МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных Технологий

Кафедра Информационных систем и технологий

Специальность 1-40 01 01 Программное обеспечение информационных технологий

Направление специальности 1-40 01 01 10 Программирование интернет-приложений

**ОТЧЁТ К ЛАБОРАТОРНОЙ РАБОТЕ №14:**

по дисциплине «Криптографические методы защиты информации»

Исполнитель

студентка 3 курса группы 5 Шкода Кристина Михайловна

(Ф.И.О.)

Руководитель работы преподаватель Савельева М. Г.

(учен. степень, звание, должность, подпись, Ф.И.О.)

Минск 2023

**Исследование стенографического метода на основе преобразования наименее значащих бит**

**Цель**: изучение стенографического 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 стенографического 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 стенографической стойкости метода НЗБ.
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Теория.** Стенографическая 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).

Синхронные потоковые шифры (СПШ) характеризуются тем поток ключей генерируется независимо от открытого текста и шифртекста. Главное свойство СПШ – нераспространение ошибок. Ошибки отсутствуют, пока работают синхронно шифровальное и дешифровальное устройства отправителя и получателя информации. Один из методов борьбы с рассинхронизацией – разбить отрытый текст на отрезки, начало и конец которых выделить вставкой контрольных меток (специальных маркеров).

Абстрактно стенографическая 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; 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.

В зависимости от формата документа-контейнера цифровую (или компьютерную) стеганографию подразделяют на классы:

* аудиостеганография,
* видеостеганография,
* графическая стеганография,
* текстовая стеганография и др.

Синхронные потоковые шифры уязвимы к атакам на основе изменения отдельных бит шифртекста. В самосинхронизирующихся потоковых шифрах символы ключевой гаммы зависят от исходного секретного ключа шифра и от конечного числа последних знаков зашифрованного текста. Основная идея заключается в том, что внутреннее состояние генератора потока ключей является функцией фиксированного числа предыдущих битов шифртекста. Поэтому генератор потока ключей на приемной стороне, приняв фиксированное число битов, автоматически синхронизируется с генератором гаммы. Недостаток этих потоковых шифров – распространение ошибок, так как искажение одного бита в процессе передачи шифртекста приведет к искажению нескольких битов гаммы и, соответственно, расшифрованного сообщения.

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.

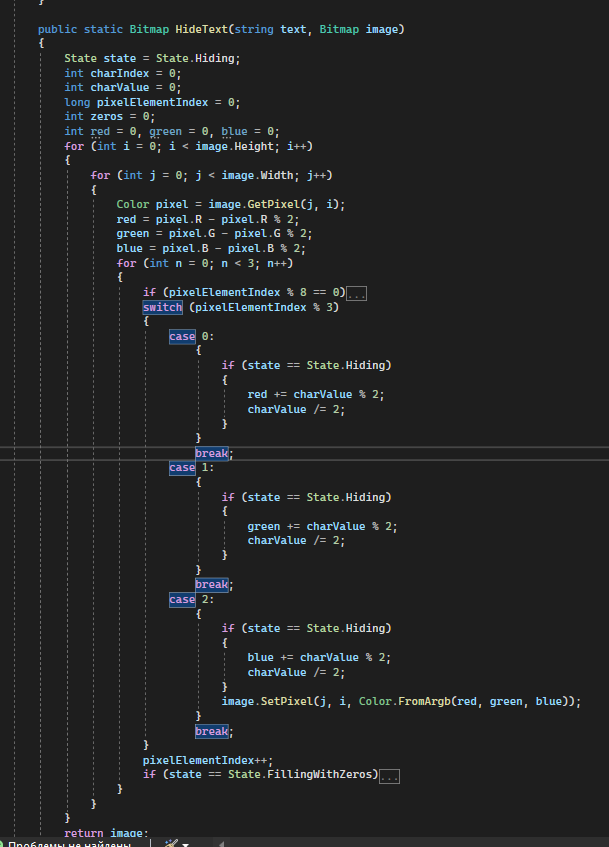


Рисунок 1 – Функция для размещения битового потока осаждаемого сообщения по содержимому контейнера

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



Рисунок 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.

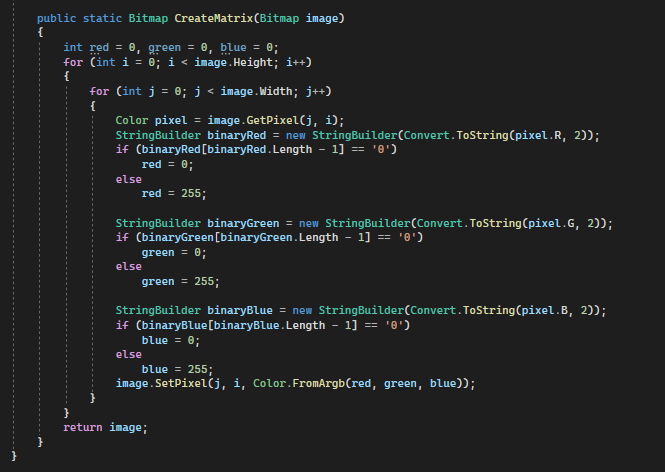


Рисунок 3 – Функция для формирования цветовой матрицы

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

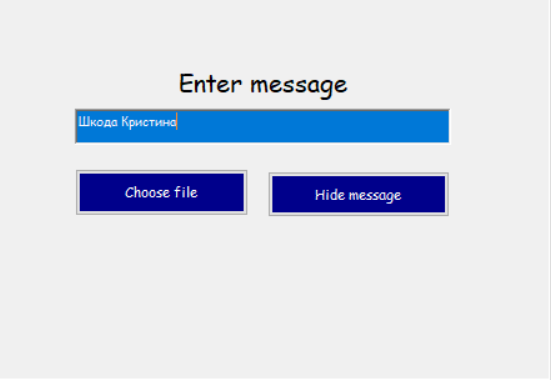


Рисунок 3 – Вкладка для размещения осаждаемого сообщения

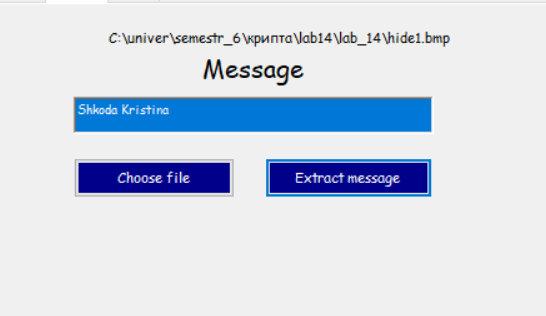


Рисунок 4 – Вкладка для извлечения сообщения из стеганоконтейнера

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

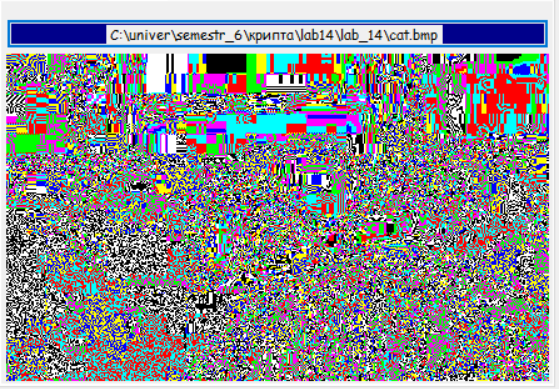


Рисунок 5 – Вкладка для формирования цветовой матрицы

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



Рисунок 6 – Слева расположен пустой контейнер, справа - стеганоконтейнер

Цветовые матрицы пустого контейнера и стеганоконтейнера продемонстрированы на рисунке 7.

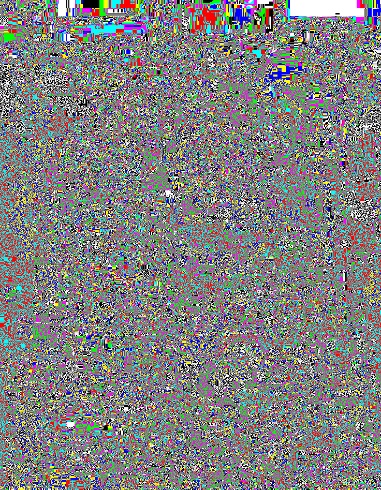


Рисунок 7 – Слева расположена цветовая матрица пустого контейнера, справа - стеганоконтейнера

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