Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПОДСТАНОВКИ (ЗАМЕНЫ) СИМВОЛОВ

Студент: Точило О. В.

ФИТ 3 курс 4 группа

Преподаватель: Сазонова Д. В.

Минск 2024

# **Текстовая стеганография**

К текстовой стеганографии относятся методы, предусматривающие использование в качестве контейнера файла-документа текстового типа. 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:

* изменение расстояния между строками электронного текста;
* изменение расстояния между словами в одной строке электронного текста;
* изменение количества пробелов между словами;
* на основе внесения специфических изменений в шрифты;
* изменение интервала табуляции;
* Null Chipper (несуществующий, нулевой лепет);
* 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.

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

# **Программное средство «Sword»**

Программное средство «Sword», используемое для внедрения текста в документы, имеет интерфейс, предсталвенный на рисунке 1.1.

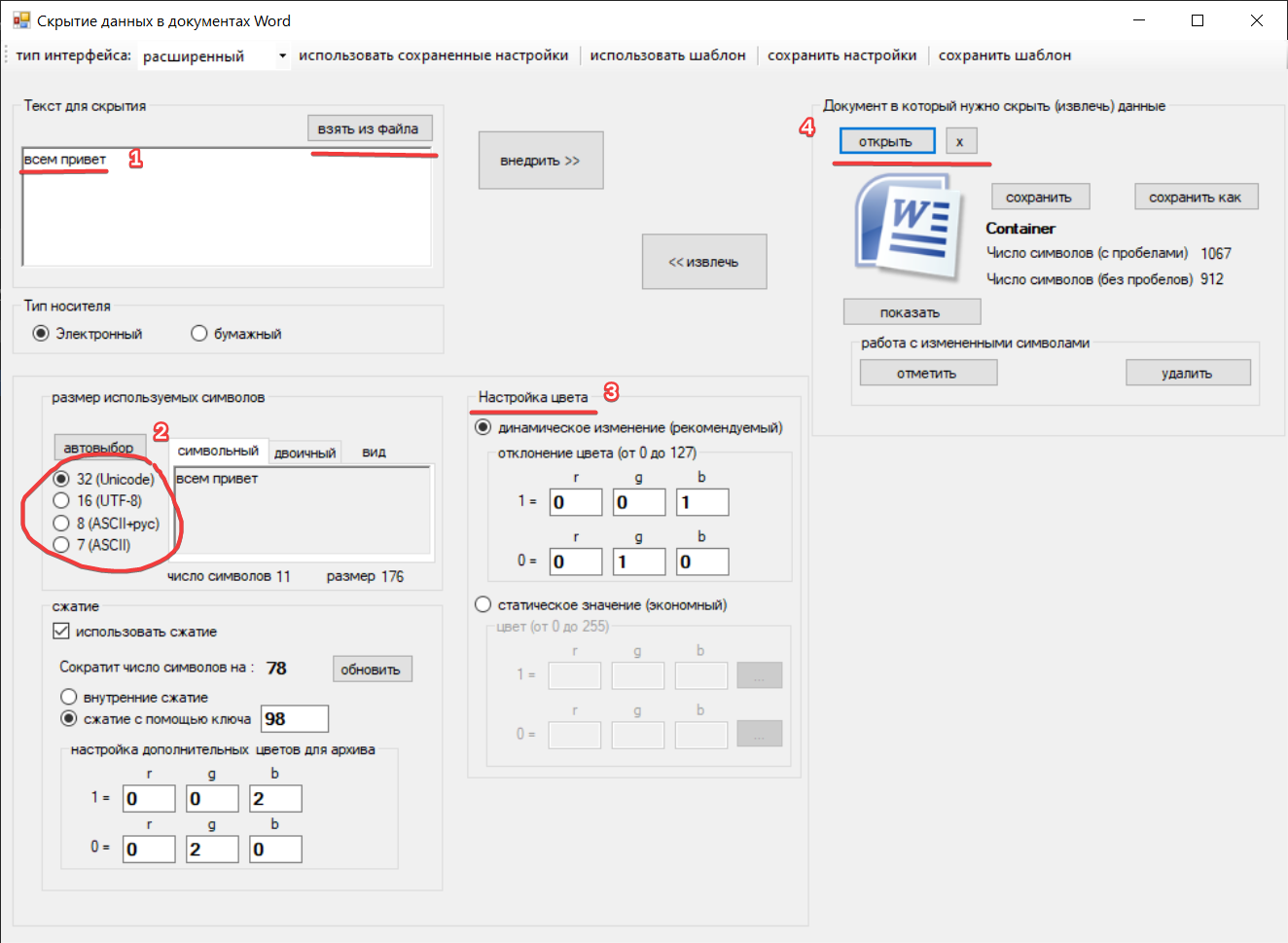


Рисунок 1.1 – Интерфейс программного средства «Sword»

На данном рисунке цифрой 1 обозначен встраиваемый текст, который можно также считать из электронного документа, цифрой 2 – возможности кодировки исходного текста в различных кодировках, цифрой 3 – создание самого ключа, то есть выбор, на сколько битов красного, зеленого и синего цвета будет изменяться наименее значащий бит для внедрения сообщения, цифрой 4 – кнопка для выбора документа-контейнера, в котором будет встроено сообщение.

Сообщения встраиваются с помощью изменения цвета букв документа-контейнера. Обе стороны должны знать, какие настройки изменения цвета используются.

Для внедрения текста в контейнер необходимо нажать кнопку «Внедрить». Результатом успешного внедрения является сообщение, представленное на рсиунке 1.2.

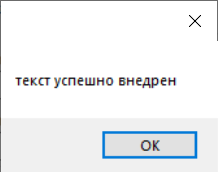


Рисунок 1.2 – Успешное внедрение текста

Нажатием на кнопки «Показать» и «Отметить» можно открыть документ-контейнер, в котором синим выделением будут отмечены буквы, в которые было встроено сообщение. Документ со встроенным сообщением изображен на рисунке 1.3.

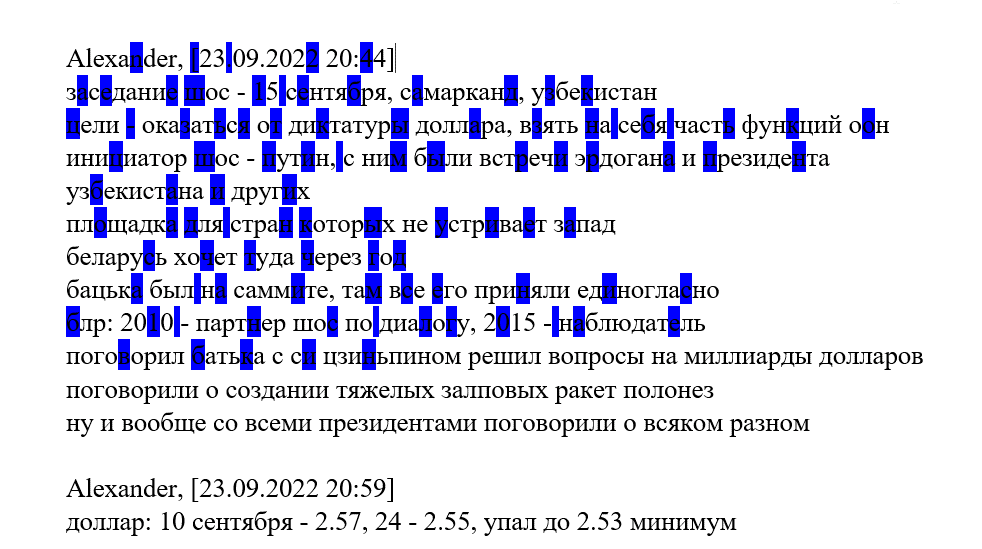


Рисунок 1.3 – Документ-контейнер со встроенным сообщением

Изучив цвет текста, можно заметить, что вместо RGB(0, 0, 0) он соответствует RGB(0, 0, 1), что изображено на рисунке 1.4.

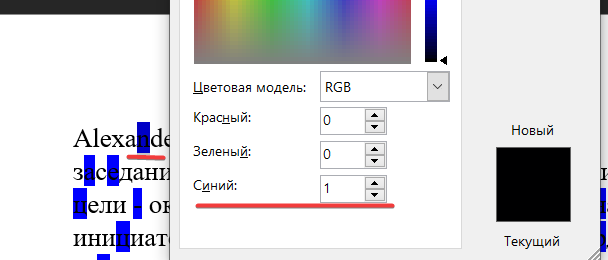


Рисунок 1.4 – Изменение цвета буквы с зашифрованным сообщением

Алгоритм является довольно эффективным, так как визуальные изменения могут быть только при изменении более чем 50 битов. Также он является достаточно быстрым по сравнению с прочими алгоритмами.

# **Собственное программное средство**

Необходимо реализовать метод изменения длины строки. Суть метода заключается в том, чтобы добавить в конце некоторых строк пробел, что не будет визуально заметно в большом тексте. Соотвественно, наличие двух пробелов шифруется единицей, а одного пробела – нулём.

Код функции, реализующей встраивание сообщения в документ-контейнер, представлен на рисунке 1.5.

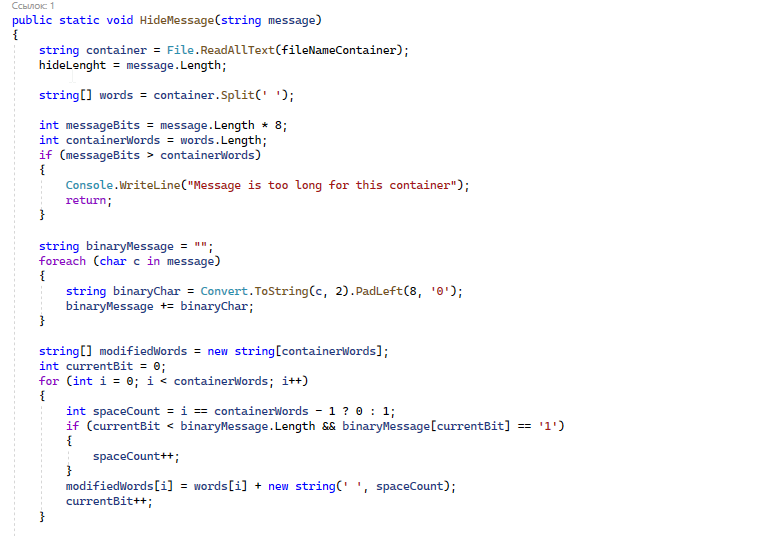


Рисунок 1.5 – Функция встраивания текста в контейнер

Вывод функции представлен на рисунке 1.6.

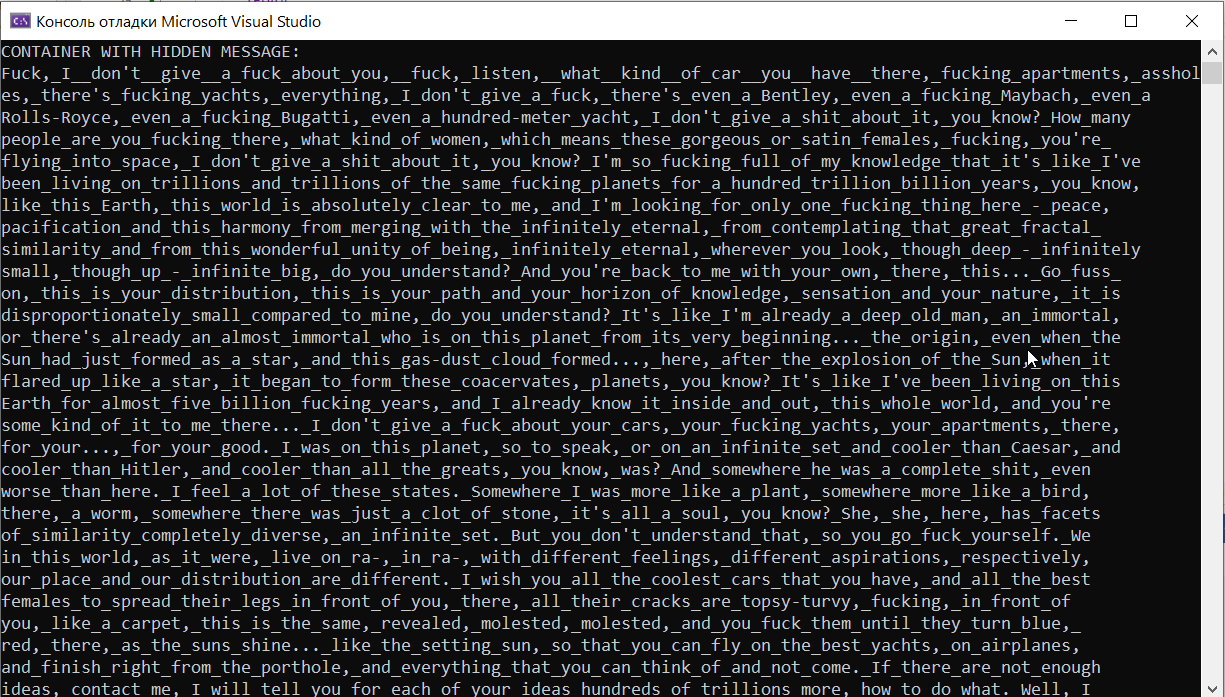


Рисунок 1.6 – Вывод функции встраивания текста в контейнер

Для извлечения текста из контейнера реализована следующая функция, представленная на рисунке 1.7.



Рисунок 1.7 – Функция извлечения текста из контейнера

Встраиваемое сообщение – «qw». Вывод функции извлечения текста из контейнера представлен на рисунке 1.8.



Рисунок 1.8 – Вывод функции извлечения текста из контейнера

Как видно из рисунка, извлеченный текст соответствует встроенному, что свидетельствует о корректном алгоритме встраивания и извлечения текста из текстового контейнера.

# **Вывод**

В данный лабораторной работе были изучены стеганографические методы встраивания и извлечения тайной информации с использованием электронного файла-контейнера текстового формата, а также приобретены практические навыки программной реализации данных методов.