Д.О. Деденев, Ю.А. Паздникова
Уральский федеральный университет имени первого Президента России Б.Н. Ельцина
г. Екатеринбург, Россия

Защита от стеганографических атак

Данная статья демонстрирует один из методов реализации стеганографической системы, а именно, используется метод под названием «Наименьший значащий бит» (LSB). Реализация этого метода наглядно демонстрируется недокументированным применением в ПО, что может являться причиной различного рода проблем. Результатом работы является демонстрация возможностей подобного рода ПО, а также приведены советы по уменьшению рисков возможного нападения.

Protection from steganographic attacks

Steganography is translated from Greek as «hidden, secret writing», and its use conceals the fact of information transmission [1].

In recent years, the aim of using this method has changed. Nowadays not only hidden information can be transmitted, but a set of commands that can bring harm to the system.

Then, there is an example of one way of secure transmission of a command and its execution on the machine of the "victim". To implement this method you will need:

1. The software which records the information into the last bits of the container.
2. Presence of the program, which will extract the information from the container, at the "victim`s".

To model this situation, assume the following:

- used operating system - Windows, which supports the NET Framework 4.5;
- the "victim" has a program on the workplace that retrieves information from a container;
- the "User Account Control" is disabled, and the work is carried out by a system user with administrative rights.

The structure of the steganography

The basic elements of any steganographic system are:

- message - as a transmitted message there will be used a command, showing the possibilities of the software;
- container – an object used to transmit the message, which is embedded in a special way;
- steganographic channel - a channel through which the container filled with the message will be transferred. The Internet will be a transmitting channel, by means of which the filled container will spread out.

Implementation of the LSB method

From the title itself, it`s clear that the values of the least significant bits vary depending on the implementation of the method [2]. As an object of message transmission there will be an image. The image format must be the one that does not produce data compression formats such is PNG and BMP.

One pixel is represented by three numbers (Fig. 1), which characterize the red, green and blue components of the color, which values are in the range from 0 to 255. If we change the last bit while representing these numbers in binary format, this modification will not be noticeable to the eye. Consequently, the last bit will be changed in further investigation.

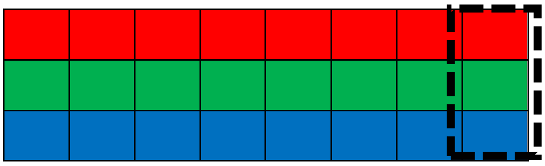
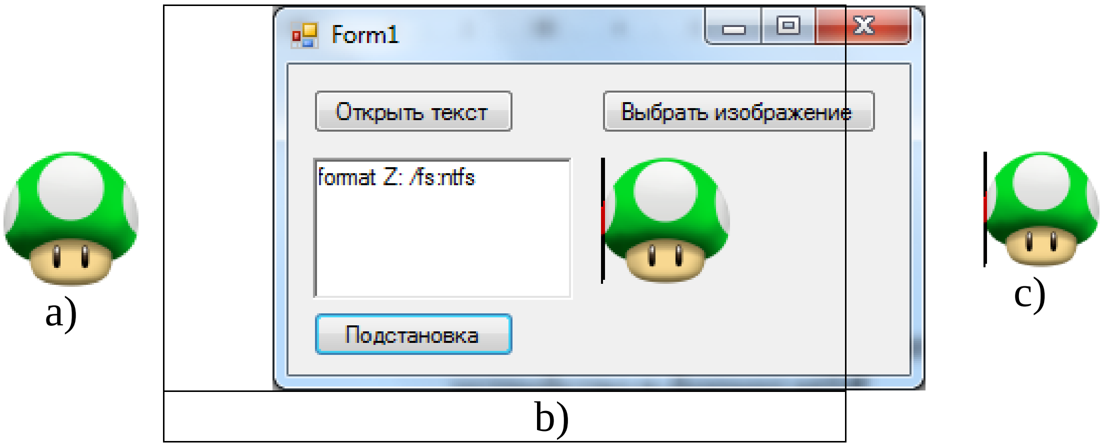


Fig. 1. Presentation of the pixel

For the representation of the text in a bit sequence ASCII was selected as a coding table. As a result, the numbers are represented in decimal form and then, divided into 2, in binary form. After receiving a sequence of binary messages, the values of the red channel were taken from the top-left pixel in the image to down column by column, and these numbers are represented in binary form, which changes the value of the last bit to the value that the binary sequence of the message had before.

As an implemented command we can take the following: format D: / fs: ntfs - formats a disk partition or removable USB drive into ntfs format.

The image of size 64x64 px was taken as the initial container (Fig. 2a). As a result of the substitution (Fig. 2b) (for better visualization the red channel is shown (Fig. 2c)), and all the rest - reset.



format Z: /fs:ntfs

Fig. 2. a) before the command insertion; b) the program work;

c) the field of command substitution after the command insertion

After the image is received the victim browses it with a program in which it is possible to read out the last bits and receive text information from them. For example, when you click “Open” (Fig. 3a) and select the desired image, the code which is responsible for processing and running the command line of a parameter, stored in the message, starts working (Fig. 3b).

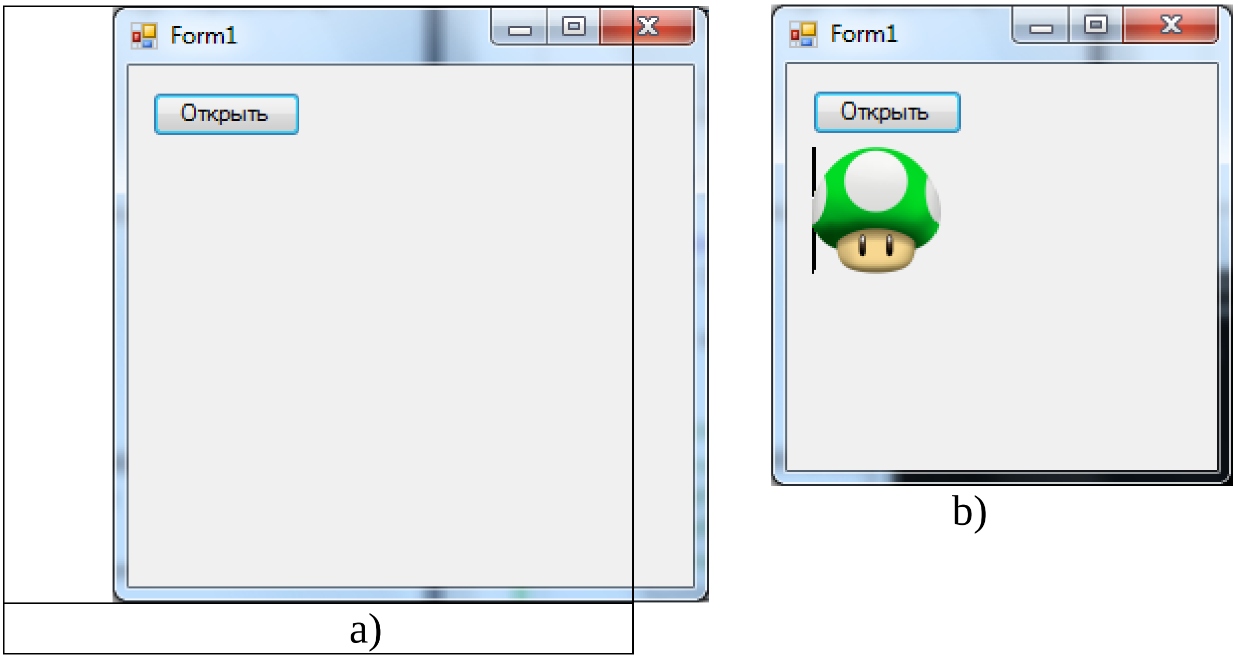
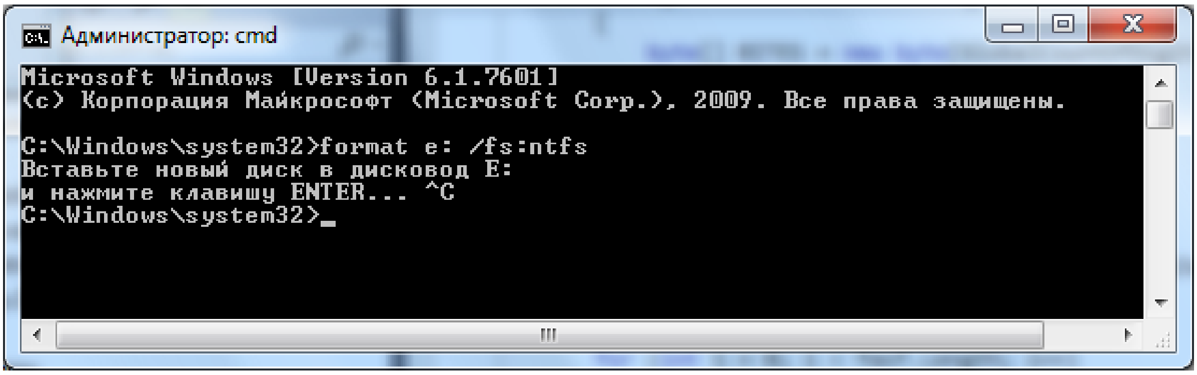


Fig. 3. a) the launch of the program handler; b) the view of the image

As a result, the next command is executed (Fig. 4).



```
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Windows\system32>format e: /fs:ntfs
Вставьте новый диск в дисковод E:
и нажмите клавишу ENTER... ^C
C:\Windows\system32>_
```

Fig. 4. Implementation of the transmitted command

The attacks of this kind are carried out by counterfeit software that is either a conversion of a licensed software with disabled activation functions or a key generator received from a pirated site. Also, the fact that the described features may be seen in the projects with a closed source pursuing venal aims, cannot be excluded.

And even if the software is licensed, do not forget about the fundamentals of security policy, with a reasonable adjustment of which it is possible to avoid fatal consequences for both the computer and the local network, where it can be located.

Список литературы:

1. Fridrich J. Goljan M. Du R. Reliable detection of LSB steganography in color and grayscale images / M.: Proceedings of the 2001 workshop on Multimedia and security: new challenges. – ACM, 2001.
2. Pierre-Marc B. Advances in malware covert communication channels, conference BlackHat. URL: https://www.blackhat.com/docs/eu-15/materials/eu-15-Bureau-Hiding-In-Plain-Sight-Advances-In-Malware-Covert-Communication-Channels-wp.pdf (дата обращения: 01.12.2015).