UDC 004.056.55
DOI https://doi.org/10.32782/2663-5941/2025.4.2/15

Dyka A.I.
National University "Odesa Law Academy"

DETECTION OF SVD-BASED HIDDEN DATA IN WEB APPLICATIONS USING WALSH-HADAMARD TRANSFORMANT ANALYSIS

Modern web applications process huge amounts of multimedia data, which creates a risk of using them as transport channels for covert information transmission using steganography. This requires steganalysis methods that can operate in real-time without excessive load on servers. In this paper, a method for detecting covert messages embedded in the singular decomposition domain is developed by analyzing coefficients in the Walsh-Hadamard transform domain. The proposed approach combines the advantages of high sensitivity to steganographic interference with the computational simplicity of the Walsh-Hadamard transform, which allows for significant reduction of resource consumption when processing large data sets. It is proven that the modification of the left and right singular vectors corresponding to the first singular value in the singular decomposition domain leads to specific changes in the selected transformants of the Walsh-Hadamard transform. For non-blind analysis scenarios, high-frequency angular transformants (8,8), (1,8), (8,1), and (1,1) were identified, which demonstrate the largest amplitudes of changes. For blind analysis, three low-frequency transformants (1,5), (5,1), and (5,5) were identified, which undergo the largest statistical shift and can serve as reliable markers of hidden information. Using only these positions allows reducing the computational complexity by a factor of 16–21 while maintaining high detection accuracy, which is especially important for web services with high query intensity. The results obtained are based on processing a set of 530 images in a lossless format, which made it possible to identify key patterns in the influence of modifications in the singular decomposition domain on the Walsh-Hadamard transform coefficients. The theoretical foundations proposed in the paper create a basis for the development of highly efficient steganalysis algorithms capable of operating in real-time with minimal computational costs. By using a limited set of informative transformants of the Walsh-Hadamard transform, these algorithms can potentially be integrated into server-side security systems of web platforms for streaming analysis of a large number of files. The theoretical provisions can also be adapted to detect covert data in video and audio streams, and in combination with machine learning methods, become the basis of hybrid solutions with increased robustness and accuracy of detection of modern steganographic algorithms.

Key words: *steganalysis, Walsh-Hadamard transform, singular value decomposition, covert communication channels, cybersecurity, web applications, frequency analysis.*

Formulation of the problem. Modern web applications have evolved into multifunctional platforms that facilitate the exchange and storage of multimedia data. This creates conditions conducive to the emergence of covert information channels, particularly through the use of steganographic techniques. The uncontrolled uploading of images, audio, and video files by users enables attackers to conceal data within these files, effectively turning the web application into a transport node for leaking confidential information or coordinating attacks [1]. Traditional security systems typically focus on monitoring network traffic and user behavior, but they struggle to effectively detect steganographic embeddings, especially when sophisticated algorithms are employed in combination with the low bandwidth characteristic of covert communication channels, considering the high resolution of modern photo, video, and audio containers. Consequently, the development and enhancement of steganalysis methods capable of operating under high data throughput conditions in web applications and detecting concealed messages – even those embedded using advanced mathematical transformations – remains a critical challenge in cybersecurity.

An analysis of the latest research and publications. Modern steganalysis approaches increasingly rely on the analysis of signals in transform domains, particularly within the singular value decomposition (SVD) domain. Such methods have demonstrated high effectiveness in detecting covert messages in images, yet remain computationally intensive, limiting their integration into web environments. For

instance, research [2] proposes a quantitative blind steganalysis technique based on SVD features, enabling the detection of a broad range of data hiding methods. However, generating a complete set of SVD features for a large number of image blocks demands substantial computational resources and time, making this approach impractical for real-time streaming data processing. A similar challenge is encountered by the universal method of Gul and Kurugollu [3], which operates in the spatial domain by modeling pixel row and column dependencies through SVD combined with additional filtering. While this method achieves high accuracy, it does so at the expense of significant computational complexity.

Another research direction involves combining SVD with other transforms, particularly the discrete cosine transform (DCT). In [4], singular values of DCT coefficients are employed for universal steganalysis, enabling the detection of various types of embeddings. However, the combined use of DCT and SVD substantially increases computational demands, rendering this approach unsuitable for resource-constrained environments. Significant theoretical advancements in applying the SVD domain for developing universal steganalysis methods are presented in [5], though it should be noted that these approaches also involve high computational complexity. Similarly, [6], which focuses on a method based on relationships between DCT transformants, utilizes resource-intensive transformations alongside artificial intelligence techniques to analyze dependencies among DCT transform components.

Modern steganalysis methods increasingly leverage machine learning techniques. In [7], the authors explore the application of deep learning models for image steganography, employing various neural network architectures to detect covert data in images. The authors also present results on comparing their effectiveness and accuracy, which indicate that deep learning models can successfully identify steganographic content, though their performance heavily depends on the quality of the training data and the model's configuration. Reference [8] offers a comprehensive overview of machine learning applications in steganography, analyzing different approaches and algorithms used to detect concealed data in multimedia files, particularly images. The review also highlights the strengths and limitations of each method, stressing the importance of selecting suitable algorithms and parameters to achieve high detection accuracy.

In [9], the authors propose a steganalysis model that integrates a deep neural network with the θ-NSGA-III algorithm for hyperparameter optimization. This approach achieves high accuracy in detecting covert data in images, particularly on the STEGRT1 dataset. However, like most deep learning models, it carries risks of overfitting and demands substantial computational resources. Paper [10] presents HSDetect-Net – a deep learning-based method incorporating fuzzy logic for detecting covert data in digital images. The proposed approach demonstrates high steganalysis accuracy; however, it requires substantial computational resources due to the model's complexity and the processing of large data volumes. A comprehensive review of machine and deep learning applications in steganalysis is provided in [11], where the authors examine various approaches, including neural network-based detection of covert messages in images. Particular emphasis is placed on methods capable of effectively identifying steganographic data even under challenging conditions, such as noisy communication channels.

However, machine learning-based approaches demand substantial computational power, specialized hardware, and optimized computing environments, which conflict with the speed and scalability requirements of web applications.

Consequently, most existing solutions, while highly effective, suffer from excessive computational complexity, which limits their practical deployment on web platforms that must handle large streams of multimedia files in real-time with minimal server load. This creates a clear need for new approaches that balance high detection accuracy with computational efficiency, while supporting scalable data processing.

In web applications that manage vast amounts of multimedia data and require minimal latency in user interactions, both accuracy and speed of steganalysis methods are critical. Therefore, the challenge is to develop algorithms that combine high sensitivity to steganographic embeddings with efficient utilization of computing resources within the dynamic environment of web platforms.

A promising direction for improving steganalysis efficiency under limited computational resources is the use of the Walsh-Hadamard transform domain. This transform offers lower computational complexity compared to other commonly used orthogonal transforms, making it particularly attractive for web applications where algorithm speed is critical. At the same time, existing approaches already employ the Walsh-Hadamard domain to detect covert channels, especially those based on the concept of code control. Such channels are particularly challenging to detect due to their high robustness and ability to preserve the statistical properties of the container, which further

underscores the importance of researching steganographic methods within this transform domain.

Overall, advancing steganography techniques in the Walsh-Hadamard transform domain paves the way for developing universal algorithms capable of detecting covert channels with minimal computational overhead. This is especially crucial for web applications processing large volumes of multimedia data and requiring high-speed security systems without compromising detection accuracy. The development of such approaches would significantly enhance protection against information leakage and abuse linked to the use of steganography in modern interactive platforms.

Formulation of the goals of the article. Therefore, the current objective is to further advance steganalysis methods operating within the Walsh-Hadamard transform domain. It is crucial not only to ensure effective detection of covert channels based on the concept of code control but also to broaden these methods' capabilities to identify other highly effective steganographic techniques. In particular, algorithms utilizing singular vectors, which are widely used in practice, represent a significant scientific interest due to their high robustness and ability to preserve the reliability of perception, making them especially difficult to detect.

The *purpose* of this paper is to develop a theoretical basis for detecting SVD-organized covert communication channels in the Walsh-Hadamard transform domain.

Outline of the main research material. Steganographic method based on the modification of singular vector values. Steganographic methods based on SVD are among the most widely used today due to their high resilience against attacks targeting the embedded message. Two main approaches can be distinguished: methods that modify the matrix of singular values (Σ-methods) and methods that operate on the left and right singular vector matrices (UV-methods). The latter, UV-methods, are notably more resistant to various types of distortions and ensure a high level of reliability of the perception of the steganographic message, making them more prevalent in practice.

One powerful approach to hiding data in multimedia containers is the steganographic method proposed in [12], which is based on modifying the singular vector values corresponding to the first singular value of a block. This technique ensures high stability of the covert channel by leveraging the properties of singular value decomposition: even minor alterations to the singular vectors can carry information without noticeable degradation of image quality while preserving high resistance to attacks against the embedded message. For completeness, we next consider a method implementing this principle through the stepwise modification of the first left or right singular vectors in each container block, along with the corresponding data embedding and extraction procedures.

Let us introduce the necessary definitions. Singular value decomposition is one of the most powerful tools in signal and image processing and is widely applied in steganography. By concentrating signal energy in singular values and capturing geometric features in singular vectors, SVD enables the development of embedding methods that combine high perception reliability with strong resistance to attacks.

For a given block B, the singular value decomposition is defined as [13]

$$B = U\Sigma V^T, \qquad (1)$$

where U, V are orthogonal matrices of left lexicographically positive and right singular vectors, respectively, $\Sigma = diag(\sigma_1,...,\sigma_8)$ is the matrix of singular values.

Embedding of the additional information [12]

Step 1. The container matrix F is standardly divided into 8×8-blocks; B is an arbitrary block.

Step 2. The next bit of additional information p_i is embedded in the next block B:

2.1. A singular decomposition (1) is constructed for the block B; u_1 and v_1 are the left and right singular vectors of the block B, respectively, corresponding to the singular value σ_1.

2.2. (embedding):

If $p_i = 1$, then $u_1 = n^o$, where $\overline{u}_1$ is perturbed during steganographic transformation u_1, n^o is n-optimal vector. Bring the left singular vectors of the block B to orthonormalized with $\overline{u}_1$ lexicographic $u_2,...,u_8$ ally positive from. Result is $\overline{u}_2,...,\overline{u}_8$.

Otherwise $\overline{v}_1 = n^o$ where v_1 is perturbed during steganographic transformation v_1. Bring the right singular vectors $v_2,...,v_8$ of the block $\overline{B}$ to orthonormalized with $\overline{v}_1$ from. Result is $\overline{v}_2,...,\overline{v}_8$.

2.3. (Formation of a steganographic message block corresponding to the container block). If $p_i = 1$, then $\overline{B} = \overline{U}\Sigma V^T$ where $\overline{U} = (n^o, \overline{u}_2,...,\overline{u}_8)$, otherwise $\overline{B} = U\Sigma\overline{V}^T$, where $\overline{V} = (n^o, \overline{v}_2,...,\overline{v}_8)$.

Extraction of additional information [12]

Step 1. The steganographic message matrix $\overline{F}$ is divided into 8×8-blocks in the standard way; $\overline{B}$ is an arbitrary block.

Step 2. From the next block $\overline{B}$, the next bit $\overline{p}_i$ of additional information is extracted:

2.1. For $\overline{B}$ a singular decomposition is constructed: $\overline{B} = \overline{U}\Sigma\overline{V}^T$; u_1 and $\overline{v}_1$ are the left and right

singular vectors of the block $\overline{B}$, respectively, corresponding to the first singular value $\overline{\sigma_1}$.

2.2. (Extraction of $\overline{p_i}$). Find UN_B and VN_B which are the angles between the vectors u_1, n^o and v_1, n^o respectively.

If $UN_B < VN_B$, then $\overline{p_i} = 1$, otherwise $\overline{p_i} = 0$.

Given the nature of the method under consideration, the modifications it introduces to container blocks are non-deterministic and depend on the initial structure of the corresponding blocks. This characteristic provides a high level of resistance of the embedded message to attacks, as the covert data adapts to and is shaped by the container's structure. At the same time, this very feature complicates establishing a clear correspondence between modifications in the singular value decomposition domain and their representation in the Walsh-Hadamard transform domain. This calls not only for a theoretical understanding of the mechanisms by which such changes take effect, but also for practical experiments to identify patterns and evaluate the effectiveness of steganography within this domain.

Theoretical foundations for developing a non-blind method for detecting steganographic messages based on the SVD UV-method. For effective steganalysis of steganographic methods based on the modification of singular vectors, it is crucial to examine how these changes affect the Walsh-Hadamard transformants of the container blocks. Since the method introduces non-deterministic modifications that depend on the initial block structure, analyzing the Walsh-Hadamard transformants makes it possible to identify distinctive patterns of the influence caused by the embedded information. This analysis is a $\overline{B_i}$ key to developing steganalysis algorithms capable of reliably and efficiently detecting covert messages in the Walsh-Hadamard transform domain, which is of particular importance for deployment in real-world web applications.

Let us now introduce the definitions necessary for further research.In applications involving graphic information processing, particularly in steganography, the two-dimensional discrete Walsh-Hadamard transform is widely used and is defined as

$$W = H'_N X H'^T_N, \qquad (2)$$

where $H'_N = \frac{1}{N} H_N$, and X is a matrix of size $N \times N$.

In turn, H_N is a Walsh-Hadamard matrix of order $N = 2^k$, which can be constructed according to Sylvester's construction

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, \qquad (3)$$

where $H_1 = 1$, and Y is a row vector of length N.

Experiment 1.

In order to research the influence of the steganographic method [12] on certain transformants of the Walsh-Hadamard transform, we will perform the following experiment on a set of 530 images of size 1024x1024 pixels in a lossless format from the database [14]. Let us present the algorithm of the experiment, which was used to process each of the images:

Step 1. Embed additional information into the next image F according to the algorithm [12] (as an embedded sequence, a pseudo-random uniformly distributed sequence was used), as a result of which we obtain the steganographic message $\overline{F}$.

2. Segment the obtained images F and $\overline{F}$ into blocks B_i and $\overline{B_i}$, $i = 1,2,...,16384$ of size 8x8, in a standard way.

3. According to (2), find for each block B_i and the matrices of the two-dimensional Walsh-Hadamard transform W_{B_i} and $W_{\overline{B_i}}$.

4. For each pair of transformant matrices W_{B_i} and $W_{\overline{B_i}}$ find the difference matrix that will reflect the change in the transformants of the Walsh-Hadamard transform in the container, which is conditioned by the steganographic transformation in the singular value decomposition domain

$$\Delta_i = \left| W_{\overline{B_i}} - W_{B_i} \right|, \quad i = 1,2,...,16384. \qquad (4)$$

5. Average the value of each matrix Δ_i element across all blocks, among all images participating in the experiment.

Fig. 1 presents a heat map of changes in the Walsh-Hadamard transformants resulting from the application of the steganographic method [12].

Analysis of the data presented in Fig. 1 leads to the conclusion that the changes caused by the steganographic transformation in the singular value decomposition domain according to the method [12] are concentrated mostly in the corner regions of the matrix of transformants of the Walsh-Hadamard transform, with the greatest amplitude of influence being exerted by the transformants (8,8), (1,8), (8,1), (1,1).

The analysis of 530 images, each of which was presented as a set of blocks of size 8×8, made it possible to determine the positions of the coefficients of the Walsh-Hadamard transform, which most often underwent maximum changes in absolute value. As a result, it was found that in the vast majority of cases, namely in 494 out of 530 images, the largest changes

Fig. 1. The heat map of changes in the transformants of the Walsh-Hadamard transform due to the steganographic transformation

were observed in the position (8,8), which may indicate a high sensitivity or variability of the high-frequency coefficient corresponding to this position in the transform domain. Less often, in 21 cases, the maximum occurred at position (8,1), and in another 13 cases at (1,8). In two cases, the largest change was recorded at position (1,1). In all other positions of the matrix of coefficients, no maximum changes were recorded.

According to the results shown in Fig. 1, it can indeed be stated that, within the framework of the chosen experimental algorithm, certain Walsh-Hadamard transform components exhibit the largest change amplitudes when comparing the steganographic message with the original container. However, it should be clearly emphasized that these observations are derived from an analysis of the steganographic message / container difference. In other words, they do not result from blind detection, but rather from a scenario in which both samples are available, or when a large set of reference containers can be used for comparison. Such an approach is valuable as a heuristic or as part of a non-blind method, but its conclusions cannot be directly generalized to cases where only the steganographic message is available.

In non-blind steganalysis, when hidden data is suspected, it is sufficient to analyze only four specific coefficients instead of all 64. This reduces computational costs and simplifies detection by up to a factor of 16. However, when the original container is unavailable, relying solely on these positions without further justification may not be sufficiently reliable.

In steganalysis, it is important to remember that large absolute changes do not necessarily indicate a strong statistical shift. For instance, if the value of the (8, 8) transform component fluctuates significantly in both directions (increase and decrease), its mean value may remain almost unchanged. In contrast, smaller but systematic changes can produce a more noticeable shift. For example, if another transform component consistently increases, even slightly, this will result in a measurable shift in its distribution.

Theoretical foundations for developing a blind method for detecting steganographic messages based on the SVD UV-method. For a more detailed analysis, we will examine the statistical characteristics of the Walsh-Hadamard transform coefficients of a steganographic message, considering both the original image from database [14] and the steganographic transformation created using method [12].

It is worth noting that the well-known statistical properties of Walsh-Hadamard transform coefficients, presented in [15], will be useful for this analysis. In [15], it is shown that if the matrices W_{X_i} of size $N \times N$ of Walsh-Hadamard transform coefficients for the n image blocks X_j, $j = 1,2,...,n$ are given, each has the form

$$W_{X_j} = \begin{bmatrix} w_{X_j,11} & w_{X_j,12} & \cdots & w_{X_j,1N} \\ w_{X_j,21} & w_{X_j,22} & \cdots & w_{X_j,2N} \\ \vdots & \vdots & \ddots & \vdots \\ w_{X_j,N1} & w_{X_j,N2} & \cdots & w_{X_j,NN} \end{bmatrix}, \quad (5)$$

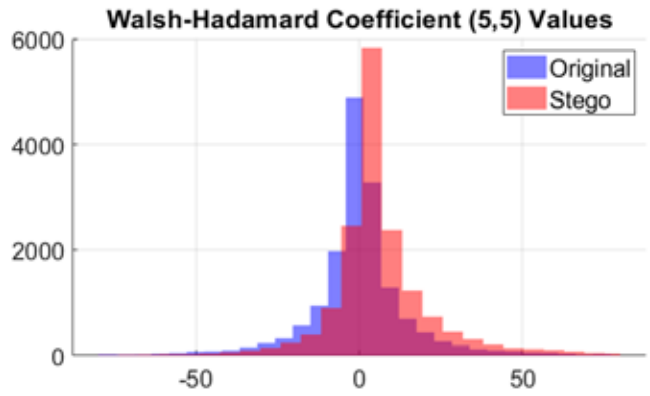
then the sequence of transformants $u_{kl} = \begin{bmatrix} w_{X_1,kl} & w_{X_2,kl} & \ldots & w_{X_n,kl} \end{bmatrix}$ has zero mathematical expectation $\mathrm{E}[u_{kl}] = 0$ for any k,l except $k = l = 1$.

This statement is very important from the perspective of steganalysis possibilities, as it concludes the absence of disturbances in the image based on its statistical data.

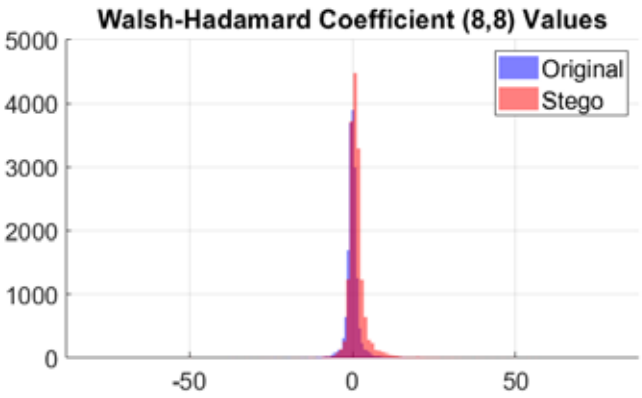
For example, Fig. 2 shows the histograms of the distribution of transformants of the Walsh-Hadamard transform (5,5) and (8,8). Note that according to Fig. 1, the transformant (8,8) belongs to those that are included in the zone of maximum influence of the steganographic method [12], for the original image and the image that has undergone steganographic interference.

As we can see from Fig. 2, the histogram of the values of the transformant (5,5) has undergone a more significant shift compared to the histogram of the transformant (8,8), the possibility of which was noted earlier. The maximum values of the amplitude of the influence on a particular transformant of the Walsh-Hadamard transform do not necessarily mean the maximum shift of its statistical features.

Let us present matrices that contain the average absolute values of all sequences u_{kl} and $\bar{u}_{kl}$ of transformants of the Walsh-Hadamard transform for the researched image and the steganographic transformation



a)



b)

Fig. 2. Histograms of the distribution of transformants a) – (5,5), b) – (8,8), for the original image and steganographic transformation

$$E[u_{kl}] = \begin{bmatrix} 1091.2 & -0.03 & -0.11 & 0 & -0.06 & 0.02 & -0.04 & -0.01 \\ 0.04 & 0 & 0 & 0 & -0.01 & 0 & 0 & 0 \\ 0.02 & 0.01 & 0.01 & -0.01 & 0.09 & 0.02 & 0.01 & -0.01 \\ 0.03 & 0 & 0.02 & -0.01 & -0.06 & 0 & -0.02 & 0 \\ 0.04 & 0 & -0.02 & 0.04 & 0 & 0 & 0 & 0 \\ 0.01 & 0 & -0.02 & 0 & 0.05 & 0 & 0.02 & 0 \\ -0.08 & 0 & -0.02 & -0.02 & 0.18 & 0.01 & 0.03 & -0.05 \\ 0.07 & 0 & 0.02 & -0.02 & 0.03 & 0 & 0 & 0 \end{bmatrix},$$

$$E[\bar{u}_{kl}] = \begin{bmatrix} 1093.2 & 0.12 & 0.18 & -0.03 & 0.46 & -0.06 & -0.09 & 0 \\ 0.06 & 0.75 & 0.68 & 0.17 & 1.02 & 0.36 & 0.04 & 0.09 \\ 0.05 & 0.55 & 2.91 & 0.21 & 1.89 & 0.12 & 0.27 & 0.06 \\ -0.02 & 0.31 & 0 & 1.58 & 0 & -0.33 & -0.05 & 0.37 \\ 0.12 & 1.03 & 1.84 & 0.03 & 7.32 & 0.10 & 0.21 & -0.95 \\ -0.01 & 0.36 & -0.04 & -0.16 & 0.05 & 1.14 & 1.24 & 0.15 \\ -0.07 & 0.08 & 0.14 & -0.19 & 0.13 & 1.14 & 3.94 & 0.18 \\ 0.06 & -0.08 & 0.32 & 0.38 & -0.95 & 0.35 & 0.04 & 1.37 \end{bmatrix}. \quad (6)$$

We see that the largest shift occurred in the transformant of the Walsh-Hadamard transform (5,5). For further practical research of this phenomenon, we will perform the following experiment.

Experiment 2.

The source material for this experiment was 530 steganographic messages of size 1024x1024 pixels in lossless format (PNG), which were generated based on the database [14].

The procedure in this experiment will be presented in the form of specific steps that must be performed for each of the images.

Step 1. Load the steganographic message $\overline{F}$. Perform its division into blocks $\overline{X}_i$ of size 8x8 in a standard way.

Step 2. For each received block, according to (2), find the matrix of transformants of the Walsh-Hadamard transform $\overline{W}_{X_j}$, as each of these matrices having the structure (6).

Step 3. Construct sequences $\bar{u}_{kl} = \left[w_{X_1,kl} \quad w_{X_2,kl} \quad \ldots \quad w_{X_n,kl} \right]$ of the Walsh-Hadamard transformants of the steganographic message.

Step 4. Find the average values $E[\bar{u}_{kl}]$.

Step 5. Perform statistical processing of the obtained values for all images involved in the experiment, construct a heat map of the shifts of the average values $E[\bar{u}_{kl}]$ from the theoretically calculated value for the original containers $E[u_{kl}] = 0$.

The heat map obtained as a result of the execution of the specified algorithm is shown in Fig. 3.

The heat map presented in Fig. 3 illustrates the average changes in the Walsh-Hadamard transform coefficients following image processing using the steganographic method. The analysis reveals that the largest shifts occur at the coefficients with coordinates (1,5), (5,1), and (5,5). These positions correspond to low-frequency components that store the overall structure of the image [16]. It is well established [17, 18] that these transform coefficients are optimal for

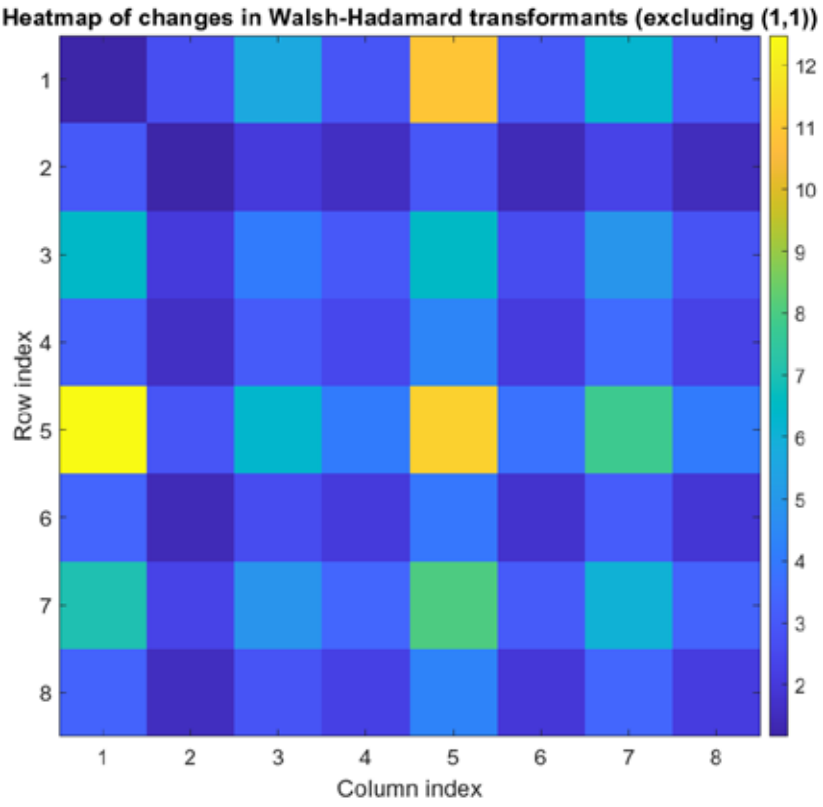


Fig. 3. Heat map of shifts of histograms of Walsh-Hadamard transformants

embedding additional information in code-controlled steganographic methods, as this approach enhances concealment and robustness while maintaining high image quality.

Moreover, these same coefficients become critical for analysis in blind steganalysis scenarios when hidden data embedding is suspected: instead of examining all 64 coefficients, analyzing only these three is sufficient, significantly reducing computational costs and simplifying the detection process by up to a factor of 21.

Conclusions. The performed research identified key patterns in how steganographic transformations in the singular value decomposition domain affect the Walsh-Hadamard transform coefficients. The obtained results are fundamentally important for advancing steganalysis methods, particularly in two main directions:

1. Non-blind analysis (with access to the original container): four key transform coefficients – (8,8), (1,8), (8,1), and (1,1) – were identified as exhibiting the greatest amplitude of changes. A mathematical framework for comparing pairs of images was developed, enabling highly accurate detection of embedded data. It was demonstrated that the most informative coefficients are the angular transform components corresponding to high-frequency regions.

2. Blind analysis (without access to the original container): three critically important low-frequency coefficients – (1,5), (5,1), and (5,5) – were found to exhibit the largest statistical shifts. A novel analytical approach was proposed based on researching changes in the distribution of these coefficients. It was proven that systematic alterations at these positions serve as reliable indicators of covert messages.

The theoretical contribution of this paper lies in revealing the mechanisms underlying the interaction between singular value decomposition and Walsh-Hadamard transformants in steganography, justifying the selection of optimal transform coefficients for analysis, and developing new criteria for detecting steganographic modifications.

Practical significance of the research: The proposed results suggest a potential reduction in computational complexity of steganalysis by a factor of 16 to 21. The developed approaches are developed for implementation in resource-constrained web environments, opening new possibilities for designing effective protection systems.

The findings also point to several promising directions for further scientific research. A key area is the adaptation of these results to dynamic multimedia containers such as video and audio, as well as their extension to modern lossy compression formats. Of particular interest is the integration of machine learning techniques to automate the detection of complex steganographic manipulations, especially through deep learning methods analyzing both spatial and frequency domain features. Furthermore, exploring the application of these results to the development of new steganographic methods with enhanced resistance to analysis offers opportunities for advancing information security tools.

Bibliography:

1. Othman N. A. et al. Image Steganography Using Web Application. Journal of Computing Research and Innovation. 2023. Vol. 8, No. 2. P. 1-11. doi: 10.24191/jcrinn.v8i2.373

2. Singhal A., Bedi P. Blind quantitative steganalysis using SVD features. International Conference on Advances in Computing, Communications and Informatics (ICACCI). IEEE, 2018. P. 369-374. doi: 10.1109/icacci.2018.8554947

3. Gul G., Kurugollu F. SVD-based universal spatial domain image steganalysis. IEEE Transactions on Information Forensics and Security. 2010. Vol. 5, No. 2. P. 349-353. doi: 10.1109/tifs.2010.2041826

4. Heidari M., Gaemmaghami S. Universal image steganalysis using singular values of DCT coefficients. 10th International ISC Conference on Information Security and Cryptology (ISCISC). IEEE, 2013. P. 1-5. doi: 10.1109/iscisc.2013.6767340

5. Khoroshko V., Kobozeva A., Bobok I. Improving the method of detecting block processing of digital images. Information control systems and technologies. Problems and solutions. 2019. P. 47-59.

6. Khalilollahi S. M. S., Mansouri A. JPEG steganalysis using the relations between DCT coefficients. International Conference on Machine Vision and Image Processing (MVIP). IEEE, 2022. P. 1-4. doi: 10.1109/mvip53647.2022.9738785

7. Kuznetsov A. et al. Image steganalysis using deep learning models. Multimedia Tools and Applications. 2024. Vol. 83, No. 16. P. 48607-48630. doi: 10.1007/s11042-023-17591-0

8. Jung K. H. A study on machine learning for steganalysis. Proceedings of the 3rd International Conference on Machine Learning and Soft Computing. 2019. P. 12-15. doi: 10.1145/3310986.3311000

9. Iskanderani A. I. et al. Artificial Intelligence-Based Digital Image Steganalysis. Security and Communication Networks. 2021. Vol. 2021, No. 1. P. 9923389. doi: 10.1155/2021/9923389

10. Bai M. et al. Towards next-generation steganalysis: LLMs unleash the power of detecting steganography. arXiv preprint arXiv:2405.09090. 2024. P. 1-13.

11. Gupta A. et al. Machine learning and deep learning in steganography and steganalysis. Multidisciplinary Approach to Modern Digital Steganography. IGI Global Scientific Publishing. 2021. P. 75-98.

12. Kobozeva A. A., Melnyk M. A. Steganographic algorithm based on sign-insensitivity of singular vectors of the image matrix. Systems of information processing. 2013.Vol. 3, No. 110. P. 90-94.

13. Klema V., Laub A. The singular value decomposition: Its computation and some applications. IEEE Transactions on automatic control. 1980. Vol. 25, No. 2. P. 164-176. doi: 10.1109/tac.1980.1102314

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

15. Dyka A.I. Detection of covert channels in web applications based on unimodality violation in the Walsh–Hadamard spectrum. Informatics and Mathematical Methods in Simulation. 2025. Vol.15, No. 1, P. 5-14. doi: 10.15276/imms.v15.no1.5

16. 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. Problemele Energeticii Regionale. 2022. No. 2 (54). P. 84-100. doi: 10.52254/1857-0070.2022.2-54.08

17. Kobozeva A.A., Sokolov A.V. Steganographic Method with Code Control of Information Embedding Based on Multi-level Code Words. Radioelectronics and Communications Systems. No. 4 (66). P. 173-189. doi: 10.3103/s0735272723040052

18. Kobozeva A.A., Sokolov A.V. Robust Steganographic Method with Code-Controlled Information Embedding. Problemele energeticii regionale. 2021. No. 4 (52). P. 115-130. doi: 10.52254/1857-0070.2021.4-52.11

Дика А.І. ВИЯВЛЕННЯ SVD-ПРИХОВАНИХ ДАНИХ У ВЕБЗАСТОСУНКАХ НА ОСНОВІ АНАЛІЗУ ТРАНСФОРМАНТ ПЕРЕТВОРЕНННЯ УОЛША-АДАМАРА

Сучасні вебзастосунки опрацьовують величезні обсяги мультимедійних даних, що створює ризик використання їх як транспортних каналів для прихованої передачі інформації за допомогою стеганографії. Це вимагає методів стеганоаналізу, здатних працювати в режимі реального часу без надмірного навантаження на сервери. У цій роботі розроблено метод виявлення прихованих повідомлень, вбудованих у просторі сингулярного розкладу, шляхом аналізу коефіцієнтів в області перетворення Уолша-Адамара. Запропонований підхід поєднує переваги високої чутливості до стеганографічних втручань із обчислювальною простотою перетворення Уолша-Адамара, що дозволяє суттєво скоротити витрати ресурсів при обробці великих масивів даних. Доведено, що модифікація лівих і правих сингулярних векторів, що відповідають старшому сингулярному числу у просторі сингулярних розкладень призводить до характерних змін у вибраних трансформантах перетворення Уолша-Адамара. Для сценаріїв несліпого аналізу визначено високочастотні кутові трансформанти (8,8), (1,8), (8,1), (1,1), які демонструють найбільші амплітуди змін. Для сліпого аналізу виявлено три низькочастотні трансформанти (1,5), (5,1) та (5,5), що зазнають найбільшого статистичного зсуву і можуть слугувати надійними маркерами прихованої інформації. Використання лише цих позицій дозволяє зменшити обчислювальну складність у 16–21 раз при збереженні високої точності детектування, що особливо важливо для веб-сервісів із високою інтенсивністю запитів. Отримані результати ґрунтуються на обробці набору з 530 зображень у форматі без втрат, що дозволило виявити ключові закономірності впливу модифікацій у просторі сингулярного розкладу на коефіцієнти перетворення Уолша-Адамара. Запропоновані у роботі теоретичні основи створюють базис для розробки високоефективних алгоритмів стеганоаналізу, здатних працювати в режимі реального часу з мінімальними обчислювальними витратами. Завдяки використанню обмеженого набору інформативних трансформант перетворення Уолша-Адамара ці алгоритми потенційно можуть бути інтегровані у серверні системи безпеки веб-платформ для потокового аналізу великої кількості файлів. Теоретичні положення також можуть бути адаптовані для виявлення прихованих даних у відео- та аудіопотоках, а у поєднанні з методами машинного навчання – стати основою гібридних рішень з підвищеною стійкістю та точністю детектування сучасних стеганографічних алгоритмів.

Ключові слова: *стеганоаналіз, перетворення Уолша-Адамара, сингулярний розклад, приховані канали зв'язку, кібербезпека, вебзастосунки, частотний аналіз.*

Дата надходження статті: 11.08.2025
Дата прийняття статті: 04.09.2025
Опубліковано: 27.10.2025