Increasing the Efficiency of Blind Decoding of the Steganographic Method with Code Control of Additional Information Embedding

Sokolov A.V.[1], Ihnatenko O.O.[1], Balandina N.M.[2]
[1]Odesa Polytechnic National University, [2]National University "Odesa Law Academy"
Odesa, Ukraine

Abstract. Modern energy systems are often used as a medium for information transmission, including confidential information, which makes relevant the task of ensuring its security, which today is solved using not only cryptographic but also steganographic means that ensure concealment of the very fact of confidential information transmission. The steganographic method with code control of the additional information embedding possesses practical important qualities, but in its original form requires the presence of a container for successful information extraction, which is not always desirable in practice, while the known modification of this steganographic method allows blind decoding is characterized by an insufficient level of resistance to attacks against the embedded message. The purpose of this paper is to improve the efficiency of the steganographic method with code control of the additional information embedding and blind decoding. This purpose was achieved by identifying two factors that determine the occurrence of errors during blind decoding of additional information in the steganographic method with code control: variation of sub-blocks, and errors caused by attacks against the embedded message. We propose the theoretical and practical rationale for codewords that provide the best level of resistance to both factors. The most significant result of the paper is a reduction in the number of decoding errors of the steganographic method with code control of the additional information embedding and blind decoding by 12.01% compared to the result known in the literature through a reasonable choice of codewords used to embed the additional information.

***Keywords*:** steganography, code control, Walsh-Hadamard transform, compression attack, JPEG, robustness.

DOI: https://doi.org/10.52254/1857-0070.2024.2-62.11
UDC: 004.056

Creșterea eficienței decodării oarbe a metodei steganografice cu controlul codului pentru introducerea informațiilor suplimentare

Sokolov A.V.[1], Ihnatenko O.O.[1], Balandina N.M.[2]
[1]Universitatea Națională Politehnică din Odesa, [2]Universitatea Națională "Academia de Drept din Odesa"
Odesa, Ucraina

Rezumat. Sistemele energetice moderne sunt adesea folosite ca mijloc de transmitere a informațiilor, inclusiv a informațiilor confidențiale, ceea ce face relevantă sarcina asigurării securității acestora, care astăzi se rezolvă folosind mijloace nu doar criptografice, ci și steganografice care asigură ascunderea faptului însuși al transmiterii informațiilor confidențiale. Metoda steganografică cu control prin cod al înglobării informațiilor suplimentare posedă calități practice importante, dar în forma sa originală necesită prezența unui container pentru extragerea cu succes a informațiilor, ceea ce nu este întotdeauna de dorit în practică, în timp ce modificarea cunoscută a acestei metode steganografice permite decodarea oarbă se caracterizează printr-un nivel insuficient de rezistență la atacurile împotriva mesajului încorporat. Scopul acestei lucrări este de a îmbunătăți eficiența metodei steganografice cu controlul prin cod al încorporarii informațiilor suplimentare și al decodării oarbe. Acest scop a fost atins prin identificarea a doi factori care determină apariția erorilor în timpul decodării oarbe a informațiilor suplimentare în metoda steganografică cu control de cod: variația sub-blocurilor și erorile cauzate de atacurile împotriva mesajului încorporat. Propunem argumentele teoretice și practice pentru cuvintele de cod care oferă cel mai bun nivel de rezistență la ambii factori. Cel mai semnificativ rezultat al lucrării este o reducere a numărului de erori de decodare ale metodei steganografice cu control prin cod al înglobării informațiilor suplimentare și al decodării oarbe cu 12,01% față de rezultatul cunoscut în literatură printr-o alegere rezonabilă a cuvintelor de cod utilizate pentru introducerea informației suplimentare.

***Keywords*:** steganografie, control de cod, transformare Walsh-Hadamard, atac de compresie, JPEG, robustețe.

Повышение эффективности слепого декодирования стеганографического метода с кодовым управлением внедрением дополнительной информации

Соколов А.В.[1], Игнатенко Е.О.[1], Баландина Н.Н.[2]
[1]Национальный университет «Одесская политехника», [2]Национальный университет «Одесская юридическая академия»
Одесса, Украина

Аннотация. Современные энергосистемы зачастую используются в качестве среды для передачи информации, в том числе, конфиденциальной, что делает актуальной задачу обеспечения её безопасности, которая сегодня решается с использованием не только криптографических, но и стеганографических средств, обеспечивающих сокрытие самого факта передачи информации. К используемым на практике стеганографическим алгоритмам выдвигаются такие требования как обеспечение надежности восприятия стеганосообщения, высокая пропускная способность, стойкость к атакам против встроенного сообщения, простота реализации и низкая вычислительная сложность. Одновременное выполнения всех указанных требований характерно для стеганографического метода с кодовым управлением внедрением дополнительной информации, который, тем не менее, в своем оригинальном виде требует для успешного извлечения информации наличия контейнера, что не всегда является желательным на практике, тогда как известная модификация данного стеганографического метода допускающая слепое декодирование характеризуются недостаточным уровнем стойкости к атакам против встроенного сообщения. Целью данной работы является повышение эффективности стеганографического метода с кодовым управлением внедрением дополнительной информации и слепым декодированием. Поставленная цель была достигнута за счет выявления двух факторов, которые определяют появление ошибок при слепом декодировании дополнительной информации в стеганографическом методе с кодовым управлением — ошибки, обусловленные вариацией подблоков и атаками против встроенного сообщения. Установлено, что для нивелирования ошибок, обусловленных вариацией подблоков, внедрение информации должно происходить в высокочастотные коэффициенты, тогда как для нивелирования ошибок, обусловленных атаками против встроенного сообщения — в низкочастотные коэффициенты. Обосновано использование кодовых слов, обеспечивающих наилучший уровень стойкости к обеим факторам. Наиболее существенным результатом работы является снижение количества ошибок декодирования стеганографического метода с кодовым управлением внедрением дополнительной информации и слепым декодированием на 12.01% по сравнению с известным в литературе результатом путем обоснованного выбора кодовых слов, используемых для внедрения дополнительной информации.

Ключевые слова: стеганография, кодовое управление, преобразование Уолша-Адамара, атака сжатием, JPEG, устойчивость.

I. INTRODUCTION AND STATEMENT OF THE PROBLEM

Currently, the PLC (Power Line Communication) technology, which involves the use of power lines for the organization of high-speed communication, has gained significant popularity. The use of this technology makes it possible to significantly reduce costs for the organization of communication systems due to the use of existing infrastructure, as well as to provide access to high-speed networks in places where it is difficult to build additional information transmission lines.

Nevertheless, due to the spread of information in electrical networks and its possible leakage outside the protected perimeter, the use of PLC technology is associated with special requirements for the information protection subsystem. Often in communication systems based on PLC technology, cryptographic methods of information protection are used, however, when transmitting particularly sensitive information, the prospects of using digital steganography are also of interest.

Modern steganographic methods not only make it impossible for attackers to read information but also hide from them the very fact of the presence of this information [1]. Today, there is a rapid development of steganography, which has led to the emergence of new steganographic methods, for example, [2...7], however, the wide application of steganography, as well as a wide variety of tasks solved with the help of steganographic methods, leads to the need to further improve their efficiency.

Features of modern information transmission systems determine the relevance of the following criteria for the effectiveness of steganographic methods: ensuring the reliability of perception, resistance to attacks against the embedded message, sufficient bandwidth, and resistance to attacks against steganalysis.

To date, the provision of the specified characteristics for most steganographic methods requires the application of transform domains: discrete cosine transform, wavelet transform, and singular value decomposition of the matrices of the container blocks. Nevertheless, the widespread use of resource-constrained platforms such as mobile devices, IoT (Internet of Things) and IoBT (Internet of Battlefield Things) devices, UAVs (Unmanned Aerial Vehicles), and embedded systems, combined with the increasing role of streaming containers, primarily digital video, make it an important requirement to reduce the computational complexity of the applied steganographic methods. Taking into account the above, the priority today is the development of steganographic methods that operate in the spatial domain of the container and, thus, provide lower computational complexity [8]. Such methods were presented, for example, in papers [9...12], but all of them are characterized by the inability to resist attacks against the embedded message.

Recently, a steganographic method that is resistant to attacks against embedded messages has been developed that can ensure steganographic processing in a space domain, known as a steganographic method with code control of additional information embedding [13]. The specified method is characterized by a significant level of resistance to attacks against the embedded message while ensuring the reliability of the perception of the steganographic message and sufficient bandwidth.

Despite the breakthrough nature of the steganographic method with code control of additional information embedding, especially from the point of view of the possibility of its operation on resource-constrained platforms, it requires the availability of an original container for additional information extraction. The requirement for a container's availability to successfully extract additional information may inhibit the use of a steganographic method with code control of additional information embedding in those applications where increasing the length of the secret key due to the use of the container as a part of the secret key is not justified, or may become an obstacle to extracting additional information in real-time.

For example, when implementing additional information protection by application of the steganographic method to embed it into the video stream, which is transmitted from the UAV to the base station.

The presence of a situation in practice when the need to transfer the container is undesirable, led to the formation of the problem of modifying the steganographic method with code control of additional information embedding, the solution to which was proposed in the paper [14], where a modified steganographic method with code control of additional information embedding with blind decoding was presented.

Nevertheless, the paper [14] contains only conceptual elements regarding the possibility of blind information extraction when applying a steganographic method with code control of additional information embedding, while detailed research on the level of its resistance to attacks against the embedded message, as well as recommendations for the selection of applied codewords were not presented.

The results presented in this paper regarding increasing the efficiency of the steganographic method with code control of additional information embedding and blind decoding, in contrast to well-known analogs based on the use of neural networks [15], as well as those where the embedding of additional information occurs in the domain of discrete cosine transform or singular value decomposition of image blocks [16...19], is characterized by significantly higher reliability of perception of the steganographic message, while, in contrast to the method [14], it is characterized by greater resistance to the attacks against the embedded information.

In contrast to the original steganographic method with code control of additional information embedding [13], the results presented in [14] provide a fundamental possibility for blind decoding of additional information, which is important for solving many practical problems.

In addition, the results presented, unlike analogs [15...20], allow embedding and extraction of additional information in the spatial domain, which makes its algorithmic implementation efficient and high-performance.

II. The possibility of blind decoding for the steganographic method with code control of additional information embedding

For the sake of completeness, let us briefly consider the features of blind decoding of additional information in the steganographic method with code control of additional information embedding [14]. The basic idea of blind decoding is to divide the container block into four sub-blocks, among which the frequency components in which additional information is embedded are averaged, which allows setting a “zero point”, relative to which the effect on the frequency component into which the additional information was embedded is measured.

Let us introduce the concepts necessary to describe the steganographic method with code control of additional information embedding and blind decoding.

The matrix W of transformants of the two-dimensional Walsh-Hadamard transform of the block matrix X of size $N \times N$ is determined by the following relation

$$W = H'_N X H'^T_N, \; H'_N = \frac{1}{\sqrt{N}} H_N,$$
$$H_N = \begin{bmatrix} H_{N/2} & H_{N/2} \\ H_{N/2} & -H_{N/2} \end{bmatrix}, H_1 = [1], \tag{1}$$

where H_N and H'_N are the unnormalized and normalized Walsh-Hadamard matrices of order $N \times N$, respectively.

The vector of transformants V of the one-dimensional Walsh-Hadamard transform of the vector Y of length N is determined by the following relation

$$V = YH_N . \tag{2}$$

One of the theoretical achievements underlying the concept of code control of information embedding is the relationship between the transformants of the two-dimensional and one-dimensional Walsh-Hadamard transform [13], which can be written (to an accuracy of the coefficient $1/N$) using the operator $\tilde{A}$, which determines the writing of the matrix A of order $N \times N$ in the form of a row vector of length N^2 by sequential concatenation of the rows of the original matrix A

$$\tilde{W} = \tilde{X} H_{N^2}, \tag{3}$$

Consider the block of the original image X of size $\mu \times \mu$, which we will represent as four sub-blocks $\chi_i, i = 1,2,...,4$ of size $\mu/2 \times \mu/2$ by dividing the original block X as follows

$$X = \left[\begin{array}{c|c} \chi_1 & \chi_2 \\ \hline \chi_3 & \chi_4 \end{array}\right]. \tag{4}$$

In the steganographic method with code control of additional information embedding and blind decoding, the container block X is used to embed one bit of additional information d, while the specified bit is distributed to the sub-blocks $\chi_j, j = 1,2,...,4$. The embedding of additional information is performed in an additive way, while the block of steganographic message will be defined as follows

$$M = X + T_\mu, \tag{5}$$

where T_μ is a codeword of size $\mu \times \mu$, which is formed as follows

$$T_\mu = \left[\begin{array}{c|c} t_1 & t_1 \\ \hline -t_1 & -t_1 \end{array}\right] + \left[\begin{array}{c|c} t_2 & t_2 \\ \hline -t_2 & -t_2 \end{array}\right] + \ldots + \left[\begin{array}{c|c} t_n & t_n \\ \hline -t_n & -t_n \end{array}\right], \tag{6}$$

where $t_i, i = 1,2,...,n$ are codewords of size $\mu/2 \times \mu/2$, having the elementary structure [23] of the Walsh-Hadamard transform $\{(\mu/2)^2(1), 0((\mu/2)^2 - 1)\}$, i.e. each of the codewords $\left[\begin{array}{c|c} t_i & t_i \\ \hline -t_i & -t_i \end{array}\right]$ with additive embedding (5) is able to provide a selective effect on a given transformant of the Walsh-Hadamard transform of sub-blocks $\chi_j, j = 1,2,...,4$.

According to [23], in order for codewords t_i to have an elementary structure $\{(\mu/2)^2(1), 0((\mu/2)^2 - 1)\}$, they must be constructed by sequentially filling the corresponding matrix t_i of size $\mu/2 \times \mu/2$ with elements of the corresponding row of the Walsh-Hadamard matrix $H_{(\mu/2)^2}$.

Statement 1. The total impact on the transformants of the Walsh-Hadamard transform of the sub-blocks $\chi_j, j = 1,2,...,4$ during the additive embedding of additional information (5) using the codeword T_μ will be determined as the sum of the impacts from each codeword $t_i, i = 1,2,...,n$.

Proof. Since the method of splitting the codeword T_μ into codewords $t_i, i = 1,2,...,n$ of size $\mu/2 \times \mu/2$ corresponds to the method of splitting the container block X into sub-blocks, we can represent the block of the steganographic message M of size $\mu\times\mu$ as follows

$$M=\left[\begin{array}{c|c} m_1 & m_2 \\ \hline m_3 & m_4 \end{array}\right]=\left[\begin{array}{c|c} \chi_1 & \chi_2 \\ \hline \chi_3 & \chi_4 \end{array}\right]+ \\ +\left[\begin{array}{c|c} t_1 & t_1 \\ \hline -t_1 & -t_1 \end{array}\right]+ \\ +\left[\begin{array}{c|c} t_2 & t_2 \\ \hline -t_2 & -t_2 \end{array}\right]+\ldots+\left[\begin{array}{c|c} t_n & t_n \\ \hline -t_n & -t_n \end{array}\right], \qquad (7)$$

where

$$\begin{cases} m_1=\chi_1+t_1+t_2+\ldots+t_n; \\ m_2=\chi_2+t_1+t_2+\ldots+t_n; \\ m_3=\chi_3-t_1-t_2-\ldots-t_n; \\ m_4=\chi_4-t_1-t_2-\ldots-t_n, \end{cases} \qquad (8)$$

then taking into account (3), the transformants of the Walsh-Hadamard transform of the sub-blocks m_1, m_2, m_3, m_4 will be defined as

$$\begin{aligned} \tilde{W}_{m_1}&=\tilde{W}_{\chi_1}+\tilde{W}_{t_1}+\tilde{W}_{t_2}+\ldots+\tilde{W}_{t_n}; \\ \tilde{W}_{m_2}&=\tilde{W}_{\chi_2}+\tilde{W}_{t_1}+\tilde{W}_{t_2}+\ldots+\tilde{W}_{t_n}; \\ \tilde{W}_{m_3}&=\tilde{W}_{\chi_3}-\tilde{W}_{t_1}-\tilde{W}_{t_2}-\ldots-\tilde{W}_{t_n}; \\ \tilde{W}_{m_4}&=\tilde{W}_{\chi_4}-\tilde{W}_{t_1}-\tilde{W}_{t_2}-\ldots-\tilde{W}_{t_n}, \end{aligned} \qquad (9)$$

which proves Statement 1.

At the same time, if codewords having the elementary structure of the Walsh-Hadamard transform $\left\{(\mu/2)^2(1), 0((\mu/2)^2-1)\right\}$ are used as matrices t_i of size $\mu/2\times\mu/2$, the resulting impact on sub-blocks χ_j, $j=1,2,...,4$ of size $\mu/2\times\mu/2$ will consist of impacts on the transformants of the Walsh-Hadamard transform provided by the applied codewords t_i.

Statement 2. The largest absolute value of the amplitude of the influence of the codeword T_μ on the element of the image block X when using codewords based on the rows of the Walsh-Hadamard matrix $H_{(\mu/2)^2}$ will be equal to n.

Proof. Since, according to the construction of (1), the first column of the matrix $H_{(\mu/2)^2}$ will consist of elements +1, the elements of all codewords t_i with index (1,1), which are constructed based on the corresponding row of the Walsh-Hadamard matrix, will contain the value +1. Thus, in expression (8), the amplitude of the maximum absolute value of the sum $t_1+t_2+\ldots+t_n$, or the amplitude of the minimum absolute value of the difference $-t_1-t_2-\ldots-t_n$ in position (1,1) will be equal to n, i.e. the number of applied codewords t_i.

Statement 3. The structure of the codeword T_μ, which is determined by the influences of the codewords t_i on the transformants of the sub-blocks $\tilde{W}_{\chi_1}, \tilde{W}_{\chi_2}, \tilde{W}_{\chi_3}, \tilde{W}_{\chi_4}$ of the block X, can be recovered from the blocks of the steganographic message m_1, m_2, m_3, m_4, if the deviation of the Walsh-Hadamard transformants affected by the codewords t_i of the sub-blocks χ_j, $j=1,2,...,4$ from the arithmetic average of the corresponding transformants of these sub-blocks is sufficiently low.

Proof. Consider a vector containing the arithmetic average values of the transformants of the Walsh-Hadamard transform

$$\begin{aligned} \tilde{W}_{\bar{m}}&=\frac{1}{4}(\tilde{W}_{m_1}+\tilde{W}_{m_2}+\tilde{W}_{m_3}+\tilde{W}_{m_4})= \\ &=\frac{1}{4}(\tilde{W}_{\chi_1}+\tilde{W}_{t_1}+\tilde{W}_{t_2}+\ldots+\tilde{W}_{t_n}+ \\ &+\tilde{W}_{\chi_2}+\tilde{W}_{t_1}+\tilde{W}_{t_2}+\ldots+\tilde{W}_{t_n}+ \\ &+\tilde{W}_{\chi_3}-\tilde{W}_{t_1}-\tilde{W}_{t_2}-\ldots-\tilde{W}_{t_n}+ \\ &\tilde{W}_{\chi_4}-\tilde{W}_{t_1}-\tilde{W}_{t_2}-\ldots-\tilde{W}_{t_n})= \\ &=\frac{1}{4}(\tilde{W}_{\chi_1}+\tilde{W}_{\chi_2}+\tilde{W}_{\chi_3}+\tilde{W}_{\chi_4}), \end{aligned} \qquad (10)$$

which are determined exclusively by the Walsh-Hadamard transformants of sub-blocks χ_j, $j=1,2,...,4$.

Let us consider the matrix of differences of the transformant of the Walsh-Hadamard transform of the sub-blocks of the steganographic message m_1, m_2, m_3, m_4 and the average value of $\tilde{W}_{\bar{m}}$.

$$\left[\begin{array}{c|c} \Delta_1 & \Delta_2 \\ \hline \Delta_3 & \Delta_4 \end{array}\right]= \\ =\left[\begin{array}{c|c} \tilde{W}_{\chi_1}-\tilde{W}_{\bar{m}}+\tilde{W}_{t_1}+\ldots+\tilde{W}_{t_n} & \tilde{W}_{\chi_2}-\tilde{W}_{\bar{m}}+\tilde{W}_{t_1}+\ldots+\tilde{W}_{t_n} \\ \hline \tilde{W}_{\chi_3}-\tilde{W}_{\bar{m}}-\tilde{W}_{t_1}-\ldots-\tilde{W}_{t_n} & \tilde{W}_{\chi_4}-\tilde{W}_{\bar{m}}-\tilde{W}_{t_1}-\ldots-\tilde{W}_{t_n} \end{array}\right]. \qquad (11)$$

It is easy to see that under the conditions

$$\begin{cases} \tilde{W}_{\chi_1} - \tilde{W}_{\overline{m}} \to 0; \\ \tilde{W}_{\chi_2} - \tilde{W}_{\overline{m}} \to 0; \\ \tilde{W}_{\chi_3} - \tilde{W}_{\overline{m}} \to 0; \\ \tilde{W}_{\chi_4} - \tilde{W}_{\overline{m}} \to 0, \end{cases} \tag{12}$$

where 0 means a zero vector of order $(\mu/2)^2$, matrix $\left[\begin{array}{c|c} \Delta_1 & \Delta_2 \\ \hline \Delta_3 & \Delta_4 \end{array}\right]$ will reproduce the structure of the codeword T_μ, which determines the fundamental possibility of its decoding.

Note that in practice, condition (12) is not fulfilled for containers into which additional information is embedded, which potentially leads to errors when decoding the codeword T_μ. We will call such errors as determined by the variation of sub-blocks.

Applying the results of Statement 1 and Statement 2, let's write down an algorithm for additional information embedding:

Step 1. The original image is divided into blocks X_i of size $\mu \times \mu$ in a standard way.

Step 2. The additional information bit d_i is embedded in each of the blocks using the codeword T_μ of size $\mu \times \mu$, i.e. the *i*-th block of the steganographic message is defined as

$$M_i = X_i + (-1)^{d_i} T_\mu,$$
$$T_\mu = \left[\begin{array}{c|c} t_1 & t_1 \\ \hline -t_1 & -t_1 \end{array}\right] + \left[\begin{array}{c|c} t_2 & t_2 \\ \hline -t_2 & -t_2 \end{array}\right] + \ldots + \left[\begin{array}{c|c} t_n & t_n \\ \hline -t_n & -t_n \end{array}\right], \tag{13}$$

where $t_i, i = 1,2,...,n$ are the codewords of size $\mu/2 \times \mu/2$ affecting two selected Walsh-Hadamard transformants.

Applying the results of Statement 3, let's write down an algorithm for extracting additional information:

Step 1. The steganographic message M' 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 blocks of size $\mu/2 \times \mu/2$ according to the following construction $M'_i = \left[\begin{array}{c|c} m_1 & m_2 \\ \hline m_3 & m_4 \end{array}\right]$.

Step 3. For each block M'_i we calculate n matrices of size 2×2

$$u_i = \left[\begin{array}{c|c} \sum_{a=1}^{4}\sum_{b=1}^{4} m_1(a,b)t_i(a,b) & \sum_{a=1}^{4}\sum_{b=1}^{4} m_2(a,b)t_i(a,b) \\ \hline \sum_{a=1}^{4}\sum_{b=1}^{4} m_3(a,b)t_i(a,b) & \sum_{a=1}^{4}\sum_{b=1}^{4} m_4(a,b)t_i(a,b) \end{array}\right], i = 1,2,...,n, \tag{14}$$

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

Step 4. We find the average values

$$\overline{u_i} = \sum_{l=1}^{2}\sum_{m=1}^{2} u_i(l,m), i = 1,2,...,n \ . \tag{15}$$

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

$$d'_i = \text{sign}(\sum_{i=1}^{n}((u_i(1,1) - \overline{u_i}) + (u_i(1,2) - \overline{u_i}) - \\ -(u_i(2,1) - \overline{u_i}) - (u_i(2,2) - \overline{u_i})). \tag{16}$$

Taking into account the content of Statement 1 and Statement 2, as well as the practical results obtained in [14], it seems reasonable to use the value of the block size $\mu = 8$ and the value of $n = 2$, which are considered further in this paper. Nevertheless, the authors believe that the optimization of these parameters is of separate interest, which goes beyond the scope of the results presented in this paper and can become subject of further research.

III. The rationale for the selection of codewords t_1 and t_2

In the original steganographic method with code control of additional information embedding [13], the use of the matrix representation of the rows of the Walsh-Hadamard matrix of order N^2 as codewords is substantiated and it is shown that only such codewords provide a selective effect on one or another transformant of the Walsh-Hadamard transform.

Assuming that the codewords t_1 and t_2 have the order $N = 4$, they can be constructed from a Walsh-Hadamard matrix of order $N^2 = 16$ by representing its rows as matrices of size 4×4.

Let's show these codewords in Table 1, where each codeword is associated with the corresponding Walsh-Hadamard transformant which it affects.

For the sake of completeness, we will consider a specific example. Let the codeword ξ_3 to be given, which performs a concentrated influence on the Walsh-Hadamard transformant (1,3). Let's find the transformants of the Walsh-Hadamard transform (1) for it (up to the normalization factor $1/N$)

$$W_{\xi_3}=\begin{bmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{bmatrix}\begin{bmatrix}1&1&-1&-1\\1&1&-1&-1\\1&1&-1&-1\\1&1&-1&-1\end{bmatrix}\times$$
$$\times\begin{bmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{bmatrix}= \quad . \qquad (17)$$
$$=\begin{bmatrix}0&0&16&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix}$$

As can be seen from (17), the codeword ξ_3 indeed has a transformant matrix of the Walsh-Hadamard transform characterized by only one nonzero transformant.

The research performed made it possible to establish that when selecting one or another set of codewords $\xi_i,\xi_j, i,j=1,2,...,16$ as t_1 and t_2, the resulting resistance of the steganographic method will be influenced by two main factors, which we will consider in detail.

1. Variation of sub-blocks. According to the algorithm for extracting additional information in the researched steganographic method, the steganographic message is segmented into blocks of size $\mu\times\mu$, after which each resulting block is further segmented into sub-blocks of size $\mu/2\times\mu/2$, after which the values of the elements of the embedded codeword are determined by the "zero point", which is the average values of $\overline{u_i}, i=1,2,...,n$.

Assuming that the codewords used in the steganographic method selectively affect a given Walsh-Hadamard transformant, the average values of $\overline{u_i}, i=1,2,...,n$ are essentially the average values of the Walsh-Hadamard transformants affected by the codewords $t_i, i=1,2,...,n$.

In practice, it is possible that the standard deviation of values of these Walsh-Hadamard transformants in the specified sub-blocks of size $\mu\times\mu$ of block of size $\mu/2\times\mu/2$ exceeds the total amplitude of the codeword's influence on this transformant, which makes it impossible to extract additional information from this block.

Let's consider a specific example of this situation. Let the input image block of size 8×8 be given

$$X=\begin{bmatrix}150&143&146&145&142&142&145&144\\129&126&129&132&134&135&132&131\\119&118&120&126&129&129&129&128\\117&121&123&126&129&136&137&132\\121&128&130&132&139&137&139&139\\124&128&133&140&143&137&138&139\\128&128&137&141&138&142&140&138\\129&132&139&138&137&145&142&133\end{bmatrix}, \quad (18)$$

into which it is necessary to embed a bit of additional information $d=1$ using $n=2$ same codewords

$$t_1=\begin{bmatrix}1&1&1&1\\1&1&1&1\\-1&-1&-1&-1\\-1&-1&-1&-1\end{bmatrix}, t_2=\begin{bmatrix}1&1&1&1\\1&1&1&1\\-1&-1&-1&-1\\-1&-1&-1&-1\end{bmatrix}, (19)$$

that is, a codeword will be used to embed information

$$(-1)T_8=\begin{bmatrix}-2&-2&-2&-2&-2&-2&-2&-2\\-2&-2&-2&-2&-2&-2&-2&-2\\2&2&2&2&2&2&2&2\\2&2&2&2&2&2&2&2\\2&2&2&2&2&2&2&2\\2&2&2&2&2&2&2&2\\-2&-2&-2&-2&-2&-2&-2&-2\\-2&-2&-2&-2&-2&-2&-2&-2\end{bmatrix}, \qquad (20)$$

whereas the steganographic message will look like

$$M=X+(-1)T_8=$$
$$=\begin{bmatrix}148&141&144&143&140&140&143&142\\127&124&127&130&132&133&130&129\\121&120&122&128&131&131&131&130\\119&123&125&128&131&138&139&134\\123&130&132&134&141&139&141&141\\126&130&135&142&145&139&140&141\\126&126&135&139&136&140&138&136\\127&130&137&136&135&143&140&131\end{bmatrix}. (21)$$

Table 1.

Possible variants of the codewords t_1 i t_2

(1,1)	(1,2)	(1,3)	(1,4)
$\xi_1=\begin{bmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{bmatrix}$	$\xi_2=\begin{bmatrix}1&-1&1&-1\\1&-1&1&-1\\1&-1&1&-1\\1&-1&1&-1\end{bmatrix}$	$\xi_3=\begin{bmatrix}1&1&-1&-1\\1&1&-1&-1\\1&1&-1&-1\\1&1&-1&-1\end{bmatrix}$	$\xi_4=\begin{bmatrix}1&-1&-1&1\\1&-1&-1&1\\1&-1&-1&1\\1&-1&-1&1\end{bmatrix}$
(2,1)	(2,2)	(2,3)	(2,4)
$\xi_5=\begin{bmatrix}1&1&1&1\\-1&-1&-1&-1\\1&1&1&1\\-1&-1&-1&-1\end{bmatrix}$	$\xi_6=\begin{bmatrix}1&-1&1&-1\\-1&1&-1&1\\1&-1&1&-1\\-1&1&-1&1\end{bmatrix}$	$\xi_7=\begin{bmatrix}1&1&-1&-1\\-1&-1&1&1\\1&1&-1&-1\\-1&-1&1&1\end{bmatrix}$	$\xi_8=\begin{bmatrix}1&-1&-1&1\\-1&1&1&-1\\1&-1&-1&1\\-1&1&1&-1\end{bmatrix}$
(3,1)	(3,2)	(3,3)	(3,4)
$\xi_9=\begin{bmatrix}1&1&1&1\\1&1&1&1\\-1&-1&-1&-1\\-1&-1&-1&-1\end{bmatrix}$	$\xi_{10}=\begin{bmatrix}1&-1&1&-1\\1&-1&1&-1\\-1&1&-1&1\\-1&1&-1&1\end{bmatrix}$	$\xi_{11}=\begin{bmatrix}1&1&-1&-1\\1&1&-1&-1\\-1&-1&1&1\\-1&-1&1&1\end{bmatrix}$	$\xi_{12}=\begin{bmatrix}1&-1&-1&1\\1&-1&-1&1\\-1&1&1&-1\\-1&1&1&-1\end{bmatrix}$
(4,1)	(4,2)	(4,3)	(4,4)
$\xi_{13}=\begin{bmatrix}1&1&1&1\\-1&-1&-1&-1\\-1&-1&-1&-1\\1&1&1&1\end{bmatrix}$	$\xi_{14}=\begin{bmatrix}1&-1&1&-1\\-1&1&-1&1\\-1&1&-1&1\\1&-1&1&-1\end{bmatrix}$	$\xi_{15}=\begin{bmatrix}1&1&-1&-1\\-1&-1&1&1\\-1&-1&1&1\\1&1&-1&-1\end{bmatrix}$	$\xi_{16}=\begin{bmatrix}1&-1&-1&1\\-1&1&1&-1\\-1&1&1&-1\\1&-1&-1&1\end{bmatrix}$

Let's try to extract additional information from block (21), and we see that

$$u_1=u_2=\begin{bmatrix}98&24\\-4&28\end{bmatrix}, \qquad (22)$$

while the average values are $\overline{u_1}=36.5$ and $\overline{u_2}=36.5$. Thus, according to (16), we have

$$\begin{aligned}d_i'&=\operatorname{sign}((98-36.5)+(24-36.5)-\\&-(-4-36.5)-(28-36.5)+\\&+(98-36.5)+(24-36.5)-\\&-(-4-36.5)-(28-36.5))=\\&=\operatorname{sign}(61.5-12.5+40.5+8.5+\\&+61.5-12.5+40.5+8.5)=196.\end{aligned} \qquad (23)$$

As we can see, a significant difference in the values of the elements of the matrices u_1 and u_2 from the average values of $\overline{u_1}$ and $\overline{u_2}$, which is due to the peculiarities of the structure of the image block. This difference exceeds the amplitude of influence of each of the applied codewords $\left[\begin{array}{c|c}t_i&t_i\\\hline -t_i&-t_i\end{array}\right]$, and led to the fact that the value of the resulting sum under the sign operator became positive, which resulted to an error in the extraction of additional information.

Thus, the risk of an error exists in those image blocks of size 8×8, in which the difference between the values of the Walsh-Hadamard transformants used for additional information embedding from the average value among the sub-blocks of size 4×4 exceeds the amplitude of influence of each of codewords $\left[\begin{array}{c|c}t_i&t_i\\\hline -t_i&-t_i\end{array}\right]$.

In other words, to avoid the risk of an error in the information bit extracted, the standard deviation δ of the Walsh-Hadamard transformant of sub-blocks of size 4×4 of block of size 8×8 into which information is embedded must be less than the amplitude of influence of each of the codewords $\left[\begin{array}{c|c}t_i&t_i\\\hline -t_i&-t_i\end{array}\right]$ used for the embedding of additional information.

For our example, the information is embedded using the codewords (19) in the transformant (3,1). In our case, for block (18), we have the following values of Walsh-Hadamard transformants (3,1) for sub-blocks of size 4×4: $[130,56,\text{-}36,\text{-}4]$, and therefore the value of the standard deviation is $\sigma=73.073$, which is significantly higher than the value of 16. Thus, block (18) is at risk for possible errors related to the structural peculiarities of the image.

The research performed allowed us to conclude that for real images, different transformants of the Walsh-Hadamard transform are characterized by different expected values σ. To evaluate the values of σ for different Walsh-Hadamard transformants, the following experiment was performed. Segmentation into X_i blocks of size 8×8 was performed for 500 randomly selected images from the NRCS database [24] in JPEG format, for each of which a two-dimensional Walsh-Hadamard transform was found according to (1).

Afterward, among the obtained blocks, the number of blocks for which the standard deviation of the corresponding Walsh-Hadamard transformants of the sub-blocks of size 4×4 exceeds 16 was found, after which the corresponding bar chart was constructed, which is shown in Fig. 1.

The analysis of the data presented in Fig. 1 allows us to conclude that the smallest values of the number of blocks with $\sigma\geq16$ have the Walsh-Hadamard transformants with numbers (2,2), (2,4), (4,2), (4,4).

Thus, the use of these Walsh-Hadamard transformants for additional information embedding using the steganographic method with code control of additional information embedding and blind decoding will minimize the number of errors due to the variation of sub-blocks.

2. Errors caused by attacks against the embedded message. Today, there are many possible attacks against an embedded message, but the most common one is a compression attack. This is explained by the fact that, in practice, images are rarely transmitted over telecommunication systems or stored in an uncompressed form, lossy compression algorithms are most often applied to them, the most common of which is the JPEG algorithm.

Despite the fact that such lossy compression algorithms are constructed to make the distortions introduced into the image least noticeable to the human eye, their impact is enough to destroy the additional information, that is embedded using most steganographic methods, except for those that are constructed to be resistant to attacks against the embedded message.

According to [24], a sufficient condition for ensuring resistance to attacks against the additional information is known: "To ensure the insensitivity of a steganographic message to perturbing actions, it is enough to embed additional information in such a way that in the Walsh-Hadamard transforms domain it would result in the perturbation of elements corresponding to the low-frequency components of the block".

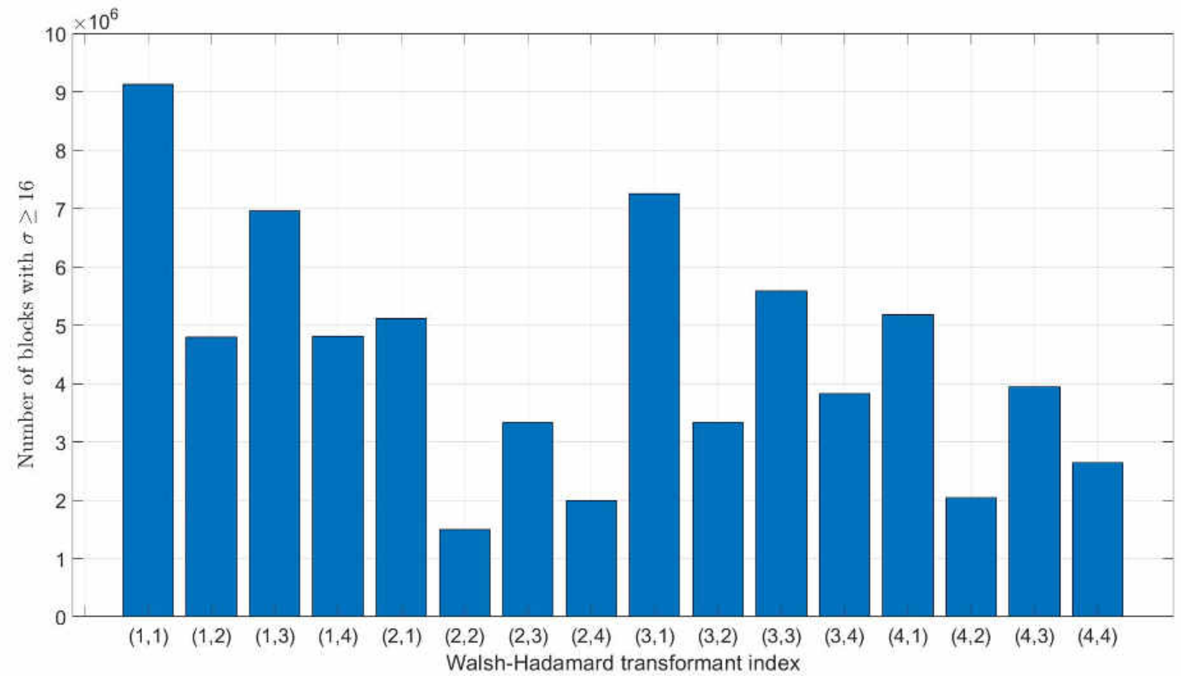

Fig. 1. Bar chart illustrating the number of blocks with the value $\sigma\geq16$.

For blocks of the size 8×8, we are talking about transformants with numbers: (1,1), (1,5), (5,1), (7,1), etc.

Note that, in accordance with the structure of codeword formation according to (6), we obtain the resulting codewords T_8 for $n=2$, which affect the corresponding transformants of the Walsh-Hadamard transform of the block of size 8×8, while the specific transformants of the Walsh-Hadamard transform affected by certain combinations of codewords $\xi_i, \xi_i, i=1,2,...,16$ are shown in Table 2.

Let's consider the data presented in Table 2 using a specific example. Using the formula (6), let's form the codeword T_8 based on ξ_3

$$T_8=\begin{bmatrix}\xi_3 & \xi_3\\ -\xi_3 & -\xi_3\end{bmatrix}+\begin{bmatrix}\xi_3 & \xi_3\\ -\xi_3 & -\xi_3\end{bmatrix}=$$

$$=\begin{bmatrix}2 & 2 & -2 & -2 & 2 & 2 & -2 & -2\\ 2 & 2 & -2 & -2 & 2 & 2 & -2 & -2\\ 2 & 2 & -2 & -2 & 2 & 2 & -2 & -2\\ 2 & 2 & -2 & -2 & 2 & 2 & -2 & -2\\ -2 & -2 & 2 & 2 & -2 & -2 & 2 & 2\\ -2 & -2 & 2 & 2 & -2 & -2 & 2 & 2\\ -2 & -2 & 2 & 2 & -2 & -2 & 2 & 2\\ -2 & -2 & 2 & 2 & -2 & -2 & 2 & 2\end{bmatrix}. \quad (24)$$

Let us find the two-dimensional Walsh-Hadamard transform of the matrix (24) using expression (1)

Table 2.

Walsh-Hadamard transformants affected by the codewords T_8 based on the codewords t_1, t_2

Codeword	ξ_1	ξ_2	ξ_3	ξ_4	ξ_5	ξ_6	ξ_7	ξ_8
Transformant	(5,1)	(5,2)	(5,3)	(5,4)	(6,1)	(6,2)	(6,3)	(6,4)
Codeword	ξ_9	ξ_{10}	ξ_{11}	ξ_{12}	ξ_{13}	ξ_{14}	ξ_{15}	ξ_{16}
Transformant	(7,1)	(7,2)	(7,3)	(7,4)	(8,1)	(8,2)	(8,3)	(8,4)

$$W_{T_8}=H_8T_8H_8^T=$$

$$=\begin{bmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1\\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1\\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1\\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1\\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1\end{bmatrix}\times\begin{bmatrix}2 & 2 & -2 & -2 & 2 & 2 & -2 & -2\\ 2 & 2 & -2 & -2 & 2 & 2 & -2 & -2\\ 2 & 2 & -2 & -2 & 2 & 2 & -2 & -2\\ 2 & 2 & -2 & -2 & 2 & 2 & -2 & -2\\ -2 & -2 & 2 & 2 & -2 & -2 & 2 & 2\\ -2 & -2 & 2 & 2 & -2 & -2 & 2 & 2\\ -2 & -2 & 2 & 2 & -2 & -2 & 2 & 2\\ -2 & -2 & 2 & 2 & -2 & -2 & 2 & 2\end{bmatrix}\times \quad (25)$$

$$\times\begin{bmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1\\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1\\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1\\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1\\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1\end{bmatrix}=\begin{bmatrix}0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 128 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\end{bmatrix}.$$

As can be seen from expression (25), the codeword T_8, which is built based on ξ_3, which affects transformant (3,1), does indeed provide an impact on transformant (5,3), as shown in Table 2.

It should be noted that the simultaneous use of different codewords t_1 and t_2 leads to the embedding of additional information in the corresponding combination of Walsh-Hadamard transformants. For example, if the matrices ξ_1 and ξ_9 are used as codewords t_1 and t_2, the resulting codewords T_8 will embed additional information in the Walsh-Hadamard transformants (5,1) and (7,1).

Thus, from the analysis of the data presented in Table 2, as well as taking into account the sufficient condition for ensuring the insensitivity of a steganographic message to disturbing actions, we can conclude that the best codewords in terms of the stability of a steganographic message to a compression attack are, first of all, the codewords ξ_1, ξ_9.

Nevertheless, according to Table 1, the codewords ξ_1, ξ_9 affect the Walsh-Hadamard transformants (1,1) and (3,1), respectively, which, according to Fig. 1, have the largest number of blocks with the value $\sigma\geq 16$, leading to errors due to the variation of sub-blocks.

Conversely, the use of codewords ξ_6, ξ_8, ξ_{14}, and ξ_{16} as t_1 and t_2, which affect the Walsh-Hadamard transformants characterized by the lowest number of blocks with the value $\sigma\geq 16$, leads to the following resulting codewords T_8, which ensure the embedding of additional information in the rather high-frequency Walsh-Hadamard transformants of the container (6,2), (6,4), (8,2), and (8,4), respectively, which does not allow to ensure the insensitivity of the steganographic message to disturbing actions.

In order to confirm the above considerations in practice, we will perform several experiments.

Experiment 1. The task solved with the help of this experiment is to research the operation of the steganographic method with code control of additional information embedding and blind decoding under the influence of a compression attack against the embedded message.

As part of this experiment, embedding of additional information in 150 randomly selected images from the NRCS database [24] was performed using codewords T_8, which are built on the basis of two identical codewords $\xi_i, \xi_i, i = 1,2,...,16$, which are used as t_1 and t_2. After embedding the additional information, the images were compressed by the JPEG algorithm with values of $QF = \{100, 90, 80, 70, 60, 50, 40, 30, 20, 10\}$.

Further, from the attacked steganographic message, additional information was extracted and the following estimation of the number of errors that occurred was performed.

The results regarding the number of errors that occurred for each of the codewords $\xi_i, \xi_i, i = 1,2,...,16$, as well as for each value of QF, are shown in the Table 3.

Analysis of the data presented in the Table 3 confirms the previously stated considerations. Thus, we can see that codewords based on matrices ξ_6, ξ_8 and ξ_{14} show the best results in terms of the number of errors when extracting additional information at values of $QF = \{100, 90\}$, that is, in fact, in conditions of minimal attack against the embedded information, which is explained by the small number of blocks with the value $\sigma \geq 16$.

On the other hand, the use of codewords ξ_1 and ξ_9, which ensure the embedding of additional information in the most low-frequency components for the steganographic method with code control of information embedding and blind decoding, as we can see from the results presented in the Table 3, provides the smallest increase in the number of errors when extracting additional information with a decrease in the value of QF.

Nevertheless, the large number of decoding errors due to variation of sub-blocks does not allow recommending them for practical use.

Thus, from a practical point of view, in order to ensure the operation of the steganographic method with code control of additional information embedding and blind decoding, a compromise is necessary between minimizing the number of errors due to the variation of sub-blocks (for which the embedding of additional information should be performed in high-frequency components) and maximizing the resistance to disturbing actions (for which the embedding of additional information should be performed to the low-frequency components of the block). The task of finding such a compromise is solved in the framework of the following experiments.

Table 3.

Results regarding the number of errors when extracting additional information under the conditions of an JPEG compression attack

$QF \setminus \xi_i, \xi_j$	ξ_1	ξ_2	ξ_3	ξ_4	ξ_5	ξ_6	ξ_7	ξ_8	ξ_9	ξ_{10}	ξ_{11}	ξ_{12}	ξ_{13}	ξ_{14}	ξ_{15}	ξ_{16}
100	9.5	0.5	2.6	1.1	2.5	0	0.3	0.1	5.9	0.2	1.7	0.8	2.5	0	0.4	0.2
90	9.6	0.9	2.8	1.2	2.5	0.4	0.8	0.5	5.7	0.4	2.0	1.1	2.5	0.5	0.9	0.6
80	9.8	1.1	3.6	1.6	2.3	24.2	9.4	20.2	6.3	0.8	2.7	2.0	3.0	22.8	4.6	17.5
70	9.8	17.1	4.0	2.5	3.9	27.7	19.3	29.5	6.8	18.9	3.4	3.2	3.1	27.3	16.8	29.6
60	9.9	24.1	4.7	3.3	13.9	29.9	24.7	31.8	7.1	24.7	4.1	10.0	3.6	30.1	25.3	32.0
50	10.3	27.0	5.5	4.9	19.3	31.2	28.3	33.3	7.4	28.0	7.3	29.1	4.6	31.6	28.4	33.4
40	11.2	30.0	9.7	15.4	25.2	33.2	31.1	34.9	8.3	30.8	19.7	33.4	10.7	33.3	31.3	34.7
30	12.6	33.0	24.9	33.0	29.4	35.1	33.9	36.3	9.7	33.9	29.3	35.7	23.0	35.2	34.0	36.4
20	18.7	36.1	33.5	37.9	34.1	37.4	37.0	38.5	21.5	36.8	35.3	38.4	31.5	37.7	37.0	38.5
10	36.0	41.3	40.8	42.5	39.3	41.8	42.1	42.3	37.7	41.6	41.7	42.4	38.7	42.0	41.9	42.5

Experiment 2. The task that is solved with the help of this experiment is to determine the codeword that provides the best resistance against the compression attack. The importance of this experiment is conditioned by the high prevalence of the JPEG compression algorithm, which is used in almost all systems for storing and transmitting digital images. For the experiment, 150 randomly selected images in JPEG format were selected from the NRCS database [24], into which information was embedded using the codewords T_8. Codewords

T_8 consist of t_1, t_2 according to the formula $T_8^+ = \left[\begin{array}{c|c} t_1 & t_1 \\ \hline -t_1 & -t_1 \end{array}\right] + \left[\begin{array}{c|c} t_2 & t_2 \\ \hline -t_2 & -t_2 \end{array}\right]$, where codewords t_1, t_2 of size $\mu/2 \times \mu/2$ are affecting two selected Walsh-Hadamard transformants (Table 1).

In the Table 4 we show percentages of errors for all combinations of codewords t_1 and t_2 at the value of $QF = 70$.

Experiment 3. The task solved with the help of this experiment is to evaluate the stability of the steganographic method with code control of additional information embedding and blind decoding when using different variants of codewords and to compare the obtained results with the best known analogues, in particular, with the results of the original steganographic method with code control of additional information embedding [13], as well as with a modified steganographic method with code control of additional information embedding and blind decoding [14].

Table 4.

Percentages of errors for all combinations of codewords t_1 and t_2

$\xi_i \setminus \xi_j$	ξ_1	ξ_2	ξ_3	ξ_4	ξ_5	ξ_6	ξ_7	ξ_8	ξ_9	ξ_{10}	ξ_{11}	ξ_{12}	ξ_{13}	ξ_{14}	ξ_{15}	ξ_{16}
ξ_1	9.8	13.9	11.0	10.6	13.2	14.2	13.9	14.1	10.7	13.9	11.8	13.3	10.3	14.2	13.8	14.2
ξ_2	13.8	17.1	7.4	11.8	19.6	25.4	23.2	25.2	10.9	23.5	13.0	23.2	9.0	26.4	25.0	25.4
ξ_3	11.1	7.4	4.1	6.2	9.4	10.1	9.6	10.0	8.2	9.7	6.9	8.9	6.2	10.9	11.6	10.1
ξ_4	10.6	11.8	6.2	2.5	11.0	13.2	11.7	13.9	8.3	11.8	7.4	12.7	6.2	13.2	11.8	18.8
ξ_5	13.2	19.6	9.4	11.1	3.9	21.6	20.1	21.9	9.0	20.2	12.3	19.6	8.4	21.7	20.1	21.9
ξ_6	14.2	25.4	10.1	13.2	21.6	27.7	24.6	29.5	11.6	24.7	10.5	27.0	9.4	29.2	25.7	29.8
ξ_7	13.9	23.2	9.6	11.7	20.1	24.6	19.3	26.0	11.1	21.1	5.8	23.8	8.8	25.9	23.5	26.3
ξ_8	14.1	25.1	10.0	13.9	21.9	29.5	26.1	29.5	11.7	26.0	14.2	15.4	9.3	29.4	25.9	30.9
ξ_9	10.7	10.9	8.2	8.3	9.0	11.6	11.1	11.7	6.8	11.1	8.7	10.5	7.7	11.6	10.9	11.7
ξ_{10}	13.9	23.5	9.7	11.9	20.2	24.6	21.1	26.0	11.1	18.9	7.1	23.9	8.9	26.1	23.4	26.4
ξ_{11}	11.7	13.0	6.9	7.4	12.3	10.5	5.9	14.2	8.7	7.0	3.4	12.9	6.4	14.2	13.1	14.3
ξ_{12}	13.3	23.2	8.8	12.7	19.6	27.0	23.8	15.5	10.5	23.9	12.9	3.2	8.3	26.8	23.8	28.3
ξ_{13}	10.3	9.0	6.2	6.2	8.4	9.4	8.8	9.3	7.7	8.9	6.4	8.3	3.1	9.3	8.6	9.3
ξ_{14}	14.2	26.4	10.8	13.3	21.7	29.2	25.9	29.4	11.6	26.2	14.1	26.9	9.3	27.3	23.8	29.6
ξ_{15}	13.7	25.0	11.6	11.8	20.1	25.7	23.5	25.9	10.9	23.4	13.1	23.8	8.7	23.8	16.8	26.2
ξ_{16}	14.2	25.4	10.1	18.8	21.9	29.8	26.3	30.9	11.7	26.4	14.3	28.2	9.3	29.6	26.2	29.6

To evaluate the level of stability of the steganographic method with code control of additional information embedding and blind decoding, 150 randomly selected images in JPEG format were selected from the NRCS database [24], and further experiments were performed on the extraction of additional information under the influence of a compression attack by the JPEG algorithm using:

- the original steganographic method with code control of additional information embedding with a codeword of size $\mu = 8$, which influences the Walsh-Hadamard transformant (5,4);
- the original steganographic method with code control of additional information embedding, with a codeword of size $\mu = 8$, which influences the transformant (5,1);
- the original steganographic method with code control of additional information embedding with blind decoding based on codewords ξ_9, ξ_6;
- the steganographic method with code control of additional information embedding with codewords, for the selection of which the rationale is proposed in this paper: ξ_4, ξ_4, which affect the transformant (5,4), as well as based on the codewords ξ_7, ξ_{11}, which affect the transformants (6,3) and (7,3).

On Fig. 2 we present graphs of the dependence of the number of errors that occur from the degree QF of compression of the image by the JPEG algorithm for all the codewords discussed above, which allows us to evaluate the effectiveness of their use in resisting compression attacks against the embedded message.

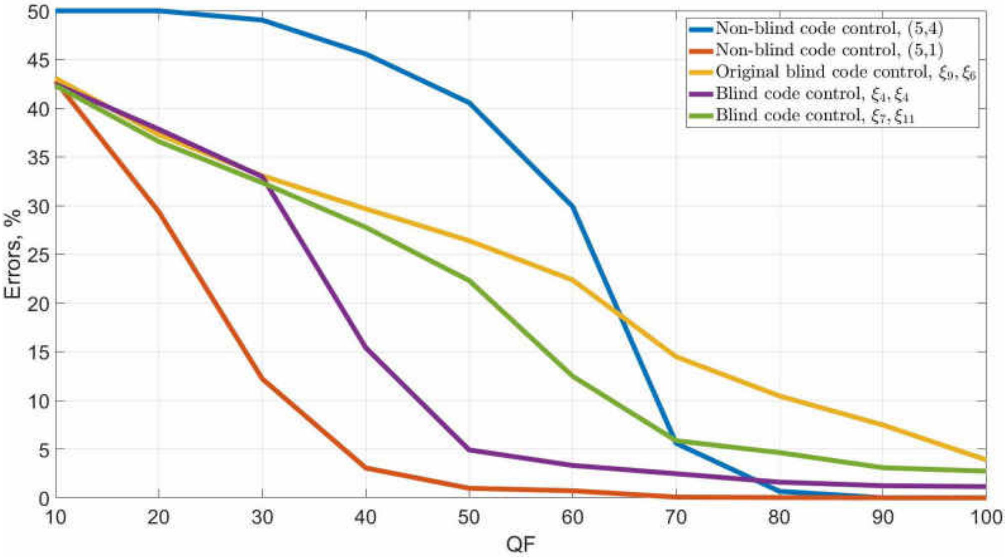

Fig. 2. Graph of the dependence of the number of errors when extracting additional information on the value of QF for the steganographic method with code control in its variations.

Analysis of the data presented on Fig. 2 shows that the use of codewords ξ_4, ξ_4, and ξ_7, ξ_{11}, in the steganographic method with code control of additional information embedding and blind decoding under the influence of the JPEG compression attack allows to reduce the number of errors for the decoding values under the influence of the JPEG compression attack in comparison with the original version of this method [14], which is based on the codewords ξ_9, ξ_6.

So, according to the data presented on Fig. 2 when using codewords ξ_4, ξ_4 in the steganographic method with code control of additional information embedding and blind decoding under the influence of a compression attack, only 2.4% more errors are observed when compared with the original steganographic method with code control without blind decoding [13] based on one of the best codeword of size $\mu = 8$, affecting the Walsh-Hadamard transformant (5,1).

IV. The characteristics of the steganographic method with code control of additional information embedding and blind decoding, as well as its comparison with best existing analogues

The steganographic method with code control of additional information embedding and blind decoding is characterized by the same advantages as the original version of the steganographic method with code control of additional information embedding [13], in particular, ensuring high reliability of steganographic message perception. In order to estimate the reliability of perception of a steganographic message, the PSNR indicator is generally accepted (although it does not comprehensively estimate the reliability of perception), which is defined as follows

$$PSNR = 20\lg\left(\frac{255}{\sqrt{MSE}}\right), \quad (26)$$

where the MSE is defined as

$$MSE = \frac{1}{nm}\sum_i\sum_j \left|X(i,j) - M(i,j)\right|^2, \quad (27)$$

where X is the matrix of the original image, M is the matrix of the steganographic message.

Considering the structure of the steganographic method with code control of additional information embedding, the PSNR indicator is stable, does not depend on the size of the container, but depends only on the set of codewords used. Thus, it was established that in the case of using the same codewords $\xi_i, \xi_i, i = 1,2,...,16$ as t_1 and t_2, all the elements of the resulting codewords T_8 are the same in amplitude, which is equal to 2. In this case the PSNR value of the steganographic message is 36.1315 dB.

In the case of different codewords $\xi_i, \xi_j, i, j = 1,2,...,16, i \neq j$ are selected as t_1 and

t_2, the elements of the resulting codewords are different in amplitude, and at the same time the maximum amplitude of these elements does not exceed the value of 2. In this case, the PSNR of the resulting steganographic message is equal to 42.1524 dB.

In any case, when applying the steganographic method with code control of additional information embedding and blind decoding, the influence on the pixel intensity of the container is insignificant and strictly controlled, which allows to achieve both high PSNR indicators and eliminate the occurrence of any artifacts in the resulting steganographic messages. For example, in Fig. 3 we show an example of an original image and a steganographic message obtained using the steganographic method with code control of additional information embedding with blind decoding using codewords ξ_4, ξ_4 as t_1 and t_2. At the same time, the size of the container in JPEG format, in which the additional information was embedded, is 1200x1200 pixels, the embedding took place in the YCbCr color space in the Y component, thus the amount of additional information was 22500 bits.

Analysis of the data presented on Fig. 3 using subjective ranking makes it possible to conclude that there are no visible distortions or artifacts on the steganographic message.

We will perform a comparative analysis of the steganographic method with code control of additional information embedding and blind decoding with the best-known analogues characterized by resistance to attacks against the embedded message.

In the Table 5 we compare the steganographic method with code control and blind decoding based on codewords ξ_4, ξ_4, as well as based on codewords ξ_7, ξ_{11} according to the following criteria: resistance to compression attack, reliability of perception which is estimated by the PSNR indicator, bandwidth R, embedding domain, and possibility of blind decoding.

In the Table 5 the following designations are adopted: S — spatial domain, DCT — discrete cosine transform domain, SVD — singular value decomposition domain, NN — steganographic transformation is performed using a neural network.

Analysis of the data presented in Table 5 shows that the steganographic method with code control of additional information embedding and blind decoding under the influence of a compression attack with the value $QF = 70$, which is usual for most modern digital image transmission systems, allows to ensure 2.47% of

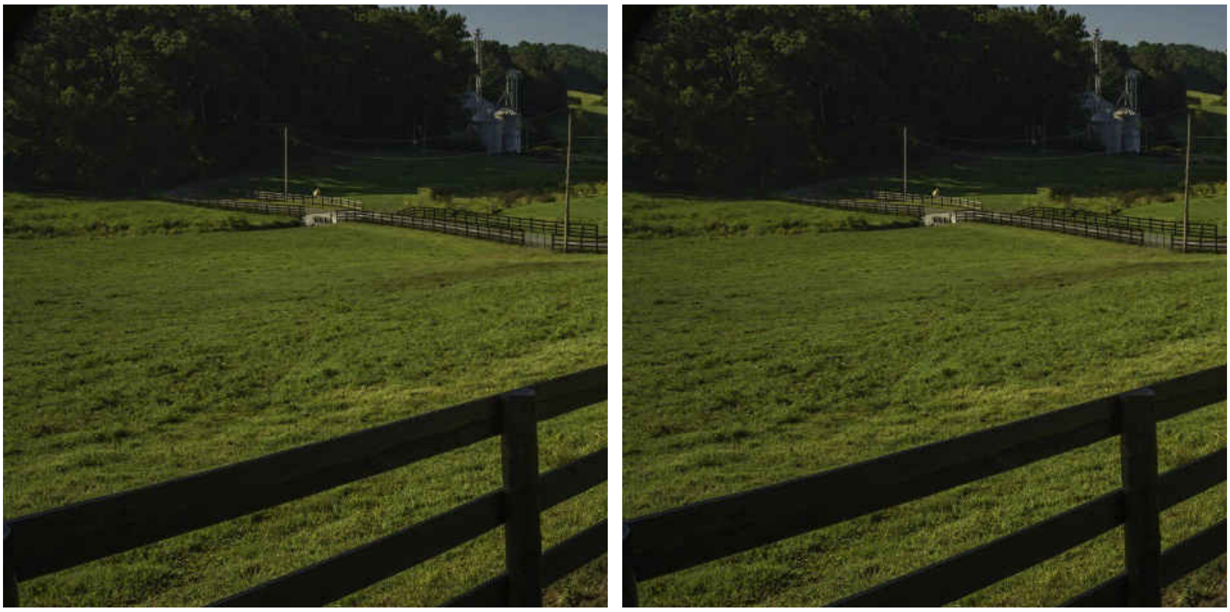

Fig. 3. An example of an original image (a) and a steganographic message (b) obtained using a steganographic method with code control of additional information embedding and blind decoding.

Table 5.

The results of comparative analysis of the steganographic method with code control of additional information embedding and blind decoding with best known analogues

Algorithm / Method	% of errors at a given level of *QF*										PSNR, dB	R	Dom.	Blind
	10	20	30	40	50	60	70	80	90	100				
Steganographic method with code control of additional information embedding [13]														
$T_{(5,1)}$	42.78	29.35	12.21	3.05	0.97	0.72	0.07	0.03	0	0	48.1	1/16	S	–
$T_{(5,4)}$	50	50	49.04	45.56	40.56	29.90	5.60	0.70	0	0	48.1	1/64	S	–
Steganographic method with code control of additional information embedding and blind decoding														
Original [14]	43.09	37.29	33.06	29.66	26.40	22.36	14.48	10.45	7.47	3.89	42.2	1/64	S	+
ξ_4, ξ_4	42.47	37.83	32.96	15.40	4.91	3.32	2.47	1.60	1.23	1.14	36.1	1/64	S	+
ξ_7, ξ_{11}	42.33	36.58	32.35	27.76	22.30	12.48	5.86	4.63	3.09	2.73	42.2	1/64	S	+
Modern analogues														
Li, 2021, [15]	—	—	0.02	—	0.02	—	0.01	—	0.01	0.01	~27.1	0.01	NN	+
Wang, 2021, [17]	—	—	0	—	0	—	—	0	—	0	~38.5	0.01	DCT	+
Zhu, 2019, [20]	—	—	—	—	—	—	33.9	7.4	0.3	—	~45	<1/8	DCT	+
Chanu, 2014, [18]	—	—	—	—	23.88	14.1	2.76	0.08	0.08	—	~32.7	1/16	SVD	+
Melnik, 2012, [19]	13	7	5	4	2	2	2	2	2	—	~ 34.7	1/64	SVD	+
Chang, 2007, [16]	—	—	—	—	24.7	14.4	2.71	0.2	0.1	—	~32.7	1/64	SVD	+

errors when using codewords ξ_4, ξ_4, which is 12.01% less than the original steganographic method with code control of additional information embedding and blind decoding [14], with a PSNR reduction of 6.1 dB.

However, with the same value of PSNR, using codewords ξ_7, ξ_{11}, the number of errors is 5.86%, which is 8.62% less than when using the original steganographic method with code control of additional information embedding and blind decoding. The results obtained in the sense of the ratio of the reliability of perception of the steganographic message and its resistance to attacks against the embedded message are better than such analogues as the algorithms proposed by Zhu, Chanu, and Melnyk, while in the steganographic method with code control of additional information embedding and blind decoding, the embedding of additional information occurs in spatial domain, which makes its computational efficiency much better than the listed analogues. It should be noted that such a modern analogue as the Wang algorithm, although is characterized by a fairly high resistance to attacks against the embedded message while ensuring a high level of reliability of perception, but is extremely sensitive to the properties of the selected container, which makes more than 50% of containers unsuitable for embedding. Such a drawback actually makes it impossible to use this method with streaming containers.

CONCLUSIONS

Let's note the main results of the research performed:

1. The number of errors during the extraction of additional information that occur without the influence of an attack against the embedded message for the steganographic method with code control of additional information embedding and blind decoding, as well as its resistance to attacks against the embedded message, primarily compression attacks, largely depends on the applied codewords. At the same time, the research performed made it possible to establish two factors that affect the number of decoding errors: the variation of sub-blocks, which acts independently of the presence of a compression attack and is caused by the presence of blocks from the risk group with values of standard deviation exceeding the value of the amplitude of the influence of the codeword, as well as errors conditioned by the attacks against the embedded message.

2. It was found that the number of blocks from the risk group, for which the value of the standard deviation of the Walsh-Hadamard

transformants of the sub-blocks exceeds the value of the amplitude of the influence of the codeword, is the lowest for the transformants of the Walsh-Hadamard transform corresponding to the high-frequency components of the container. At the same time, according to the sufficient condition for ensuring the insensitivity of the steganographic message to disturbing actions, the embedding of additional information must be performed in the transformants of the Walsh-Hadamard transform, which correspond to the low-frequency components of the container, which, in turn, are characterized by the presence of a large number of blocks characterized by high values of the standard deviation of the Walsh-Hadamard transformants of sub-blocks. Thus, the requirement to minimize the number of errors due to variation of sub-blocks for a steganographic method with code control of additional information embedding and blind decoding conflicts with the requirement to ensure that the steganographic message is robust against compression attacks.

3. The research performed made it possible to determine which codeword is the best from a practical point of view and provide the highest level of resistance to attacks against the embedded message with a small number of errors caused by variation of sub-blocks. Thus, during the compression attack with $QF = 70$ the use of codewords ξ_4, ξ_4 allows to ensure 2.47% of errors, which is 12.01% less than for the original steganographic method with code control of additional information embedding and blind decoding, while when using codewords ξ_7, ξ_{11}, the number of errors is 5.86%, which is 8.62% less than when using the original steganographic method with code control of additional information embedding and blind decoding. A comparative analysis of the obtained results with the best existing analogues providing blind decoding made it possible to establish that the steganographic method with code control of additional information embedding and blind decoding is characterized by the best ratio of ensuring resistance to attacks against the embedded message when performing steganographic transformation in the spatial domain, which allows to obtain a high level of computational efficiency, which allows the application of this method, in particular, on resource-constrained devices.

References

[1] Kobozeva A. A., Horoshko V. A. Analiz informacionnoj bezopasnosti [Information security analysis]. Kiev: Izd. GUIKT, 2009. 251 p. (In Russian)

[2] 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.

[3] Kumar A., Rani R., Singh S. A survey of recent advances in image steganography. Security and Privacy. 2023. Vol. 6. No. 3. P. e281.

[4] Rustad S. et al. Digital image steganography survey and investigation (goal, assessment, method, development, and dataset). Signal Processing. 2023. Vol. 206. P. 108908.

[5] Luo J. et al. Reversible adversarial steganography for security enhancement. Journal of Visual Communication and Image Representation. 2023. Vol. 97. P. 103935.

[6] Rahman S. et al. Multi Perspectives Steganography Algorithm for Color Images on Multiple-Formats. Sustainability. 2023. Vol. 15. No. 5. P. 4252.

[7] Patwari B., Nandi U., Ghosal S. K. Image steganography based on difference of Gaussians edge detection. Multimedia Tools and Applications. 2023. P. 1-21.

[8] Kostyrka O.V. Analiz preimushhestv prostranstvennoj oblasti cifrovogo izobrazhenija-kontejnera dlja steganopreobrazovanija [Analysis on the benefits of spatial domain of cover image forsteganography transformation]. Informatika ta matematichni metodi v modeljuvanni [Informatics and Mathematical Methods in Simulation]. No. 3. P. 275-282. (In Russian)

[9] Jianhua Yang et al. Spatial Image Steganography Based on Generative Adversarial Network. Spatial Image Steganography Based on Generative Adversarial Network. arXiv:1804.07939v1. P. 1-7.

[10] Hussain M. et al. Image steganography in spatial domain: A survey. Signal Processing: Image Communication. 2018. Vol. 65. P. 46-66. doi: 10.1016/j.image.2018.03.012

[11] Samidha D., Agrawal D. Random image steganography in spatial domain. International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System, 2013. pp. 1-3. doi: 10.1109/icevent.2013.6496564

[12] Hu D. et al. A spatial image steganography method based on nonnegative matrix factorization. IEEE signal processing letters. 2018. Vol. 25. No. 9. pp. 1364-1368. doi: 10.1109/lsp.2018.2856630

[13] Kobozeva A.A., Sokolov A.V. Robust Steganographic Method with Code-Controlled Information Embedding. Problemele energeticii re-

gionale. 2021. No. 4 (52). P. 115-130. doi: 10.52254/1857-0070.2021.4-52.11

[14] Ziginova Yu.K. Modifikovanij steganografichnij metod z kodovim upravlinnyam vbudovuvannyam dodatkovoyi informaciyi iz slipim dekoduvannyam [Modified steganographic method with code control of additional information embedding with blind decoding]. Mizhnarodna naukovo-praktichna konferenciya «Suchasni aspekti didzhitalizaciyi ta informatizaciyi v programnij ta komp'yuternij inzheneriyi» [International scientific and practical conference "Modern aspects of digitalization and informatization in software and computer engineering"], June 1-3, 2023. P. 68-70.

[15] Li Z., Zhang M., Liu J. Robust image steganography framework based on generative adversarial network. Journal of Electronic Imaging. 2021. Vol. 30, Issue 2. P. 023006 doi: 10.1117/1.JEI.30.2.023006

[16] Chang C. C., Lin C. C., Hu Y. S. An SVD oriented watermark embedding scheme with high qualities for the restored images. International journal of innovative computing, information & control. 2007. Vol. 3, No. 3. P. 609-620.

[17] Wang S., Zheng N., Xu M. A Compression Resistant Steganography Based on Differential Manchester Code. Symmetry. 2021. Vol. 13, No. 2. P. 345. doi: 10.3390/sym13020165

[18] 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. P. 717-726.doi: 10.1049/ic:20070706

[19] Melnik M. A. Compression-resistant steganographic algorithm. Information security. 2012. No. 2(8). P. 99-106.

[20] 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

[21] Mazurkov M. I. Sistemy shirokopolosnoj radiosvjazi [Broadband radio systems]. Odessa : Nauka i Tehnika [Odessa: Science and Technology], 2010. 340 p.

[22] Logachev O. A., Sal'nikov A. A., Jashhenko V. V. Bulevy funkcii v teorii kodirovanija i kriptologii [Boolean functions in coding theory and cryptology]. M.: MCNMO, 2004. 472 p. (In Russian)

[23] Mazurkov M.I., Sokolov A.V., Barabanov N.A. Synthesis method for bent sequences in the Vilenkin-Chrestenson basis. Radioelectronics and Communications Systems, 2016. Vol. 59, N 11. P. 510-517. doi: 10.3103/S0735272716110054

[24] Natural Resources Conservation Service (NRCS) // United States Department of Agriculture. URL: https://www.nrcs.usda.gov "

Information about authors.

Sokolov Artem Viktorovich. Odesa Polytechnic National University. Department of Cybersecurity and Software, Associate Professor, Doctor of Technical Sciences. Research interests include information security methods based on perfect algebraic constructions.
E-mail: radiosquid@gmail.com

Ihnatenko Olena Olehivna. Odesa Polytechnic National University. Department of Cybersecurity and Software, Student of Cybersecurity and Social Engineering. Research interests include steganography and social engineering.
E-mail: elenaignatenko19082002@gmail.com

Balandina Natalia Mykolayivna. National University “Odesa Law Academy”. Department of Cybersecurity. Senior lecturer. Research interests include mathematical methods in information protection systems.
E-mail: nataliabalandina2103@gmail.com