Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование стеганографического метода на основе

преобразования наименее значащих бит

Студент: Николаева Е.В.

ФИТ 3 курс 5 группа

Преподаватель:

Савельева Маргарита Геннадьевна

Минск 2023

1. **Описание приложения**

Приложение написано на языке программирования C# и позволяет выполнить 2 задачи:

* использован файл-контейнер формата bmp;
* реализованы методы размещения битового потока осаждаемого сообщения;
* выполнен визуальный анализ стеганоконтейнеров с различным внутренним содержанием.

1. **Методика выполнения поставленных задач**

Был использован метод НЗБ (наименее значащий бит), его суть заключается в замене последних значащих битов в контейнере на биты скрываемого сообщения. Метод НЗБ основывается на ограниченных способностях зрения или слуха человека, вследствие чего людям тяжело различать незначительные вариации цвета или звука.

Замена одного или даже нескольких младших битов для человеческого глаза будет почти незаметна, поскольку реально человек может различать около полторы сотни цветовых оттенков.

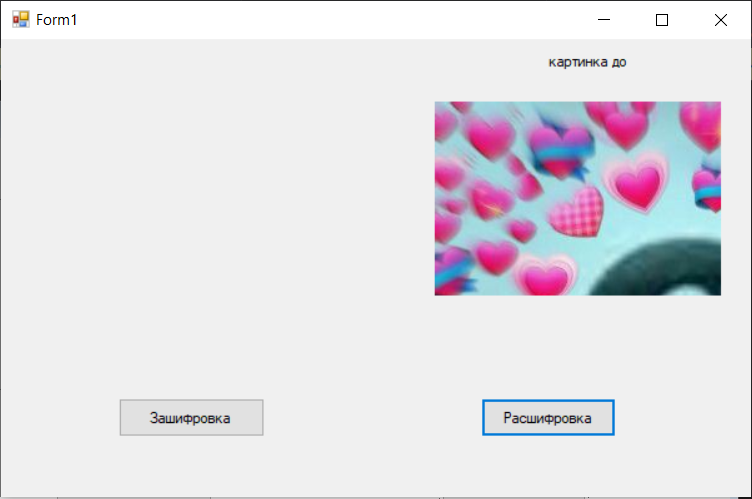
Одним из простейших и понятных для решения наших задач является формат BMP (BitMaP) – одна из форм представления растровой графики. 

Рис. 2.1 – Разработанное приложение

На экране приложения первоначально видна картинка до шифрования. После выполнения зашифрования рядом появится картинка для того, чтобы показать, что человеку невооруженным взглядом не увидеть разницы между двумя картинками.

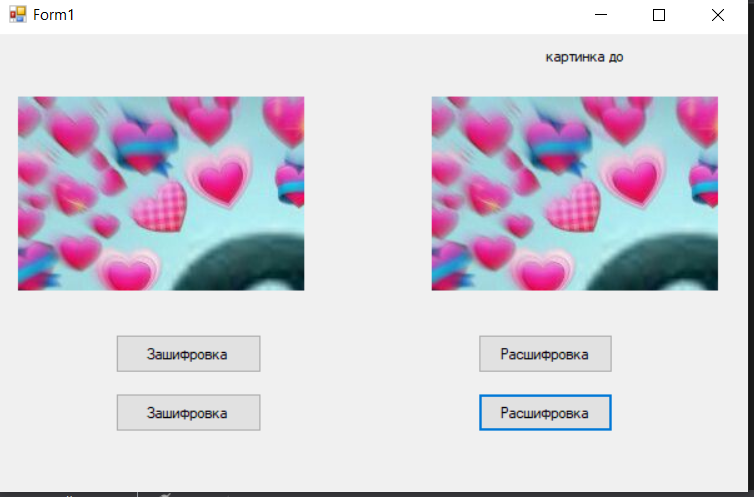


Рис. 2.2 – Разработанное приложение, после зашифровки

Пользователь может нажать на две кнопки. Путь к различным файлам уже прописан в коде.

На рисунке 2.3. изображено то, как берется файл и зашифровывается, на рисунке 2.4. уже расшифровка.

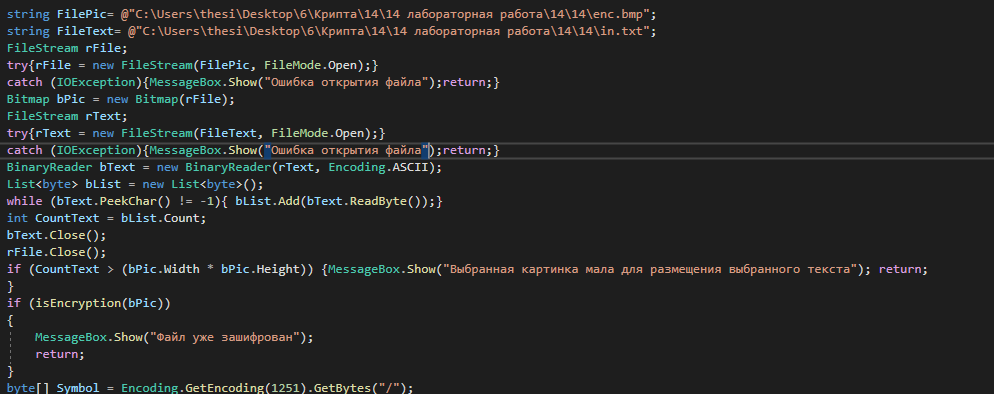


Рис. 2.3 – Функция зашифровки

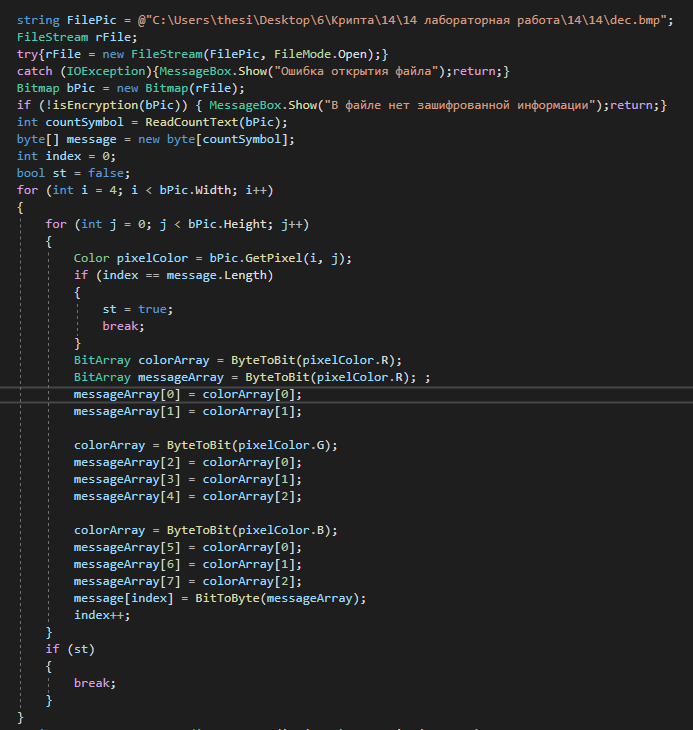


Рис. 2.4 – Функция расшифровки

Так же присутствует функция проверки, зашифровано ли изображение или нет. Эта функция изображена на рисунке 2.5.

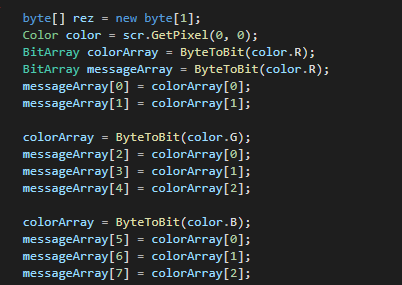


Рис. 2.5 – Функция проверки на кодировку

Так же реализован второй метод: Метод комплексного спектра. Этот метод основан на преобразовании Фурье и размещает битовый поток сообщения в частотной области изображения. Он менее заметен для человеческого восприятия, чем тот, что мы использовали сверху. На рисунках 2.6 и 2.7 представлены две функции.

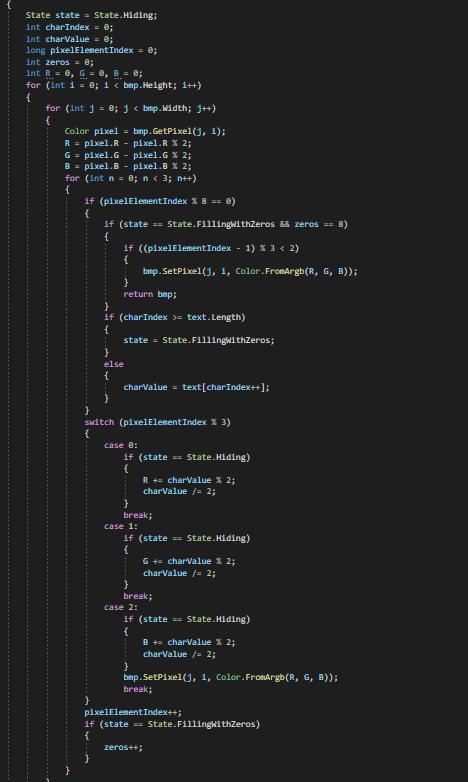
****

Рис. 2.6 – Функция зашифровки

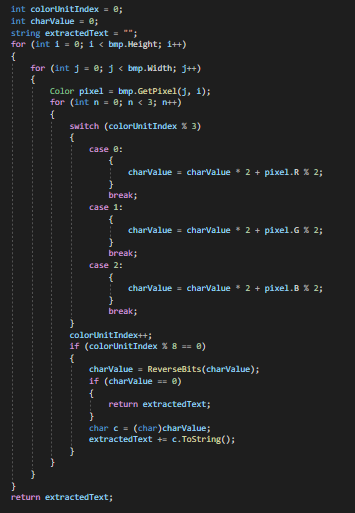


Рис. 2.7 – Функция расшифровки

Сравним два контейнера: пустой и полный. На рисунках 2.6, 2.7. представлены пустой контейнер и стеганоконтейнер, в котором осаждено сообщение. Человеческому глазу не удастся выявить никакой разницы в двух контейнерах.



Рис. 2.6 – Пустой контейнер



Рис. 2.7 – Контейнер с осажденым сообщением

Сформируем цветовые матрицы отображающие пиксели, воспользовавшись сайтом. На рисунках 2.8 и 2.9. видны сразу же отличия. Потому мы можем сделать вывод, что без цветовой матрицы мы не сможем найти отличия между двумя контейнерами.



Рис. 2.8 – Контейнер с осажденым сообщением

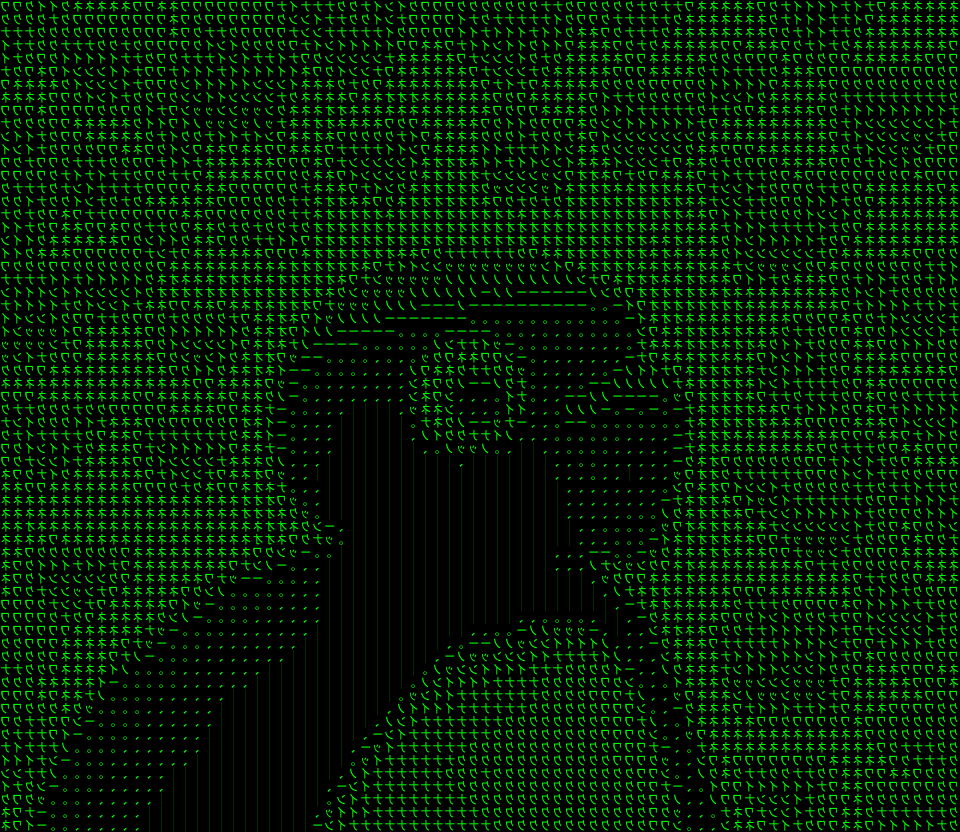


Рис. 2.9 – Пустой контейнер

**Вывод**

В ходе лабораторной работы были приобретены практические навыки программной реализации стеганографического метода осаждения/извлечения тайной информации с использованием электронного файла-контейнера (bmp) на основе преобразования наименее значащих бит (НЗБ).