

Секция информационных технологий
ЛИТЕРАТУРА

1. Урбанович П.П. Защита информации методами криптографии, стеганографии и обfuscации/ П.П. Урбанович. – Минск: БГТУ. – 2016. – 220 с.
2. Сущеня, А. А. Стеганографическое преобразование текстовых контейнеров на основе языков разметки / А. А. Сущеня // 68-я научно-техническая конференция учащихся, студентов и магистрантов БГТУ, 17-22 апреля, Минск: сборник научных работ: в 4 ч., Ч.4/ Белорусский государственный технологический университет. – Минск : БГТУ, 2017. – С. 145-149.
3. Интернет-портал [Электронный ресурс]/ Стеганография в XML, HTML: метод изменения порядка следования атрибутов в файлах с разметкой. – Режим доступа: <http://www.nestego.ru/2012/05/xml-html.html>. – Дата доступа: 20.03.1017.
4. Интернет-портал [Электронный ресурс]/ Текстовая стеганография. Метод хвостовых пробелов. – Режим доступа: http://www.nestego.ru/2012/05/blog-post_03.html. – Дата доступа: 20.03.1017.

УДК004.056

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

**ПРОГРАММНОЕ СРЕДСТВО ДЛЯ АНАЛИЗА
ПРОСТРАНСТВЕННО-ГЕОМЕТРИЧЕСКИХ ПАРАМЕТРОВ
ТЕКСТОВЫХ ДОКУМЕНТОВ**

Одним из способов решения проблемы защиты передаваемой информации является стеганография. Стеганография – способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи (хранения). Информация, которую необходимо передать защищенно (скрыть), помещается (осаждаются) в контейнер – данные (изображения, текст, видеофайлы и т.д.), используемые для осаждения информации. Само же осаждаемое сообщение при этом называется стегосообщением.

Большую часть передаваемой информации составляет текст, а наиболее распространенным форматом, используемым для представления текстовых данных, является DOCX. Следовательно, в качестве контейнера для осаждения информации данный формат подходит больше всего.

Стеганография, использующая в качестве контейнера текст, называется текстовой стеганографией [1]. В данном методе используются допущения в количестве и расположении символов в тексте, которые не учитываются при прочтении человеком и при компьютерном анализе файла. Это может быть дополнительное количество пробелов и знаков табуляции в разных частях строки, без учета служебных символов, больших и маленьких букв, букв из разных алфавитов.

Кроме того, еще одним способом осаждения данных является изменение пространственно-геометрических параметров текстовых документов (в качестве таковых используются апрош, кернинг, кегль шрифта).

Однако, несмотря на простоту реализации текстовой стеганографии и ее возможное широкое распространение, в настоящее время почти не реализованы методики и программные средства для ее выявления.

Было разработано программное средство для упрощения анализа текстовых документов формата .docx. Данный формат был выбран из-за своего широко распространения среди пользователей.

В разработанном программном продукте анализу подвергаются такие параметры, как количество пробелов и значение кернинга [2]. Пользователю предлагается выбор, по какому из двух параметров будет произведен анализ загруженного им документа.

Также программное средство реализует в себе следующий функционал:

- загрузка документа формата .docx для проведения анализа;
- проведение анализа документа по выбранную параметру;
- предоставление результатов анализа стегоаналитику;
- предоставление стегоаналитику средств для построения предполагаемого алгоритма выявления осажденной информации;
- получение осажденной информации, согласно определенным в предыдущем пункте правилам;
- выделение частей текстового документа, содержащих предполагаемые наборы значений анализируемых параметров, используемых при извлечении осажденной информации.

Для анализа результатов используется набор контроллов, представленных на рисунке 1 в нижней части экрана.

Левый выпадающий список содержит найденные в загруженном документе значения анализируемого параметра. Стегоаналитику предоставляется возможность комбинирования этих значений в группы и сопоставление с этим набором символа или символов двоичного или иного алфавита.

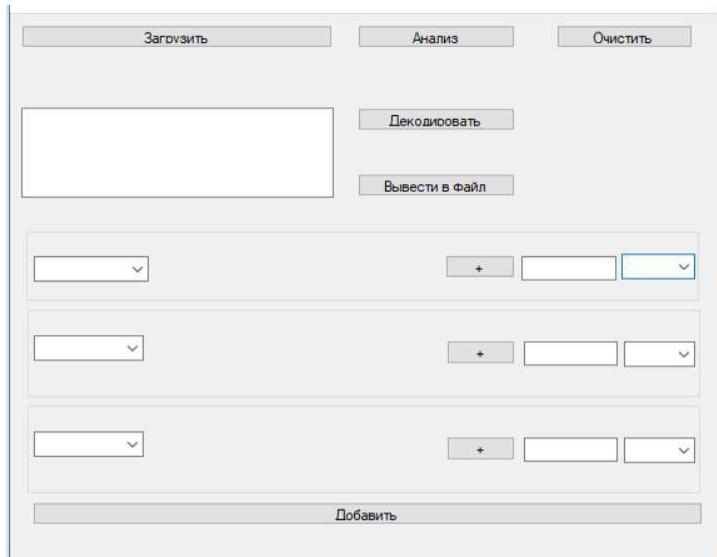


Рисунок 1 – Главное окно разработанного программного средства

Результатом данного шага является получение возможных способов кодирования, используемых для осаждения сообщения в контейнер, выявленных стегоаналитиком [3-5]. Описание предполагаемого метода, используемого для сокрытия информации в контейнере, представляет собой массив формата ключ-значение, в котором в качестве ключа выступает последовательность значений анализируемых параметров текста, а в качестве значения предполагаемый закодированный символ или набор символов.

На этапе декодирования происходит повторный анализ текстового документа с целью получения элементов, соответствующих ключам из массива, и замене их значениями из того же массива. В результате стегоаналитик получает осажденное сообщение.

Выпадающие списки, помещенные справа, содержат набор цветов, разрешенный при использовании выделений в тексте. Т.е. каждой последовательности можно поставить в соответствие один из этих цветов и далее выбрать документ, который будет проанализирован. Результатом данного процесса будет являться документ, содержащий выделения текста в местах, где были найдены совпадения с последовательностями, установленными стегоаналитиком. Такой подход упростит процесс выявления алгоритма, который активно использовал непосредственно содержание контейнера.

При разработке программного средства для взаимодействия с документами формата .docx, а именно для проведения стеганографического анализа текстовых данных, содержащихся в документе, была использована библиотека «Microsoft.Office.Interop.Word». Анализ осу-

ществляется за счёт использования функций указанной библиотеки, которые позволяют выполнять переход между символами внутри документа и просматривать значения пространственно-геометрических параметров, примененных к символам документа.

Данное программное средство ускоряет процесс анализа и выявление сокрытого сообщения в текстовом контейнере за счет возможности автоматизации решения задачи об определении факта наличия сокрытой информации в документе.

ЛИТЕРАТУРА

1. Урбанович, П.П. Защита информации методами криптографии, стеганографии и обfuscации/ П.П. Урбанович. – Минск : БГТУ, 2016, – 220 с.
2. 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.
3. Интернет-портал [Электронный ресурс]/Wikipedia. – Режим доступа:<https://ru.wikipedia.org/wiki/Стеганография>. – Дата доступа: 25.03.1017.
4. Интернет-портал [Электронный ресурс]/Стеганография & путешествия. – Режим доступа: http://www.nestego.ru/2012/04/blog-post_28.html. – Дата доступа: 26.03.1017.
5. Urbanovich, P. Theoretical Model of a Multi-Key Steganography 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.