Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Криптографические методы защиты информации

Студент: Сенченя В.И.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М. Г.

Минск 2023

**Лабораторная работа №15**

**Тема «****исследование методов текстовой стеганографии»**

Цель: изучение стеганографических методов встраивания/извлечения тайной информации с использованием электронного файла-контейнера текстового формата, приобретение практических навыков программной реализации методов.

Задачи:

1. Закрепить теоретические знания из области текстовой стеганографии, классификации, моделирования стеганосистем подобного вида и сущности основных методов.
2. Изучить основные алгоритмы встраивания/извлечения тайной информации на основе методов текстовой стеганографии, получить опыт практической реализации методов.
3. Разработать приложение для реализации алгоритмов встраивания/извлечения тайной информации на основе методов текстовой стеганографии.
4. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Модификация количества пробелов между словами**

Основан на модифицировании количества пробелов между словами. В моём случае сообщение разбивается на биты и потом сообщение записывается следующим образом: 1 преобразуется в два пробела 0 в один.

Код внедрения текста в текст предоставлен на рисунке 1.1, а код для извлечения на рисунке 1.2.

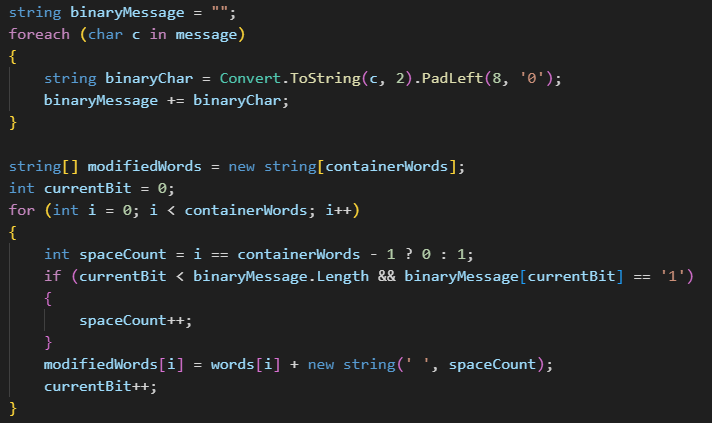


Рисунок 1.1 – Код внедрения текста

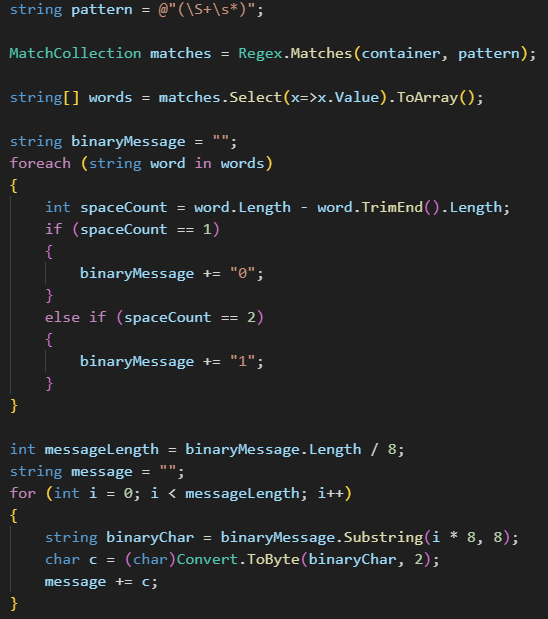


Рисунок 1.2 – код извлечения текста

Также на рисунке 1.3 предоставлен пример преобразованного текста с заменённым пробелами на спец. символ для наглядности.

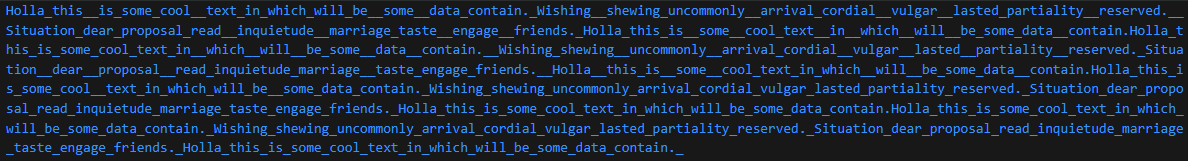


Рисунок 1.3 – Результат внедрения текста

На рисунке 1.4 показан полученный текст после извлечения из текста.



Рисунок 1.4 – Извлечённый текст

Используя метод модификации количества пробелов между словами можно почти сразу заметить, что текст был как-то модифицирован. Мною была использована самая простая версия данного метода, в усложнённых версиях пробелы могут стоять в разных местах либо для записи одного бита используется некоторая последовательность из пробелов разной длины.

**Sword**

На рисунке 1.5 изображён программный интерфейс.

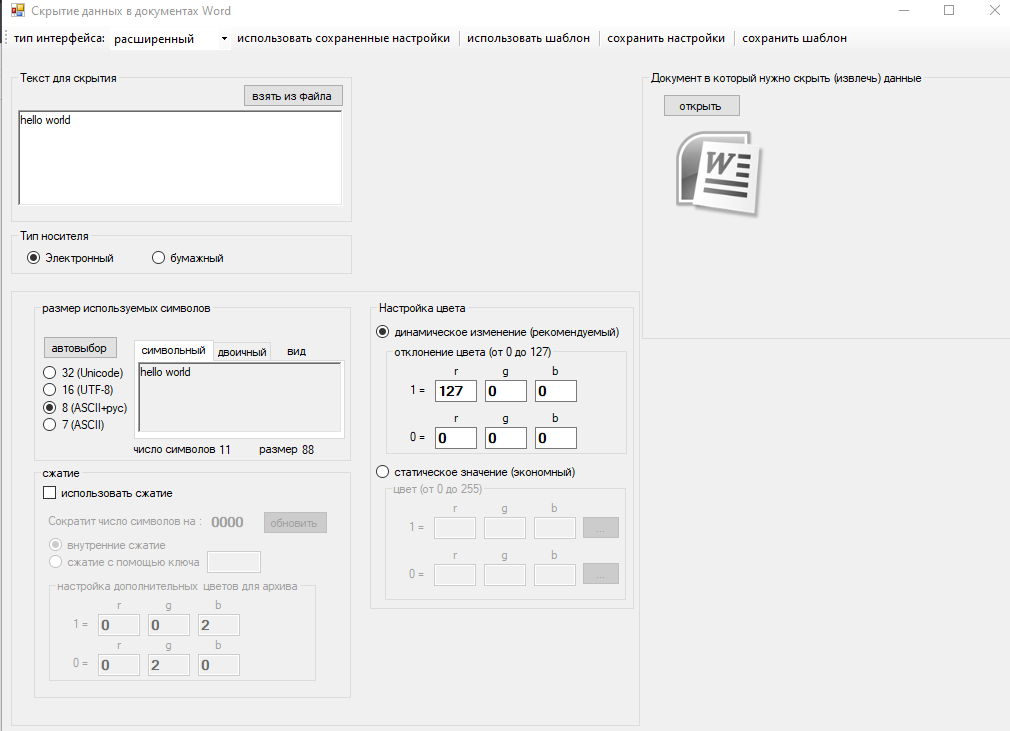


Рисунок – 1.5 – Интерфейс

На рисунке 1.6 изображён исходный текст

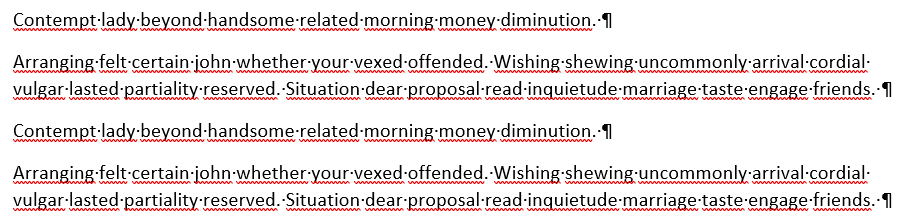


Рисунок 1.6 – Исходный текст

На рисунке 1.7 изображен текст, в которой было внедрено сообщение, при этом использовалось минимальное отклонение текста (0,0,1;0,0,0).

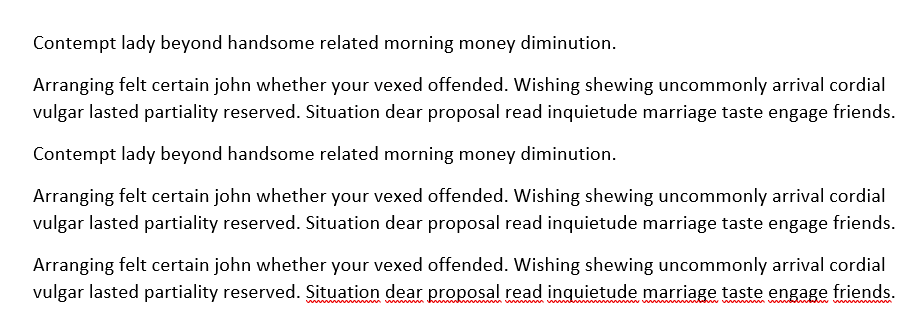


Рисунок 1.7 – Модифицированный текст

Как мы видим, в модифицированном тексте невозможно заметить разницу, поэтому отметим изменённые символы функцией в программе. Отмеченный текст показан на рисунке 1.8

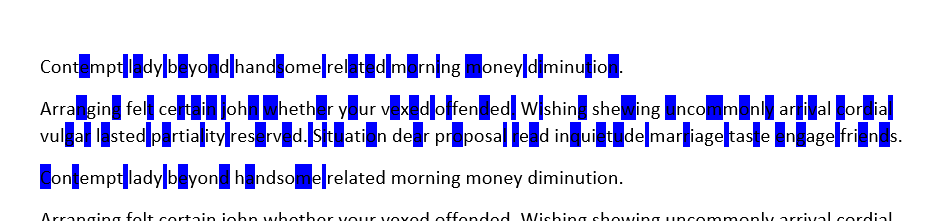


Рисунок 1.8 – Отмеченный текст

Теперь изменим параметр отклонения цвета на более значимый (127,0,0; 0,0,1). На рисунке 1.9 показан результат.

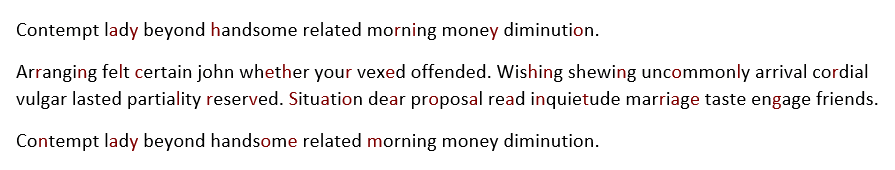


Рисунок 1.9 – Результат сокрытия

При использовании программы важно знать, что изменение параметров цвета не влияет на размер исходного сообщения, нужного для шифрования, влияет только текст для скрытия и размеры используемых символов(кодировка). *ASCII* использует 7 бит для сокрытия 1 символа, *ASCII* с рус. Символами 8 бит, *UTF*-8 и *Unicode* используют 16 бит

**Вывод**

В ходе выполнения лабораторной работы я приобрёл и закрепил навыки практические навыки разработки приложения для реализации стеганографических методов встраивания/извлечения тайной информации с использованием электронного файла-контейнера текстового формата.