Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование стеганографического метода на основе  
преобразования наименее значащих бит

Студент: Чистякова Ю.А.

ФИТ 3 курс 5 группа

Преподаватель: Берников В.О.

Минск 2020

## 1. Описание приложения

Приложение написано на языке программирования C# и реализует метод НЗБ. При этом:

* использован файл-контейнер формата bmp;
* реализовано 2 варианта осаждаемого/извлекаемого сообщения: собственные ФИО и текстовая часть отчета по одной из лабораторных работ;
* выполнен визуальный анализ (с привлечением одногруппников в качестве экспертов) стеганоконтейнеров с различных внутренним содержанием; сделаны выводы на основе выполненного анализа.

## 2. Методика выполнения поставленных задач

В данной лабораторной работе в качестве стеганоконтейнера выбрано изображение формата \*.bmp по следующим причинам:

* в него можно внедрить большой объем данных;
* заранее известен размер контейнера (у нас 1024х768);
* есть текстурные области, у которых есть шумовая текстура – в нее легко встроить информацию;
* человеческий глаз слабо чувствителен к небольшим изменениям изображения (яркость, контрастность);
* разработаны хорошие методы цифровой обработки изображений.

Был использован метод НЗБ (наименее значащий бит), его суть заключается в замене последних значащих битов в контейнере на биты скрываемого сообщения.

Рассмотрим процесс сокрытия битов в разработанном приложении. При первоначальном запуске пользователю откроется окно, представленное на рисунке 2.1.

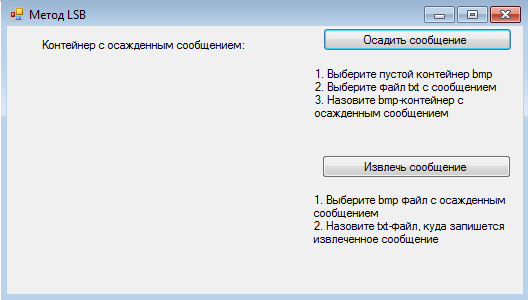


Рис. 2.1 – Окно приложения

Пользователю предоставлены 2 кнопки. При нажатии на кнопку «Осадить сообщение» откроется диалоговое окно для выбора файла-контейнера С с фильтром файлов формата bmp.

После выбора изображения и нажатия кнопки «ОК» пользователю откроется еще одно диалоговое окно для выбора текстового файла с фильтром формата txt. В данном текстовом файле и распологается тайное сообщение М, которое мы хотим осадить в выбранном контейнере.

На этом шаге происходит проверка, поместится ли исходный текст тайного сообщения в выбранной нами картинке. Для этого проверяем, чтобы количество байтов в текстовом файле не превышало размера картинки – длина х ширина.

Затем произойдет проверка: может быть картинка уже зашифрована. Для этого получаем байт символа, записанного в первом пикселе: если он равен ‘/’, значит файл уже зашифрован. Иначе переходим на следующий шаг.

Далее откроется диалоговое окно для сохранения файла-стеганоконтейнера. Там будет хранится модифицированное изображение с уже осажденным сообщением.

Нажмем на кнопку «Осадить сообщение» и выберем все необходимые файлы. В окне приложения откроется выбранный контейнер, представленный на рисунке 2.2.

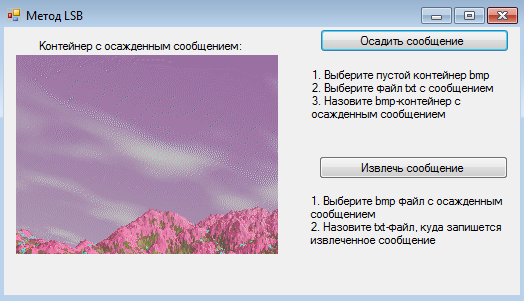


Рис. 2.2 – Стеганоконтейнер сформирован

Рассмотрим, как происходит осаждение тайного сообщения в контейнере. Сначала в первый пиксель (0.0) контейнера мы помещаем символ ‘/’, который говорит о том что картинка зашифрована.

Далее записываем количество символов для шифрования в первые биты картинки. В соответствии с этим будут получены новые цвета первых пикселей, которые будут записаны в картинку. Реализация функции, осуществляющей запись количества символов для шифрования в первые биты картинки, представлена на рисунке 2.3.

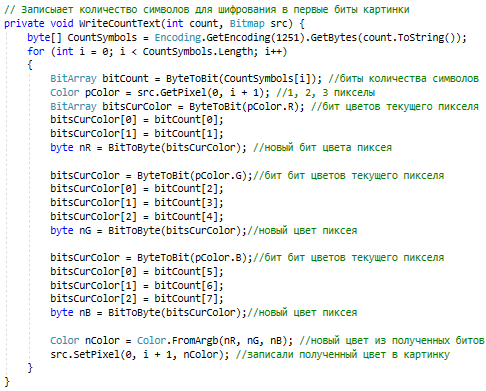


Рис. 2.3 – Запись количества символов

Далее собственно записываем информацию в стеганоконейнер по тому же принципу.

На рисунке 2.4 представлены пустой контейнер и стеганоконтейнер, в котором осаждено сообщение с ФИО студента. Как и следовало ожидать, человеческому глазу не удалось выявить никакой разницы в цвете, яркости, контрастности изображений.

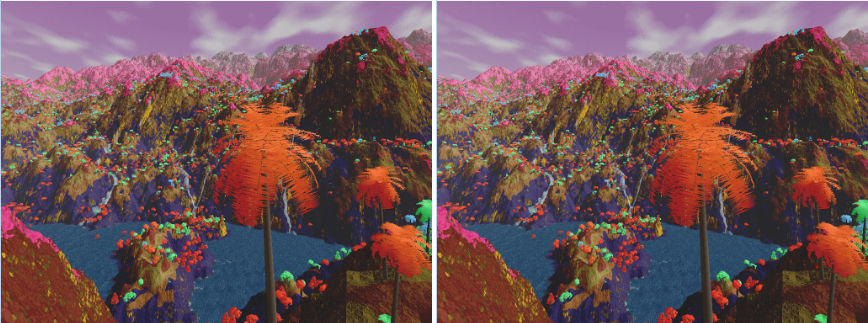


Рис. 2.4 – Пустой контейнер и стеганосообщение

Далее рассмотрим извлечение тайного сообщения из стеганоконтейнера. Для этого нажмем кнопку «Извлечь сообщение».

Откроется диалоговое окно для выбора файла-стеганоконтейнера с фильтром bmp-изображений. Произойдет проверка равенства символа в первом пикселе ‘/’, описанная ранее.

Если проверка выполнена, ПС считает количество зашифрованных символов из первых бит картинки.

Далее откроется диалоговое окно для сохранения извлеченного тайного сообщения в текстовый файл.

На рисунке 2.5 продемонстрированы исходный файл и файл с извлеченным тайным сообщением. Нетрудно заметить, что текст идентичен.

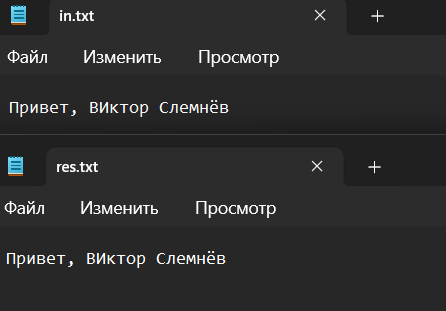


Рис 2.5 – Осажденное/извлеченное сообщение

Реализация алгоритма, осуществляющего чтение сообщения из стеганоконтейнера, представлена на рисунке 2.6.

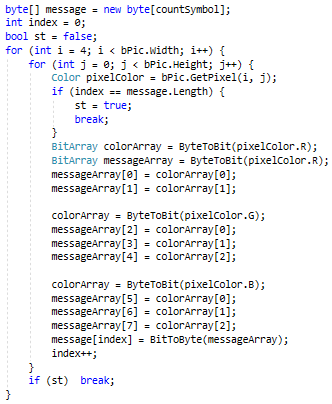


Рис. 2.6 – Чтение текста из стеганосообщения

## Вывод

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