цифровой подписи заключается в том, хрупкие ЦВЗ все же допускают некоторую модификацию контейнера. Это важно для защиты мультимедийной информации, так как законный пользователь может, например, пожелать сжать изображение. Другое отличие заключается в том, хрупкие ЦВЗ должны не только отразить факт модификации контейнера, но также вид и местоположение модификации.

**Полухрупкие ЦВЗ** устойчивы по отношению к одним воздействиям и неустойчивы по отношению к другим. Полухрупкие ЦВЗ специально проектируются так, чтобы быть неустойчивыми по отношению к определенного вида операциям. Например, они могут позволять сжатие изображения, но запрещать вырезку из него или вставку в него фрагмента.

### Физиологические особенности человеческого восприятия

При разработке алгоритмов встраивания ЦВЗ необходимо учитывать особенности зрительной системы человека (ЗСЧ), поскольку незаметность внедренных сообщений является одним из главных требований к любой стеганосистеме. Особенности восприятия зрительной систем подразделяются на две группы: низкоуровневые (физиологические) и высокоуровневые (психофизиологические).

Среди низкоуровневых особенностей человеческого восприятия видеоданных выделяют три наиболее важных свойства, влияющих на заметность постороннего шума в изображении:

* чувствительность зрения к изменению контрастности (яркости) изображения;
* частотную чувствительность;
* эффект маскирования сигнала изображения.

дописать

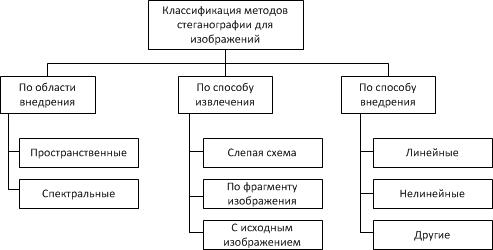
### Классификация методов встраивания ЦВЗ в изображения

Для методов встраивания водяных знаков может использоваться широкий диапазон изменений в любой области. Перед внедрением или извлечением водяного знака исходные данные могут быть преобразованы в пространственную область методом Фурье или дискретного косинусного преобразования, вейвлет-преобразования или даже в область фрактального кодирования, что позволяет использовать конкретные в преобразования. В этих областях могут быть произведены следующие преобразования:

* модификация наименее значимого бита,
* добавление шума,
* изменения порядка коэффициентов,
* удаления коэффициента,
* деформация части данных и блоков на основании их сходства.

Кроме того, если учитывать визуальную модель человека, то визуальное воздействие изменений на человека нужно свести к минимуму. В таком случае модификации могут быть адаптированы с учетом дальнейшей обработки или используемого формата сжатия данных.

Методы встраивания ЦВЗ можно классифицировать по различным критериям, в том числе, по способу их внедрения, по способу извлечения, а также по области встраивания (рис. 1).



**Рис. 1** Классификация методов встраивания ЦВЗ

По способу извлечения скрытой информации из контейнера алгоритмы маркировки изображений можно разделить на три группы:

* алгоритмы, выполняющие поиск секретного сообщения без исходного промаркированного изображения (слепые алгоритмы);
* алгоритмы, требующие наличия исходного изображения;
* алгоритмы, выполняющие поиск сообщений с использованием фрагмента оригинала контейнера.

По способу внедрения ЦВЗ существующие методы можно разделить на следующие группы:

* линейные, основанные на линейной модификации изображения;
* нелинейные, использующие векторное или скалярное преобразование;
* другие (в том числе использующие фрактальные преобразования).

По области встраивания скрытых данных существующие методы можно разделить на две группы:

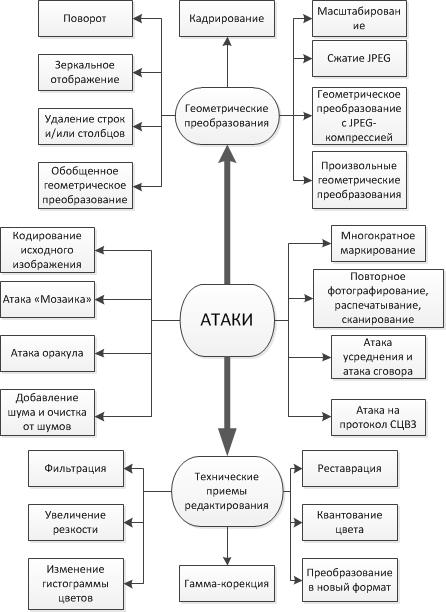
* пространственные, основанные на внедрении бит ЦВЗ в результате изменений яркостных или цветовых составляющих изображения;
* спектральные, основанные на декомпозиции маркируемых областей изображения.

### Атаки на стеганографические системы

Рассмотрим классификацию атак на системы цифровых водяных знаков.

Классификация предназначена для того, чтобы выделить основные типы атак, а также проанализировать и определить критерии уязвимости и устойчивости ЦВЗ к деструктивным воздействиям, ведь именно список атак определяет основу для оценки стойкости ЦВЗ.

Выделяют следующие виды атак (рис. 2).



**Рис. 2** Виды атак на системы ЦВЗ

**Геометрические преобразования.**

*Зеркалъное отображение.* Большинство компьютерных изображений можно зеркально отобразить относительно вертикальной или горизонтальной оси. Однако немногие системы ЦВЗ могут сохранить внедренный знак после данного преобразования. При этом основной проблемой является рассинхронизация стеганодекодера.

*Поворот*. Поворот изображения на небольшой угол часто применяется к отсканированному изображению, чтобы выровнять картинку по горизонтали или вертикали, но может применяться и для того, чтобы не обнаруживался водяной знак. Обычно поворот совмещается с кадрированием.

*Кадрирование* (обрезка и наращивание изображения). В некоторых случаях нарушители заинтересованы «центральной» частью материала, защищенного авторским правом. Тогда они вырезают центральный сегмент изображения. Однако рассеивание (размножение) ЦВЗ по всей площади изображения предотвращает вырезание встроенного знака.

*Масштабирование*. Масштабирование применяют, когда цифровое изображение с высоким расширением используется для электронных приложений, таких как публикации в Интернете или отправка по электронной почте. Масштабирование бывает пропорциональное и непропорциональное. Под пропорциональным масштабированием понимают такое, при котором коэффициенты масштабирования по горизонтали и вертикали одинаковы. Непропорциональное масштабирование использует различные коэффициенты по горизонтали и вертикали. Достаточно часто методы ЦВЗ устойчивы только к пропорциональному масштабированию.

*Удаление строк и/или столбцов*. Удаление нескольких строк или столбцов изображения, выбранных псевдослучайным образом из всей картинки, считается эффективной атакой против внедрения ЦВЗ.

*Сжатие JPEG*. В настоящее время JPEG — один из широко используемых алгоритмов сжатия изображения, поэтому любая система ЦВЗ должна быть устойчива к сжатию. Важным является показатель уровня сжатия, рекомендуется проверять устойчивость к JPEG -сжатию до 70 %. Обобщенное геометрическое преобразование. Обобщенное геометрическое преобразование — это комбинация непропорционального масштабирования, поворота и обрезания.

*Произвольные геометрические искажения*. Программные инструментальные средства (например, StirMark) используют различные комбинации геометрических искажений для оценки устойчивости систем ЦВЗ к атакам.

*Геометрические искажения вместе с JPEG-компрессией*. Следует отдельно выделить комбинацию геометрического преобразования и сжатия JPEG, так как это очень распространенная операция при редактировании цифровых фотографий. Однако исчерпывающий тест на устойчивость к атакам должен включать и обратное к JPEG-сжатию преобразование, так как подобное может использоваться злоумышленником.

**Технические приемы редактирования.**

*Преобразование в новый формат*. Для надежного скрытия водяных знаков необходимо, чтобы методы внедрения были инвариантны (устойчивы) относительно множества методов преобразования цифрового образа в новый формат файла.

*Фильтрация*. Фильтрация включает линейные и нелинейные фильтры, применяемые с целью редактирования изображения. Часто используют медианный и гауссовский фильтры. Фильтрацией посредством сглаживания образа можно удалить ЦВЗ. Современные системы маркировки не позволяют отфильтровать ЦВЗ без значительных повреждений самого образа.

*Увеличение резкости*. Функция увеличения резкости принадлежит к стандартным возможностям программного обеспечения для обработки изображений. Это преобразование эффективно определяет шумы в высоких частотах, вводимые программами внедрения ЦВЗ, и поэтому может быть использовано для атак на системы ЦВЗ.

*Изменение гистограммы цветов*. Указанная атака включает увеличение (вытягивание) или выравнивание гистограммы с целью компенсации уровней цвета или изменения контрастности.

*Гамма-коррекция* — часто используемая операция для улучшения цветовой схемы изображений или адаптации изображений под дисплей, например, после сканирования.

*Квантование цвета* применяется при конвертации изображения в формат графического обмена GIF (Graphics Interchange Format), который используется для публикаций в Интернете. Квантование цвета сопровождается сглаживанием переходов и изменением ошибки квантования.

*Реставрация* обычно используется для снижения эффектов от специфических процессов деградации «бумажной копии».

**Добавление шума и очистка от шумов**. Многие ЦВЗ эффективно противостоят добавлению помех (аддитивный шум или некоррелированная мультипликативная помеха) в изображения. Этот вид преобразований широко рассмотрен в теории связи и теории обработки сигналов и разработаны алгоритмы защиты от шума. Однако важным является допустимый уровень шума относительно уровня сигнала самого маркированного изображения.

**Повторное фотографирование, распечатывание, сканирование**.Этот процесс вводит геометрические искажения, такие же, как шумоподобные искажения.

**Атака «Мозаика»**. При этой атаке картинка разбивается на фрагменты, которые являются отдельными, но состыкованными в единое целое. Такие сегментированные изображения могут использоваться при оформлении Интернет-сайтов. Если злоумышленнику удастся разбить маркированное изображение на немаркированные фрагменты, то он сможет обмануть автоматическую систему поиска в Интернете произведений с внедренными ЦВЗ.

**Атака усреднения и атака сговора**.Имея несколько копий одной и той же картинки, но с разными знаками, можно удалить водяные знаки путем усреднения этих изображений (атака усреднения) или путем разделения всех копий изображения на небольшие части и затем составления оригинальной картинки, но из соответствующих частей различных копий (атака сговора).

**Многократное маркирование**. При этой атаке в контейнер добавляются несколько различных ЦВЗ. Однако современные разработки (например, Р1свигеМагс) откажутся от выполнения добавления водяного знака, если другой уже внедрен. Следовательно, для избыточного маркирования атакующему нужен специальный доступ к маркирующей программе, например дизассемблированный исходный код программного обеспечения. Водяной знак владельца должен оставаться даже после нанесения многих фальшивых ЦВЗ.

**Атака оракула**. Когда доступен открытый стеганодетектор, атакующий может удалить метку, последовательно внося небольшие изменения в изображение до тех пор, пока стеганодетектор еще определяет наличие ЦВЗ.

**Атаки на протокол систем ЦВЗ**. Указанные атаки направлены против функционирования самого протокола выработки и проверки ЦВЗ. Одной из таких атак является атака, основанная на инверсии последовательности действий при внедрении метки, в результате чего в случае необратимости ЦВЗ злоумышленнику удается промаркировать уже защищенное изображение. При разработке всей системы необходимо анализировать слабости не только ЦВЗ, но и стеганографические протоколы взаимодействия участников коммуникационного процесса.

**Копирование (кража) исходного изображения**. Атакующий с целью компрометации ЦВЗ может попытаться получить доступ к исходному немаркированному изображению. Рассмотренный список атак является основой для оценки стойкости ЦВЗ. При этом при разработке ЦВЗ необходимо тестировать систему не только для основных видов атак, но и для комбинаций перечисленных атак.

### Оценка качества стеганосистемы

Создание и эксплуатация надежного стеганографического средства предусматривает наличие определенного инструментария для его контроля и оценки. Количественное оценивание стойкости стеганографической системы защиты к внешним воздействиям представляет собой достаточно сложную задачу, которая обычно на практике реализуется методами системного анализа, математического моделирования или экспериментального исследования.

Как правило, профессионально разработанная стеганосистема обеспечивает трехуровневую модель защиты информации, решающую две основные задачи:

* скрытие самого факта наличия защищаемой информации (первый уровень защиты);
* блокирование несанкционированного доступа к информации, осуществляемое путем избрания соответствующего метода скрытия информации (второй уровень защиты).

Наконец, необходимо принимать во внимание и вероятность существования третьего уровня — предварительной криптографической защиты (шифрования) скрываемой информации.

Оценка качества основной характеристики стеганосистемы — *уровня* *скрытости* — обеспечивается путем проведения аналитических исследований (стеганоанализа) и натурных испытаний. Для оценки качества стеганографического скрытия часто используются известные методы из других областей, в первую очередь — криптоанализа.

Поскольку абонент-получатель может восстанавливать скрытую информацию принятого сообщения, то очевидно, что существует некий механизм ее извлечения.

Если нарушитель, выдвигая гипотезы о возможном стеганографическом преобразовании, имеет некоторый инструмент для их проверки, то он имеет шансы подтвердить факт существования скрытой информации, выполнив поиск механизма извлечения секретного сообщения и, наконец, раскрыть содержание сообщения. По этой причине, в первую очередь, для детектирования стеганограмм можно использовать разновидности описанных выше атак на стеганосистему и значительную часть методов криптоанализа.

Достаточно эффективны в некоторых случаях методы оценки уровня скрытости стеганосредств на основании анализа их статистических характеристик. Статистическая теория дает количественные критерии вероятности, что позволяет создавать детекторы, которые будут обнаруживать статистические расхождения между последовательностями. В случае наличия достаточного объема анализируемой информации с достаточно высокой вероятностью можно делать выводы об основных характеристиках последовательности, выделенной для анализа из контейнера.

Для сравнительного оценивания качества стеганографических средств разрабатываются разные показатели, дающие количественные оценки. Больше всего их разработано для стеганометодов, которые работают с изображениями и видео (методов ЦВЗ). Зачастую такие показатели оперируют с изображениями на уровне пикселей, хотя после надлежащей адаптации они применимы и к другим способам описания изображения, а также к аудиоданным.

# Вейвлет-преобразования

Несколько слов о том, как вейвлет-преобразования классная, перспективная, современная штука, и почему именно их я выбрала для реализации своей задачи.

## Общая теория

Традиционно для анализа временных рядов используется преобразование Фурье, дающее разложение исследуемого временного процесса *f(t)* в ряд по тригонометрическим функциям, или в более общей форме записи

|  |  |
| --- | --- |
|  | (1) |

Коэффициенты  являются амплитудами гармонических колебаний соответствующей частоты и определяются формулой

|  |  |
| --- | --- |
| . | (2) |

Множество функций  образует ортонормированный базис пространства ), которое является пространством определенных на ) функций, действительных, ограниченных на ) и непрерывных всюду за исключением конечного числа точек.

Аппарат Фурье-преобразований дает достаточно простые для расчетов формулы и прозрачную интерпретацию результатов, но имеет некоторые недостатки. Преобразование, например, не отличает сигнал, являющийся суммой двух синусоид, от ситуации последовательного включения синусоид, не дает информации о преимущественном распределении частот во времени, может дать неверные результаты для сигналов с участками резкого изменения. Исрследуемые ряды также далеко не всегда удовлетворяют требованию пеиодичности и более того, как правило, заданы на ограниченном отрезке времени.

Основы вейвлет-анализа были разработаны в середине 80-х годов Гроссманом и Морле как альтернатива преобразованию Фурье для исследования временных (пространственных) рядов с выраженной неоднородностью. В отличие от преобразования Фурье, локализующего частоты, но не дающего временного разрешения процесса, вейвлет-преобразование, обладающее самонастраивающимся подвижным частотно-временным окном, одинаково хорошо выявляет как низко-частотные, так и высокочастотные характеристики сигнала на разных временных масштабах. По этой причине вейвлет-анализ часто сравнивают с "математическим микроскопом", вскрывающим внутреннюю структуру существенно неоднородных объектов.

Указанная универсальность обеспечила вейвлет-анализу широкое использование в самых различных областях знаний. Семейства анализирующих функций, называемых вейвлетами, применяются при анализе изображений различной природы, для изучения структуры турбулентных полей, для сжатия больших объемов информации, в задачах распознавания образов, при обработке и синтезе сигналов, например, речевых, для определения характеристик фрактальных объектов.

Подобно тому, как в основе аппарата преобразований Фурье лежит единственная функция , порождающая ортонормированный базис пространства ) путем масштабного преобразования, так и вейвлет-преобразование строится на основе единственной базисной функции , принадлежащей пространству ) , т.е. всей числовой оси.

В западной литературе за этой функцией закрепилось название "вейвлет", что означает "маленькая волна", в отечественной иногда ее называют "всплеском", отражая в этом названии и локализацию, и осцилляционный характер поведения.

При конструировании базисной анализирующей функции  должны выполняться следующие необходимые условия.

1. Локализация - вейвлет должен быть локализован вблизи нуля аргумента как во временном, так и в частотном пространстве.
2. Нулевое среднее:
3. Как следствие, вейвлет должен быть знакопеременной функцией.
4. Ограниченность:
5. Вейвлет должен быть достаточно быстро убывающей функцией временной (пространственной) переменной.

Базис одномерного дискретного вейвлет-преобразования (ДВП) строится на основе вейвлета   посредством операций сдвигов и растяжений вдоль оси . Вводя аналог синусоидальной частоты и принимая для простоты в качестве ее значений степени двойки, получаем для функций базиса yjk(t)= 2j/2y(2jt-k)

Базис нормирован, если вейвлет имеет единичную норму.

Вейвлет называется ортогональным, если семейство {yjk} представляет ортонормированный базис функционального пространства L2(R), т.е. <yjk,ylm>=djl dkm. В этом случае любая функция fО L2(R) может быть представлена в виде ряда

https://www.krsu.edu.kg/vestnik/2002/v2/frl/a15_f05.gif  
где  
https://www.krsu.edu.kg/vestnik/2002/v2/frl/a15_f06.gif

Непрерывное вейвлет-преобразование (НВП) строится аналогичным образом с помощью непрерывных масштабных преобразований и переносов вейвлета *(t)* с произвольными значениями масштабного коэффициента ***a*** и параметра сдвига ***b***:

https://www.krsu.edu.kg/vestnik/2002/v2/frl/a15_f07.gif

где символ \* обозначает операцию комплексного сопряжения.

Вейвлет-преобразование обратимо для функций *f* из *L2(R)*

https://www.krsu.edu.kg/vestnik/2002/v2/frl/a15_f08.gif

Таким образом, любая функция из *L2(R)* может быть представлена суперпозицией масштабных преобразований и сдвигов базисного вейвлета с коэффициентами, зависящими от масштаба (частоты) и параметра сдвига (времени).

Двухпараметрическая функция *W(a,b)* дает информацию об изменении относительного вклада компонент разного масштаба во времени и называется спектром коэффициентов вейвлет-преобразования.

## Применение вейвлет-преобразования

В заключение нашей статьи перечислим некоторые области, где использование вейвлетов может оказаться (или уже является) весьма перспективным.

1. **Обработка экспериментальных данных.**Поскольку вейвлеты появились именно как механизм обработки экспериментальных данных, их применение для решения подобных задач представляется весьма привлекательным до сих пор. Вейвлет-преобразование дает наиболее наглядную и информативную картину результатов эксперимента, позволяет очистить исходные данные от шумов и случайных искажений, и даже "на глаз" подметить некоторые особенности данных и направление их дальнейшей обработки и анализа. Кроме того, вейвлеты хорошо подходят для анализа нестационарных сигналов, возникающих в медицине, анализе фондовых рынков и других областях.
2. **Обработка изображений.**Наше зрение устроено так, что мы сосредотачиваем свое внимание на существенных деталях изображения, отсекая ненужное. Используя вейвлет-преобразование, мы можем сгладить или выделить некоторые детали изображения, увеличить или уменьшить его, выделить важные детали и даже повысить его качество!
3. **Сжатие данных.** Особенностью ортогонального многомасштабного анализа является то, что для достаточно гладких данных полученные в результате преобразования детали в основном близки по величине к нулю и, следовательно, очень хорошо сжимаются обычными статистическими методами. Огромным достоинством вейвлет-преобразования является то, что оно не вносит дополнительной избыточности в исходные данные, и сигнал может быть полностью восстановлен с использованием тех же самых фильтров. Кроме того, отделение в результате преобразования деталей от основного сигнала позволяет очень просто реализовать сжатие с потерями – достаточно просто отбросить детали на тех масштабах, где они несущественны! Достаточно сказать, что изображение, обработанное вейвлетами, можно сжать в 3-10 раз без существенных потерь информации (а с допустимыми потерями – до 300 раз!). В качестве примера отметим, что вейвлет-преобразование положено в основу стандарта сжатия данных MPEG4.
4. **Нейросети и другие механизмы анализа данных.** Большие трудности при обучении нейросетей (или настройке других механизмов анализа данных) создает сильная зашумленность данных или наличие большого числа "особых случаев" (случайные выбросы, пропуски, нелинейные искажения и т.п.). Такие помехи способны скрывать характерные особенности данных или выдавать себя за них и могут сильно ухудшить результаты обучения. Поэтому рекомендуется очистить данные, прежде чем анализировать их. По уже приведенным выше соображениям, а также благодаря наличию быстрых и эффективных алгоритмов реализации, вейвлеты представляются весьма удобным и перспективным механизмом очистки и предварительной обработки данных для использования их в статистических и бизнес-приложениях, системах искусственного интеллекта и т.п.
5. **Системы передачи данных и цифровой обработки сигналов.** Благодаря высокой эффективности алгоритмов и устойчивости к воздействию помех, вейвлет-преобразование является мощным инструментом в тех областях, где традиционно использовались другие методы анализа данных, например, преобразование Фурье. Возможность применения уже существующих методов обработки результатов преобразования, а также характерные особенности поведения вейвлет-преобразования в частотно-временной области позволяют существенно расширить и дополнить возможности подобных систем.

**Достоинства:**

* Вейвлетные преобразования обладают всеми достоинствами преобразований Фурье.
* Вейвлетные базисы могут быть хорошо локализованными как по частоте, так и по времени. При выделении в сигналах хорошо локализованных разномасштабных процессов можно рассматривать только те масштабные уровни разложения, которые представляют интерес.
* Базисные вейвлеты могут реализоваться функциями различной гладкости.

**Недостатки:**

* Можно выделить один недостаток, это относительная сложность преобразования.

# Алгоритм внедрения цифрового водяного знака в изображение с помощью вейвлет-преобразований

Краткая сводка: алгоритм является неслепым, и таким-то таким-то. Я выбрала его потому что.

В реализованном мною алгоритме И.Р. Кима используется трехуровневое разложение с использованием вейвлет-преобразования Хаара. ЦВЗ встраивается в коэффициенты всех уровней разложения последовательно, начиная с третьего и заканчивая первым. Для встраивания выбираются коэффициенты, превышающие значение определенного порога.

Для встраивания используется аддитивный алгоритм

|  |  |
| --- | --- |
| , | (1) |

где – измененный коэффициент, – выбранный для внедрения коэффициент, – бит ЦВЗ, коэффициент масштабирования, который регулируется для каждого уровня разложения. Для получения изображения, содержащего ЦВЗ, используется обратное 2D-ДВП.

Для извлечения ЦВЗ необходимо исходное изображение. Применяется инверсия формулы внедрения, учитывая адаптивно-уровневый коэффициент масштабирования ,

|  |  |
| --- | --- |
|  | (2) |

Количество встраиваемой информации относительно невелико. В среднем оно составляет примерно 1/120 от размера исходного изображения, однако при расчете возможного количества встраиваемой информации следует учитывать не только размер изображения, но и насыщенность цвета определенных составляющих.

## Алгоритм И.Р. Ким

### Встраивание ЦВЗ

Обобщенная блок-схема встраиваемых данных водяного знака с помощью 2D-ДВП изображена на рис. 3.



Рис. 3 Обобщенная блок-схема внедрения ЦВЗ

**Шаг 1.** Импортированиеисходного изображение и извлечение его синей составляющей.

Как отмечено в пункте 1.3.2 настоящей работы изменения в синей составляющей наименее заметны человеческому глазу.

**Шаг 2.** Импортирование ЦВЗ и преобразование его в одномерный массив бит.

**Шаг 3.** Разложение синей составляющей исходного изображения с помощью вейвлет-преобразования Хаара на 3 уровня и формирование коэффициентов аппроксимации и детализации.

**Шаг 4.** Вычисление порогов, в зависимости от которых будут выбраны пригодные для встраивания коэффициенты.

Пороги вычисляются отдельно для каждого уровня. На каждом уровне разложения находится абсолютный максимум для каждого набора коэффициентов, аппроксимации и детализации – горизонтальных , вертикальных и диагональных . Затем из них берется максимум . Порог вычисляется по следующей формуле:

|  |  |
| --- | --- |
|  | (5) |

**Шаг 5.** Процесс встраивания ЦВЗ. Начиная с 3-го уровня разложения, перебираются коэффициенты аппроксимации и детализации. Каждый коэффициент сравнивается со значением порога, соответствующего данному уровню. Коэффициенты, превышающие значение порога, изменяются в соответствии с формулой 1. Аналогичные операции производятся на 2 и на 1 уровне. В процессе выполнения этого шага функция периодически проверяет, сколько символов ЦВЗ осталось встроить. Если ЦВЗ встроено полностью, процесс останавливается. Соответственно, ЦВЗ не всегда встраивается во все коэффициенты.

**Шаг 6.** Восстановление синей составляющей изображения, в которое был встроен ЦВЗ, из измененных коэффициентов с помощью обратного вейвлет-преобразования. Изображение визуально ничем не должно отличаться от исходного.

### Извлечение ЦВЗ

**Шаг 1.** Выполнение шага 1 и шага 3 алгоритма встраивания к изображению со встроенным ЦВЗ. В результате чего получаем коэффициенты аппроксимации и детализации 3 уровней разложения Хаара.

**Шаг 2.** Выполнение шага 1 и шага 3 алгоритма встраивания к исходному изображению. Это действие необходимо в связи с тем, что алгоритм И.Р. Ким является неслепым, а это значит, что для извлечения ЦВЗ необходимо исходное изображение.

**Шаг 3.** Вычисление порогов для коэффициентов. Вычисление производится с помощью исходного изображения аналогично шагу 4 предыдущего алгоритма.

**Шаг 4.** Извлечение ЦВЗ. Для извлечения ЦВЗ производится перебор коэффициентов синей составляющей исходного изображения, начиная с 3 уровня. Если коэффициент больше порога , то находим соответствующий коэффициент в изображении со встроенным ЦВЗ и извлекаем бит ЦВЗ в соответствии с формулой 2.

**Шаг 5.** Перевод одномерного извлеченного массива бит ЦВЗ к двумерному виду и сохранение его в формате изображения. Для выполнения этого шага необходимо указать размеры исходного ЦВЗ.

## Программная реализация алгоритма И.Р. Ким

Программа, реализующая алгоритм И.Р., описанный в пункте 2.1, написана на языке C# на платформе .NET Framework. Реализовано 7 классов, код которых приведен в приложениях А-Д. Далее следует описание основной функциональности каждого класса.

### Хранение и обработка изображений

Для реализации хранения и обработки изображений было написано два класса. Вспомогательный класс DoublePixel (Приложение А) дает возможность оперировать значениями пикселей. Он содержит функции для быстрого доступа к конкретному пикселю, замены его значения и приведения пикселя к формату RGB.

Класс DoubleImage (Приложение Б) был реализован с целью замены стандартного класса для обработки изображений Bitmap. Он дает более быстрый доступ к отдельным пикселям в отличие от класса Bitmap за счет использования класса DoublePixel. Класс DoubleImage позволяет извлекать отдельные цветовые компоненты по выбору и обновлять их. Этот класс также содержит функцию для преобразования изображения в стандартный формат Bitmap для последующего сохранения.

Для работы ЦВЗ оказалось недостаточно реализованных классов для работы с изображением, поэтому потребовалось реализовать класс Watermark (Приложение В). Он позволяет преобразовывать изображение в двумерный массив бит и обратно.

### Вейвлет-преобразование

Для осуществления вейвлет-преобразования Хаара были реализованы два класса, HaarTransfrom (Приложение Г) и Wavelet (Приложение Д).

Класс HaarTransfrom содержит функцию Transform, принимающую на вход матрицу вещественных чисел, а также заданную ширину и высоту для преобразования отдельной части матрицы. Функция Transform сначала осуществляет преобразования по строкам матрицы, затем аналогично по столбцам. Для этого создается пустая матрица такого же размера для сохранения промежуточных результатов. В ходе преобразований по строкам для каждой строки *k* берется пара соседних чисел пробегает от 0 до *width/*2, где *width* – это ширина матрицы, с шагом 2, и преобразуется следующим образом:

|  |  |
| --- | --- |
|  | (3) |
|  | (4) |

Затем полученные значения аппроксимации *approx* и детализации *detal* сохраняются в промежуточную матрицу в строку *k* по индексам *i* и *width/2*, соответственно.

Преобразования по столбцам производятся на промежуточной матрице, полученной в результате преобразований по строкам. Преобразования производятся аналогично описанным выше преобразованиям по строкам. Результат сохраняется в конечную матрицу, которую возвращает функция Transform. Если преобразования производятся только на отдельной части матрицы, остальную часть марицы, полученной в результате преобразований, необходимо заполнить значениями из исходной матрицы. Для этого в классе HaarTransfrom используется вспомогательная функция FillRestMatrix.

Класс HaarTransfrom также содержит функцию Untransform, которая производит обратные преобразования для восстановления исходной матрицы.

Класс Wavelet содержит функцию Transform, которая принимает на вход матрицу вещественных чисел и необходимый уровень разложения. После проверки возможности разложения до указанного уровня запускается функция Transform класса HaarTransfrom. Размеры изменяемой части матрицы зависят от уровня разложения. Для первого уровня разложения требуется вся матрица, для последующих уровней размеры изменяемой части определяются следующим образом:

*variableWidth = width / i,*

*variableHeight = height / i,*

где *width и height –* исходные размеры изображения, а *i –* текущий уровень разложения.

Класс Wavelet содержит функцию Untransform, которая производит обратное вейвлет-преобразование.

Также класс Wavelet содержит функцию GetCoefficient, которая возвращает матрицу коэффициентов (аппроксимации и детализации – горизонтальных, вертикальных и диагональных) в зависимости от требуемого уровня разложения.

### Алгоритмы встраивания и извлечения ЦВЗ

Алгоритмы по встраиванию извлечению ЦВЗ реализованы в классе JRKimAlgorithm (Приложение Е). Также реализован вспомогательный класс Threshold (Приложение Ж) для подсчета порогов.

Функция KIMembed осуществляет встраивание ЦВЗ в изображение. Она получает на вход исходное изображение и ЦВЗ. Далее извлекается синяя составляющая исходного изображения с помощью функции GetColorComponent класса DoubleImage. Затем вызывается функция Transform класса Wavelet с синей составляющей и значением 3 уровня разложения в виде параметров. Затем все коэффициенты разложения извлекаются из полученной в результате разложения матрицы с помощью функции GetCoefficient класса Wavelet и сохраняются в отдельные двумерные массивы.

Затем необходимо получить значения порогов. Для этого используется функция GetTreshold класса Treshold. Функция GetTreshold перегружена и может принимать на вход 3 или 4 матрицы в зависимости от уровня разложения, поскольку на 1 и 2 уровнях разложения используются только коэффициенты детализации, а на 3 уровне еще и коэффициенты аппрокисмации.

После получения порогов ЦВЗ преобразуется с помощью функции TransformWatermark. Ее назначение поменять все нулевые биты ЦВЗ на значение -1 для осуществления дальнейших арифметических операций.

Затем происходит последовательное встраивание ЦВЗ в коэффициенты, начиная с коэффициентов аппроксимации с 3 уровня разложения и заканчивая коэффициентами детализации 1 уровня разложения.

После чего собирается новая матрица с измененными коэффициентами с помощью функции SetCoefficient класса Wavelet. К ней применяется обратное вейвлет-преобразования Хаара с помощью функции Untransfrom класса Wavelet. В результате получается измененная синяя составляющая, которая несет в себе код ЦВЗ. Далее синяя составляющая исходного изображение заменяется на измененную с помощью функции UpdateColorComponent класса DoubleImage.

Функция KIMextract класса JRKimAlgorithm осуществляет извлечение ЦВЗ с помощью исходного изображения. Ее алгоритм описан в пункте 2.1.2. Данная функция использует аналогичные вспомогательные функции как в функции KIMembed.

### Пользовательская часть программы

Здесь возможно стоит, а возможно и не стоит описать, что происходит со стороны пользователя и какими средствами оно реализовано.

## Анализ алгоритма

В этой главе будет приведен анализ алгоритма на быстродействие, эффективность и робастность.

В первую очередь алгоритм был проверен на быстродействие. Внедрение ЦВЗ размером 100х100 пикселей в изображение высокого разрешения размером 2048х2048 пикселей заняла 2,474 секунд. Обработка меньших по размеру изображений происходит быстрее. Соответственно, на внедрения ЦВЗ большего размера уходит больше времени, однако, как выяснилось в дальнейшем, размер встраиваемого ЦВЗ сильно зависит от размера изображения и его цветовой насыщенности и даже для больших ярких изображений максимально возможный размер ЦВЗ весьма небольшой. Например, для полностью белого (то есть максимально насыщенного по всем цветовым составляющим) изображения размером 2048х2048 максимально возможный размер ЦВЗ 443x443. Поэтому выявить зависимость количества времени от размера ЦВЗ не удалось. Однако результаты работы алгоритма для

Анализ на быстродействие. На робастность (сжатие, обрезка, поворот, масштабирование)

## Оптимизация алгоритма

### Встраивание ЦВЗ в несколько цветовых компонент

### Предварительный расчет максимально возможного и оптимального размера ЦВЗ

### Вывод предупреждения о невозможности встроить ЦВЗ целиком

### Алгоритм определения схожести восстановленного ЦВЗ в случае потери данных

# Заключение

# Список литературы

Астафьева Н.М. Вейвлет-анализ: основы теории и примеры применения //УФН. - 1996. - Т.166. - № 11. - С. 1145-1170.



[Роби Поликар Введение в Вейвлет-преобразование](http://www.autex.spb.su/cgi-bin/download.cgi?wvlt_tutorial)

Книжка по стеганографии

Никольский С.М. Курс математического анализа: Учебник для вузов.— 5-е изд., перераб.— М.: Физико-математическая литература, 2000. — 592 с.

Алгоритм Ким статья