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

Сокрытие информации в графических файлах

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Логинова Ильи Олеговича

Научный руководитель
к.п.н., доцент _____ А. С. Гераськин
21.01.2023 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
21.01.2023 г.

Саратов 2023

ВВЕДЕНИЕ

Развитие средств вычислительной техники и широкое распространение глобальной сети Интернет привело к необходимости разработки новых средств защиты мультимедийной информации от незаконного распространения. На сегодняшний день известны две эффективные технологии обеспечения защиты безопасности мультимедийной информации (в частности в компьютеризированных системах электронного документооборота): стеганография и криптография.

Криптографические методы подвергают шифрованию объект защиты при помощи определенного алгоритма с использованием ключа. При этом содержание объекта защиты доступно только ограниченному кругу лиц (владельцам ключа) и только после дешифрования. Однако зашифрованный объект может привлечь внимание злоумышленников.

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. Сообщения, факт шифрования которых не скрыт, вызывают подозрение и могут быть сами по себе уличающими в тех странах, в которых запрещена криптография. Таким образом, криптография защищает содержание сообщения, а стеганография – сам факт наличия каких-либо скрытых посланий.

В конце 1990-х годов выделилось несколько направлений стеганографии: классическая, компьютерная, цифровая.

Классическая стеганография представляет собой набор методов для сокрытия информации в физических объектах. Например, сообщение на листке бумаге с помощью невидимых чернил или трафареты, выделяющие в тексте значимые буквы.

Компьютерная стеганография – направление классической стеганографии, основанное на особенностях компьютерной платформы. Например, использование зарезервированных полей компьютерных форматов файлов или скрытие информации в неиспользуемых местах гибких дисков.

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 настоящее время под стеганографией чаще всего понимают скрытие информации в текстовых, графических либо аудиофайлах путём использования специального программного обеспечения. На практике методы стеганографии применяются для идентификации, защиты авторских прав и сокрытия передаваемых сообщений. В качестве решения данных вопросов в качестве контейнеров отлично подходят изображения.

Целью работы является реализация программного обеспечения, выполняющего встраивание и извлечение ЦВЗ, а также оценку его качества и устойчивости к JPEG компрессии.

Таким образом в рамках дипломной работы решаются следующие задачи:

– Анализ технологий цифрового маркирования неподвижных изображений в частотной области.

– Выбор подходящего преобразования и метода встраивания.

– Разработка программного обеспечения.

– Анализ работы программы на различных изображения.

Дипломная работа состоит из введения, 3 разделов, заключения, списка использованных источников и 1 приложения. Общий объем работы – 55 страниц, из них 26страниц – основное содержание, включая 24 рисунка и 1 таблицу, список использованных источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В главе 1 «Цифровая стеганография» представлены основные используемые в настоящее время понятия и рассмотрены методы стеганографии. Согласно исследованию было выявлено, что основными понятиями являются:

– Контейнер – любая информация, используемая для сокрытия тайного сообщения. В свою очередь контейнер подразделяется на фиксированный (например, изображения) и потоковый (например, телефонный разговор). Наибольшее распространение получили исследования с использованием фиксированного контейнера

– Пустой контейнер – контейнер, не содержащий секретного послания.

– Заполненный контейнер (стегоконтейнер) – контейнер, содержащий секретное послание.

– Стеганографический канал (стегоканал) – канал передачи стегоконтейнера.

– Ключ (стегоключ) – секретный ключ, нужный для сокрытия стегоконтейнера. Ключи в стегосистемах бывают двух типов: закрытые (секретные) и открытые. Если стегосистема использует закрытый ключ, то он должен быть создан или до начала обмена сообщениями, или передан по защищённому каналу. Стегосистема, использующая открытый ключ, должна быть устроена таким образом, чтобы было невозможно получить из него закрытый ключ. В этом случае открытый ключ можно передавать по незащищённому каналу.

– Встроенное (скрытое) сообщение – сообщение, встраиваемое в контейнер. В данном случае таким встраиваемым сообщением является ЦВЗ.

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

В качестве стеганографических методов подробно рассматривалась классификация по области встраивания ЦВЗ. В работе сравнивались пространственные методы, такие как LSB (англ. Least Significant Bit – Наименее значимый бит), PVD (англ. Pixel Value Difference – Разность значений пикселей), GLM (англ. Grey Level Modification – Изменение уровня серого), и методы, использующие преобразование изображения.

Был сделан вывод о том, что алгоритмы, использующие частотные методы обладают значительным преимуществом, так как являются более устойчивыми ко всем видами вредоносных воздействий. Это легко объясняется тем, что встраивание осуществляется в более значимые области изображения, а именно средне или низкочастотные области. Вследствие этого уменьшается вероятность потери информации, например, при сжатии изображения или даже каких-либо прямых модификаций значений пикселей.

В главе 2 «Обзор алгоритма Elham» идет пошаговый разбор алгоритма, а именно:

1. Предварительная обработка встраиваемого изображения. Показано как применять ДКП и выбирать коэффициенты по зигзаг сканированию, формируя таким образом вектор-строку коэффициентов ЦВЗ.

2. Обработка контейнера и встраивание. Показано, как считать энтропию блока пикселей, модифицировать частотный коэффициент исходного изображения, а также показана общая схема встраивания на рисунке 1.

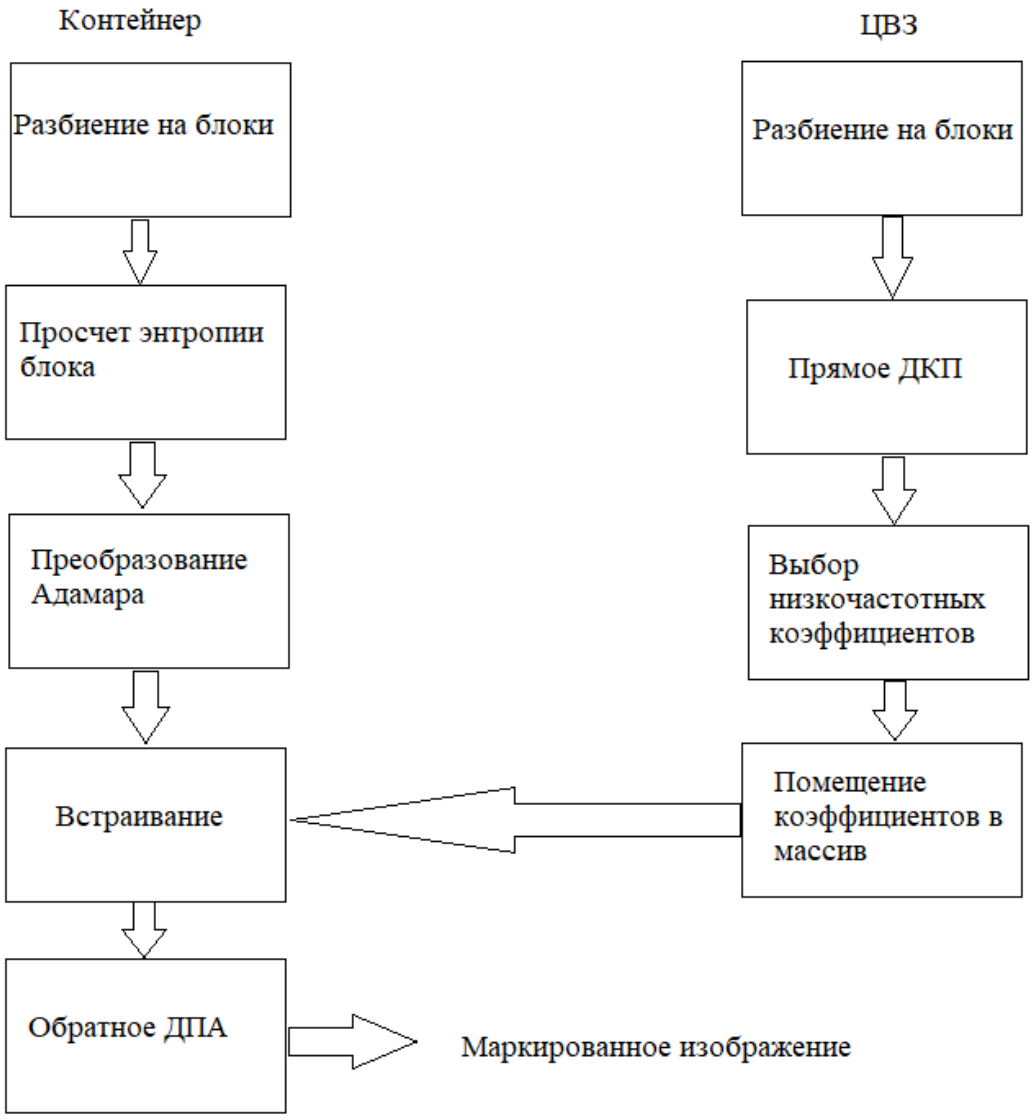


Рисунок 1 – Схема встраивания

3. Преобразование Адамара. Показано, что такое преобразование Адамара и как оно применяется в алгоритме.

4. Схема извлечения. Показан порядок действий для извлечения ЦВЗ на рисунке 2, необходимые для этого формулы (обратное ДКП и извлечение частотного коэффициента).

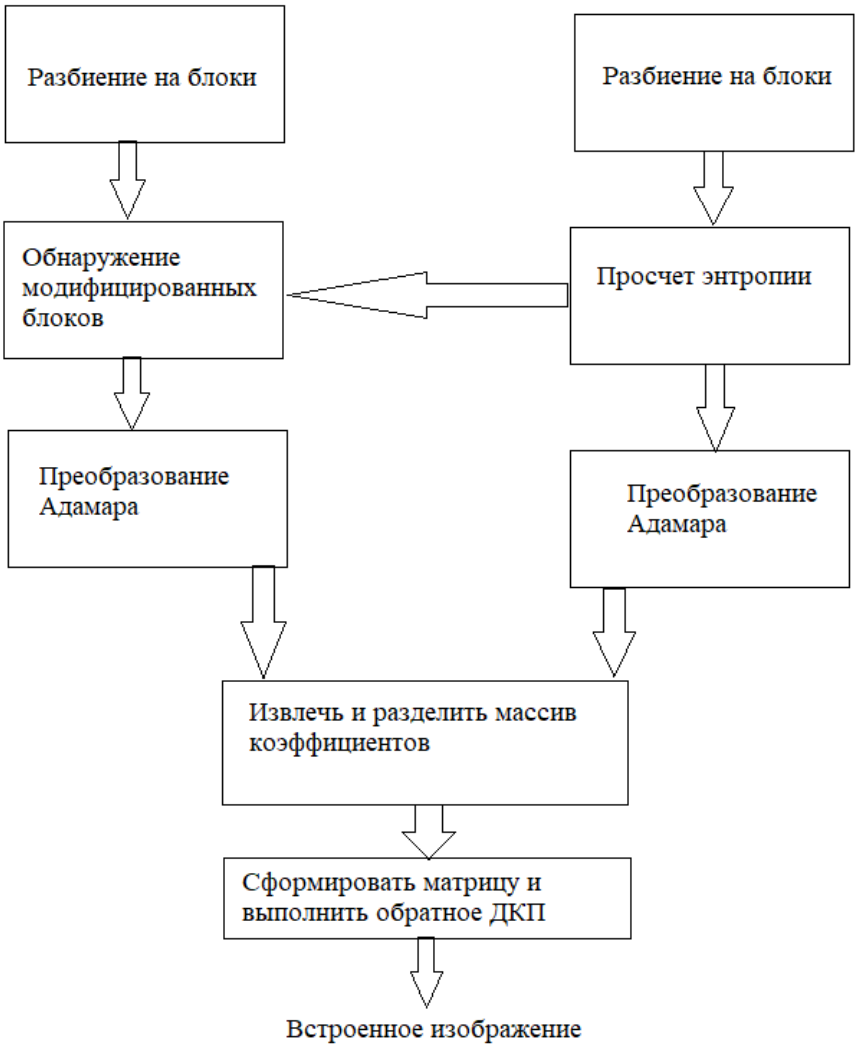
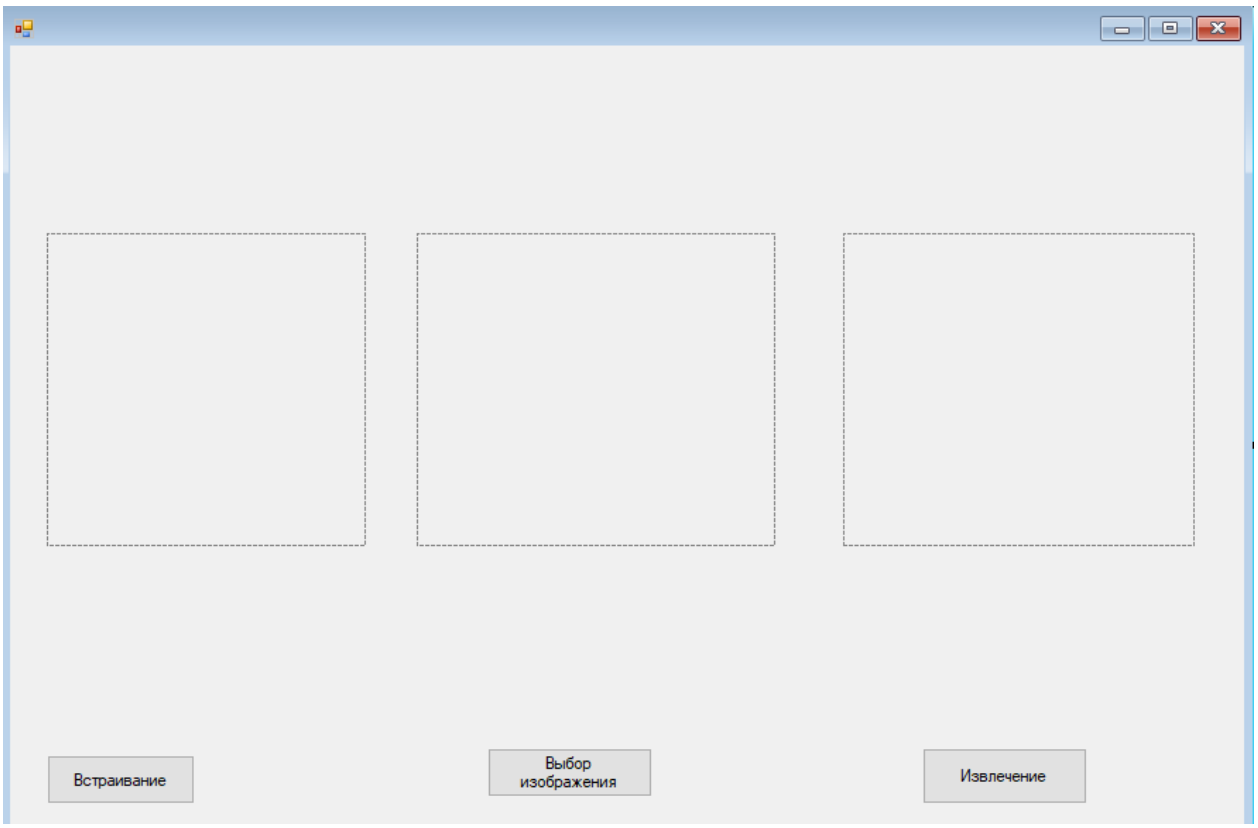


Рисунок 2 – Схема извлечения

В главе 3 «Программная реализация и практические результаты» описывается разработка и тестирование программного продукта. В начале описывается процесс преобразования в обе стороны между пространствами RBG и YCbCr для работы с цветными изхображениями. Далее на рисунке 3 – представлен интрефейс программы.



Рисукно 3 – Интерфейс программы

Кнопка выбор изображения отвечает за обработку ЦВЗ, встраивание позволяет выбрать изображение-контейнер и встроить в него ЦВЗ, а извлечение позволяет выбрать исходное изображение, маркированное изображение и извлечь из него ЦВЗ.

Также 3 центральных квадрата – это объекты PictureBox, в которые выводятся изображения. В центральном отображается исходное изображение, в правом стегоконтейнер, а в левом извлеченный ЦВЗ.

Тестирование программы производилось на цветных и черно-белых изображениях различных форматов, таких как jpg, png, bmp. ЦВЗ встраивался в контейнер и проводилось визуальное сравнивание оригинала и стегоконтейнера. Искажения были минимальны, ЦВЗ впоследствии извлекался успешно.

После этого проверялась устойчивость ЦВЗ к JPEG компрессии. Полученный стегоконтейнер ужимался на 20%, 50% и 80%, а затем из него

извлекался ЦВЗ и данные вносились в таблицу. Анализ показал, что ЦВЗ к компрессии устойчив.

ЗАКЛЮЧЕНИЕ

Таким образом, был проведен анализ технологий цифрового маркирования, а именно были рассмотрены пространственные и частотные методы встраивания, были изучены их преимущества и недостатки. Также были рассмотрены основные преобразования для частотных методов и был обоснован выбор преобразования для работы. Результатом практической части стал алгоритм, реализующий частотные методы и основанный на преобразовании Адамара, как на основном преобразовании, и на дискретном косинусном преобразовании, как на дополнительном. Данный алгоритм показал свою работоспособность на изображениях различных форматов и характеристик, ЦВЗ из каждого типа изображений извлекался, и его качество было оценено как хорошее. Была проведена проверка ЦВЗ на устойчивость к JPEG сжатию. Данная устойчивость является одним из главных преимуществ реализованного алгоритма, поэтому результаты он показал отличные. ЦВЗ устойчив к JPEG сжатию вплоть до 80%. Все поставленные задачи выполнены, цель работы достигнута.