UDC 004.056.5

DESIGNING THE STEGOSYSTEM, BASED ON HIDING TEXT DATA IN IMAGES BY USING DISCRETE TRANSFORMATIONS

A. KOHANOVSKIY, Y. PASTUHOV
Polotsk State University, Belarus

The article presents a practical way of creating a reliable stegosystem with an unconventional way of hiding information. The purpose of this work is to build a system based on hiding text messages in images, as well as to study the attacks and to find out, whether such a system is suitable for practical usage.

Introduction. This article is about hiding data in images using one of the methods of steganography. Digital steganography refers to the concealment of one information in another. Moreover, concealment must be implemented in such a way that, first, the properties and some value of the hidden information are not lost, and secondly, the inevitable modification of the information carrier not only does not destroy the semantic functions, but also at a certain level of abstraction does not even change them. Thus, the transmission of one message within another is not detected by traditional methods.

Both spatial and frequency parameters of the image container can be subjected to steganographic modification. All these parameters are suitable for steganographic modification, but before the embedding procedure, it is necessary to evaluate the limits of modification of parameters of a container, as well as the distortions introduced in this case. The throughput, reliability, and stability of the steganographic system will largely be determined by the degree of modification of the image container [1].

The principle of a steganographic system designing and the description of the data hiding algorithm. The standard steganographic scheme is maintained regardless of the technology that implements it. The stegosystem performs the task of embedding and selecting messages from other information. The stegosystem consists of the following main elements (fig. 1).

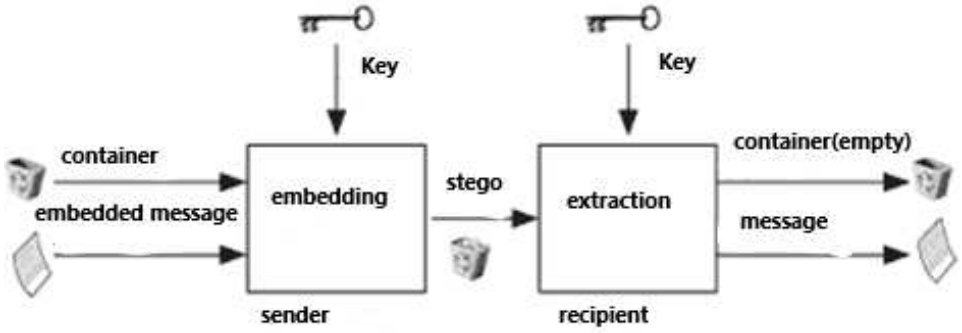


Figure 1. – Block diagram of a typical stegosystem

As the data may be any information: text, message, image, etc., Container any information that is intended to conceal secret messages. Empty container - a container without an embedded message; a filled container or stegocontainer containing embedded information. Embedded (hidden) message - a message that is embedded in a container. Steganographic channel - stego transmission channel. Stegokey or just the key - the secret key is needed for hiding information. Depending on the number of security levels (for example, embedding a pre-encrypted message), the stegosystem may have one or more keys.

Data containing a hidden message may be subject to deliberate attacks or accidental interference. As shown in figure 1, the stegosystem combines two types of information so that they can be distinguished by two fundamentally different detectors. One of the detectors is a digital watermark selection system, and the other is a human [5].

Steganographic replacement methods are unstable to any distortion, and the use of lossy compression operation leads to the complete destruction of all secret information hidden by the method of the Least Significant Bit of the image. More resistant to various distortions, including compression, are methods that use a frequency domain rather than a time domain to hide data [2].

The vast majority of computer steganography methods are based on two key principles:

– files that do not require absolute accuracy (in this case, image files) can be modified without losing their functionality;

– the human senses are unable to reliably distinguish minor changes in files modified in this way, and / or there is no special tool that would be able to perform this task.

The basic approaches to implementing computer steganography methods within an information environment are based on selecting insignificant fragments of this environment and replacing existing information with information that needs to be hidden.

Considered in this paper, the Koch-Zhao algorithm for embedding information uses the frequency domain of the container and consists in the relative replacement of the values of the coefficients of the discrete cosine transformation (DCT) [3].

The image is divided into 8×8 blocks (in our case, 2×2, 3×3, and 4×4 blocks) of pixels, and a Discrete Cosine Transform is applied to each block. Each block is suitable for recording one bit of information.

The hiding algorithm will be as follows:

- iterate the image with a double array in 8 steps;
- at each iteration, we create a temporary array of 8×8 pixels, each element of which will be a set of three pixel colors;
- we apply a DCT to this array, and get an array of coefficients of size 8×8;
- select 2 coefficients and calculate their difference modulo;
- if the difference is less than or equal to 25, then assign the first coefficient a positive value of the second + constant, or the same, but with a minus sign (this is called bit transfer);
- if the difference is less than or equal to -25, then we perform the same actions only for the second coefficient;
- then the reverse DCT is applied to translate our coefficients back into the spatial domain;
- then copy the color values to the image.

Advantages of the method:

- resistance to JPEG compression with a low compression ratio.

Disadvantages:

- noticeable visual distortion of the container image with a large threshold value of the difference between the DCT coefficients of the blocks;
- small message size than can be embedded.

Estimation of the implemented system stability. Each image has unique properties that can be used as a basis for dividing them into classes.

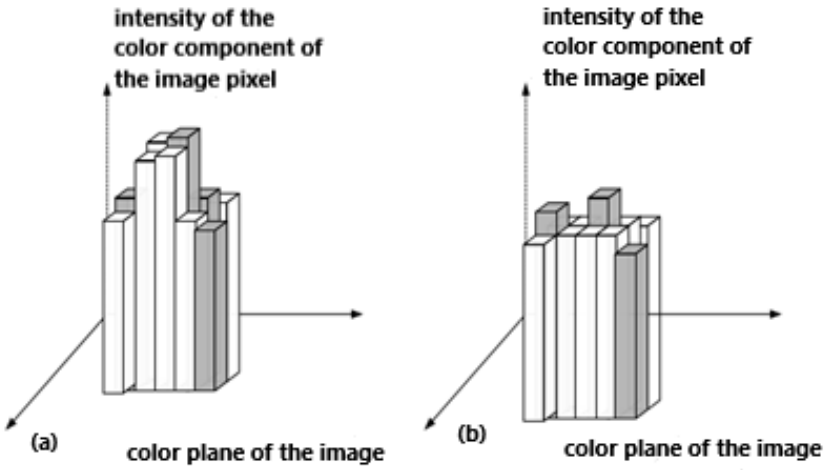
1. Images with a small number of colors (4-16) and large areas filled with a single color.
2. Computer-generated images with smooth color transitions.
3. Photorealistic images.
4. Photorealistic images with business graphics overlay.
5. Map images.
6. Space images.

To ensure that data is hidden in image containers, you must select images that contain areas with sharp color transitions and object borders, since they can hide small changes in the intensity of the color components of the container pixel in relation to neighboring pixels (fig. 2). Modified pixels in the drawing are grayed out. You can see that even a slight change in the intensity of some color component of individual pixels, in areas filled with a single color (fig. 2B), increases the possibility of visual or computer detection of the fact of steganographic data hiding.

It is advisable to analyze the contents of image containers using a mathematical transformation that allows you to select its frequency parameters and evaluate the contribution of individual frequencies to the image composition. One of these transformations is the discrete cosine transform [3], which is applied to images by means of n×n pixel windows. Discrete cosine transformation allows you to get information about sharp and smooth borders of image colors, areas filled with a single color or with a gradient color change, etc.

It is advisable to assess the suitability of the image for steganographic modification in two stages.

At the first stage, images are divided into classes according to the relative weight of their spatial frequencies. Positive results were obtained using spectral classification of images, which allows them to be divided into 8 classes [4]. Classes 1 through 3 describe images with the highest relative weight of low frequencies; classes 4 through 7 differentiate images by spectral components concentrated in areas close to the low-frequency and / or high-frequency ranges; the eighth class separates images that have a uniform spectrum within the entire considered range.



(a) the region of sharp transition of colors,
(b) area filled with a single color

Figure 2. – Color planes of modified image areas

In the second stage, the throughput of the container image is evaluated by excluding areas that are not suitable for modification, such as those filled with a single color or a gradient color change. It is possible to detect such regions in an image when analyzing its spectral composition (the presence of borders in the image leads to an increase in the contribution of medium and high frequencies), and when evaluating changes in the intensity of a pixel in relation to neighboring pixels.

In the Koch-Zhao method, it is undesirable to use images with a small number of colors and large areas filled with a single color (in particular, white) to ensure that data is hidden in image containers. Since in this case, after encryption, the image will clearly show the fact of hiding information.

The following types of attacks are distinguished for the Koch-Zhao method:

1. Attacks against the embedded message, directed to removal of or damage to the integrated information through the manipulation of the filled container. The attack methods included in this category are not aimed at evaluating and highlighting the message. Examples of such attacks in this paper are image compression.
2. The attack against the embedded message is directed to the use of filters. In this case, the message remains in the image, but the ability to receive it is lost. This category includes attacks such as attacks using effects in various photo editors.
3. The attack against the embedded message is directed to the use of geometric transformations. This category of attacks is related to truncation and changing the dimension of our image.
4. An attack aimed at changing the brightness and contrast of an image. This type of attack is associated with a significant change in the image.

Conclusion. Research in the field of steganography is a very promising area of information protection, since in the modern world the task of transmitting secret information is on a par with hidden communication, i.e. hiding the fact of transmitting messages. Therefore, it is necessary to continue research in this area to find new, effective, methods or improve existing ones. In this paper, we considered the method of embedding information in images. The most promising method, however, requires improvement in terms of bandwidth, and the probability of correct extraction of embedded bits of information. The efficiency of using the Discrete Cosine Transformation in this method for image compression is explained by the fact that it well models the image processing process in the human vision system (HVS), separates the "significant" details from the "insignificant" ones. This means that it is more appropriate to use it in the case of an active violator. The software product is implemented and ready for use with the possibility of further development.

REFERENCES

1. Садов, В. С. Компьютерная стеганография / В. С. Садов. – М: МГВРК, 2012. – 289 с.
2. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин. – М.: СОЛОН-Пресс, 2002. – 272 с.

3. Тихоненко, С.Г. Формирование критерия качества фильтрованных изображений / С. Г. Тихоненко // Тезисы докладов IX республиканской научной конференции студентов и аспирантов РБ, Гродно, 26-27 мая 2004 г. В 8-ми частях / Гродненский гос. университет; редкол.: А. И. Жук. – Гродно, 2004. – Ч.6. – С. 241– 243. 40.
4. Чернявский, А.Ф. Оценка информационных потерь при фильтрации изображений / А.Ф. Чернявский, С.Г. Тихоненко, В.С. Садов // Информатика. – 2005. – № 3(7). – С. 52–59.
5. Matsui K., Tanaka K., and Nakamura Y. Digital signature on a facsimile document by recursive MH coding / Symposium On Cryptography and In-formation Security, 1989.