МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Применение преобразования Уолша-Адамара при реализации метода Коча для встраивания ЦВЗ в изображения.

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Черватюка Сергея Александровича

Научный руководитель
к. п. н., доцент _____ А. С. Гераськин
19.01.2026 г.

Заведующий кафедрой
д. ф.-м. н., профессор _____ М. Б. Абросимов
19.01.2026 г.

Саратов 2026

ВВЕДЕНИЕ

Человечество испытывало потребность в защите информации с древнейших времён. Одним из способов её обеспечения является стеганография - наука о тайной передаче информации путём сокрытия самого факта передачи.

В наше время, с ростом количества мультимедийного контента, вопросы защиты авторских прав и соблюдения аутентичности становятся важнее с каждым днём. Одним из способов их решения является цифровой водяной знак (ЦВЗ) - специальная метка, встраиваемая в контент. Методы встраивания ЦВЗ могут отличаться по области встраивания, силе встраивания, сложности вычислений и множеству других параметров.

Одной из важнейших характеристик метода встраивания ЦВЗ является устойчивость ЦВЗ к атакам, которые могут быть направлены на модификацию или полное удаление ЦВЗ.

Атаки на ЦВЗ представляют собой преднамеренные или побочные воздействия на контейнер и могут быть классифицированы по множеству различных признаков, таких как цель атаки, область воздействия, сложность обнаружения и др.

Цель данной работы - рассмотреть возможность использования преобразования Уолша-Адамара при реализации метода Коча для встраивания ЦВЗ в изображения, который обеспечивает защиту от атак на ЦВЗ.

Для достижения этой цели необходимо поставить следующие задачи:

- провести обзор популярных форматов графических файлов;
- описать методы противостояния атакам;
- предложить метод встраивания ЦВЗ, обеспечивающий защиту от атак:
- программно реализовать и протестировать предложенный метод;
- провести анализ устойчивости метода к атакам;
- провести анализ искажений, вызванных работой программы;

Дипломная работа состоит из введения, 5 разделов, заключения, списка использованных источников и 4 приложений. Общий объем работы – 61 страниц,

из них 44 страницы – основное содержание, включая 25 рисунков и 7 таблиц, список использованных источников из 22 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

Первый раздел дипломной работы «Описание форматов графических файлов» содержит описание графичейских файлов BMP, JPEG и PNG.

Форматы BMP, JPEG и PNG относятся к числу наиболее распространённых растровых графических форматов и широко применяются в цифровой обработке изображений. Несмотря на общее назначение, они существенно различаются по структуре данных, способам сжатия и областям использования, что делает их показательными объектами для анализа при исследовании методов стеганографии и цифровых водяных знаков.

Формат BMP характеризуется простой и наглядной структурой хранения данных и отсутствием сжатия. Это обеспечивает точное представление пикселей и удобство прямого доступа к ним, однако приводит к значительному размеру файлов. Благодаря предсказуемости структуры BMP широко используется в учебных и инженерных задачах, а также при анализе низкоуровневых графических алгоритмов, несмотря на ограниченную применимость в сетевых приложениях.

Формат JPEG ориентирован на эффективное сжатие полноцветных изображений с допустимой потерей качества. Использование дискретного косинусного преобразования и квантования позволяет существенно уменьшать размер файлов при сохранении приемлемого визуального качества. JPEG получил массовое распространение в цифровой фотографии и веб-среде, однако не поддерживает прозрачность и плохо подходит для изображений с резкими границами и текстовой графикой.

Формат PNG, в отличие от JPEG, использует сжатие без потерь и поддерживает альфа-канал, что обеспечивает высокую точность цветопередачи и корректную работу с прозрачностью. Модульная структура файла и эффективный алгоритм сжатия делают PNG универсальным решением для хранения графики с чёткими контурами, интерфейсных элементов и изображений, требующих сохранения исходных пиксельных данных.

Таким образом, различия в принципах кодирования и обработки изображений в форматах BMP, JPEG и PNG определяют особенности поведения встроенных данных при различных видах преобразований и делают данные форматы обоснованным выбором для исследования устойчивости стеганографических методов и цифровых водяных знаков.

Второй раздел дипломной работы «Типы атак на ЦВЗ» содержит описание геометрических, пространственных и частотных атака, а также способы противодействия им.

Чем проще реализуется атака на цифровой водяной знак, тем выше вероятность её практического применения, поэтому наибольший интерес представляют геометрические, пространственные и частотные атаки, широко встречающиеся при обычной обработке изображений. Их объединяет способность существенно ослаблять или разрушать ЦВЗ без заметного ухудшения визуального качества, что делает такие воздействия особенно опасными.

Геометрические атаки основаны на изменении структуры изображения и координатной системы пикселей и направлены на десинхронизацию встроенного водяного знака и алгоритма его извлечения. Даже незначительные преобразования, такие как обрезание, могут привести к утрате ЦВЗ или сделать его недоступным для обнаружения. Наиболее эффективной мерой повышения устойчивости к таким атакам является размещение водяного знака в центральной области композиции изображения, которая реже подвергается удалению и обычно содержит наибольшую визуальную и энергетическую значимость.

Пространственные атаки воздействуют непосредственно на значения пикселей и особенно опасны для методов, использующих малозаметные изменения яркости или младшие значащие биты. Одной из самых простых и эффективных является статическая атака, основанная на модификации LSB, которая практически не воспринимается визуально, но способна разрушить встроенную информацию. Защита от таких воздействий требует увеличения

амплитуды встраиваемых изменений до уровня, при котором попытка повреждения ЦВЗ становится визуально заметной.

Частотные атаки выполняются в спектральной области изображения и включают сжатие с потерями, фильтрацию и изменение частотных поддиапазонов. Наиболее распространённой является атака сжатием, реализуемая при перекодировании изображения в JPEG, где квантизация частотных коэффициентов может существенно ослабить или полностью уничтожить водяной знак. Устойчивость к таким воздействиям достигается за счёт встраивания ЦВЗ с амплитудой, превышающей порог стандартной квантизации, что делает его удаление возможным только ценой заметного ухудшения качества изображения.

Таким образом, анализ геометрических, пространственных и частотных атак позволяет сформулировать ключевые требования к устойчивым системам цифровых водяных знаков и определить принципы противодействия наиболее распространённым и практически значимым видам искажений.

Третий раздел дипломной работы «Практическое применение преобразования Уолша-Адамара в стеганографии» содержит описание метода Коча, преобразования Уолша-Адамара.

Метод Коча основан на встраивании информации в частотную область изображения. Исходное изображение разбивается на блоки 8×8 пикселей, к каждому из которых применяется дискретное косинусное преобразование (ДКП). В полученной матрице частотных коэффициентов бит сообщения кодируется за счёт соотношения модулей двух коэффициентов средней частоты. Изменение этих коэффициентов определяется параметром силы встраивания ε, который задаёт компромисс между устойчивостью водяного знака и визуальными искажениями. Извлечение осуществляется повторным применением ДКП и сравнением выбранных коэффициентов.

Преобразование Уолша–Адамара является ортогональным преобразованием, использующим базис функций Уолша, принимающих значения ±1. Оно может быть представлено в матричной форме с использованием

матрицы Адамара, которая строится рекурсивно и обладает простой структурой. В отличие от ДКП, преобразование Уолша–Адамара не содержит встроенных нормирующих коэффициентов, что требует дополнительной нормализации при практическом применении.

Использование преобразования Уолша–Адамара в методе Коча заключается в замене матрицы ДКП на матрицу Адамара порядка 8. При этом сохраняется общий принцип встраивания: работа с блоками 8×8 и модификация коэффициентов в выбранной области спектра. Прямое и обратное преобразования дополняются нормирующим множителем, что обеспечивает корректное восстановление изображения. Такой подход позволяет адаптировать метод Коча к альтернативному частотному представлению и исследовать влияние выбора преобразования на устойчивость цифрового водяного знака.

Четвёртый раздел дипломной работы «Программная реализация» содержит описание алгоритма предложенного метода, порядок работы с пользовательским интерфейсом и анализ искажений, которые возникают в изображениях.

Программа для встраивания и изъятия цифрового водяного знака реализована на языке Python 3.12.2 с использованием PyQt5 для графического интерфейса, Pillow для обработки изображений и NumPy для матричных операций. Алгоритм основан на модифицированном методе Коча с применением преобразования Уолша–Адамара и работает с блоками изображения размером 8×8 пикселей. Сообщение предварительно кодируется в двоичную строку фиксированным алфавитом, при этом один бит встраивается в каждый блок и дублируется по всем цветовым компонентам, что позволяет повысить устойчивость за счёт мажоритарного голосования при извлечении.

Процесс встраивания заключается в поблочном обходе изображения и модификации выбранных спектральных коэффициентов с заданной силой встраивания ε, после чего формируется ключ, содержащий координаты коэффициентов и длину сообщения. Изъятие выполняется в обратном порядке с

использованием этого ключа. Пользовательский интерфейс представлен на рисунке 1.

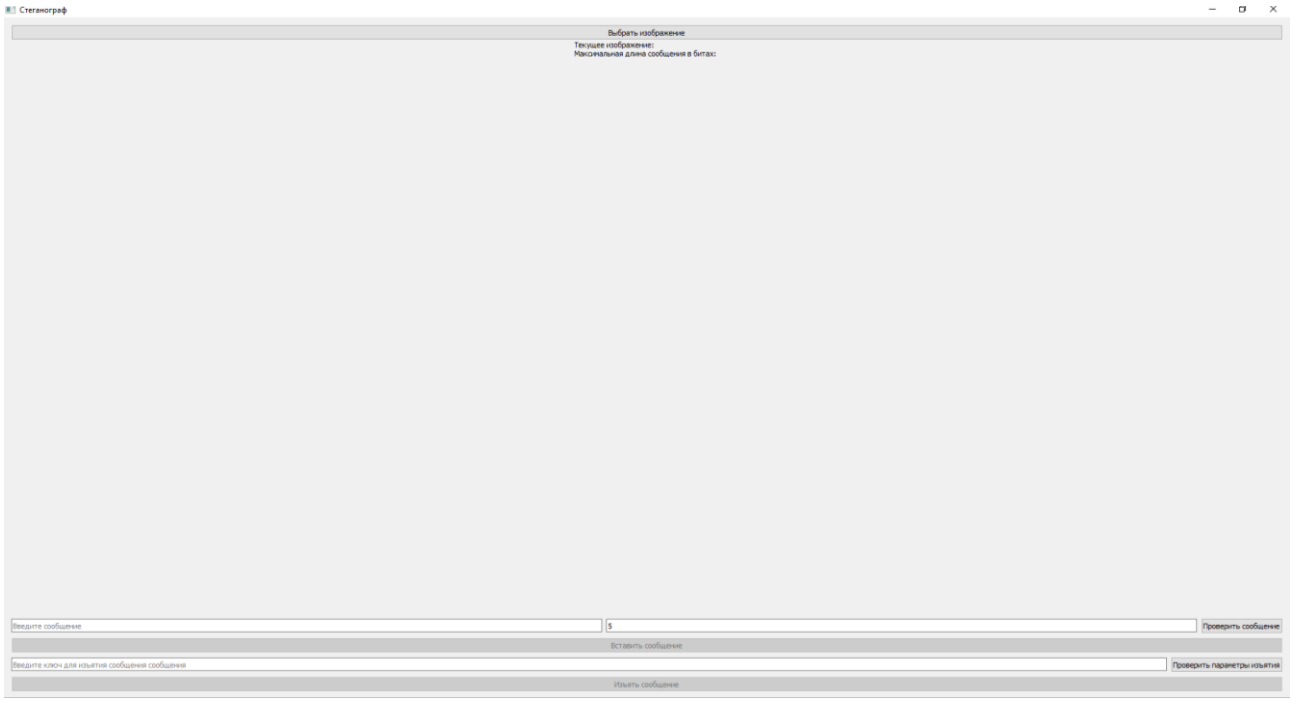

Рисунок 1 - Пользовательский интерфейс

Он обеспечивает выбор изображения, ввод сообщения или ключа и отображение результатов встраивания и извлечения.

Анализ искажений показал, что искажения, возникающие что при метке центрального блока композиции (рисунок 2), что при встраивании ЦВЗ (рисунок 3), визуально малозаметны.

Рисунок 2 - Искажение в центральном блоке

Рисунок 3 - Фрагмент изображения после встраивания с использованием коэффициента встраивания 10

Наиболее выраженные искажения наблюдаются при увеличении коэффициента встраивания, однако их рост не является пропорциональным. Исследование по цветовым компонентам показало, что наибольшую устойчивость к искажениям демонстрирует зелёный канал, несколько меньшую — синий, тогда как красный канал оказывается наиболее чувствительным. В целом увеличение коэффициента встраивания повышает точность извлечения сообщения без существенного ухудшения визуального качества изображениях в результате работы программы.

Пятый раздел дипломной работы «Анализ устойчивости метода к атакам» содержит описания атак обрезанием, сжатием и статической атаки на изображения, а также описание способов противодействия им

Проведён анализ устойчивости разработанного метода встраивания цифрового водяного знака к типовым атакам: обрезанию, сжатию с потерями и без потерь, а также статической атаке. Во всех экспериментах в изображение встраивалось сообщение «hello, world».

Показано, что базовая реализация метода уязвима к атаке обрезанием: удаление краевых областей приводит к потере блоков с встроенной информацией и существенному снижению точности извлечения. Для противодействия была предложена модификация алгоритма, предусматривающая встраивание, начиная с центра композиции изображения с помощью пометки центрального блока с

использованием преобразования Уолша–Адамара. Эксперименты подтвердили, что такой подход обеспечивает успешное извлечение сообщения даже после значительного обрезания контейнера.

Исследование устойчивости к сжатию показало, что при малых значениях коэффициента встраивания метод недостаточно устойчив как к JPEG-сжатию с потерями, так и к PNG-сжатию без потерь. Увеличение коэффициента встраивания приводит к резкому росту точности извлечения. Для JPEG устойчивое извлечение достигается при $\varepsilon \geq 30$, а для PNG — при $\varepsilon \geq 10$–20, при этом визуальные искажения остаются малозаметными.

Анализ статической атаки, основанной на замене наименее значащих бит пикселей, показал, что метод сохраняет работоспособность при изменении до 3–4 бит. Увеличение коэффициента встраивания повышает устойчивость лишь незначительно, тогда как замена 5 и более бит приводит к заметным визуальным искажениям, что делает подобные атаки легко обнаружимыми.

В целом результаты подтверждают, что предложенный метод обладает достаточной устойчивостью к распространённым атакам при корректном выборе коэффициента встраивания и использовании центрального размещения цифрового водяного знака.

ЗАКЛЮЧЕНИЕ

В рамках данной работы была рассмотрена возможность использования преобразования Уолша-Адамара при реализации метода Коча для встраивания ЦВЗ в изображения.

По результатам анализа поведения метода при воздействии различных атак были определены ключевые факторы, влияющие на надёжность встроенного сообщения. На основе выявленных особенностей были предложены меры повышения устойчивости, направленные на минимизацию потерь информации и обеспечение корректного извлечения ЦВЗ.

Разработанный метод был реализован на языке Python, что позволило провести экспериментальные исследования, подтвердившие эффективность предложенных решений. Показано, что устойчивость цифрового водяного знака к статической атаке, атаке обрезанием, а также сжатию значительно возросла по сравнению с базовой реализацией.

Таким образом, все поставленные задачи были выполнены, а цели работы достигнуты. Полученные результаты подтверждают перспективность применения комбинации метода Коча и преобразования Уолша–Адамара для построения устойчивых стеганографических систем и могут служить основой для дальнейших исследований и улучшения алгоритмов защиты цифровых изображений.