УДК 004.056.5 **DOI:10.30837/rt.2021.4.207.02**

A.A. KOBOZEVA, Sc.D., A.V. SOKOLOV, PhD.

THE THEORETICAL FOUNDATIONS FOR CONSTRUCTING EFFECTIVE CODEWORDS FOR THE CODE-CONTROLLED INFORMATION EMBEDDING STEGANOGRAPHIC METHOD

1. Introduction and statement of the problem

Steganographic subsystem is the important element of modern complex information security systems, the purpose of which is not only to ensure the impossibility of information reading by intruders, but also to hide the very fact of the presence of secret information.

The modern direction of development of cyberspace involves a significant increase in the amount of graphical information in traffic, which leads to an expansion of the scope of steganographic methods application and an increase in their significance in complex information security systems [1]. This circumstance has led to increased attention of modern researchers to steganography and the emergence of a significant number of new steganographic methods operating both in the spatial (temporal) domain and in the domain of various transformations of the original container: DCT [2 – 5], wavelet transforms [6 – 9], singular value decomposition of the corresponding content matrix [10 – 13], Walsh-Hadamard transform [14 – 17].

The use of steganographic methods in modern cyberspace is associated with possible intentional and unintentional attacks against an embedded message, which may include such common effects as: lossy compression, noise, blur, filtering, etc., which can lead to damage of additional information carried by the image considered in this paper as a container. Considering the enormous volumes of transmitted, stored, and processed digital information, a compression attack is the most common today. These circumstances necessitate the development of steganographic methods that would ensure not only the reliability of the perception of the resulting steganographic message, but also resistance to possible attacks against the embedded message.

Modern researchers in the field of steganography agree [18, 19] that considering the computational complexity and features of machine arithmetic, the most rational is the use of the spatial domain of a digital image (DI) for the embedding and extraction of additional information. However, the task of the development of steganographic method corresponding to the necessary requirements for the steganographic message, in particular, ensuring its reliability of perception, insensitivity to disturbing influences, etc., causes significant difficulties in the spatial domain. The existing sufficient conditions for ensuring the above requirements are usually considered in the transform domains of the DI (frequency, singular/spectral value decomposition domain of the corresponding matrix, etc.), which, under such conditions, places the spatial domain in a deliberately “losing” position, in particular, in the development of robust against disturbing influences steganographic methods.

Some modern papers postulate the fact that it is possible to provide resistance to attacks against an embedded message, in particular to lossy compression, exclusively in the DI transform domain, which is clearly not true [20] and is confirmed by the code-controlled information embedding steganographic method recently proposed by the authors in [21]. The mentioned method provides both reliability of perception and perturbation insensitivity of the steganographic message using the spatial domain for steganographic transformation more efficiently than methods that make use of the DI transform domains for steganographic transformation.

As it is known, the efficiency of methods which are based on the code structures directly depends on the properties of the codes used in them. The code-controlled information embedding steganographic method developed in [21] is based on the use of codewords based on the rows of the Walsh-Hadamard matrix (first-order Reed-Muller code) to control the embedding of additional information, the optimality of which has not been researched properly to this point. This circumstance

determines the task of developing a theoretical basis for the construction of effective codewords for their application in the code-controlled information embedding steganographic method.

The *purpose* of this paper is a theoretical substantiation of a method for improving the properties of codewords used in the spatial domain of the container in order to reduce the sensitivity to disturbing influences of the steganographic message generated with their help.

2. The code-controlled information embedding steganographic method

One of the main transforms that is used in processing (in particular, compression) of images and videos is the DCT, defined by the following relation

$$S = C_N X C_N^T, \tag{1}$$

where X is a fragment of the original image of size $N \times N$, C_N is the $N \times N$ DCT matrix, the elements $C(i, j)$, $i, j = 0,1,..., N-1$ of which are calculated in accordance with the following formula

$$C(i, j) = \begin{cases} \dfrac{1}{\sqrt{N}}, & \text{when } i = 0; \\ \sqrt{\dfrac{2}{N}} \cos\left(\dfrac{(2j+1) \cdot i \cdot \pi}{2N} \right), & \text{when } i > 0. \end{cases} \tag{2}$$

Significant attention in the development of modern steganographic methods for DI is given to the two-dimensional Walsh-Hadamard transform [22], which is specified using the following relation

$$W = H'_N X H'^T_N, \tag{3}$$

where X is a matrix of size $N \times N$, $H'_N = \dfrac{1}{\sqrt{N}} H_N$, and the Hadamard matrix H_N of order N is given using the Sylvester construction

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, \; H_1 = 1. \tag{4}$$

In [21], the relationship between the two-dimensional and one-dimensional Walsh-Hadamard transform was established (up to a coefficient $1/N$)

$$\tilde{W} = \tilde{X} H_{N_2}, \tag{5}$$

where the operator $\tilde{A}$ denotes the representation of the matrix A of order $N \times N$ as a row vector of length N^2 by sequential concatenation of the rows of the original matrix A.

The established relationship between the two-dimensional and one-dimensional Walsh-Hadamard transform makes it possible to simplify and make more demonstrative the mathematical transformations used to develop steganographic methods operating directly in the Walsh-Hadamard transform domain or using this domain for their functioning.

The further development of the direction of using the spatial domain of the DI container for the embedding of the additional information, the prospects of which are indicated in [19], is the method for code control of the embedding of additional information, proposed in [21]. The main idea of this method is based on the application of the linearity property of the Walsh-Hadamard transform.

Formally, the steganographic transformation of a container with matrix X, regardless of the domain of embedding of the additional information (spatial, frequency, singular value

decomposition of the matrix, etc.), can be represented as: $M = X + \Delta X$, where M is the matrix of steganographic message, ΔX is the matrix of container perturbation as a result of the steganographic transformation. In other words, steganographic transformation can be represented as an additive embedding of additional information in the spatial domain [18]. Due to this, without limiting the generality of the foregoing, we further consider that the embedding of the additional information is performed as a summation of the initial matrix of the container image X and the matrix corresponding to bits of additional information D , i.e., the following relation takes place

$$M = X + D . \tag{6}$$

In the general case, the matrix D is the result of a preliminary coding of the additional information bits obtained at the output of the precoder in the steganographic system. For the method proposed in [21], D according to a certain rule is assigned to each bit of the additional information.

In the Walsh-Hadamard transform domain, action of (6) is equivalent to summing the transformants of the original container image and the preliminary encoded additional information

$$\tilde{M}H_{N^2} = (\tilde{X} + \tilde{D})H_{N^2} = \tilde{X}H_{N^2} + \tilde{D}H_{N^2} . \tag{7}$$

In other words, by performing the preliminary coding of the additional information in the form of a matrix D , it is possible to perform a targeted impact on one or another transformant of the Walsh-Hadamard transform in order to give to the steganographic message the specified properties determined by the Walsh-Hadamard transformant to which the impact is directed. For example, when information is embedded in such a way that the transformants corresponding to low and medium frequencies are perturbed, it is possible to obtain steganographic messages that are resistant to attacks against the embedded message. The specified is the basis for the code-controlled information embedding method.

The use of code-controlled information embedding in combination with codewords over the alphabet $\{+1,-1\}$ made it possible to obtain a steganographic method [21], which is superior in efficiency to known analogs that are resistant to attacks against an embedded message. However, the number of errors that occur when decoding additional information from a steganographic message subjected to a compression attack with low quality factors $QF < 40$ is more than 5,5 %, which may be unacceptable in some practical applications. In this paper, we propose a further improvement of the method proposed in [21] by researching the characteristics of the codewords used in it.

3. Codewords energy and selectivity

The operation of the code-controlled information embedding method implies the use as a matrix D of size $\mu \times \mu$, which is the result of encoding of the additional information bit, with help of such codewords that would selectively modify those frequency components of the container block that are least affected by attacks against an embedded message (in the case of lossy compression attacks, noisy or blurring, we are talking about components corresponding to low and medium frequencies).

At the same time, the perturbing effect that the attack has on the embedded message, as well as the embedding of the additional information itself, can be represented as an additive perturbation matrix, thus, for the case of the attacked steganographic message, expression (6) takes the form

$$M' = X + D + \varepsilon , \tag{8}$$

where ε is the matrix of the error introduced by the attack, M' is the matrix of the perturbed steganographic message.

It is clear that if the element of the error matrix ε is opposite to the element of the matrix D and will be equal to it or exceed it in amplitude, an error will occur on the decoder side when decoding the specified element of the codeword. Let's denote the probability of such an event as p_e .

To reduce the negative effect from the impact of possible disturbances and increase the resistance of the code-controlled steganographic method, we can increase the energy of the applied codewords, which we define as follows

$$E = \sum_{i=1}^{\mu} \sum_{j=1}^{\mu} t_{i,j}^2 , \tag{9}$$

where $t_{i,j}$ are the elements of the applied codeword.

To construct specific codewords in [21], using a direct correspondence between the Walsh-Hadamard transformants and the DCT transformants, the Walsh-Hadamard transformants were selected corresponding to the low-frequency and mid-frequency components of the DI block

DCT	Size	Walsh-Hadamard transform
$(1,1);\ (1,2);\ (2,1);$ $(3,1);\ (2,2);\ (1,3)...$	4×4	$(1,1);\ (1,3);\ (3,1);\ (4,1);\ (3,3);\ (1,4)...$
	8×8	$(1,1);\ (1,5);\ (5,1);\ (7,1);\ (5,5);\ (1,7)...$
	16×16	$(1,1);\ (1,9);\ (9,1);\ (13,1);\ (9,9);\ (1,13)...$

. (10)

Based on the data (10), it was proposed to use the matrix representation of the rows of the Walsh-Hadamard matrix of order N^2 as codewords. For example, to effect the DCT transformant (1,2) in 4×4-blocks, the matrix representation of the third row of the Walsh-Hadamard matrix of the order $N=16$ is used as a codeword, which, for clarity, we present together with its transformants of the Walsh-Hadamard transform (3), as well as the transformants of the DCT (1)

$$T^{+}_{b,4,(1,2)} = \begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{bmatrix},\ W^{+}_{b,4,(1,2)} = \begin{bmatrix} 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, C^{+}_{b,4,(1,2)} = \begin{bmatrix} 0 & 3.7 & 0 & -1.53 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \tag{11}$$

where the index $b,4,(1,2)$ denotes: *b* is the binary nature of the codeword, 4 is the order of the matrix of the codeword, (1,2) is the transformant of the DCT, on which the given codeword has the greatest impact.

In view of the fact that the codeword $T^{+}_{b,4,(1,2)}$ consists exclusively of elements belonging to the set $\{\pm1\}$, its energy, in accordance with (9), is equal to $E=16$.

An analysis of expression (11) shows that the codeword $T^{+}_{b,4,(1,2)}$ has an exclusive effect on the transformant (1,3) of the Walsh-Hadamard transform $W^{+}_{b,4,(1,2)}$. However, the relationship established in [21] between Walsh-Hadamard transformants and DCT transformants is not one-to-one; the point is that a given Walsh-Hadamard transformant is related to a certain DCT transformant "mainly". This circumstance leads to the fact that in the DCT transformants of the codeword there is an impact not only on the desired transformant (1,2), but also on the transformant (1,4). In other words, while providing a selective effect on the Walsh-Hadamard transformant (1,3), the codeword $T^{+}_{b,4,(1,2)}$ is not selective in terms of the effect on the DCT (1,2) transformant, while a significant part of its energy is spent on changing the DCT transformant (1,4), which is higher frequency, and therefore more susceptible to attacks against the embedded message. From the point of view of steganography, this can be considered as the distribution of the embedded additional information ($T^{+}_{b,4,(1,2)}$ or $T^{-}_{b,4,(1,2)}$ is the result of preliminary coding of additional information), over the frequency components of the DCT (1,2) and (1,4), or otherwise, as a representation of the additional information in

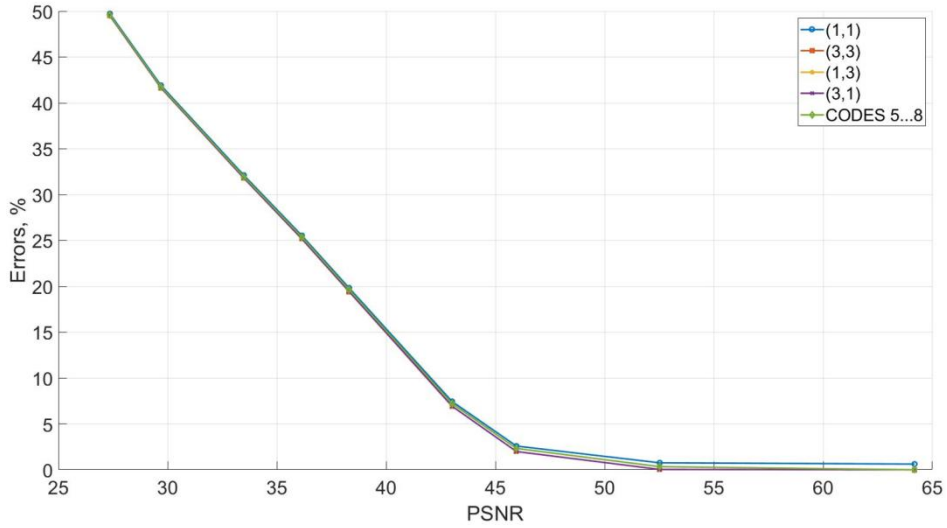
the frequency domain in the form of perturbations of the corresponding frequency coefficients. At a formal level, the additional information decoding will be the more efficient the less these frequency coefficient perturbations change as a result of an attack against an embedded message, in particular, a lossy compression attack. At the same time, that "part of the additional information", the formal representation of which is the perturbation of the DCT coefficient (1,2), is "more protected" from lossy compression attack than the part, the representation of which is the perturbation of the mid-frequency coefficient (1,4). In this regard, an urgent task for the block size 4×4 is to ensure the reduction (minimization) of the perturbation of the DCT coefficient (1,4) as a result of the embedding of an additional information to increase the efficiency of its decoding under conditions of attacks against an embedded message. Similar problems arise for blocks of other sizes.

To quantify the selectivity of the impact of a codeword on the frequency components of a steganographic message, we propose to determine the selectivity coefficient κ as follows

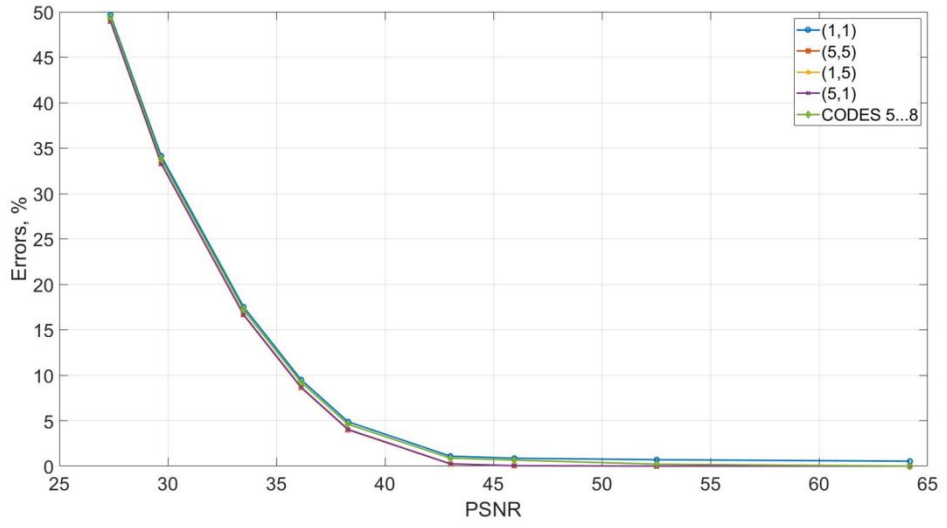
$$\kappa = \frac{\left|c_{n,m}\right|}{\sum_{i=0}^{\mu-1}\sum_{j=0}^{\mu-1}\left|c_{i,j}\right|}. \qquad (10)$$

It directly follows from definition (10) that for a fixed codeword size, with an increase in the selectivity coefficient κ, the expected "effect" from using a particular codeword will increase (in particular, the resistance of the steganographic transformation to attacks against the embedded message for the corresponding codewords will increase) with increasing of $\left|c_{n,m}\right|$ and decrease of $\sum_{i=0}^{\mu-1}\sum_{j=0}^{\mu-1}\left|c_{i,j}\right|$.

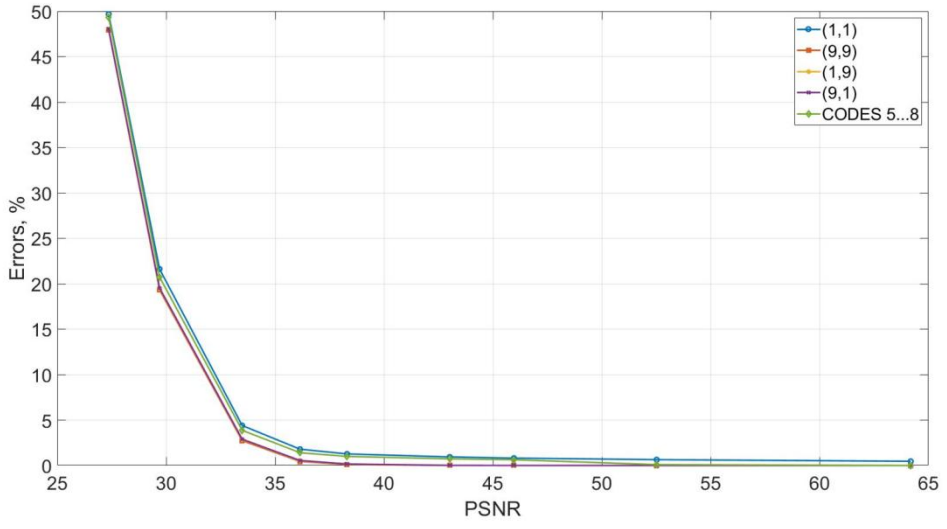
The result of "scattering" the impact of the codeword will increase with the growth of its size. Indeed, as μ increases, the step of changing of the argument of the cosines used in the DCT will decrease. This will cause the increasing in codeword energy, which affects mainly low frequencies (by codeword construction), to be redistributed to more close low frequencies that differ slightly from each other, and this difference decreases with increasing in μ. In this case, the DCT coefficient (n,m) corresponds to different (low) frequencies in blocks of different sizes, as follows from formula (2). Let's call this the "close neighbor" effect. The "close neighbor" effect will lead to a decrease in the value of the selectivity coefficient κ with increasing in μ, determined in accordance with (10) (Table 1), where only the impact on a given frequency coefficient (n,m) is put at the forefront. The increase in total impact on low-frequency "close neighbors" of (n,m) will be strictly shown below. Thus, a decrease in κ with growth in μ in the general case does not reflect a decrease in the resistance of the steganographic transformation to an attack against the embedded message, an illustration of which is Fig. 1, where the resistance of a stenographic message to an attack by Gaussian noise increases with a decrease in κ (increase in μ). Graphs (Fig. 1) were obtained using an experiment to determine the resistance of the code-controlled information embedding steganographic method to a noise attack using 500 images in TIFF format from the NRCS database [23].



a



b



c

Fig.1. Dependence of the number of errors during the extraction of the additional information under the conditions of imposition of Gaussian noise on the steganographic message from the value of the PSNR when using codewords with $\mu \times \mu$-matrices: *a* – $\mu = 4$; *b* – $\mu = 8$; *c* – $\mu = 16$

Table 1

DCT Transformant	Codeword, $\mu = 4$	κ	Codeword, $\mu = 8$	κ	Codeword, $\mu = 16$	κ
(1,1)	$T^{+}_{b,4,(1,1)}$	1	$T^{+}_{b,8,(1,1)}$	1	$T^{+}_{b,16,(1,1)}$	1
(1,2)	$T^{+}_{b,4,(1,2)}$	0.7071	$T^{+}_{b,8,(1,2)}$	0.5603	$T^{+}_{b,16,(1,2)}$	0.4675
(2,1)	$T^{+}_{b,4,(2,1)}$	0.7071	$T^{+}_{b,8,(2,1)}$	0.5603	$T^{+}_{b,16,(2,1)}$	0.4675
(3,1)	$T^{+}_{b,4,(3,1)}$	1	$T^{+}_{b,8,(3,1)}$	0.7071	$T^{+}_{b,16,(3,1)}$	0.5603
(2,2)	$T^{+}_{b,4,(2,2)}$	0.5	$T^{+}_{b,8,(2,2)}$	0.314	$T^{+}_{b,16,(2,2)}$	0.2186
(1,3)	$T^{+}_{b,4,(1,3)}$	1	$T^{+}_{b,8,(1,3)}$	0.7071	$T^{+}_{b,16,(1,3)}$	0.5603

As it can be seen from Table 1, when the codeword size is $\mu = 4$, the codewords $T^{+}_{b,4,(3,1)}$ and $T^{+}_{b,4,(1,3)}$ have the value of the selectivity coefficient equal to $\kappa = 1$ (which means the absolute selectivity). Let us consider in more detail the nature of the existence of absolute selectivity for some codewords. Let codewords $T^{+}_{□,4,(2,1)}$ and $T^{+}_{□,4,(3,1)}$ to be given over a ring of real numbers that have a selectivity coefficient $\kappa = 1$. These codewords can be constructed by solving the following matrix equations

$$CT^{+}_{□,4,(2,1)}C^{T} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ \alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad CT^{+}_{□,4,(3,1)}C^{T} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{11}$$

Solving these matrix equations using the property of the relationship between two-dimensional and one-dimensional DCT [21], we obtain the following codewords

$$\begin{gathered} T^{+}_{□,4,(2,1)} = \alpha \begin{bmatrix} 0.32665 & 0.32665 & 0.32665 & 0.32665 \\ 0.1353 & 0.1353 & 0.1353 & 0.1353 \\ -0.1353 & -0.1353 & -0.1353 & -0.1353 \\ -0.32665 & -0.32665 & -0.32665 & -0.32665 \end{bmatrix}; \\ T^{+}_{□,4,(3,1)} = \alpha \begin{bmatrix} 0.25 & 0.25 & 0.25 & 0.25 \\ -0.25 & -0.25 & -0.25 & -0.25 \\ -0.25 & -0.25 & -0.25 & -0.25 \\ 0.25 & 0.25 & 0.25 & 0.25 \end{bmatrix}. \end{gathered} \tag{12}$$

In the case of the codeword $T^{+}_{□,4,(3,1)}$, taking the value $\alpha = \sqrt{E}$ (where the energy of the codeword $T^{+}_{b,4,(3,1)}$ is equal to $E = 16$), we get exactly the codeword $T^{+}_{b,4,(3,1)}$, while the specified is not true for the codeword $T^{+}_{□,4,(2,1)}$. In order to map the codeword $T^{+}_{□,4,(2,1)}$ on the binary alphabet $\{\pm 1\}$, we must first take the value $\alpha = \sqrt{E}$, and then round the elements of the resulting matrix to the nearest integer. It is clear that the operation of rounding to the nearest integer will lead to damage of the original structure of the codeword and, accordingly, to the "scattering" of its energy over the other frequency components.

In Table 2 we list the possible codewords for $\mu = \{4,8,16\}$ that have an exclusive effect on one or another DCT transformant, which are characterized by absolute selectivity.

Table 2

Size 4×4	Size 8×8	Size 16×16
$T_{b,4,(1,1)}$, $T_{b,4,(1,3)}$, $T_{b,4,(3,1)}$, $T_{b,4,(3,3)}$	$T_{b,8,(1,1)}$, $T_{b,8,(1,5)}$, $T_{b,8,(5,1)}$, $T_{b,8,(5,5)}$	$T_{b,16,(1,1)}$, $T_{b,16,(1,9)}$, $T_{b,16,(9,1)}$, $T_{b,16,(9,9)}$

Among the DCT coefficients, the DC coefficient is guaranteed not to be affected by the "close neighbor" effect, since it is always determined by the zero frequency, its properties do not depend on the size of the codeword, which is confirmed by Table 1 (for $T^{+}_{b,n,(1,1)}$ the selectivity coefficient has a maximum value and does not change with change in μ). In addition, based on the results of research presented, for example, in [24], it can be argued that the DC coefficients are highly resistant to external influences, which can even exceed the AC coefficients, i.e. are preferred for the organization of steganographic transformation. Taking this into account, we will show that the resistance of the steganographic transformation organized using $T^{+}_{b,\mu,(1,1)}$, will increase with increase in the value of μ.

The matrix $T^{+}_{b,\mu,(1,1)}$ is symmetric, so it is possible to construct a spectral expansion for it in the form of outer products [25]

$$T^{+}_{b,\mu,(1,1)} = \sum_{i=1}^{\mu} \lambda_i u_i u_i^T , \tag{13}$$

where λ_i are real eigenvalues of $T^{+}_{b,\mu,(1,1)}$, and u_i are orthonormal lexicographically positive eigenvectors, $i = \overline{1,\mu}$. Since for $\forall\mu$: $\operatorname{rank}\left(T^{+}_{b,\mu,(1,1)}\right)=1$, relation (13) can be refined

$$T^{+}_{b,\mu,(1,1)} = \lambda_1 u_1 u_1^T , \tag{14}$$

where λ_1 is the only non-zero eigenvalue of $T^{+}_{b,\mu,(1,1)}$. Based on the Frobenius theorem [26], considering the indecomposability and non-negativity of the matrix $T^{+}_{b,\mu,(1,1)}$: $\lambda_1 > 0$. Using the formulas for calculating the energy E of $T^{+}_{b,\mu,(1,1)}$ through the eigenvalues of the matrix, as well as through its elements $T^{+}_{b,\mu,(1,1)}(i,j)$, $i,j=\overline{1,\mu}$, we have [18]

$$E = \sum_{i,j=1}^{\mu} \left(T^{+}_{b,\mu,(1,1)}(i,j)\right)^2 = \mu^2 = \sum_{i=1}^{\mu} \lambda_i^2 = \lambda_1^2 , \tag{15}$$

where

$$\lambda_1 = \mu . \tag{16}$$

Then by direct calculations from (14) we obtain that $u_1 = \left(\frac{1}{\sqrt{\mu}}, \frac{1}{\sqrt{\mu}}, ..., \frac{1}{\sqrt{\mu}}\right)^T$, which is the *n*-optimal vector of the space R^{μ} [18], denoted below as n^O, and the expression (14) itself is transformed to the form

$$T^{+}_{b,\mu,(1,1)} = \mu\left(\frac{1}{\sqrt{\mu}}, \frac{1}{\sqrt{\mu}}, ..., \frac{1}{\sqrt{\mu}}\right)^T \left(\frac{1}{\sqrt{\mu}}, \frac{1}{\sqrt{\mu}}, ..., \frac{1}{\sqrt{\mu}}\right) = \mu n^O \left(n^O\right)^T . \tag{17}$$

For the $\mu\times\mu$-block F of the DI matrix, a normal singular value decomposition is possible, which in the representation of outer products has the form [25]

$$F = \sum_{i=1}^{\mu} \sigma_i u_i v_i^T , \tag{18}$$

where σ_i are singular numbers F, $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_\mu \geq 0$, u_i, v_i are respectively left and right orthonormal singular vectors, u_i are lexicographically positive, $i = \overline{1, \mu}$. It is shown in [18] that for the original DI: $u_1 \approx v_1 \approx n^O$.

If F is a block of the matrix of the DI-container, then the stenographic transformation using the codeword $T^+_{b,\mu,(1,1)}$ in accordance with (6) will have the form

$$\begin{aligned} F + T^+_{b,\mu,(1,1)} &= \sum_{i=1}^{\mu} \sigma_i u_i v_i^T + \mu n^O \left(n^O\right)^T = \sigma_1 n^O \left(n^O\right)^T + \sum_{i=2}^{\mu} \sigma_i u_i v_i^T + \mu n^O \left(n^O\right)^T = \\ &= \left(\sigma_1 + \mu\right) n^O \left(n^O\right)^T + \sum_{i=2}^{\mu} \sigma_i u_i v_i^T . \end{aligned} \tag{19}$$

Thus, formally, steganographic transformation (6) for $D = T^+_{b,\mu,(1,1)}$ can be represented as a perturbation of the maximum singular value of the container block by a value equal to the size of the block (codeword). It is known [18] that the first singular triple F corresponds in DI mainly to the low-frequency component. If we look at the steganographic transformation (19) in the spatial domain $F + T^+_{b,\mu,(1,1)}$, then here the perturbation of each pixel is the same, equal to ± 1 and does not depend on the block size, but if we analyze the result of the steganographic transformation in accordance with the right side, then the obvious conclusion is that with growth of μ increases the perturbation of the low-frequency component. It is known that for the fundamental possibility of decoding the additional information, the perturbation that the container undergoes during the steganographic transformation must be greater than the perturbation that the steganographic message undergoes as a result of the attack. In this regard, it is obvious that with growth of μ, the ability of a steganographic message to resist a stronger attack increases, while *PSNR* does not change.

All the codewords presented in Table 1 have a unit rank, and even without being symmetric matrices, they can be represented in a form similar to (14), but using a singular value decomposition in the form of outer products

$$T^+_{b,\mu,(k,m)} = \sigma_1 u_1 v_1^T , \tag{20}$$

where $\sigma_1 > 0$ is the only nonzero singular value of $T^+_{b,\mu,(k,m)}$, u_1, v_1 are the left and right singular vector respectively corresponding to σ_1. Thus, any codeword, including $T^+_{b,\mu,(1,1)}$, is determined by the only singular triple corresponding to the maximum singular value, i.e. are focused mainly on low frequencies, which formally demonstrates the achievement of the goal of their construction. With an increase of μ, the first singular triple, taking into account the effect of a “close neighbor”, will correspond to an increasing number of close low frequencies (with the exception of $T^+_{b,\mu,(1,1)}$ considered above), and although the selectivity (10) will decrease, the total contribution of the low-frequency DCT coefficients will increase, considering the properties of the first singular triple. In this case, with increasing of μ, the perturbation and the number of perturbed low-frequency coefficients will increase, considering the “close neighbor” effect (at the same time, for definiteness and uniformity for any μ, we will consider the DCT coefficients belonging to the upper left triangle of the DCT matrix (Fig. 2) to be low-frequency, including the one to which the codeword is initially directed, as a result of steganographic transformation (6), thereby providing an increase in resistance to attacks against the embedded message.

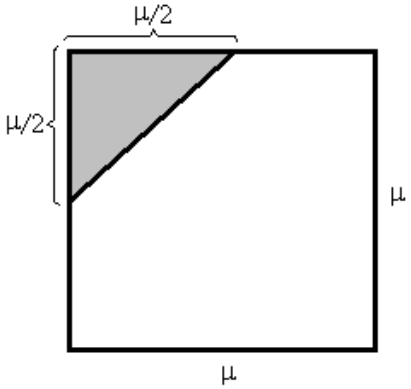


Fig. 2. Matrix of DCT $T^{+}_{b,\mu,(1,1)}$ coefficients with a selected area of coefficients considered as low-frequency

Table 3 illustrates the above, where data are presented on the values of the coefficient η which represents the ratio of the sum of absolute values of low-frequency DCT coefficients to the sum of absolute values of all other DCT coefficients for codewords used in the code-controlled information embedding steganographic method [21].

Table 3

DCT Transformant	Codeword, $\mu = 4$	η	Codeword, $\mu = 8$	η	Codeword, $\mu = 16$	η
(1,2)	$T^{+}_{b,4,(1,2)}$	2.4142	$T^{+}_{b,8,(1,2)}$	3.1165	$T^{+}_{b,16,(1,2)}$	3.8739
(2,1)	$T^{+}_{b,4,(2,1)}$	2.4142	$T^{+}_{b,8,(2,1)}$	3.1165	$T^{+}_{b,16,(2,1)}$	3.8739
(3,1)	$T^{+}_{b,4,(3,1)}$	-	$T^{+}_{b,8,(3,1)}$	2.4142	$T^{+}_{b,16,(3,1)}$	3.1165
(2,2)	$T^{+}_{b,4,(2,2)}$	-	$T^{+}_{b,8,(2,2)}$	0.4576	$T^{+}_{b,16,(2,2)}$	0.9305
(1,3)	$T^{+}_{b,4,(1,3)}$	-	$T^{+}_{b,8,(1,3)}$	2.4142	$T^{+}_{b,16,(1,3)}$	3.1165

Analysis of the data presented in Table 3 confirms that as the size of the codewords μ increases, the concentration of their energy in the low-frequency components increases, which leads to an increase in the resistance of the code-controlled steganographic method to attacks against the embedded message.

This is fully consistent with the coding theory [27], according to which

$$p_{e\,decode} \le 1 - p_{correct} - p_{corrected} = 1 - \sum_{i=1}^{t} C_n^i p_e^t (1 - p_e)^{N-1}, \qquad (21)$$

where $p_{e\,decode}$ is the probability of a decoding error, $p_{correct}$ is the probability of correctly receiving a codeword, $p_{corrected}$ is the probability of successfully correcting an error in a codeword, $t = \frac{d-1}{2}$ is the number of errors that can be guaranteed to be corrected by the code, d is the code distance of the correction code used, and $N = \mu^2$ is the length of the codewords of the code used.

In view of the fact that the code-controlled steganographic method uses a code consisting of a pair of codewords, one of which is the inverse of the other, its code distance is $d = N$, and, therefore, $t = \frac{N-1}{2}$.

On Fig. 3 we show the graphs of the decoding error probability $p_{e\,decode}$ dependence from the length of the codeword N for various values of the error probability p_e in the codeword symbol.

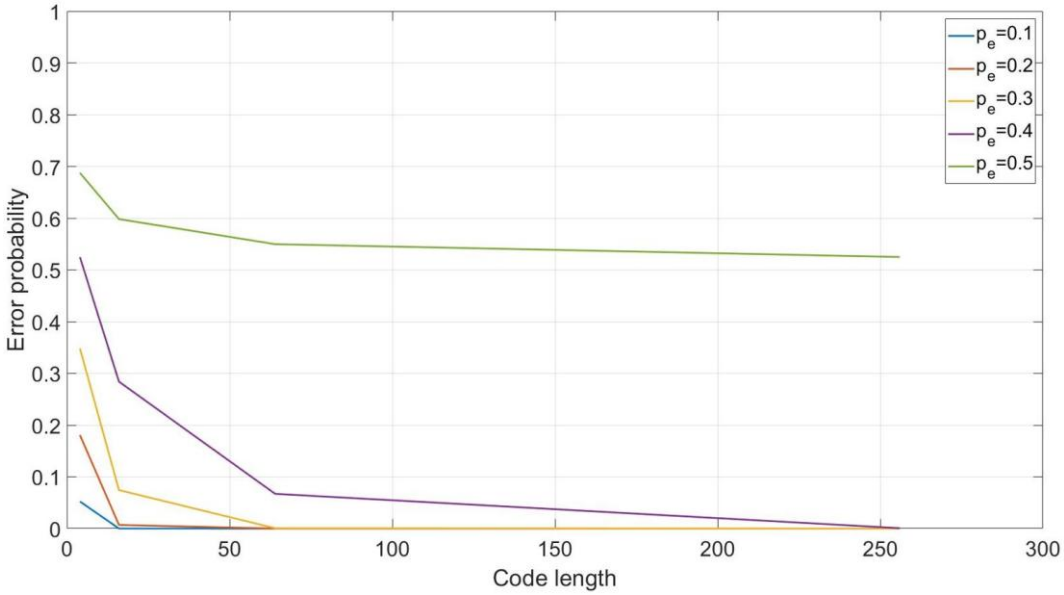


Fig. 3. Graphs of decoding error probability $p_{e\,decode}$ dependence from the codeword length N

Analysis of the data presented in Fig. 3 shows the decrease in the decoding error probability with increasing of codeword length. In this case, for the values of the decoding error probability $p_e \le 0.3$ for the length of the codeword $N = 64$, which corresponds to the value $\mu = 8$, the decoding error probability actually reaches zero.

The obtained results suggest that increasing the length of the codeword is one of the possibilities for increasing the resistance of the stenographic transformation to attacks against the embedded message, although the possibilities here are not unlimited, since an increase in the length of the codeword entails a decrease in the throughput of the generated covert communication channel.

Practical confirmation of the obtained theoretical conclusions are the results of computational experiments, some of which are presented in Fig. 2.

Thus, increasing the resistance of the code-controlled steganographic method to possible attacks by lossy compression, noise, and blurring is directly related to three tasks: increasing the energy of the codeword, which can be achieved by increasing of the absolute values of its elements, increasing the level of selectivity of the codeword, and also increasing of the length of the used codewords.

However, it is obvious here that in the case of an increase in the energy of the codeword, the reliability of the perception of the steganographic message worsens, in the case of an increase in the size of the codewords used, the throughput of the covert communication channel decreases. Increasing the selectivity of the used codewords, in the general case, is the task of optimizing of their structure, which does not lead to a deterioration in the characteristics of the steganographic method.

Conclusions

We note the main results of the research:

1. The definitions of the energy and the selectivity coefficient of the codeword used in the code-controlled steganographic method are introduced and substantiated. The values of the selectivity coefficient of codewords based on the rows of the Walsh-Hadamard matrix used in the code-controlled steganographic method are calculated. The existence of codewords with absolute selectivity is established and substantiated.

2. It has been established that with an increase in the size of the blocks used, there is a tendency to decrease in the selectivity coefficient value due to the presence of the “close neighbor” effect, which, however, occurs due to the use of transformants with similar frequencies that have similar resistance to possible attacks on the embedded message. In this case, the ratio of the sum of abso-

lute values of low-frequency DCT coefficients to the sum of absolute values of all other DCT coefficients grows with the size of the codeword. It has been proven and practically confirmed that an increase in the size of a codeword leads to an increase in the resistance of a code-controlled steganographic transformation.

3. Possible ways of further practical improvement of codewords used in the code-controlled steganographic method are established: increasing of their length, and also increasing of their selectivity. In the general case, the problem of increasing the selectivity of codewords is a problem of optimizing of their structure, the solution of which does not lead to a deterioration in other parameters of the steganographic method, which makes it a priority for further developing the direction of code-controlled embedding of additional information in the spatial domain of the container.

References:

1. Evsutin O., Melman A., Meshcheryakov R. Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions // IEEE Access, 2020. No. 8. P. 166589-166611. doi: 10.1109/ACCESS.2020.3022779
2. Zhu Z., Zheng N., Qiao T., Xu M. Robust Steganography by Modifying Sign of DCT Coefficients // IEEE Access, 2019. Vol. 7. P. 168613-168628. doi: 10.1109/access.2019.2953504
3. Bansal D., Chhikara R. An improved DCT based steganography technique // International Journal of Computer Applications. Vol. 102, No.14. P. 46-49. doi: 10.5120/17887-8861
4. Bao Z. et al. A robust image steganography based on the concatenated error correction encoder and discrete cosine transform coefficients // Journal of Ambient Intelligence and Humanized Computing. 2020. Vol. 11, No. 5. P. 1889-1901.
5. Rachmawanto E. H. et al.Secure image steganography algorithm based on dct with otp encryption // Journal of Applied Intelligent System, 2017. Vol. 2, No. 1. P. 1-11. doi: 10.33633/jais.v2i1.1330
6. Kadhim I. J., Premaratne P., Vial P. J. High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform // Cognitive Systems Research. 2020. Vol. 60. P. 20-32.
7. Valandar M. Y. et al. An integer wavelet transform image steganography method based on 3D sine chaotic map // Multimedia Tools and Applications. 2019. Vol. 78, No. 8. P. 9971-9989.
8. Atta R., Ghanbari M. A high payload steganography mechanism based on wavelet packet transformation and neutrosophic set // Journal of Visual Communication and Image Representation. 2018. Vol. 53. P. 42-54.
9. Emad E. et al. A secure image steganography algorithm based on least significant bit and integer wavelet transform // Journal of Systems Engineering and Electronics. 2018. Vol. 29,No. 3. P. 639-649.
10. Melnik M.A. Compression-resistant steganographic algorithm // Information security. 2012. No. 2(8). P. 99-106.
11. Subhedar M. S., Mankar V. H. Secure image steganography using framelet transform and bidiagonal SVD // Multimedia Tools and Applications. 2020. T. 79. №. 3. P. 1865-1886.
12. Chanu Y. J., Singh Kh. M., Tuithung T. A Robust Steganographic Method based on Singular Value Decomposition // International Journal of Information & Computation Technology, 2014. Vol. 4, No. 7. pp. 717-726.
13. Subhedar M. Image Steganography Using Ridgelet Transform and SVD. Proceedings of the International e-Conference on Intelligent Systems and Signal Processing. Springer, Singapore, 2022. P. 81-91.
14. Bhattacharyya S., Mondal S., Sanyal G. A Robust Image Steganography using Hadamard Transform. International Conference on Information Technology in Signal and Image Processing, Mumbai, 2013. P. 416-426.
15. Sheidaeian H., Zolfaghari B., Zobeiri M. An Efficient and Secure Approach to Multi-User Image Steganography Using CRC-Based CDMA. International Conference on Signal Acquisition and Processing. Singapore, 2011. Vol. 2. pp. 1-5.
16. Amirtharajan R., Rayappan J. B. B. Covered CDMA multi-user writing on spatially divided image. International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace &Electronic Systems Technology (Wireless VITAE), 2011. P. 1-5. doi: wirelessvitae.2011.5940912
17. Sneha P. S., Sankar S., Kumar A. S. A chaotic colour image encryption scheme combining Walsh–Hadamard transform and Arnold–Tent maps // Journal of Ambient Intelligence and Humanized Computing, 2020. Vol. 11, No. 3. P. 1289-1308. doi: 10.1007/s12652-019-01385-0
18. Kobozeva A. A., Horoshko V. A. Information security analysis. Kiev : Izd. GUIKT, 2009. 251 p.
19. Kostyrka O.V. Analysis on the benefits of spatial domain of cover image forsteganography transformation // Informatics and Mathematical Methods in Simulation.2013.No.3. P. 275-282.
20. Gribunin V. G., Okov I. N., Turintsev I. V. Digital steganography. M. : Solon-Press, 2009. 265 p.
21. Kobozeva A.A., Sokolov A.V. Robust Steganographic Method with Code-Controlled Information Embedding // ProblemeleEnergeticiiRegionale. 2021. Vol. 52, No. 4. P. 115-130.
22. Horadam K. J. Hadamard matrices and their applications. Princeton university press, 2012. 280 p.

23. NRCS Photo Gallery // United States Department of Agriculture. URL: https://www.nrcs.usda.gov/wps/portal/nrcs/main/national/newsroom/multimedia/
24. Prokhozhev N. N., Mikhailichenko O. V., and Korobeinikov A. G., Influence of external perturbations on DC coefficients of DCT matrices in grayscale images // Scientific and technical bulletin of information technologies, mechanics and optics. 2008. No. 56. P. 57-62.
25. Demmel J. Computational linear algebra. M. : Mir, 2001. 430 p.
26. Gantmakher F. R. Matrix Theory. M. : Nauka, 1966. 576 p.
27. Mazurkov MI Fundamentals of information transfer theory. Odessa : Science and Technology, 2005. 168p.

Received 05.10.2021

Information about the authors:
Kobozeva Alla Anatolyevna – Doctor of Science, Professor, Odessa Polytechnic National University, Head of the Department of Cybersecurity and Software; e-mail: alla_kobozeva@ukr.net; ORCID: https://orcid.org/0000-0001-7888-0499
Sokolov Artem Viktorovich – PhD, Odessa Polytechnic National University, Associate Professor in the Department of Cybersecurity and Software; e-mail: radiosquid@gmail.com; ORCID: https://orcid.org/0000-0003-0283-7229