Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Криптографические методы защиты информации

Студент: Сенченя В.И.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М. Г.

Минск 2023

**Лабораторная работа №14**

**Тема «**исследование стеганографического метода на основе преобразования наименее значащих битов**»**

Цель: изучение стеганографического метода встраивания\* /извлечения тайной информации с использованием электронного файлаконтейнера 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. Познакомиться с методиками оценки стеганографической стойкости метода НЗБ.
4. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Метод замены младшего бита**

Метод НЗБ основывается на ограниченных способностях зрения или слуха человека, вследствие чего людям тяжело различать незначительные вариации цвета или звука. Рассмотрим это на примере 24-битного растрового RGB-изображения. Как известно, каждая точка кодируется тремя байтами. Каждый байт определяет интенсивность красного (Red), зеленого (Green) и синего (Blue) цветов. Совокупность интенсивностей цвета в каждом из трех каналов определяет оттенок пикселя.

Младшие биты (выделены бледным, справа) дают незначительный «вклад» в изображение по сравнению со старшими. Замена одного или даже нескольких младших битов для человеческого глаза будет почти незаметна, поскольку реально человек может различать около полторы сотни цветовых оттенков.

Код для замены младшего бита в изображении на бит сообщения предоставлен на рисунке 1.1, вывод консоли предоставлен на рисунке 1.2. В первом варианте я использовал пиксели для внедрения по строкам, во тором случае по столбцам.

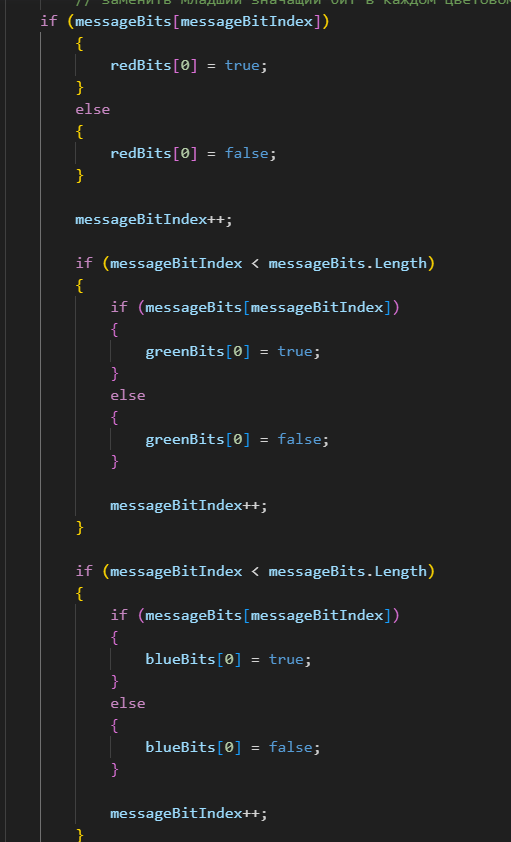


Рисунок 1.1 – Код замены бита



Рисунок 1.2 – Вывод консоли

Исходное изображение и результат внедрения сообщения предоставлен на рисунках 1.3 и 1.4.



Рисунок 1.3 – Исходное изображение



Рисунок 1.4 – Измененное изображение

Как мы видим, на рисунках невозможно или очень сложно заметить разницу человеческим глазом.

Матрица битов для исходного и изменённого изображений предоставлены на рисунках 1.5 и 1.6.



Рисунок 1.5 – Матрица битов исходного сообщения



Рисунок 1.6 – Матрица битов изменённого сообщения

Как мы видим, на рисунках невозможно или очень сложно заметить разницу человеческим глазом.

По итогам стеганографии мы смогли внедрить в изображение сообщение, при этом невозможно или очень сложно с виду понять, что это изображение было модифицировано.

**Вывод**

В ходе выполнения лабораторной работы я приобрёл и закрепил навыки практические навыки разработки приложения для реализации криптографических алгоритмов на основе эллиптических кривых.