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
Снежко М.А.

Проверил: ассистент кафедры информатики
Герчик А.В.

Минск 2025

СОДЕРЖАНИЕ

1 ЦЕЛЬ РАБОТЫ

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*), 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 и этапы внедрения и извлечения данных.

2 ХОД РАБОТЫ

Программное средство реализовано при помощи языка программирования *Python*.

В рамках лабораторной работы было разработано программное средство для сокрытия и извлечения текстовых сообщений в *JPEG*-изображениях с использованием метода сокрытия в частотной области.

На рисунке 2.1 изображено исходное изображение.

Рисунок 2.1 – Исходное изображение

После выполнения процедуры сокрытия текстового сообщения было получено стегоизображение представлено на рисунке 2.2.

Рисунок 2.2 – 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.

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.

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

```
class SteganographyApp:
    def __init__(self):
        ctk.set_appearance_mode("Dark")
        ctk.set_default_color_theme("blue")
        self.root = ctk.CTk()
        self.root.title("Скрытие и извлечение сообщений")
        self.root.geometry("1100x800")
        self.root.minsize(1000, 700)
        self.center_window()
        self.image_path = ""
        self.output_path = "img/output.jpeg"
        self.preview_image = None
        self.current_mode = "encrypt"

        self.setup_ui()

    def center_window(self):
        self.root.update_idletasks()
        width = self.root.winfo_width()
        height = self.root.winfo_height()
        x = (self.root.winfo_screenwidth() // 2) - (width // 2)
        y = (self.root.winfo_screenheight() // 2) - (height // 2)
        self.root.geometry(f'{width}x{height}+{x}+{y}')
    def setup_ui(self):
        main_container = ctk.CTkFrame(self.root, corner_radius=15)
        main_container.pack(fill="both", expand=True, padx=20, pady=20)

        header_frame = ctk.CTkFrame(main_container, fg_color="transparent")
        header_frame.pack(fill="x", padx=20, pady=(20, 10))

        title_label = ctk.CTkLabel(
            header_frame,
            text="Steganography Laboratory",
            font=ctk.CTkFont(size=26, weight="bold"),
            text_color="#2E86AB"
        )
        title_label.pack()
        subtitle_label = ctk.CTkLabel(
            header_frame,
           text="Скрытие и извлечение сообщений в изображениях с использованием
DCT",
            font=ctk.CTkFont(size=14),
            text_color="#A8DADC"
        )
        subtitle_label.pack(pady=(5, 0))
        mode_frame = ctk.CTkFrame(header_frame, fg_color="transparent")
        mode_frame.pack(pady=10)
        self.mode_var = ctk.StringVar(value="encrypt")
        encrypt_radio = ctk.CTkRadioButton(
            mode_frame,
            text="Режим шифрования",
            variable=self.mode_var,
            value="encrypt",
            command=self.switch_mode,
            font=ctk.CTkFont(weight="bold")
        )
        encrypt_radio.pack(side="left", padx=20)
```