УДК 003.26+347.78

Студ. И.А. Лесняк
Науч. рук. проф. П.П.Урбанович
(кафедра информационных систем и технологий, БГТУ)

АНАЛИЗ ЦЕЛОСТНОСТИ ТЕКСТОВЫХ ФАЙЛОВ-СТЕГАНОКОНТЕЙНЕРОВ С ОСАЖДЕННОЙ ИНФОРМАЦИЕЙ НА ОСНОВЕ ПРИМЕНЕНИЯ КЕРНИНГА ПОСЛЕ СТРУКТУРНЫХ ИЗМЕНЕНИЙ СТЕГАНОКОНТЕЙНЕРА

Цифровая стеганография – направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов.

Целью данной работы является создание программного средства позволяющего производить стегопреобразование, модифицируя кернинг и проанализировать устойчивость стеганоконтейнера к конвертации. Кернинг – избирательное изменение интервала между буквами в зависимости от их формы [1] (рисунок 1).

Рисунок 1 – Демонстрация текста при использовании кернинга

Office Open XML — серия форматов файлов для хранения электронных документов пакетов офисных приложений — в частности, Microsoft Office. Формат представляет собой zip-архив, содержащий текст в виде XML, графику и другие данные, которые могут быть переведены в последовательность битов (сериализованы) с применением защищённых патентами двоичных форматов, спецификации которых были опубликованы Microsoft для пользователей OOXML на условиях Microsoft Open Specification Promise [2].

Для разработки была выбрана платформа .NET. Данный выбор обусловлен необходимостью тонкой работы с форматом OpenXML. Кроме того, данная платформа имеет хорошую производительность и документацию.

Как видно на рисунке 2, при открытии файла, который будет выступать в роли стеганоконтейнера, происходит поиск символов, пригодных для модификации, используя в качестве параметра кернинг.

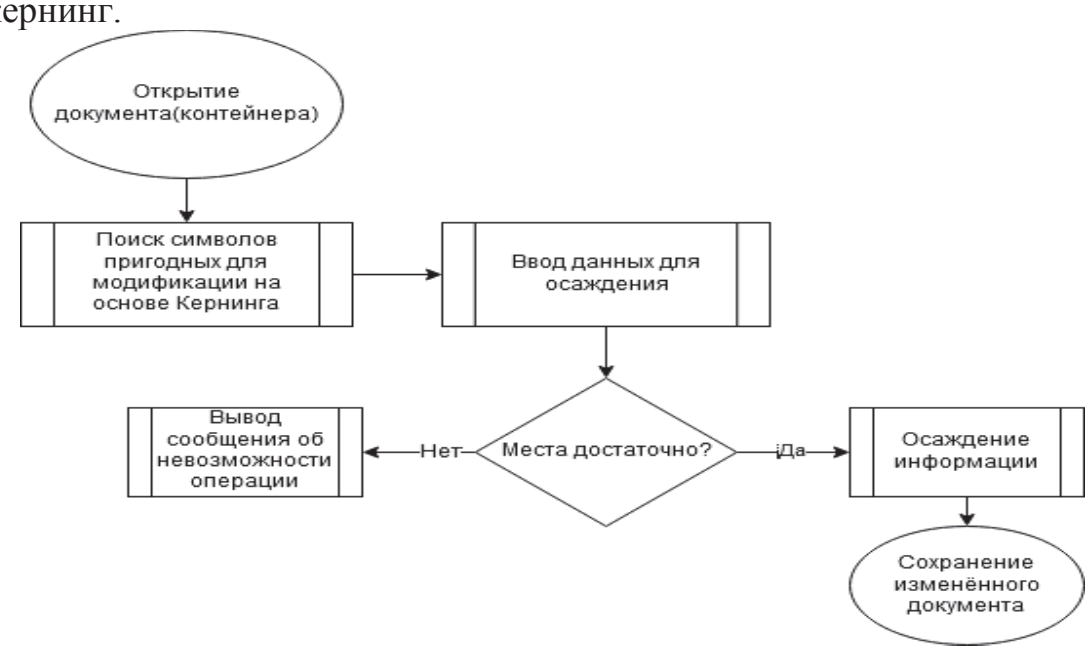

Рисунок 2 – Общая схема процесса осаждения информации

На деле это не совсем так. Дело в том, что каждый символ-буква, пригоден для осаждения в нём информации, используя кернинг. А будет ли изменяться внешний вид буквы, зависит от используемого шрифта и текстового процессора. Мы же, по сути, меняем размер шрифта, при котором будет применяться кернинг. Этот факт можно использовать для повышения секретности. Например, если задать параметр кернинга в значение 70 пт или выше, то без специального анализа обнаружить факт сокрытия информации не удастся, так как внешне текст изменяться не будет. Поэтому на данном этапе производится поиск всех символов-букв.

На рисунке 3 показано окно, в котором данные параметры, используя программу «Microsoft Word» можно задавать вручную.

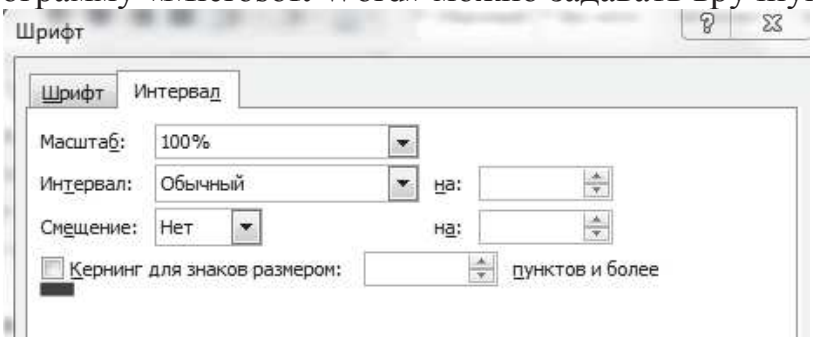

Рисунок 3 – Окно для задания значения кернинга в Microsoft Word

На рисунке 4 представлено главное окно программного средства. На данный момент оно позволяет вводить скрываемый текст вручную или загрузкой из файла. Использовать код Хэмминга перед осаждением информации, тут стоит отметить, что размер информации, которую мы можем скрыть, значительно уменьшается. Так же пользователь может сам задавать значение размера шрифта, при котором будет визуально заметно, использование кернинга. Важно отметить, что при обратном стегопреобразовании нужно будет указывать такой же параметр кернинга. И извлекать скрытую информацию.

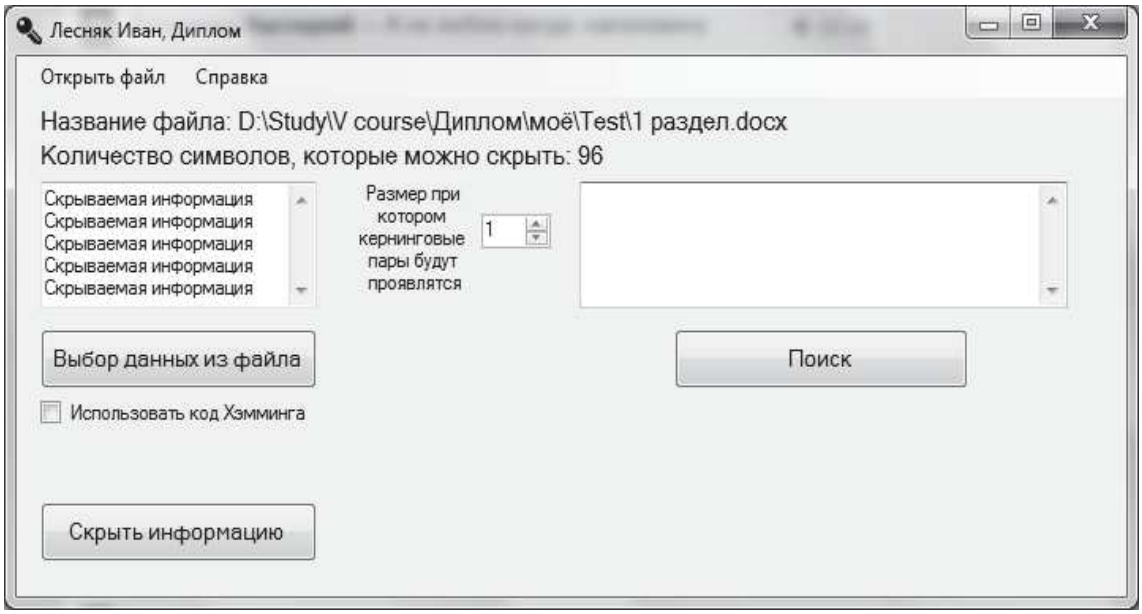

Рисунок 4 – Главное окно программного средства

Можно наверняка сказать, что при конвертации документа в формат, который поддерживает форматирование текста, потери информации не происходит. Но при конвертации в форматы, не поддерживающие форматирования, информация полностью теряется.

Таким образом, скрытие информации методами стеганографии на основе модификации кернинга является достаточно надёжным способом для защиты информации, который имеет свои плюсы и недостатки. К плюсам можно отнести гибкую настройку параметров осаждения, возможность абсолютной невидимости для глаз человека. Среди недостатков самым главным является полная потеря данных при конвертации в формат, не поддерживающий форматирования текста, хотя это уже скорее вопрос использования данного файла.

ЛИТЕРАТУРА

1. Wikipedia. Электронная энциклопедия [Электронный ресурс]: Кернинг. – Режим доступа: https://ru.wikipedia.org. – Дата доступа: 23.04.2017.

2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. — К.: МК-Пресс, 2006. — 288 с.

УДК 003.26+347.78

Студ. О.Л. Панченко
Науч. рук. проф. П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

АНАЛИЗ УСТОЙЧИВОСТИ ПРОЦЕССА СИНХРОНИЗАЦИИ ДВУХ НЕЙРОННЫХ СЕТЕЙ В ЗАДАЧАХ ГЕНЕРАЦИИ КРИПТОГРАФИЧЕСКОГО КЛЮЧА

Для безопасной передачи данных применятся наиболее популярная технология – криптографическое преобразование информации. Криптографические системы подразделяются на асимметричные и симметричные. Их особенности заключаются в том, что в первом случае для зашифрования и расшифрования используются разные ключи, а во втором – один.

Симметричным системам свойственна проблема распределения ключей. Одни из способов решения данной проблемы является использование нейронных сетей. Данная идея была предложена И. Кантером и В. Кинцелем. В ее основе лежит использование архитектуры TPM (англ. Tree Parity Machine, древовидная машина четности). Возможно достижение состояния так называемой синхронизации нейронных сетей, под которой следует понимать равенство значений весовых коэффициентов нейронных сетей. Это и служит основой для протокола выработки общего ключа.

Нейронные сети представляют собой математическую модель, построенную на основе принципов работы биологических нейросетей. Нейрон представляет собой единицу обработки информации в нейронной сети. В этой модели можно выделить три основных элемента (рис. 1).