Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный университет   
информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Методы защиты информации

ОТЧЁТ

к лабораторной работе №8

на тему

**СТЕГАНОГРАФИЧЕСКИЕ МЕТОДЫ**

Выполнил: студент гр.253505 Ющук И.А.

Проверил: ассистент кафедры информатики Герчик А.В.

Минск 2025

**СОДЕРЖАНИЕ**

[Введение 3](#_Toc207721845)

[1 Ход работы 4](#_Toc207721846)

[Заключение 5](#_Toc207721847)

[Приложение А (обязательное) Листинг программного кода 6](#_Toc207721848)

# ВВЕДЕНИЕ

Современный этап развития информационных технологий характеризуется повсеместным обменом цифровыми данными и острой необходимостью обеспечения конфиденциальности передаваемой информации. Под скрытой передачей понимается гарантия того, что сообщение остается невидимым для третьих лиц и может быть получено только предназначенным получателем. Для решения этой фундаментальной задачи информационной безопасности используются методы стеганографии.

В отличие от алгоритмов криптографии, которые делают содержание сообщения недоступным без ключа, стеганография основана на принципах сокрытия самого факта существования сообщения. Она преобразует произвольный массив данных в скрытое сообщение, внедренное в цифровой контейнер (изображение, аудио или видео файл). Ключевыми свойствами стеганографических методов являются незаметность (невозможность визуального обнаружения изменений), емкость (количество скрываемой информации) и устойчивость к анализам.

Одним из наиболее эффективных подходов является метод сокрытия в частотной области изображения, который обеспечивает высокую степень незаметности и устойчивости к сжатию. Его основное преимущество заключается в том, что изменения вносятся в коэффициенты частотного преобразования (например, DCT или DWT), что делает их менее заметными для человеческого восприятия. Алгоритм работает с JPEG изображениями, что обеспечивает совместимость с большинством современных форматов хранения и передачи изображений.

Целью данной лабораторной работы является теоретическое и практическое изучение принципов стеганографических методов и реализация программного средства сокрытия и извлечения текстовых сообщений в JPEG изображениях. В рамках работы будет проведена реализация и анализ метода сокрытия в частотной области. Это позволит на практике оценить математические основы преобразований, этапы внедрения и извлечения данных, а также особенности работы с коэффициентами дискретного косинусного преобразования.

Программное средство будет включать модуль сокрытия текстового сообщения в JPEG изображение, модуль извлечения скрытого сообщения из стего-контейнера и модуль анализа устойчивости внедренных данных. Реализация позволит продемонстрировать практическое применение стеганографических принципов и обеспечить понимание механизмов работы современных систем скрытой передачи информации.

# **1 ХОД РАБОТЫ**

В рамках лабораторной работы было разработано программное средство для сокрытия и извлечения текстовых сообщений в *JPEG*-изображениях с использованием метода сокрытия в частотной области. Работа выполнялась на языке *Python* с использованием библиотек *OpenCV* и *NumPy* для обработки изображений. Исходное изображение представлено на рисунке 1.1.



Рисунок 1.1 – Исходное изображение

После выполнения процедуры сокрытия текстового сообщения было получено стегоизображение представлено на рисунке 1.2.



Рисунок 1.2 – Стегоизображение

Для проверки работы программы был выполнен процесс извлечения скрытого сообщения. Результат показал, что сообщение было успешно извлечено.

# ЗАКЛЮЧЕНИЕ

В результате выполнения лабораторной работы была успешно реализована система стеганографического сокрытия информации в JPEG-изображениях с использованием метода работы в частотной области. Практическая реализация охватила все ключевые этапы обработки изображений: преобразование в частотную область с помощью дискретного косинусного преобразования, внедрение текстового сообщения в коэффициенты средних частот и обратное преобразование в пространственную область. Основным достижением работы стало создание работоспособного программного средства сокрытия и извлечения данных, наглядно демонстрирующего принципы современных стеганографических методов.

Реализация подтвердила теоретические положения метода, в частности, важность корректного выбора коэффициентов для внедрения информации и строгого соблюдения процедуры модификации частотных компонентов. Особое значение имела точная реализация алгоритма квантования коэффициентов ДКП и обеспечения минимальных искажений визуального качества изображения. Разработанная система продемонстрировала способность надежно скрывать текстовые сообщения и корректно извлекать их без потерь исходной информации.

Практическая ценность работы заключается в создании инструмента для изучения принципов стеганографии и обработки цифровых изображений. Реализованная система может использоваться для демонстрации механизмов сокрытия информации, изучения особенностей частотного представления изображений, а также для понимания методов обеспечения скрытности передаваемых данных. В процессе реализации были приобретены навыки работы с библиотеками обработки изображений, освоены методы частотного анализа и отработаны приемы тестирования стеганографических систем.

Перспективы развития работы включают оптимизацию алгоритмов для работы с изображениями большого размера, реализацию поддержки различных форматов изображений, а также исследование стойкости реализованного метода к различным типам стегоанализа. Дальнейшее развитие может включать интеграцию с системами защищенной передачи данных и реализацию адаптивных алгоритмов сокрытия информации.

Таким образом, реализованная система стеганографического сокрытия информации представляет собой законченное решение, которое демонстрирует принципы построения средств скрытой передачи данных и служит основой для дальнейшего изучения современных методов защиты информации.

# ПРИЛОЖЕНИЕ А (обязательное) Листинг программного кода

import cv2

import struct

import bitstring

import numpy  as np

import zigzag as zz

import image\_preparation as img

import data\_embedding as stego

NUM\_CHANNELS = 3

if \_\_name\_\_=='\_\_main\_\_':

    image\_filepath  = "./image.jpg"

    stego\_image\_filepath  = "./stego\_image.jpg"

    test\_message = "Love. Calm. Kidness. Kinship."

    #--------Вставка--------

    raw\_cover\_image = cv2.imread(image\_filepath, flags=cv2.IMREAD\_COLOR)

    height, width   = raw\_cover\_image.shape[:2]

    while(height % 8): height += 1

    while(width  % 8): width  += 1

    valid\_dim = (width, height)

    padded\_image = cv2.resize(raw\_cover\_image, valid\_dim)

    #переводим картинку RGB в float32

    cover\_image\_f32 = np.float32(padded\_image)

    #переводим их RGB в YCbCr и сохраняем в классе YCC\_Image

    cover\_image\_YCC = img.YCC\_Image(cv2.cvtColor(cover\_image\_f32, cv2.COLOR\_BGR2YCrCb))

    #пустое место под будующую картинку

    stego\_image = np.empty\_like(cover\_image\_f32)

    for chan\_index in range(NUM\_CHANNELS):

        #DCT

        dct\_blocks = [cv2.dct(block) for block in cover\_image\_YCC.channels[chan\_index]]

        # квантование, необходимо чтобы перейти от fl32 к int так как в int проще вставлять данные

        dct\_quants = [np.around(np.divide(item, img.JPEG\_STD\_LUM\_QUANT\_TABLE)) for item in dct\_blocks]

        #переставляем коэффициенты зигзагом

        sorted\_coefficients = [zz.zigzag(block) for block in dct\_quants]

        #вставляем в Y слой

        if (chan\_index == 0):

            secret\_data = ""

            for char in test\_message.encode('ascii'):

                secret\_data += bitstring.pack('uint:8', char)

            embedded\_dct\_blocks   = stego.embed\_data\_into\_DCT(secret\_data, sorted\_coefficients)

                #переставляем коэффициенты зигзагом обратно

            desorted\_coefficients = [zz.inverse\_zigzag(block, vmax=8,hmax=8) for block in embedded\_dct\_blocks]

        else: