11th International Conference

New Electrical and Electronic Technologies and their Industrial Implementation

Zakopane, Poland, June 25 – 28, 2019

Edited by **Tomasz N. Kołtunowicz**

ISBN: 978-83-7947-369-4

Publisher: Lublin University of Technology
20-618 Lublin, 38d Nadbystrzycka Str.
Realization: Lublin University of Technology Library
e-mail: wydawca@pollub.pl

Software tool for the analysis of the text steganography method based on the modification of the characters color

P. Urbanovich[1,2], E. Blinova[1], V. Plaskovitski[1], N. Shutko[1]
[1] Belarusian State Technological University, Minsk, Belarus, E-mail: shutko_bstu@mail.ru
[2] Lublin Catholic University, Lublin, Poland, E-mail: pav.urb@yandex.by

It is known that *.docx files are created using the open XML format. Documents are stored as separate files and folders in a compressed package: docx-files contain XML files and three folders. Because of this, the docx-file can be split into its components. Given this feature, we have programmatically implemented some new methods of text steganography [1, 2]. One of the purposes of using of the methods is to protect the copyright of electronic and paper text documents.

In particular, the application Sword v.1.0 is based on the use of the method of modifying color parameters (RGB channels) of text characters [3]. It allows you to work with documents of formats that can store the color of characters: * .doc, *. docx, * .rtf, * .odt. When selecting and analyzing the type of carrier (electronic or paper), it is necessary to take into account that in the first case secret information is embedded only in visible characters, in the second – and in invisible (spaces, line end). A feature of the implemented algorithm is the introduction of two additional colors for the description of special numerical values characterizing the number of consecutive message characters (which is previously processed by the Burrows-Wheeler method).

Two types of color changes are applied - dynamic and static. In the first case, one character of the text container is taken as a basis, its color is read. The required secret message is converted to binary cjde. The application creates variables to which it assigns values for color channels, and distributes the secret message approximately evenly inside the text container (see Fig. 1).

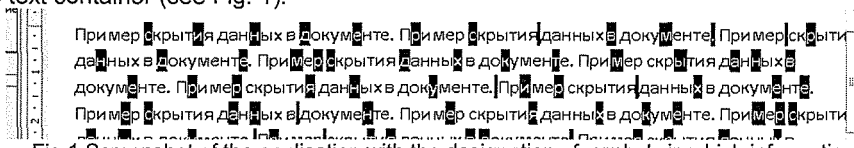

Fig.1 Screenshot of the application with the designation of symbols in which information is embedded

Parameters that are used to hide text can be saved to files for later reading. These files are plain text documents that store settings that are structured in a special way. Performed a series of studies. For example, the message extraction rate is approximately 50 characters per second. The report analyzes the steganographic resistance of the method and the effectiveness of its implementation with various encodings of the embedded message (2nd, 4th, 8th, 16th, 32nd).

References

[1] Urbanovich P.P.: Zashchita informatsii metodami kriptografii, steganografii i obfuskatsii: ucheb.-metod. posobiye dlya stud. - Minsk: BGTU, 2016, 220 s.
[2] Shutko N., Urbanovich P., Zukowski P.: A method of syntactic text steganography based on modification of the document-container aprosh, Przegląd elektrotechniczny, 2018, R. 94, n.6, p. 82-85.
[3] Shutko N. P.: Zashchita avtorskikh prav na elektronnyye tekstovyye dokumenty metodami steganografii, Trudy BGTU, Minsk: BGTU, 2013, n.6 (162), s. 131-134.