Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование методов текстовой стеганографии

Студент: Шулаков А.А.

ФИТ 3 курс 5 группа

Преподаватель:

Савельева М. Г.

Минск 2023

1. **Описание приложения**

Приложение написано на языке программирования C# и позволяет выполнить и реализовывать метод стеганографии.

1. **Методика выполнения поставленных задач**

Был использован метод на основе апроша.

Метод апроша (или метод приближения) - это техника в типографии, которая используется для коррекции пробелов между символами в тексте. Этот метод основан на приближенной оценке оптимальных пробелов между символами на основе контекста и формы символов. В процессе апроша, интервалы между символами рассчитываются с учетом их формы и взаимодействия с соседними символами, чтобы достичь более равномерного и гармоничного расстояния. Апрош является эффективным инструментом для тонкой настройки визуального восприятия текста, особенно в случаях, когда стандартные методы кернинга не дают достаточного результата. Правильное применение метода апроша позволяет улучшить читабельность и эстетику текстового контента, создавая более гармоничное и приятное визуальное впечатление.

На рисунке 2.1. изображено то, как берется сообщение и зашифровывается, на рисунке 2.2 уже расшифровка. Путь к различным файлам уже прописан в коде

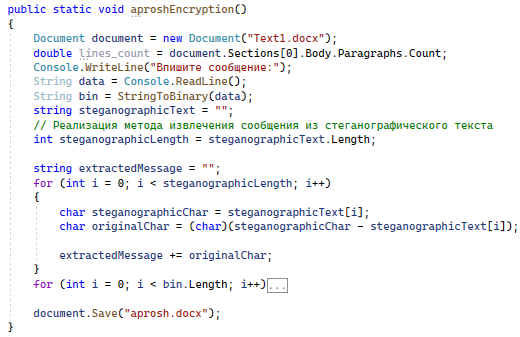


Рис. 2.1 – Функция зашифровки

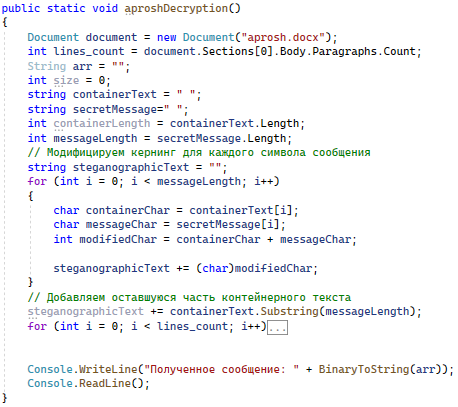


Рис. 2.2 – Функция расшифровки

Результат работы приложения представлен на рисунке 2.3.

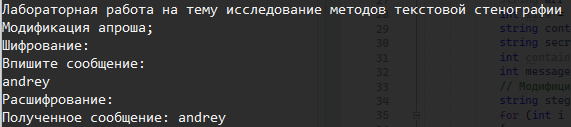


Рис. 2.3 – Результат работы приложения

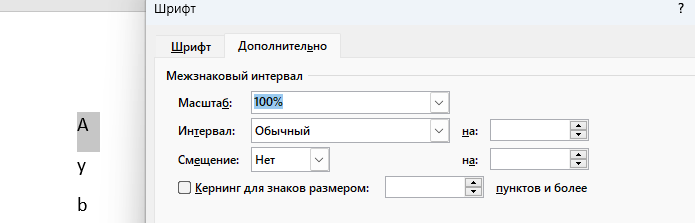


Рис. 2.4 – Шрифт исходного документа

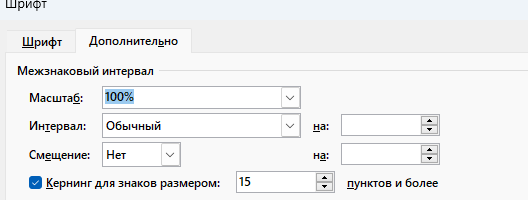


Рис. 2.5 – Шрифт документа с тайным сообщением

Рассмотрим, приложение Sword. Оно изображено на рисунке 2.6. В нем уже есть сообщение, которое мы хотим осадить. На рисунке 2.7 изображен процесс осаждения сообщения в файл Text1.txt.

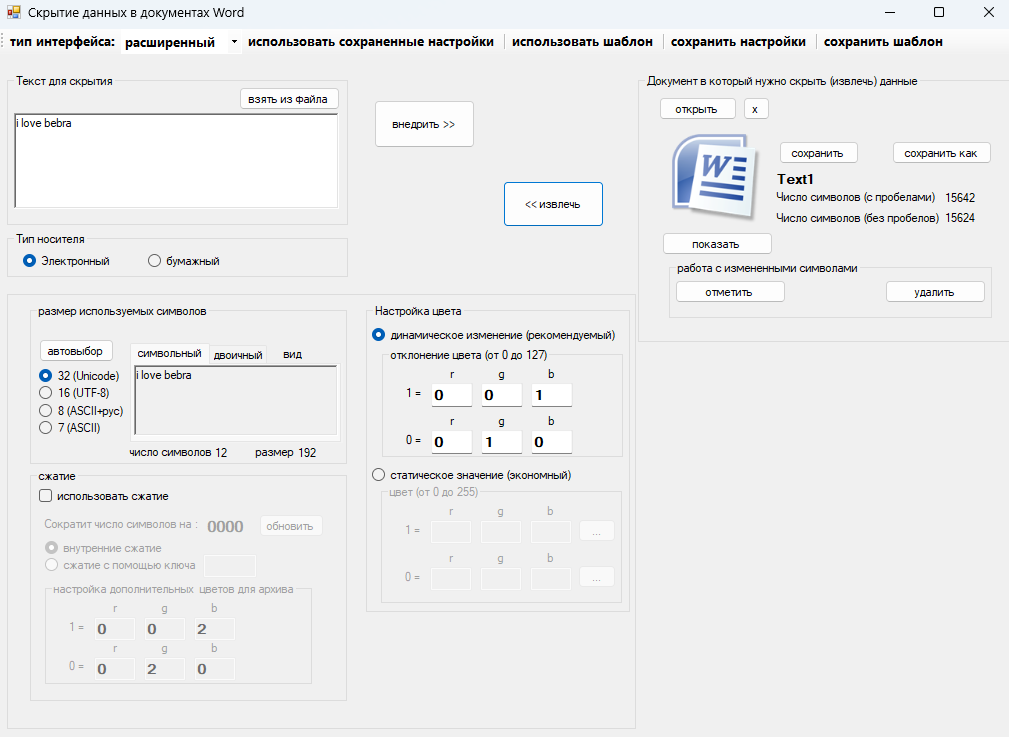


Рис. 2.6 – Приложение Sword

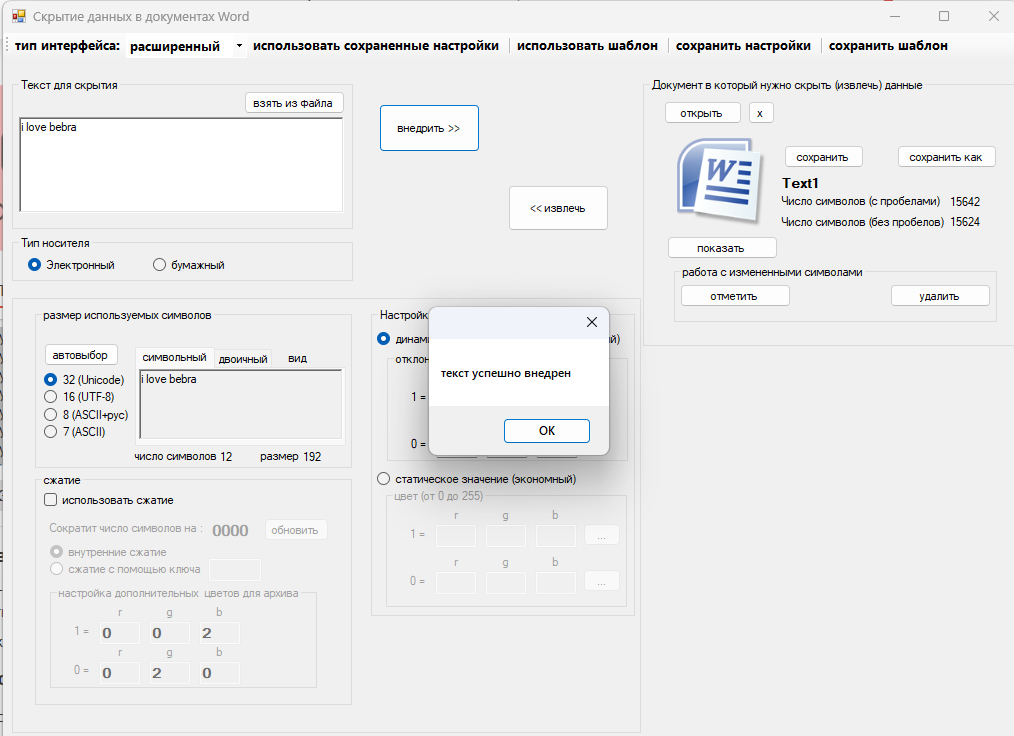


Рис. 2.7 – Осаждение сообщения с помощью Sword

На рисунке 2.8 мы делаем расшифрование сообщения из нашего файла. На рисунке 2.9 уже видно и уведомление, и само расшифрованное сообщение.

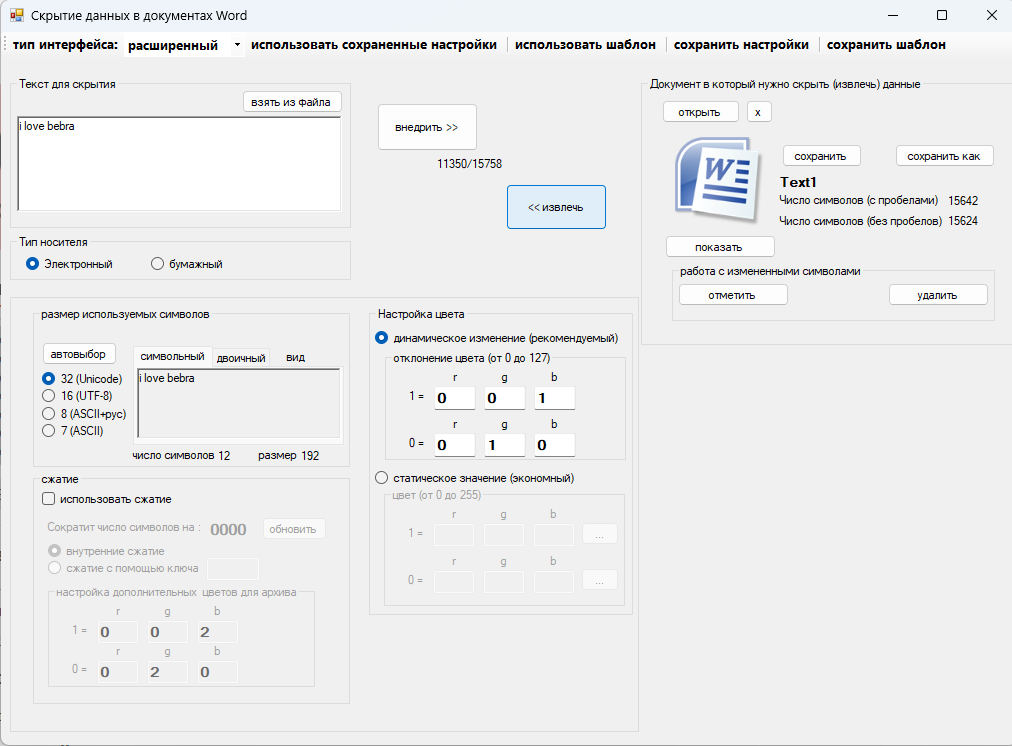


Рис. 2.8 – Извлечения сообщения с помощью Sword

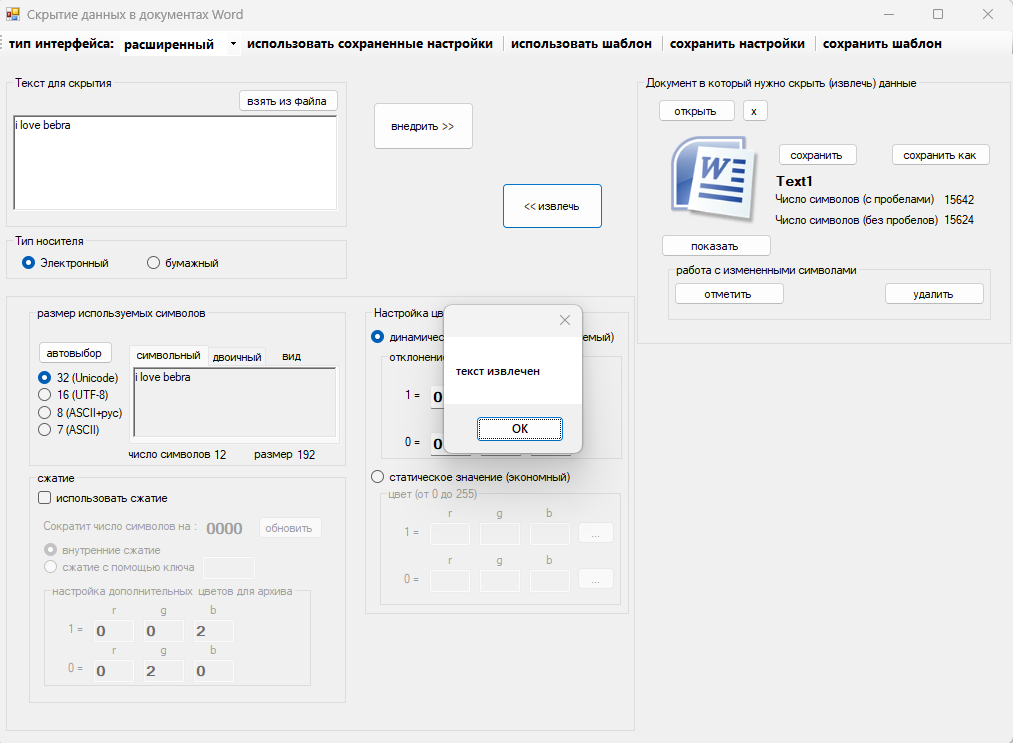


Рис. 2.9 – Извлеченное сообщение

Пример Word документа со скрытым сообщением на рисунке 2.10:

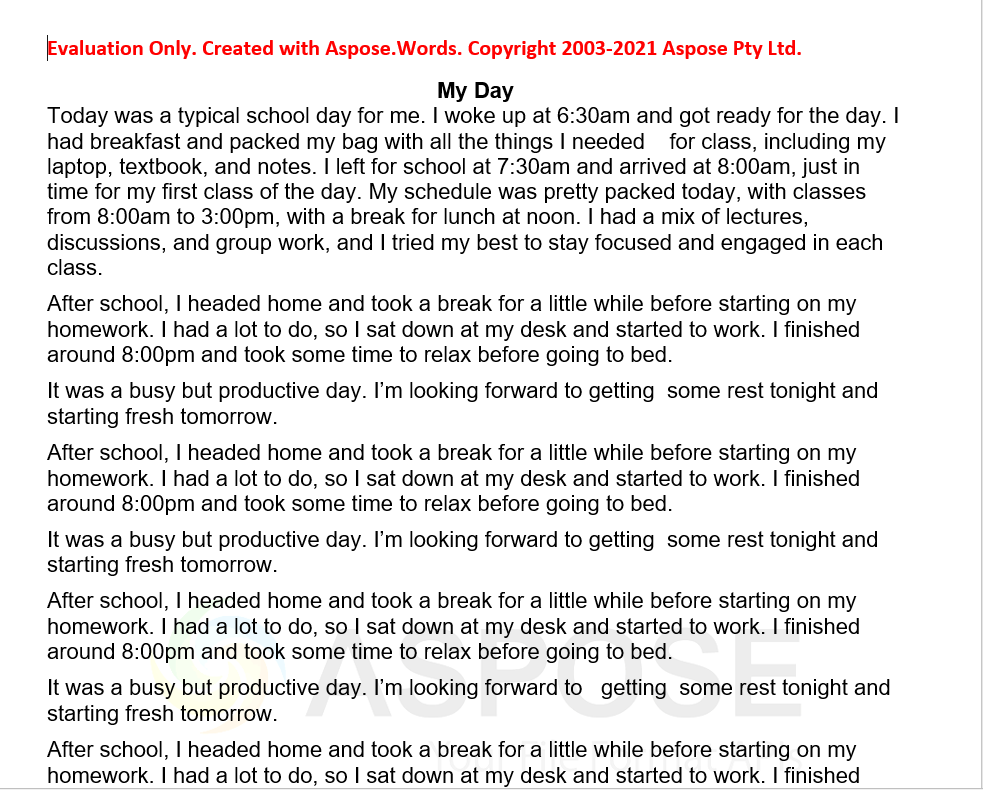


Рис. 2.10 – Документ с скрытым сообщением

**Вывод**

В ходе лабораторной работы мы получили практические навыки в программной реализации стеганографического метода осаждения и извлечения тайной информации с использованием текстовой стеганографии. Мы изучили принципы работы этого метода и применили его на практике.

При осаждении тайной информации мы успешно внедрили скрытые данные в текстовый контейнер, таким образом, обеспечивая конфиденциальность и незаметность передачи секретной информации. Мы ознакомились с различными методами встраивания данных в текст, такими как замена пробелов, добавление лишних символов или использование специальных шаблонов.

При извлечении тайной информации мы успешно восстановили скрытые данные из текстового контейнера, используя знание о методе и особых признаках, по которым можно определить наличие скрытой информации. Мы научились извлекать данные без искажения и потери информации, чтобы получить исходное секретное сообщение.

Эти практические навыки открывают перед нами возможности для решения различных задач в области информационной безопасности и коммуникации. Мы осознали важность стеганографии как инструмента для обеспечения конфиденциальности и скрытной передачи информации, а также ознакомились с ее применением в реальных сценариях и задачах. Эти навыки будут полезны в нашей дальнейшей работе и исследованиях в области информационной безопасности.