Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

Специальность 1-40 05 01 «Информационные системы и технологии»

Специализация 1-40 05 01 03 «Информационные системы и технологии»

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

**КУРСОВОГО ПРОЕКТА**

по дисциплине Защита информации и надежность информационных систем

Тема: Реализация стеганографического метода Коха-Жао в изображениях формата .bmp

Исполнитель

|  |  |  |
| --- | --- | --- |
| студент 3 курса группы 2    Руководитель |  | \_\_\_\_\_\_\_\_\_  подпись, дата |
|  |  | \_\_\_\_\_\_\_\_\_\_\_\_  подпись, дата |
| Курсовой проект защищен с оценкой |  | \_\_\_\_\_\_\_\_\_ |
| Руководитель \_\_\_\_\_\_\_ |  |  |

подпись

Минск 2021

Оглавление

[Введение 3](#_Toc71364230)

[1. Постановка задачи 4](#_Toc71364231)

[2. Аналитический обзор литературы 5](#_Toc71364232)

[2.1 Алгоритм сокрытия информации Коха-Жао 5](#_Toc71364233)

[2.2 Дискретное косинусное преобразование 5](#_Toc71364234)

[2.3 Алгоритм шифрования информации 6](#_Toc71364235)

[2.4 Алгоритм дешифрования информации 6](#_Toc71364236)

[2.5 Стегоанализ и надёжность сокрытия информации 7](#_Toc71364237)

[2.6 Аналоги алгоритма Коха-Жао 9](#_Toc71364238)

[2.7 Сравнение алгоритмов Коха-Жао и LSB 11](#_Toc71364239)

[3. Проектирование 12](#_Toc71364240)

[Заключение 13](#_Toc71364241)

[Список литературных источников 14](#_Toc71364242)

Введение

Задача защиты информации от несанкционированного доступа решалась во все времена на протяжении истории человечества. Уже в древнем мире выделилось два основных направления решения этой задачи, существующие и по сегодняшний день: криптография и стеганография. Целью криптографии является скрытие содержимого сообщений за счет их шифрования. В отличие от этого, при стеганографии скрывается сам факт существования тайного сообщения.

Цифровая стеганография объединяет методы скрытой передачи данных в объектах цифрового вида. Чаще всего в качестве так называемых стеганографических контейнеров используются цифровые данные, содержащие некоторую избыточность информации: изображения, аудио- и видеоданные, хотя также может использоваться обычный текст, файлы и т. д. При формировании цифровой подписи для объектов интеллектуальной собственности незначительный объем данных встраивается так, чтобы информация сохранялась при различных модификациях объекта.

Методы стеганографии могут применяться и для скрытого копирования секретных данных, а также в средствах коммуникации преступных и террористических формирований.

Данная работа посвящена реализации стеганографического метода Коха-Жао, который на сегодняшний день является достаточно востребованным.

1. Постановка задачи

Требуется изучить существующую литературу и материалы, касающиеся описания стеганографического метода встраивания информации Коха-Жао, для последующей реализации алгоритма в виде программного средства. Программное средство должно быть разработано согласно описываемым алгоритмам шифрования и дешифрования входного сообщения.

Функционально должны быть выполнены следующие задачи:

* разработать программное средство для реализации механизмов зашифрования и дешифрования входного сообщения с использованием стеганографического метода шифрования Коха-Жао;
* провести тестирование программного средства;
* составить руководство пользователя.

Программное средство будет написано на языке C# в среде программирования Visual Studio 2019. В качество графического интерфейса будет использоваться интерфейс прикладного программирования – Windows Forms, отвечающий за графический интерфейс пользователя и являющийся частью Microsoft .NET Framework. Данный интерфейс упрощает доступ к элементам интерфейса Microsoft Windows за счёт создания обёртки для существующего Win32 API в управляемом коде. Причём управляемый код – классы, реализующие API для Windows Forms, не зависящие от языка разработки.

2. Аналитический обзор литературы

## 2.1 Алгоритм сокрытия информации Коха-Жао

Алгоритм Коха-Жао для встраивания информации использует частотную область контейнера и заключается в относительной замене величин коэффициентов дискретного косинусного преобразования (ДКП). Изображение разбивается на блоки размерностью 8×8 пикселей и к каждому блоку применяется ДКП. Каждый блок пригоден для записи одного бита информации.

## 2.2 Дискретное косинусное преобразование

Стеганографические методы скрытия данных в пространственной области изображения являются нестойкими к большинству из известных видов искажений. Так, например, использование операции компрессии с потерями (относительно изображения, это может быть JPEG-компрессия) приводит к частичному или, что более вероятно, полному уничтожению встроенной в контейнер информации. Более стойкими к разнообразным искажениям, в том числе и компрессии, являются методы, использующие для скрытия данных не пространственную область контейнера, а частотную.

Существует несколько способов представления изображения в частотной области. При этом используется та или иная декомпозиция изображения, используемого в качестве контейнера. Например, существуют методы на основе использования дискретного косинусного преобразования (ДКП), дискретного преобразования Фурье (ДПФ), вейвлет-преобразования, преобразования Карунена-Лоева и некоторые другие. Подобные преобразования могут применяться либо к отдельным частям изображения, либо к изображению в целом.

Наибольшее распространение среди всех ортогональных преобразований в стеганографии получили вейвлет-преобразования и ДКП, что определенной мерой объясняется значительным распространением их использования при компрессии изображений. Кроме того, для скрытия данных целесообразно применять именно то преобразование изображения, которому последнее будет подвергаться со временем при возможной компрессии. Например, известно, что алгоритм ДКП является базовым в стандарте JPEG, а вейвлет-преобразования — в стандарте JPEG2000.

Во время цифровой обработки изображения часто применяется двумерная версия дискретного косинусного преобразования:

(2.1 a)

(2.1 б)

где C(x, у) и S(x, у) — соответственно, элементы оригинального и восстановленного по коэффициентам ДКП изображения размерностью N×N; х, у — пространственные координаты пикселей изображения; — массив коэффициентов ДКП; — координаты в частотной области; , если , и , если .

## 2.3 Алгоритм шифрования информации

На начальном этапе первичное изображение разбивается на блоки размерностью 8x8 пикселей. ДКП применяется к каждому блоку — формула (2.1 а), в результате чего получают матрицы 8x8 коэффициентов ДКП, которые зачастую обозначают , где b — номер блока контейнера С, a - позиция коэффициента в этом блоке. Каждый блок при этом предназначен для скрытия одного бита данных.

Было предложено две реализации алгоритма: псевдослучайно могут выбираться два или три коэффициента ДКП. Рассмотрим первый вариант.

Во время организации секретного канала абоненты должны предварительно договориться о двух конкретных коэффициентах ДКП из каждого блока, которые будут использоваться для скрытия данных. Зададим данные коэффициенты их координатами в массивах коэффициентов ДКП: и . Кроме этого, указанные коэффициенты должны отвечать косинус-функциям со средними частотами, что обеспечит скрытость информации в существенных для ЗСЧ областях сигнала, к тому же информация не будет искажаться при JPEG-компрессии с малым коэффициентом сжатия.

Непосредственно процесс скрытия начинается с псевдослучайного выбора блока изображения, предназначенного для кодирования b-го бита Сообщения. Встраивание информации осуществляется таким образом: для передачи бита 0 стремятся, чтобы разница абсолютных значений коэффициентов ДКП превышала некоторую положительную величину, а для передачи бита 1 эта разница делается меньшей по сравнению с некоторой отрицательной величиной:

(2.2)

Таким образом, первичное изображение искажается за счет внесения изменений в коэффициенты ДКП, если их относительная величина не отвечает скрываемому биту. Чем больше значение Р, тем стеганосистема, созданная на основе данного метода, является более стойкой к компрессии, однако качество изображения при этом значительно ухудшается.

## 2.4 Алгоритм дешифрования информации

После соответствующего внесения коррекции в значения коэффициентов, которые должны удовлетворять неравенству (2.2), проводится обратное дискретное косинусное преобразование (ОДКП).

Для извлечения данных, в декодере выполняется аналогичная процедура выбора коэффициентов, а решение о переданном бите принимается в соответствии со следующим правилом:

(2.3)

## 2.5 Стегоанализ и надёжность сокрытия информации

Для большинства современных методов, которые используются для скрытия сообщений в файлах цифрового формата имеет место зависимость надежности системы от объема встраиваемых данных, представленная на рисунке 2.1. Из неё видно, что увеличение объема встраиваемых данных значительно снижает надежность системы.

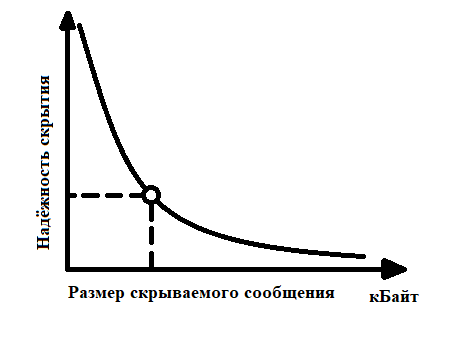


Рисунок 2.1 – Зависимость надёжности и размера скрываемого сообщения

Как уже могло быть замечено, алгоритм сокрытия информации Коха-Жао жертвует количеством скрываемой информации для получения большей устойчивости к JPEG-преобразованию изображения (1 бит информации на 64 точки или на 192 байта изображения RGB без альфа-канала). Однако он не получает абсолютную устойчивость к искажению встраиваемого сообщения при JPEG-преобразовании, так как в любом случае происходит потеря визуальной информации. С помощь изменения параметра P можно довести гарантию целостности скрытой информации до 100 процентов, однако вместе с этим будет происходить большее искажение изображения.

В связи с низкой чувствительностью зрительной системы человека к каналу синего цвета и возможным при определенных обстоятельствах довольно значительным искажением контейнера при встраивании, обычно применяется встраивание информации именно в синий спектр изображения.

При отборе сегментов ДКП также нужно принимать некоторые обстоятельства. Коэффициент в левом верхнем углу матрицы ДКП содержит информацию о яркости всего сегмента (его зачастую называют DC-коэффициентом). Другие коэффициенты называются АС-коэффициентами. Коэффициенты AC делятся на три области (рисунок 2.2) в зависимости от отдалённости от DC-коэффициента: низкочастотная (НЧ), среднечастотная (СЧ), высокочастотная (ВЧ). НЧ компоненты содержат преобладающую часть энергии изображения и, следовательно, носят шумовой характер. ВЧ компоненты больше поддаются влиянию со стороны различных алгоритмов обработки. Таким образом, для встраивания сообщения оптимальными являются СЧ компоненты спектра изображения.

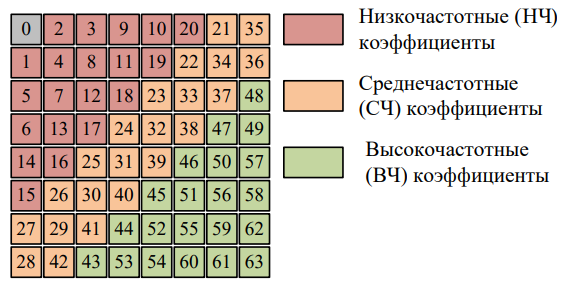


Рисунок 2.2 – Области матрицы ДКП

После разового встраивания информации в матрицу ДКП и получении его ОДКП, даже если не производилось JPEG-преобразования, не гарантируется, что при повторном получении ДКП, матрица ДКП будет соответствовать той, что была до ОДКП. Даже скорее наоборот, она будет изменена из-за округления при ОДКП. Потому при встраивании информации обычно производится цикл ОДКП с последующим получением его ДКП. Если при данном извлечении получаемый бит не соответствует встраиваемому значению, то происходит повторное встраивание бита в ДКП. Цикл повторяется до тех пор, пока алгоритм не убедится, что извлечённое сообщение соответствует встраиваемому.

После того, как мы получили ОДКП и совместили с остальными цветовыми спектрами, мы можем получить изображение, в котором будут отчётливо видны точки изображения, которые резко выдают наличие информации в используемом спектре (рисунок 2.3).



Рисунок 2.3 – Изображение без нормализации

Для предотвращения таких искажений, полученный ОДКП надо пропустить через алгоритм нормализации спектра, где будет происходить его смягчение в соответствии с минимальным и максимальным значениями в спектре. После нормализации, точки, выдающие применении стеганографического алгоритма, исчезнут (рисунок 2.4).



Рисунок 2.4 – Изображение с нормализацией

Если встраиваемая информация не заполняет весь контейнер изображения, то рекомендуется заполнить остальное пространство спектра случайными значениями битов. Особенно данный момент касается сокрытия информации с применением большого значения P.

Встраивание информации с большим значении P, в случае если требуется довести устойчивость сокрытой информации к JPEG-преобразованию до высоких показателей, рекомендуется только в изображениях с большим разрешением, так как искажения, произведённые использованием алгоритма, в таком случае могут быть приняты за шумы изображения или наложенный на изображение фильтр.

## 2.6 Аналоги алгоритма Коха-Жао

В качестве аналогов стеганографического алгоритма Коха-Жао здесь будут рассматриваться другие алгоритмы сокрытия информации в изображениях. Такие алгоритмы разделяются на пространственные и частотные методы. К последним относится наш алгоритм Коха-Жао, потому поподробнее остановимся на рассмотрении пространственных методов.

1. Наименее значимый бит (LSB)

Данный метод заключается в выделении наименее значимых бит изображения-контейнера с последующей их заменой на биты сообщения. Поскольку замене подвергаются лишь наименее значимые биты, разница между исходным изображением-контейнером и контейнером, содержащим скрытые данные невелика и обычно незаметна для человеческого глаза. Метод LSB применим лишь к изображениям в форматах без сжатия (например, BMP) или со сжатием без потерь (например, GIF), так как для хранения скрытого сообщения используются наименее значимые биты значений пикселей, при сжатии с потерями эта информация может быть утеряна. Форматы без сжатия имеют очень большой размер и могут вызвать подозрение, потому для стеганографии чаще используют другие форматы.

Встраивание информации происходит следующим образом. К примеру, берётся чёрно-белое изображение, представленное в виде матрицы . Каждый элемент этой матрицы представлен 8 битами информации, которые определяют уровень яркости точки. Младшие биты влияют на яркость точки в меньшей степени, чем старшие биты. Выбирается, какое количество бит выделяется в точке под сокрытие информации, чем меньше бит будет выделятся, тем меньше будет искажений в изображении с информацией. Например, выделим 2 бита, тогда, если нам нужно будет записать 5 байт информации, то нам понадобится 20 байт, то есть точек изображения. Скрываемая информация последовательным образом записывается в выделенных битах без каких-либо особых операций. Остальная область выделенных битов изображения заполняется шумом, чтобы область со скрытой информацией не выделялась в общей картине. Длина сообщения фиксируется для дальнейшего извлечения данных.

Извлечение происходит по тому же правилу и той же длинны, что и встраивание информации.

1. Разность значений пикселей (PVD)

Этот метод учитывает тот факт, что на гладких участках (где значение яркости меняется незначительно) изменение будет более заметно, нежели на участках, содержащих более значительные перепады яркости.

Встраивание информации происходит следующим образом. Исходное изображение разделяется на блоки по 2 пикселя, и скрытые данные кодируются как разность значений внутри этих блоков. Как и в случае с LSB, необходим закон, по которому будут выбираться блоки для встраивания. Для каждого используемого блока вычисляется модуль разности значений пикселей, по которому определяется диапазон допустимых значений. Чем больше перепад яркости внутри блока – тем шире выбранный диапазон. Например, в блок с диапазоном шириной можно записать 2 бита скрываемого сообщения (эти два бита, по сути, представляют собой выбор конкретного числа из диапазона). Блоки, изменение которых может привести к выходу за пределы допустимых значений яркости пикселей (от 0 до 255) не используются.

Для извлечения данных, изображение вновь делится на блоки по 2 пикселя. В соответствии с заранее известными правилом выбора блоков и последовательностью их обхода, для блоков рассчитывается разность значений пикселей и определяется диапазон, в который она попадает. Далее выполняется проверка на выход за пределы диапазона от 0 до 255: если при максимальной разности, входящий в диапазон, один из пикселей принимает значение больше 255 или меньше 0, то данный блок пропускается, так как он был отброшен аналогичной проверкой на стадии встраивания. Из оставшихся блоков извлекаются данные: по ширине диапазона определяется количество бит, встроенных в блок, которые потом извлекаются, начиная с наименее значимого. В общем же случае, когда ширина диапазона не является степенью 2, полезная нагрузка вычисляется как , где – извлекаемые данные, , – значения пикселей блока, – нижняя граница диапазона.

1. Изменение уровня серого (GLM)

Метод GLM заключается в изменении чётности значения яркости изображения в чёрно-белом представлении. В каждый пиксель изображения встраивается 1 бит скрываемого сообщения.

При встраивании информации значения яркости всех пикселей делаются чётными, путём изменения всех нечётных значений на 1. Далее чётность этих значений сравнивается с чётностью битов данных. Например, если первый бит данных чётный (то есть равен 0), то первый пиксель не изменяется, если же он нечётный (равен 1), то значение яркости изменяется на нечётное.

При извлечении для каждого пикселя, содержащего скрытое сообщение, определяется значение яркости. Если оно чётное – то соответствующий бит сообщения равен 0, если нечётное – то 1.

## 2.7 Сравнение алгоритмов Коха-Жао и LSB

Для наглядности особенностей алгоритма Коха-Жао в качестве сравнения был выбран алгоритм наименее значимого бита (LSB). Для примера возьмём изображение 688x1080 формата BMP.

1. Количество вмещаемой информации

Алгоритм Коха-Жао может сокрыть в себе информации: бит в одном из трёх цветовых спектров.

Алгоритм наименее значимого бита может в себе сокрыть информации при выделении 1 бита в спектре точки: бит в одном из трёх цветовых спектров. Количество скрываемой информации можно увеличить при выделении 2, 3 и более битов в спектре точки.

В итоге алгоритм наименее значимого бита умещает в себе в раза больше информации, чем алгоритм Коха-Жао. Разрыв можно кратно увеличить, если выделять больше битов под сокрытие информации в LSB.

1. Устойчивость к сжатию

Алгоритм LSB не устойчив к сжатию какого-либо вида.

Алгоритм Коха-Жао устойчив к сжатию, использующему дискретное косинусное преобразование, в том числе к сжатию JPEG.

1. Искажение изображения

Было произведено сокрытие информации обоими алгоритмами, результат которых можно увидеть на рисунке 2.5.



Рисунок 2.5 – Изображения слева-направо: оригинальное, алгоритм Коха-Жао, алгоритм LSB

Как можно заметить, алгоритм Коха-Жао почти не исказил оригинальное изображение, так как параметр P был установлен в наименьшее значение. LSB больше выделяется, так как алгоритм более плотно вносит изменения в изображение.

3. Проектирование

В качестве языка программирования был выбран C#, а в качестве интерфейса программирования приложения (API) – Windows Forms. Windows Forms был выбран по причине простоты оформления интерфейса приложения, а также установки взаимосвязи событий взаимодействия с интерфейсом с обработчиками событий. Структура приложения выглядит следующим образом (Рисунок 3.1).

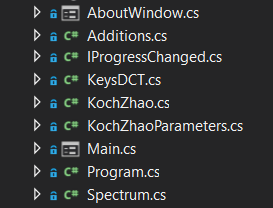


Рисунок 3.1 – Структура проекта

Проект включает в себя следующие окна:

* Main – окно приложения, на котором располагаются все элементы управления (кнопки, ползунки, выпадающее меню и т.д.);
* AboutWindow – окно, на котором располагается информация о приложении, его версии и т.д.

Проект включает в себя следующие классы, структуры, интерфейсы и перечисления:

* Additions – это статический класс, содержащий методы расширения, для работы с данными, массивами чисел с двойной точностью и изображениями;
* IProgressChanged – это интерфейс, реализация которого позволит изменять индикатор прогресса выполнения кодирования, декодирования и анализа кодирования информации с декодированием из формата JPEG;
* KeysDCT – это статический класс, содержащий просчитанные значения, для избегания рутинных операций и ускорения кодирования и декодирования;
* KochZhao – это статический класс, содержащий основные методы кодирования, декодирования и анализа изображения, а также сопутствующие методы;
* KochZhaoParameters – это структура, содержащая параметры для алгоритма Коха-Жао;
* Program – это статический класс, содержащий лишь точку входа в приложение;
* Spectrum – это перечисление спектров изображения: красный (Red), зелёный (Green) и синий (Blue).

Подробное описание классов, структур, интерфейсов и перечислений расписано в приложении А.

4. Разработка программного средства

5. Тестирование

6. Руководство пользователя

Заключение

В ходе выполнения данной курсовой работы было разработано программное средство, позволяющее поместить и извлечь текстовое сообщение при помощи стеганографического алгоритма Коха-Жао.

Созданное программное средство было протестировано. Результаты тестирования показали её правильную работу. Полученные результаты работы программного средства были проанализированы и позволяют сделать вывод о том, что поставленная задача была успешно выполнена.

Реализация системы проводилась с использованием интегрированной среды разработки Visual Studio 2019 и технологии Windows Forms.

Список литературных источников

1. Шилдт Г. – Полный справочник по C# Вильямс, 2004. – 752 с
2. Рихтер Д. – Программирование на платформе Microsoft .NET Framework, СПБ.: Русская редакция, 2005. – 512 с
3. Г. Ф. Конахович, А. Ю. Пузыренко – Компьютерная стеганография. Теория и практика, "МК-Пресс" Киев, 2006. – 288 с
4. Белобокова Ю. А. – Диссертация по теме «Модели и алгоритмы защитной маркировки для обеспечения аутентичности и целостности растровых изображений», Москва, 2014
5. Habr.com. – Электронный ресурс. – Ссылка: [Реализация стеганографического метода Коха-Жао на Ruby/Хабр](https://habr.com/ru/post/216207/#:~:text=%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC%20%D0%9A%D0%BE%D1%85%D0%B0%2D%D0%96%D0%B0%D0%BE%20%D0%B4%D0%BB%D1%8F%20%D0%B2%D1%81%D1%82%D1%80%D0%B0%D0%B8%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F,%D0%BA%20%D0%BA%D0%B0%D0%B6%D0%B4%D0%BE%D0%BC%D1%83%20%D0%B1)