High-Capacity Spatial Steganography Based on Perfect Binary Arrays*

Artem Sokolov[1,*†], Denys Yevdokymov[1,†] and Oleksii Fraze-Frazenko[2,†]

[1] National University "Odesa Law Academy", Fontanska Road, 23, Odesa, Ukraine
[2] Odesa I.I. Mechnikov National University, Vsevolod Zmienko Street, 2, Odesa, Ukraine

Abstract

We propose a fundamentally new steganographic approach based on perfect binary arrays — two-dimensional algebraic structures with ideal 2D periodic autocorrelation properties. The method operates in the spatial domain and utilizes the symmetry of perfect binary arrays under cyclic shifts and inversion to encode information with mathematically guaranteed control over signal perturbation. By assigning each message fragment to a specific transformation from a set of $2N^2$ possible states (where N is the block size), the method enables flexible, high-capacity embedding: for instance, up to 7 bits per 8×8 block, which exceeds the capacity of classical code-controlled schemes by a factor of seven. We derive general modulation and decoding formulas, rigorously analyze perceptual impact, and demonstrate that pixel modifications are limited to ±1, resulting in PSNR values above 48 dB even at 100% embedding density. Moreover, the method shows resilience under JPEG compression, maintaining message integrity at low compression levels. These results highlight the potential of algebraic structures such as perfect binary arrays not only to redefine payload capacity limits but also to inspire a shift in steganographic design toward structured, high-order embedding, as originally envisioned in Shannon's coding theory.

Keywords

steganography, perfect binary arrays, code-controlled embedding, spatial domain, autocorrelation, cyclic shift, embedding capacity, information security, JPEG compression, Shannon's theory

1. Introduction

The rapid growth of digital technologies and the exponential increase in the volume of multimedia data — including images, audio, and video — have led to heightened concerns regarding the protection of sensitive information and the confidentiality of communication. In this context, steganography has emerged as a vital field of research, offering the ability to conceal the very existence of a message within innocuous-looking media. Unlike cryptography, which protects the content of a message, steganography focuses on hiding the act of communication itself, making it an essential tool in modern information security. As the digital ecosystem continues to expand, the development of robust and imperceptible steganographic techniques, particularly those based on mathematically sound structures, becomes increasingly important.

The effectiveness of steganographic methods is typically evaluated through several key criteria: perceptual transparency, ensuring that modifications to the cover medium are imperceptible to human senses; robustness against attacks, including signal processing and noise; embedding capacity, indicating the amount of information that can be hidden; resilience to steganalysis, which reflects the ability to withstand statistical or machine learning-based detection; and computational efficiency, which determines the feasibility of real-time or large-scale deployment. Modern steganographic techniques often achieve high performance across these metrics by operating in transform domains, such as the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Singular Value Decomposition (SVD).

*Proceedings of the Workshop on Scientific and Practical Issues of Cybersecurity and Information Technology at the V international scientific and practical conference Information security and information technology (ISecIT 2025), June 09–11, 2025, Lutsk, Ukraine
* Corresponding author.
† These authors contributed equally.
radiosquid@gmail.com (A. Sokolov); denisyevdokymov@gmail.com (D. Yevdokymov); frazenko@gmail.com (O. Fraze-Frazenko)
0000-0003-0283-7229 (A. Sokolov); 0009-0007-5735-1660 (D. Yevdokymov); 0000-0002-2288-8253 (O. Fraze-Frazenko)

Recent advances in image steganography have introduced a variety of techniques aimed at improving payload capacity, imperceptibility, and robustness. Vakani et al. [1] proposed a novel "DCT-in-DCT" scheme that enhances the quality of payload extraction by embedding data within nested DCT domains. Sabeti and Aghabagheri [2] developed an adaptive DCT-based method employing a genetic algorithm to dynamically optimize embedding, achieving a favorable balance between capacity and distortion. Kaur and Singh [3] introduced an n-ary steganographic approach in the DCT domain that leverages chaotic maps to enhance both robustness and visual quality. In another contribution, Sahu and Pradhan [4] integrated AES encryption into a DCT-based framework, increasing security without significantly degrading image fidelity. Liu et al. [5] proposed a method combining wavelet-domain SVD and adaptive QIM for JPEG image steganography, resulting in improved resistance to compression attacks. Similarly, Pramanik [6] utilized integer wavelet transform and genetic algorithms to adaptively control embedding locations, thus enhancing imperceptibility. Ahmad et al. [7] explored a CNN-DCT hybrid model that applies deep learning for steganographic embedding over cloud systems, maintaining high visual fidelity. Ray et al. [8] applied edge detection via deep learning to identify perceptually insensitive embedding regions, improving both security and transparency. Hassaballah et al. [9] addressed steganography in the context of Industrial Internet of Things by proposing a lightweight, secure method suitable for resource-constrained environments. Finally, Meenadshi et al. [10] introduced an AI-enhanced LSB framework that leverages machine learning to optimize concealed data embedding, offering improvements in both embedding efficiency and concealment quality. These developments highlight the ongoing trend toward adaptive, transformation-domain, and AI-driven steganographic solutions tailored for diverse application scenarios.

However, these transformations are computationally intensive, making such methods unsuitable for resource-constrained environments, such as Internet of Things devices, where memory and processing power are severely limited. This limitation motivates the exploration of alternative approaches that combine mathematical rigor with low computational complexity.

A breakthrough in this context has been achieved by code-controlled steganographic methods, which operate directly in the spatial domain of the cover medium while preserving precise control over the desired frequency components [11]. Unlike traditional transform-based techniques, these methods leverage structured code constructions to guide the embedding process in a way that ensures both low computational overhead and predictable spectral characteristics of the resulting steganographic message. By avoiding explicit transformations, code-controlled methods significantly reduce the complexity of embedding and extraction procedures, making them particularly attractive for deployment on lightweight or embedded platforms. Moreover, they open new avenues for achieving fine-grained trade-offs between imperceptibility, robustness, and security.

Existing code-controlled steganographic methods often rely on Walsh functions as codewords, taking advantage of their orthogonality and binary nature to selectively affect specific transform coefficients in the Walsh-Hadamard domain. This selective modulation enables controlled manipulation of particular frequency components within the spatial domain, without performing an explicit transform. However, such approaches typically embed only one bit of information per block, which significantly limits the embedding capacity. In applications where capacity is a critical requirement, such as covert communication or high-volume data hiding, this limitation becomes a significant drawback. To address this, we propose a novel approach based on perfect binary arrays — well-structured algebraic constructions that allow for efficient partitioning of the embedding space. We show that equivalence classes of perfect binary arrays enable the embedding of one bit of information per pixel, drastically increasing capacity while maintaining control over the signal's spectral properties and preserving computational efficiency.

The purpose of this paper is to develop and justify a conceptual framework for a high-capacity, code-controlled steganographic method based on perfect binary arrays.

The proposed approach is designed to operate in the spatial domain while ensuring selective control over frequency characteristics through structured algebraic encoding. By leveraging the

inherent properties of perfect binary arrays, the concept of the steganographic method aims to significantly increase embedding capacity — up to $\log_2(2N^2)$ bit per pixel — without sacrificing the possibility of code control or computational efficiency, where N is the order of the perfect binary array. This work focuses on the theoretical foundations and structural principles of the method, laying the groundwork for future practical implementations and performance evaluation.

2. Theoretical foundations

Let us briefly consider the basic idea of the concept of code-controlled information embedding. Let X to be the matrix of the container block of size $N \times N$. The Walsh-Hadamard transform for X can be calculated according to the following formula

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

where H'_N is the normalized Walsh-Hadamard matrix of order $N = 2^k$, H'_N is determined as $H'_N = (1/N)H_N$, and H_N is constructed following the Sylvester construction

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

On the other hand, the transform vector V of the one-dimensional Walsh-Hadamard transform of a vector Y of length N is determined by the following relation

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

One of the theoretical achievements underlying the concept of code-controlled information embedding is the relationship between the two-dimensional and one-dimensional Walsh-Hadamard transforms [12], which can be written (with an accuracy to the coefficient $1/N$) using the operator $\tilde{A}$, which defines the writing of the matrix A of size $N \times N$ in the form of a row vector of length N^2 by sequential concatenation of the rows of the original matrix A

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

Let d to be the bit of the additional information, which should be embedded in the given image block. In correspondence with this bit, a codeword T of size $N \times N$ is placed, by means of which the bit d is embedded.

Then the block of the steganographic message M, will have the form

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

Let us consider the Walsh-Hadamard transform of a row vector $\tilde{M}$

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

Expression (6) allows us to make a fundamental conclusion about the nature of the perturbation of Walsh-Hadamard transformants in the steganographic message after additive embedding of the

additional information into it. The magnitude and localization of such perturbations will depend on the specific type of term $\tilde{T}H_{N^2}$, which represents the Walsh-Hadamard transformants for the row vector $\tilde{T}$, with the help of which the additional information bit d is encoded.

The $N \times N$ matrix representation of the Walsh functions of length N^2 has been widely employed in code-controlled steganographic schemes as codewords due to their ability to influence specific frequency components in the Walsh-Hadamard transform domain. When used in the spatial domain, these functions enable selective spectral shaping of the modified image blocks, allowing the embedding process to target certain frequency bands. This property is particularly useful for maintaining resisting attacks against the embedded message.

For example, let us consider the codeword $T_{8,(5,1)}$ targeting (5,1) Walsh-Hadamard transformant and its Walsh-Hadamard transform (assuming 1-based indexing)

$$T_{8,(5,1)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \end{bmatrix}, W_{T_{8,(5,1)}} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 64 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \quad (7)$$

However, due to their rigid structure and block-wise application, Walsh-based embedding schemes typically offer limited capacity, motivating the search for more flexible algebraic frameworks such as perfect binary arrays.

Definition 1 [13]. A perfect binary array is a two-dimensional sequence (matrix)

$$H(N) = \left\| h_{i,j} \right\|, \quad i, j = 0,1,\ldots,N-1, \quad h_{i,j} \in \{-1,1\}, \quad (8)$$

having an ideal two-dimensional periodic autocorrelation function (2DPACF), whose elements

$$R(m,n) = PACF(m,n) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} h_{i,j} h_{i+m,j+n} = \begin{cases} N^2, \ for \ \ m = n = 0; \\ 0, \text{for any other } m \text{ and } n, \end{cases} \quad (9)$$

where $m, n = 0,1,\ldots,N-1$, and all indices of elements $h_{i+m,j+\tau}$ are reduced modulo N.

Let us give as an example a perfect binary array of order $N = 8$ as well as its two-dimensional periodic autocorrelation function

$$A=\begin{bmatrix} 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 \end{bmatrix},\ R=\begin{bmatrix} 64 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \quad (10)$$

Statement 1 [14]. Each perfect binary array of order N generates an E(N)-class of equivalent matrices — perfect binary arrays by operations of cyclic shift on rows and columns and inversion, while the cardinality of the class of equivalent matrices is

$$J_{E(N)}=2N^2. \quad (11)$$

From the research [14], the following is known. If an arbitrary generating perfect binary array $A_0(N)$ of order N is given, then all its cyclic shifts are defined as $L_{k_1}AQ_{k_2}$, $k_1,k_2=0,1,...,N-1$ and let the two-dimensional periodic cross-correlation function (2DPCCF) between $A_0(N)$ and its cyclically shifted array be defined by the relation

$$B(m,n)=A_0(N)**L_{k_1}A_0(N)Q_{k_2}=\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}h_{i,j}h_{i+m,j+\tau}, \quad (12)$$

where the symbol ** denotes a two-dimensional correlation (convolution); $m,n=0,1,...,N-1$.

The following statement is known:

Statement 2 [14]. The 2DPCCF $B(m,n)$ of an array $A_0(N)$ and array $L_{k_1}A_0(N)Q_{k_2}$ of order N, $k_1,k_2=0,1,...,N-1$, is a 2DPACF $\|R(m,n)\|$ of an array $A_0(N)$ shifted by k_1 rows and k_2 columns, i.e.

$$B(m,n)=R(m+k_1,n+k_2),\quad m,n=0,1,...,N-1. \quad (13)$$

The core of the proposed steganographic method is based on an information modulation principle that exploits a key property of perfect binary arrays: the 2DPCCF between a perfect binary array and its cyclically shifted version (in rows or columns) is structurally equivalent to the corresponding cyclic shift of the 2DPACF of the original array. This algebraic symmetry enables precise and predictable manipulation of correlation peaks. We propose to encode information by selecting one of $2N^2$ possible states, through controlled cyclic shifts (either along rows or columns) combined with optional binary inversion. The embedding process thus corresponds to a particular transformation of the array structure within an image block. During extraction, the method relies on non-blind decoding, typical for code-controlled schemes: the cover component is reconstructed, the 2DPCCF is computed, and the position of its global maximum uniquely determines the embedded message bit pattern.

3. The concept of the steganographic method based on the perfect binary arrays

This section introduces the conceptual foundation of a steganographic method that leverages the

structural properties of perfect binary arrays. Unlike conventional transform-based approaches, the proposed method operates entirely within the spatial domain, using perfect binary arrays as code carriers to embed information through carefully controlled spatial transformations. The key idea is to exploit the unique autocorrelation and cross-correlation characteristics of perfect binary arrays, particularly their behavior under cyclic shifts and inversion. These algebraic symmetries enable reliable and high-capacity data encoding while maintaining low computational complexity and compatibility with resource-constrained environments. We describe the encoding and decoding procedures, and the modulation scheme used to map information onto structured transformations of perfect binary arrays.

The main steps of the proposed steganographic method based on [11] are as follows.

Additional information embedding.

Step 1. Perform a standard partition of the source container image into non-overlapping blocks of size $N \times N$.

Step 2. Choose a reference perfect binary array $A_0(N)$ of size N.

Step 3. Let X be the next container block involved in the steganographic transformation. Choose a vector $D = \{d_1\ d_2\ \dots\ d_{\log_2(2N^2)}\}$ that contains the next $\log_2(2N^2)$ bits of information to be embedded in this container block.

Step 4. Define the bit d_1 value as the encoding sign of the perfect binary array, the decimal equivalents of the bits $k_1 = \{d_2\ d_3\ \dots\ d_{\log_2(N)+1}\}_{10}$ as the value of the row shift, and the bits $k_2 = \{d_{\log_2(N)+2}\ d_{\log_2(N)+3}\ \dots\ d_{\log_2(2N^2)}\}_{10}$ as the column shift.

Step 5. Construct an array $L_{k_1} A_0(N) Q_{k_2}$ of the $E(N)$-class for embedding additional information and perform embedding, then the next block of the steganographic message will be defined as

$$M = X + L_{k_1} A_0(N) Q_{k_2}. \tag{14}$$

Note that when embedding the value +1 into the container pixel value 255, as well as when embedding the value -1 into the container pixel value 0, the embedding operation for these pixels is not performed.

Additional information extraction.

Step 1. Perform a standard partition of the steganographic message into non-overlapping blocks of size $N \times N$.

Step 2. Let $\overline{M}$ to be the next block of the possibly perturbed steganographic message, involved in the steganographic transformation, corresponding to the block *X* of the container.

2.1. Construct a matrix $\Delta = \overline{M} - X$ with elements $\Delta(i,j)$, $i,j = 0,1,\dots,\mu-1$ for which to construct the 2DPCCF matrix

$$B(m,n) = A_0(N) **\Delta. \tag{15}$$

2.2. Find the row x and column y indices of the maximum (absolute value) of the matrix $B(m,n)$.

2.3. Restore the $\log_2(2N^2)$ embedded information bits as

$$\begin{cases} d_1 = sign(B(x,y)) - 1 (\mathrm{mod}\, 3); \\ \{d_2 \;\; d_3 \;\; \ldots \;\; d_{\log_2(N)+1}\}_{10} = x; \\ \{d_{\log_2(N)+2} \;\; d_{\log_2(N)+3} \;\; \ldots \;\; d_{\log_2(2N^2)}\}_{10} = y. \end{cases} \quad (16)$$

4. Experimental data

This section presents the experimental evaluation of the proposed steganographic method based on perfect binary arrays. The method's performance is assessed according to key steganographic metrics, including embedding capacity, perceptual transparency, and robustness against message-targeted attacks.

To evaluate the efficiency of the proposed method in terms of data payload, we compare its embedding capacity with that of the classical code-controlled steganographic approach based on Walsh-Hadamard functions. The comparison is performed for various block sizes $N \times N$, which determine the granularity of embedding. While the classical method typically encodes a single bit per block regardless of size, the proposed scheme leverages the structural properties of perfect binary arrays to encode up to $\log_2(2N^2)$ bits per block. Table 1 summarizes the resulting capacities in terms of bits per block and bits per pixel.

Table 1
Throughput for steganographic methods

Block size N	Classical code-controlled method		Proposed code-controlled method	
	Bit per block	Bit per pixel	Bit per block	Bit per pixel
4	1	0,0625	5	0,3125
8	1	0,0156	7	0,1093
16	1	0,0039	9	0,0351

The data presented in Table 1 demonstrates the significant advantage of the proposed method over the classical code-controlled approach in terms of embedding capacity. While the classical method consistently embeds only 1 bit per block regardless of block size, the proposed method exploits the combinatorial richness of perfect binary arrays to achieve a markedly higher payload. Notably, for small block sizes (e.g., $N = 4$), the proposed method achieves a fivefold increase in throughput per pixel. Even for larger blocks, where embedding density typically declines, the method maintains a considerable advantage in both bits per block and bits per pixel. This highlights the method's potential for applications requiring high-capacity embedding, particularly when maintaining visual quality is essential.

Assessing perceptual fidelity is a complex task due to the subjective nature of human visual perception. The human visual system exhibits varying sensitivity to spatial, frequency, and color distortions, making formal evaluation inherently limited. Nevertheless, in the proposed method, the modification of container elements is strictly bounded: changes do not exceed ± 1 in magnitude. This constraint ensures a minimal distortion footprint, which is expected to be imperceptible under normal viewing conditions. To support this claim, we provide a quantitative analysis using the peak signal-to-noise ratio (PSNR) metric for different embedding densities, reflecting the proportion of modified blocks in the image.

The PSNR is evaluated as

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{255^2}{\mathrm{MSE}}\right), \tag{17}$$

where MSE is the root mean square error between the original and modified image. If $p\%$ pixels are changed by ±1, then

$$MSE = p\frac{1^2}{100} = \frac{p}{100}. \tag{18}$$

In Table 2 we present the values of PSNR for different embedding rates

Table 2
PSNR values for different embedding rates

Embedding Rate (%)	MSE	PSNR (dB)
25%	0.25	54.15
50%	0.50	51.14
75%	0.75	49.38
100%	1.00	48.13

The results presented in Table 2 confirm that the proposed method preserves excellent perceptual fidelity across different embedding rates. Even at 100% embedding, where each block contributes to data hiding, the PSNR remains above 48 dB — well within the range considered visually imperceptible. This robustness stems from the method's foundational design, inherited from the code-controlled paradigm, where modifications are limited to ±1 per pixel. By carefully constraining the amplitude of changes, the proposed approach ensures that the embedded information does not introduce noticeable visual artifacts, thus maintaining the visual integrity of the cover image.

The experiments were performed on standard 500 test images subjected to JPEG compression to simulate realistic transmission conditions. We show in Table 3 the obtained dependency of the decoding error rate on the compression rate QF.

Table 3
The dependency of the decoding error rate on the QF in conditions of JPEG compression attack

QF	100	90	80	70	60
Error rate, %	0.02	26.53	42.88	46.41	47.77
QF	50	40	30	20	10
Error rate, %	48.40	48.88	49.23	49.53	49.82

The experimental results demonstrate that even with a relatively small block size of 8×8 and embedding of 7 bits per block, representing a sevenfold increase in payload compared to classical code-controlled methods, the proposed technique maintains acceptable performance under low levels of JPEG compression, which is an impressive outcome given the aggressive payload and lossy compression. These results raise an important and underexplored question in steganographic design: Is it more effective to use small blocks with limited payload to ensure robustness, or to utilize larger blocks that accommodate more data per unit but may exhibit different distortion-resilience properties? As Shannon observed in his foundational work [15], larger codes often yield better efficiency and robustness. Extrapolating this principle, larger block sizes may potentially provide enhanced resistance not only to compression artifacts but also to steganalytic attacks, due to increased structural complexity and embedding variability. This hypothesis suggests that the traditional preference for small embedding units in spatial and transform-domain steganography might need to be re-evaluated. Consequently, this opens a compelling direction for rethinking the very foundation of steganographic design, possibly leading to the emergence of new principles and embedding architectures grounded in large-block algebraic frameworks.

5. Conclusion

This paper introduced a novel steganographic method based on perfect binary arrays, offering a fresh algebraic perspective on payload encoding within digital images. The proposed technique significantly increases embedding capacity by exploiting the unique autocorrelation and cross-correlation properties of perfect binary arrays and their cyclic shifts, enabling the modulation of up to $2N^2$ distinct states within a block of size $N \times N$. Compared to classical code-controlled approaches that typically embed only one bit per block, our method demonstrates up to sevenfold improvements in throughput without compromising perceptual quality.

Experimental results confirm that the modifications introduced to the spatial domain are minimal, with pixel-level changes constrained within ±1, yielding high PSNR values and excellent visual imperceptibility. Moreover, the method retains robustness under moderate compression, suggesting suitability for real-world applications, including constrained environments such as IoT platforms. The analysis also raises essential theoretical considerations: while smaller blocks have traditionally dominated steganographic designs, larger blocks, as advocated by Shannon for coding, may offer increased resistance to compression and steganalysis, pointing toward the need for reevaluating current paradigms.

Overall, the proposed concept not only advances the practical utility of spatial-domain steganography but also opens new avenues for integrating algebraic structures into the core of information-hiding systems.

Declaration on Generative AI

The authors used Grammarly for grammar and spelling checks and GPT-4 for paraphrasing and rewording several sentences. All scientific ideas, analyses, conclusions, and interpretations are solely the authors' own, and no generative AI tools were used to develop or formulate the scientific content of the manuscript.

References

[1] H. Vakani et al. "Dct-in-dct: A novel steganography scheme for enhanced payload extraction quality" IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (2021): 201-206. doi: 10.1109/iaict52856.2021.9532553

[2] V. Sabeti , A. Aghabagheri, Developing an adaptive DCT-based steganography method using a genetic algorithm, Multimedia Tools and Applications 82,13 (2023) 19323-19346. doi: 10.1007/s11042-022-14166-3

[3] R. Kaur, B. Singh, A robust and imperceptible n-Ary based image steganography in DCT domain for secure communication, Multimedia Tools and Applications 83,7 (2024) 20357-20386. doi: 10.1007/s11042-023-16330-9

[4] A. Sahu, C. Pradhan "A novel image steganography technique using AES encryption in DCT domain" International Conference on Distributed Computing and Intelligent Technology, Cham, Springer Nature Switzerland (2023): 349-354. doi: 10.1007/978-3-031-24848-1_26

[5] J. Liu et al. "Robust JPEG Image Steganography Using Wavelet Domain SVD and Adaptive QIM" International Conference on Signal and Image Processing (2023): 434-438. doi: 10.1109/icsip57908.2023.10270839

[6] S. Pramanik, An adaptive image steganography approach depending on integer wavelet transform and genetic algorithm, Multimedia Tools and Applications 82,22 (2023) 34287-34319. doi: 10.1007/s11042-023-14505-y

[7] S. Ahmad et al., Enhanced CNN-DCT Steganography: Deep Learning-Based Image Steganography Over Cloud, SN Computer Science 5,4 (2024) 408. doi: 10.1007/s42979-024-02756-x

[8] B. Ray et al., Image steganography using deep learning based edge detection, Multimedia Tools and Applications 80,24 (2021) 33475-33503. doi: 10.1007/s11042-021-11177-4

[9] M. Hassaballah et al., A novel image steganography method for industrial internet of things security, IEEE Transactions on Industrial Informatics 17,11 (2021) 7743-7751. doi: 10.1109/tii.2021.3053595

[10] M. Meenadshi et al. "AI-Enhanced LSB Steganography Interface: Concealed Data Embedding Framework" International Conference on Smart Structures and Systems (2023): 1-4. doi: 10.1109/icsss58085.2023.10407062

[11] A.A. Kobozeva, A.V. Sokolov, Robust Steganographic Method with Code-Controlled Information Embedding, Problemele energeticii regionale 4,52 (2021) 115-130. doi: 10.52254/1857-0070.2021.4-52.11

[12] A.A. Kobozeva, A.V. Sokolov, The Sufficient Condition for Ensuring the Reliability of Perception of the Steganographic Message in the Walsh-Hadamard Transform Domain, Problemele Energeticii Regionale 54,2 (2022) 84-100. doi: 10.52254/1857-0070.2022.2-54.08

[13] M.I. Mazurkov, V.Y. Chechelnytskyi, P. Murr, Information security method based on perfect binary arrays, Radioelectronics and Communications Systems 51,11 612-614. doi:10.3103/s0735272708110095

[14] M.I. Mazurkov, Broadband radio communication systems, Science and Technology, 2010.

[15] C.E. Shannon, A mathematical theory of com-munication, The Bell system technical journal 27,3 (1948) 379-423.