МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №13**

**«ИССЛЕДОВАНИЕ МЕТОДОВ**

**ТЕКСТОВОЙ СТЕГАНОГРАФИИ»**

Выполнила:

Cтудентка 3 курса 2 группы

Бобрик В.С.

Проверила: Копыток Д.В.

Минск 2021

Цель: изучение стеганографических методов встраивания/извлечения тайной информации с использованием электронного файла-контейнера текстового формата, приобретение практических навыков программной реализации методов (рассчитана на 4 часа аудиторных занятий: 2 часа – часть 1, 2 часа – часть 2).

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. Познакомиться с методиками оценки стеганографической стойкости методов.

5. Результаты выполнения лабораторной работы (отдельно по каждой из 2 частей) оформить в виде описания разработанного приложения (для части 2), методики выполнения экспериментов с использованием приложений и результатов экспериментов.

**1.Теоретическая часть.**

Многообразие методов текстовой стеганографии подразделяется на синтаксические методы, которые не затрагивают семантику текстового сообщения, и лингвистические, которые основаны на эквивалентной трансформации текстовых файлов-контейнеров, сохраняющей смысловое содержание текста, его семантику.

К синтаксическим методам компьютерной стеганографии, которые характеризуются сравнительно невысокой эффективностью(с точки зрения объема встраиваемой информации), относятся следующие (такие методы мы отнесем к числу базовых синтаксических методов):

* метод изменения межстрочных интервалов
* изменение расстояния между словами
* изменение количества пробелов между словами
* на основе внесения специфических изменений в шрифты
* изменение интервала табуляции
* Null Chipper
* увеличение длины строки
* использование регистра букв
* использование невидимых символов

Существуют также стеганографические методы, которые интерпретируют текст как двоичное изображение. Необходимо отметить,что данные методы нечувствительны к изменению масштаба документа, что обеспечивает им хорошую устойчивость к большинству искажений, которые могут иметь место при активных атаках.

К числу основных лингвистических методов относятся:

* метод синонимов
* метод переменной длины слова
* метод первой буквы
* мимикрия

**Метод на основе апроша**

Апрош определяет расстояние между соседними символами текста. Фактически апрош состоит из двух таких расстояний – полуапрошей, являющихся как бы пространством, прилегающим к каждому из символов-соседей.Согласно существующим техническим правилам набора нормальный апрош должен быть равен половине кегля (размера) шрифта.

Идея метода заключается в следующем. Встраивание сообщения в контейнер может быть основано на модификации базового (устанавливаемого текстовым процессором по умолчанию) значения апроша, его изменением от базового до некоторого максимального, которое зрительно не должно отличаться от стандартного. Такое изменение производится с определенным шагом (дискретно), каждому значению которого присваивается определенный бит или определенная комбинация битов.

**Метод на основе кернинга**

В текстовых документах встречаются такие сочетания знаков,которые образовывают визуальные «дыры» либо «сгущения».Например, в текстах на основе кириллицы – это такие сочетания:«ГА», «TA», «ATA», «ЬТ» и т. п., на основе латиницы – «AY»,«AV», «T;», «ff», а на основе греческого алфавита – «ΘΑ», «ΔΟ»,«λκ» и др. Такие сочетания называются кернинговыми парами. Особенности «кернингования» приведены на рис. 13.6. Под кернингом обычно понимается процесс изменения межсимвольного расстояние между отдельными парами символов или кернинговыми парами (именно фактор парности отличает кернинг от апроша).

**Практическая часть.**

Разработать авторское приложение, реализующее один из методов текстовой стеганографии на основе модификации пространственно-геометрических параметров текста-контейнера. Реализация функции модификации числа пробелов представлена на рисунке 1.

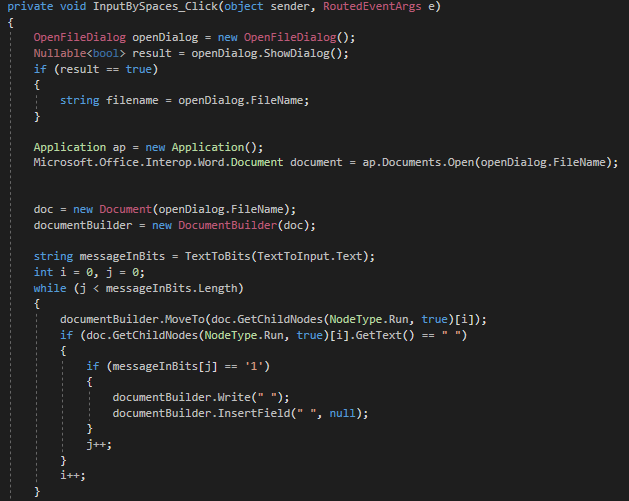


Рис. 1 – Функция модификации числа пробелов

На рисунке 2 представлена реализация модификации апроша.

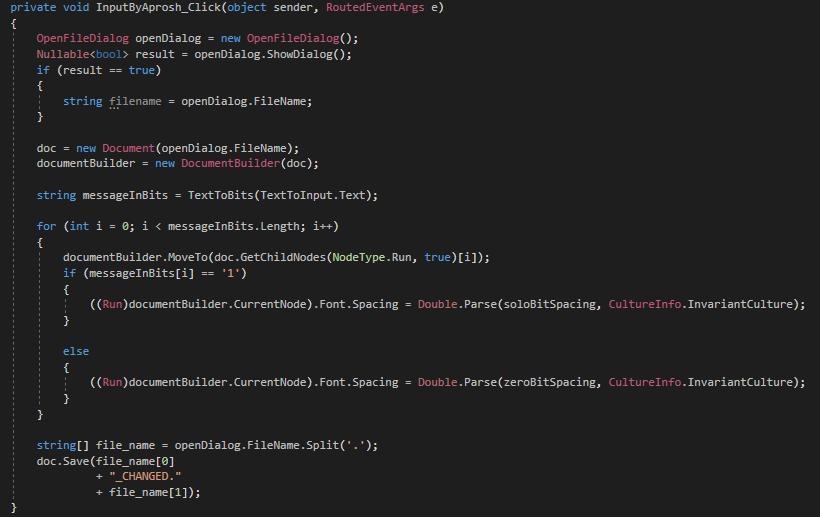
.

Рис. 2 – Функция модификации апроша

Результат выполнения модификации Апроша представлен на рисунке 3.

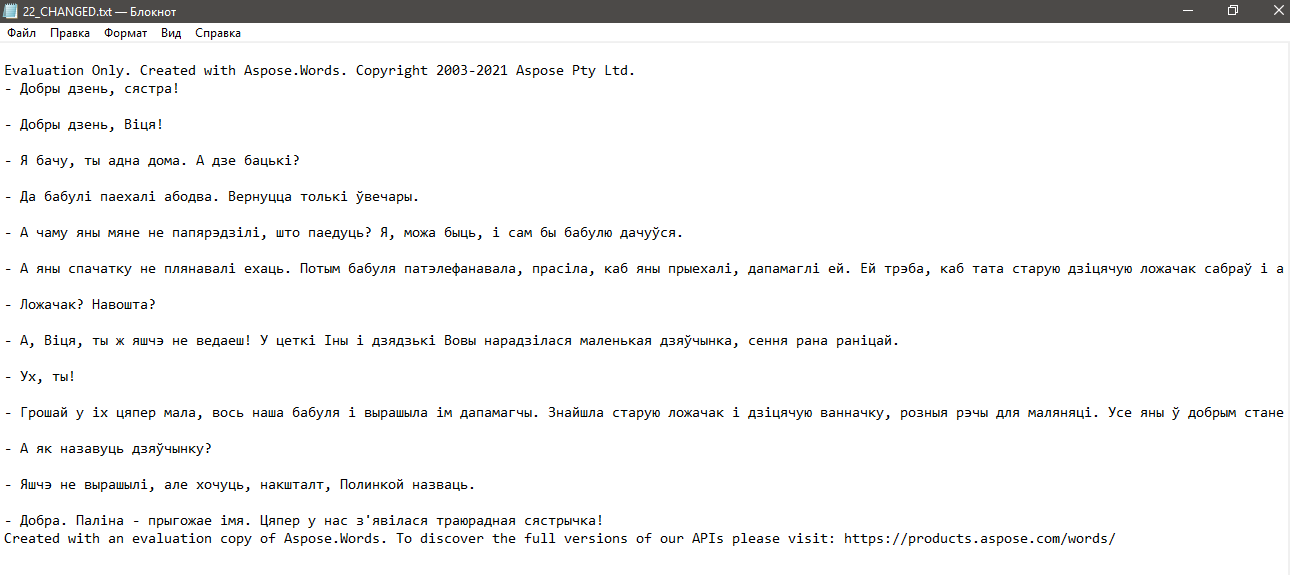


Рис. 3 – Результат модификации Апроша

Вывод: в результате данной лабораторной работы было разработано собственное приложение, в котором были реализованы методы модификации пробелов и Апроша.