Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование стеганографического метода на основе преобразования наименее значащих битов

Студент: Валдайцев А. Д.

ФИТ 3 курс 5 группа

Пр*еп*одаватель: Савельева М. Г.

Минск 2023

# Стеганографическая система

Стеганографическая система – это совокупность средств и методов, которые используются для формирования скрытого канала передачи (или хранения) информации. При этом скрытый канал организуется на базе и внутри открытого канала с использованием особенностей восприятия информации.

«Скрытость» канала передачи тайной информации отличает стеганографию от криптографии: в первом случае тайной является сам факт наличия канала (передачи информации)

Абстрактно стеганографическая система обычно определяется как некоторое множество отображений одного пространства (множества возможных сообщений *М*) в другое пространство (множество возможных стеганосообщений *S*), и наоборот.

Основные компоненты стеганосистемы:

* контейнер *С* (файл-контейнер или электронный документ произвольного формата), в котором размещается (осаждается, скрывается) тайное сообщение *М*; именно контейнер является упомянутым скрытым каналом;
* тайное сообщение *М*, осаждаемое в контейнер для передачи или хранения (например, с целью доказательства или защиты авторских прав на документ-контейнер;
* ключи, или ключевая информация, *K* системы, выполняющие ту же функцию, что и криптографические ключи; ключей может быть несколько, в соответствии с этим современные стеганосистемы характеризуют как многоключевые;
* контейнер со встроенным сообщением, или стеганоконтейнер, *S*, который передается по открытому каналу, также являющемуся важным компонентом анализируемой системы; стеганоконтейнер будем именовать также стеганосообщением.

# Метод наименее значимых битов

Большинство исследований в предметной области посвящено использованию в качестве стеганоконтейнеров изображений (текст также можно рассматривать как изображение).

Метод наименее значимых битов основывается на ограниченных способностях зрения или слуха человека, вследствие чего людям тяжело различать незначительные вариации цвета или звука.

Младшие биты каждой составляющей цвета пикселя 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.

В основе стеганографических преобразований лежит изображение, представленное на рисунке 1.1.



Рисунок 1.1 – Изначальное изображение для преобразований

Цветовая матрица наименее значащих битов для исходного изображения представлена на рисунке 1.2.



Рисунок 1.2 – Цветовая матрица НЗБ исходного изображения

Для реализации встраивания сообщения (по строкам) реализована следующая функция, представленная на рисунке 1.3.

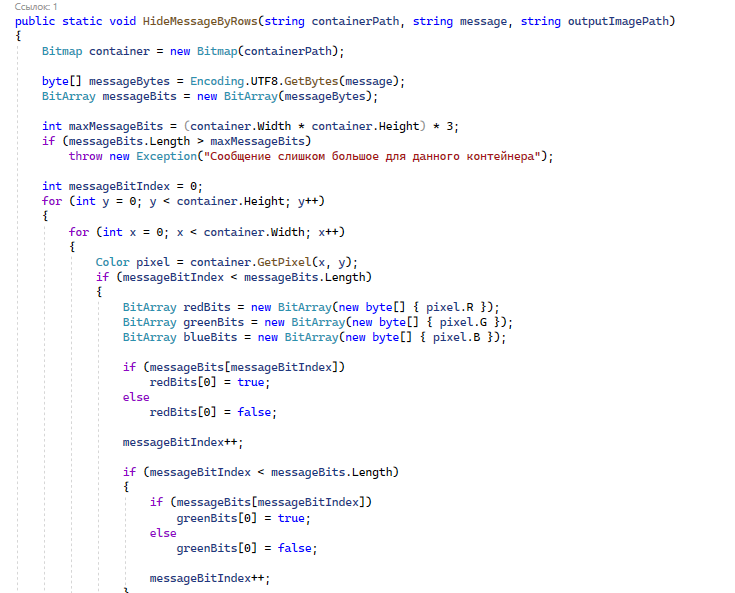


Рисунок 1.3 – Функция встраивания текста в контейнер

В результате получаем изображение, предсталвенное на рисунке 1.4.



Рисунок 1.4 – Изображение с встроенным текстом

Цветовая карта наименее значащих битов данного изображения представлена на рисунке 1.5.



Рисунок 1.5 – Цветовая матрица НЗБ с встроенным текстом

Из рисунка можно заметить, что на изображении не заметно никаких изменений. Однако, в левом верхнем углу цветовой матрицы можно заметить небольшое различие, в котором встроено наше сообщение.

Полученное из изображения сообщение выводится на экран, что изображено на рисунке 1.6.



Рисунок 1.6 – Вывод функции встраивания текста по строкам

Аналогичные результаты получаются для встраивания текста по столбцам, а не по строкам. Код данной функции представлен на рисунке 1.7.

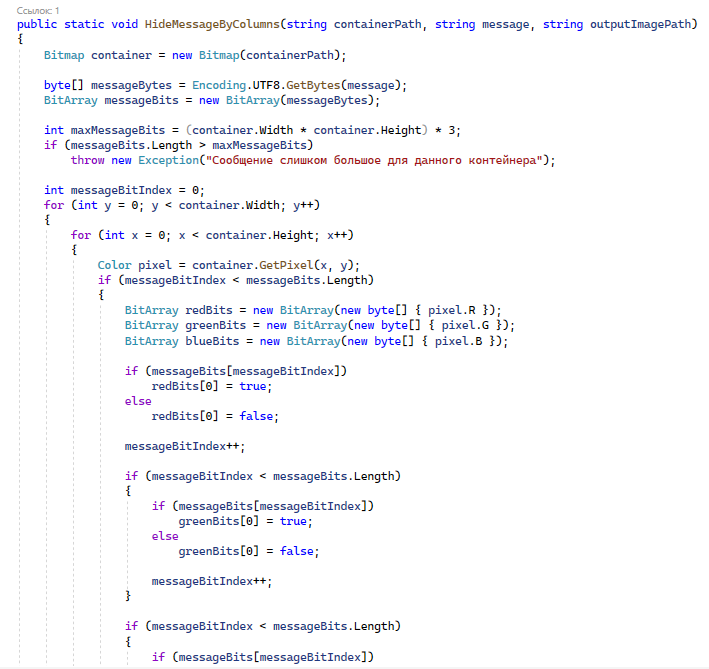


Рисунок 1.7 – Функция встраивания сообщения по столбцам

Аналогично, изменения возможно заметить только в цветовой матрице. Это является уязвимостью алгоритма, посколько по методу «Хи-квадрата» возможно выяснить, что в изображение стенографическим методом встроено некоторое сообщение. Для избежания этого необходимо использовать случайных разброс наименее значимых битов с информацией.

# Вывод

В данный лабораторной работе был изучен стеганографический метод встраивания и извлечения тайной информации с использованием электронного файла-контейнера на основе преобразования наименее значащих битов (НЗБ), а также приобретены практические навыки программной реализации данного метода.