DOI 10.15276/imms.v15.no1.5
UDC 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 1, pp. 5-14

DETECTION OF COVERT CHANNELS IN WEB APPLICATIONS BASED ON UNIMODALITY VIOLATION IN THE WALSH–HADAMARD SPECTRUM

A.I. Dyka

National University "Odesa Law Academy"
23, Fontanska road, Odesa, 65009, Ukraine

This paper presents the theoretical foundations of an innovative method for steganalysis of digital images based on detecting violations of unimodality in the Walsh–Hadamard transform spectrum. The method targets the detection of covert information transmission channels in web applications, particularly in scenarios where users are allowed to upload graphic content. The relevance of this research stems from the increasing use of modern steganographic techniques that are resistant to classical steganalysis methods, thereby posing potential threats of data leakage or the transmission of hidden commands within seemingly legitimate content. The paper formalizes the concept of code-controlled embedding in the spatial domain by selectively affecting individual Walsh–Hadamard transformants. It is shown that such embedding leads to statistically significant deviations from unimodality in the distribution of the corresponding spectral components, which can serve as indicators of hidden activity. Two theoretical propositions are proven: the first describes the expected statistical behavior of Walsh–Hadamard transformants in natural images, while the second demonstrates the emergence of bimodal histograms under steganographic embedding. The theoretical framework is supported by computational experiments across large datasets of real-world images. The findings form a basis for the development of effective detection systems for covert channels in web applications. The proposed approach can be used to generate meaningful features for training artificial intelligence models integrated into automated security testing pipelines, as well as for monitoring uploaded content for the presence of hidden information. The method is format-agnostic and retains effectiveness even under common attack conditions, such as lossy JPEG compression.

Keywords: steganography; Walsh–Hadamard transform; code control; web application security; covert communication channels; unimodality of distribution; digital images; machine learning; steganalysis; information security

1. Introduction and statement of the problem. In the modern software development lifecycle, security testing is critical to identifying vulnerabilities that may lead to unauthorized access, data leakage, or system disruption. From a cybersecurity perspective, testing the security of software components, particularly those exposed to user interaction, is essential for identifying and mitigating threats and covert communication channels [1-3].

For web applications, one of the underexplored but increasingly relevant threats is the use of steganographic methods to covertly transmit information via seemingly legitimate user-uploaded content [4]. While legacy steganographic algorithms were often detectable using classical steganalysis techniques [5], modern methods exhibit high resistance to traditional detection, making them a greater threat in practice.

A notable example is a recently proposed method based on code-controlled embedding, which allows selective modification of spatial regions of an image while maintaining the ability to influence specific frequency components. This makes the approach robust to steganalytic attacks and suitable for use in constrained environments such as mobile devices, IoT systems, and UAVs, where computational resources are limited but reliability and stealth remain important. Research has shown that this method achieves superior resistance to detection compared to popular transform-domain methods, including those based on singular value decomposition (SVD) [6…7].

Prior research [8] demonstrated that the code-controlled embedding method exhibits high robustness against known steganalysis tools such as StegExpose, which failed to reliably detect covert messages even under ideal analysis conditions. Although some statistical signs of embedding were identified, resulting in a preliminary steganalytic approach, its detection accuracy was limited (~80%) and significantly decreased when the embedding density was low or when lossy compression formats were applied.

The very concept of code-controlled embedding presents a major risk for web infrastructure, as it enables the construction of covert communication channels that are resistant to both perceptual and analytical detection. Addressing this threat requires the development of new theoretical and algorithmic foundations for steganalysis, capable of detecting such subtle manipulations.

In this context, the Walsh-Hadamard Transform offers a promising mathematical basis due to its high computational efficiency and clear interpretability of its spectral components. Theoretical analysis and empirical research presented in this paper demonstrate that Walsh-Hadamard Transform domain features can reveal structural changes in image data resulting from code-controlled embedding, particularly through violations of the unimodal distribution of specific transformants. This paper lays a theoretical foundation for future AI-based detection models capable of identifying covert channels in web applications.

The purpose of this paper is to improve the efficiency of detecting covert communication channels based on the code-controlled steganographic method in web applications.

The paper is structured as follows: Section 2 formalizes the concept of code-controlled embedding and presents the core mathematical relationships. Section 3 provides an in-depth analysis of the statistical behavior of Walsh-Hadamard Transform coefficients under steganographic influence and demonstrates the presence of a bimodal distribution that can serve as a detection criterion.

2. General definitions and mathematical foundations of code-controlled steganographic method. One of the important tools for processing digital images in the context of steganography and steganalysis is the two-dimensional Walsh-Hadamard Transform [9]. This orthogonal transform is based on functions that take only the values +1 and −1, and allows you to effectively represent the signal as a sequence of transformants that characterize its frequency components.

Let a digital image block X of size $N \times N$ to be defined. Then the Walsh-Hadamard transform of this block is defined as

$$W_X = H'_N X H'^T_N, \tag{1}$$

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

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

In addition to the two-dimensional Walsh-Hadamard transform, its one-dimensional version is also known, which for a vector Y is given as

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

at the same time, in [10], a relationship was established between the two-dimensional and one-dimensional versions of the Walsh-Hadamard transform, within the framework of which it was proved that

$$\tilde{W} = \tilde{X} H_{N^2}, \tag{4}$$

where the notation $\tilde{W}$ and $\tilde{X}$ means the representation of the corresponding matrices of size $N \times N$ in the form of a vector of length N^2 by sequential concatenation of the rows of the corresponding matrix, while the calculation of the Walsh-Hadamard transformants is performed with an accuracy of up to the normalization coefficient $1/N$.

Expression (4) became the basis of the concept of code-controlled embedding of additional information, which consists in the fact that the embedding occurs by representing each information bit d_i in the form of a codeword T, which selectively affects one or another transformant of the Walsh-Hadamard transform, which is additively embedded in the corresponding container block

$$\tilde{M} = \tilde{X} + \tilde{T}, \tag{5}$$

then

$$\tilde{W} = \tilde{M} H_{N^2} = (\tilde{X} + \tilde{T}) H_{N^2} = \tilde{X} H_{N^2} + \tilde{T} H_{N^2}. \tag{6}$$

As evident from equation (6), the influence on the Walsh–Hadamard transformants of the container block is entirely determined by the structure of the transformants of the selected codeword. Since the codeword selectively affects a specific Walsh–Hadamard transformant, this enables precise embedding of additional information into that particular transformant.

Let us consider a specific example for the block size 8×8. Let us give a container block for which we find the matrix of the Walsh-Hadamard transformants

$$X = \begin{bmatrix} 93 & 102 & 102 & 106 & 110 & 115 & 116 & 118 \\ 99 & 109 & 102 & 112 & 117 & 114 & 116 & 115 \\ 103 & 114 & 106 & 111 & 121 & 116 & 123 & 111 \\ 113 & 116 & 113 & 115 & 115 & 114 & 121 & 116 \\ 113 & 113 & 115 & 113 & 113 & 109 & 109 & 115 \\ 128 & 111 & 114 & 117 & 114 & 114 & 117 & 116 \\ 126 & 111 & 112 & 116 & 109 & 111 & 128 & 130 \\ 118 & 117 & 110 & 114 & 111 & 107 & 111 & 120 \end{bmatrix};$$

$$W_X = \begin{bmatrix} 7256 & -20 & -64 & 40 & -128 & -40 & 80 & 20 \\ -36 & -4 & -40 & -28 & -68 & 0 & 0 & -8 \\ -102 & -22 & 6 & 2 & -30 & 14 & -74 & -10 \\ -70 & -34 & -6 & -14 & 34 & 18 & -22 & -58 \\ -108 & -48 & 0 & -88 & -156 & -108 & -88 & -20 \\ -44 & -4 & 28 & -8 & -20 & -8 & -20 & 4 \\ -62 & -54 & -54 & 22 & -70 & 14 & 42 & -6 \\ 62 & 26 & -46 & 10 & -10 & 62 & 50 & 62 \end{bmatrix}, \tag{7}$$

as well as the codeword used to target the Walsh–Hadamard transformant (5,1), which belongs to the lower-frequency components and, according to [11], provides the highest robustness against attacks on the embedded message when used for additional data embedding.

$$T=\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \end{bmatrix}. \quad (9)$$

Then, according to equation (6), the resulting steganographic message and its Walsh–Hadamard transform coefficients will take the following form

$$M=\begin{bmatrix} 94 & 103 & 103 & 107 & 111 & 116 & 117 & 119 \\ 100 & 110 & 103 & 113 & 118 & 115 & 117 & 116 \\ 104 & 115 & 107 & 112 & 122 & 117 & 124 & 112 \\ 114 & 117 & 114 & 116 & 116 & 115 & 122 & 117 \\ 112 & 112 & 114 & 112 & 112 & 108 & 108 & 114 \\ 127 & 110 & 113 & 116 & 113 & 113 & 116 & 115 \\ 125 & 110 & 111 & 115 & 108 & 110 & 127 & 129 \\ 117 & 116 & 109 & 113 & 110 & 106 & 110 & 119 \end{bmatrix};$$

$$W_M=\begin{bmatrix} 7256 & -20 & -64 & 40 & -128 & -40 & 80 & 20 \\ -36 & -4 & -40 & -28 & -68 & 0 & 0 & -8 \\ -102 & -22 & 6 & 2 & -30 & 14 & -74 & -10 \\ -70 & -34 & -6 & -14 & 34 & 18 & -22 & -58 \\ -44 & -48 & 0 & -88 & -156 & -108 & -88 & -20 \\ -44 & -4 & 28 & -8 & -20 & -8 & -20 & 4 \\ -62 & -54 & -54 & 22 & -70 & 14 & 42 & -6 \\ 62 & 26 & -46 & 10 & -10 & 62 & 50 & 62 \end{bmatrix}. \quad (10)$$

By comparing expressions (10) and (7), we conclude that the embedding of additional information was performed specifically in the (5,1) Walsh–Hadamard transformant, as it is the only one among all transformants that underwent modification.

3. Analysis of the properties of Walsh-Hadamard transformants of digital images under code-controlled embedding. Detecting steganographic messages requires a more detailed analysis of the patterns to which the container is subjected during the steganographic embedding process. Identifying such patterns, in turn, requires an understanding of the probabilistic and structural characteristics of the Walsh-Hadamard transform coefficients of real images.

Proposition 1. Let there be given a set of matrices W_{X_j} of size $N\times N$ representing the Walsh-Hadamard transformants of image blocks X_j, $j=1,2,...,n$, and each having the form

$$W_{X_j}=\begin{bmatrix} w_{X_j,11} & w_{X_j,12} & \cdots & w_{X_j,1N} \\ w_{X_j,21} & w_{X_j,22} & \cdots & w_{X_j,2N} \\ \vdots & \vdots & \ddots & \vdots \\ w_{X_j,N1} & w_{X_j,N2} & \cdots & w_{X_j,NN} \end{bmatrix}, \quad (11)$$

then the sequence of transformants $u_{kl}=\begin{bmatrix} w_{X_1,kl} & w_{X_2,kl} & \dots & w_{X_n,kl} \end{bmatrix}$ has zero mathematical expectation $\mathrm{E}[u_{kl}]=0$ for all k,l except $k=l=1$.

Proof. To prove Proposition 1, we note that according to (4) each matrix W_{X_j} can be represented as a vector of transformants $W_{X_j}=X_jH_{N^2}=[w_{X_1,11} \quad w_{X_1,12} \quad \dots \quad w_{NN}]$, of the Walsh-Hadamard transform, thus each coefficient $w_{X_1,kl}$ obtained by multiplying the

corresponding vector X formed by successive concatenation of the rows of the block matrix X by the corresponding row of the Walsh-Hadamard matrix H_{N^2}, which by construction is a Walsh function h_g of length N^2. Then we can write the corresponding coefficient $w_{X_j,kl}$ as

$$w_{X_j,kl} = \sum_{\alpha=1}^{N^2} h_{g,\alpha} x_\alpha \ . \tag{12}$$

In other words, since the intensity values x_α of the pixels of an arbitrary image do not depend on the elements of the Walsh functions $h_{g,\alpha}$, the mathematical expectation $\mathrm{E}[w_{X_j,kl}]$ for each $w_{X_j,kl}$ will be defined as

$$\mathrm{E}[w_{X_j,kl}] = \mathrm{E}[h_{g,\alpha} x_\alpha] = \mathrm{E}[h_{g,\alpha}]\mathrm{E}[x_\alpha] \ . \tag{13}$$

Since by their construction the Walsh functions are balanced for any $g \neq 1$, then $\sum_{\alpha=1}^{N^2} h_{g,\alpha} = 0$, and therefore the product $\mathrm{E}[w_{X_j,kl}] = 0$.

Given that $\mathrm{E}[w_{X_j,kl}] = 0$ for $\forall k,l$ except $k = l = 1$, i.e. when $g \neq 1$, we obtain $\mathrm{E}[u_{kl}] = 0$ for any k,l except $k = l = 1$, which proves the conditions of Proposition 1.

Computational experiment 1.

To practically verify the conditions of Proposition 1, we will perform the following computational experiment. For a sample of 500 images from the NRCS database [12], we will form a vector for blocks of size 4×4, 8×8, 16×16, after which we will find the average value of the vector u_{kl} elements for all values k,l according to the block size.

The results of the computational experiment for blocks of sizes 4×4 and 8×8 are shown in Table 1.

Empirically constructed average values of the transformants of the Walsh-Hadamard transform

Table 1.

Block size 4×4				
k/l	1	2	3	4
1	$1.8\cdot10^3$	0	0	0
2	0.1	0	0	0
3	0.4	0	0	0
4	0	0	0	0

Block size 8×8								
k/l	1	2	3	4	5	6	7	8
1	$7.3\cdot10^3$	0	0	0.2	-0.2	0	0	0
2	0.7	0	0	0.1	0	0	0	0
3	1.7	0	0	0	0	0	0	0
4	0.3	0	0	0.2	0	0	0	0
5	3.0	0.2	0	-0.1	0	-0.1	0	-0.1
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

Note that for blocks of size 16×16 the average value of the element $(1,1)$ is equal to $2.9\cdot10^4$, while other values in the computational experiment are practically equal to 0.

Analysis of the data in Table 1 leads to practical confirmation of Proposition 1, because the average values of the transformants of the Walsh-Hadamard transform when averaging over blocks are indeed close to 0 in practice, except for the case of values $k=l=1$.

Note that the standard deviation and dispersion of vector u_{kl} values in practice depend very much on the specific image and its structure, which, in our opinion, sets a number of restrictions on their generalization and limits their application in practice for detecting steganographic messages.

For greater clarity, let us form histograms of the distribution of vector u_{15} and u_{51} element values for the size of the blocks 8×8 (Fig. 1).

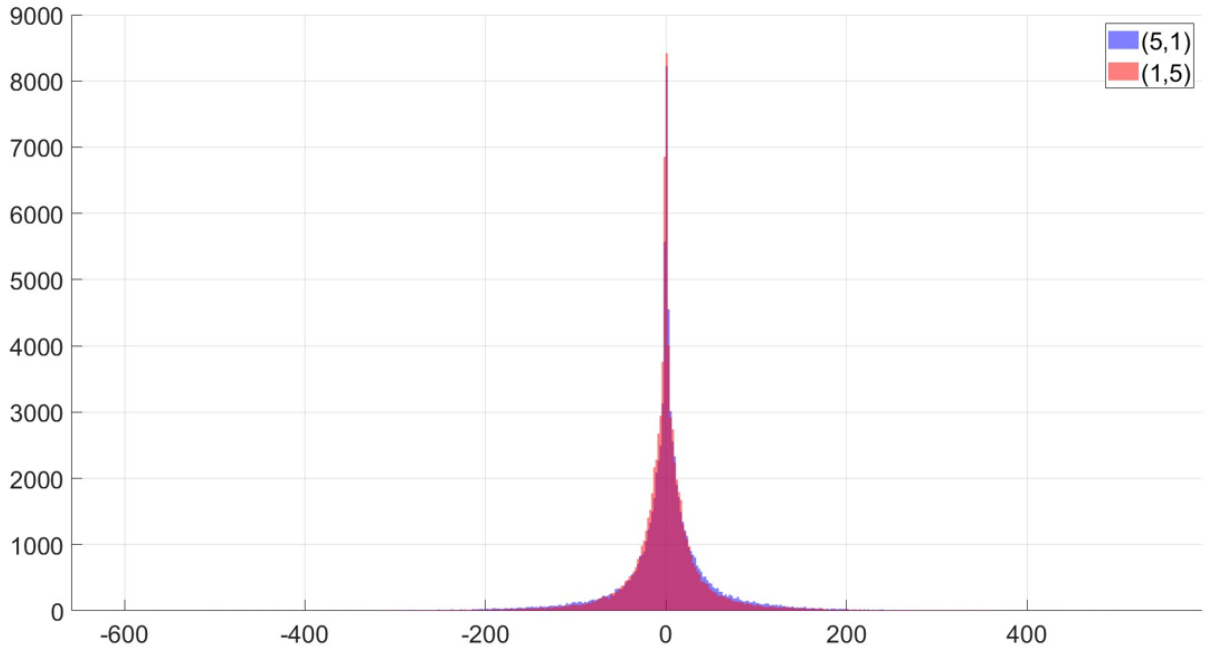


Fig. 1. — Histogram of the distribution of element values for vectors u_{15} and u_{51}

Let us research the effect of steganographic transformation using the code-controlled method with embedding additional information on the statistical characteristics of vectors u_{kl}.

According to conditions (6) of using the code-controlled steganographic method with codewords that selectively affect a given transformant, the Walsh-Hadamard transform leads to a change in its value in each block by the value of N^2.

Proposition 2. The histogram of the distribution of vectors u_{kl}, in which additional information was embedded using the code-controlled steganographic method with codewords based on Walsh functions, will have a bimodal character with maxima at points $\pm N^2$.

Proof. To prove Proposition 2, we note that one of the important components of the steganographic system is the precoder, the function of which is to form a sequence $\{d_j\}$ using analog-to-digital conversion operations (if necessary), effective coding, noise-resistant coding of information, and encryption. The use of high-quality encryption algorithms leads to a uniform distribution of symbols "0" and "1" in the sequence $\{d_j\}$. Therefore, in the context of using the steganographic method with code control, we will assume that the distribution of symbols in the sequence $\{d_j\}$ is uniform.

Taking into account the above, from a statistical point of view, steganographic message vectors u'_{kl} can be represented as

$$u'_{kl} = \begin{cases} u'_{kl} + N^2, \text{ with probability } 0.5; \\ u'_{kl} - N^2, \text{ with probability } 0.5. \end{cases} \quad (14)$$

Since, according to the conditions of Proposition 1, the probability density $f_{u_{kl}}$ has a maximum (since the random variable u_{kl} is distributed according to a symmetric unimodal distribution, which is confirmed by the obtained empirical data for a given sample of images, the maximum of the probability density $f_{u_{kl}}$ will coincide with its mathematical expectation) at point 0.

Then the probability density $f_{u_{kl}}(u_{kl} - N^2)$ has a maximum at $u_{kl} - N^2 = 0,$, i.e. at $u_{kl} = N^2$. Similarly, $f_{u_{kl}}(u_{kl} + N^2)$ will have a maximum at $u_{kl} + N^2 = 0$, i.e. at $u_{kl} = N^2$. Therefore, $f_{u'_{kl}}$ will have two maxima: at points $-N$ and N, since both terms contribute their maxima independently.

The above proves the conditions of Proposition 2.

Fig. 2 shows the u_{51} distribution histograms for the original image, as well as the steganographic message for the transformant of the Walsh-Hadamard transform (5,1), into which additional information was embedded using the corresponding codeword (9) of size 8×8.

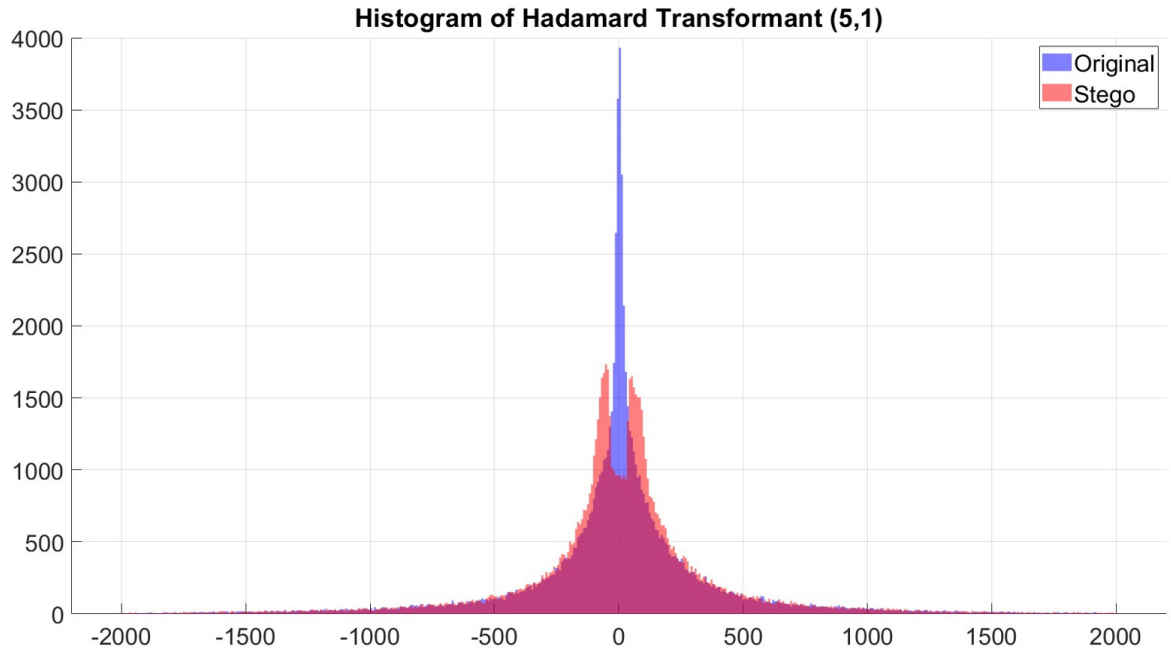


Fig. 2. — Histogram of distribution of u_{51} for the original image and u'_{51} for the steganographic message

The analysis of the data in Fig. 2 confirms the conditions of Proposition 2: for a steganographic message, unlike the original image, the distribution of the transformant of the Walsh-Hadamard transform, which has undergone the embedding of additional information, is bimodal with maxima in the values $\pm N = \pm 64$, which confirms that the size of the block in which the embedding occurred is indeed $N = 8$.

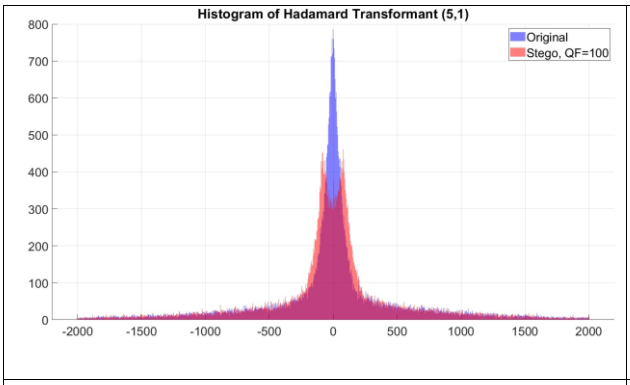
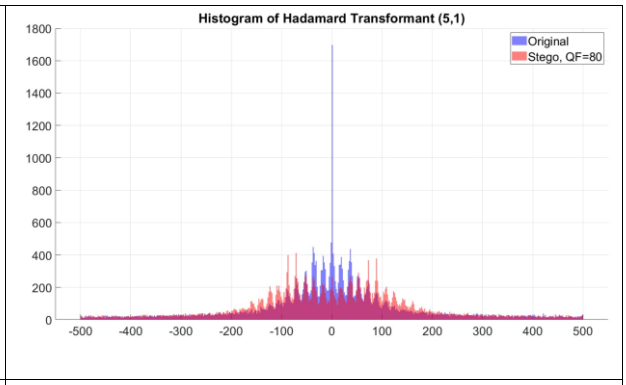
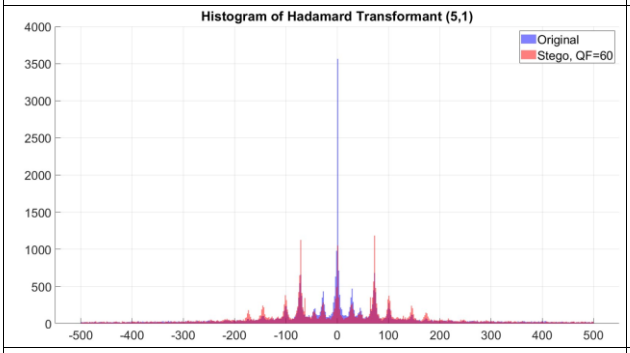
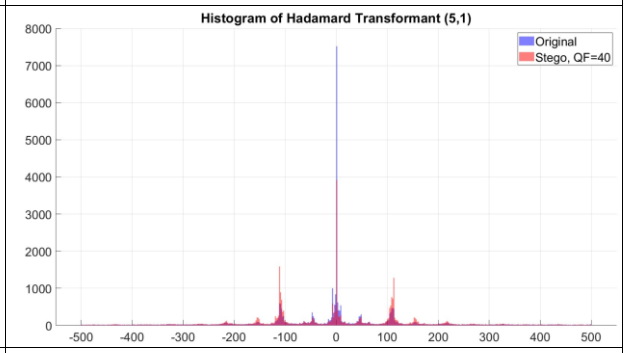
Obviously, taking into account the conditions of Proposition 2, this type of deviation of the histogram of the distribution of vectors u_{kl} from the classical unimodal probability distribution is a sign of the use of a steganographic method with code control for embedding additional information into a given transformant of the Walsh-Hadamard transform.

An important factor influencing the practical applicability of Proposition 2 for detecting the embedding of additional information embedded using the code-controlled steganographic method is its robustness under disruptive conditions, in particular, compression attacks, which are among the most common forms of attacks targeting embedded messages. Experimental data [6] confirm the resilience of this method to such attacks.

Table 2 shows the histograms of steganographic message vectors u'_{51} that were subjected to compression attacks against the embedded message with different values of the quality factor $QF = \{100, 80, 60, 40, 20\}$.

Histograms of steganographic message vectors u'_{51} for different QF compression levels

Table 2.

	
QF=100	*QF*=80
	
QF=60	*QF*=40

Analysis of the data presented in Table 2 leads to the conclusion that, although image compression leads to multimodality of the distribution of the Walsh-Hadamard transformants, we see that for the steganographic message it remains noticeable due to a significantly higher concentration of the Walsh-Hadamard transform values in the side lobes of the histogram, while for the original images this concentration remains significant near the zero value. This makes it possible to detect the embedding of additional information using the steganographic method with code control using the conditions of Proposition 2, even after a compression attack against the embedded message.

Conclusions. The paper proposes the theoretical foundations of the steganalysis method, which is based on the detection of a violation of the unimodality of the distribution of the Walsh-Hadamard transformants in images to which code-controlled steganographic embedding has been applied. It is shown that such a feature allows us to formalize the criterion for the presence of embedded information, which can be used for the automated detection of covert channels in web applications.

The obtained analytical statements are confirmed by computational experiments that demonstrate the high sensitivity of transformants histograms to the fact of embedding. In particular, it was established that selective embedding leads to the formation of bimodal distributions, which is a reliable sign of hidden influence.

The proposed approach has practical significance for web application protection systems that allow users to upload images. The theoretical framework developed in this paper can be used as a basis for training artificial intelligence models capable of detecting atypical patterns in image transformants that signal the presence of hidden messages.

Integrating such analysis into content monitoring will increase the level of information security of web-based systems, complementing classic vulnerability detection methods with mechanisms for controlling covert data transmission channels.

References

1. Trofymenko O., Dyka A., Loboda Y. Analysis of vulnerabilities and security problems of web applications. System technologies. 2023. Vol. 3, No. 146. P. 25-37.
2. Kranthi A. G. et al. Securing web apps: Analysis to understand common vulnerabilities, attack scenarios, and protective measures. ICCDE 2024. P. 64.
3. Mohammed A. et al. Security of web applications: Threats, vulnerabilities, and protection methods. International Journal of Computer Science & Network Security. 2021. Vol. 21, No. 8. P. 167-176.
4. Othman N. A. et al. Image Steganography Using Web Application. Journal of Computing Research and Innovation. 2023. Vol. 8, No. 2. P. 1-11.
5. 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.
6. Kobozeva A.A., Sokolov A.V. Robust Steganographic Method with Code-Controlled Information Embedding. Problemele energeticii regionale. 2021. No. 4 (52). P. 115-130.
7. Kobozeva A.A., Sokolov A.V. Steganographic Method with Code Control of Information Embedding Based on Multi-level Code Words. Radioelectronics and Communications Systems. Vol. 66, No. 4. P. 173-189.
8. Lanovska O.O., Sokolov A.V. Steganalysis of a method with code-controlled information embedding in the Walsh-Hadamard transform domain. Informatics and mathematical methods in simulation. 2024. V.1. No 4. P.1-12
9. Beer T. Walsh transforms. American Journal of Physics. 1981. Vol. 49, No. 5. P.466-472.
10. Kobozeva A.A., Sokolov A.V. The Sufficient Condition for Ensuring the Reliability of Perception of the Steganographic Message in the Walsh-Hadamard Transform Domain. 2022. Problemele Energeticii Regionale 54 (2). P. 84-100.
11. Karampidis K., Kavallieratou E., Papadourakis G. A review of image steganalysis techniques for digital forensics. *Journal of Information Security and Applications.* 2018. 40. P. 217-235.
12. Natural Resources Conservation Service (NRCS) // United States Department of Agriculture. URL: https://www.nrcs.usda.gov

A.I. Dyka

ВИЯВЛЕННЯ ПРИХОВАНИХ КАНАЛІВ У ВЕБ-ЗАСТОСУНКАХ НА ОСНОВІ АНАЛІЗУ ПОРУШЕНЬ ОДНОМОДАЛЬНОСТІ СПЕКТРА УОЛША-АДАМАРА

А.І. Дика

Національний університет «Одеська юридична академія»
23, Фонтанська дорога, м.Одеса, 65009, Україна

У цій статті представлено теоретичні основи нового методу стеганоаналізу цифрових зображень, заснованого на виявленні порушень унімодальності в спектрі перетворення Уолша-Адамара. Метод спрямований на виявлення прихованих каналів передачі інформації у веб-застосунках, зокрема в сценаріях, де користувачам дозволено завантажувати графічний контент. Актуальність цього дослідження пов'язана зі зростаючим використанням сучасних стеганографічних методів, стійких до класичних методів стеганоаналізу, що створює потенційні загрози витоку даних або передачі прихованих команд у межах, здавалося б, легітимного контенту. У статті формалізовано концепцію кодового управління вбудовуванням в просторовій області шляхом вибіркового впливу на окремі трансформанти перетворення Уолша-Адамара. Показано, що таке вбудовування призводить до статистично значущих відхилень від унімодальності в розподілі відповідних спектральних компонентів, які можуть служити індикаторами прихованої активності. Доведено два теоретичні твердження: перше описує очікувану статистичну поведінку коефіцієнтів перетворення Уолша-Адамара в природних зображеннях, а друге демонструє появу бімодальних гістограм при стеганографічному вбудовуванні. Теоретичну основу підтверджують обчислювальні експерименти на великих наборах даних реальних зображень. Отримані результати формують основу для розробки ефективних систем виявлення прихованих каналів у веб-застосунках. Запропонований підхід може бути використаний для створення значущих ознак для навчання моделей штучного інтелекту, інтегрованих в автоматизовані конвеєри тестування безпеки, а також для моніторингу завантаженого контенту на наявність прихованої інформації. Метод не залежить від формату та зберігає ефективність навіть за поширених умов атаки, таких як стиснення JPEG з втратами.

Ключові слова: стеганографія; перетворення Уолша-Адамара; кодове управління; безпека веб-застосунків; приховані канали зв'язку; унімодальність розподілу; цифрові зображення; машинне навчання; стеганоаналіз; інформаційна безпека.