Nadzeya URBANOVICH, Vladimir PLASKOVITSKY

Belarusian State Technological University

The use of steganographic techniques for protection of intellectual property rights

Abstract. *A new method of text steganography to protect intellectual property rights, based on the use colour and size attributes fonts is proposed. The efficiency of this method was analysed.*

Streszczenie. *Została przedstawiona nowa metoda steganografii tekstowej do ochrony praw autorskich, wykorzystująca atrybuty koloru i rozmiaru czcionki. Metoda ta została przeanalizowana pod kątem efektywności (**Zastosowanie technik steganografii do ochrony praw własności intelektualnej**).*

Keywords: information hiding, steganography, intellectual property rights, attributes of the font.
Słowa kluczowe: ukrywanie informacji, steganografia, intelektualne prawa własności, atrybuty czcionki.

Introduction

As it is known, the copyright is an important component of universal system of human rights. Digital technologies allow to solve this problem at new, higher level [1]. One of such technologies is based on use of steganographic methods.

Unlike cryptography, which hides contents of the confidential message, steganography hides its existence. As it is known, the purpose of cryptography is to block unauthorized access to information by encrypting the content of secret messages. Steganography has other problem, and its purpose – to suppress the fact of existence of the confidential message. In this case, both methods can be combined and used to improve protection of information (for example, to transfer the cryptographic keys).

Then shortly describe the basic elements of steganographic system: a message and a container.

The non-sensitive data, which are used to conceal messages, is called container (carrier). In computer steganography various digitized data can be used as containers: text-based electronic documents, bitmap graphics, video etc.

A secret information you want to hide into the container is called a message or an embedded message (stego).

Steganography, using text containers, is called text steganography. The fact of presence stego is confidential [2, 3].

In the context of the problem of copyright in text documents, we note that, as a secret information may be: the data about the author of the text document, date and place of work is created, the numbers of documents confirming the authorship, date, priority, etc.

Now computer steganography continues to develop: the theoretical base is formed, working out of new, more proof methods of embedding of messages [4] is conducted.

Many existing methods of text steganography is not enough to effectively hide the message, the fact of secret information (key) is a clear or almost clear [5]. This conclusion was drawn by the article's authors based on a comparative analysis of the known methods of text steganography with the help specially designed software tools. The results of our research show a relatively low efficiency of the known methods of text steganography.

This article presents the results of creating and using a new method of text steganography based on the color settings of the font.

The essence of the proposed method

It is known, the color of each character (on screen) is represented in a certain color model. In a word processor MS Word 2007 the whole spectrum of used colors is described by the model RGB (red, green and blue).

We examined the effectiveness of embedding secret information (including the copyright symbol) in the text. It is proposed to hide a secret message in binary sequences corresponding to the color of the characters.

Because of the color in a word processor MS Word is represented in the RGB, as we said above, the coordinates of the corresponding base colors are exposed to change.

Let's analyze the essence of the proposed method by an example. We inserted the message «Урбанович Надежда Павловна» (secret, copyright information) in a document in English, using specially developed software tool. For this purpose the ciphered message (original text) is translated into binary form.

The algorithm of color coordinates' modification of the text characters consists in the following.

1. The deviation from primary color for symbols in RGB system is set in settings (the variation range of the parameter of each color channel, RGB – from 0 to 127; for example, code (0;0;0) does not change the original color of the text characters).
2. Hiding secret information. In the process of hiding a secret text two consecutive characters are taken from the container: the first one – sample, the second one – the one in which the text will be hidden. The color of symbol, the information will be hidden in, is formed on the basis of the color of the symbol sample and a given (see the step 1) offset in the settings. By default, this offset is added to the main color.

To evaluate the effectiveness of the method the experiment was carried out. Examples of the text documents with built-in stegomessage were offered to the students of 2-3 courses of «Graphic art» Faculty (I) as well as pupils of 8-10 classes (II). The participants of the experiment were asked the following questions: Evaluate the visual representation of the text. Do you see something unusual in the text? The results are displayed in table 1.

Tab. 1. The results of the experiment «by eye»

The number of embedded bits	The color	
	Negative answers, %	
	I	II
1	100,00	100,00
2	100,00	100,00
3	96,15	100,00
4	65,40	70,50
5	27,08	29,50
6	0,00	0,00

Due to the fact that the increase the number of used bits of color in the text, as compared with the graphic objects, comes from the fact that the image usually contain gradations and transitions from the one color to another one. Text is monotonic and runs in most cases the same color. So it becomes possible to increase the use to embed the color range.

For example, it is necessary to introduce the confidential message «101» in the text-container «A», using a word-processor (Fig. 1). In the given processor color of symbols is presented in system RGB in 8 bits on the channel (each of 3 standard colors is presented by 8 bits – number from 0 to 255). Embedding of the confidential message we will make in younger bits of color of symbols. As a result color will be received: (00000001, 00000000, 00000001). As you can see, there is no difference between the two characters.

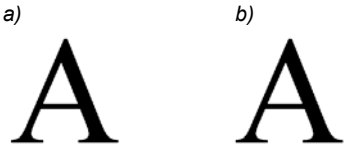

Fig.1. Application of the method changes the color of characters: *a)* the standard graphic symbols; *b)* the modified symbol (with built-secret message «101»)

With the help of the author's software tools we investigated the efficiency of embedding information by using the attributes of a font as aprosh, kerning, color, scale. This method allows the most imperceptibly hiding produce the necessary data.

The software tool for the analysis method

Installation of necessary parameters is carried out by means of three blocks (are designated accordingly by numbers 1–3 on fig. 2) in which it is set: secret massage – 1 (in case of extraction it is not necessary to fill), the container – 2 and options on which basis there is a concealment/extraction messages (key) – 3.

Language development: C # (Framework 2.0 + libraries Microsoft.Vbe.Interop.dll, Microsoft.Office.Interop.Word.dll, office.dll).

OS Requirements: Windows + Framework 2.0 (XP, Vista, Seven).

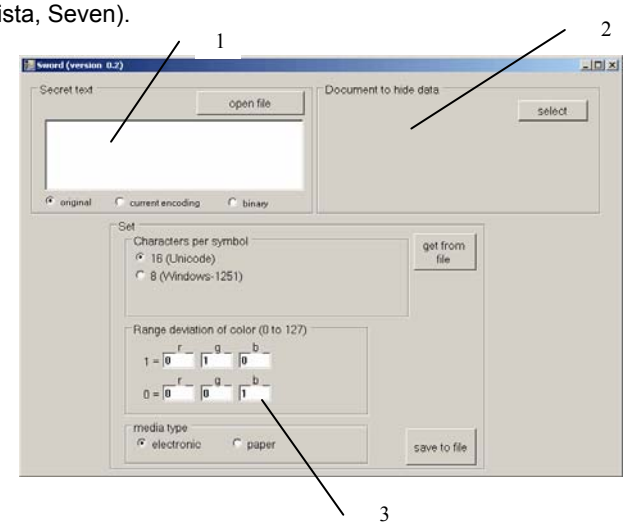

Fig.2. General view of the program

Supported document formats to hide: all that can be opened with MS Office Word and can store characters color: Word 93–2010 (*.doc, *.docx), *.rtf (cross-platform format for storing text documents marked) *.odt (open document format for office applications). Support for these formats should be available from The described method and the software currently used now for studying of possibility of placing information in text documents the information, which protects intellectual property rights.

It is possible to enter secret massage from the keyboard, to insert from the buffer, to open from a file. When you select the required document is provided three filters, as well as the choice of any file (Fig. 3).

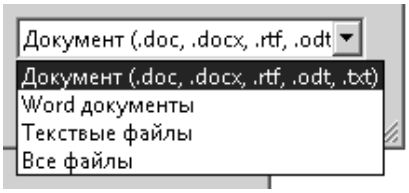

Fig.3. Possible types of documents

Conclusion

It is proposed to use a binary representation of text characters as a container for placing information in order to protect copyright creators of the documents.

During enough bulk experiments (about 130 participants) it was established that the modification of up to 4 minor characters of color coordinates of each channel (RGB) in 100% of the cases unnoticed by the user, who does not know the fact of deposition in the document invisible information.

This allows to use the method for the procedure of text documents authorization.

REFERENCES

[1] Конахович Г.Ф., Пузыренко А.Ю., Компьютерная стеганография, Теория и практика, «МК-Пресс» (2006), 288

[2] Wayner P., Disappearing Cryptography, Information Hiding: Steganography&Watermarking, 2nd. ed. San Francisco: Morgan Kaufmann, 2002

[3] Urbanovich P., Urbanovich N., Chourikov K., Rimorev A., Niektóre aspekty zastosowania metod steganograficznych do przechowywania powiadomień tekstowych, *Przegląd Elektrotechniczny*, 86 (2010), nr 7, 95-97

[4] Eason R., Digital Steganography, Proc. of Pacific Rim Workshop on Digital Steganography, (2002), 1-6

[5] Kopniak P., Zabezpieczenie informacji poprzez jej ukrycie-steganografia i jej narzędzia, W: Bezpieczeństwo informacji: od teorii do praktyki, Marek Miłosz, Warszawa, MIKOM, (2005), 145-156

Authors: *student Nadzeya Urbanovich, engineer Vlarimir Plaskovitsky, Belarusian State Technological University, 13a Sverdlova Str., 220000 Minsk; E-mail: nadya_ur@rambler.ru.*