DOI: 10.5604/01.3001.0012.8016

DEVELOPMENT OF THE METHOD OF INDIRECT STEGANOGRAPHIC DATA HIDING IN THE CONTAINER IMAGE CONTOUR

Volodymyr Barannik[1], Oleg Shatun[1], Dmitriy Barannik[2], Veronika Kobtseva[2]
[1]Ivan Kozhedub Kharkiv National University of Air Force, Faculty of Automated control systems and aviation ground support,
[2]Kharkiv National University of Radio Electronics, Department of information and network engineering

Abstract. *The article discusses issues related to the use of methods of digital steganography for information security in systems of critical appointment. The advantages of using data embedding in an image container are shown. The main disadvantages of the existing methods of embedding in the image container are given. The issues of JPEG image compression for digital steganography are described. The allocation of stable regions in the attacking effects on the basis of the moving mask is proposed. The mathematical apparatus for masking images by the Sobel method is shown. The indirect steganography method of hiding data in blocks which contain information about the circuit is developed.*

Keywords image-container, image contour, discrete cosine transformation, indirect method

OPRACOWANIE METODY POŚREDNIEGO STEGANOGRAFICZNEGO UKRYWANIA DANYCH W INFORMACJI O KONTURZE

Streszczenie*. Artykuł dotyczy konieczności stosowania cyfrowych metod steganograficznych do ochrony informacji w systemach o krytycznym znaczeniu. Pokazano zalety używania osadzania danych w kontenerze w postaci obrazu. Przeanalizowano główne wady większości istniejących systemów steganograficznych. Rozważono problemy kompresji obrazów JPEG występujące przy steganografii cyfrowej. Zaproponowano przydział stabilnych obszarów w oparciu o przesuwną maskę. Przedstawiono aparat matematyczny do maskowania obrazów metodą Sobela. Opracowano pośrednią metodę steganograficzną polegającą na ukrywaniu danych w blokach zawierających informacje o konturze.*

Słowa kluczowe: kontener obrazu, kontur obrazu, dyskretna transformacja kosinusowa, metoda pośrednia

Introduction

In the modern world, information and telecommunication systems (ITS) are widely used for data transmission to ensure the efficiency and quality of information. In the operation of state agencies to enhance economic, defence and social impacts of the use of the system critical applications (SCA). The functioning of the SCA is characterized by the presence of an attacker who can carry out active actions [7, 8]. This can lead to a breach of confidentiality, leakage of important information and lead to significant material and human losses. Therefore, the protection of information in data transmission systems is one of the most important problems of modern science.

1. Analysis

Cryptographic data protection is used to encrypt information resources in the UPC, which provides reliable protection against unauthorized access [4, 10]. Since cryptography only encrypts, not hides, the enemy can intercept the encrypted message and distort it. Therefore, an alternative to cryptography is the use of digital steganography [9, 12].

Digital steganography (DS) is a direction of steganography that hides data in computer files that have analog origin. The most developed and common methods of DS are data embedding in the image-content (IC). This is due to the following reasons:

- distribution of images in the information space;
- the presence in the image of high redundancy, which can potentially be used for embedding information;
- relatively large capacity of the steganographic channel using IC;
- unfavourable human vision to minor distortions in color and brightness.

Methods of embedding data in the IC are divided into direct and indirect [9].

When hiding information in direct methods, bits are embedded in the images, which leads to distortion [1, 6, 11, 13, 14] and reduced container resistance to attacks. In indirect data hiding, information is embedded by creating dependencies between certain elements of the image [17]. These methods are more complex due to the presence of mathematical calculations, but are more resistant to attacks [3, 15].

The Editor reserves the right to editorial redaction of the submitted texts.

2. Problem formulation

Analysis of recent publications [2, 3, 6, 7] showed that the use of indirect methods of hiding data in images provides reliability and reliability of hidden data. The concept of indirect data concealment is based on the creation of image element dependency.

This occurs most often after carrying out a discrete cosine transform (DCT).

The use of prep when embedding information due to the fact that the existing image, the transfer process technology with JPEG loss, part of which is prep.

The generalized analysis of data embedding methods in IC showed the following disadvantages:

- existing methods do not meet the requirements for the steganographic container capacity;
- the methods used are unstable to known attacks on the steganographic system;
- visual analysis of low-level imagery;
- methods have a low probability of correct data extraction.

The above mentioned disadvantages lead to a decrease in the resistance of steganosystems and the probability of loss of information when transmitting through channels [18].

Thus, it is necessary to use a method of hiding data, which will increase the resistance of the container to attacks and increase the probability of correct data extraction.

The basis of this approach is proposed to apply blocks that will be resistant to attacks and will not be distorted during transmission. Therefore, the purpose of the article is to develop a method of hiding data in stable blocks of the image contour, namely elements that contain information about the contour.

3. The allocation of persistent fields based on moving mask

For digital images, the most useful semantic loads are the contours of objects. Contours are lines that pass at the boundaries of homogeneous regions. Elements $\{z_{ij}\}$ of the spatial-temporal representation of the image, whose values do not exceed a certain threshold, form homogeneous areas [19]. This is set by the following condition:

$$|z_{\max} - z_{\min}| \le 1, \tag{1}$$

where $z_{\max}$ is the largest element of the image area; $z_{\min}$ is smallest element of the image.

Existing image compression algorithms reduce redundancy and, thus, introduce the smallest distortion that, while maintaining a high level, provides a disadvantageous human vision to distortion [6, 16]. Therefore, to identify areas resistant to compression effects, it is necessary to use methods of image contour selection, for their further use in steganographic embedding.

The contours of the images are formed at the boundaries of homogeneous areas of the image [5]. In order to determine the belonging of the elements of the spatial representation of the image to a homogeneous area at the same time checking the presence of the contour, the following conditions must be met:

- belonging of the image element to a homogeneous area is given by the condition:

$$|z_{i,j} - z_{i\pm1,j\pm1}| \le 1, \tag{2}$$

$i = \overline{1,x},\ j = \overline{1,y}.$

- belonging of the image element to the adjacent homogeneous region is given by the condition:

$$|z_{i,j} - z_{i\pm1,j\pm1}| > 1, \tag{3}$$

$i = \overline{1,x},\ j = \overline{1,y}.$

Most often used in practice for the selection of image contours and gradient methods.

The most common way to find contours is to process the image *Z* with a sliding mask *K*. The mask *K* is a square matrix with coefficients {k}. The process of image processing *Z* based on the matrix *K* is called filtering or masking and is given by the following functionality $f(\bullet)$:

$$M = f(Z,K), \tag{4}$$

where M is image obtained from the processing of the image *Z* based on the mask K. The filtering process is based on the gradual spatial movement of the filter mask from the element to the image element. The value of the $m_{i,j}$ (filter response) element is calculated using the values of the previous and subsequent elements in two-dimensional space. In this case, the value of the element mi, j of the image M, obtained as a result of masking is calculated by the formula:

$$m_{i,j} = \sum_{\xi=i-1}^{i+1} \sum_{\tau=i-1}^{\tau+1} z_{\xi,\tau} \cdot k\,. \tag{5}$$

The Sobel operator is proposed to be used as a method of image contour selection. This operator is most often used in practice and has the following form:

$$m_{i,j} = \sqrt{G_i^2 + G_j^2}\,, \tag{6}$$

$$G_i = K_i \cdot m_{i,j} = \begin{bmatrix} -1 & 0 & +1 \\ -2 & 0 & +2 \\ -1 & 0 & +1 \end{bmatrix} \cdot m_{i,j}; \tag{7}$$

$$G_j = K_j \cdot m_{i,j} = \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ +1 & +2 & +1 \end{bmatrix} \cdot m_{i,j}. \tag{8}$$

where K_i and K_j are operators that determine the increment value of an image element horizontally and vertically, respectively; G_i and G_j are blocks of the image each element of which contains approximate values of derivatives horizontally and vertically, respectively.

Thus, the use of a sliding Sobel mask allows identifying the contours of objects at the boundaries of homogeneous areas [9]. It is proposed to use this technology to identify areas that will be used in steganographic embedding.

4. Embedding data in areas resistant to compression attacks

We will formulate the requirements for the developed method.

This method should ensure the reliability of hiding information in images, embedding a relatively large amount of information and resistance to distortion. Therefore, it is proposed to build the view steganographic embedding, by indirect modification of the elements of the image blocks that contain contour information.

Step 1. You must select the contours of the image to embed the data.

When selecting contours, it was found that the elements that are located on the positions of the contours, the detection that uses the image mask have the following properties:

1) a limited number of elements that contain contour information, that is, the area of values for embedding information is limited by the width of the contour. In most cases, the contour is not wide (Fig.1);

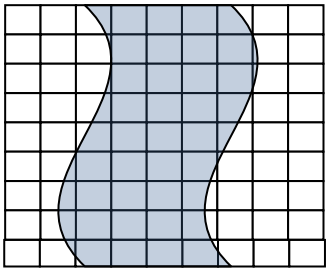

Fig. 1. The width of the contour image

2) through a large number of contours in the image, for the successful integration of data in steganographic transformations, it is necessary to take into account the different directions of the contour of the image: vertical and horizontal (Fig. 2)

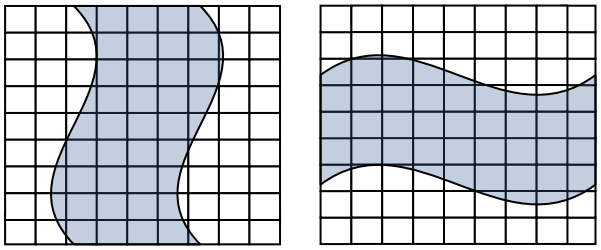

Fig. 2. The direction of the contour depicted (left: vertical position, right: horizontal position)

Step 2. Consider the possible options for selecting the matrix of contour elements for embedding information, taking into account these features.

It is necessary to consider that the allocation of a smart block to be embedded in the contour image, it can get items that are not part of the contour elements.

In this case, when sending a message, the data contained in the IC may be damaged. That is, when choosing a block with dimensions of 4×4 or 5×5 and embedding information in it, the messages will go beyond the contour, which does not meet the requirements for the developed method (Fig. 3).

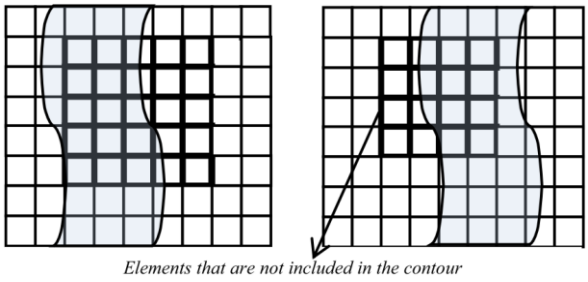

Fig. 3. Example of selection of blocks for embedding

It follows that the most optimal size of the contour for embedding is a matrix of dimension 3×3 elements (Fig. 4).

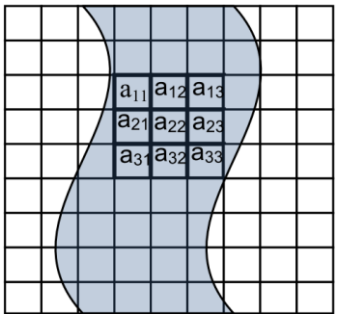

Fig. 4. Choice of the block for embedding data

By selecting the appropriate block and selecting the matrix a 3×3 it is necessary for further calculations to determine the following elements:

- no variability in the process of embedding (reference elements);
- elements that are modified in the process of embedding.

To select the elements that will not change during the implementation process, you must do the following:

In matrix A, the maximum and minimum elements should be defined.

These elements will remain unchanged for the selection of the interval on which the data is embedded.

$$A = \begin{matrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{matrix}. \tag{9}$$

For example, $a_{12} = a_{min}$, $a_{32} = a_{max}$.

Calculate the width of the interval d. This value is required to calculate the interval boundaries and is characterized by the dynamic range of elements in the block matrix. Determined by the formula:

$$d = \frac{a_{\max} - a_{\min}}{3} \tag{10}$$

Step 3. At this stage, the interval boundaries are calculated. These elements are used for comparison. These elements are not modified in the process of data embedding – reference elements, they are used in the process of creating a dependency in indirect embedding. Since the range of values must be divided into 3 intervals, it is necessary to determine the 4 reference elements. These elements are calculated by the formula:

$$z_i = a_{\min} + d(i-1) \tag{11}$$

where z_i is a reference element for comparison, i = [1,4].

Step 4. The items that are selected for embedding of the matrix A, which will be involved in embedding distributed according to intervals. These elements are allowed to change in the process of embedding data modificam elements. The modifier elements must be placed in ascending order and their belonging to the intervals between the reference elements $\{z_i\}$, $i = \overline{1,4}$.

Step 5. It is necessary to calculate the average value of the SJ modifier elements that fall within the interval between two reference elements $\{z_i\}$, $i = \overline{1,4}$. These values will be used for further embedding of the data using the modifier elements.

The calculation of this value is necessary to create a dependency on the embedding of the data. This value is calculated by the formula:

$$S_j = \frac{\sum_{m=1}^{n} a_m}{n}, \tag{12}$$

where j is number of the interval j = [1,3]; a_m is matrix modifier element m = [1, n]; n is number of elements in the interval.

Step 6. To implement indirect embedding of information in the image contours, it is necessary to calculate the reference coefficient K.

This coefficient is constant, that means, it will not change from the modification of the block elements. This coefficient is calculated for each embedding block separately, takes the values $0 < k \le 1$ and is calculated by the formula:

$$k = \frac{z_4}{z_2 + z_3} \tag{13}$$

Data embedding will be performed by modifying the elements of the block according to the rule:

$$b = \begin{cases} 0, \ if\ H > k; \\ 1, \ if\ H \le k. \end{cases} \tag{14}$$

where b is the bit to be embedded in this loop block; H is the coefficient of comparison, and is calculated by the formula:

$$H = \frac{S_3}{S_1 + S_2} \tag{15}$$

If the condition is met, the data injection is complete. That is, it is assumed that the elements have values that satisfy the embedding condition.

Consider cases where the embedding condition does not hold.

Failure to comply with the rules of the embedding of H should increase or decrease for the condition of embedding. Then the rule of embedding will have the following form:

$$b = \begin{cases} 0, if\ H = \dfrac{S_3 + x}{(S_1 - x) + (S_2 - x)} > k; \\ 1, if\ H = \dfrac{S_3 - x}{(S_1 + x) + (S_2 + x)} \le k. \end{cases} \tag{16}$$

where x is modification factor $x \in [-255; 255]$.

Implementation will be the selection of the values of H thus, to ensure the performance of condition 16.

The values of the modified elements a'_{ij} of the block contain information about the contour and is calculated by the following formula:

$$a_i' = a_i + x. \tag{17}$$

The value of x is calculated by the formula:

$$x = \begin{cases} \dfrac{H(S_1 + S_2) - S_3}{1 + 2H}, \ for\ b = 0; \\ \dfrac{S_3 - H(S_1 + S_2)}{1 + 2H}, \ for\ b = 1. \end{cases} \tag{18}$$

We rewrite the finding formula 17 taking into account x:

$$a_i' = \begin{cases} a_i + \dfrac{H(S_1 + S_2) - S_3}{1 + 2H}, \ for\ b = 0; \\ a_i + \dfrac{S_3 - H(S_1 + S_2)}{1 + 2H}, \ for\ b = 1. \end{cases} \tag{19}$$

After finding the values of the modific elements, we perform steganographic embedding of the data in the blocks according to rule 14.

Extracting data occurs after receiving the stegoimage by image analysis, and comparison of the values of H and k in the blocks.

5. Conclusion

1) Reviewed current trends in the information security, it is proposed to apply the methods of digital steganography to protect your data for increased protection and reliability in the transmission of information. Using a container image is the most promising way to hide data.
2) Analysis of existing methods of data embedding in the image container showed that these methods have a low probability of correct data extraction, unstable to existing attacks and have a small steganographic bandwidth.
3) A method for allocating the blocks of the outline of the image based on the moving mask. These blocks are resistant to compression attacks and cause minor distortions in the image, which allows you to use the image mask for steganographic data hiding.
4) The method of indirect steganographic data hiding in the image contours is developed. This method allows hiding bits in image blocks with high probability of correct extraction of embedded data. The developed method is resistant to known active attacks and steganographic analysis by the enemy.

References

[1] Ablamejko S., Lagunovskij D.: Obrabotka izobrazhenij: teh-nologija, metody, primenenie. Amalfeja, Minsk 2000.
[2] Barannik V. V., Alimpiev A. M., Bekirov A., Barannik D. V., Barannik N. D.: Detections of sustainable areas for steganographic embedding. Proc. East-West Design & Test Symposium (EWDTS), 2017, 555–558 [doi: 10.1109/EWDTS.2017.8110028].
[3] Barannik V., Barannik D., Bekirov A., Lekakh A.: Steganographic method based on the modification of regions of the image with different saturation. Proc of 14th International Conference: Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering, 2018, 542–545 [doi: 10.1109/TCSET.2018.8336260].
[4] Barannik V., Krasnorutsky A., Larin V., Hahanova A., Shulgin S.: Model of syntactic representation of aerophoto images segments. Proc of. XVI-th Intern. conf.: Modern Problems of Radio Engineering, Telecommunications and Computer Science, 2018, 974–977 [doi: 10.1109/TCSET.2018.8336356].
[5] Christophe E., Lager D., Mailhes C.: Quality criteria benchmark for hiperspectral imagery. IEEE Transactions on Geoscience and Remote Sensing 43(9), 2005, 2103–2114.
[6] Gonzalez R., Woods R.: Tsyfrova obrobka zobrazhen. Tekhnosfera, Kiev 2018.
[7] Gribunin V., Okov I., Turincev I.: Tsifrovaya steganografiya. Solon-Press, Moscow 2018.
[8] Grundmann M., Kwatra V., Han M., Essa I.: Efficient hierarchical graph based video segmentation. IEEE CVPR, 2010.
[9] Konakhovich G. M, Puzyrenko A.: Computernaya steganographiya. Teoriya i praktika. To Press, Kiev 2016.
[10] Melnik A. M.: Informatsiyni systemy ta merezhi. Bulletin "Lviv Polytechnic" 673, 2010, 365–374.
[11] Miano J.: Compressed image file formats: JPEG, PNG, GIF, XBM, BMP. Addison-Wesley Professional, New York 1999.
[12] Miano J.: Formats and image compression algorithms in action. Triumph, Kiev 2013.
[13] Pratt W., Chen W., Welch L.: Slant transform image coding. Proc. Computer Processing in Communications. Polytechnic Press, New York 1969.
[14] Sindeev M., Konushin A., Rother C.: Alpha-flow for video matting. Technical Report, 2012.
[15] Stankiewicz O., Wegner K., Karwowski D., Stankowski J., Klimaszewski K., Grajek T.: Encoding mode selection in HEVC with the use of noise reduction. Proc. International Conference on Systems, Signals and Image Processing (IWSSIP), Poznan, 2017, 1–6.
[16] Wallace G.: Overview of the JPEG (ISO/CCITT) – Still image compression: image processing algorithms and techniques. Processing of the SPIE 1244, 1990, 220–233.
[17] Wallace G.: The JPEG Still Picture Compression Standard. Communication in ACM 34(4), 1991, 31–34.
[18] Wang S., Zhang X., Liu X., Zhang J., Ma S., Gao W.: Utility-Driven Adaptive Preprocessing for Screen Content Video Compression. IEEE Transactions on Multimedia 19(3), 2017, 660–667.
[19] Yudin O., Boiko Y., Frolov O.: Organization of decision support systems for crisis management. Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), 2015, 115–117 [doi; 10.1109/INFOCOMMST.2015.7357287].

Oleg Shatun
e-mail: shatun_oleg@ukr.net

Cadet of Ivan Kozhedub Kharkiv National University of Air Force. Active participant of scientific conferences, computer science olympiads. Winner of the competition of students scientific works in the field of cyber defense. Scientific interests: systems, technologies of transformation, encoding, defence and information transfer.

ORCID ID: 0000-0002-5323-2580

Dmitriy Barannik
e-mail: d.v.barannik@gmail.com

Student of the Kharkiv National University of Radioelectronics. Scientific interests: systems, technologies of transformation, encoding, defence and information transfer, semantic processing of images. He has 15 scientific publications, including a monograph and scientific articles.

ORCID ID: 0000-0002-7074-9864

D. Sc. Volodymyr Barannik
e-mail: vvbar/off@gmail.com

Doctor of engineering sciences, professor, chief of department of the Ivan Kozhedub Kharkiv National Air Force University. Scientific interests: systems, technologies of transformation, encoding, defence and information transfer, semantic processing of images.

ORCID ID: 0000-0002-2848-4524

M.Sc. Veronika Kobtseva
e-mail: Veronika.Kobtseva@nure.ua

In 2018 she graduated from Kharkiv National University of Radio Electronics from the Master of Education. Active participant of scientific conferences. Deals with data protection issues. Scientific interests: systems, technologies of transformation, encoding, defence and information transfer

ORCID ID: 0000-0002-0914-5156

otrzymano/received: 1.10.2018 *przyjęto do druku/accepted: 15.12.2018*