I.I. Borisenko.

SEGMENTATION OF A CONTAINER IN STEGANOGRAPHIC ALGORITHMS OF SPACE DOMAIN OF EMBEDDING

This paper is devoted to the solving of the problem of the improving of the resist to the perturbation of the spatial domain steganographic algorithms. Segmentation of container blocks, as one of the efficiency instruments for pred-processing of the matrix of container, is used.

Keywords: *steganography, container, stego, segmentation.*

Introduction

Communication in contemporary society is unthinkable without the use of computer networks, continuous improvement which increases the security of the information that circulates in a network environment. Widely used as a way to implement a hidden connection, methods of computer steganography. Image, video, audio, which are used to conceal secret information (SI), commonly referred to as the container, after embedding information container becomes steganocontainer, which openly is network TV to the receiver. The main property that must meet the steganographic method, is the resistance to detect the hidden SEA, which, understandably, does not guarantee the effectiveness of its decoding when you pass steganocontainer (SC) over the network. Therefore, at the present stage it becomes increasingly important to ensure the sustainability of steganomethods and steganoalgorithms (SA) to perturbation that can be subjected to SC when, for example, the noise in the communication channel.

Despite the fact that SEA implementing instruments in the area of container conversions, are considered to be more stable, many authors [1–3] dedicate their works to the SM and SA spatial field embedded in a number of benefits that are achieved, such algorithms do not use additional computing resources and time to go to the region, as well as the amount of C in a container being implemented (the so-called hidden bandwidth) morethan spectral SA. The question of resistance to strong perturbations of such algorithms remains relevant.

The aim of this work is to increase the stability of steganographic algorithms for embedding spatial domain to the perturbation.

In order to achieve the goals were set and solved tasks: analysis of SA with small resistance to perturbation and research opportunities to increase on the basis of known methods and approaches; the development of more sustainable modifications from existing unsustainable SA:

the algorithm "Payload Transformation", the first step of which is the breakdown of the container-the image into blocks of size 2*2: $X = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}$. Blocks are checked for uniqueness of rows if the strings match, the brightness of one of the elements of row changes to enforce the unique constraint. Next, check the difference of brightness of block elements: x 11-x 12, x 11, x 21, x 21, x 22. The difference must not exceed prescribed threshold preset value Δ, that will ensure the reliability of perception of the container (distortion you make when diving C, will not be visible). If one of the calculated differences is greater than the threshold, the unit is not used for the C implementation, thus the threshold condition is used to select the blocks that do not fall into the area of the image where there is a drastic change in intensity. Classified information, which is embedded, is represented as a binary sequence. In each block is two bits.

Is the identity matrix, which is a specific type of conversions depending on the type of the embedded binary pairs. If the steam is embedded (0000), then the matrix remains unchanged. If the steam is embedded (01), then the matrix is converted to a type. If the steam is embedded

(10), then the matrix is converted to a type. If the steam is embedded (11), then the matrix is converted to a type. The resulting matrix is multiplied by the matrix unit, that is steganotransformation on Y = HT * X. As a result of such conversion formed steganocontainer, blocks which have a distinctive feature: when was built a couple of bits (01) or (10), line block are the same if the same was built a couple of bits (0000) or (11), the line block is different.

Simultaneously with the formation of steganocontainer is the key that is used during decoding. The first key element corresponds to the first block of steganocontainer, the i-th element is the i-th block. As noted above, when you embed a (01) or (10) of the formed units, composed of identical strings, the ambiguity of travel, using the key. If this key is set to 0, then the block was built in couple (01) if the key is set to 1, it was a pair of (10). Similar to overcome ambiguity and for blocks with different lines: If this key is set to 0, then the block was built in steam (0000), if the key is set to 1, it was a pair of (11). The authors examined SA lead experimental evidence in favour of the sustainability of the algorithm to disturbance. However, perturbations were modeled by the manipulation of the least significant bits of the steganocontainer, so this level of perturbations only in some cases it may be sufficient to reproduce the actual conditions. Moreover, the real disturbance in the communication channel, usually taken to model using the additive Gaussian noise is overlaid on the SC. If we take into account the specificity of steganotransformation, after which the line block of IC must be the same (if you built a pair of bit 01 or 10), then change the value of any element of this unit even per unit will result in an error when decoding.

The algorithm is sufficiently long key-he only half the length of the embedded sequence that also requires a reliable way to send it. According to [5] steganographic algorithm was proposed for the transfer and decoding classified information based on graph theory. Initially an algorithm designed for such information-hiding systems where hidden bandwidth is maximized, while ensuring the required secrecy stegokanala and resilience to disturbance are minimum requirements. Later, Stego_Graph was modified to improve interference resistance [6]. The idea of steganoalgorithm Stego_Graph is a binary sequence that performs the role of the SEA, immersed in another binary sequence — a container by comparing the C bits with bits of the container, define it in further localization of C. In case of discrepancy between the c and the corresponding bits of the container the container element adjustment is made with a view to bringing them to binary mind. It is clear that to ensure the reliability requirements of SC its element's computed value must be within the specified limits. For example, if the container is to be used as an image, the brightness of the pixel is calculated must satisfy the condition:

$$f(x,y) - \delta \le f'(x,y) \le f(x,y) + \delta, \qquad (1)$$

where is the maximum permissible deviation from the original pixel brightness values. Of image processing theory known conversion threshold rule, leading it to binary (characteristic) mind [7] (2) where T is the threshold, calculated as halfsum of the maximum and minimum values of the pixels of the scope for which it is calculated.

$$g(x,y) = \begin{cases} 0, \textit{если } f(x,y) \le T, \\ 1, \textit{если } f(x,y) > T \end{cases} \qquad (2)$$

where is the maximum permissible deviation from the original pixel brightness values. Of image processing theory known conversion threshold rule, leading it to binary (characteristic) mind [7] (2) where is the threshold, calculated as halfsum of the maximum and minimum values of the pixels of the scope for which it is calculated.

Stegotransformation, Stego_Graph, consists in the following. SI, which has views of the binary sequence is broken into 8-bit-long substring, then each is represented as a binary tree for which you want the adjacency matrix [7], elements of which are zeros and ones. It is a portrait of adjacency matrix of C Specifies further its localization in the UK. Container-image is broken down into 8 x 8 blocks, and then undergoes a conversion threshold to bring it to binary. The block container conversion threshold feature-image is that this transformation is not always possible to do using the global threshold that is defined for the entire block because, despite the relatively small size of the unit, the difference between the maximum and the minimum value of

the items can be a large number. So, using (2) as a rule, the requirement is violated (1). To avoid such a situation the algorithm contains a block segmentation step on the subdomain, the elements of which lie within the specified limits (the difference between the maximum and the minimum value is a subregion of the elements), and then each sub-field is the threshold.

213	214	212	197	137	112	110	109
189	210	213	210	165	119	110	108
159	204	210	212	189	137	119	107
133	186	204	209	194	153	128	107
137	175	201	210	195	145	126	107
189	164	175	199	175	131	121	108
214	186	164	154	142	121	113	107
213	200	177	131	119	113	112	106

а

1	1	1	0	0	0	0	0
0	1	1	1	0	1	0	0
0	1	1	1	0	0	1	0
0	1	1	1	0	1	1	0
0	1	1	1	0	1	1	0
0	0	1	0	1	0	1	0
1	1	0	1	0	1	0	0
1	0	1	0	1	0	0	0

б

Fig. 1. 8 x 8 Block-container: segmented block matrix (a); the result of the block thresholding segmentation (b)

Illustration of the result of the segmentation unit on and bring it to the binary type is presented in Figure 1. The block container is segmented into four subfields with the following gradation brightness [214-186], [186-158] [130-158] [130-102] (right border does not belong to the area, except for the last) and threshold values T1 = T2 = 172, 200, T3 = 144, T4 = 116. A more detailed look at the process of adjustment of the brightness of a pixel container, which is used when the characteristic value (the value of the corresponding bit) does not match the value a bit. The matrix, as it is shown in Fig. 1, will be in the form of the scale.

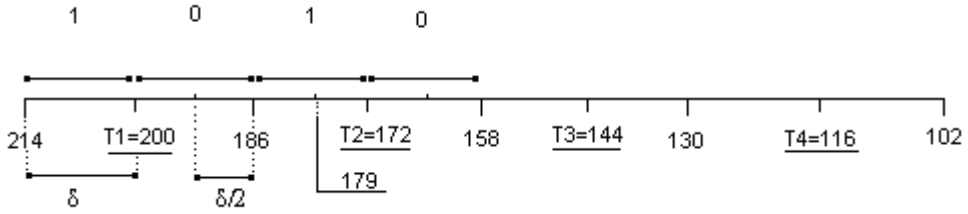

Fig. 2: Block container in the form of a scale

A characteristic value for the pixel that is equal to 1 (except the first subregion), it does not matter what sub-field it is transferred, all while maintaining the reliability of perception. For example, consider the area boundaries [186−158] and threshold. If pixel brightness value that satisfies the criteria, should be amended so that its characteristic value equal to zero, then assign a value, if a pixel has a brightness that satisfies the condition, you must assign the value, and the difference between the original and the new value will satisfy the condition (1), that is placed within. The stegotransformation will ensure stability of the C bits to disturbance of equivalent luminance (10.2).

Modificationof Payload Transformation

1. Modification Of Payload Transformation The algorithm for generating the stenographic container: Entrance: image-container, SI in binary representation. Output: SC. 1. break the container into blocks the size of 8 x 8 each 2. slice the block into subareas; calculate thresholds for each subdomain 3. perform the thresholding to bring the unit to a binary type by using the thresholds obtained in the previous step 4. break up into blocks of size 2 x 2 each 5. for the current bit pairs C determine the type matrix. If bit pair contains

value (0.0) $H = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, the couple's (0.1)- $H = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$ for couples (1.0)-for couples (1.1)- $H = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

6. compared with the current unit. In case of discrepancy between the values of the elements of the container adjust by following Stego_Graph algorithm. The order in which matrix will be built into the unit, can be used as a steganographic key, indeed, changing this order, changing the localization of SI and SA do not require adjustment. SI extraction algorithm from the UK: Login: SC. Output: C. 1. break the container into blocks the size of 8 x 8 each 2. slice the block into subareas; calculate thresholds for each subdomain 3. perform the thresholding to bring the unit to a binary type by using the thresholds obtained in the previous step 4. break up into blocks of size 2 x 2 each.

5. perform the extraction rule: If C is a bit pair contains value (0.0), in the case of steam is extracted (0.1), the matrix corresponds to the pair (1.0), and the matrix corresponds to the pair (1.1). Order of processing blocks to extract bits of C corresponds to the order of the embedding.

Conclusion

In a new more resistant to disturbance of steganographic algorithm, based on an existing container block segmentation using the threshold conversion. New algorithm from the baseline, in addition to improved noise immunity, does not require the key derivation, and uses all the blocks of the container for the introduction of SEA, which increases the latent capacity. According to provisional results, the container blocks allowed to apply segmentation threshold conversion and is an effective preprocessing matrix when bringing it to binary that can be used to enhance noise immunity, similar steganoalgoritms as set out in the work, in which containers can be represented in matrix form.

LIST OF USED SOURCES

1. *Fridrich J.* Steganalysis of LSB Encoding in Color Images/ J. Fridrich, R. Du, M. Long // A Proceedings of ICME 2000, New York City, July 31 – August 2, New York, USA.

2. *Husrev T.* Senear Data Hiding Fundamentals And Applications. Content Security In Digital Multimedia / Husrev T. Senear, Mahalingam Ramkumar, Ali N. Akansu // ELSEVIER science and technology books, 2004. – 364 p.

3 .*Neil F. Johnson*, Information Hiding : Steganography and Watermarking. – Attacks and Countermeasures / Neil F. Johnson, Zoran Duric, Sushil Jajodia // Kluwer Academic Publishers, 2001. – I60 p.

4. *Shiva Kumar K. B.* Steganography Based on Payload Transformation / K. B. Shiva Kumar, K. B. Raja, R. K. Chhotaray, Sabyasachi Pattnaik // IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011.

5. *Борисенко И.И.* Особенности применения многоуровневого порогового преобразования изображения в компьютерной стеганографии / И.И. Борисенко // Праці УНДІРТ. Теоретичний та науково-практичний журнал радіозв'язку, радіомовлення і телебачення. – 2006. – 4(48). – С. 53–59.

6. *Борисенко И.И.* Повышение помехоустойчивости стеганографического алгоритма / И.И. Борисенко // Сучасний захист інформації. – 2010. – № 1. – С. 36–42.

7. *Гонсалес Р.* Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. под ред. П.А. Чочиа. – М. : Техносфера, 2005. – 1072 с.

8. *Харари Ф.* Теория графов / Ф. Харари. – М. : Мир, 1973. – 300 с.