УДК 003.26+004.056

Маг. В.О. Берников
Науч. рук. проф. П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

АНАЛИЗ СТЕГАНОГРАФИЧЕСКОЙ СТОЙКОСТИ ТЕКСТОВОГО ДОКУМЕНТА-КОНТЕЙНЕРА В МНОГОКЛЮЧЕВОЙ СТЕГАНОСИСТЕМЕ

Многоключевая модель информационной системы предполагает интегрированное использование различных методов стеганографии, криптографии и помехоустойчивого кодирования для повышения криптостойкости системы. Данная модель подразумевает использование отдельного ключа для каждого компонента стеганографической системы [1].

Известны методы стеганографии (на основе цвета и параметра апроша), на основе которых создано программное средство их реализующее. Методы основаны на использовании предварительного преобразования осаждаемой информации (помехоустойчивое кодирование, шифрование).

Стегоконтейнером служит электронный документ Microsoft-Word. Интерфейс программного средства представлен на рисунке 1.

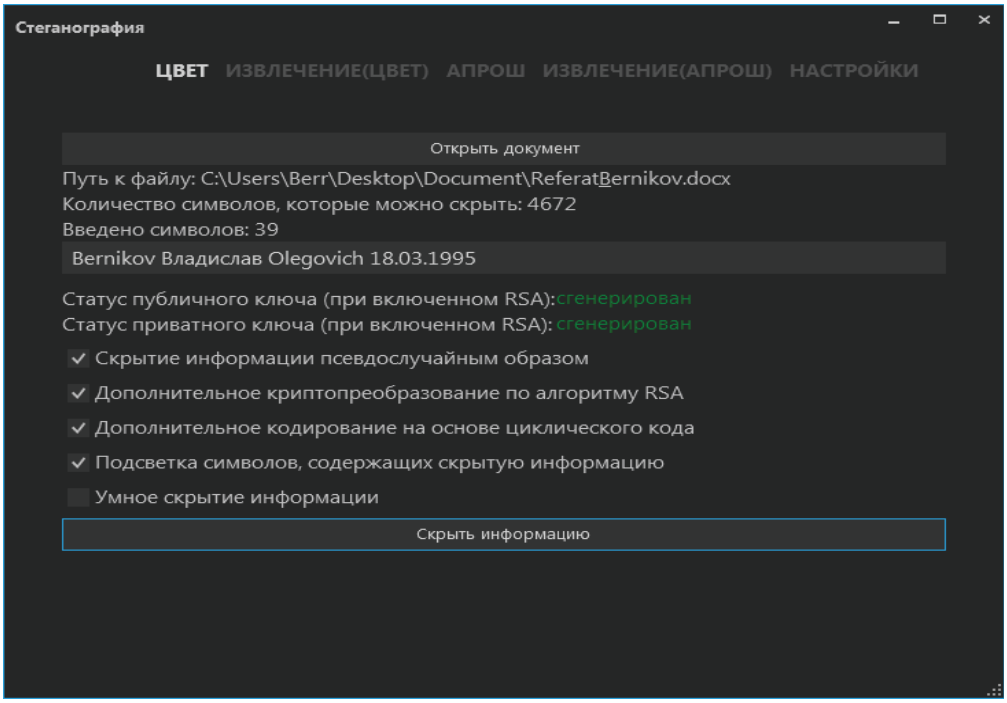

Рисунок – Интерфейс программного средства

Производится подсчет символов, которое можно скрыть в выбранном документе, то есть на каждый символ в стеганоконтейнере можно скрыть один бит секретной информации. Информация может осаждаться псевдослучайным образом по всему документу, а также в начале документа, если не выбран соответствующий пункт в меню [2, 3].

Секретное сообщение преобразуется в двоичный код согласно кодировке Unicode. Английские и русские символы занимают 2 байта (16 битов) в данной кодировке. Для шифрования данных использовалась библиотека RSA, написанная на языке C# с дополнительным хешированием криптопреобразованного сообщения. На выходе при использовании алгоритма хеширования SHA получается фиксированная последовательность внедряемого сообщения, которая составляет 172 байта.

При передаче и хранении осажденного документа могут появляться некоторые ошибки. В программном средстве используется дополнительное кодирование с использованием циклического кода согласно классическому полиному Хемминга при длине информационного слова равной 4 бита. Выходная зашифрованная последовательность нацело делится на *n*-ое количество блоков по 4 бита и для каждого блока производятся вычисления избыточных битов. Зашифрованное сообщение увеличилось на 75%. Данный корректирующий код позволяет исправить одну ошибку в каждом 7-битном слове осажденного документа [4].

Для успешного извлечении информации необходимо указать, какие компоненты многоключевой стеганосистемы были использованы (рисунок 2). А при извлечении информации на основе параметра апроша необходимо указать, такие же отступы для единичного и нулевого бита соответственно, которые использовались при скрытии информации.

Был произведен анализ стеганографической стойкости текстового документа-контейнера после преобразования в другой формат, который поддерживает MicrosoftWord. Исследовались форматы *docm, *doc, dotx, dotm, *dot, *pdf, *xps и *rtf (таблица 1). Документ-контейнер конвертировался в эти форматы, и исследовалась целостность внедренного секретного сообщения.

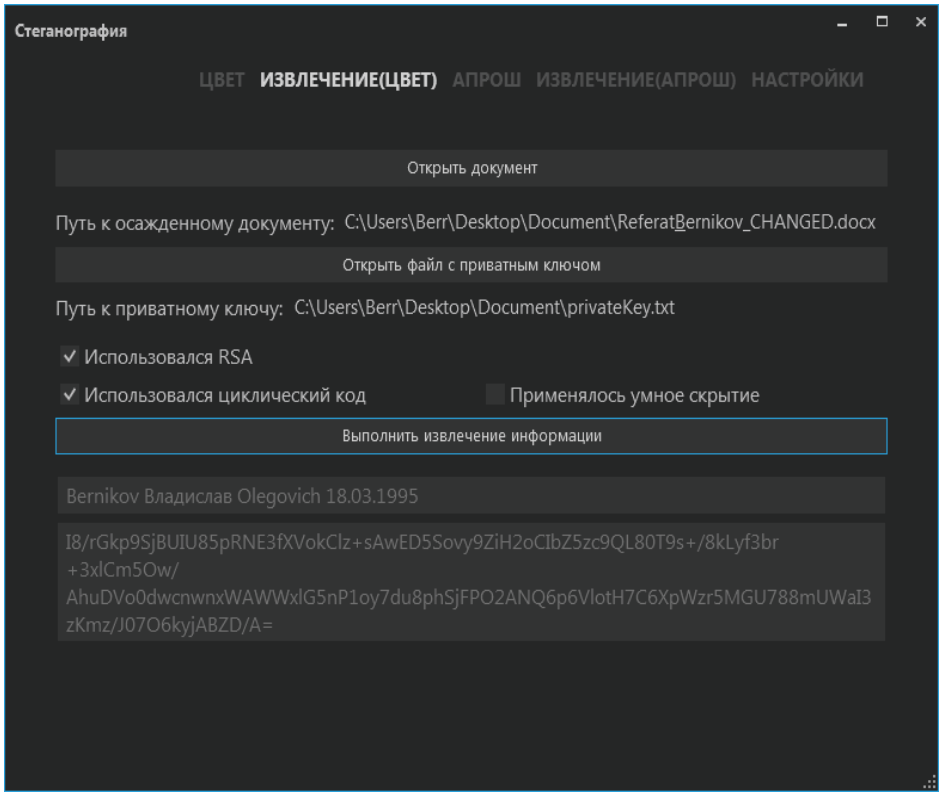

Рисунок – Извлечение секретного сообщения

Таблица – Форматы, которые поддерживаются MocrosoftWord

Название формата	Расширение формата
Документ с поддержкой макросов	*.docm
Документ Word 97-2003	*.doc
Шаблон Word	*.dotx
Шаблон Word с поддержкой макросов	*.dotm
Шаблон Word 97-2003	*.dot
PDF	*.pdf
Документ XPS	*.xps
Текст в формате RTF	*.rtf

Анализ показал, что при конвертации осажденного документа в форматы xps и pdf информация теряется. Это объясняется тем, что данные форматы имеют свои собственные межбуквенные интервалы (чем и объясняется потеря информации при использовании сокрытия секретного сообщения на основе параметра апроша).

ЛИТЕРАТУРА

1. Урбанович, П.П. Защита информации методами криптографии, стеганографии и обфускации/ П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.

2. Urbanovich, P. Theoretical Model of a Multi-Key Steganogra-

phy System/ P. Urbanovich, N. Shutko. – In: Recent Developments in Mathematics and Informatics, Contemporary Mathematics and Computer Science, V. 2, Chapter 11. – Lublin: Wyd. KUL, 2016. – P. 181-202.

3. Шутько, Н.П. Математическая модель системы текстовой стеганографии на основе модификации пространственных и цветовых параметров символов текста/ Н.П. Шутько, Д.М. Романенко, П.П. Урбанович// Труды БГТУ. Серия 6: Физ.-мат. науки и информатика. – Минск: БГТУ. – 2015. – №6. – С. 152-156.

4. Урбанович, П.П. Защита информации и надежность информационных систем/ П.П. Урбанович, Д.В. Шиман. – Минск: БГТУ, 2014. – 90 с.

УДК 502.3

Магистрант Т. С. Петунина
Науч. рук. доц., канд. физ.-мат. наук Н. И. Гурин
(кафедра информационных систем и технологий)

ВЕБ-ПОРТАЛ ДИСТАНЦИОННОГО ОБУЧЕНИЯ С ИНТЕГРАЦИЕЙ ИНФОРМАЦИОННОЙ МУЛЬТИМЕДИЙНОЙ СРЕДЫ

В соответствии с необходимостью совершенствования технологий дистанционного обучения разрабатывается система электронного обучения с интеграцией информационной мультимедийной среды. Основной целью разработки является создание структуры для построения системы дистанционного обучения (СДО), включающую мультимедийную интерактивную среду – анимации, 3D-симуляторы, диалог, в том числе речевой, с базой знаний обучающей среды.

Для достижения этой цели последовательно решаются следующие задачи:

1. Разработка базы данных СДО.
2. Разработка интерфейса системы.
3. Просмотр мультимедиа контента курса и его редактирование.
4. Внедрение мультимедийной интерактивной среды в систему дистанционного обучения.

В качестве технологии разработки СДО с мультимедийной средой была выбрана технология ASP.Net MVC, поэтому в