МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №14**

по дисциплине «Криптографические методы защиты информации»

на тему: ИССЛЕДОВАНИЕ СТЕГАНОГРАФИЧЕСКОГО

МЕТОДА НА ОСНОВЕ ПРЕОБРАЗОВАНИЯ

НАИМЕНЕЕ ЗНАЧАЩИХ БИТОВ

Выполнил студентка 3 курса 5 группы специальность ПОИТ Буранко В.Д.

(Ф.И.О.)

Преподаватель ассистент Савельева Маргарита Геннадьевна

(Ф.И.О.)

**Содержание**

[**Практические задания** 4](#_Toc136545865)

[**Выводы** 6](#_Toc136545866)

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации криптографических алгоритмов на основе эллиптических кривых.

**Задачи:**

* Закрепить теоретические знания по алгебраическому описанию и геометрическому представлению операций над эллиптическими кривыми (ЭК):
  + по алгоритмам согласования ключевой информации на основе ЭК;
  + алгоритмам зашифрования/расшифрования информации на основе асимметричной криптографии и ЭК;
  + алгоритмам генерации и верификации электронной цифровой подписи на основе асимметричной криптографии и ЭК;
  + оценке криптостойкости систем на основе ЭК.
* Разработать приложение для реализации указанных преподавателем методов криптопреобразования на основе ЭК;
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

# **Практические задания**

В данной лабораторной работе необходимо было разработать собственное приложение, в котором должен быть реализован метод НЗБ. В качестве файла-контейнера мною было выбрано jpg-изображение. Также приложение имеет функционал для формирования цветовых матриц изображений.

Интерфейс приложения представлен на рисунке 1.

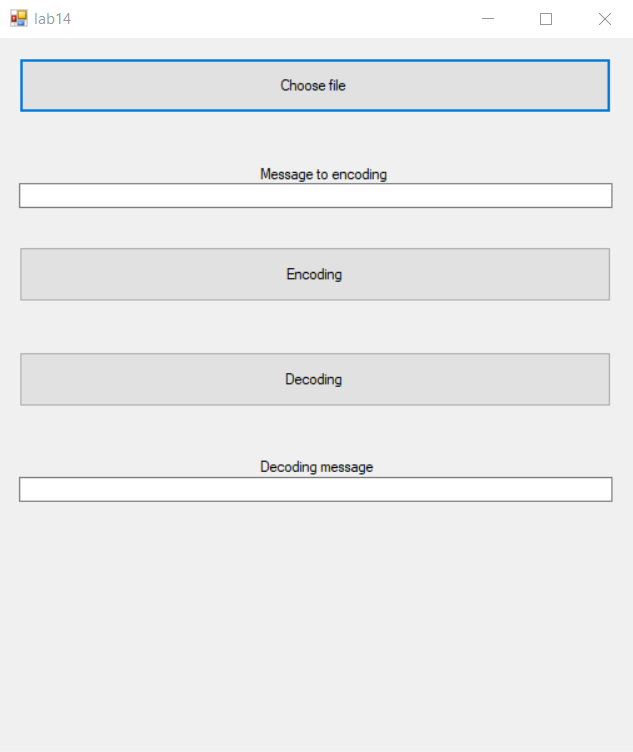


Рисунок 1 – Интерфейс приложения

Исходное изображение представлено на рисунке 2. Для зашифрования сообщения необходимо выбрать изображение, нажав на кнопку «Choose file», написать текст сообщения в поле «Message to encoding» и нажать на кнопку «Encoding». Изображение с осажденными данными при помощи алгоритма наименее значимых битов сохранится в файл с названием «steganography1.png». Данное изображение представлено на рисунке 3.



Рисунок 2 — Исходное изображение



Рисунок 3 — Изображение с сообщением «My pug» методом осаждения в наименее значимых битах

Так же был разработан алгоритм осаждения сообщения в младших разрядах яркости. Метод осаждения в младших разрядах яркости позволяет скрыть данные в изображении, используя младшие биты компоненты яркости каждого пикселя. Результат работы алгоритма сохраняется в файл с названием «stenography2.png», изображенный на рисунке 4.



Рисунок 4 — Изображение с сообщением «My pug» методом осаждения в младших разрядах яркости

Для извлечения сообщения из стеганоконтейнера необходимо нажать на кнопку «Decoding». Результат расшифрования сообщения представлен на рисунке 5.

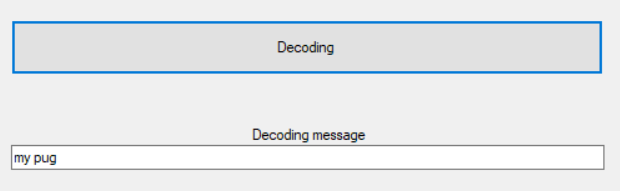


Рисунок 5 — Результат расшифрования сообщения

Так же автоматически при выборе контейнера формируется цветовая матрица и результат сохраняется в файл с названием «matrix.png», который представлен на рисунке 6.

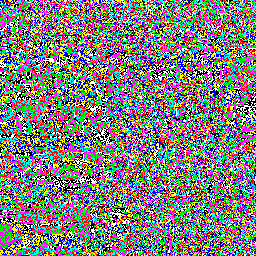


Рисунок 6 – Цветовая матрицаконтейнера

Пустой контейнер и контейнер с осажденным сообщением представлены на рисунке 7.

Рисунок 7 – Визуальный анализ пустого контейнера и контейнера с осажденным сообщением

# **Выводы**

В ходе выполнения данной лабораторной работы было разработано собственное приложение, в котором был реализован метод НЗБ.