Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**Криптографические методы защиты информации**

**Лабораторная работа №14**

ИССЛЕДОВАНИЕ СТЕГАНОГРАФИЧЕСКОГО МЕТОДА НА ОСНОВЕ ПРЕОБРАЗОВАНИЯ НАИМЕНЕЕ ЗНАЧАЩИХ БИТОВ

Вариант №6

Выполнил:

Студент 3 курса 4 группы ФИТ

Левша Марк Сергеевич

Минск 2023

**Цель**: изучение стеганографического метода встраивания\* /извлечения тайной информации с использованием электронного файла контейнера на основе преобразования наименее значащих битов (НЗБ), приобретение практических навыков программной реализации данного метода.

**Задачи**:

1. Закрепить теоретические знания из области стеганографического преобразования информации, моделирования стеганосистем, классификации и сущности методов цифровой стеганографии.

2. Изучить алгоритм встраивания/извлечения тайной информации на основе метода НЗБ (LSB – Least Significant Bit), получить опыт практической реализации метода.

3. Разработать приложение для реализации алгоритма встраивания/извлечения тайной информации с использованием электронного файла-контейнера на основе метода НЗБ.

4. Познакомиться с методиками оценки стеганографической стойкости метода НЗБ.

5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента

**Практическое задание**

В ходе лабораторной работы было разработано приложение, которое в качестве входного параметра принимает картинку и текст и осаждает текст на картинке в последних битах двумя способами, получая новую картинку. Так же приложение формирует цветовые матрицы отдельно по трем цветам и по всем цветам вместе.

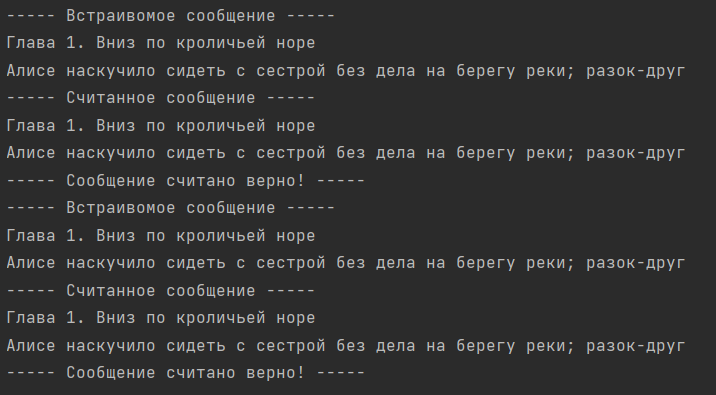
Консольный вывод программы представлен на рисунке 1.

Рис. 1 – консольный программы

Если взглянуть на исходную картинку и на картинку, в которую было осажено сообщение. На рисунке 2 представлена исходная картинка, а на рисунках 3 и 4 картинки с осаженным текстом.

Рис. 2 – исходная картинка

Рис. 3 – картинка в которую страивали биты последовательно

Рис. 4 – картинка в которую страивали биты когерентным методом

Был произведен визуальный анализ с привлечением одногруппника. Анализ показал, что визуально все 3 картинки схожи и разницу в картинках не удалось найти. Это говорит о том, что если изменить младший бита одного из цветов, то визуально для человека ничего не изменится и узнать, что в картинке скрыта информация с первого взгляда невозможно.

Так же были сформированы цветовые матрицы по каждому цвету в отдельности и по всем 3 цветам исходного изображения и цветовую матрицу по синему цвету изображения с осаженным текстом. Цветовые матрицы представлены на рисунках 5-9.

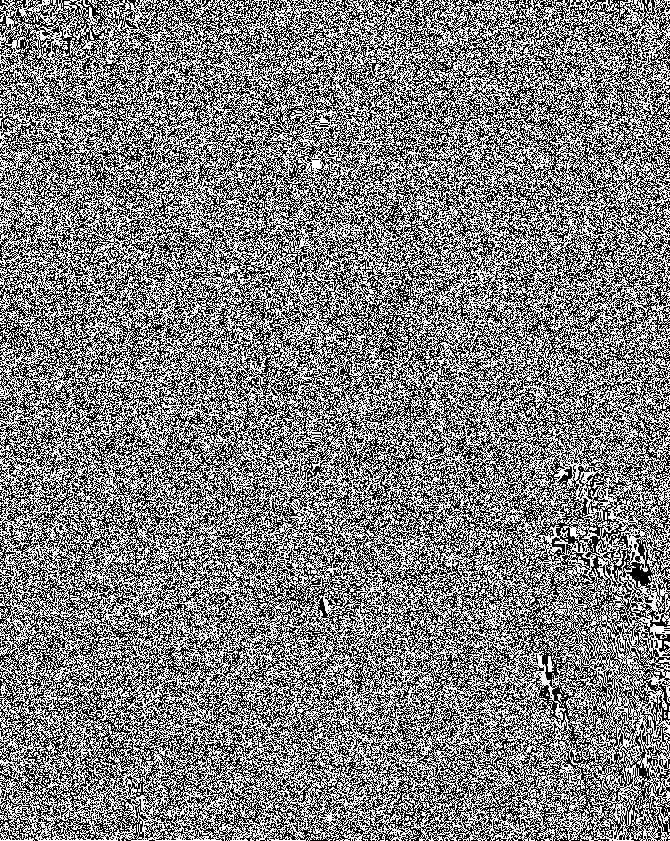
Рис. 5 –цветовая матрица по синему цвету исходного изображения

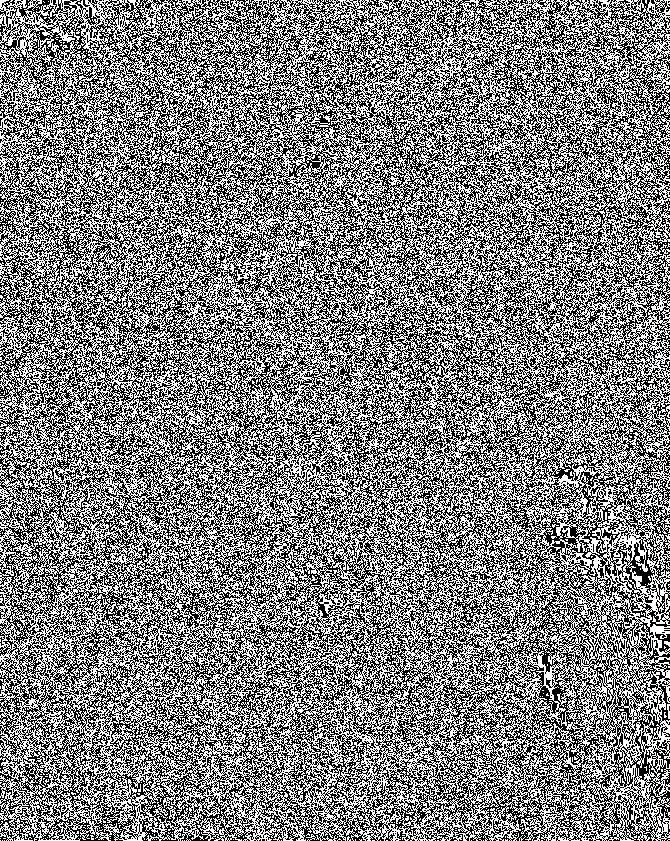
Рис. 6 – цветовая матрица по зелёному цвету исходного изображения

Рис. 7 – цветовая матрица по красному цвету исходного изображения

Рис. 8 – цветовая матрица по всем цветам исходного изображения

**Вывод**: в ходе лабораторной работы были изучены стеганографический метод преобразования младших битов для скрытия сообщения, а также разработана программа, реализовывающая этот метод.