Computer-aided system of data protection by steganography methods

Kiseleva A.V., Kudrina M.A.

Samara State Aerospace University

Abstract. The article contains the description of the computer-aided system which allows to hide information by means of steganography methods. The system involves methods of hiding text information such as LSB, Koch-Zhao method, and method of Kutter-Jordan-Bossen, as well as the method of hiding color bmp images.

Keywords: steganography methods, data hiding, information security, data protection

Citation: Kiseleva A.V., Kudrina M.A. Computer-aided system of data protection by steganography methods. Proceedings of Information Technology and Nanotechnology (ITNT-2015), CEUR Workshop Proceedings, 2015; 1490: 277-284. DOI: 10.18287/1613-0073-2015-1490-277-284

1. Introduction

Modern society faces an up-to-date problem concerning the means which help to protect confidential information when it is stored or sent. The steganography is one of ways of data protection.

Steganography involves hiding message in such a way that the casual observer would not be able to detect the hidden information.

Due to the increase of global computer networks role, the value of steganography becomes more and more important. Now steganography systems are actively used for the solution of the following main tasks [1]:

- protecting confidential information against unauthorized access;
- overcoming the monitoring and management systems of network resources;
- camouflaging the software;
- copyright protection of some types of intellectual property.

2. Theoretical part

The *steganography system* is a set of means and methods which are used for formation of the hidden channel of information transfer [2, 3]. The *embedded-message* or *payload* is something to be hidden in something else. Any type of information can be used as the embedded-message: texts, images, videos, etc.

The *carrier* or the *cover message* is the signal, stream, or data file that hides the embedded-message. The resulting signal, stream, or data file with the encoded payload is called the *package* or *stego-file*.

Computer steganography methods can be divided into two basic classes in accordance with the hiding principle: methods of direct replacement and spectral methods. Methods of direct replacement use redundancy of data environment and consist in the replacement of insignificant part of the cover message with bits of the embedded-message. Spectral methods of data hiding use spectral representations of the environment elements with the embedded-message within the environment structure.

LSB method

The method of replacement of *Least Significant Bits* (*LSB method*) is the most common nowadays. The method consists in replacing final bits in cover message bytes with bits of the embedded-message. The difference between empty and filled cover message has to be imperceptible for the human perception system [4]. The scheme of LSB method is shown in figure 1.

Method of Kutter-Jordan-Bossen

This method is based on the peculiarity of human visual system, which consists in low susceptibility of a human to changes in brightness of blue color in comparison with red and green colors.

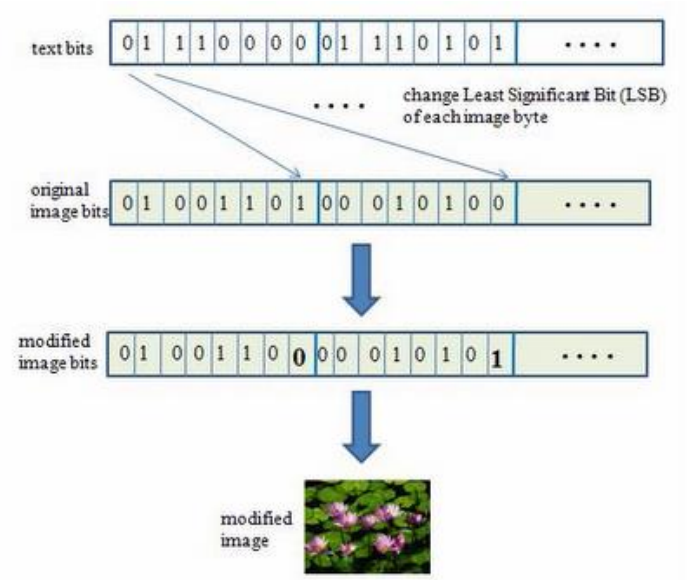

Fig. 1. – The scheme of LSB method

One bit of the embedded-message is written to one pixel of the cover message. The brightness of red and green components of pixel remains unchanged, but the brightness of blue component changes in accordance with the following formula [5]:

$$B^*_{x,y} = \begin{cases} B_{x,\,y} + \lambda Y_{x,\,y}, \text{ if } m_i = 1, \\ B_{x,\,y} - \lambda Y_{x,\,y}, \text{ if } m_i = 0, \end{cases} \quad (1)$$

where $B_{x,y}$– the brightness of blue component of the pixel with coordinates (x,y);

$B^*_{x,y}$ – the changed brightness of blue component of the pixel with coordinates (x,y);

$Y_{x,v} = 0.29890R_{x,y}+0.58662G_{x,y}+0.11448B_{x,y}$ – pixel brightness;

$R_{x,y}$ – the brightness of red component of the pixel with coordinates (x,y);

$G_{x,y}$ – the brightness of green component of the pixel with coordinates (x,y);

m_i – i-bit of the embedded-message;

$\lambda = 0.1$ – the coefficient setting the energy of the built-in bit of data (it is set depending on the functional purpose and features of steganography system). When λ increases, the embedded-message becomes more apparent, but it is more resistant to distortions.

Since the recipient doesn't have the original image, it is impossible to find out whether the brightness of blue component increased or decreased. Therefore, in order to extract the information, brightness of blue component should be predicted [6]:

$$\overline{B}_{x,\,y} = \frac{\sum_{i=1}^{\sigma} (B_{x,\,y+i} + B_{x,\,y-i} + B_{x+i,\,y} + B_{x-i,\,y})}{4\sigma}, \quad (2)$$

where $\sigma = 1 \div 3$ – the size of the area on which brightness will be predicted.

The following formula is used for extracting the embedded-message:

$$m_i = \begin{cases} 1, \text{if } B^*_{x,y} > \overline{B}_{x,y}, \\ 0, \text{if } B^*_{x,y} < \overline{B}_{x,y}. \end{cases}$$

Koch-Zhao method

Koch-Zhao method uses frequency characteristics of the cover message and consists in relative replacement of the discrete cosine transformation (DCT) coefficients. The image is divided into blocks with dimension 8×8 pixels and DCT is applied to each block. Each block is suitable for recording one information bit [7]. This method has high resistance to image distortion, even to its significant change, but it can't be used for hiding large volumes of data.

Hidden transmission of color images

24-bit bitmap-pictures are used as input images; each color contains 8 bits of information. The data are hidden by using LSB method. The essence of the algorithm is that the secret image is divided into three color primitives (tints of red, green and blue), and then each primitive is put into the least significant bits of one of image containers. Thus, after the data is hidden, each cover message will contain only one color component of the secret image [8-10].

Two most significant bits from each color primitive of the secret image are recorded to the least significant bits of the corresponding color of the corresponding carrier. In figure 2 you can see the illustration of the method of image hiding. Two least significant bits of other colors are nulled. This operation is repeated for each pixel.

To restore the secret image, you need to take the first pixel from each carrier. Two least significant bits of each color component of this pixel are becoming the most significant bits and corresponding color components are added. This operation is repeated for each pixel and secret image is restored.

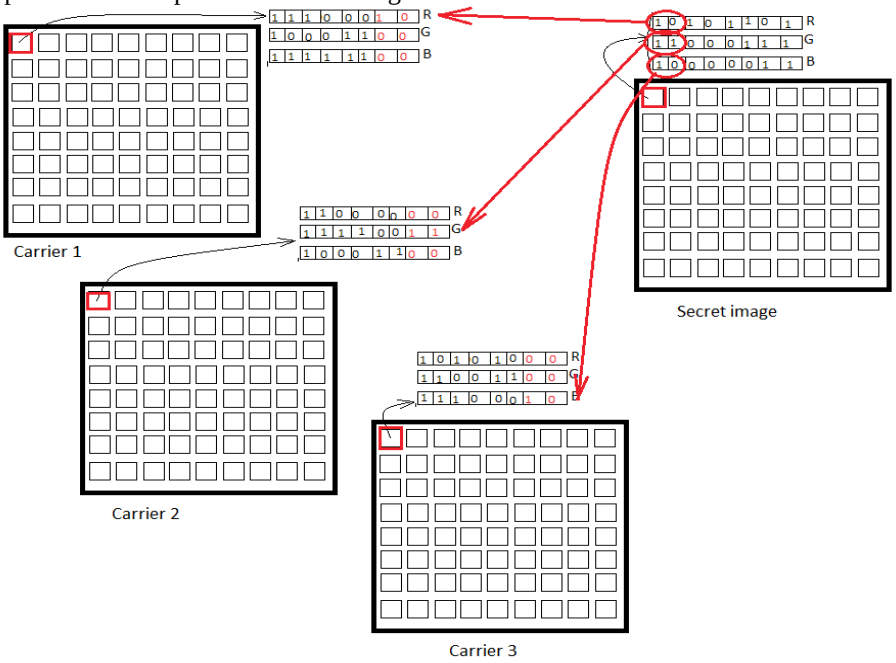

Fig. 2. – Illustration of the method of image hiding

3. Realization of the system

The researched carried out within the frame of bachelor's final qualifying work initiated the development of computer-aided system of data protection, which hides information using steganography methods. This system allows you to select a container for embedding information, to choose an embedding method, to create a stego-file and to extract secret information from the stego-file.

The system performs the following functions:

- embedding text information;
- embedding an image;
- extracting text information;
- extracting an image.

After the system starts, the window for embedding messages opens and the user can click "Load Container" in the menu and select a file to download. The selected image will be displayed on the screen. After that the user has to choose an embedding method, for example, LSB, and click on "Write" button to enter the secret message. After embedding, the user can save the filled cover message. For extraction of the embedded message, it is necessary to pass to "Read the message" tab. Click on "Read" button, select the file, and the secret message appears in the text field.

To hide an image, the user needs to go to the tab "Hide the picture" (see figure 3), to load three containers and the secret image. All images will be displayed in the form. The user needs to select the number of replaceable bits. It influences the quality of the stego-file and the extracted message.

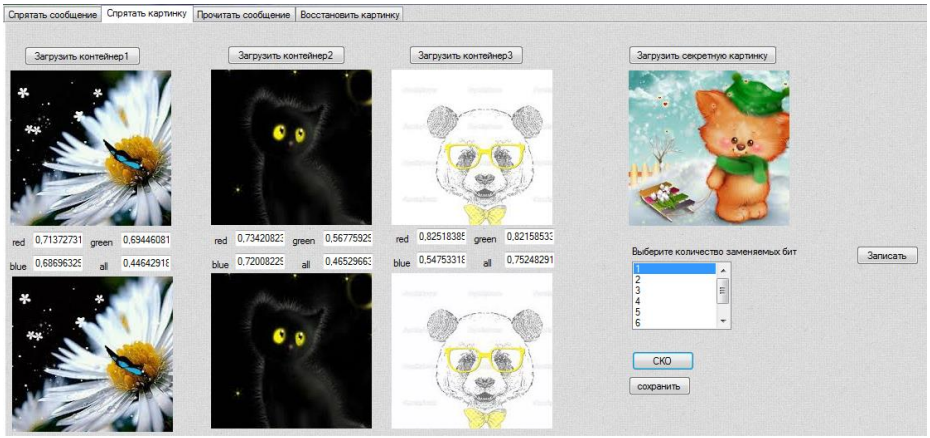

Fig. 3. – Embedding the image using 1 bit of container color

Select the number of replaceable bits which equals 1, press "Save" button and save all of the containers.

To restore the image, it is necessary to pass to tab «Restore image», to load containers and to press «Restore» button.

4. Experimental part

The carried out research demonstrated how the number of replaced bits in RGB components of the container pixels influences the quality of the restored image and container distortion.

Figures 4 - 6 illustrate results of LSB-algorithm with 1, 4 and 8 replaced bits.

It's clear that 1 bit replacement distorts the secret image considerably, but the change of the containers is invisible. When 4 bits are replaced, the secret message is distorted slightly, but embedding can be noticed in the containers. When 8 bits are replaced, the secret image can not be transmitted unnoticed because containers are RGB components of the secret image. Furthermore, when the amount of replaced bits

is the same (e.g., 4), the distortion can be seen better in the light container than in the dark one.

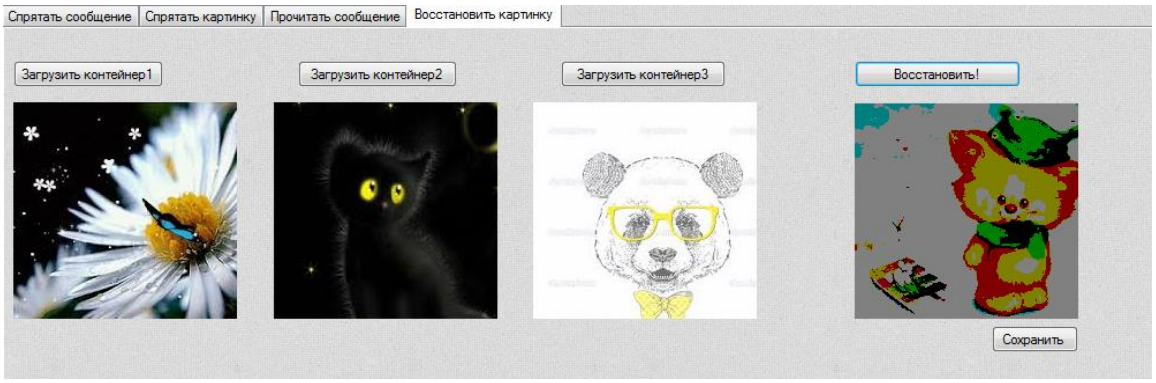

Fig. 4. – Restoring the image with 1 replaced bit

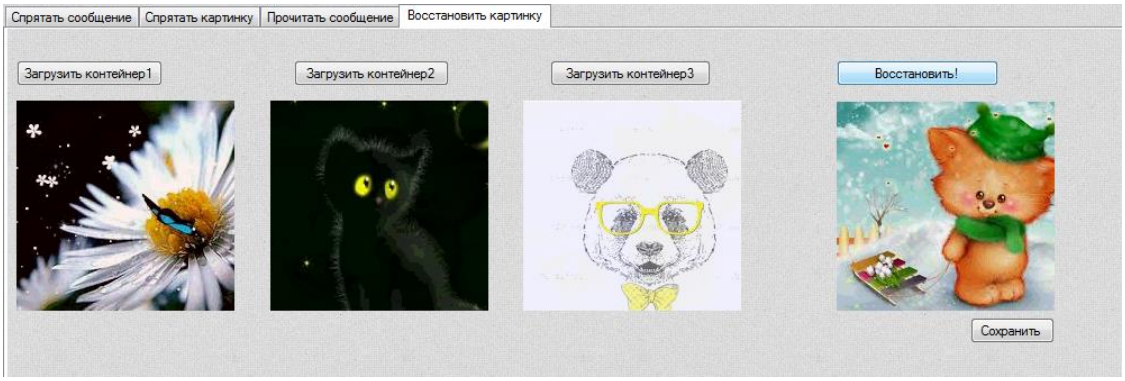

Fig. 5. – Restoring the image with 4 replaced bits

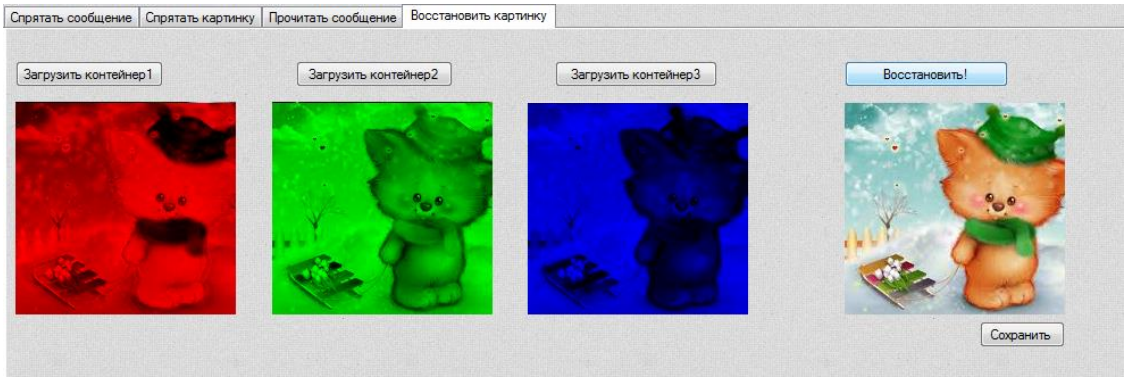

Fig. 6. – Restoring the image with 8 replaced bits

Figures 7-8 are dependency graphs which illustrate the relation between mean-square-error of RGB container distortion and the number of replaced bits in containers, presented for the dark and the light image containers respectively.

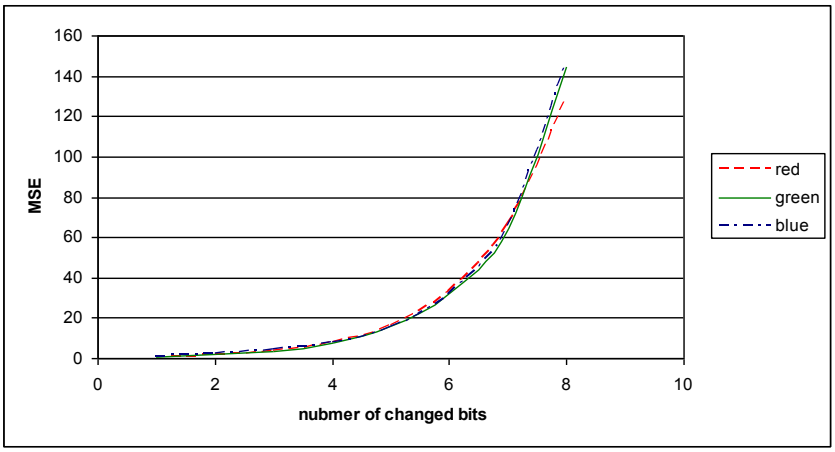

Fig. 7. – Dependency graphs of MSE distortion and the quantity of changed bits for the dark container

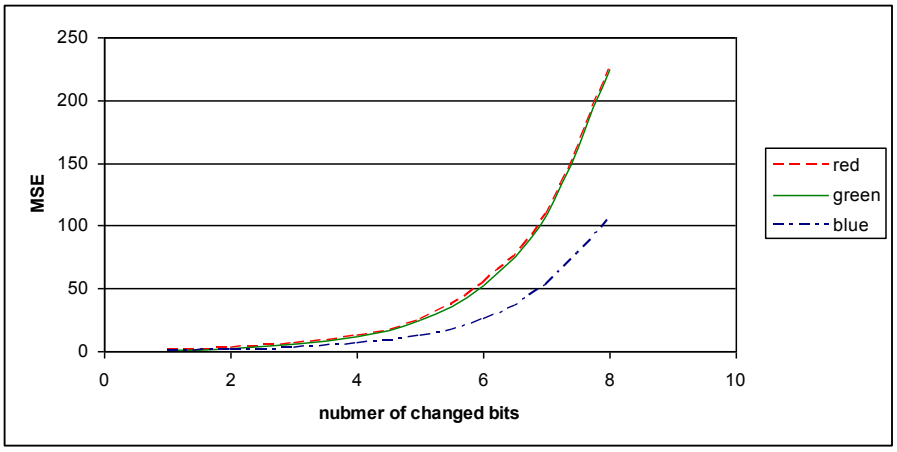

Fig. 8. – Dependency graphs of MSE distortion and the quantity of changed bits for the light container

Mean-square-error (MSE) is calculated using the following formula:

$$MSE = \sqrt{\frac{\sum_{i=1}^{n}\sum_{j=1}^{m}(x_{i,j} - x^{*}_{i,j})^2}{m \cdot n}}, \quad (3)$$

where n – the length of the image;

m – the width of the image;

$x_{i,j}$ – the value of pixel color component of the original image;

$x^*_{i,j}$ – the value of pixel color component of the modified image.

The graphs show that the increase in the number of changed bits leads to MSE increase. In addition, it is evident that mean-square-error for the light image is larger than for the dark one.

Thus, it can be concluded that darker images serve better in the function of containers and the number of bits should be restricted to 3-4. Following these recommendations will help to achieve the best balance between the quality of the transmitted image and the degree of distortion of containers.

5. Conclusion

The researched carried out within the frame of bachelor's final qualifying work implied the study of steganography methods and the development of computer-aided system of data protection by means of the following steganography methods: LSB method, Koch-Zhao method, Kutter-Jordan-Bossen method and the method of color bmp images hiding.

References

1. Steganography yesterday, today and tomorrow. Source: <http://www.ess.ru/ sites/default /files/files/articles/1998/0405 /1998_0405_03.pdf >. [in Russian]
2. Basic principles of steganography. Source: <http://citforum.ru/internet/securities/ stegano.shtml>. [in Russian]
3. **Pfitzmann B.** Information hiding terminology. Lecture Notes in Computer Science, 1996; 1174: 347-350.
4. Replacement of the least significant bit, or LSB. Source: <http://www.nestego.ru/2012/07/lsb.html>. [in Russian]
5. Modification of Kutter-Jordan- Bossen method of information hiding. Source: <http: //www.amursu.ru/attachments/article/11563/11.pdf>. [in Russian]
6. Kutter-Jordan-Bossen method of steganography. Source: <http:// habrahabr.ru /post/115287/>. [in Russian]
7. Koch-Zhao method of steganography. Source: <http:// habrahabr.ru /post/216207/>. [in Russian]
8. Visual cryptography for color images. Source: <http://habrahabr.ru /post/121878/>. [in Russian]
9. **Dryuchenko MA, Sirota AA.** Steganography algorithm for information hiding based on spatial deformation of full-color image fragments. Computer Optics, 2014; 38(4): 833-842. [in Russian]
10. **Glumov N, Mitekin V.** A new semi-fragile watermarking algorithm for image authentication and information hiding. Computer Optics, 2011; 35(2): 262-267. [in Russian]