МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №12**

**″Исследование стеганографического метода на основе преобразования наименее значащих бит ″**

Выполнила:

Cтудентка 3 курса 2 группы

Бобрик В.С.

Проверила: Копыток Д.В.

Минск 2021

**Цель**: изучение стеганографического метода осаждения/ извлечения тайной информации с использованием электронного файла-контейнера на основе преобразования наименее значащих бит (НЗБ), приобретение практических навыков программной реализации данного метода.

**Задачи**:

* Закрепить теоретические знания из области стеганографического преобразования информации, моделирования стеганосистем, классификации и сущности методов цифровой стеганографии.
* Изучить алгоритм осаждения/извлечения тайной информации на основе метода НЗБ (LSB – Least Significant Bit), получить опыт практической реализации метода.
* Разработать приложение для реализации алгоритма осаждения/ извлечения тайной информации с использованием электронного файла-контейнера на основе метода НЗБ.
* Познакомиться с методиками оценки стеганографической стойкости метода НЗБ.
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Теоретическая часть.**

Стеганографическая система – 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 стеганографии от криптографии: в первом случае тайной является сам факт наличия канала (передачи информации).

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; здесь речь может идти о невидимых цифровых водяных знаках, ЦВЗ);
* 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: один ключ отождествляется с методом осаждения/извлечения тайной информации, другой – с выбором элементов (например, битов) контейнера для его модификации при осаждении тайной информации, третий (или третьи) – для предварительного (перед осаждением) преобразования тайной информации (например, на основе помехоустойчивого кодирования, сжатия или зашифрования) и т. д.;
* контейнер с осажденным сообщением или стеганоконтейнер, S, который передается по открытому каналу, также являющемуся важным компонентом анализируемой системы; стеганоконтейнер будем именовать также стеганосообщением;
* отправитель и получатель.

Метод НЗБ основывается на ограниченных способностях зрения или слуха человека, вследствие чего людям тяжело различать незначительные вариации цвета или звука. Рассмотрим это на примере 24битного растрового RGB-изображения. Как известно, каждая точка кодируется 3-мя байтами. Каждый байт определяет интенсивность красного (Red), зеленого (Green) и синего (Blue) цветов. Совокупность интенсивностей цвета в каждом из 3-х каналов определяет оттенок пикселя. Младшие биты дают незначительный «вклад» в изображение по сравнению со старшими. Замена одного или даже нескольких младших бит для человеческого глаза будет почти незаметна, поскольку реально человек может различать около полторы сотни цветовых оттенков.

**Практическая часть.**

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

Реализация функции для размещения битового потока осаждаемого сообщения по содержимому контейнера представлена на рисунке 1.

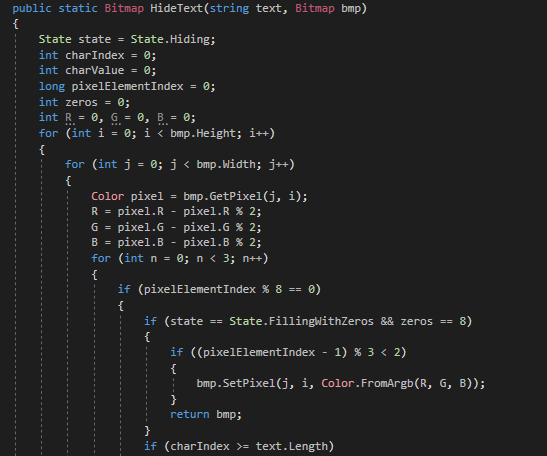


Рис. 1 – Функция для размещения битового потока осаждаемого сообщения по содержимому контейнера

На рисунке 2 представлен программный код функции для извлечения сообщения из стеганоконтейнера.

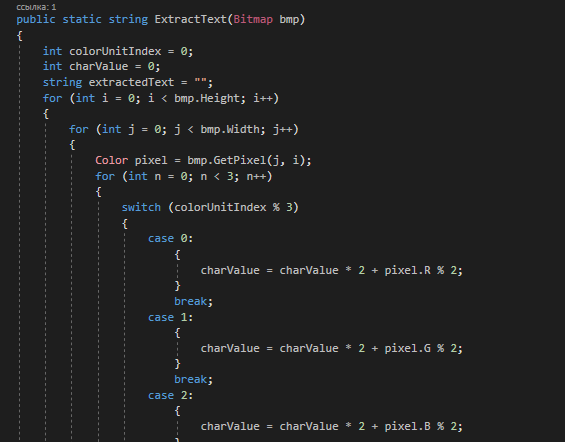


Рис. 2 – Функция для извлечения сообщения из стеганоконтейнера

Чтобы представить цветовую матрицу трех компонент в одном изображении, достаточно компоненту в пикселе, где НЗБ равен единице, заменить на 255, и в обратном случае заменить на 0.

Реализация функции для формирования цветовой матрицы, отображающей каждый задействованный для осаждения уровень младших значащих бит контейнера, представлена на рисунке 3.

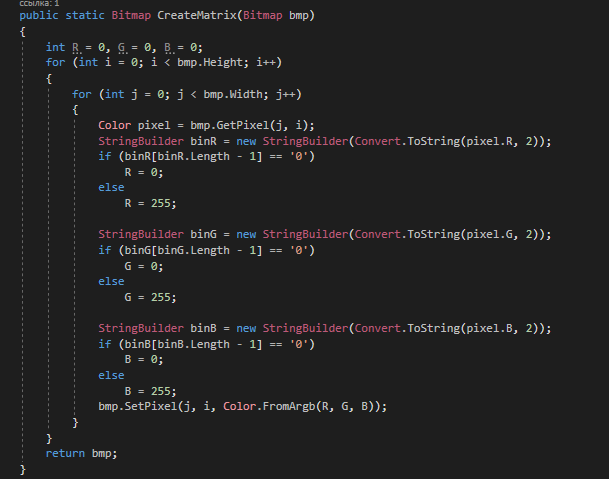


Рис. 3 – Функция для формирования цветовой матрицы

Интерфейс приложения, а также демонстрация размещения и извлечения сообщения представлены на рисунках 3 и 4.

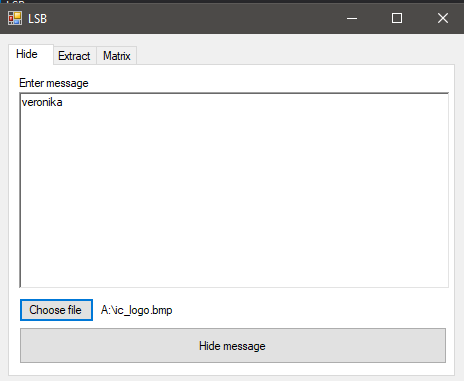


Рис. 3 – Вкладка для размещения осаждаемого сообщения

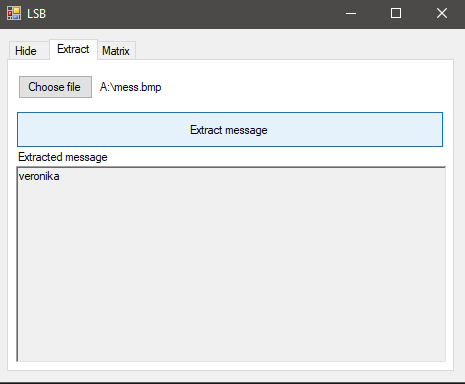


Рис. 4 – Вкладка для извлечения сообщения из стеганоконтейнера

На рисунке 5 представлена вкладка для формирования цветовой матрицы и результат в виде цветовой матрицы пустого контейнера.

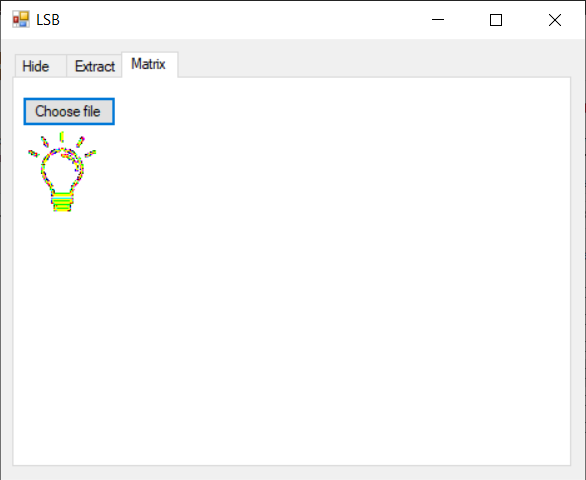


Рис. 5 – Вкладка для формирования цветовой матрицы

Пустой контейнер и контейнер с осажденным сообщением представлены на рисунке 6.



Рис. 6 – Слева расположен пустой контейнер, справа - стеганоконтейнер

Цветовые матрицы пустого контейнера и стеганоконтейнера продемонстрированы на рисунке 7.



Рис. 7 – Слева расположена цветовая матрица пустого контейнера, справа - стеганоконтейнера

Вывод: в результате данной лабораторной работы было разработано собственное приложение, в котором должен быть реализован метод НЗБ.