УДК 003.26+004.56

Н. П. Шутько, канд. техн. наук, доц.,
П. П. Урбанович, д-р техн. наук, проф.
(БГТУ, г. Минск)

СТОЙКОСТЬ ТЕКСТОВОГО СТЕГАНОКОНТЕЙНЕРА К ИСКАЖЕНИЯМ

Цифровая стеганография – направление, основанное на реализации методов сокрытии или внедрении тайной информации в цифровые объекты, называемые контейнерами [1]. Контейнерами могут выступать, например, электронные документы различного типа. При этом и использование стеганографических методов может преследовать различные цели [2-5].

Идея представленного исследования состоит в том, чтобы оценить стеганостойкость метода текстовой стеганографии, основанного на модификации цветовых параметров символов текста [1, 4].

Под стеганоконтейнером будем понимать текстовый документ (несекретные данные) со скрытой в нем тайной информацией.

С помощью авторского программного средства Sword [6] (рисунок 1) в электронный текстовый документ осаждалась (секретная) информация.

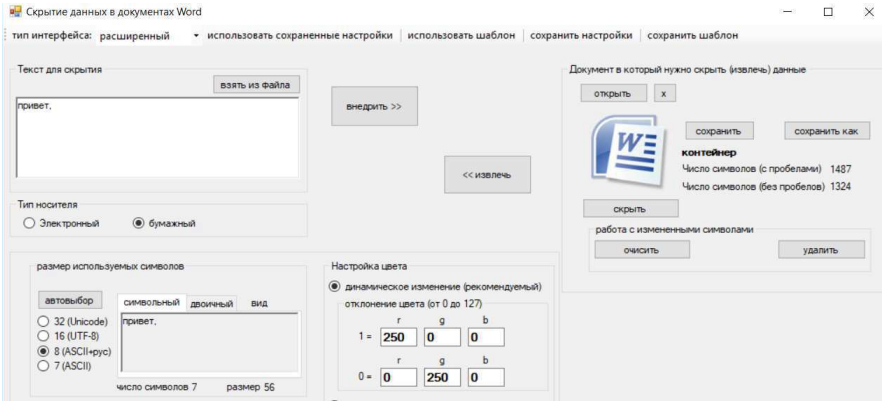

Рисунок 1 – Диалоговое окно программного средства Sword

В качестве контейнера выступил документ, созданный в текстовом процессоре MS Word (общее число символов – 1324). Секретное сообщение – «привет.» (число символов – 7, размер – 56 бит). Встраивание производилось за счет изменения значений трех основных цветовых каналов (красного, зеленого и синего) на определенное значение.

Необходимо отметить, почему изменялось значение именно данных трех цветов. Информация, выводимая на экран монитора, представлена в цветовой модели RGB (red – красный, green – зеленый, blue – си-

ний). Изменение исходных значений цвета символов в документе обусловлено значением ключа. В данном случае ключом выступает последовательность, представленная на рисунок 2.

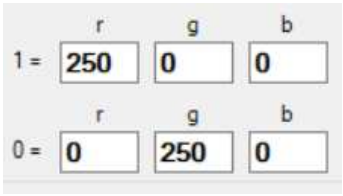

Рисунок 2 – Значения ключа

В результате осаждения контейнер принял вид, фрагментарно показанный на рисунок 3. Зеленым и красным цветами отмечены модифицированные символы. В них содержится осажденная информация, представленная в двоичном виде).

Начало 21 века характеризуется глобальными изменениями в области информационных или информационно-коммуникационных технологий (ИКТ). Эти изменения обусловили трансформации всех сторон жизнедеятельности отдельных людей, в частности, и государств, вообще. Как подчеркивается в Концепции национальной безопасности Республики Беларусь [1], «информационная сфера превращается в системообразующий фактор жизни людей, обществ и государств». Информацию сейчас рассматривают в качестве важнейшей, одной из самых дорогих сущностей мира. А информационные системы и процессы стали определяющим фактором реализации инновационного подхода, повышения эффективности

Рисунок 3 – Модифицированный контейнер

Для оценки стеганостойкости описываемого метода стеганоконтейнер был распечатан на цветном МФУ Canon G3400. Впоследствии напечатанный документ был отсканирован с использованием того же устройства (качество как печати, так и сканирования – высокое). Для проведения анализа необходимо конвертировать полученный PDF-файл в документ Word, а также распознать его, так как программное средство Sword работает только с документами, созданными с помощью текстового процессора MS Word.

Для чистоты эксперимента в ходе исследования для конвертации и распознавания текста было использовано несколько онлайн сервисов: Onlineocr, Convertio, Convertonlinefree, Img2txt, Pdfcandy, Pdf2go. Опытным путем было установлено, что почти все конверторы недостаточно успешно распознают текст. Только Pdf2go наиболее полно и точно распознал текст документа. Кроме того, было установлено, что при такой многоступенчатой комбинации (встраивание – печать – сканирование – конвертация – распознавание) цвет символов не сохраня-

ется. Таким образом, было установлено, что метод текстовой стеганографии, основанный на модификации цветовых параметров, не устойчив к такого рода искажениям. Однако, необходимо отметить, что данный метод имеет достаточно высокую эффективность для осаждения информации при условии, что стеганоконтейнер будет храниться/передаваться в электронном виде.

ЛИТЕРАТУРА

1. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. Пособие/ П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.
2. Shutko, N. A method of syntactic text steganography based on modification of the document-container aprosh / Nadzeya Shutko, Pavel Urbanovich, Pawel Zukowski // Przegląd elektrotechniczny. – 2018. – R. 94, NR 6.– P. 82–85.
3. Urbanovich, P. Theoretical Model of a Multi-Key Steganography System / P. Urbanovich, N. Shutko // Recent Developments in Mathematics and Informatics. Contemporary Mathematics and Computer Science. Vol. 2, Chapter 11. – Lublin: KUL, 2016. – P. 181–202.
4. Шутько, Н. П. Защита авторских прав на текстовые документы на основе стеганографической модификации цвета символов текста / Н. П. Шутько, П. П. Урбанович // Информационные технологии: материалы 83-й научно-техн. конф. проф.-препод. состава, науч. Сотр. и аспирантов (с междунар. участием), Минск, 4–15 февраля 2019 г.– Минск:: БГТУ, 2019. – С. 41–43.
5. Блинова, Е.А. Стеганографический метод на основе встраивания дополнительных значений координат в изображения формата SVG/ Е. А. Блинова, П.П. Урбанович// Труды БГТУ. Сер. 3, Физико-математические науки и информатика. – Минск: БГТУ, 2018. – № 1 (206). – С. 104–109.
6. Свидетельство о регистрации компьютерной программы Sword v.1.0 / В. А. Пласковицкий, Н. П. Шутько // Реестр Национального Центра интеллектуальной собственности РБ. – 2011. – Запись № 383 от 04.01.2012.