DOI 10.15276/imms.v16.no1.16
UDC 004.056.55

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 16-25

THE IMPACT OF CODEWORD SIZE ON THE ROBUSTNESS OF CODE-CONTROLLED STEGANOGRAPHIC METHODS

Sokolov A.V.[1], Pohorieltsev P.M[2]., Zhuk Ye.A.[3], Filipenko N.O.[2]

[1]National University "Odesa Law Academy"
23, Fontanska Road, Odesa, 65009, Ukraine
[2]National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
[3]Kharkiv National University of Radio Electronics
14, Nauky Ave., Kharkiv, 61166, Ukraine
Email: radiosquid@gmail.com[1]

The paper is devoted to a novel direction in digital steganography, the concept of code-controlled information embedding, which allows adaptive management of the embedding process based on the properties of specially designed codewords. In contrast to conventional spatial- or transform-domain techniques, the approach of code control enables precise localization of embedding effects in the frequency domain while maintaining minimal computational complexity. The research aims to determine how the size of the codeword affects the robustness of the steganographic message under identical conditions. To achieve this, a series of controlled experiments was performed using digital images subjected to JPEG compression at varying quality factors. Two embedding strategies were compared: embedding a single bit per smaller block and embedding multiple bits into a larger block at the same capacity. The results show that increasing the codeword size and embedding several bits per block can significantly improve robustness without degrading the reliability of perception, as confirmed by stable PSNR values. However, the experiments also reveal that the benefits of enlarging the codeword size tend to saturate beyond a certain threshold, since larger blocks become more susceptible to compression-induced distortions. The research provides new insights into the balance between robustness, reliability of perception, and embedding efficiency in code-controlled steganography. The results contribute to the optimization of block sizes and embedding strategies, offering practical guidelines for the development of next-generation steganographic systems. The results obtained not only enhance the resilience of hidden data but also lay the foundation for creating adaptive, intelligent, and computationally efficient information-hiding algorithms that can be integrated into modern cybersecurity infrastructures.
Keywords: digital steganography, code-controlled embedding, Walsh-Hadamard transform, robustness, reliability of perception, information hiding, block optimization, JPEG compression, cybersecurity.

Introduction and statement of the problem. In the modern digital era, the exponential growth of multimedia content – ranging from images and audio to video and interactive media – has created both opportunities and challenges for information security. While cryptography has long been recognized as a cornerstone for protecting the confidentiality and integrity of data, steganography is increasingly emerging as a complementary technique that addresses a different aspect of secure communication: the concealment of information itself. By embedding sensitive data within seemingly innocuous multimedia carriers, steganography not only adds a layer of secrecy but also enhances resilience against unauthorized detection and interception. As the volume of digital information continues to expand, and as sophisticated analytical tools become more prevalent, steganography is poised to become an indispensable component of modern information protection systems, operating together with cryptographic methods to ensure both secrecy and security.

Today, the main efforts of researchers in the field of steganography are focused on improving several key characteristics of steganographic methods. These include reliability of

perception, ensuring that the embedded information remains undetectable to human perception; capacity, maximizing the amount of hidden data that can be embedded without compromising the carrier; robustness against attacks, maintaining the integrity of the embedded message under various distortions or manipulations; and resistance to steganalysis, reducing the likelihood of detection by automated or statistical analysis tools. Optimizing these characteristics simultaneously remains a central challenge, guiding the development of both traditional and emerging steganographic techniques.

Today, steganographic techniques have become highly diverse, encompassing a wide range of approaches to embedding additional information into digital media. Traditional methods leverage transform domains [1], such as Discrete Cosine Transform (DCT) or wavelet transforms, to subtly modify carrier signals. At the same time, more recent approaches exploit machine learning and artificial intelligence to optimize embedding patterns and improve imperceptibility. Among these, code-controlled steganography has emerged as an auspicious direction. By using codewords to control the embedding process, these methods can achieve higher efficiency and robustness compared to many other techniques, even when operating directly in the spatial domain of the carrier. This capability allows for precise control over information hiding, making code-controlled methods a powerful tool in the modern steganography arsenal.

We provide a concise overview of recent advances in the aforementioned areas of steganography. Our focus will encompass traditional transformation-domain methods, machine learning- and Artificial Intelligence (AI) based techniques, as well as the emerging field of code-controlled steganography. By highlighting the strengths, limitations, and current trends in each approach, we intend to offer a clear perspective on the state-of-the-art, setting the stage for a deeper discussion on the optimization of code-controlled methods in terms of embedding efficiency and robustness.

A considerable body of recent research has focused on developing transform-domain steganographic methods that enhance the robustness and reliability of the perception of embedded data. Song et al. [2] proposed a robust JPEG steganographic scheme that combines the DCT and Singular Value Decomposition (SVD) within the nonsubsampled shearlet transform (NSST) domain, achieving improved resistance to compression and noise. Liu et al. [3] developed a method that integrates the wavelet-domain SVD with adaptive Quantization Index Modulation (QIM), effectively balancing embedding capacity and robustness for JPEG images. Subhedar [4] explored the use of the ridgelet transform together with SVD, demonstrating high imperceptibility in the spatial-frequency representation of images. Similarly, Singh and Singla [5] combined SVD and the Discrete Wavelet Transform (DWT) to create a multi-level embedding framework capable of preserving image quality while maintaining robustness against steganalysis detection. Collectively, these papers highlight the growing trend of hybrid transformation-based approaches that exploit both frequency-domain properties and matrix factorization techniques to enhance the overall performance of image steganography.

Recent advances in artificial intelligence have significantly influenced the development of next-generation steganographic systems. Chang and Echizen [6] introduced a pioneering concept of steganography beyond space and time using a chain of multimodal AI models capable of synchronizing semantic features across different media types, thereby redefining the boundaries of covert communication. Carol et al. [7] proposed an AI-powered adaptive steganography framework that dynamically selects embedding parameters based on content characteristics, improving both imperceptibility and adaptability to diverse media. Raja Rajeswari N. et al. [8] designed an AI-enhanced LSB steganography interface that leverages neural network feedback to optimize pixel-level embedding, leading to higher accuracy and security. In a comprehensive review, Wani and Sultan [9] analyzed deep learning-based image steganography methods, highlighting how convolutional and generative networks outperform traditional algorithms in balancing payload, reliability of perception, and resistance to

steganalysis. Collectively, these papers illustrate a paradigm shift toward intelligent, context-aware steganographic systems that integrate machine learning to autonomously optimize information hiding strategies.

The direction of code-controlled steganography represents a truly novel paradigm in the field of covert communication. Introduced by the authors, this concept enables embedding additional information directly in the spatial domain of the container, under code-controlled influence of selected carrier components, thereby combining the minimal computational complexity typical for spatial-domain schemes with the robustness advantages often found in transform-domain methods. In particular, the paper [10] demonstrates that by pre-coding the payload with specially designed codewords (for example, with specific Walsh-Hadamard transform characteristics), one can achieve impressive results both in terms of reliability of perception and resistance to attacks (for example, compression-attacks) with minimal embedding cost and low algorithmic overhead. Research [10] shows that carefully constructed classes of codewords localize the embedding disturbances in the targeted transform domain of the container and thus optimize the trade-off between capacity, reliability of perception, and robustness. The multi-level codewords extension [11] further enhances the method's resistance and throughput, making code-controlled steganography a compelling and practically efficient option in modern information-security systems. The most recent advancement in code-controlled steganography is the development of methods enabling blind decoding, where the embedded information can be reliably extracted without prior knowledge of the original container [12]. This approach significantly simplifies the decoding process while maintaining high imperceptibility and robustness against various attacks. By carefully designing the code structures and embedding strategies, these methods optimize the trade-off between computational efficiency, embedding capacity, and resistance to steganalysis, making blind code-controlled steganography an efficient and promising tool for modern secure information systems.

As demonstrated by the research results presented in this paper, the concept of code-controlled steganography not only enables the design of highly efficient embedding methods but also provides a framework for investigating the fundamental properties of steganographic embedding. This, in turn, allows for further refinement and optimization of practically applicable steganographic techniques. For instance, from coding theory, it is well known that the efficiency of error-correcting codes increases with the length of the code. However, there is a lack of publicly available data regarding the optimization of the block size used for embedding information in steganographic systems. In the present paper, we employ the concept of code control to explore this question and investigate which strategy is more effective: embedding multiple bits into a larger block or a single bit into a smaller one.

The *purpose* of this paper is to research the impact of codeword size on the robustness of steganographic messages against attacks on the embedded information, under otherwise equal conditions.

Specifically, the paper seeks to determine whether embedding multiple bits into larger blocks or single bits into smaller blocks provides superior robustness, thereby providing insights that can guide the development of more effective and practically applicable steganographic methods.

Code control concept. The code control concept represents a new paradigm in steganography that allows adaptive control of the embedding process based on the properties of the codewords used.

Let a digital image block X of size $N \times N$ 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

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix},\ H_1 = 1. \quad (2)$$

In addition to the two-dimensional Walsh-Hadamard Transform, its one-dimensional version is also commonly used for a vector Y

$$V = YH_N. \quad (3)$$

At the same time, in [10], a fundamental relationship was established between the two-dimensional and one-dimensional forms of the Walsh-Hadamard Transform, within which it was demonstrated that the two representations are mathematically equivalent and can be converted into each other through vectorization operations

$$\tilde{W} = \tilde{X}\, H_{N^2}, \quad (4)$$

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

$$\tilde{M} = \tilde{X} + \tilde{T}, \quad (5)$$

then

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

As follows from equation (6), the impact on the Walsh-Hadamard transform components of the container block is fully determined by the internal structure of the transform components of the selected codeword. Because each codeword interacts selectively with a specific transform component, this approach enables precise and localized embedding of additional information within the corresponding region of the transform domain.

In the framework of code-controlled embedding, there exists a fundamental flexibility in how codewords are employed within a container block. In the simplest scenario, a single codeword T can be used to represent one bit of additional information per block.

Formally, for a block X_k and a single bit $m_i \in \{-1, 1\}$, the embedding can be expressed as

$$M_k = X_k + m_i T, \quad (7)$$

where T is the codeword selected for the whole embedding process.

Alternatively, it is possible to embed multiple bits within a single block by using a set of codewords $\{T_0, T_1, ..., T_{2^L-1}\}$.

In this case, for a set of L bits $\boldsymbol{m} = \{m_0, m_1, ..., m_{\log L-1}\}$, the embedding is performed as

$$M_k = X_k + T_m. \quad (8)$$

where each codeword T_m selectively influences specific transform components of the block.

This formulation highlights the principled ability to control the number of embedded bits per block by choosing either a single codeword or a combination of multiple codewords, providing a flexible trade-off between embedding capacity and reliability of perception.

This paper addresses the fundamental question of which strategy is more effective under otherwise equal conditions: embedding a single bit into a smaller codeword (7), or embedding multiple bits into a larger codeword (8). By systematically analyzing these two approaches, the

research aims to provide practical guidance for optimizing code-controlled steganographic methods in terms of robustness, imperceptibility, and embedding efficiency.

Experimental Methodology. To ensure the correctness of the comparison between codewords of different lengths, the research is designed so that the experimental conditions remain as similar as possible for all variants. In particular, the embedding process is performed within the same frequency segment of the image representation, and the amplitude of the embedding signal is kept constant. In addition, the density of the additional information relative to the number of pixels in the container is maintained at the same level. This approach allows isolating the influence of the codeword length itself on the resulting resistance of the steganographic message to attacks against the embedded data.

In this research, we perform a comparative analysis of two embedding strategies. The first comparison considers embedding four bits into a single 8×8 codeword versus embedding one bit into a 4×4 codeword.

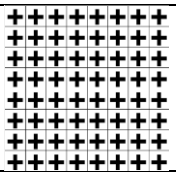
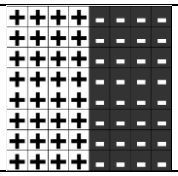
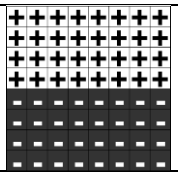
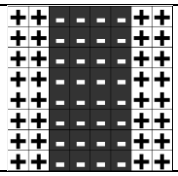
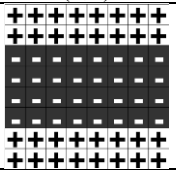
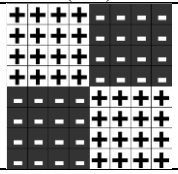
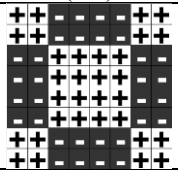
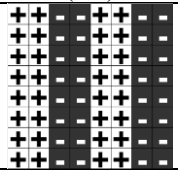
The second comparison evaluates the embedding of four bits in a 16×16 codeword against the embedding of one bit in an 8×8 codeword. These experiments are performed under identical embedding conditions, allowing a direct assessment of the impact of codeword size and the number of embedded bits on the robustness and perceptual quality of the steganographic message.

For the case of four bits embedded into 8×8 codewords, the codewords used are shown in Table 1. For brevity, only the non-inverted variants are presented, i.e., eight codewords, although the total number of such codewords is sixteen.

These codewords serve as the basis for the embedding process, selectively influencing specific low-frequency transform components within each container block. The code distance between these codewords is $d = 32$, ensuring sufficient separation to enhance robustness and reduce decoding errors.

Table 1.

Non-inverse codewords of size 8x8

			
(1,1)	(1,5)	(5,1)	(1,7)
			
(7,1)	(5,5)	(7,7)	(1,3)

In the experiment where a single bit of information is embedded into an 8×8 codeword from Table 1, the embedding specifically targets the (5,1) transform component.

In the experiments involving the embedding of information into 4×4 blocks, a single codeword was used for each block

$$T_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \end{bmatrix}. \quad (9)$$

In the experiment involving the embedding of four bits of additional information into 16×16 blocks, the codewords used are shown in Table 2. For brevity, only the non-inverted variants are presented, i.e., eight codewords, although the total number of such codewords is sixteen.

The code distance between these codewords is 128, providing significant separation to enhance robustness and reduce decoding errors. These codewords selectively influence specific

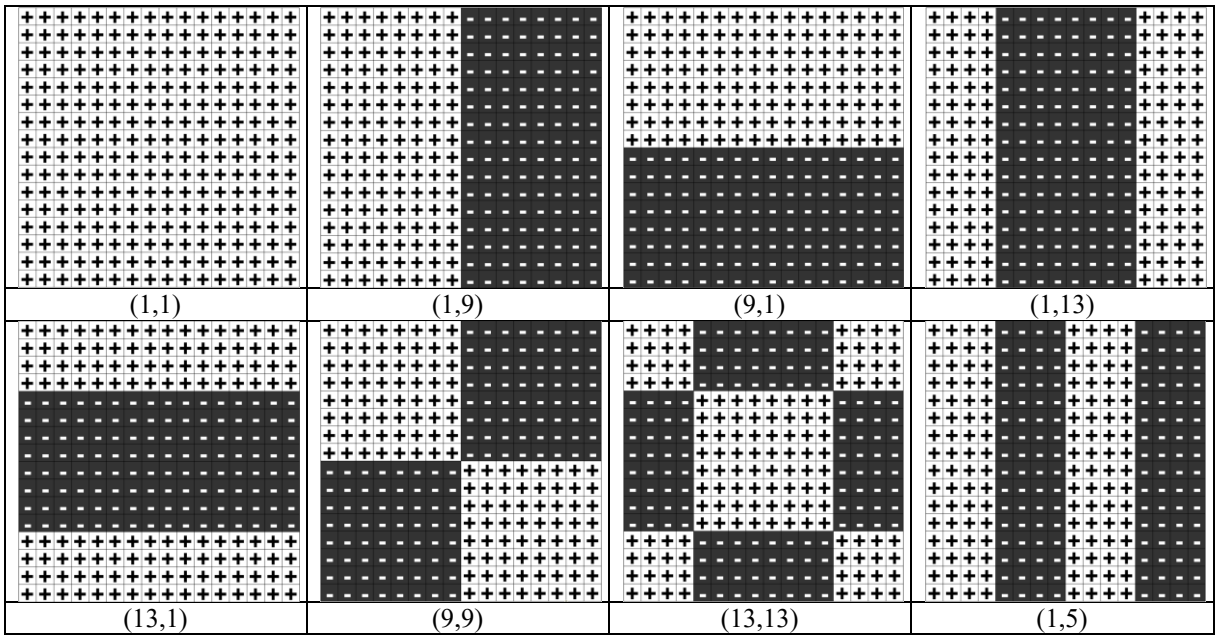
transform components within each block, ensuring controlled embedding while maintaining consistent amplitude and information density across all experiments.

For the experiments involving the embedding of a single bit of additional information into 8×8 blocks, the codeword from Table 2 was used. The embedding specifically targeted the (9,1) transform component of the codeword, ensuring controlled and localized modification of the container block.

It is worth noting that selecting an appropriate set of codewords for embedding additional information is an inherently complex task. The design and optimization of such codeword sets involve numerous considerations, including code distance, transformant selection, and robustness against steganalysis attacks, and therefore deserve dedicated and comprehensive research.

Table 2.

Non-inverse codewords of size 16x16



To evaluate the effectiveness of code-controlled embedding, a series of experiments was performed using digital images and different embedding strategies. The methodology can be summarized as follows:

1. Original color images were converted from the RGB to the YCbCr color space, and only the luminance component (Y) was used as the carrier. Images were cropped to a fixed size of 1200×1200 pixels to ensure uniformity across all experiments.
2. Random binary sequences were generated to represent the additional information to be embedded. For experiments with multi-bit embedding, each block contained 4 bits of information. Each 4-bit group was then mapped to a unique codeword from a predefined set, corresponding to the code-controlled embedding concept.
3. Two independent experimental comparisons were performed:
   - Experiment 1: embedding 1 bit per block in 4×4 codewords versus 4 bits per block in 8×8 codewords.
   - Experiment 2: embedding 1 bit per block in 8×8 codewords versus 4 bits per block in 16×16 codewords.

   In both cases, the overall embedding density (bits per pixel) and the embedding amplitude were kept constant to enable fair comparison.
4. For multibit 8×8 and 16×16 embedding, predefined sets of 16 codewords (8 original and 8 inverted) were employed. The Hamming distance between codewords was 32 and 128, respectively, ensuring high robustness and low decoding error probability. Each

codeword selectively influenced specific Walsh-Hadamard Transform components, allowing localized and controlled embedding.

5. Image blocks were sequentially modified according to the selected codeword and corresponding message bits. The modified luminance component was then recombined with chrominance channels, and the resulting steganographic image was saved in JPEG format with a predefined quality factor (QF).
6. For extraction, the difference between the steganographic and original blocks was computed. Correlations between this difference and all codewords were evaluated to determine the most likely embedded codeword, and the corresponding message bits were recovered. The error rate was calculated as the proportion of incorrectly recovered bits relative to the total number of embedded bits. The bit error rate was calculated as the ratio of incorrectly recovered bits to the total number of embedded bits.

Results of experiments. The results of all performed experiments are summarized in Table 3. This table presents a comprehensive comparison of various embedding strategies, including the use of different codeword sizes and the number of embedded bits per block. The metrics reported allow evaluation of the impact of codeword size and bit quantity on the robustness against compression attack.

Table 3.

Experimental results

Code-word size	Bits per block	Bit per pixel	PSNR, dB	QF									
				10	20	30	40	50	60	70	80	90	100
4x4	1	1/16	48.13	47.8	43.9	38.8	32.7	26.5	20.5	13.5	7.4	1.3	0
8x8	4	1/16	48.13	48.5	44.7	37.7	29.5	21.5	14.7	7.9	2.5	0.7	0.3
8x8	1	1/64	48.13	41.5	29.3	14.9	5.9	3.1	2	0.8	0.3	0	0
16x16	4	1/64	48.13	45.2	34.6	19.2	6.8	2.3	1.4	1	0.5	0.4	0.2

To further assess the robustness of the proposed embedding approach, we constructed Fig. 1, which represents a dependency graph of the percent of extraction errors on the JPEG compression quality factor (QF). This analysis was performed to compare two embedding strategies:

1. embedding one bit of additional information into 4×4 blocks, and
2. embedding four bits of additional information into 8×8 blocks.

Such a comparison enables the determination of which strategy provides a better balance between payload capacity and resistance to compression-induced distortions under otherwise identical embedding conditions.

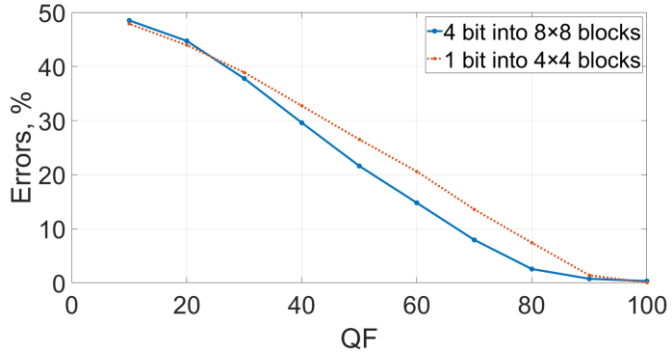


Fig. 1. A dependency graph of the percent of extraction errors on the JPEG compression quality factor (QF) for the case of embedding 1 bit in 4x4 blocks vs 4 bits in 8x8 blocks

A comparative analysis of the embedding results demonstrates a significant improvement in robustness when moving from 4×4 codewords with a single bit per block to 8×8 codewords with four bits per block at the same embedding rate (1/16 bit per pixel). As shown in Fig. 1, increasing the codeword size and the number of embedded bits substantially

reduces the error rate across all JPEG quality factors (QF). The improvement is especially pronounced at QF = 70, which is widely used in practice: the error rate for 8×8 codewords with 4 bits per block is 5.6% lower than that for 4×4 codewords with a single bit. Notably, this increase in robustness is achieved without any degradation of image quality, with PSNR values remaining 48.13 dB.

In this part of the paper, another scenario is examined, as the graph in Fig. 2 illustrates the relationship between the percentage of extraction errors and the JPEG compression quality factor (QF). The experiment compares two embedding strategies:

1. embedding one bit of additional information into 8×8 blocks, and
2. embedding four bits of additional information into 16×16 blocks.

This comparison is intended to evaluate whether increasing the codeword size further enhances the robustness of the embedded data when the embedding rate and all other conditions remain constant, or whether the improvement tends to saturate beyond a certain block size.

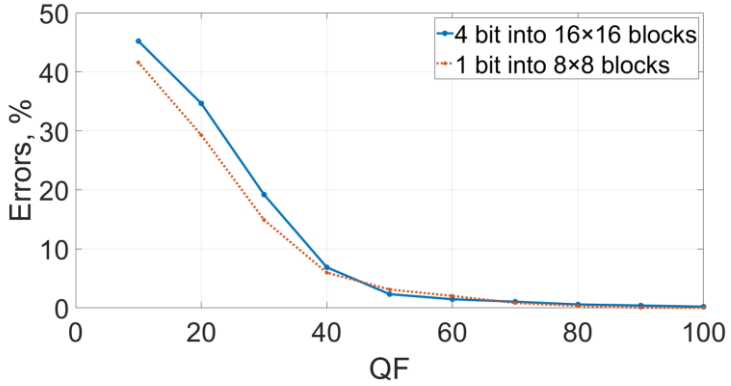


Fig. 2. A dependency graph of the percent of extraction errors on the JPEG compression quality factor (QF) for the case of embedding 1 bit in 8x8 blocks vs 4 bits in 16x16 blocks

A more detailed examination of the results reveals that a straightforward increase in codeword size does not necessarily lead to improved robustness. As shown in Fig. 2, when transitioning from 8×8 blocks with one bit per block to 16×16 blocks with four bits per block, the number of extraction errors decreases only slightly for intermediate JPEG compression levels (QF = 50 and 60). For all other compression levels, however, robustness either remains nearly the same or even decreases despite the larger block size.

This phenomenon can be explained by considering the interaction between block size and embedding capacity. While larger blocks allow embedding more bits per block, they also aggregate more image information, making each embedded bit more sensitive to compression-induced distortions. In other words, the benefits of increasing the codeword size saturate because the relative impact of JPEG quantization on each embedded bit becomes more pronounced as the block grows. Consequently, beyond a certain block size, further enlargement does not yield additional robustness and may even slightly degrade performance for higher compression levels.

Conclusions. The performed research confirms the efficiency of the code-controlled embedding concept as a promising paradigm in modern digital steganography. The approach provides flexible control of the embedding process through specially designed codewords, ensuring a precise balance between reliability of perception, robustness, and computational simplicity. Experimental analysis demonstrates that, under equal embedding density, increasing the codeword size and embedding multiple bits per block significantly improves robustness against compression attacks (especially for JPEG with QF ≈ 70), while maintaining high reliability of perception (PSNR ≈ 48 dB).

The obtained results reveal a saturation effect: beyond a certain block size, further growth of the codeword does not yield additional robustness gains and may even reduce performance at high compression levels. This phenomenon is caused by the cumulative influence of quantization noise on large transform blocks. Comparative evaluation of the tested

strategies indicates that the optimal configuration corresponds to embedding several bits per medium-sized block (e.g., 8×8), which offers the best trade-off between payload, resistance to distortion, and decoding accuracy.

The findings provide a theoretical and practical basis for optimizing block sizes and codeword structures in code-controlled steganography, enabling the development of efficient and adaptive algorithms for secure information hiding in modern cybersecurity systems.

References

1. Abdulla A. A. Digital image steganography: challenges, investigation, and recommendation for the future direction. *Soft Computing.* 2024. Vol. 2. No. 15. P. 8963-8976. DOI: 10.1007/s00500-023-09130-8
2. Song X. et al. Robust JPEG steganography based on DCT and SVD in nonsubsampled shearlet transform domain. *Multimedia Tools and Applications.* 2022. Vol. 81. No. 25. P. 36453-36472. DOI: 10.1007/s11042-022-13525-4
3. Liu J. et al. Robust jpeg image steganography using wavelet domain SVD and adaptive QIM. *8th International Conference on Signal and Image Processing (ICSIP). IEEE*, 2023. P. 434-438. DOI: 10.1109/icsip57908.2023.10270839
4. Subhedar M. Image steganography using ridgelet transform and SVD. *International e-Conference on Intelligent Systems and Signal Processing: e-ISSP. Singapore.* 2021. P. 81-91. DOI: 10.1007/978-981-16-2123-9_6
5. Singh J., Singla M. Image steganography technique based on singular value decomposition and discrete wavelet transform. *International Journal of Electrical and Electronics Research.* 2022. Vol. 10, No. 2. P. 122-125. DOI: 10.37391/ijeer.100212
6. Chang C. C., Echizen I. Steganography beyond space-time with chain of multimodal *AI. Scientific Reports.* 2025. Vol. 15. No. 1. P. 12908. DOI: 10.1038/s41598-025-97238-2
7. Carol I. K. S., Kumar D. K., Ragavan V. A. N. AI-Powered Adaptive Steganography. Smart System for Integrated Computing and Communication: First International Conference, ICSSICC 2024, Coimbatore, India, November 15–16, 2024, Proceedings. Springer Nature, 2025. P. 328.
8. Raja Rajeswari N. et al. AI-enhanced LSB steganography interface: concealed data embedding framework. *9th International Conference on Smart Structures and Systems (ICSSS). IEEE*. 2023. P. 1-4. DOI: 10.1109/icsss58085.2023.10407062
9. Wani M. A., Sultan B. Deep learning based image steganography: A review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery.* 2023. Vol. 13, No. 3. P. e1481. doi: 10.1002/widm.1481
10. 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
11. 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. DOI: 10.3103/s0735272723040052
12. Sokolov A.V., Ihnatenko O.O., Balandina N.M. Increasing the Efficiency of Blind Decoding of the Steganographic Method with Code Control of Additional Information Embedding. *Problems of regional energetics.* 2024. Vol. 62. No. 2. P. 121-137. DOI: 10.52254/1857-0070.2024.2-62.11

ВПЛИВ РОЗМІРУ КОДОВОГО СЛОВА НА СТІЙКІСТЬ СТЕГАНОГРАФІЧНИХ МЕТОДІВ З КОДОВИМ УПРАВЛІННЯМ

Соколов А.В.[1], Погорєльцев П.М.[2], Жук Є.А.[3], Філіпенко Н.О.[2]

[1]Національний університет «Одеська юридична академія»
23, Фонтанська дорога, Одеса, 65009, Україна
[2]Національний університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044, Україна
[3]Харківський національний університет радіоелектроніки
14, Науки пр., Харків, 61166, Україна
Email: radiosquid@gmail.com[1]

Стаття присвячена новому напрямку в цифровій стеганографії – концепції вбудовування інформації з кодовим управлінням, яка дозволяє адаптивно керувати процесом вбудовування на основі властивостей спеціально розроблених кодових слів. На відміну від традиційних методів, що працюють у просторовій області, або в областях перетворень, концепція кодового управління дозволяє точно локалізувати ефекти вбудовування в частотній області, зберігаючи при цьому мінімальну обчислювальну складність. Мета дослідження – визначити, як розмір кодового слова впливає на стійкість стеганографічного повідомлення при інших однакових умовах. Для досягнення цієї мети було проведено серію контрольованих експериментів з використанням цифрових зображень, що піддавалися стисненню JPEG з різними коефіцієнтами якості. Було порівняно дві стратегії вбудовування: вбудовування одного біта в менший блок та вбудовування кількох бітів у більший блок з тією ж пропускною спроможністю. Результати показують, що збільшення розміру кодового слова та вбудовування кількох бітів у блок може значно покращити стійкість без погіршення надійності сприйняття, що підтверджується стабільними значеннями PSNR. Однак, експерименти також показують, що переваги збільшення розміру кодового слова мають тенденцію до насичення після досягнення певного порогу, оскільки більші блоки стають більш схильними до спотворень, викликаних стисненням. Дослідження дає нове розуміння балансу між стійкістю, надійністю сприйняття та ефективністю вбудовування в стеганографії з кодовим управлінням. Результати сприяють оптимізації розмірів блоків та стратегій вбудовування, пропонуючи практичні рекомендації для розробки стеганографічних систем наступного покоління. Отримані результати не тільки підвищують стійкість прихованих даних, але й закладають основу для створення адаптивних, інтелектуальних та обчислювально ефективних алгоритмів приховування інформації, які можна інтегрувати в сучасні інфраструктури кібербезпеки.

Ключові слова: цифрова стеганографія, вбудовування з кодовим управлінням, перетворення Уолша-Адамара, стійкість, надійність сприйняття, приховування інформації, блокова оптимізація, стиснення JPEG, кібербезпека.