Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)

Институт информатики и вычислительной техники

09.04.01 ”Информатика и вычислительная техника”
профиль ”Научные исследования в области
информатики и вычислительной техники”

Кафедра прикладной математики и кибернетики

Лабораторная работа №5
по дисциплине
Прикладная стеганография

Выполнил:

студент гр.МГ-411 Каргин Роман Александрович

ФИО студента

«17» апреля 2025 г.

Новосибирск 2025 г.

Содержание

Задание

1. Составить обзор статистических методов стегоанализа изображений: анализ статистики Хи-квадрат, RS-анализ, метод AUMP.
2. Реализовать программное средство для стегоанализа изображений, включающее в себя:
   (a) Визуальную атаку на стегоконтейнер, взятую из задания №1;
   (b) Анализ статистики Хи-квадрат по частям изображения;
   (c) RS-анализ, взятый из источника: https://github.com/b3dk7/StegExpose/blob/master/RSAnalysis.java
   (d) Метод AUMP, взятый из источника: http://dde.binghamton.edu/download/structural_lsb_detectors/
   (e) Дополнительно можно реализовать стегоанализ на основе сжатия.

Необходимо, чтобы программа позволяла загружать как отдельное изображение, так и сразу несколько изображений, предоставив пользователю возможность выбрать расположение файлов.

Результаты стегоанализа должны отображаться в интерфейсе программного средства в понятном для пользователя виде, предполагая работу стороннего стегоаналитика. При анализе нескольких файлов сразу, результаты должны записываться в текстовый файл по выбранному пути сохранения.

Отчет по работе должен содержать результаты всех пунктов задания, включая описание кода программы.

Имплементация

Ссылка на код — https://github.com/Nulliream/steg/tree/main/Task5

Все алгоритмы реализованы в модуле control. В качестве библиотеки для обработки изображений использовался PILLOW.

Интерфейс — в модуле ui. В качестве библиотеки дял интерфейса использовался Qt.

χ^2

χ^2 анализ используется для определения вероятности того, что оба распределения, основываясь на большой выборке данных, относятся к одному типу распределения.

В качестве сравниваемых выборок мы берём значения младших трёх битов: 000, 001 и т.д. Мы попарно нормализируем блоки ряда: 000 и 001, 010 и 011, 100 и 101, 110 и 111, суммируя значения и деля их на два. Данные два распределения мы и сравниваем.

Код алгоритма предоставлен в классе Chi2. В логике реализовано вручную лишь построение выборок и их нормализация. Для выполнения теста χ^2 используется функция пакета scipy со степенью свободы 1.

RS

Изображение делится на группы соседних пикселей размером n. Определяется функция, принимающая в качестве аргумента пиксели группы и возвращающая некоторое вещественное число, описывающее их схожесть друг с другом ($f(x)$). Определяется функция, переворачивающая младший бит пикселя ($F(x)$).

Определяются три группы:

$$\text{Регулярная: } G \in R \Leftrightarrow f(F(G)) > f(G)$$
$$\text{Сингулярная: } G \in S \Leftrightarrow f(F(G)) < f(G)$$
$$\text{Неиспользуемая: } G \in U \Leftrightarrow f(F(G)) = f(G)$$

где $F(G) = (F(x_1), \ldots, F(x_n))$. Чтобы решать, какие пиксели переворачивать, используется маска M, являющаяся массивом из значений -1, 0, 1.

Пусть R_M — число регулярных групп для маски M, S_M — число сингулярных групп для маски M. По условиям $R_M + S_M \leq 1$ и $R_{-M} + S_{-M} \leq 1$ мы можем предположить, что в обычном изображении $R_M \cong R_{-M}$ и $S_M \cong S_{-M}$. При увеличении вложенного сообщения разница между R_M и S_M уменьшается, а между R_M и R_{-M}, S_M и S_{-M} увеличивается. Основываясь на этом, можно вычислить вероятный размер вложенного сообщения.

AUMP

Пиксели собираются в группы размером n каждый, чтобы их распределение зависело от малого числа параметров. После тестируется гипотеза о том, что распределения без спрятанных битов и со спрятанными совпадают.

Результаты

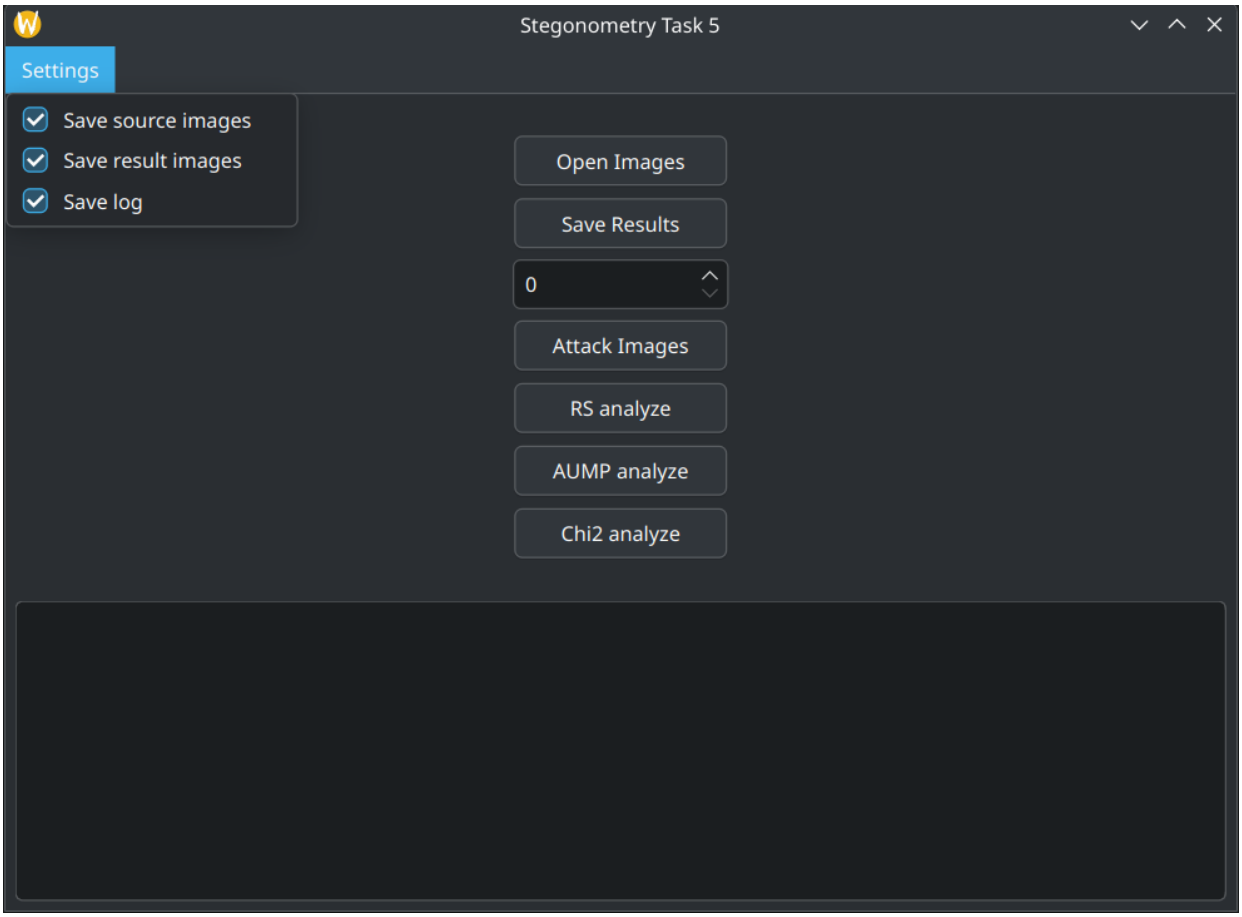

Рис. 1: Главное окно программы

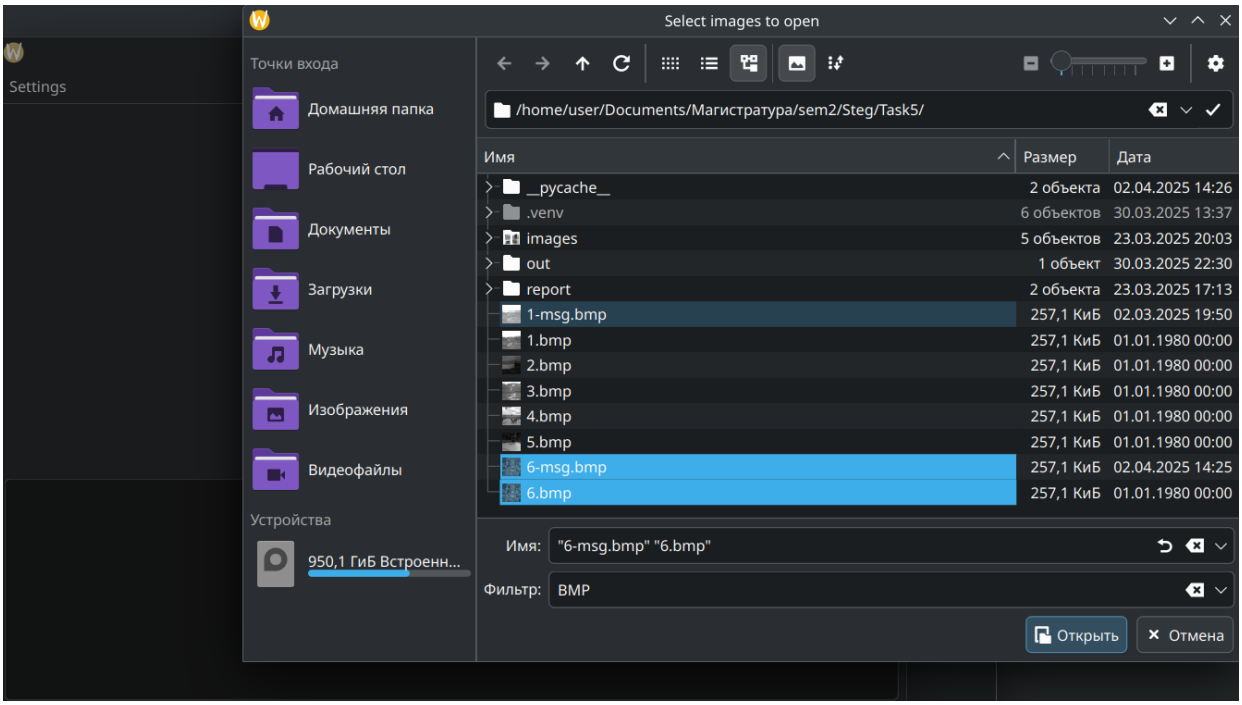

Рис. 2: Открытие изображений

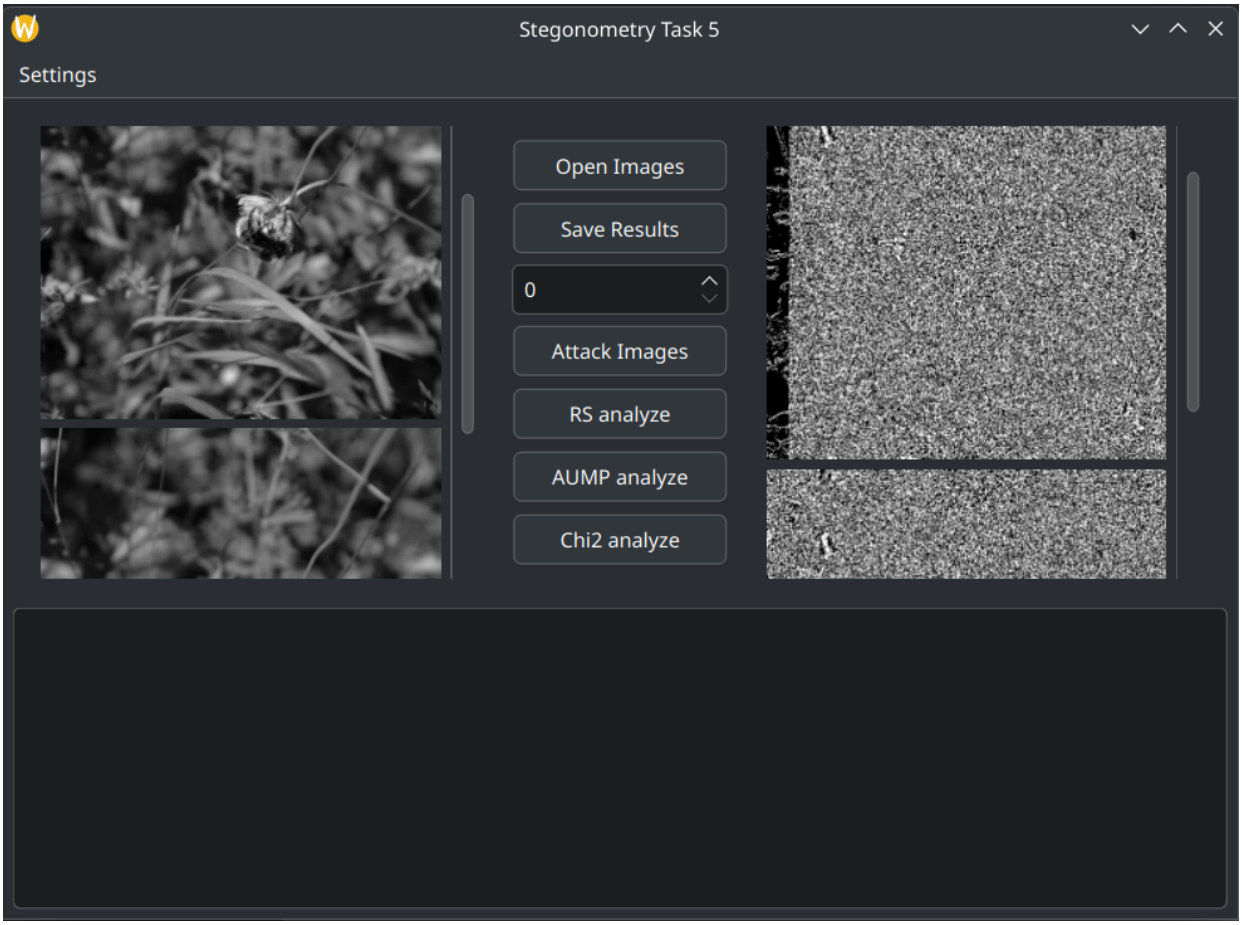

Рис. 3: Визуальная атака

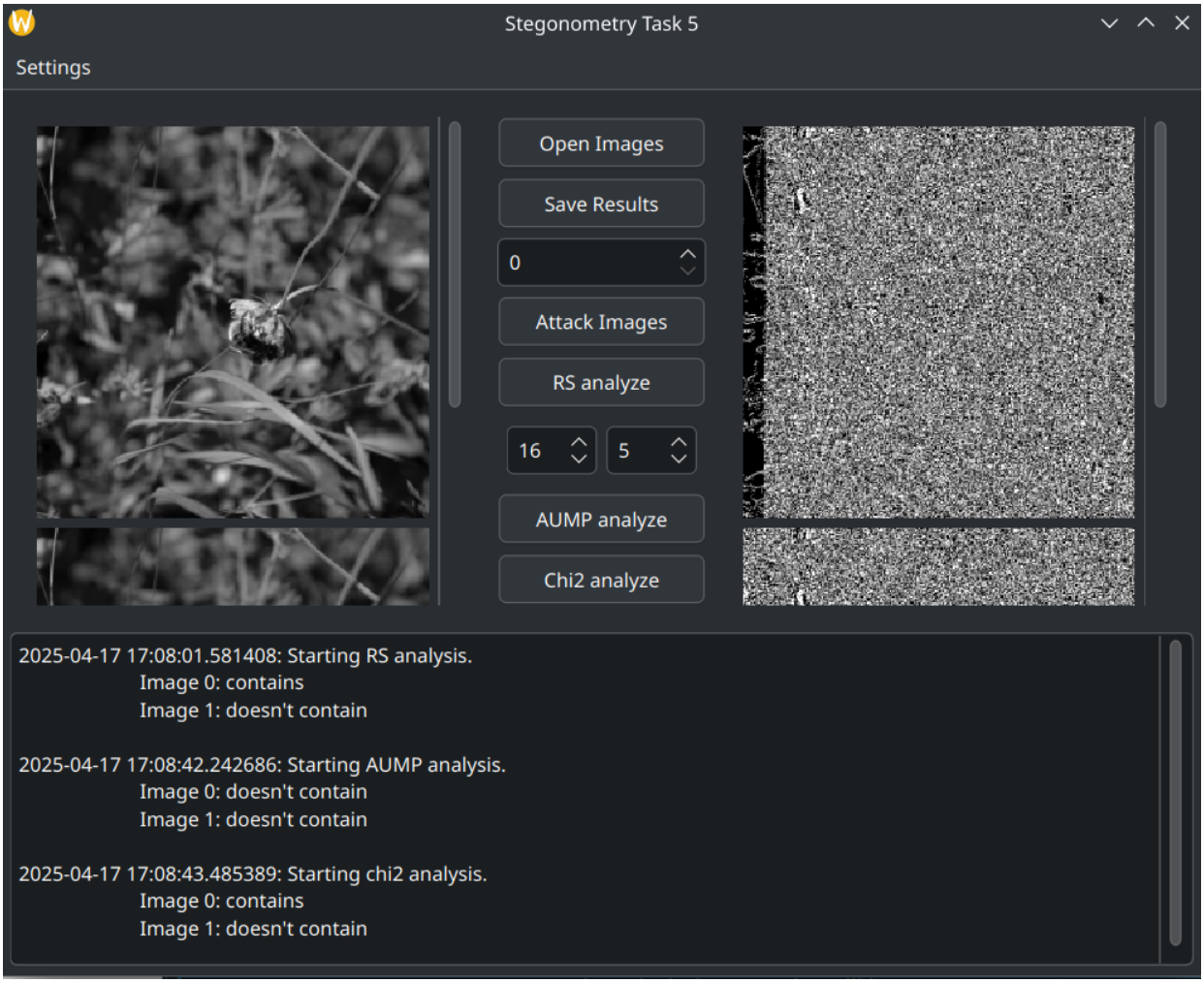

Рис. 4: Анализирование

Рис. 5: Сохранение результатов

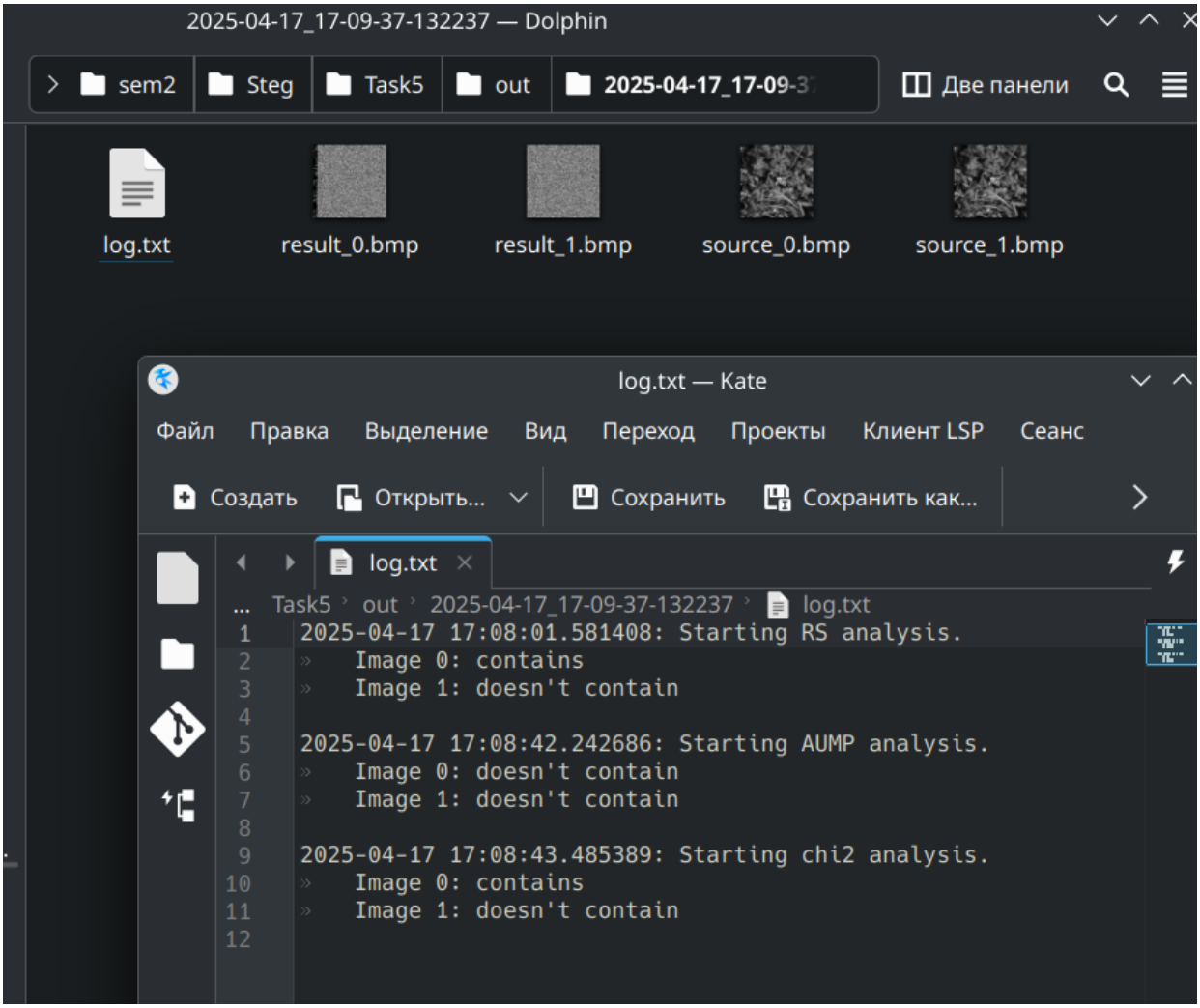

Рис. 6: Сохранённые результаты