DOI 10.15276/imms.v14.no4.314
UDC 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 4, pp. 314-323

INCREASING THE ROBUSTNESS OF THE STEGANOGRAPHIC METHOD WITH CODE CONTROL AND BLIND DECODING

J. K. Ziginova[1], A.V. Sokolov[2]

[1]National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
[2]National University "Odesa Law Academy"
23, Fontanska rd, Odesa, 65009, Ukraine
Email: radiosquid@gmail.com

Due to the increasing amount of multimedia content in global traffic, steganographic methods are becoming a key element of information protection systems. Modern steganographic methods fall under such requirements as: ensuring the reliability of perception, resistance to attacks against the embedded message, ensuring sufficient bandwidth. These requirements must be met while ensuring high computational efficiency, which, as practice shows, is possible when performing steganographic transformation in the spatial domain of the container. One of the promising steganographic methods that meet all of the above requirements while ensuring high computational efficiency is the steganographic method with code control, for which a new modification with blind decoding was created. However, this modification was researched only when operating with codewords of size 8x8, while in practice, in the case of creating covert channels in conditions of significant attacks, or when operating with digital video, it may be necessary to ensure greater resistance to attacks against the embedded message. The purpose of this paper is to modify the steganographic method with code control and blind decoding to increase its resistance to attacks against the embedded message by using codewords of size 16x16. The paper shows that simply increasing the length of the codeword does not lead to an increase in the resistance of the steganographic method with code control and blind decoding, which justifies the need to search for new structures of codewords of larger size. The paper proposes a new method of formation of codewords and a modification of the steganographic method with code control and blind decoding based on them. The performed experimental research has allowed us to establish the high efficiency of the proposed modification of the steganographic method, in particular, when using codewords of size 16x16 it becomes possible to ensure an error rate of 1.2% when extracting additional information, which is twice as good as using the original modification of the steganographic method with code control and blind decoding.
Keywords: steganography, code control, Walsh-Hadamard transform, spatial domain.

Introduction and statement of the problem. A significant increase in the amount of multimedia content in global traffic leads to a rise in the relevance of using steganographic methods for information protection. Today, a set of criteria has been formed by which modern steganographic methods are evaluated, among which the following main criteria can be distinguished: ensuring the reliability of perception, high throughput, resistance to attacks against the embedded message, and high computational efficiency. It should be noted that today there are several concepts for building steganographic methods. The first of them involves the use of the transform domain for embedding and extracting additional information, which makes it possible to quite easily provide the specified characteristics of the steganographic message, such as its resistance to attacks against the embedded message. In particular, methods based on the discrete cosine transform [1,2,3,4] have been proposed, which give a high percentage of correctly extracted additional information even under conditions of attacks against the embedded message. For example, a method [1] even under conditions of compression attack with a quality factor QF=70 provides an error rate of 0%. Methods based on singular value decomposition [5,6,7] are also able to provide their high efficiency in countering attacks against

embedded messages. However, the group of methods that use container transform domains for their operation is characterized by a significant drawback, which is associated with the fact that the use of such transforms is characterized by high computational costs both when embedding and when extracting additional information. This significantly limits the use of such methods in many common platforms that are used today, for example, mobile platforms, IoT devices, embedded systems, etc.

In contrast to the methods that use the transform domain for their operation, there is a group of steganographic methods that perform steganographic transformation in the spatial domain of the container. Among such methods, we can distinguish, for example, the classical LSB method and its numerous modifications [8,9,10]. Despite the simplicity of their algorithmic implementation, the absolute majority of steganographic methods operating in the spatial domain of the container are characterized by the inability to resist attacks against the embedded message, in particular compression attacks. In [11], the concept of code control was proposed, which combines the advantages of steganographic methods operating in the transform domains of the container with the computational simplicity offered by steganographic methods operating in the spatial domain of the container. The steganographic method with code control [11] was further developed in [12], where a blind decoding algorithm was proposed, which provides the possibility of extracting additional information that was embedded using the steganographic method with code control without the presence of the original container. In [13], the issue of selecting sets of codewords that provide the best characteristics of the steganographic method with code control and blind decoding was researched. However, to date, only codewords of size 8×8, have been practically researched, while in practice it may be necessary to use codewords of larger size to ensure the greatest robustness of the steganographic method. This is relevant, for example, when creating covert channels, under very strong attacks, or when operating with digital video as a container.

Thus, the relevant task is to research the possibilities and the results provided by the use codewords of size 16×16 in the steganographic method with code control and blind decoding.

The *purpose* of this paper is to modify the steganographic method with code control and blind decoding to increase its resistance to attacks against the embedded message by using codewords of size 16×16.

This paper has the following structure: in Section 2, the original steganographic method with code control and blind decoding is considered. In Section 3, the modified steganographic method for operation with blocks of size 16×16 is proposed. Section 4 presents experimental research and a comparison of the results with other existing methods. Conclusions and suggestions for further work are presented in Section 5.

Modification of the steganographic method with code control and blind decoding. The theoretical basis of the steganographic method with code control [11] is the Walsh-Hadamard transform, which is promising for modern steganographic methods and can be determined using the following relation [14]

$$W_X = H_N^{'} X H_N^{'T}, \tag{1}$$

where $H_N^{'} = \frac{1}{\sqrt{N}} H_N$,

X is matrix of size $N\times N$, the Hadamard matrix H_N is determined by the Sylvester construction

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, \; H_1 = 1. \tag{2}$$

Embedding of additional information in the steganographic method with code control occurs using codewords designed in such a way as to selectively affect a given transformant of the Walsh-Hadamard transform, while according to [11] there is a strict correspondence between the transformants of the Walsh-Hadamard transform and the transformants of the discrete cosine transform. Thus, by selecting the type of codeword, it is possible to embed additional information into a given frequency component of the container, ensuring the given properties of the steganographic message.

Thus, the method is truly resistant to compression attacks, as proven by experiments with embedding information into images. Under conditions of compression attack with a value of QF=70, the error rate value is close to 0 when extracting additional information.

A significant drawback of this method, which limited its practical application, was the lack of the ability to provide blind decoding. This problem was solved in [12] by using spatial and frequency duplication of additional information and the idea of extracting information considering the averaging of subblocks of a macroblock. For the sake of completeness, we will briefly describe this method for the case of using two codewords, which is the most practically valuable.

To embed additional information, the image is divided into blocks of size 8×8, a codeword is added to each block, carrying one bit of additional information

$$M_i = X_i + (-1)^{d_i} * T_8^+, \tag{3}$$

where $T_8^+ = \begin{bmatrix} T_{4_1}^+ + T_{4_2}^+ & T_{4_1}^+ + T_{4_2}^+ \\ T_{4_1}^- + T_{4_2}^- & T_{4_1}^- + T_{4_2}^- \end{bmatrix}$ is the codeword;

X_i is the original image block of size 8×8;

d_i is the bit of additional information;

T_{4_1} and T_{4_2} are the codewords selected for embedding additional information, which exert a concentrated effect on the transformants of the Walsh-Hadamard transform.

The extraction of the additional information is performed using the following steps:

Step 1. The message is divided into blocks M_i' of size $\mu\times\mu$.

Step 2. Each block M_i' of size $\mu\times\mu$ is divided into 4 more blocks of size $\mu/2\times\mu/2$ according to the following construction

$$M_i' = \left[\begin{array}{c|c} \psi_{i11} & \psi_{i12} \\ \hline \psi_{i21} & \psi_{i22} \end{array}\right]. \tag{4}$$

Step 3. For each block M_i', we calculate two matrices $u_{1_{lm}}, u_{2_{lm}}$ of size 2×2 using the following formulas

$$\begin{aligned} u_{1_{lm}} &= \sum_{a=1}^{4}\sum_{b=1}^{4}\psi_{ilm}(a,b)T_{4_1}(a,b); \\ u_{2_{lm}} &= \sum_{a=1}^{4}\sum_{b=1}^{4}\psi_{ilm}(a,b)T_{4_2}(a,b), \quad l,m=1,2. \end{aligned} \tag{5}$$

Step 4. We find the average values

$$\begin{aligned} \overline{u_1} &= \sum_{l=1}^{2}\sum_{m=1}^{2}u_1(l,m); \\ \overline{u_2} &= \sum_{l=1}^{2}\sum_{m=1}^{2}u_2(l,m). \end{aligned} \tag{6}$$

Step 5. We find the value of the extracted additional information bit for this block M_i' as

$$d_i' = \text{sign}((u_{1_{11}} - \overline{u_1}) + (u_{1_{12}} - \overline{u_1}) - (u_{1_{21}} - \overline{u_1}) - (u_{1_{22}} - \overline{u_1}) + \\ + (u_{2_{11}} - u_2) + (u_{2_{12}} - u_2) - (u_{2_{21}} - u_2) - (u_{2_{22}} - u_2)). \quad (7)$$

In [13], all groups of codewords of order 4 were researched. Table 1 shows these codewords and the DCT coefficient mostly affected by the codeword.

Table 1.

Effect of codeword on DCT coefficient

Codeword	DCT transformant	Codeword	DCT transformant
$T_{(1,1)} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$	(1,1)	$T_{(1,2)} = \begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \end{bmatrix}$	(1,4)
$T_{(1,3)} = \begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{bmatrix}$	(1,2)	$T_{(1,4)} = \begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$	(1,3)
$T_{(2,1)} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \end{bmatrix}$	(4,1)	$T_{(2,2)} = \begin{bmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \end{bmatrix}$	(4,4)
$T_{(2,3)} = \begin{bmatrix} 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$	(4,2)	$T_{(2,4)} = \begin{bmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$	(4,3)
$T_{(3,1)} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \end{bmatrix}$	(2,1)	$T_{(3,2)} = \begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 \end{bmatrix}$	(2,4)
$T_{(3,3)} = \begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$	(2,2)	$T_{(3,4)} = \begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$	(2,3)
$T_{(4,1)} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$	(3,1)	$T_{(4,2)} = \begin{bmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix}$	(3,4)
$T_{(4,3)} = \begin{bmatrix} 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 \end{bmatrix}$	(3,2)	$T_{(4,4)} = \begin{bmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$	(3,3)

We present the results of an experiment on increasing the size of the applied codeword to 16×16. Within the framework of this experiment, a similar method of constructing codewords was used as for the size 8×8

$$T_{16}^{+}=\begin{bmatrix} T_{8_1}^{+}+T_{8_2}^{+} & T_{8_1}^{+}+T_{8_2}^{+} \\ T_{8_1}^{-}+T_{8_2}^{-} & T_{8_1}^{-}+T_{8_2}^{-} \end{bmatrix}, \tag{8}$$

where $T_{8_1}^{+}$ and $T_{8_2}^{+}$ are the first and second codeword, respectively.

The use of codewords constructed according to (8) led to the formation of a steganographic message with resistance to attacks against the embedded message comparable to the resistance provided by the method [13], however, with reduced throughput. Such results lead to the conclusion that it is necessary to restructure the codeword with an increase in its size.

The proposed solution. As a basis for constructing codewords T_{16}^{+}, we will use expression (3), accordingly, we will choose the following codeword structure

$$T_{16}^{+}=\begin{bmatrix} T_8^{+} & T_8^{+} \\ T_8^{-} & T_8^{-} \end{bmatrix}=\begin{bmatrix} T_{4_1}^{+}+T_{4_2}^{+} & T_{4_1}^{+}+T_{4_2}^{+} & T_{4_1}^{+}+T_{4_2}^{+} & T_{4_1}^{+}+T_{4_2}^{+} \\ T_{4_1}^{-}+T_{4_2}^{-} & T_{4_1}^{-}+T_{4_2}^{-} & T_{4_1}^{-}+T_{4_2}^{-} & T_{4_1}^{-}+T_{4_2}^{-} \\ T_{4_1}^{-}+T_{4_2}^{-} & T_{4_1}^{-}+T_{4_2}^{-} & T_{4_1}^{-}+T_{4_2}^{-} & T_{4_1}^{-}+T_{4_2}^{-} \\ T_{4_1}^{+}+T_{4_2}^{+} & T_{4_1}^{+}+T_{4_2}^{+} & T_{4_1}^{+}+T_{4_2}^{+} & T_{4_1}^{+}+T_{4_2}^{+} \end{bmatrix}, \tag{9}$$

where $T_{4_1}^{+}$ and $T_{4_2}^{+}$ are the first and second codewords, respectively.

According to the structure of the codeword T_{16}^{+}, we can conclude that the method operates as if one bit of additional information were embedded using four codewords T_8^{+}. Considering the structure of the codeword (9), we write an algorithm for embedding additional information, which is similar to the algorithm for embedding additional information [13].

Step 1. The image is divided into blocks 16×16.

Step 2. A codeword is added to each block, which is modulated by a bit of additional information. Then each subsequent block of the steganographic message M_i will be defined as

$$M_i=X_i+(-1)^{d_i}*T_{16}^{+}, \tag{10}$$

where X_i is the block of the original image of size 16×16;

d_i is the bit of additional information;

T_{16}^{+} is the codeword constructed according to formula (9).

Below we present the algorithm for extracting additional information in the form of specific steps.

Step 1. The original image is divided into blocks of size 16×16 in a standard way. For each block, we define the matrix $P=\begin{bmatrix} p_1 & p_2 \\ p_3 & p_4 \end{bmatrix}$.

Step 2. For each block M_i, we perform its division in a standard way into 4 blocks Y_j, $j=1,2,...,4$ of size 8×8.

Step 3. For each block Y_j of size 8×8, we perform its division into 4 more blocks of size 4×4 according to the following construction $Y_i=\left[\begin{array}{c|c} y_1 & y_2 \\ \hline y_3 & y_4 \end{array}\right]$.

Step 4. For each block Y_j, we calculate the matrices

$$u_{i,1}=\left[\begin{array}{c|c}\sum\limits_{a=1}^{4}\sum\limits_{b=1}^{4}y_1(a,b)T_{4_1}(a,b) & \sum\limits_{a=1}^{4}\sum\limits_{b=1}^{4}y_2(a,b)T_{4_1}(a,b)\\ \hline \sum\limits_{a=1}^{4}\sum\limits_{b=1}^{4}y_3(a,b)T_{4_1}(a,b) & \sum\limits_{a=1}^{4}\sum\limits_{b=1}^{4}y_4(a,b)T_{4_1}(a,b)\end{array}\right],$$
$$u_{i,2}=\left[\begin{array}{c|c}\sum\limits_{a=1}^{4}\sum\limits_{b=1}^{4}y_1(a,b)T_{4_2}(a,b) & \sum\limits_{a=1}^{4}\sum\limits_{b=1}^{4}y_2(a,b)T_{4_2}(a,b)\\ \hline \sum\limits_{a=1}^{4}\sum\limits_{b=1}^{4}y_3(a,b)T_{4_2}(a,b) & \sum\limits_{a=1}^{4}\sum\limits_{b=1}^{4}y_4(a,b)T_{4_2}(a,b)\end{array}\right], \quad (11)$$

where the notation $y(a,b)$ means the element of the matrix with index (a,b).

Step 5. We find the average values

$$\overline{u_{i,1}}=\sum_{l=1}^{2}\sum_{m=1}^{2}u_{i,1}(l,m);\quad \overline{u_{i,2}}=\sum_{l=1}^{2}\sum_{m=1}^{2}u_{i,2}(l,m). \quad (12)$$

Step 6. We find the values $p_i, i=1,2,...,4$ for the given block Y_j as

$$p_i=\text{sign}\left(\sum_{l=1}^{2}\left((u_{i,l}(1,1)-\overline{u_{i,l}})+(u_{i,l}(1,2)-\overline{u_{i,l}})-(u_{i,l}(2,1)-\overline{u_{i,l}})-(u_{i,l}(2,2)-\overline{u_{i,l}})\right)\right). \quad (13)$$

Step 7. We calculate the bit of additional information in the block M_i as $d_j=sign\left(\sum\limits_{l=1}^{4}p_l\right)$.

The results of experiments. For experimental research, 500 images were selected from the NRCS database [16]. Additional information was embedded using the YCbCr space in the Y component of each image block. The pairs $T^{+}_{4(1,4)}$ and $T^{+}_{4(1,4)}$, $T^{+}_{4(2,3)}$ and $T^{+}_{4(3,3)}$, $T^{+}_{4(4,1)}$ and $T^{+}_{4(4,1)}$ were used as codewords T_{4_1} and T_{4_2}.

Experimental research on the stability of the proposed modification of the steganographic method was performed as follows. Additional information was embedded in each image, after which the resulting steganographic message was compressed using the JPEG compression algorithm with a given quality factor *QF*. After that, the embedded information was extracted and the number of errors was estimated.

Fig. 1 shows the results of the experimental research on the number of errors in the extracted additional information depending on the quality factor *QF*.

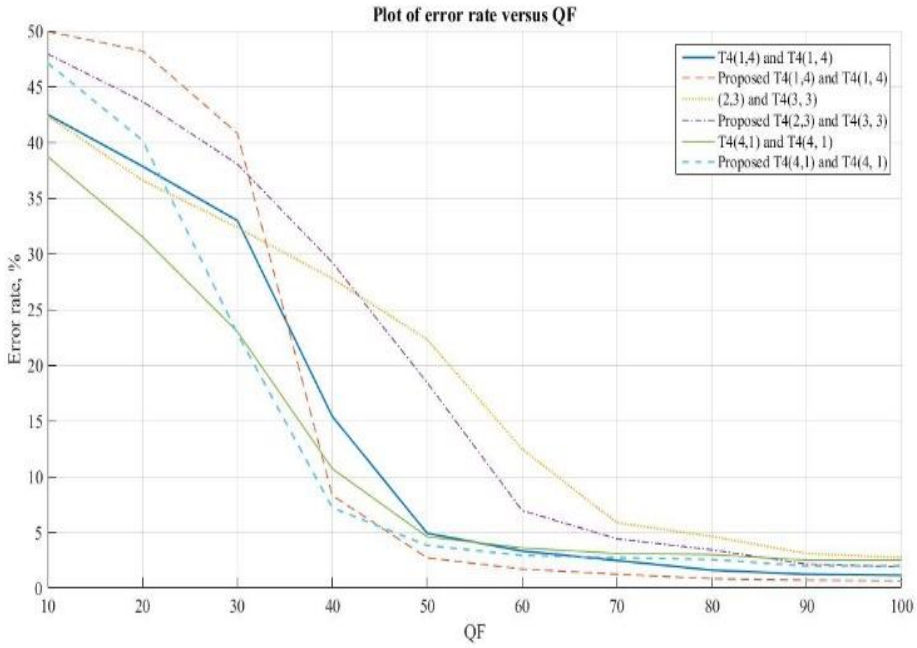

Fig. 1. Number of errors in extracted information depending on the quality factor *QF*

Fig. 2 shows an example of embedding additional information using the proposed modification of the steganographic method.

a) b)

Fig. 2. .Example of embedding additional information using the proposed modification of the steganographic method with code control, a) – original message, b) – steganographic message

Subjective ranking of the images presented in Fig. 2 leads to the conclusion that there are no artifacts or visible distortions in the steganographic message.

Table 2 presents the results of a comparative analysis of the proposed modification of the steganographic method with code control of additional information embedding with the classical steganographic method with code control, the steganographic method with code control and blind decoding, as well as other known analogs.

Table 2.

Comparative analysis of the proposed modification of the steganographic method with code control

Code	QF										PSNR, dB	R	Domain	Blind
	10	20	30	40	50	60	70	80	90	100				
Original [11]														
(5,1)	42.8	29.4	12.2	3.05	0.97	0.72	0.07	0.03	0	0	48.1	1/16	S	-
Modified [13]														
(1,4) (1,4)	42.5	37.8	32.9	15.4	4.9	3.3	2.5	1.6	1.2	1.1	36.1	1/64	S	+
(2,3) (3,3)	42.3	36.6	32.4	27.8	22.3	12.5	5.86	4.63	3.09	2.73	42.2	1/64	S	+
(4,1) (4,1)	38.7	31.5	23.0	10.7	4.6	3.6	3.1	3.0	2.5	2.5	37	1/64	S	+
Proposed														
(1,4) (1,4)	49.9	48.2	40.8	8.3	2.7	1.7	1.24	0.84	0.71	0.65	36	1/256	S	+
(2,3) (3,3)	47.9	43.6	38.0	29.2	18.4	6.96	4.42	3.43	2.15	1.9	36.8	1/256	S	+
(4,1) (4,1)	47.1	40.2	22.8	7.2	3.82	2.93	2.72	2.56	1.98	1.99	36.3	1/256	S	+
[15]														
	-	-	0.02	-	0.02	-	0.01	-	0.01	0.01	27.1	0.01	NN	+
[1]														
	-	-	0	-	0	-	-	0	-	0			DCT	+
[2]														
	-	-	-	-	-	-	33.9	7.4	0.3	-	45	<1/8	DCT	+
[17]														
	13	7	5	4	2	2	2	2	2	-	34.7	1/64	SVD	+
[5]														
	-	-	-	-	23.9	14.1	2.76	0.08	0.08	-	32.7	1/16	SVD	+
[18]														
	-	-	-	-	24.7	14.4	2.71	0.2	0.1	-	32.7	1/64	SVD	+

Analysis of the data presented in Table 2 leads to the conclusion that the proposed modification of the steganographic method with code control allows to provide actually two times fewer errors in the compression attack with the coefficient QF=70 when compared to classical steganographic method with code control and blind decoding. At the same time, on all sets of codewords that were researched, the percentage of correctly extracted additional information is higher than on the same sets of codewords [13]. The PSNR indicator is practically the same as in [13].

Conclusions. The paper proposes a modification of the steganographic method with code control of additional information embedding and blind decoding, which is capable of operating with codewords of size 16×16. The modification, in comparison with analogs, gives better results on the same sets of codewords. At QF values used in real-time information transmission channels, the number of errors is practically 2 times less. The PSNR indicator is constant and equal to ~36 dB, indicating steganographic message reliability of perception.

Further research may concern larger blocks and an increase in the percentage of correctly extracted additional information.

References

1. Wang S., Zheng N., Xu M. A Compression Re-sistant Steganography Based on Differential Manchester Code. *Symmetry*. 2021. V. 13, No. 2. P. 345. URL: https://doi.org/10.3390/sym13020165
2. Zhu Z., Zheng N., Qiao T., Xu M. Robust Ste-ganography by Modifying Sign of DCT Coeffi-cients. *IEEE Access*. 2019. V. 7. P. 168613-168628. URL: https://doi.org/10.1109/access.2019.2953504
3. Rabie T., Kamel I. On the embedding limits of the discrete cosine transform. *Multimed Tools Appl.* 2016. V.75. P.5939–5957. URL:https://doi.org/10.1007/s11042-015-2557-x
4. Rabie T., Kamel I. Toward optimal embedding capacity for transform domain steganography: a quad-tree adaptive-region approach. *Multimed Tools Appl*. 2017. V.76. P.8627–8650. URL:https://doi.org/10.1007/s11042-016-3501-4
5. Chanu Y. J., Singh Kh. M., Tuithung T. A Robust Steganographic Method based on Singular Value Decomposition. *Int. J. of Information & Computation Technology*. 2014. V. 4, No. 7. P. 717-726.
6. Thanki R., Borra S., Dwivedi V., Borisagar K. A steganographic approach for secure communication of medical images based on the DCT-SVD and the compressed sensing (CS) theory. *The Imaging Science Journal*. 2017. V.65., No. 8. P.457-467. URL: https://doi.org/10.1080/13682199.2017.1367129
7. Arunkumar S., Subramaniyaswamy V., Vijayakumar V., Chilamkurti N., Logesh R. SVD-based robust image steganographic scheme using RIWT and DCT forsecure transmission of medical images. *Measurement*. 2019. V.139. P.426-437. URL:https://doi.org/10.1016/j.measurement.2019.02.069
8. Bairagi A. K., Khondoker R., Islam R. An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures. *Information Security Journal: A Global Perspective*. 2016. V.25., No. 4-6. P. 197-212. URL:https://doi.org/10.1080/19393555.2016.1206640
9. Parah S.A., Sheikh J.A., Ahad F., Bhat G.M. High Capacity and Secure Electronic Patient Record (EPR) Embedding in Color Images for IoT Driven Healthcare Systems. *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence*. 2017. V.30. P.411-437. URL:https://doi.org/10.1007/978-3-319-60435-0_17
10. Huang C.T., Tsai M.Y., Lin L.C. VQ-based data hiding in IoT networks using two-level encoding with adaptive pixel replacements. *The Journal of Supercomputing*. 2018. V.74. P.4295–4314. URL: https://doi.org/10.1007/s11227-016-1874-9
11. Kobozeva A.A., Sokolov A.V. Robust Steganographic Method with CodeControlled Information Embedding. *Problemele Energeticii Regionale*. 2021. V.4, No.52. P.115-130. URL: https://doi.org/10.52254/1857-0070.2021.4-52.11
12. Ziginova Yu.K. Modified steganographic method with code control of additional information embedding with blind decoding. *Modern aspects of digitalization and informatization in software and computer engineering*: International scientific and practical conference. 2023. P. 68-70. (In Ukrainian). URL: https://duikt.edu.ua/uploads/n_11337_64054605.pdf
13. Sokolov A.V., Ihnatenko O.O., Balandina N.M. Increasing the Efficiency of Blind Decoding of the Steganographic Method with Code Control of Additional Information Embedding. *Problemele energeticii regionale*. 2024. V.2, No. 62. P.121-137. URL: https://doi.org/10.52254/1857-0070.2024.2-62.11
14. Logachev O. A., Sal'nikov A. A., Jashhenko V. V. Boolean functions in coding theory and cryptology. M.: MCNMO, 2004. 472 p. (In Russian)
15. Li Z., Zhang M., Liu J. Robust image steganography framework based on generative adversarial network. *Journal of Electronic Imaging*. 2021. V. 30, No 2. P. 023006 URL: https://doi.org/10.1117/1.JEI.30.2.023006
16. Natural Resources Conservation Service (NRCS). URL: https://www.nrcs.usda.gov

ПІДВИЩЕННЯ СТІЙКОСТІ СТЕГАНОГРАФІЧНОГО МЕТОДУ З КОДОВИМ УПРАВЛІННЯМ ТА СЛІПИМ ДЕКОДУВАННЯМ

Ю. К. Зігінова[1], А. В. Соколов[2]

[1] Національний університет «Одеська політехніка»
1, Шевченка пр., м.Одеса, 65044, Україна
[2]Національний університет «Одеська юридична академія»
23, Фонтанська дорога, м.Одеса, 65009, Україна
Email: radiosquid@gmail.com

Через зростання долі мультимедійного контенту у світовому трафіку стеганографічні методи стають ключовим елементом систем захисту інформації. До сучасних стеганографічних методів пред'являються такі вимоги як: забезпечення надійності сприйняття, стійкість до атак проти вбудованого повідомлення, забезпечення достатньої пропускної спроможності. Зазначені вимоги мають виконуватися при забезпечення високої обчислювальної ефективності, що, як показує практика, є можливим при виконанні стеганоперетворення у просторовій області контейнера. Одним з перспективних стеганографічних методів, що задовольняє всім зазначеним вимогам при забезпеченні високої обчислювальної ефективності є стеганографічний метод з кодовим управлінням, для якого була створена новітня модифікація із сліпим декодуванням. Тим не менш, зазначена модифікація була досліджена тільки при роботі з кодовими словами розміру 8x8, тоді як на практиці в разі створення прихованих каналів в умовах значних атак, або при роботі з цифровим відео може виникати необхідність забезпечення більшої стійкості до атак проти вбудованого повідомлення. Метою даної статті є модифікація стеганографічного методу з кодовим управлінням та сліпим декодуванням для підвищення його стійкості до атак проти вбудованого повідомлення шляхом застосування кодових слів розміру 16x16. У роботі показано, що просте нарощування довжини кодового слова не призводить до збільшення стійкості стеганографічного методу з кодовим управлінням та сліпим декодуванням, що обґрунтовує необхідність пошуку нових структур кодових слів більшого розміру. У роботі запропоновано новий спосіб формування кодових слів та модифікація стеганографічного методу з кодовим управлінням та сліпим декодуванням на їх основі. Проведені експериментальні дослідження дозволили встановити високу ефективність запропонованої модифікації стеганографічного методу, зокрема, при застосування кодових слів розміру 16x16 стає можливим забезпечити відсоток помилок при вилученні додаткової інформації 1.2%, що є фактично у два рази меншим від застосування оригінальної модифікації стеганографічного методу з кодовим управлінням та сліпим декодуванням.

Ключові слова: стеганографія, кодове управління, перетворення Уолша-Адамара, просторова область.