DOI 10.15276/imms.v14.no4.273
UDC 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 4, pp. 273-283

STEGANALYSIS OF A METHOD WITH CODE CONTROL OF INFORMATION EMBEDDING IN THE WALSH-HADAMARD TRANSFORM DOMAIN

O. O Lanovska[1], A. V. Sokolov[2]

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

Steganography is an integral part of modern information protection systems. The steganographic method with code control of information embedding is a modern steganographic method that operates in the spatial domain of the container. The advantages of this method include: ensuring the reliability of perception, resistance to attacks against the embedded message, sufficient bandwidth, and high computational efficiency. In contrast to steganographic methods, steganalysis methods are created to allow the detection of embedded information. To date, no research has been performed on the resistance of the steganographic method with code control to cryptanalysis attacks. The specific methods for detecting interference using the steganographic method with code control are also unknown. The purpose of this paper is to develop a steganalysis method for detecting a covert channel organized using the steganographic method with code control of information embedding in the Walsh-Hadamard transform domain. In the paper, the research on the behavior of the Walsh-Hadamard transformants of containers and steganographic messages is performed, which allowed us to formulate the conditions for the presence of additional information in the image. These conditions became the basis for the development of an efficient and mathematically simple steganographic method that uses the Walsh-Hadamard transform domain. The performed research on the proposed method allowed us to establish its high efficiency in various conditions with low computational complexity. In particular, it is shown that the efficiency of the proposed method exceeds the efficiency of the histogram analysis method and methods implemented in the well-known StegExpose tool. The results obtained allow us to recommend the proposed steganographic method for practical application for detecting covert communication channels created using the steganographic method with code control. In particular, the simplicity of its algorithmic implementation makes the proposed method effective in conditions of constrained computing resources.

Keywords: steganography, Walsh-Hadamard transform, steganalysis, code control of information embedding.

Introduction and statement of the problem. The constant development of information technologies and their integration into all areas of societal activities occurs in the modern World. This increases the importance of information security systems, while the growing share of multimedia information in global traffic leads to the rising significance of steganographic methods in information protection systems. These methods can conceal the very fact of the protected information's existence. New steganographic methods are continually evolving and improving, which, in turn, emphasizes the importance of developing steganalysis methods in parallel. In situations where the transmission of information through covert channels can become critically important, the development of fast and computationally efficient methods for detecting these covert channels becomes crucial. These methods should consider the specifics of particular techniques to achieve more accurate results.

At the moment, there are many steganographic methods, but they are mainly divided into two categories: the first category involves hiding data in the spatial domain, and the second — in the domain of container transformants.

Methods operating in the spatial domain of the container, for example, the classical LSB method, are characterized by high computational efficiency, high bandwidth, and the ability to easily ensure the reliability of perception, which, despite their simplicity, makes them quite widespread in practice. As the modern versions of the implementation of the LSB method we can consider, for example, the method [1], the main focus of which is on ensuring high bandwidth of the covert channel; method [2], depending on the marking algorithm of connected components; a method [3] that hides more of the secret message in the (sharpest) edges of the image, etc. Such a modification of the LSB methods as LSB-matching (LSBM) also must be considered [4]. The disadvantages of most methods working in the spatial domain of the container include their instability to attacks against the embedded message (for example, compression or noise attacks), and instability to steganalysis.

The methods applying container transform domains can be based on discrete cosine transform (DCT) [5, 6], discrete wavelet transform (DWT) [7], integer wavelet transform (IWT) [8], discrete Fourier transform (DFT) [9].

A characteristic feature of these methods is the preliminary transformation of the container or its blocks into a selected transformation domain, followed by the execution of embedding of additional information. A notable aspect of most of these methods is their ability to provide resilience against attacks targeting the embedded message. However, the use of transformation domains significantly reduces the computational efficiency of these methods, which greatly complicates their implementation on resource-constrained platforms.

The steganographic method with code control of information embedding, which is proposed in [10] is a recent achievement in steganography that has proved its effectiveness. This method is characterized by performing steganographic transformation in the spatial domain of the container, with the capability of selectively influencing the required frequency components of the container blocks. This approach combines the advantages of methods operating in the spatial domain with those methods that operate in the transformation domains: providing resistance to attacks on the embedded message, significant computational efficiency, and ensuring the reliability of perception.

Despite the high prospects and practical application, today the resistance of the steganographic method with code control to steganalysis attacks remains poorly researched, specific methods for detecting covert channels of information transmission, organized using a steganographic method with code control of additional information embedding, are unknown.

As the research performed in this paper shows, the steganographic method with code control of information embedding remains resistant to known steganalysis tools, however, the application of the properties of the Walsh-Hadamard transform opens up prospects for the development of a mathematically simple method for detecting a covert channel based on the steganographic method with code control of information embedding.

The purpose of this paper is to develop a steganalysis method for detecting a covert channel organized using the steganographic method with code control of information embedding in the Walsh-Hadamard transform domain.

This paper is organized as follows: Section 2 provides an overview of the steganographic method with code control. Section 3 explains the proposed steganalysis method. Section 4 presents a comparison of results with other existing methods, while conclusions and suggestions for further research are presented in Section 5.

Steganographic method with code control of information embedding. The foundation of the steganographic method with code control of information embedding lies in the correspondence between the discrete cosine transform (DCT) and the Walsh-Hadamard transform. The core idea of this method is based on utilizing the linearity property of the Walsh-Hadamard transform [11], which enables the embedding of additional information in the spatial domain of the container while targeting a specified frequency component. This method architecture ensures significant computational efficiency, high resistance to attacks against the embedded message, ensuring the reliability of perception, and adequate bandwidth.

Let’s introduce the key definitions necessary for our research. The DCT is defined by the following relation

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

where X is the $N \times N$ block of the original image,

C_N^T is the $N \times N$ DCT matrix, the elements $C(i, j)$ of which are calculated using the following equation

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

Another promising type of discrete transform used in the tasks of steganography and steganalysis is the discrete Walsh-Hadamard transform. In matrix form, the one-dimensional version of the Walsh-Hadamard transform can be written as the following matrix product

$$V = YH_N, \tag{3}$$

where Y is the line-vector of length N,

H_N is a Walsh-Hadamard matrix of order $N = 2^k$, which can be constructed following Sylvester's construction, which is represented by the following equation

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

At that time, the two-dimensional discrete Walsh-Hadamard transform is defined as follows

$$W = H'_N X H'^T_N, \tag{5}$$

where $H'_N = \dfrac{1}{\sqrt{N}} H_N$ is the normalized Walsh-Hadamard matrix,

X is the matrix of the $N \times N$ size.

As the elements of the Walsh-Hadamard matrix are the numbers from $\{-1, 1\}$, the Walsh-Hadamard transform is computationally more efficient than the DFT, DCT, and DST transforms [12].

The Walsh-Hadamard transform returns a sequence of values, which represents a generalized notion of frequency.

In [13], a relationship was established between the two-dimensional and one-dimensional Walsh-Hadamard transform. According to this relationship, the coefficients of the two-dimensional Walsh-Hadamard transform can be determined, up to a scaling factor $\dfrac{1}{N}$, using the one-dimensional Walsh-Hadamard transform.

$$W = XH_{N^2}, \tag{6}$$

where the operation A represents a vector of length N^2 obtained by sequentially concatenating the rows of the matrix A of size $N \times N$.

In the research [10], a relationship was identified between the transform matrix of the Walsh-Hadamard transform, the DCT transform, and the components of the singular value decomposition (SVD) of the original matrix. These results provided the theoretical foundation for developing the method with code control of information embedding.

The essence of code control of information embedding lies in ensuring the desired properties of the steganographic message in the spatial domain with minimal computational costs and disturbances introduced to the container during additive embedding of ± 1.

In this approach, one bit of additional information is embedded into each container block, distributed uniformly among the elements of the block.

Let the block $X = \left\| x_{i,j} \right\|, i, j, = 0,1,...,N-1$ of a digital image be a matrix of size $N \times N$ while d is the additional information bit needs to be embedded into this image block. A codeword T of size $N \times N$ is assigned to this bit, and used to embed the bit d.

Then, the steganographic message block M will have the form

$$\tilde{M} = \tilde{X} + \tilde{T}. \tag{7}$$

Considering the connection between one-dimensional and two-dimensional Walsh-Hadamard transforms the Walsh-Hadamard transformants of the resulting vector M

$$\tilde{W} = \tilde{M} H_{N^2} = (\tilde{X} + \tilde{T}) H_{N^2} = \tilde{X} H_{N^2} + \tilde{T} H_{N^2}. \tag{8}$$

Expression (8) allows for a fundamental conclusion about the nature of perturbations in the Walsh-Hadamard transform coefficients within the steganographic message after the additive embedding of additional information.

The magnitude and localization of such perturbations depend on the specific form of the term $\tilde{T} H_{N^2}$, which represents the Walsh-Hadamard transformants of the row vector $\tilde{T}$ used to encode the additional information bit d.

Therefore, to implement code control of information embedding its bits must first be encoded with codewords of size $N \times N$ that enable selective influence on specific Walsh-Hadamard transform coefficients and, consequently, on the DCT transformants.

Such pre-coding allows for focused influence on a given Walsh-Hadamard transformant of a selected block of size $N \times N$ while limiting the impact on each container element to a unit amplitude.

This ensures the desired properties of the steganographic transformation depending on which transformant the selected codeword is targeted.

As codewords that provide selective influence on specific Walsh-Hadamard transformant, the matrix representation of the rows of the Walsh-Hadamard matrix of order N^2 is used. As mentioned above, based on the connection between the DCT, it is most appropriate to use codewords that affect the low-frequency transformants. For the DCT, these are the transformants (2,1), (2,2), (1,2), and the transformant (1,1).

Therefore, for the Walsh-Hadamard transform [11], these will correspond to the transformants (5,1), (5,5), (1,5), and the transformant (1,1), respectively. Table 1 presents the most commonly used codewords of order 8×8 that influence the low-frequency and mid-frequency components of the container blocks, as well as their corresponding Walsh-Hadamard transform matrices, up to a scaling factor $1/N$.

Thus, it can be seen how steganographic method with code control influences the Walsh-Hadamard transformants while operating in the spatial domain. This leads to the natural conclusion regarding the feasibility of using the Walsh-Hadamard transform domain for the steganalysis of this method, as the changes occurring in this domain are the most specific and noticeable.

Proposed steganalysis method. For the computational experiment, the main dataset of 530 digital images from the NRCS database in lossless TIFF format was used. An additional dataset of 470 images in lossy JPEG format was also included.

For each dataset, steganographic message sets were created using the codewords affecting (5,1), (5,5), and (1,5) transformants. Additional information was embedded in the red channel.

To determine the criteria that could be applied for detecting interference, the values of the Walsh-Hadamard transformants for the steganographic messages and original containers were analyzed, as obtained according to (7).

The performed research led to the conclusion that steganographic transformation does not cause the amplitude values of the Walsh-Hadamard transformants to exceed the limits typical for the original images. However, for blocks of size 8×8 the following pattern was found, which we will write in the form of the following statement.

Table 1.

Mapping of codewords and their Walsh-Hadamard transformant matrices

Codeword	Walsh-Hadamard transformants
$T^{+}_{8(1,1)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$	$W_{(1,1)} = \begin{bmatrix} 64 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$
$T^{+}_{8(5,1)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \end{bmatrix}$	$W_{(5,1)} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 64 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$
$T^{+}_{8(1,5)} = \begin{bmatrix} 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \end{bmatrix}$	$W_{(1,5)} = \begin{bmatrix} 0 & 0 & 0 & 0 & 64 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$
$T^{+}_{8(5,5)} = \begin{bmatrix} 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \end{bmatrix}$	$W_{(5,5)} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 64 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$

*Statement 1***.** In the blocks of a steganographic message of size 8×8, the Walsh-Hadamard transformant, where the additional information was embedded, is more likely to take the maximum value in the block compared to the original images. This dependence can be represented by the following formula

$$U_{orig}(k,l,c) < U_{steg}(k,l,c), \tag{9}$$

where c is the color channel, and U_{orig} and U_{steg} are defined by the following relation

$$\begin{gathered} U_{orig}(k,l,c) = P(W_{orig}(k,l,c)) = \max_{i,j}\{W_{orig}(i,j,c)\}), \\ U_{steg}(k,l,c) = P(W_{steg}(k,l,c) = \max_{i,j}\{W_{steg}(i,j,c)\}), \quad (i,j,c) \neq (1,1,c). \end{gathered}, \tag{10}$$

where W_{orig} and W_{steg} are the matrices of the Walsh-Hadamard transformants for the original and steganographic images, respectively.

$P(W_{orig}(k,l,c)) = \max_{i,j}\{W_{orig}(i,j,c)\})$ is the probability of the event that the Walsh-Hadamard transformant with index (i,j) of the block in the original image acquires the maximum value;

$P(W_{steg}(k,l,c) = \max_{i,j}\{W_{steg}(i,j,c)\})$ is the probability of the event that the transformant of the Walsh-Hadamard transform with the index (i,j) of the steganographic message block acquires the maximum value.

The transformant (1,1) is not taken into account, as it is zero-frequency and always takes a value significantly higher than the other transformants.

At the same time, the frequency of maximum values occurring in all other Walsh-Hadamard transformants of the block, except for the one influenced by the codeword, decreases in the steganographic message.

To research the values of U_{orig} and U_{steg}, experiments were performed, and the results are shown in Fig 1 and Fig.2. Using the results, which demonstrate certain patterns of behavior in images during the embedding of information, it is possible to define specific criteria by which an image can be identified as one in which information has been embedded using a steganographic method with code control. Additionally, it is possible to not only detect the presence of interference but also determine the specific channel of embedding and the codeword used with the help of the detected index that disrupts the patterns of the original containers.

So, first of all, the average threshold values of the frequency of occurrence of maximum were determined for each index of the 8×8 block and each channel. However, these values are averaged, which means that it is important to adjust them experimentally. For this, it was decided to focus on the red color channel, namely on the Walsh-Hadamard transformants with indexes (5,1), (5,5), (1,5), in which it is recommended to embed information.

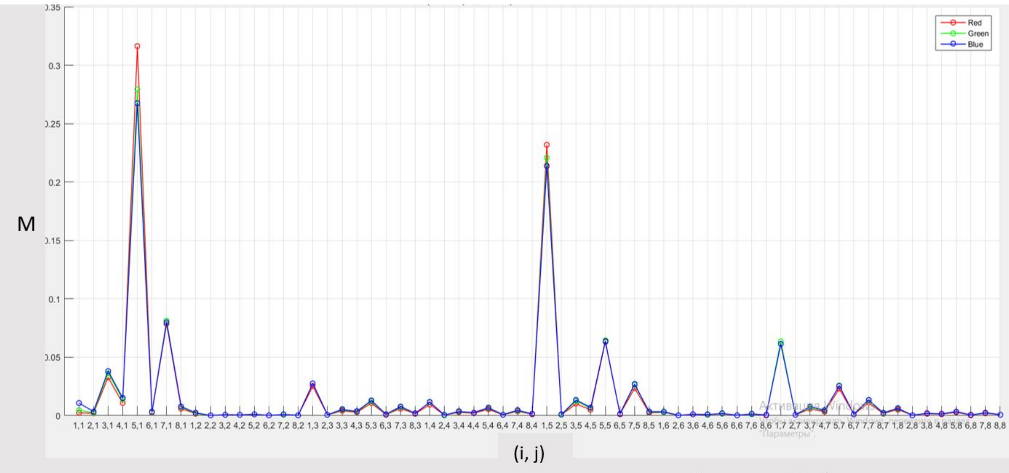

Fig. 1. Graph of the frequency of the location of the maximum value by the index for images without embedded information

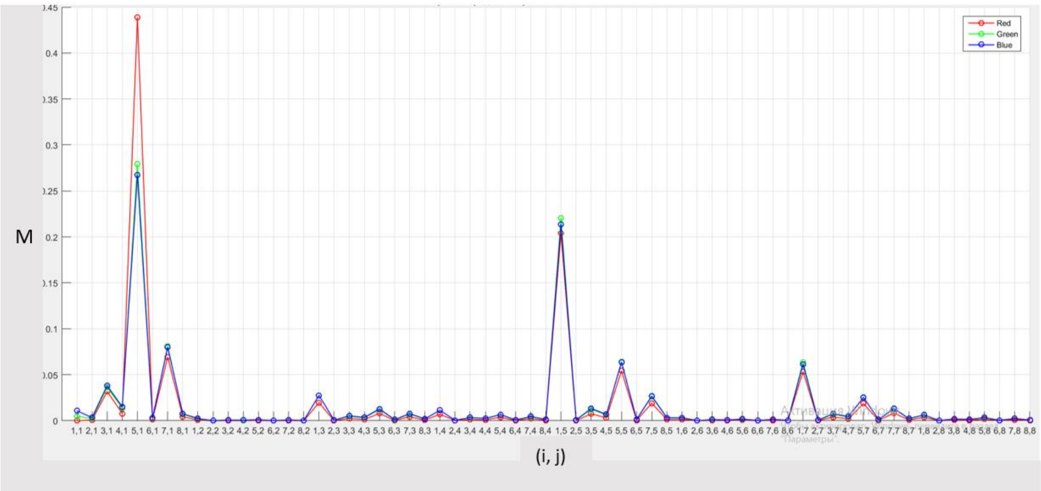

Fig. 2. Graph of the frequency of the location of the maximum value by the index for images with embedded information

To determine the initial matrix of threshold values for each color channel of the set of original images, the matrix of the frequency of occurrence of maximums by index was found. These matrices are formed according to the following formula

$$M(i,j,c) = \frac{1}{N}\sum_{k=1}^{N}\delta\left((i,j,c), \max_{i_{\max},j_{\max},c} W_k(i_{\max},j_{\max},c)\right),$$
$$(i,j) \neq (1,1,c), (i_{\max},j_{\max},c) \neq (1,1,c), \tag{11}$$

where N is the number of blocks in image,

c is the color channel,

k is the number of the block being analyzed,

W_k is the matrix of Walsh-Hadamard transformants of the original image for the k-th block,

δ the Kronecker delta, which is defined as

$$\delta\left((i,j,c), \max_{i_{\max},j_{\max},c} W_k(i_{\max},j_{\max},c)\right) = \begin{cases} 1, (i,j,c) = (i_{\max},j_{\max},c), \\ 0, (i,j,c) \neq (i_{\max},j_{\max},c). \end{cases} \tag{12}$$

We present the experimentally obtained matrix $M(i,j,c)$ for the case of the red channel, where the values corresponding to the low-frequency Walsh-Hadamard transformants often used in practice are highlighted in blue

$$M(i,j,c) = \begin{bmatrix} 0 & 0.008 & 0.03 & 0.009 & 0.25 & 0.004 & 0.07 & 0.006 \\ 0.01 & 0.004 & 0.003 & 0.002 & 0.003 & 0.002 & 0.003 & 0.002 \\ 0.026 & 0.003 & 0.006 & 0.003 & 0.009 & 0.002 & 0.006 & 0.0025 \\ 0.1 & 0.003 & 0.004 & 0.003 & 0.005 & 0.002 & 0.003 & 0.002 \\ 0.3 & 0.004 & 0.009 & 0.005 & 0.06 & 0.002 & 0.0025 & 0.003 \\ 0.0055 & 0.002 & 0.002 & 0.002 & 0.003 & 0.002 & 0.002 & 0.002 \\ 0.2 & 0.003 & 0.005 & 0.003 & 0.03 & 0.002 & 0.0085 & 0.0025 \\ 0.008 & 0.002 & 0.002 & 0.002 & 0.004 & 0.002 & 0.003 & 0.002 \end{bmatrix}. \tag{13}$$

Similarly, matrices $M(i,j,c)$ can be obtained for other color channels, in particular, for channels of the YCbCr color space, if it is used for information embedding.

Based on the obtained results (graphically presented in Fig. 1) and a series of performed experiments, three primary conditions were derived. These conditions allow for the blind detection (i.e., without access to the original image) of images affected by the steganographic method with code control.

The conditions are as follows:

1.Threshold values for indices (5,1), (5,5), and (1,5) are set at 0.3; 0.06, and 0.25, respectively. This condition is used to minimize False Negative results.

2.The analyzed value in the examined color channel must differ from the values in the other channels by at least 0.02 (experiments with higher and lower values yielded less satisfactory results). This condition is also used to minimize False Negative results.

3.At least in 40% of cases, all other values in the color channel, except for the analyzed one, must be lower than the corresponding values in the other channels (experiments with higher and lower percentages yielded less satisfactory results). This condition is used to minimize False Positive results.

Thus, the fulfillment of all three conditions is necessary to identify an image as having been affected by the steganographic method with code control. This allows for the determination of the specific channel where the information was embedded, as well as the transformant that was influenced (which indicates the type of codeword used).

Experimental results. Proposed method. A series of experiments were performed using the selected image datasets. The steganographic message sets in lossless TIFF format using the codewords affecting (5,1), (5,5), and (1,5) were analyzed in the RGB space (embedding in the red channel) and the YCbCr space (embedding in Y). The datasets in lossy JPEG format (at 100% quality) were analyzed in the RGB space (embedding in the red channel). In all cases, embedding occurred in 100% of the blocks. The results of the percentage of errors are presented in Table 2. It should be noted that False Positive cases are those where multiple embedding locations/channels are detected (even if one of them is correct) when it is known that there is only one. False Negative refers to cases where no impact was detected.

Table 2.

The number of errors when using the proposed method of steganalysis

Format	Space	Code	False Positive	False Negative	All errors
.tif	RGB	(5,1)	3,4%	16,3%	19,7%
.tif	RGB	(5,5)	7,7%	13,9%	13,9%
.tif	RGB	(1,5)	5,3%	14,7%	20%
.tif	YCbCr	(5,1)	5,3%	10,2%	15,5%
.tif	YCbCr	(5,5)	7,7%	4,6%	12,3%
.tif	YCbCr	(1,5)	5,5%	11,3%	16,8%
.jpg	RGB	(5,1)	0%	34,9%	34,9%
.jpg	RGB	(5,5)	0%	4,3%	4,3%
.jpg	RGB	(1,5)	0%	23,2%	23,2%

Table 2 shows that the best results are obtained when operating in YCbCr space in a lossless format. The worst results in two of the three cases (namely for codewords (5,1) and (1,5)) produce lossy .jpg images. However, they also give zero false positives — which is also a good result. This may be due to small changes in the average threshold results.

Another observation is that statistically, detection works best when the codeword affecting (5,5) transformant is used for embedding information, meaning that the (2,2) DCT transformant is affected. This is because the threshold value for this index is quite low (0,06), making a significant jump in the color channel more noticeable compared to other channels. As a result, this jump more frequently meets the established three conditions, contributing to better detection in most cases.

The method was also tested for different percentages of utilized blocks (for lossless .tif format, codeword affecting (5,1) transfromant, embedding in the red color channel). Table 3 contains the obtained results.

Table 3.

The number of errors when using the proposed steganalysis method depending on the percent of blocks embedded

Format	Space	% of blocks embedded	Code	False Positive	False Negative	All errors
.tif	RGB	100	(5,1)	3,4%	16,3%	19,7%
.tif	RGB	70	(5,1)	3,8%	20,4%	24,2%
.tif	RGB	50	(5,1)	3,2%	27,6%	30,8%
.tif	RGB	25	(5,1)	4,7%	47,1%	51,8%
.tif	RGB	10	(5,1)	4,5%	60,7%	65,2%

Thus, in this case, it is evident that at 25% of blocks embedded (in large images), the presented method loses effectiveness and detects the covert channel with code control in less than 50%. However, at 100-50% of blocks embedded, it still operates at a fairly significant level of correct detections.

Similar methods. In general, steganalysis methods can be categorized based on various criteria. First, they can be classified according to the information available to the analyst. For example, the steganographic object is known; the steganographic object and the container are known; the hidden message is known; the algorithm is known; both the hidden message and the algorithm are known, as well as the case where all of the aforementioned elements are known.

The proposed method is a blind method since only the steganographic object is known. Currently developing blind steganalysis methods can be categorized into statistical analysis methods [14], adaptive steganalysis methods [15, 16], and methods based on deep learning [17, 18]. These methods of steganalysis are promising, but they suffer from disadvantages such as high computational requirements and the need for large training data sets.

A popular tool that uses the methods of adaptive steganalysis is StegExpose. StegExpose is a steganalysis tool that specializes in detecting steganography in lossless images such as PNG and BMP (LSB detection methods). It has a command-line interface and is designed for batch image analysis, providing reporting capabilities and intuitive settings [19].

This tool provides blind analysis. Testing this tool on the aforementioned datasets of influenced images in lossless TIFF format led to the conclusion that it is unable to detect covert communication channels created using a steganographic method with code control of information embedding. The experiments showed that correct detection occurs only in 0.2% of cases for any codeword, while a false positive result occurs in 99.8% of cases, demonstrating the complete ineffectiveness of the utility.

The paper [20] also discusses several tools for detecting LSB embedding, including LSB-matching, but most of them require the presence of the original image, which diminishes their value for blind detection. In general, methods for detecting LSB embedding [21, 22] most often require the original image, or they analyze the images in grayscale, which makes it impossible to determine the specific embedding channel, as proposed by the method presented in this paper. Table 4 presents the results of the analysis of the aforementioned datasets in lossless TIFF format using the histogram comparison method [21].

Table 4.

The number of errors when using the method of comparative analysis of histograms

Format	Space	Code	True Positive	False Negative
.tif	RGB	(5,1)	32,3,%	67,7%
.tif	RGB	(5,5)	37,2%	62,8%
.tif	RGB	(1,5)	29,6%	70,4%

The analysis of Table 4 leads to the conclusion that the number of errors significantly exceeds the number of errors when using the proposed method.

Conclusions. In this paper, a steganalysis method for detecting a covert channel with code control is presented. This method uses the Walsh-Hadamard transform domain for analysis, which is a promising field for further research and the development of more steganalysis methods. This method is mathematically simple and offers fewer errors than other listed analogs; it also provides the ability to identify the specific transform that has been affected and the channel into which additional information was embedded using the steganographic method with code control.

Such further research directions can be highlighted: experimental determination of more effective threshold values for all other block indices, apart from those considered (5,1), (5,5), and (1,5); exploring the possibility of detecting embedding using the codeword (1,1), as this component is not accounted for the calculations. Further research is also needed to analyze images that have been attacked by compression.

The Walsh-Hadamard transform domain opens up significant potential for such research.

References

1. Chang C. C., Liu Y., Chen K. Real-time adaptive visual secret sharing with reversibility and high capacity. *J. Real-Time Image Process*. 2019. No. 16. P. 871-881. DOI: 10.1007/s11554-018-0813-9.
2. Zyara A. Suggested method for hiding secret data in cover image depending on the Connected Component Labeling algorithm. *International Journal of Electrical and Computer Engineering (IJECE).* 2016. P. 2349-7084.
3. Wang Y., Tang M., Wang Z. High-capacity adaptive steganography based on LSB and Hamming code. *Optik*. 2020. P. 164685. DOI: 10.1016/j.ijleo.2020.164685.
4. Ker A. Improved detection of LSB steganography in grayscale images. Information Hiding Workshop. 2004. V. 3200. P. 97-115.
5. Zhiqiang Z., Ning Z., Tong Q., Ming X. Robust Steganography by Modifying Sign of DCT Coefficients. *IEEE Access.* 2019. P. 1-16. DOI: 10.1109/ACCESS.2019.2953504.
6. Di F., Zhang M., Huang F., Liu J., Kong Y. Reversible data hiding in JPEG images based on zero coefficients and distortion cost function. *Multimedia Tools Applications.* 2019. V. 78. P. 34541–34561. DOI: 10.1007/s11042-019-08109-8.
7. Ping P., Zeming W., Bing Y. C., Bing Z. Double-Matrix Decomposition Image Steganography Scheme Based on Wavelet Transform with Multi-Region Coverage. *Entropy.* 2022. V. 24. P. 256. DOI: 10.3390/e24020246.
8. Valandar M. Y., Ayubi P., Barani M. J. A new transform domain steganography based on modified logistic chaotic map for color images. Journal of Information Security and Applications. 2017. No. 3. P. 142-151. doi: 10.1016/j.jisa.2017.04.004.
9. Hamidi M., Haziti M. E., Cherifi H., Hassouni M. E. Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform. Multimedia Tools Applications. 2018. Vol. 77. P. 1-34. doi: 10.48550/arXiv.1911.00753.
10. Kobozeva A., Sokolov A. Robust Steganographic Method with Code-Controlled Information Embedding. Problems of the Regional Energetics. 2021. P. 115-130. Vol. 4. doi: 10.52254/1857-0070.2021.4-52.11.
11. Kobozeva A., Sokolov A. Theoretical foundations for constructing effective codewords for the code-controlled information embedding steganographic method. *Radiotekhnika.* 2021. No. 4. P. 27-39. DOI: 10.30837/rt.2021.4.207.02.
12. Bhattacharyya S. A Robust Image Steganography using Hadamard Transform. *International Conference on Information Technology in Signal and Image Processing*. 2013. P. 132-142.
13. Steganalysis: How to Detect Steganography, [Electronic resource]. 2018. URL: https://digitnet.github.io/m4jpeg/about-steganography/how-to-detect-steganography.htm.

14. Cai K., Li X., Zeng T., Yang B., Lu X. Reliable histogram features for detecting LSB matching. *IEEE International Conference on Image Processing, Hong Kong, China*. 2010. P. 1761 – 1764. DOI: 10.1109/ICIP.2010.5651567.
15. Jackson J. T., Gunsch G. H., Claypoole R. L., Lamont G. B. Blind Steganography Detection Using a Computational Immune System: A Work in Progress. *International Journal of Digital Evidence*. 2003. V. 4. P. 1-19.
16. StegAlyzerAS. 2018. URL: https://www.sciencedirect.com/topics/computer-science/steganography-tool.
17. Lin J., Yang Y. Multi-Frequency Residual Convolutional Neural Network for Steganalysis of Color Images. *IEEE Access*. 2021. No. 9. P. 1-13. DOI: 10.1109/ACCESS.2021.3119664.
18. Agarwal S., Kim C., Jung K.-H. Steganalysis of Context-Aware Image Steganography Techniques Using Convolutional Neural Network. *Appl. Sci.* 2022. No. 12. P. 10793. DOI: 10.3390/app122110793.
19. StegExpose. 2015. URL: https://github.com/b3dk7/StegExpose.
20. Pelosi M., Easttom C. Identification of LSB image Steganography using Cover Image Comparisons. *Journal of Digital Forensics Security and Law*. 2021. No. 15. P. 6. DOI: 10.15394/jdfsl.2021.1551.
21. Jung K. H. Comparative Histogram Analysis of LSB-based Image Steganography. *WSEAS Transactions on Systems and Control*. 2018. No. 13. P.1991-8763.

СТЕГАНОАНАЛІЗ МЕТОДУ ІЗ КОДОВИМ УПРАВЛІННЯМ ВБУДОВУВАННЯ ІНФОРМАЦІЇ В ОБЛАСТІ ПЕРЕВТОРЕННЯ УОЛША-АДАМАРА

О. О. Лановська, А. В. Соколов

Національний університет «Одеська політехніка»
1, Шевченка пр., м.Одеса, 65044, Україна
Email: radiosquid@gmail.com

Стеганографія є невід’ємною частиною побудови сучасних систем захисту інформації. Стеганографічний метод з кодовим управлінням вбудовуванням інформації є сучасним стеганографічним методом, що оперує в просторовій області контейнеру. Перевагами цього методу є забезпечення надійності сприйняття, стійкості до атак проти вбудованого повідомлення, достатньої пропускної спроможності, високої обчислювальної ефективності. На противагу стеганографічним методам створюються методи стеганоаналізу, що дозволяють виявляти вбудовану інформацію. На сьогоднішній день дослідження щодо стійкості стеганографічного методу з кодовим управлінням до атак криптоаналізу не проводилися, специфічні методи виявлення втручання за допомогою стеганографічного методу з кодовим управлінням невідомі. Метою цієї роботи є розробка методу стеганоаналізу для виявлення прихованого каналу, організованого за допомогою стеганографічного методу з кодовим управлінням вбудовування інформації в області перетворення Уолша-Адамара. У роботі проведені дослідження поведінки трансформант перетворення Уолша-Адамара контейнерів та стеганоповідомлень, які дозволили сформулювати умови наявності додаткової інформації в зображенні. Зазначені умови стали основою для розробки легкого та математично простого методу стеганоаналізу, який використовує область перетворення Уолша-Адамара. Проведені дослідження запропонованого методу дозволили встановити його високу ефективність в різних умовах при низькій обчислювальній складності. Зокрема показано, що ефективність запропонованого методу перевищує ефективність методу аналізу гістограм, та методів, реалізованих у відомому інструменті StegExpose. Отримані результати дозволяють рекомендувати запропонований метод стеганоаналізу для практичного застосування для виявлення прихованих каналів зв’язку, що створенні із застосуванням стеганографічного методу з кодовим управлінням. Зокрема, зважаючи на простоту своєї алгоритмічної реалізації, запропонований метод буде ефективним в умовах обмежених обчислювальних ресурсів.

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