Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование стеганографического метода на основе

преобразования наименее значащих бит

Студент: Раченок И.А.

ФИТ 3 курс 4 группа

Преподаватель:

Сазонова Дарья Владимировна

Минск 2023

1. **Описание приложения**

Приложение позволяет выполнить следующие задачи:

* реализцаия метода НЗБ (файл-контейнер был выбран формата bmp);
* реализация метода размещения битового потока осаждаемого сообщения;
* выполнен визуальный анализ стеганоконтейнеров с различным внутренним содержанием.

1. **Методика выполнения поставленных задач**

В стеганографии термин "НЗБ" (Наименее значащий бит) обычно относится к методу скрытия информации в младших битах цветовых компонентов изображений.

Основная идея метода НЗБ заключается в том, что младшие биты цветовых компонентов (обычно красного, зеленого и синего) могут быть изменены сравнительно незаметно для человеческого восприятия. При этом, каждый байт пикселя может содержать 8 бит информации, однако изменение младших бит не вызывает значительных изменений в яркости и цветовом восприятии изображения.

Процесс скрытия информации с использованием метода НЗБ включает следующие шаги:

* Разбиение сообщения, которое нужно скрыть, на последовательность битов.
* Чтение пикселей изображения построчно.
* Изменение младших битов цветовых компонентов пикселей в соответствии с битами сообщения.
* Повторение шагов 2-3 для всех пикселей изображения до тех пор, пока все биты сообщения не будут скрыты.

При извлечении информации изображение проходит обратный процесс:

* Чтение пикселей изображения построчно.
* Извлечение младших битов цветовых компонентов пикселей.
* Формирование последовательности извлеченных битов.
* Обработка последовательности битов для восстановления исходного сообщения.

Метод НЗБ является одним из простых и широко применяемых методов стеганографии. Однако, он может быть подвержен различным атакам и детектированию, поэтому в более требовательных задачах стеганографической защиты информации могут использоваться более сложные и надежные методы.

Формат, в котором мы передавали сообщение был выбран BMP (BitMaP). Далее будет представлен пример работы с приложением, куда мы вводим текст который хотим передать в нашем изображении, само изображение (мы передали только путь, а для наглядности рядом были размещены два изображения, одно которое не содержит информации, а другое содержит), и результат сохраняется в новом изображении, рисунок 2.1

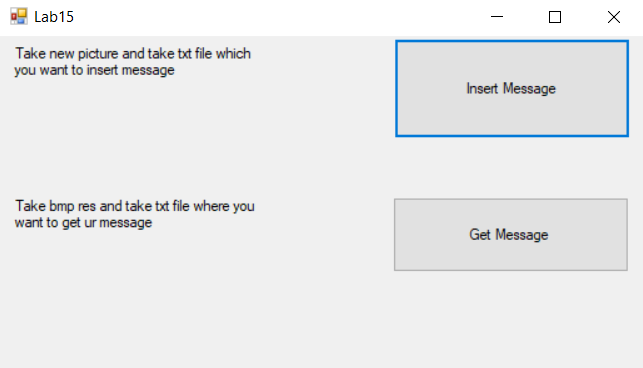


Рисунок 2.1 – Пример работы с приложением

На рисунке 2.2 представлен анализ двух изображений (слева отредактированная, а справа нет).



Рисунок 2.2 – Сравнение изображений

На рисунке 2.3 представлены файл сообщение которое мы зашифровывали и файл сообщение которое мы достали из изображения.

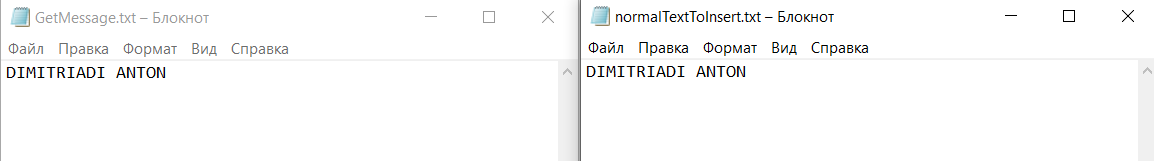


Рис. 2.3 – Результат сообщений

На рисунке 2.4 представлен алгоритм записи сообщения в текст.

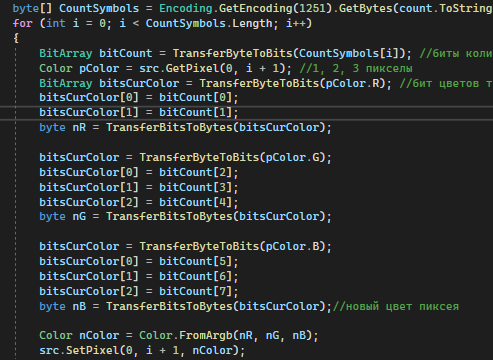


Рисунок 2.4 – Функция вставки сообщения в изображение

На рисунке 2.5 представлен алгоритм извлечения сообщения из изображения.

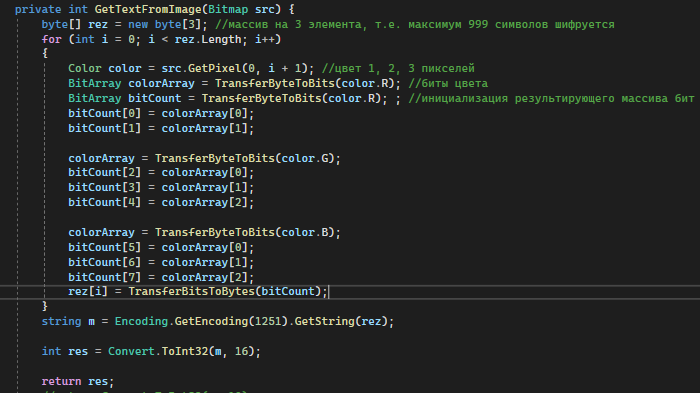


Рисунок 2.5 – Функция извлечения сообщения из изображения

Также приведен метод поиска по строкам и по столбцам, рисунок 2.6.

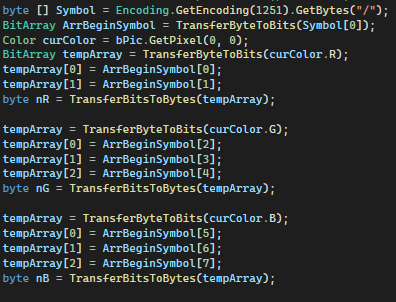


Рисунок 2.6 – Метод шифрования (инверсный)

Попробуем рассмотреть разницу между исходным изображением и обработанным, представим изображения в виде цветовых матриц. Рисунки 2.7 и 2.8 отличаются. Из этого следует вывод, что с помощью цветовой матрицы можно увидеть различия между изображениями.

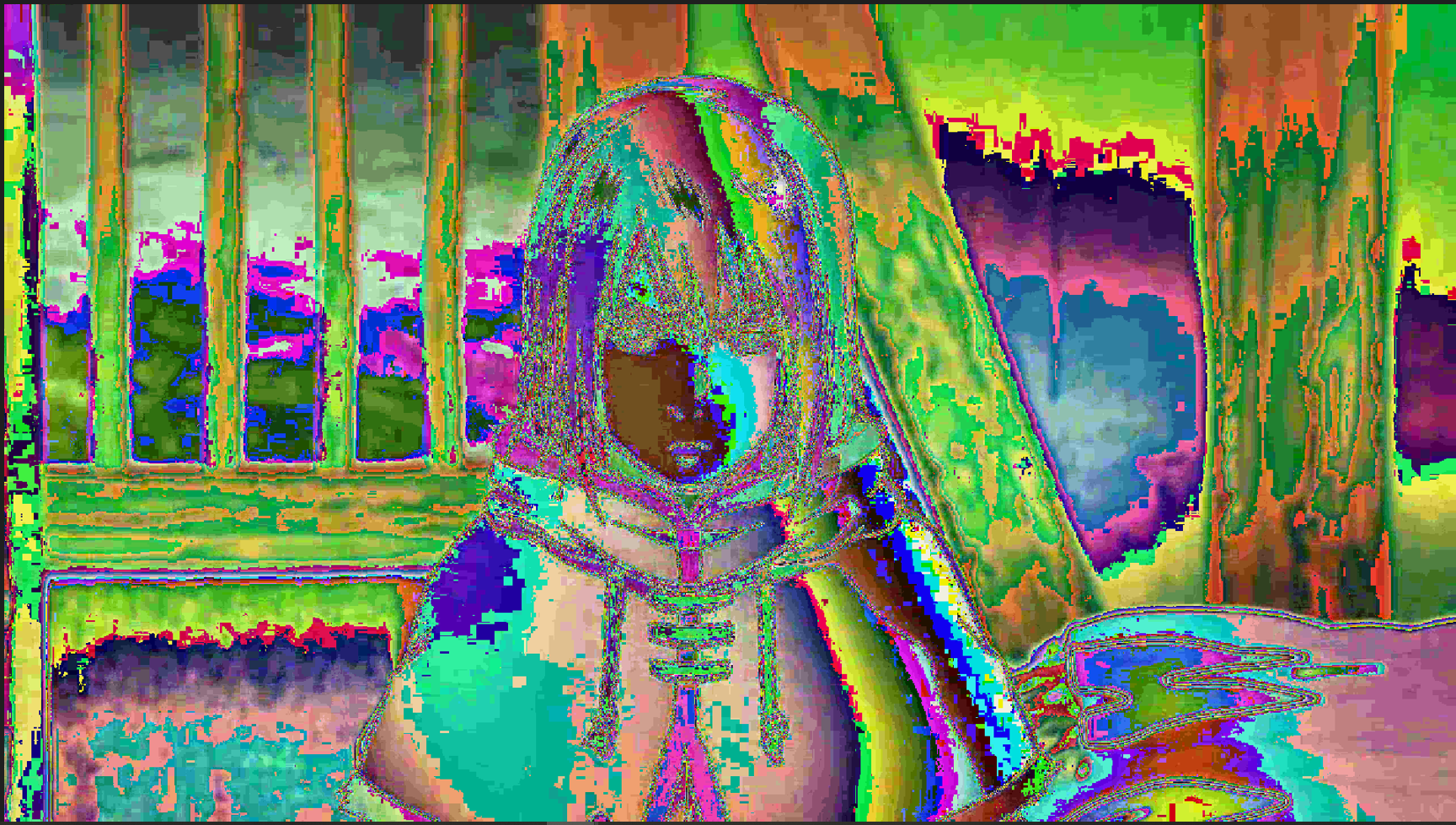


Рисунок 2.7 – Контейнер с сообщением



Рисунок 2.8 – Пустой контейнер

Проанализировав цветовые матрицы, здесь более возможно отличить изменения НЗБ и определить изменения картинок.

**Вывод**

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