Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование стеганографического метода на основе преобразования наименее значащих битов.**

Студент: Буданова К. А.

ФИТ 3 курс 5 группа

Преподаватель:

Савельева Маргарита Геннадьевна

1. **Цель работы**

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.

1. **Задания**

Разработать собственное приложение, в котором должен быть реализован метод НЗБ. При этом:

* выбор файла-контейнера – по согласованию с преподавателем;
* реализовать два варианта осаждаемого/извлекаемого сообщения:
* собственные фамилия, имя и отчество;
* текстовая часть отчета по одной из выполненных лабораторных работ;
* реализовать два метода (на собственный выбор) размещения битового потока осаждаемого сообщения по содержимому контейнера;
* сформировать цветовые матрицы (по аналогии с рис. 12.7), отображающие каждый задействованный для осаждения уровень младших значащих битов контейнера;
* выполнить визуальный анализ (с привлечением коллег в качестве экспертов) стеганоконтейнеров с различным внутренним содержанием; сделать выводы на основе выполненного анализа.

3. Результаты выполнения работы оформить в виде отчета по установленным правилам.

1. **Ход работы**

В ходе работы для осаждения сообщения было разработано два метода: EmbedPixelPermutation и EmbedLSB. Первый метод реализует алгоритм псевдослучайной перестановки. Код его реализации представлен на рисунке 3.1.

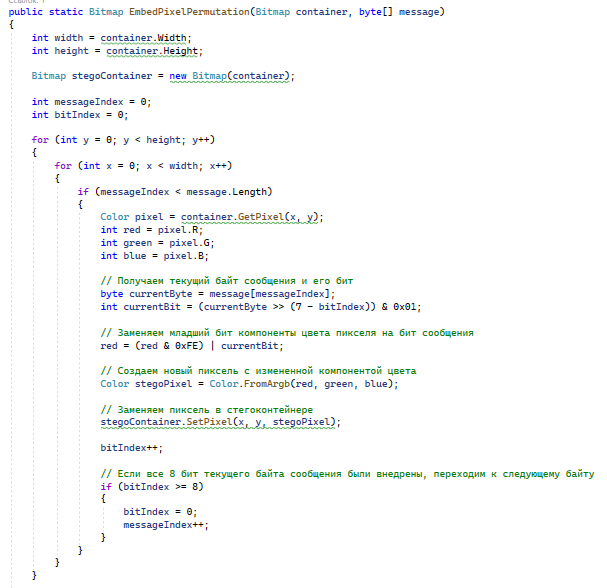


Рисунок 3.1 – Метод EmbedPixelPermutation

Для извлечения сообщения из стеганоконтейнера была разработана функция ExtractPixelPermutation, код которой представлен на рисунке 3.2.

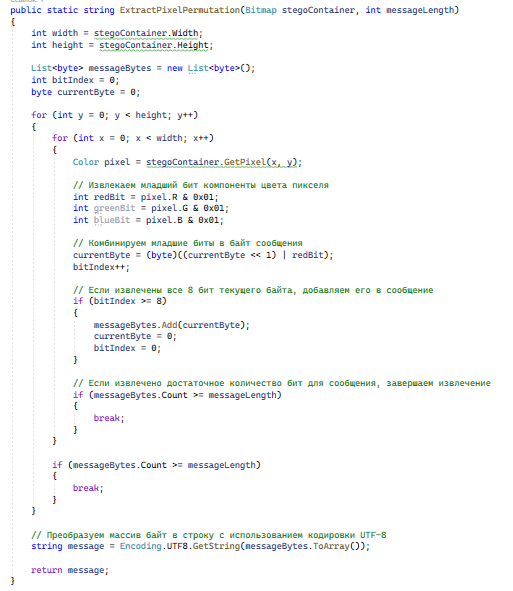


Рисунок 3.2 – Метод ExtractPixelPermutation

В качестве файла-контейнера был выбран следующий рисунок 3.3.

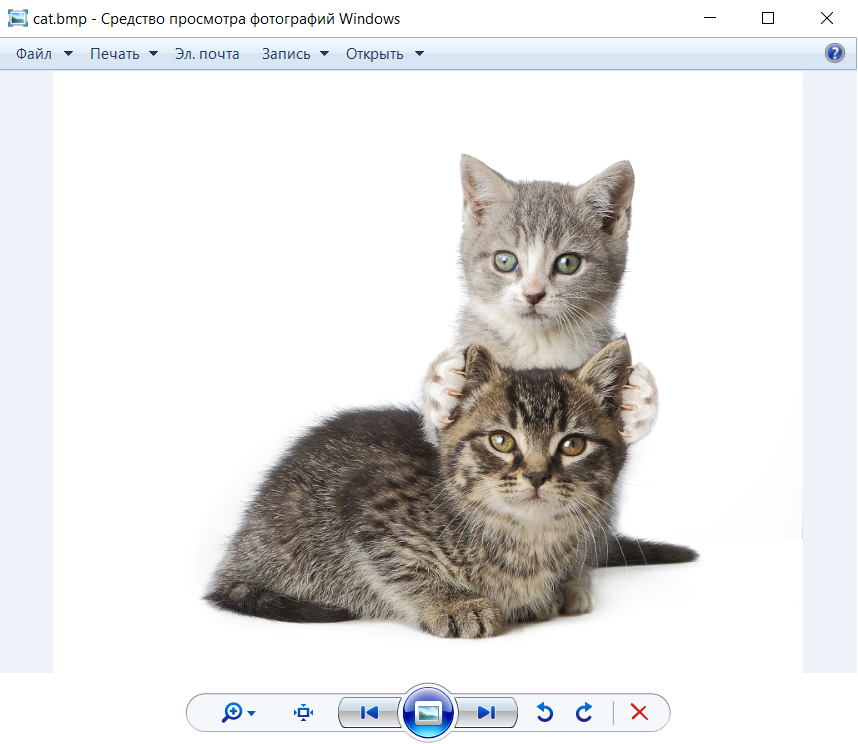


Рисунок 3.3 – Выбранный стеганоконтейнер

Входные данные и результат работы представлены на рисунках 3.4 – 3.5.



Рисунок 3.4 – Входные данные

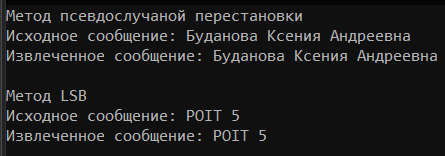


Рисунок 3.5 – Результат работы

Также, с помощью метода GenerateColorMatrix была сформирована цветовая матрица, отображающая каждый задействованный для осаждения уровень младших значащих битов контейнера. Сам метод и результат его работы представлены на рисунках 3.6 – 3.7.

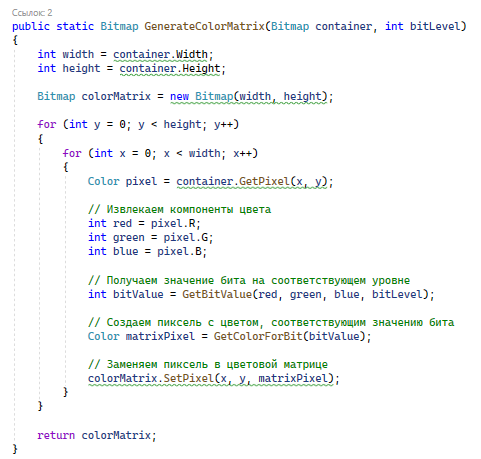


Рисунок 3.6 – Метод GenerateColorMatrix

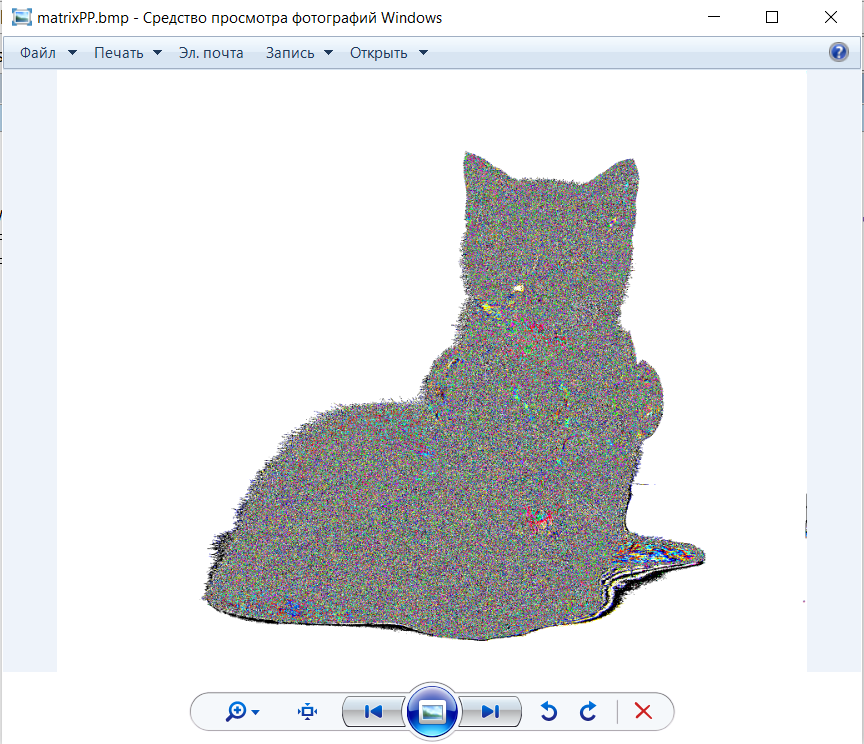


Рисунок 3.7 – Результат работы метода GenerateColorMatrix

Для реализации второго метода размещения битового потока осаждаемого сообщения по содержимому контейнера был выбран алгоритм LSB. Его реализация представлена в методе EmbedLSB на рисунке 3.8.

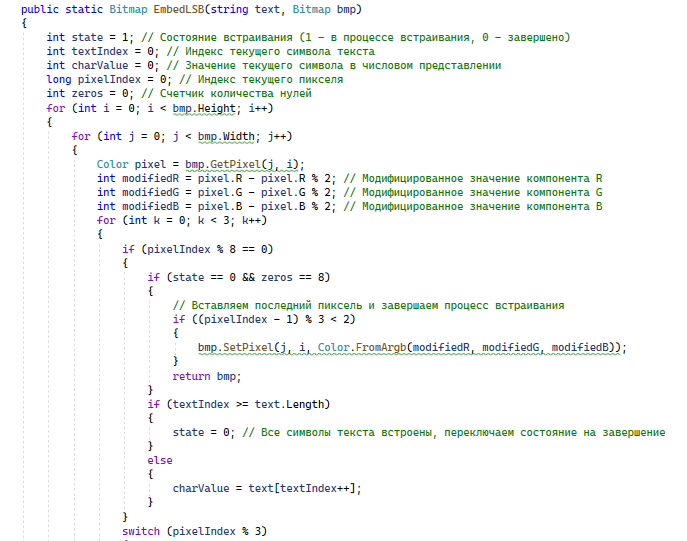


Рисунок 3.8 – Метод EmbedLSB

Для извлечения сообщения из стеганоконтейнера была разработана функция ExtractLSB, код которой представлен на рисунке 3.9.

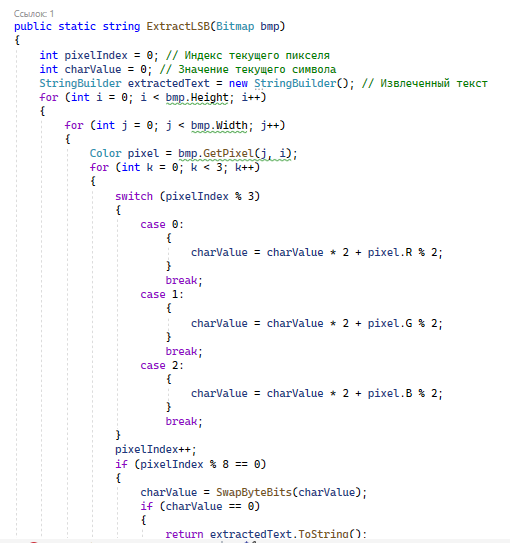


Рисунок 3.9 – Метод ExtractLSB

Входные данные, результат работы и цветовая матрица представлены на рисунках 3.10 – 3.12.

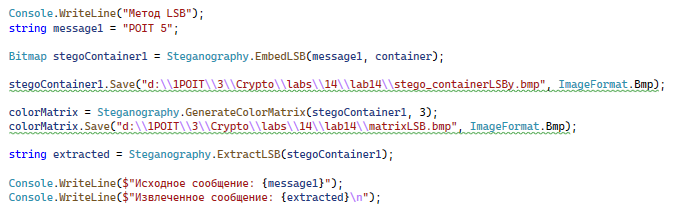


Рисунок 3.10 – Входные данные

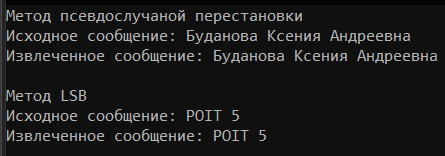


Рисунок 3.11 – Результат работы

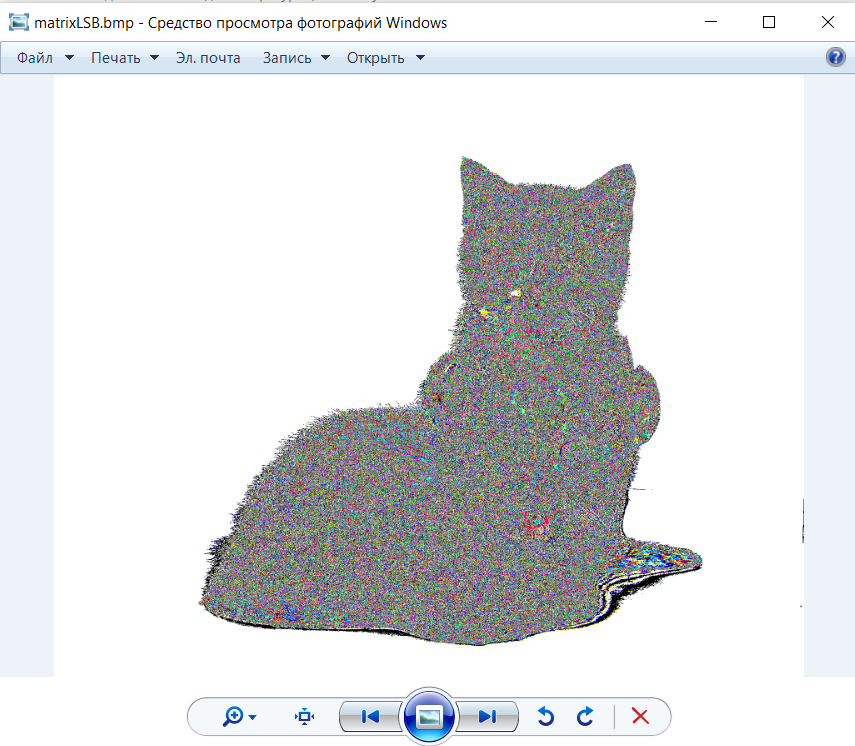


Рисунок 3.12 – Цветовая матрица

**Вывод**

В ходе лабораторной работы были изучены стеганографические методы встраивания/извлечения тайной информации с использованием электронного файла-контейнера на основе преобразования наименее значащих битов (НЗБ), приобретение практических навыков программной реализации данного метода.

Также было разработано авторское приложение в соответствии с целью лабораторной работы.