Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №14**

Студент: Бобрович Г.С.

ФИТ 3 курс 7 группа

Преподаватель: Савельева М.Г.

Минск 2023

**Разработать приложение для реализации алгоритма встраивания/извлечения тайной информации с использованием электронного файла-контейнера на основе метода НЗБ.**

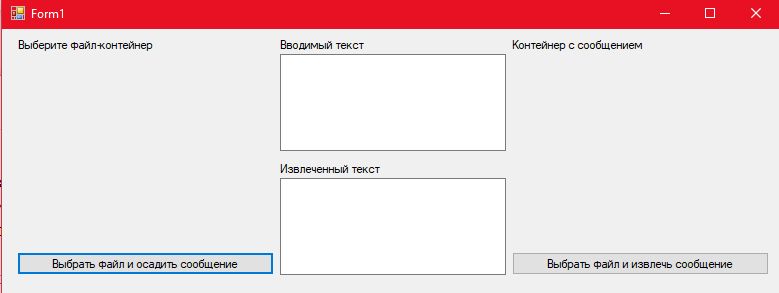
****

Рисунок 1.1 — Приложение

Проверим работоспособность приложения. Выберем файл-контейнер и осадим в нем сообщение:

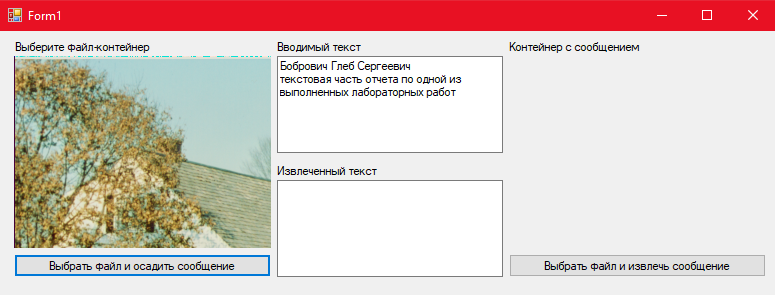


Рисунок 1.2 — Результат

Тут мы выбираем наш bmp-файл. Затем, необходимо выбрать файл с текстом. В моем случае, это файл с сообщением «Бобрович Глеб Сергеевич текстовая часть отчета по одной из выполненных лабораторных работ». Затем мы сохраняем новый файл с результатом. Попробуем его выбрать и извлечь из него сообщение:

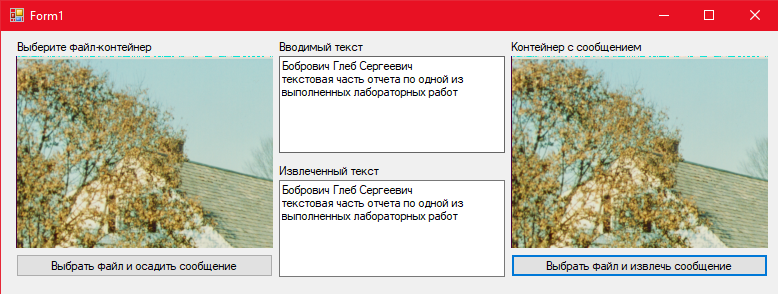


Рисунок 1.3 — Результат извлечения

Как видно, сообщения совпадают. Тут происходит извлечение осаженного раннее сообщения из нашего изображения.

Сформируем цветовые матрицы отображающие пиксели, с помощью сторонних приложений. На рисунках 1.4 и 1.5 показаны пустой контейнер и осаженный.

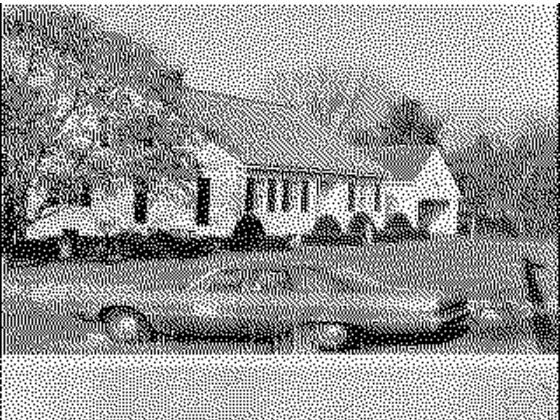


Рисунок 1.4 — Пустой контейнер



Рисунок 1.5 — Контейнер с сообщением

Визуальный анализ двух контейнеров представлен на рисунках 1.6 и 1.7

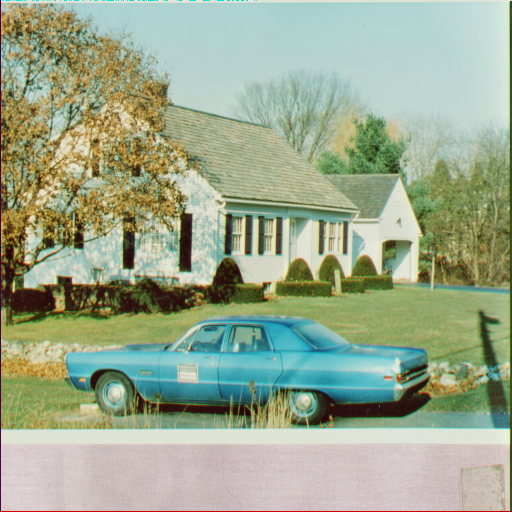


Рисунок 1.6 — Пустой контейнер

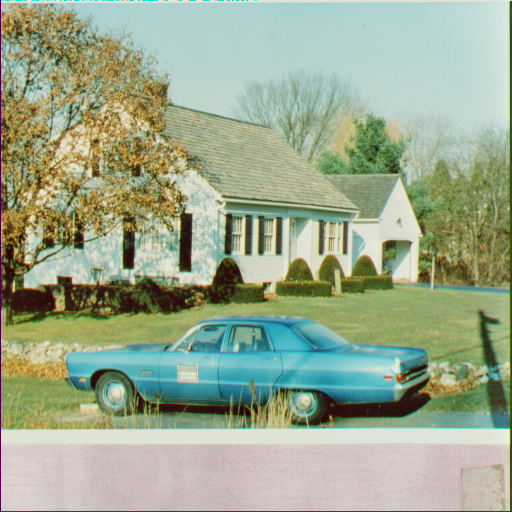


Рисунок 1.7 — Контейнер с сообщением

Как видно, никаких визуальных отличий не наблюдается. Два изображения кажутся идентичными, однако если мы воспользуемся дополнительными инструментами (составим цветовую матрицу изображений), то отличия станут заметны.

Также, необходимо было реализовать два метода размещения битов в контейнере. Был выбран метод размещения по строкам и метод размещения по столбцам. Программная реализация показана на картинках 1.8 и 1.9

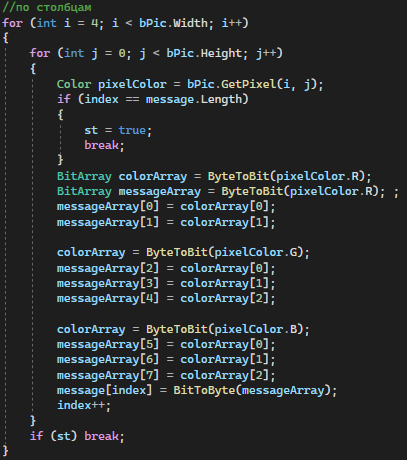


Рисунок 1.8 — Метод размещения по столбцам

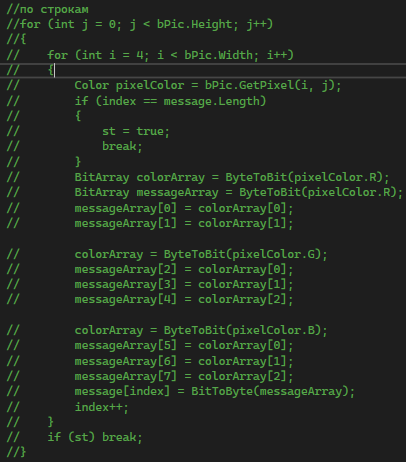


Рисунок 1.9 — Метод размещения по строкам

**Вывод**

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