УДК 004.056.55

**Н.П. Шутько**
Белорусский государственный технологический университет
Минск, Беларусь

# ИСПОЛЬЗОВАНИЕ ОСОБЕННОСТЕЙ ФОРМАТА DOCX ДЛЯ ХРАНЕНИЯ И ПЕРЕДАЧИ АВТОРСКОЙ ИНФОРМАЦИИ МЕТОДАМИ КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ

***Аннотация.*** *Описаны и проанализированы некоторые особенности нового метода встраивания тайной информации в электронных документ методами компьютерной стеганографии. Такая информация позволяет подтвердить авторские права на электронный контент.*

**N.P. Shutko**
Belarusian State Technological University
Minsk, Belarus

# USING THE FEATURES OF THE DOCX FORMAT FOR STORING AND TRANSMITTING AUTHOR'S INFORMATION BASED ON COMPUTER STEGANOGRAPHY METHODS

***Abstract.*** *Some features of the new method of embedding secret information into electronic documents using computer steganography methods are described and analyzed. Such information allows you to confirm the copyright of electronic content.*

Развитие современных технологий, сферы IT и компьютерной стеганографии, в частности, приводит к необходимости создания новых более эффективных методов передачи и защиты данных. В опубликованных ранее работах были предложены и исследованы методы стеганографии, которые учитывают особенности электронных документов различных форматов [1, 2].

В [3] описан метод встраивания секретного сообщения в электронный растровый документ-контейнер в формате .jpg. Сущность метода заключается в использовании особенностей данного формата, который состоит в том, что контейнер формата .jpg имеет флаги начала и конца файла. Программа для работы с изображениями указанного формата не учитывает все данные, которые записаны после флага конца файла, так как они находятся вне контейнера. Кроме того, приложения, работающие с файлами архивами (например, WinRar) отбрасывают все данные файла до тех пор, пока не найдут заголовок архива. Дальнейшая работа состоит в так называемой «склейке» двух форматов − .jpg (данный файл выступает в роли контейнера) и пустого файла с расширением .rar. В результате

получается валидный файл-изображение, который можно при необходимости представить в виде архива.

Далее исследуем особенности описанного метода, адаптировав его под решение задач в области текстовой стеганографии.

За основу метода будет взят тот факт, что электронные текстовые документы формата .docx представляют собой архив, в котором содержится размеченный при помощи XML текст и другие данные о документе, которые могут быть интерпретированы текстовым редактором (рис. 1). Более подробно данная особенность была рассмотрена в [2, 4].

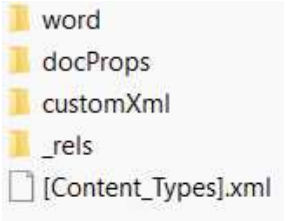


**Рис. 1 - Файловая структура документа в формате *.docx**

Для примера в качестве документа-контейнера будет выступать электронный текстовый документ в указанном выше формате .docx, размер контейнера составляет 19,7 килобайт (рис. 2).

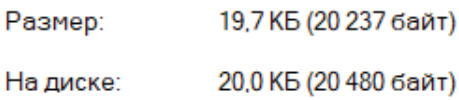


**Рис. 2 - Объем документа-контейнера**

Эксперимент будет состоять из нескольких этапов. Первоначально в роли секретного сообщения будет выступать текстовый документ формата .txt. Содержимое данного файла приведено на рис. 3.

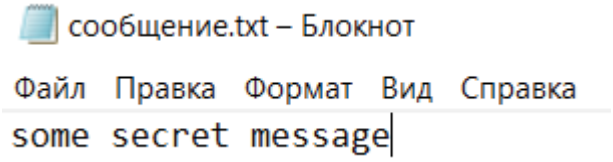


**Рис. 3 - Содержимое стегосообщения**

Для оценки корректности и точности проведения стеганографического преобразования будет использоваться редактор шестнадцатеричных и бинарных файлов *Hex Editor Neo*. Указанное выше стегосообщение будет иметь вид, представленный на рис. 4.

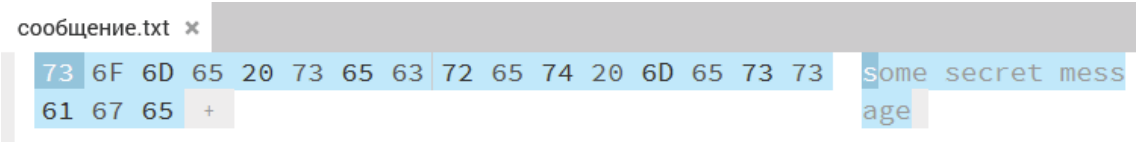


**Рис. 4 - Представление сообщения в шестнадцатеричном формате**

Путем добавления файла с авторским текстом в архив исходного документа-контейнера получаем стегоконтейнер, который имеет следующие свойства (рис. 5).


**Рис. 5 - Размер стегоконтейнера**

Визуально внедрение секретной информации не внесло никаких корректировок в содержимое исходного текстового документа. Изменению подвергся лишь набор файлов, входящих в архив данного контейнера.

Авторская информация может быть представлена не только формате текстового документа с расширением .txt, но и .xml. Методика осаждения идентична. Однако необходимо отметить, что полученный в результате такого стеганографического преобразования документ имеет меньший объем, нежели в случае встраивания стегосообщения в формате .txt (рис. 6).


**Рис. 6 - Размер стегоконтейнера**

Использование данного стеганографического метода повышает стойкость передаваемого стегосообщения в сравнении с методами, которые используют цветовые и пространственно-геометрические параметры символов текста. Это возникает в виду того, что пользователь не может преднамеренно или случайно изменить осажденное сообщение, например, в результате форматирования электронного документа.

Применение данного метода и его стойкость к искажениям различного рода представляет интерес для проведения дальнейших исследований.

## Список использованных источников

1. Шутько, Н. П. Использование цветовых координат HSL для защиты и передачи авторской информации / Н. П. Шутько // Информационные технологии: материалы 86-й научно-технической конференции профессорско-преподавательского состава, научных сотрудников и аспирантов, Минск, 31 января–12 февраля 2022 г. – Минск: БГТУ, 2022. – С. 125–128.

2. Шутько Н. П. Передача текстовой информации на основе изменения апроша с использованием особенностей формата XML / Н. П. Шутько // Технические средства защиты информации: тез. докл. XXI Белорусско-российской науч.-техн. конф., Минск, 6 июня 2023 года. – Минск: БГУИР, 2023. – С. 102–103.

3. Стеганография. Общий обзор [Электронный ресурс]. – Режим доступа: https://m.vk.com/@fractal_utmn-steganografiya-obschii-obzor?context=author_page_date&ref=author_page. – Дата доступа: 01.11.2023.

4. Использование особенностей формата XML в методах текстовой стеганографии / П. П. Урбанович, О. А. Нистюк, М. Г. Савельева, Н. П. Шутько, А. Н. Николайчук // Информационные системы и технологии: материалы международного научного конгресса по информатике. – Ч. 1. – Минск: БГУ, 2022. – С. 120–126.

УДК 004.421.2

**А.Н. Щербакова, Д.М. Романенко**
Белорусский государственный технологический университет
Минск, Беларусь

## ОСОБЕННОСТИ ФОРМИРОВАНИЯ КЛЮЧА ДЛЯ КОДИРОВАНИЯ ВЕКТОРНЫХ ИЗОБРАЖЕНИЙ

***Аннотация***. *В статье рассмотрены особенности формирования ключа для кодирования векторных изображений с целью внедрения в электронные документы, содержащие векторные изображения, при этом построение графического ключа должно быть индивидуально для кодированного сообщения.*

**A.N. Shcherbakova, D.M. Romanenko**
Belarusian State Technological University
Minsk, Belarus

## FEATURES OF KEY GENERATION FOR ENCODING VECTOR IMAGES

***Abstract***. *The article discusses the features of the formation of a key for encoding vector images for the purpose of embedding in electronic documents containing vector images, while the construction of a graphic key should be individual for the encoded message.*

Кодирование – перевод данных, отображенных в виде первичного алфавита, в последовательность кодов [1].