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

Разработка программного продукта для сокрытия информации в цифровых изображениях методом Куттера-Джоржана-Боссена

АВТОРЕФЕРАТ
дипломной работы

студентки 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Богатовой Екатерины Дмитриевны

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

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

Саратов 2026

ВВЕДЕНИЕ

Количество алгоритмов для внесения изменений в фото, аудио, видео и многие другие виды цифровой информации, очень большое. В настоящее время проблема выявления следов фальсификации остается актуальной не только для криминалистической сферы, но и для всего мира в целом. Поэтому требуется совершенствование имеющихся методов обнаружения ретуши или более глобальных изменений, а также создания новых, улучшенных алгоритмов, ведь развитие навыков фотообработки и монтажа людей также не стоит на месте и развивается с каждым днем.

Методы встраивания информации в контейнеры всех видов находят широкое применение в современном мире. Встраивание информации применяется как в легальных целях, так и в ходе противоправной деятельности.

К примерам легального использования таких алгоритмов можно отнести цифровые водяные знаки в документах и объектах интеллектуальной собственности, организацию каналов скрытной передачи информации спецслужбами в рамках их деятельности, а также другими пользователями, например, для сохранения коммерческой тайны.

К наиболее распространённым способам противоправного применения техник встраивания информации относятся передача скрытых сообщений в целях организации и координации деятельности, нарушающей закон, например, террористических актов. Сокрытие каких-либо данных также может использоваться хакерами или кибершпионами для тайного обмена ими или передачи команд и инструкций во время кибератак. Такие действия могут направляться на кражу конфиденциальных данных, нарушение сетевой безопасности или шпионаж.

И чтобы реализовать все описанные выше цели, используя внесения изменений и встраивание каких-либо сообщений в файлы, подходят любые виды цифровой информации, будь то аудио или видео. Но на мой взгляд, наиболее распространенными и подходящими контейнерами в этом случае все же являются фотоизображения.

Из-за того, что сейчас у большинства людей всегда под рукой имеется техника, а именно телефон или ноутбук, то действия с фотографиями стали совершенно обычным, повседневным явлением. Фотомонтаж используется во многих сферах деятельности человека, таких как реклама, журналистика, и даже политика.

В наше время некоторые научились настолько искусно обращаться с графическими редакторами, что на первый взгляд и даже после беглого анализа невозможной найти никаких следов фальсификации, и отличить подделку от оригинала очень сложно.

В целом, проблема внесения изменений в фотоизображения, встраивания в них различных сообщений, и использование методов стеганографии остается актуальной в свете быстрого развития цифровых технологий, и появления все большего и большего количества новых видов угроз.

Целью работы является исследование методов сокрытия информации в изображениях, оценка их эффективности, анализ работы метода «креста» в различных цветовых каналах и проверка его стойкости к атакам.

В соответствии с поставленной целью, можно выделить следующие задачи исследования:

- изучение метода внесения изменений в фотоизображения, выявление его плюсов и минусов;
- изучение цветовой системы RGB и особенностей ее цветовых каналов;
- определение критериев оценки эффективности встраивания информации в цифровые изображения;
- приведение примера практической реализации метода Куттера-Джордана-Боссена;
- Реализация метода для всех цветовых каналов системы RGB и составление рекомендаций на основе получившихся результатов;
- Реализация некоторых атак и проверка выбранного метода на устойчивость к ним во всех рассмотренных цветовых каналах.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 1 приложения. Общий объем работы – 74 страницы, из них 54 страницы – основное содержание, включая 51 рисунок и 1 таблицу, список использованных источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

Первый раздел дипломной работы под названием «Стеганография» содержит теоретическое описание одноименного понятия и принципы работы выбранной для рассмотрения методики сокрытия какой-либо информации внутри других носителей, таких как изображения, аудиофайлы, видео или документы. А также приведен обзор некоторых наиболее распространенных методов встраивания информации в частную область статических изображений: метод LSB, метод Коха-Жао, метод Куттера-Джордана-Боссена.

В первой части был более детально рассмотрен метод LSB, также известного как метод замены наименьших значащих битов. Приведено описание алгоритма, основные формулы для его реализации и примеры работы с черно-белыми и цветными изображениями.

Во второй части был рассмотрен метод, основанный на изменениях отношений между абсолютными значениями коэффициентов дискретно-косинусное преобразование (ДКП) в среднечастотной области изображения, более известный как метод Коха-Жао. Приведено краткое описание алгоритма и основные формулы для реализации.

В третьей части подробно рассмотрен Метод Куттера-Джордана-Боссена или метод «креста», который основан на сравнительно плохой чувствительности человеческого зрения к несильным изменениям яркости синего цвета. Приведено описание алгоритмов кодирования и декодирования данного метода, а также основные формулы для их реализации.

В четвертой части была составлена наглядная таблица плюсов и минусов рассмотренных методов стеганографии.

На основе собранной информации мной был проведен сравнительный анализ, по результатам которого удалось выявить один из самых скрытных и эффективных методов стеганографии, по моему мнению, а именно метод Куттера-Джордана-Боссена.

Второй раздел содержит в себе информацию о существующих цветовых каналах.

В первой части данного раздела представлено теоретическое описание цветовой системы RGB, в частности общая информация, особенности восприятия цветов человеческим глазом, способы их кодировки и основные принципы данной модели.

Во второй части была проведена аналитическая работа с особенностями каждого цветового канала рассмотренной цветовой модели, а именно красного, зеленого и синего. Приведено описание каждого цвета в разрезе человеческого восприятия и технической составляющей.

В третьей части представлены критерии оценки эффективности встраивания информации, по которым в дальнейшем будет оцениваться практичность выбранного метода сокрытия информации в фотоизображениях. В частности, были рассмотрены такие критерии, как: визуальная незаметность, устойчивость к искажениям и емкость встраиваемой информации. В каждом критерии были рассмотрены преимущества и недостатки основных цветов модели RGB.

В целом, система RGB является основой для работы с цветами в цифровом мире. Каждый из цветовых каналов RGB играет уникальную роль в формировании изображения. Зеленый канал обеспечивает наибольшую информативность и яркость, красный канал добавляет насыщенность, а синий канал, хотя и менее чувствителен, также важен для создания полного спектра цветов, а также является отличным контейнером для сокрытия информации. Понимание этих особенностей помогает лучше управлять цветами в цифровой фотографии и графическом дизайне.

В третьем разделе представлена методология атак: какими ресурсами может оперировать злоумышленник, какие последовательные задачи он решает и как классифицируются его действия в рамках теории безопасности стеганографических систем. В данном разделе описаны два ключевых блока:

1. Этапы и цели атак – от простейшего визуального обнаружения до активного разрушения скрытого сообщения, с разделением на пассивные и активные угрозы.

2. Классификация атак – разделение атак на типы в зависимости от того, какой информацией располагает нарушитель (например, известный контейнер, пустой контейнер, модель данных). Каждый из видов поясняется логикой его применения и целью.

В заключении раздела рассматривается особая категория геометрических атак, которые моделируются аффинными преобразованиями, такими как масштабирование, поворот, кадрирование, сдвиг, усечение, отражение, и направлены на нарушение целостности скрытого сообщения путём искажения контейнера.

Устойчивость стеганографической системы – это её способность противодействовать комплексной модели угроз, включающей не только попытки чтения данных, но и их обнаружение, искажение и блокировку. В совершенном виде разработка и оценка любой стегосистемы должны проводиться с учётом всех классификаций атак, описанных в тексте, где успешной считается уже та атака, которая лишь доказывает наличие скрытого канала.

Четвертый раздел описывает практическую реализацию метода Куттера-Джордана-Боссена – интерфейс, написанный с помощью языка программирования Python и библиотеки Tkinter, который в данном случае работает с сокрытием текстовой строки в цифровых изображениях. Он имеет четыре основных раздела для удобства: «Основные операции», «Редактирование», «Стеганография», «Тестирование», и позволяет:

- Загружать файл в PNG или JPG формате;
- В выбранном цветовом канале цветовой модели RGB осуществлять кодирование сообщения в предоставленном снимке;
- Осуществлять декодирование;
- Производить ряд атак на стеганоконтейнер
- Производить автоматизированное тестирование работы программы

В первой части представлены математическая формула встраивания информации в контейнер и пошаговая инструкция кодирования текстового файла в изображение при помощи написанной программы.

Во второй части описан процесс декодирования ранее зашифрованного сообщения. Представлена поэтапная инструкция с примерами различной мощности кодировок, получаемыми результатами и визуализацией в программе. Пример работы интерфейса приведен на рисунках 1, 2, 3.

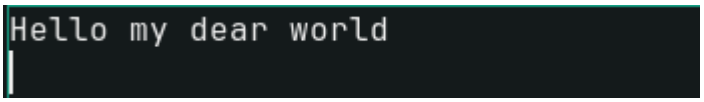

Рисунок 1 – Пример текста для кодирования

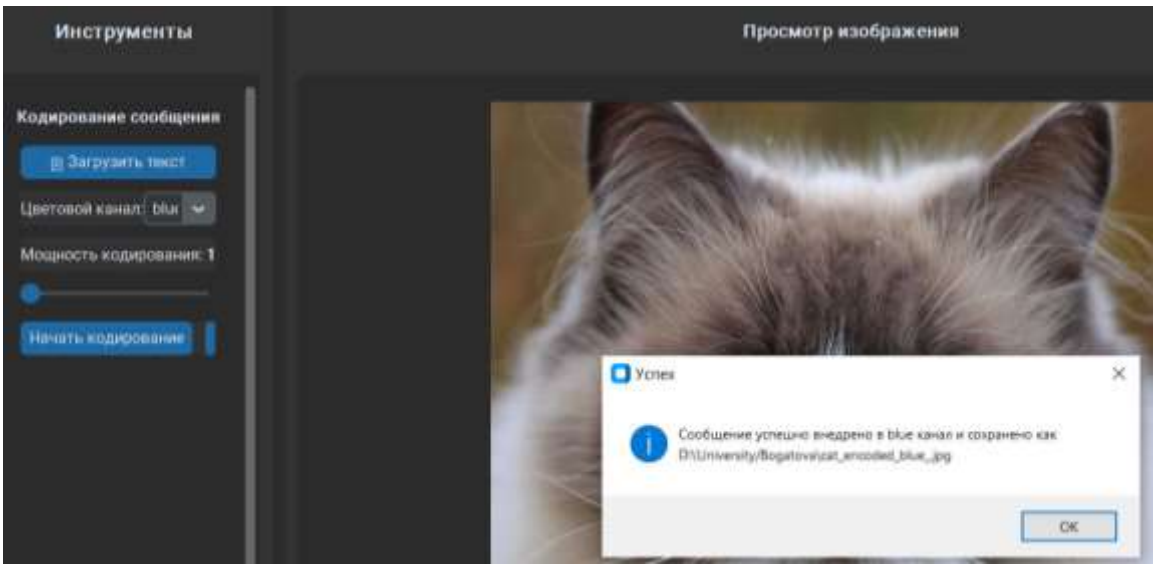

Рисунок 2 – Кодирование сообщения в выбранный для примера цветовой канал

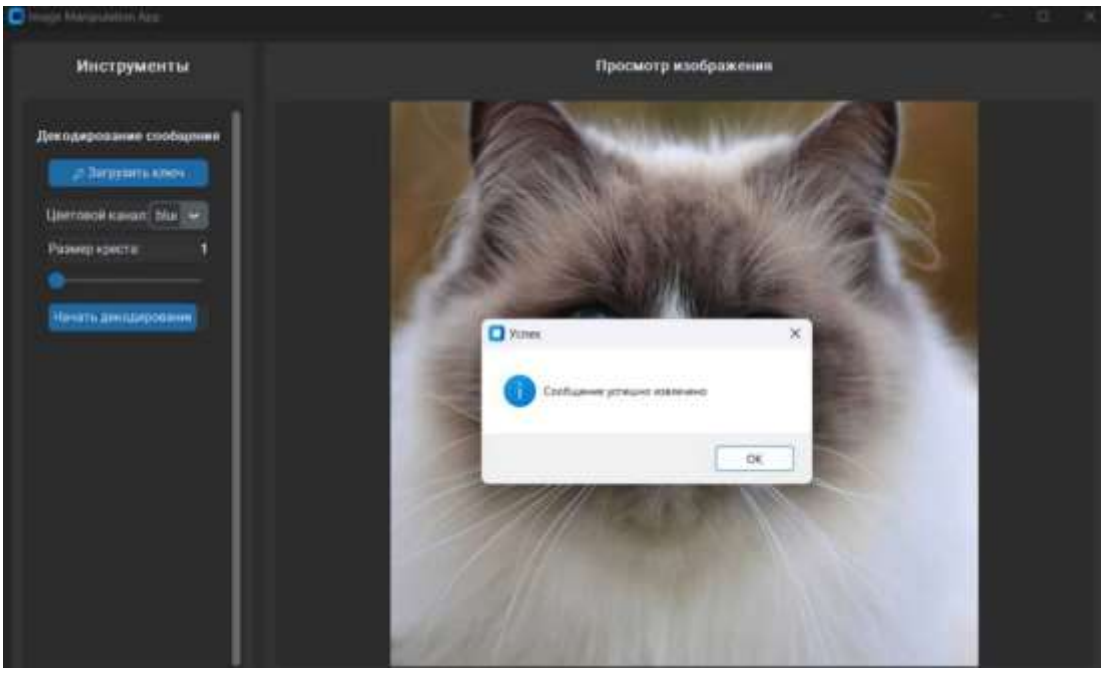

Рисунок 3 – Декодирование сообщения

В третьей части были протестированы другие цветовые каналы – красный и зеленый, на предмет удовлетворения ранее основных приведенных критериев эффективности внесения изменений в фотоизображения: точность восстановления исходного сообщения и появление видимых для человеческого глаза артефактов кодирования.

На рисунках 4, 5, 6 приведены примеры раскодированных сообщений при минимальном значении мощности.

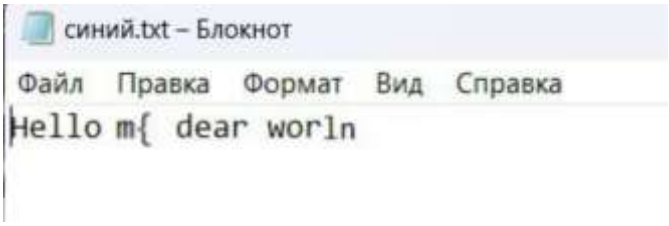

Рисунок 4 – Полученное сообщение после декодирования в синем цветовом канале при минимальной мощности

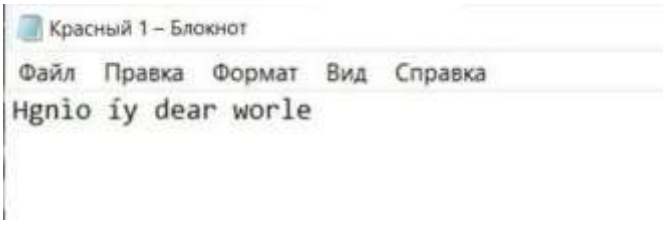

Рисунок 5 – Полученное сообщение после декодирования в красном цветовом канале при минимальной мощности

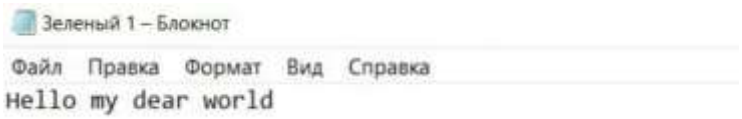

Рисунок 6 – Полученное сообщение после декодирования в зеленом цветовом канале при минимальной мощности

В результате чего были получены наиболее оптимальные диапазоны мощности кодирования для основных цветов модели RGB, которые выглядит следующим образом:

- Красный канал – диапазон от 4 до 6;
- Зеленый канал – диапазон от 1-4;
- Синий канал – диапазон от 2 до 8.

В четвертой части была проведена детальная проверка метода Куттера-Джордана-Боссена на устойчивость к таким атакам, как:

1 Изменение насыщенности изображения;

2 Изменение яркости изображения;

3 Добавление шумов;

4 Добавление черных квадратов.

На основе полученных результатов исследования были составлены графики зависимости эффективности кодирования от значений, указанных ваше параметров атак. После сравнительного анализа было получено, что метод «креста» в целом достаточно устойчив к изменениям насыщенности, зеленый цветовой канал более устойчив к добавлению шумов, синий цветовой канал – к изменению яркости, а красный цветовой канал наименее устойчив к искажениям.

ЗАКЛЮЧЕНИЕ

В ходе работы было изучено такое понятие, как стеганография. А также были рассмотрены наиболее распространенные стенографические методы внесения изменений в фотоизображения.

На основе имеющейся информации о приведенных методах была составлена таблица достоинств и недостатков каждого из них, благодаря которой был выявлен наиболее надежный метод скрытия информации на мой взгляд, а именно метод Куттера-Джордана-Боссена. Выбор в его пользу был сделан из-за двух наиболее важных показателей надежности:

1. Внесенные изменения в структуру изображения не несут за собой сильных видимых для человеческого глаза искажений, тем самым обеспечивая максимально возможную скрытность;
2. Следы применения алгоритма сложно выявить.

Также была рассмотрена цветовая система RGB, особенности ее цветовых каналов и критерии оценки эффективности встраивания информации в каждый из них.

В практической части работы была предложена программная реализация метода «креста» на языке Python. Созданное программное приложение в виде интерфейса успешно прошло тестирование на встраивание информации в три цветовых канала системы RGB. Итог получился следующий:

- Красный канал показал самые худшие результаты. Восстановить полностью исходную текстовую информацию получилось при значении мощности, равном 6. Видимые человеческому глазу артефакты кодирования начали появляться со значения мощности, равном 5;
- Зеленый канал с точки зрения точности раскодирования показал самый лучший результат. Восстановить фразу получилось со значения мощности, равном 1. Но явные артефакты начали появляться со значения мощности, равном 3;

- Синий канал показал самый оптимальный результат. Фраза была восстановлена при мощности, равной 3. Артефакты появились при мощности, равной 8. Но даже при максимальной мощности видимых точек не так много, по сравнению в красным и зеленым каналами.

Также были реализованы четыре атаки, при помощи которых метод был проверен на устойчивость. Результат анализа показал, что эффективность работы варьируется в зависимости от цветового канала и значения выбранного параметра. Если говорить обобщенно, то синий и зеленый каналы показывают лучшие результаты по сравнению с красным. В свою очередь, метод при работе в синем цветовом канале более устойчив к изменениям яркости изображения, а при работе в зеленом – к добавлению шумов.

Таким образом, все поставленные задачи были выполнены. Выбранный для реализации метод Куттера-Джордана-Боссена может успешно применяться для сокрытия информации в цифровых изображениях. Если рассматривать соотношение количества встраиваемой информации, точности раскодирования, устойчивость к атакам и появление артефактов, то работа метода «креста» в синем цветовом канале является наиболее эффективной. При минимальном значении мощности погрешность декодирования небольшая, а именно, от одного до четырех символов, в зависимости от объема встраиваемой информации. Но при этом видимые человеческому глазу артефакты кодирования появляются при более больших значениях мощности, по сравнению с зеленым цветовым каналом.