symmetry

MDPI

Article

Adaptive Code-Controlled Steganography with Enhanced Robustness to JPEG Compression

Nadiia Kazakova [1,*], Ruslan Shevchuk [2,3,*], Artem Sokolov [4], Denys Yevdokymov [4], Katarzyna Marczak [5] and Balzhan Smailova [6]

[1] Department of Information Technology, Odesa I.I. Mechnikov National University, V. Zmiienka Str., 2, 65082 Odesa, Ukraine
[2] Department of Computer Science and Automatics, University of Bielsko-Biala, Willowa Str., 2, 43-309 Bielsko-Biala, Poland
[3] Department of Computer Science, West Ukrainian National University, Lvivska Str., 11, 46009 Ternopil, Ukraine
[4] Department of Cybersecurity, National University "Odesa Law Academy", Fontans'ka doroga Str., 23, 65000 Odesa, Ukraine; radiosquid@gmail.com (A.S.); denisyevdokymov@gmail.com (D.Y.)
[5] Department of Software Engineering, Institute of Security and Computer Science, University of the National Education Commission, Podchorążych Str., 2, 30-084 Krakow, Poland; katarzyna.marczak@uken.krakow.pl
[6] Department of Mathematics, Shakarim University, 071412 Semey, Kazakhstan; b.smailova@shakarim.kz
* Correspondence: kaz2003@ukr.net (N.K.); rshevchuk@ubb.edu.pl (R.S.)

Abstract

This paper addresses the problem of improving the robustness of image steganographic methods under lossy compression while preserving high perceptual quality and low computational complexity. The paper proposes an adaptive code-controlled steganographic method that enables spectrally selective embedding in the spatial domain through structured codewords. The proposed approach introduces block-level adaptivity in which the energy of the embedding codeword is dynamically selected according to the robustness characteristics of each image block. Instead of applying uniform embedding strength, the method determines the minimal codeword energy required to guarantee reliable message extraction under a predefined worst-case JPEG compression level. Experimental evaluation demonstrates that the proposed adaptive strategy significantly improves robustness to compression attacks while preserving high perceptual reliability and strong resistance to statistical steganalysis techniques. In particular, for JPEG quality factor (QF) = 50, the bit error rate is reduced to 1.25% while a high perceptual quality of 52.07 dB peak signal-to-noise ratio (PSNR) is achieved. For stronger attack conditions, QF = 20, the method achieves 6.6% bit errors with a PSNR of 47.7 dB. Overall, the proposed adaptive energy selection provides up to 22.68% fewer errors or up to 6.05 dB higher PSNR compared to the classical code-controlled steganographic method, confirming its effectiveness for practical steganographic applications.

Keywords: steganography; code-based control; adaptive embedding; robustness; codewords; spatial domain; discrete cosine transform; Walsh–Hadamard transform; JPEG compression

Check for updates

Academic Editors: Shuang Xu and Sergei Odintsov

Received: 15 March 2026
Revised: 29 March 2026
Accepted: 7 April 2026
Published: 9 April 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

The rapid expansion of digital multimedia content has made the secure and covert transmission of information increasingly critical. Every day, vast amounts of images, audio, and video data are generated and shared across networks worldwide. In this environment,

steganography, the art and science of hiding information within multimedia containers, plays a crucial role in protecting sensitive information while maintaining the usability and appearance of the original data. As the volume and diversity of multimedia content continue to grow, so does the importance of effective steganographic methods.

Today, a wide range of steganographic methods has been developed, and the field continues to advance at a rapid pace [1]. These techniques are traditionally evaluated based on several fundamental criteria. Among the most important are resistance to steganalysis, which ensures that the presence of hidden information remains undetectable; robustness against attacks that aim to corrupt or remove the embedded message; high embedding capacity, which determines the amount of information that can be concealed; and the ability to preserve perceptual reliability, ensuring that the original multimedia content remains visually or acoustically indistinguishable from its modified version [2].

In recent years, computational efficiency has emerged as an increasingly critical evaluation metric. With the proliferation of resource-constrained devices, including mobile phones, Internet of Things nodes, drones, and other embedded systems, steganographic algorithms must not only be secure and robust but also capable of operating in real time under limited processing power and memory. This growing demand for fast, lightweight, yet effective methods has driven researchers to explore novel approaches that balance the classical objectives of secrecy, robustness, and capacity with the practical constraints of modern computing environments.

To date, a wide variety of steganographic methods have been proposed, reflecting the increasing demand for secure and covert communication [1–3]. Broadly speaking, two main paradigms dominate the field. The first approach involves embedding information in transform domains, such as the discrete cosine transform (DCT) [4–9], wavelet-based transforms [10–12], singular value decomposition (SVD) [13–19], and Arnold transform [20,21] applied to blocks of the multimedia container. Embedding in these domains effectively exploits the energy compaction properties of the transform, allowing modifications to be concentrated in components that are less sensitive to attacks against the embedded message, while maintaining high reliability of perception. This ensures that the hidden information remains largely intact even when the container undergoes compression, filtering, or other common signal processing operations. From a physical and signal-theoretic perspective, transform-domain methods operate by modulating coefficients that represent global or semi-global patterns in the container, thereby embedding information in the structure of the signal rather than in individual samples. However, such manipulations often require intensive matrix operations, iterative optimization, or block-wise decompositions, which result in high computational complexity, limiting their applicability in real-time scenarios or on resource-constrained devices.

The second paradigm relies on embedding information in the spatial domain [22–25], directly modifying the values of individual pixels or blocks. From a physical standpoint, this approach interacts with the local signal characteristics at the finest granularity, producing immediate and localized modifications. The primary advantage is low computational overhead, as no complex transformations or decompositions are required. However, because the embedding is highly localized and does not exploit the structural redundancy of the container, these methods are intrinsically more vulnerable to common operations such as compression, filtering, or noise, leading to lower robustness of the hidden information. In essence, spatial-domain methods trade off robustness for efficiency, operating directly on the observable signal without leveraging its underlying transform structure.

In recent years, artificial intelligence-based steganographic methods, particularly those leveraging deep learning and generative adversarial networks, have emerged as a

promising direction [26,27], enabling adaptive and data-driven embedding strategies that significantly improve imperceptibility and resistance to modern steganalysis techniques.

Recently, a steganographic method using code-based control has been developed [28–30], successfully combining the advantages of both transform-domain and spatial-domain approaches. Operating primarily in the spatial domain, this method allows for targeted influence on specific frequency components of the container, effectively embedding information while preserving desired properties of the steganographic message. The method achieves high robustness to attacks on the embedded message, comparable to or even better than transform-domain techniques, while maintaining the computational efficiency characteristic of spatial-domain approaches. This paradigm demonstrates that it is possible to control the spectral characteristics of the embedding process by leveraging the structural and spectral properties of the codewords used to modulate the embedded information bits. As a result, code-based control provides a flexible and adaptive framework, capable of optimizing the trade-offs between imperceptibility, robustness, and efficiency in modern multimedia steganography.

The experimental results obtained for the code-based steganographic method are highly encouraging. Even when using relatively small blocks of size 8×8, corresponding to an embedding capacity of $\frac{1}{64}$ bits per pixel, the method achieves an extraction error rate of merely 3.11% under QF = 50 JPEG compression attack, while maintaining high visual reliability with a peak signal-to-noise ratio (PSNR) of 48.13 dB. These results confirm the effectiveness of code-based control in achieving a favorable balance between reliability of perception and robustness, even under constrained embedding conditions.

Nevertheless, many practical applications require higher robustness, especially under stronger attacks or more aggressive signal processing operations. This underscores the need for further improvement of the code-based steganographic method. In particular, introducing adaptivity into the embedding process by dynamically adjusting the strategy to local container properties is a promising direction for enhancing robustness and overall performance.

From a practical perspective, an adaptive code-based steganographic method opens significant opportunities for real-world deployment. The ability to dynamically adjust the embedding process according to local characteristics of the container enables the method to operate effectively under diverse and unpredictable conditions, such as varying compression levels, transmission noise, and post-processing operations. This makes the approach particularly suitable for modern communication scenarios where multimedia data are frequently modified, resized, or recompressed during distribution.

Moreover, the combination of high reliability of perception, enhanced robustness, and low computational complexity positions the proposed adaptive method as a promising solution for resource-constrained and real-time systems, including mobile devices, Internet of Things (IoT) platforms, unmanned aerial vehicles (drones), and edge-computing environments. In such systems, the capability to reliably embed and extract information without significant computational overhead is critical. Consequently, further development of adaptive code-based steganographic techniques is not only of theoretical interest but also of substantial practical relevance for secure communication, digital rights management, and covert data exchange in contemporary multimedia systems.

The objective of this paper is to develop and research an adaptive code-based steganographic method that enhances the robustness of embedded information while preserving high perceptual reliability and computational efficiency.

The proposed approach aims to exploit local structural properties of the multimedia container by identifying blocks with different levels of resilience and adjusting the embedding strength accordingly. By introducing adaptivity into the code-based control

framework, the method seeks to improve resistance to attacks on the embedded message without sacrificing real-time performance or embedding capacity.

To provide the necessary background for the proposed approach, we briefly outline the fundamental principles of steganography and review recent research on steganographic methods that have significantly influenced the development of modern information hiding techniques.

Steganography is a branch of information security that focuses on the covert embedding of information within digital media in such a way that the very presence of the hidden message remains imperceptible. Unlike cryptography, which aims to protect the content of a message by transforming it into an unreadable form, steganography seeks to conceal the existence of communication itself. As a result, steganographic techniques are increasingly regarded as a complementary component of modern information protection systems, particularly in scenarios where confidentiality, deniability, and robustness are required.

To provide a unified view of the steganographic process, a generalized scheme of a steganographic system is introduced. This scheme, illustrated in Figure 1, outlines the principal components and interactions involved in the embedding and extraction of hidden information. It highlights the roles of the cover container, the secret message, the embedding mechanism, and the extraction process, forming a conceptual framework for analyzing and comparing different steganographic approaches.

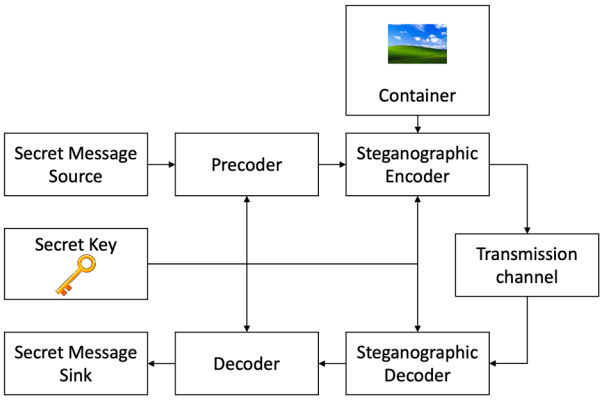


Figure 1. The generalized scheme of a steganographic system.

The system illustrated in Figure 1 operates on a secret message and a digital container under the control of a secret key, forming a closed embedding-decoding loop between the sender and the receiver.

At the transmitter side, the process begins with a secret message source, which generates the information to be concealed. Before embedding, the message is processed by a precoder, whose role is to adapt the message to the properties of the steganographic encoder and the container. The precoding stage may include operations such as encryption, compression, error-correcting coding, or code-based transformations aimed at increasing security, robustness, or embedding efficiency. The precoder is typically controlled by a secret key, ensuring that the resulting representation of the message cannot be reconstructed without key knowledge.

The steganographic encoder embeds the precoded message into the selected container, which may be an image, audio signal, video sequence, or other digital medium. The embedding procedure modifies the container in a manner that preserves the reliability of perception while maintaining the ability to reliably extract the hidden data. The encoder may also utilize the secret key to determine embedding positions, modulation rules, or adaptive strategies, thereby increasing resistance to steganalysis.

After embedding, the stego-container is transmitted through a communication channel, which may introduce distortions due to noise, compression, or intentional attacks. These channel effects must be considered during system design, as they directly influence the robustness and reliability of the hidden communication.

At the receiver side, the steganographic decoder processes the received stego-container to extract the embedded signal. Using the corresponding secret key, the steganographic decoder identifies the embedding structure and retrieves the precoded message representation. The extracted data is then passed to the decoder, which performs the corresponding inverse operations of the precoding stage, such as decryption and error correction, thereby reconstructing the original secret message and delivering it to the secret message sink.

In contemporary digital environments, steganographic methods are widely applied in secure communications, copyright protection, digital watermarking, and covert data exchange. The rapid growth of multimedia content and the widespread use of open communication networks have further reinforced the relevance of steganography as a practical tool for information security. Consequently, the development of effective steganographic techniques has become an active research area, integrating concepts from signal processing, coding theory, and statistical analysis.

We present in Figure 2 the classification of the modern steganographic methods.

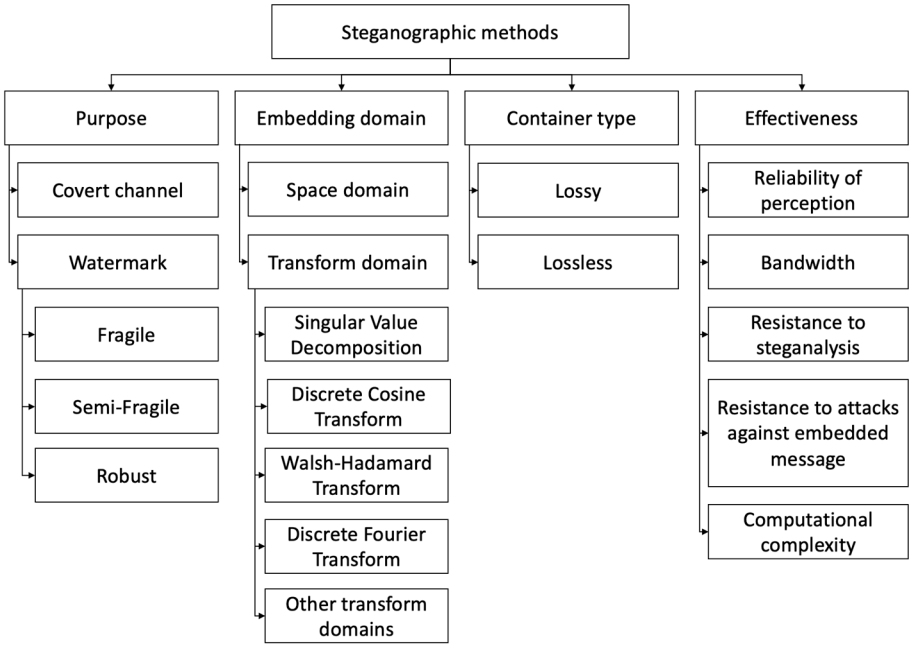


Figure 2. The classification of the modern steganographic methods.

Accordingly, to the information presented in Figure 2, the steganographic methods can be systematically classified according to several complementary criteria that reflect their purpose, embedding strategy, container characteristics, and overall effectiveness. Such a multidimensional classification provides a structured view of the field and helps to analyze trade-offs between imperceptibility, robustness, capacity, and computational cost.

From the perspective of purpose, steganographic methods are commonly divided into covert communication systems and digital watermarking techniques. Covert communication aims to conceal the very existence of a hidden message, ensuring that the presence of embedded data remains undetectable to unintended observers. In contrast, watermarking methods are typically designed to protect intellectual property or verify authenticity. Depending on their sensitivity to modifications, watermarking techniques can further be classified as fragile, semi-fragile, or robust. Fragile watermarks are destroyed

by any modification and are mainly used for integrity verification, while semi-fragile and robust watermarks tolerate certain transformations and are applied in copyright protection and content authentication.

Another important classification criterion is the embedding domain. Steganographic methods operating in the spatial (or time) domain directly modify the container samples, for example, pixel intensities in images or amplitude values in audio signals. These methods are usually simple and computationally efficient, but often less resistant to attacks. Transform-domain methods embed information into transformed representations of the container, such as those obtained using the Discrete Cosine Transform, Discrete Fourier Transform, Walsh–Hadamard Transform, or Singular Value Decomposition. Embedding in transform domains generally provides improved robustness and better control over perceptual reliability, as modifications can be aligned with the intrinsic properties of human perception. Other transform domains and hybrid approaches further expand the design space of modern steganographic systems.

Steganographic techniques can also be categorized by container type, distinguishing between lossy and lossless media. Lossy containers, such as JPEG images or compressed audio, introduce irreversible distortions during compression, which impose strict requirements on the robustness of embedded data. Lossless containers, on the other hand, preserve the original information exactly, allowing for reversible or distortion-free steganographic schemes. The choice of container type strongly influences both embedding strategies and achievable performance metrics.

Finally, the effectiveness of steganographic methods [3] is evaluated using several key criteria. These include the reliability of perception, embedding capacity, resistance to steganalysis, resistance to intentional or unintentional attacks on the embedded message, and computational complexity. In practice, improving one criterion often degrades another, making steganography a field of inherent trade-offs. A comprehensive classification based on these effectiveness measures enables objective comparison of methods and highlights directions for developing more secure and efficient steganographic techniques.

The field of steganography has gained significant attention in recent years due to the growing demand for secure and imperceptible data embedding techniques. The increasing prevalence of digital media and the corresponding need to protect sensitive information have made the development of robust steganographic methods a critical area of research. Consequently, a considerable body of work has been dedicated to advancing both theoretical foundations and practical implementations, reflecting the importance and timeliness of this topic in the broader context of information security.

Recent advances in DCT-based steganographic methods have focused on improving robustness against lossy compression and enhancing imperceptibility by exploiting the frequency domain structure of images. One notable contribution by Venugopala et al. in [4] proposes an integrated approach combining least significant bit (LSB) and DCT steganography for secure medical data communication, where the DCT embedding improves robustness and imperceptibility compared to pure spatial techniques, and evaluated performance using PSNR, structural similarity index measure (SSIM), and mean squared error (MSE) metrics to demonstrate its effectiveness in practical scenarios involving medical images and varying compression conditions.

In ref. [5], Al Ali et al. introduce a DCT-based steganography algorithm designed specifically to resist JPEG quantization by adaptively selecting embedding locations based on image texture, achieving high message extraction accuracy even after compression and demonstrating significant improvements in robustness and undetectability compared to traditional LSB methods. Other research [6] explores coverless and robust DCT-related schemes, such as robust coverless steganography algorithms that utilize DCT with topic

classification or domain adaptation to resist steganalysis and maintain embedding security without modifying the carrier image directly. Further, work [7] by Lan and collaborators has shifted toward integrating DCT domain embedding with deep learning, for example using invertible neural networks to embed messages directly in DCT coefficients, significantly improving robustness to JPEG compression across a range of quality factors with very low error rates, highlighting a trend toward hybrid signal-processing and learning-based approaches for robust frequency-domain steganography.

Two well-established steganographic frameworks [8,9] based on DCT coefficient manipulation have demonstrated exceptionally strong robustness and practical effectiveness, making them important benchmarks when comparing against DCT-based schemes.

Wang, Zheng, and Xu in ref. [8] introduced a compression-resistant steganography method based on Differential Manchester coding that explicitly targets the challenges of JPEG compression encountered in real communication channels such as social networks. The core idea is to exploit the invariance of the sign of selected DCT coefficients before and after compression, using a weighted cost function to choose robust embedding positions and Differential Manchester coding to encode location features. This design significantly enhances the ability to correctly extract hidden messages after repeated or forced JPEG compression attacks, outperforming many conventional robust methods in both undetectability and robustness on platforms like Facebook and Twitter.

Earlier, Zhu, Zheng, Qiao, and Xu in ref. [9] proposed a robust steganography algorithm that embeds data by modifying the sign of DCT coefficients, combined with an optimized distortion function and error-correcting codes (e.g., Syndrome-Trellis Codes). By selecting coefficients whose sign remains unchanged after JPEG compression as embedding candidates, this approach preserves message integrity under lossy compression while minimizing visual distortion and embedding cost. Extensive experiments show that this method achieves a favorable balance between undetectability and robustness compared to traditional adaptive steganography schemes that are vulnerable to compression attacks.

Wavelet-based steganographic methods have attracted significant attention due to their ability to provide multi-resolution analysis and effective localization of both spatial and frequency characteristics of the signal. In ref. [10], Durafe et al. propose a hybrid steganographic approach combining integer wavelet transform (IWT) and discrete wavelet transform (DWT) with singular value decomposition (SVD) and fractal-based cover modeling. The method demonstrates improved robustness and imperceptibility by exploiting both multi-resolution decomposition and structural redundancy of fractal representations.

In ref. [11], Pramanik et al. introduced an adaptive steganographic scheme based on integer wavelet transform and a genetic algorithm, where optimal embedding parameters are selected through evolutionary optimization. This approach enhances imperceptibility and embedding capacity while maintaining resistance to common signal processing attacks. In ref. [12], a reversible hybrid steganographic framework combining the Radon transform and integer lifting wavelet transform is presented by El-den and collaborators. The method achieves high robustness and reversibility by integrating complementary transform-domain properties, enabling accurate recovery of both the embedded data and the original cover image.

Recent advances in steganography have increasingly leveraged SVD to enhance both imperceptibility and robustness.

For image steganography, Liu et al. in ref. [13] combined wavelet-domain SVD with adaptive quantization index modulation (QIM) to achieve high resistance to JPEG compression while preserving image quality. Expanding on the use of wavelets, Khandelwal and Sharma in ref. [14] applied dual-tree complex wavelet transforms (DTCWT) with SVD and convolutional neural network (CNN)-based subspace selection, exploiting directional

selectivity and shift invariance to further enhance robustness against geometric and signal distortion attacks.

Recent hybrid approaches, such as those by Teoh et al. in ref. [15] and Kumari et al. in ref. [16], emphasize optimization and multi-component embedding. Teoh et al. employed in ref. [15] both U and V orthogonal vectors in SVD for improved imperceptibility and resilience, while Kumari et al. in ref. [16] combined DWT-SVD with tunicate swarm optimization, allowing adaptive selection of embedding locations and parameters, yielding better PSNR and SSIM performance.

In ref. [17] Chanu, Singh, and Tuithung proposed a robust SVD-based steganographic method that divides the cover image into equal-sized blocks and embeds secret messages into the singular values of each block. Unlike some earlier schemes, this method carefully handles singular values to avoid introducing negative values, and experimental results demonstrate resilience against various attacks while preserving good reliability perception. This thorough block-based approach and its evaluation against attacks establish it as a strong baseline in SVD-based image steganography research.

Chang, Lin, and Hu in ref. [18] developed an SVD-oriented watermark embedding scheme notable for its high restoration quality and resistance to distortions. Their approach modifies the singular matrices in a way that allows hidden watermarks to be extracted and images to be restored with minimal degradation after ownership verification, illustrating both high reliability perception and practical usability. Over the years, this scheme has been referenced and extended in numerous works, underlining its influence and well-validated performance in the literature.

Melnik, in an earlier foundational contribution [19], proposed a compression-resistant steganographic algorithm leveraging SVD properties to ensure that the embedded data survives lossy operations and common preprocessing. This algorithm is widely cited in steganography literature as an early demonstration of exploiting SVD for robustness against compression and noise, reinforcing the importance of singular value manipulation in resilient information hiding.

Taken together, SVD-based methods [13–19] form a well-researched and robust comparative baseline. They are repeatedly analyzed in follow-on research for their ability to maintain high image quality, resist attacks, and preserve hidden payloads under diverse conditions.

Steganographic methods based on the Arnold transform have gained attention due to their ability to effectively permute pixel positions, thereby enhancing security through controlled spatial scrambling of the container while preserving its statistical properties. Pattanayak, Solanki, and colleagues in ref. [20] introduced an image steganography approach using the Arnold Transform, a chaotic pixel rearrangement that scrambles the secret or cover image before embedding. Although details in the chapter are limited, the Arnold Transform is typically used to randomize spatial relationships, enhancing resistance to statistical detection when combined with subsequent transform embedding. Similarly, Nipanikar et al. in ref. [21] combined an Arnold chaotic map with an optimized Curvelet Transform for color image steganography, leveraging the multi-scale, directional properties of curvelets to embed data in coefficients that are both imperceptible and robust to common image processing operations.

Overall, transform-domain steganography represents a powerful and well-established class of information hiding techniques. By exploiting frequency, scale, directional, or algebraic properties of transforms such as DCT, wavelet, SVD, Radon, and curvelet, these methods are capable of achieving high robustness against attacks on the embedded message, including compression, noise, filtering, and geometric distortions. This makes transform-

based steganography particularly suitable for secure communication in real-world transmission channels.

However, these advantages come at the cost of several inherent limitations. Transform-based schemes typically involve high computational complexity, multiple decomposition stages, and parameter optimization procedures, which significantly complicate their implementation on resource-constrained systems. In addition, embedding operations in complex transform domains may introduce uncontrolled modifications to the container, potentially degrading perceptual reliability, especially when parameter tuning is imperfect or adaptive constraints are not strictly enforced. As a result, despite their strong robustness characteristics, transform-based steganographic methods require careful design to balance security, complexity, and perceptual reliability.

Spatial-domain steganography remains an active area of research due to its computational simplicity and direct manipulation of pixel intensities, which make such methods attractive for real-time and resource-constrained applications despite typically lower robustness compared to transform-domain schemes.

Recent work [22] by Septinaputri et al. presented an enhanced spatial domain image steganography technique targeting IoT security and privacy applications. Their approach focuses on intelligently selecting embedding locations based on local pixel characteristics to improve perception reliability and reduce distortion in contexts where devices have limited processing power and memory. The authors demonstrate that careful spatial embedding can achieve acceptable visual quality while providing basic protection against casual inspection, making it relevant for lightweight security in IoT ecosystems.

In a complementary direction, Milosav, Milosavljević, and Banjac in ref. [23] proposed a spatial domain steganographic method that embeds information in selected areas of the cover image. By restricting modification to specific regions (e.g., less visually sensitive areas), this scheme seeks to balance embedding capacity with perceptual reliability, showing improved performance over naive least significant bit (LSB) techniques in terms of reduced perceptual distortion. Similarly, Sulong and Wimmer in ref. [24] developed a spatial domain hiding scheme that extends classical LSB embedding with adaptive selection criteria to distribute hidden bits more uniformly across an image. Their results indicate that embedding strategies that consider local pixel statistics can yield stego-images with better visual quality and reduced detectability compared to uniform LSB approaches.

Finally, Wahono et al. in ref. [25] investigated enhancements to data security through spatial domain steganography in standard images. Their research focuses on optimizing embedding patterns and combining encryption with spatial hiding to strengthen confidentiality. By integrating a lightweight encryption stage before spatial embedding, the authors report improved resistance to basic extraction attacks while maintaining simple implementation requirements.

Collectively, these spatial-domain methods emphasize ease of implementation and low computational overhead, making them suitable for applications such as IoT and real-time systems. However, due to the direct manipulation of pixel values, they generally offer lower robustness against aggressive signal processing and steganalysis compared to transform-domain counterparts, highlighting the trade-off between simplicity and security.

Artificial intelligence-based steganographic methods have recently emerged as a powerful direction, leveraging deep learning models to automatically learn optimal embedding strategies and improve robustness against advanced steganalysis techniques. In ref. [26], Sushma et al. proposed a Mellin transform-based video steganography approach to improve resistance to deep-learning-based steganalysis by exploiting invariant transform-domain features. In ref. [27], Li et al. introduced a generative adversarial

network (GAN)-based framework, where adversarial training enables the generation of stego-images with high imperceptibility and reduced detectability.

However, despite promising performance of the artificial intelligence-based steganographic methods, these approaches are still at an early stage of development and typically require substantial computational resources for training and deployment, which limits their practical applicability, especially in real-time or resource-constrained environments.

The main contributions of this paper can be summarized as follows:

1. An adaptive code-controlled steganographic framework is developed, enabling block-wise adjustment of embedding strength according to local robustness characteristics of the image.
2. A principled codeword energy selection mechanism is proposed, which ensures reliable message extraction under predefined JPEG compression conditions while avoiding excessive embedding distortion.
3. An improved robustness–imperceptibility trade-off is achieved, demonstrating superior performance compared to conventional code-controlled steganographic methods and other best-known analogs.
4. The proposed approach retains low computational complexity, making it applicable to real-time and resource-constrained scenarios.
5. Comprehensive experimental results validate the effectiveness of the method, showing notable improvements in both bit error rate and perceptual quality under various compression levels.

The remainder of the paper is organized as follows.

Section 2 presents the proposed adaptive code-controlled steganographic method, including its theoretical foundations, embedding, and extraction algorithms. Section 3 describes the experimental setup and discusses the obtained results, including perceptual reliability, robustness against compression attacks, and resistance to steganalysis techniques. Finally, Section 4 concludes the paper and outlines directions for future research.

While the proposed method is evaluated on still images, its conceptual foundation, adaptive code-controlled embedding based on block-wise robustness assessment, is inherently generalizable to other media types, including video and audio, which will be explored in future work.

2. Materials and Methods

2.1. Theoretical Background

Code-controlled steganography represents an important class of information hiding techniques that bridges the advantages of both transform-domain and spatial-domain approaches. In code-controlled schemes, embedding is guided by a predefined code structure, which is applied to the cover in the spatial (or temporal) domain to indirectly control the frequency components where secret information is embedded. By forming and enforcing such code patterns, the method enables adaptive and structured modification of the cover's spectral content, allowing precise control of where and how the payload affects the transform domain. This approach enhances security, robustness, and resistance to steganalysis by introducing controlled, code-driven perturbations that are both difficult to detect and carefully aligned with the container's frequency characteristics.

In paper [28], authors introduced the concept of code-controlled steganography, establishing a framework in which embedding is directed by a predefined code structure. They proposed using Walsh functions as code patterns to selectively influence specific frequency components of the cover, enabling precise and targeted modification of the spectral domain through operations applied in the spatial (temporal) domain. This approach allows embedding to be carefully controlled, balancing imperceptibility and robustness, and effectively

mitigating the typical vulnerabilities of uniform LSB or fixed transform methods. The authors demonstrated that code-controlled embedding significantly enhances resilience to various attacks while maintaining acceptable reliability of perception, laying the groundwork for subsequent research on multi-level and blind-decoding code-controlled schemes.

Extending this concept, in paper [29], the notions of energy and selectivity of codewords were introduced, demonstrating how multi-level code structures with higher energy can be constructed to maximize the effectiveness of code-controlled embedding. This multi-level approach not only enhances flexibility and precision in controlling embedding but also improves the overall trade-off between capacity, imperceptibility, and robustness, making the steganographic method significantly more effective.

More recently, in paper [30], the field of techniques for increasing the efficiency of blind decoding in code-controlled embedding systems was advanced. By optimizing codeword structures and decoding strategies, this work allows the correct message extraction without requiring knowledge of cover content, thereby enhancing practicality in real-world applications. This analysis shows that carefully designed code control not only supports robust embedding but also facilitates reliable blind retrieval under noise and distortions.

Together, these works highlight that code-controlled steganography effectively unifies the structured embedding capabilities of transform-domain methods with the simplicity and direct manipulation of spatial techniques. By leveraging code control, these methods achieve strong robustness and controllability while mitigating some limitations of traditional approaches, making them a compelling reference point for comparative studies in modern steganographic research.

Furthermore, the code-controlled steganographic method satisfies the key effectiveness criteria of modern steganographic systems in an integrated manner. Operating in the spatial domain, this method ensures a high level of reliability of perception, as the method does not introduce visually noticeable distortions.

Despite working in the spatial domain, the method demonstrates enhanced resistance to attacks against the embedded message, exceeding the robustness of many transform-domain techniques under a wide range of common signal processing operations such as compression, noise addition, or filtering.

In addition, the code-based steganographic method exhibits robustness against multiple steganalysis attacks, as the statistical characteristics of the container are preserved more effectively than in conventional spatial-domain schemes. The controlled distribution of modifications and the use of structured coding mechanisms reduce detectable artifacts, thereby improving security against both targeted and blind steganalysis methods.

Let us briefly outline the fundamental idea behind the concept of code-controlled information embedding. Let X denote a container block represented as a matrix of size $N \times N$. The Walsh–Hadamard transform of X is computed as follows [31]

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

where H'_N is the normalized Walsh–Hadamard matrix of order $N = 2^k$, $H'_N = \left(\frac{1}{\sqrt{N}}\right) H_N$, H_N, constructed in accordance with the Sylvester construction

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

On the other hand, in addition to the two-dimensional Walsh–Hadamard transform, its one-dimensional version is also employed. Specifically, 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 fundamental theoretical foundations of the concept of code-controlled information embedding is the intrinsic relationship between the two-dimensional and one-dimensional Walsh–Hadamard transforms [32]. This relationship can be expressed (up to a constant scaling factor $\frac{1}{N}$) using the operator $\widetilde{A}$, which converts a matrix A of size $N \times N$ into a row vector of length N^2 by sequentially concatenating of the rows of the original matrix A. Then we can rewrite expression (1) as

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

Let d be the bit of additional information to be embedded in a given image block. Corresponding to this bit, a codeword T of size $N \times N$ is assigned, which is used to embed the bit d into the block. As a result, the block of the steganographic message M can be represented in the following form

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

Let us consider the Walsh–Hadamard transform applied to a row vector $\widetilde{M}$

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

Expression (6) provides a key insight into the nature of perturbations occurring in the Walsh–Hadamard transform coefficients of a steganographic message following the additive embedding of additional information. Specifically, these perturbations are not arbitrary: their magnitude, distribution, and localization are determined by the particular type of term $\widetilde{T}H_{N^2}$ representing the Walsh–Hadamard transform coefficients of the row vector $\widetilde{T}$ that encodes the additional information bit d. This establishes a direct and predictable link between the embedded information and the corresponding changes in the transform domain, which is fundamental for the design of code-controlled embedding schemes.

2.2. Codeword Construction

In practical implementations, the $N \times N$ matrix representation of Walsh functions of length N^2 has been extensively used as codewords. This is primarily because Walsh functions possess a unique property: they can selectively influence specific frequency components within the Walsh–Hadamard transform domain. By leveraging this property, one can achieve controlled modifications of particular spectral components, rather than indiscriminately altering the entire transform spectrum. When applied in the spatial domain, these functions facilitate targeted spectral shaping of the modified image blocks, allowing the embedding process to concentrate on frequency bands that are less perceptible to the human visual system, more resistant to statistical detection methods, and more robust against attacks targeting the embedded message.

Such selective embedding is particularly advantageous in enhancing the robustness of the steganographic system. By controlling the spectral distribution of perturbations, the embedded message can better withstand various attacks, including standard steganalysis techniques, compression, and other signal processing operations.

Numerous studies have investigated the use of various types of codewords in code-controlled steganographic schemes, demonstrating that the choice of a particular codeword configuration can impart fundamentally different properties to the embedding method,

including perceptual reliability, robustness, embedding capacity, and resistance to steganalysis attacks. Different codewords lead to distinct patterns of perturbations in the Walsh–Hadamard transform domain, thereby determining how the embedded information interacts with both the host signal and potential signal processing distortions.

However, in accordance with the results reported in ref. [28], the most effective performance is achieved when the codeword is designed to deliberately target a specific Walsh–Hadamard transform coefficient, namely the transformant with indices $(1,5)$

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

Nevertheless, the application of code-controlled steganographic methods is not limited to binary codewords. The approach can be generalized to construct multilevel codewords. Underpinning this generalization is a critical insight: the primary factor determining robustness is not the direct influence on a specific WHT coefficient, but rather the targeted effect on the corresponding spectral components of the DCT.

While a relationship exists between the WHT and DCT bases, it is non-unique and complex. A change in a single WHT coefficient (representing a square wave) projects onto a range of DCT coefficients (representing cosines). Therefore, robustness in typical transform-domain steganography (e.g., against compression like JPEG) is ultimately governed by how the embedding process shapes the DCT domain.

Consequently, the design of a codeword, whether binary or multilevel, must be driven by the goal of inducing a predictable and deliberate modification in the target DCT coefficients, particularly the perceptually significant low- and mid-frequency ones. This targeted influence on the DCT domain, not the intermediate WHT manipulation, is the definitive factor for ensuring reliable data hiding and extraction.

To illustrate how codewords are synthesized according to the criterion of influencing a specific DCT coefficient, it is necessary to first highlight an important result obtained in ref. [29]. Specifically, a two-dimensional DCT of the form [33]

$$S = C_N X C_N^T, \tag{8}$$

where

$$C(i,j) = \begin{cases} \frac{1}{\sqrt{N}}, \text{ for } i = 0; \\ \sqrt{\frac{2}{N}} \cos\left(\frac{(2j+1)\cdot i\cdot \pi}{2N}\right), \text{ for } i > 0, \end{cases} \tag{9}$$

can be represented through a one-dimensional transform $\widetilde{S} = \widetilde{X} A1_{N^2}$. This representation allows for a systematic construction of the corresponding transformation matrix $A1$, which can be assembled in accordance with the method described in ref. [34].

To ensure the highest selectivity of the constructed codewords, they must be designed so that the target DCT coefficient assumes a specified value α, while all other DCT coefficients are set to zero. This requirement can be formulated as a system of N^2 equations, which in matrix form can be expressed as

$$V \cdot A1 = Z, \tag{10}$$

where V is the row vector representing the codeword to be synthesized, and Z is a row vector consisting entirely of zeros, except for the entry on position $N \cdot n + m$ with value of corresponding to the (n, m)-th DCT coefficient, which is set to α when the two-dimensional DCT is represented in vectorized form, i.e.,

$$Z = \begin{pmatrix} 0 & \cdots & \alpha & \cdots & 0 \end{pmatrix}. \tag{11}$$

This formulation reduces the problem of codeword synthesis to the problem of solving a linear equation system, allowing precise control over the influence of the codeword on a chosen DCT coefficient while suppressing any unintended perturbations in the remaining spectrum.

By solving Equation (10), we obtain an example of a codeword that selectively influences the (2,1)-th coefficient of the DCT

$$T_{8,DCT(2,1)} = \begin{bmatrix} 0.17\alpha & 0.17\alpha & 0.17\alpha & 0.17\alpha & 0.17\alpha & 0.17\alpha & 0.17\alpha & 0.17\alpha \\ 0.15\alpha & 0.15\alpha & 0.15\alpha & 0.15\alpha & 0.15\alpha & 0.15\alpha & 0.15\alpha & 0.15\alpha \\ 0.1\alpha & 0.1\alpha & 0.1\alpha & 0.1\alpha & 0.1\alpha & 0.1\alpha & 0.1\alpha & 0.1\alpha \\ 0.03\alpha & 0.03\alpha & 0.03\alpha & 0.03\alpha & 0.03\alpha & 0.03\alpha & 0.03\alpha & 0.03\alpha \\ -0.03\alpha & -0.03\alpha & -0.03\alpha & -0.03\alpha & -0.03\alpha & -0.03\alpha & -0.03\alpha & -0.03\alpha \\ -0.1\alpha & -0.1\alpha & -0.1\alpha & -0.1\alpha & -0.1\alpha & -0.1\alpha & -0.1\alpha & -0.1\alpha \\ -0.15\alpha & -0.15\alpha & -0.15\alpha & -0.15\alpha & -0.15\alpha & -0.15\alpha & -0.15\alpha & -0.15\alpha \\ -0.17\alpha & -0.17\alpha & -0.17\alpha & -0.17\alpha & -0.17\alpha & -0.17\alpha & -0.17\alpha & -0.17\alpha \end{bmatrix}. \tag{12}$$

The coefficients appearing in the codeword matrix (12), namely 0.17, 0.15, 0.10, and 0.03, are obtained by solving the linear system of Equation (10). Specifically, the transformation matrix $A1$ (constructed according to the method described in ref. [34]) maps the vectorized image representation to the DCT coefficients. By setting the target DCT coefficient (2,1) to a specified value α and all other coefficients to zero, we obtain a system of N^2 linear equations. The solution V yields the codeword coefficients, which produce the values shown in (12).

These coefficients exhibit several notable properties. First, they are symmetric with alternating signs, reflecting the structure of the DCT basis function for the (2,1) coefficient, which corresponds to a vertical frequency pattern. Second, the coefficients sum to zero within each row, ensuring that the mean pixel intensity of the block remains unchanged after embedding. Third, the magnitude of the coefficients decreases from the center of the block outward, which aligns with the fact that modifications near block boundaries have a different spectral impact than those near the center.

However, the codeword obtained from (12) cannot be used directly in its original form, since its matrix representation contains fractional values. When such a codeword is applied in the embedding process, the subsequent rounding operation inevitably alters its effective impact, making the actual influence on the image dependent on the rounding procedure rather than on the intended spectral design.

Therefore, a more reasonable approach is to select an appropriate scaling coefficient α and to perform rounding of the codeword in advance. This procedure allows the amplitude of the codeword to be normalized and its influence on the image to be controlled predictably, ensuring that the desired effect on the target DCT coefficient is preserved after quantization while maintaining consistency in the embedding strength.

It is also reasonable to introduce the notion of the energy of a codeword $T = \left\| t_{i,j} \right\|$ as

$$E = \sum_{i=1}^{\mu} \sum_{j=1}^{\mu} t_{i,j}^2. \tag{13}$$

The energy characterizes the overall strength of the codeword and quantifies the degree of its impact on the container. A higher codeword energy results in stronger modifications of the image blocks, which, on the one hand, leads to a greater disturbance of the reliability of perception. On the other hand, increased energy enhances the robustness of the steganographic method against attacks targeting the embedded message.

Thus, the energy of the codeword represents a fundamental trade-off between perceptual reliability and resistance to attacks, making it a key parameter in the design of adaptive code-controlled steganographic schemes.

Further, Table 1 presents the codewords constructed using (12) for different values of the scaling coefficient α, corresponding to impact amplitudes on the image elements ranging from 0 to 3. This comparison illustrates how the choice of α affects the magnitude of the embedding perturbation and allows an informed selection of the codeword amplitude based on the desired balance between embedding strength and reliability of perception.

Table 1. Codewords for different values of α.

α	Codeword	Energy E
3	$T_{8,DCT(2,1),\alpha 3} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \end{bmatrix}$	16
4	$T_{8,DCT(2,1),\alpha 4} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \end{bmatrix}$	32
6	$T_{8,DCT(2,1),\alpha 6} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \end{bmatrix}$	48
9	$T_{8,DCT(2,1),\alpha 9} = \begin{bmatrix} 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -2 & -2 & -2 & -2 & -2 & -2 & -2 & -2 \end{bmatrix}$	96

Table 1. *Cont.*

α	Codeword	Energy E
15	$T_{8,DCT(2,1),\alpha 15} = \begin{bmatrix} 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -2 & -2 & -2 & -2 & -2 & -2 & -2 & -2 \\ -3 & -3 & -3 & -3 & -3 & -3 & -3 & -3 \end{bmatrix}$	240

Codewords presented in Table 1 form the basis for an adaptive approach to selecting the appropriate codeword during information embedding in code-controlled steganographic methods. Such an adaptive strategy accounts for the image's underlying structure, ensuring reliable perception and enhancing robustness against attacks targeting the embedded information. By tailoring the choice of codewords to the local characteristics of image blocks, it is possible to optimize both the perceptual reliability and the security of the steganographic method.

The energy values presented in Table 1 are computed according to Equation (13). Notably, these values are not arbitrarily selected but are directly determined by the scaling coefficient α and the rounding procedure applied to the fractional codeword coefficients. Specifically:

- For $\alpha = 3$, rounding yields the codeword shown in the first row of Table 1, with energy $E = 16$.
- For $\alpha = 4$, the codeword contains two rows of ones and two rows of minus ones, resulting in $E = 32$.
- For $\alpha = 6$, three rows of ones and three rows of minus ones yield $E = 48$.
- For $\alpha = 9$, the codeword includes values of 2, 1, 0, -1, -2, leading to $E = 96$.
- For $\alpha = 15$, the codeword includes values of 3, 2, 1, -1, -2, -3, resulting in $E = 240$.

The non-uniform spacing between these energy levels is a consequence of the discrete rounding of fractional coefficients and the quadratic dependence of energy on the coefficient magnitudes.

2.3. Proposed Adaptive Embedding Method

Although code-controlled steganographic methods demonstrate excellent performance in terms of perceptual reliability and attack robustness, their further development is possible by introducing adaptivity. Different image blocks exhibit varying structural characteristics, which necessitate different levels of embedding amplitude to ensure the resilience of the embedded message against potential attacks. By adapting the codeword selection and embedding strength to the local properties of each block, it is possible to enhance both the security and the perceptual reliability of the steganographic method, providing a more flexible and effective approach to information hiding.

We propose the following approach. Let us formally represent the container as a set of image blocks

$$\{B_1, B_2, \ldots, B_N\}. \tag{14}$$

For each block B_i, a robustness functional

$$\Upsilon = R(B_i), \tag{15}$$

is introduced. This functional quantifies the resilience of the embedded message within the block against potential attacks or distortions, taking into account the local structural characteristics of the image.

In general, the problem of determining the robustness functional for each block is quite challenging, given the nonlinearity of potential attacks against the embedded message, particularly compression-based attacks. Experimental research indicates that the a priori estimation of the robustness of a given block can be approached using artificial intelligence methods; however, this in itself constitutes a highly complex task. The difficulty arises from the need to account for both the structural variability of image blocks and the unpredictable effects of nonlinear transformations introduced by attacks, which makes precise prediction of block-specific robustness a nontrivial problem.

One possible approach is to perform experimental attacks on the block containing the embedded information to observe its behavior under such manipulations. By analyzing the block's response to these attacks, it becomes possible to conclude its robustness. This empirical method offers practical insights into how different blocks withstand various types of distortions, enabling more informed decisions when selecting codewords and embedding energies in an adaptive steganographic scheme.

The robustness functional $R(B_i)$ is determined empirically by testing each block with progressively higher codeword energies. For each energy level E_j from the set $\{E_{min}, E_{min+1}, \ldots, E_{max}\}$, we embed a test bit into the block using the corresponding codeword, apply JPEG compression at the target quality factor QF_{target}, and evaluate whether the bit can be correctly extracted. The minimal energy level E_j that yields correct extraction is recorded as the required embedding energy for block B_i. If extraction fails even at E_{max} the block is considered unsuitable for embedding, and the maximum energy is used with the understanding that the embedded bit may be unrecoverable under the target attack.

This empirical approach is adopted because the relationship between block characteristics and robustness to JPEG compression is highly nonlinear and depends on complex interactions between the block's frequency content, the spectral properties of the codeword, and the JPEG quantization process. Analytical prediction of this relationship is impractical, making empirical evaluation the most reliable and straightforward method. To maintain computational efficiency, robustness assessments are precomputed for all blocks before the main embedding process, and the results are cached for subsequent use.

We propose an adaptive approach to selecting the embedding energy E of the codeword. Instead of using a fixed energy for all image blocks, the energy is adjusted individually for each block based on its characteristics and robustness. This strategy allows the embedding process to account for variations in the local structure of the image, ensuring that each block receives an appropriate level of modification. By tailoring the energy in this way, it is possible to achieve a better balance between the reliability of perception of the embedded information and its resilience against potential attacks.

The robustness of the corresponding block determines the energy of the codeword. Formally, this relationship can be expressed as

$$E_i = f(\Upsilon), \tag{16}$$

where E_i denotes the embedding energy for the i-th block, and $f(\cdot)$ is a monotonic decreasing function, reflecting the inverse relationship between block robustness and embedding strength. In other words:

- A weak block leads to a higher embedding energy;
- A strong block leads to a lower embedding energy.

This adaptive strategy ensures that blocks with lower inherent robustness receive stronger embedding signals, enhancing the overall reliability of the embedded message while still taking into account the local structure of the image.

Based on the proposed concept and the theoretical foundation developed above, we can now present a concrete code-controlled steganographic method. This method leverages the principles of adaptive codeword selection and the dependence of embedding energy on block robustness to achieve a balance between perceptual reliability and robustness against attacks. By integrating these elements, the method provides a systematic approach to embedding additional information into image blocks while taking into account their local structural characteristics and spectral properties.

Additional information embedding.

Input:

1. Cover image $\mathcal{I}$.
2. Additional information (message) $D = \{d_1, d_2, \ldots, d_L\}$ of length L.
3. Target compression level QF_{target}, defining the minimum compression quality, such that the embedded message remains extractable for all JPEG compression levels $QF \geq QF_{target}$.

Output:

1. Stego-image $\mathcal{I}_S$ containing the embedded message.

Embedding steps:

Step 1. Block Partitioning:

Partition the cover image $\mathcal{I}$ into non-overlapping blocks of size $N \times N$, where $N = 2^n$ and $n \in \mathbb{N}$. Denote the resulting set of blocks as

$$\mathcal{B} = \{B_1, B_2, \ldots, B_K\}. \tag{17}$$

Step 2. Initialization:

Let $B_i \in \mathcal{B}$ be the current block selected for embedding the next bit $d_i \in D$. Embed the bit d_i with the minimal initial codeword energy E_{min}, producing the modified block B_i' with help of additive embedding

$$B_i' = B_i + (-1)^{d_i} T_{N,DCT(\beta,\gamma)}. \tag{18}$$

Formally, set the embedding amplitude $E_j = E_{min}$.

Boundary Handling. After computing the modified block B_i', the resulting pixel values may, in some cases, fall outside the valid range of $[0, 255]$ for 8-bit image representation. To ensure the integrity of the stego-image, we apply a clamping operation:

$$B_i'(n,m) = \begin{cases} 0, & if\ B_i'(n,m) < 0, \\ 255, & if\ B_i'(n,m) > 255, \\ B_i'(n,m), & otherwise. \end{cases} \tag{19}$$

This clamping strategy, while introducing a slight nonlinearity, preserves the overall embedding structure. The extraction process described in Equation (21) relies on the correlation between the difference matrix Δ and the codeword, rather than on the exact magnitude of individual pixel modifications. Consequently, the sign-based detection mechanism remains robust even when boundary clamping occurs. Moreover, the adaptive energy selection mechanism ensures that codeword amplitudes are kept relatively low, making boundary violations rare in practice. For the codeword energies used in this study (as presented in Table 1), the maximum modification amplitude per pixel is 3, which

limits the occurrence of boundary violations to pixels already near the extremes of the intensity range.

Step 3. Compression Simulation and Error Detection:

Apply a set of JPEG compressions $QF \in \left\{QF_{target}, QF_{target} + \Delta\text{QF}, \ldots, 100\right\}$ to the partially constructed stegoimage $\mathcal{I}_S$ and attempt to extract the embedded information D'. Mark any blocks B_i' for which extraction of d_i fails as error blocks

$$\varepsilon = \left\{B_i' \middle| d_i' \neq d_i\right\}. \tag{20}$$

Step 4. Adaptive Embedding Iteration:

If $\varepsilon = \varnothing$ or the codeword energy has reached the maximum permissible value E_{max}, terminate the algorithm. Otherwise, for each block B_i', increase the embedding energy E_j to the next level E_{j+1} in accordance with the rubusness functional $R(B_i)$ and re-embed the corresponding bit. Repeat Steps 3–4 until correct extraction is achieved for all considered compression qualities, or until $E_j = E_{max}$.

Step 5. Output Stego-Image:

Construct the final stego-image $\mathcal{I}_S$ by assembling all modified blocks B_i' after successful completion of the adaptive embedding procedure.

Extraction of the additional information

Step 1. Partition the received stego-image into non-overlapping blocks of size $N \times N$.

Step 2. Let B_i' to be the next block of size $N \times N$ of the possibly perturbed steganographic image, corresponding to the block B_i.

Step 2.1. Construct the difference matrix $\Delta = B_i' - B_i$ with elements $\Delta(n, m)$, $n, m = 0, 1, \ldots, N-1$.

Step 2.2. Extracting the additional information bit from the block is performed accordingly to the formula

$$\overline{d_i} = sign(\sum_{n=0}^{N-1} \sum_{m=0}^{N-1} \Delta(\mathrm{i}, \mathrm{j}) T_{N,DCT(\alpha,\beta)}). \tag{21}$$

Note that Step 2.2 in the information extraction algorithm, in fact, implements the optimal reception algorithm.

Also note that the proposed method performs energy adaptation under a worst-case compression assumption, selecting for each block the minimal embedding energy that guarantees correct extraction under any JPEG compression with quality factor not lower than QF_{target}.

3. Results

In the next stage, the proposed method will be evaluated in practice in order to determine its key performance characteristics. The experimental study aims to evaluate the reliability of perception, resistance to steganalysis attacks, and robustness of the embedded message against intentional and unintentional distortions. The obtained results will be compared with those of state-of-the-art steganographic algorithms and with alternative modifications of code-controlled steganographic methods. Such a comparative analysis will allow us to objectively evaluate the effectiveness of the proposed adaptive approach and to identify its advantages and limitations relative to existing solutions.

In the experimental study, we employ the codewords presented in Table 1, which are designed to influence the (2,1)-th DCT coefficient. Accordingly, the corresponding energy vector can be expressed as

$$E_i = \{16,32,48,96,240\}. \tag{22}$$

These energy values are derived directly from the codewords in Table 1, with each value corresponding to a specific scaling coefficient α as detailed in Section 2.2.

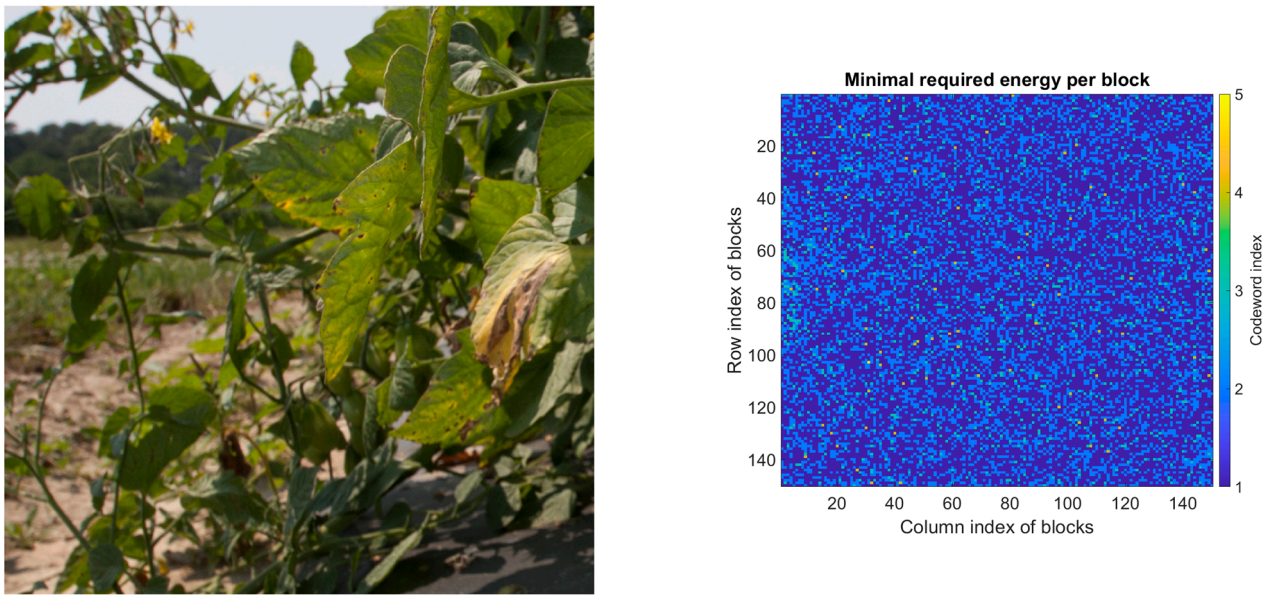
All experiments were conducted using MATLAB R2023b (The MathWorks, Inc.) with the Image Processing Toolbox. The implementation follows the adaptive embedding procedure described in Section 2.3, with block size 8×8 pixels and codewords constructed according to the rounding procedure illustrated in Table 1.

For the experiment, a 1200×1200 pixel image in lossless PNG format was used. Given that the embedding block size was 8×8 pixels, the image was divided into 150×150 blocks, allowing for the embedding of a total of 22,500 bits of additional information using the proposed adaptive codeword-based method, while the value of parameter $QF_{target} = 50$ was selected.

To evaluate the proposed method under more stringent robustness requirements, we also considered $QF_{target} = 20$. This choice corresponds to scenarios demanding high resilience against aggressive JPEG compression, for instance, when images are transmitted via legacy systems, or stored in low-bandwidth environments. While $QF_{target} = 50$ provides a safety margin relative to typical messaging applications (QF ≈ 70), $QF_{target} = 20$ represents a worst-case condition, allowing us to assess the fundamental limits of the adaptive codeword-based method. Comparing both thresholds demonstrates the trade-off between reliability of perception and robustness, which is critical for practical steganographic systems.

In our implementation, the embedding of additional information was performed in the Y channel of the YCbCr color space. This choice is motivated by practical considerations: in most real-world systems, image compression operates in the YCbCr space, and the luminance component (Y channel) typically undergoes the least amount of compression compared to the chrominance channels (Cb and Cr). Therefore, embedding information in the Y channel ensures higher robustness to compression while minimizing perceptual distortion, making it the most suitable choice for practical steganographic applications.

Figure 3 illustrates the container alongside the energy distribution map of the codewords, indicating the minimal energy required for each block to ensure robust embedding for $QF_{target} = 50$.



(**a**). (**b**).

Figure 3. Container (**a**) and the energy distribution map (**b**).

As observed in Figure 3, the majority of blocks require the use of codewords with minimal energy values. This indicates the redundancy of indiscriminately applying identical codewords to all blocks and highlights the effectiveness of the proposed adaptive approach combined with codeword-controlled embedding of additional information.

The proposed method is block-based, and consequently, its embedding capacity is inherently determined by the block size, as is typical for most block-based steganographic techniques. Specifically, when using an 8×8 block, as in our experiments, the embedding capacity of the hidden channel is $1/64$ bit per pixel, which provides a sufficient level of throughput. Increasing the block size reduces the embedding capacity but may potentially enhance robustness against attacks on the embedded message, whereas decreasing the block size increases the capacity at the expense of reduced robustness.

Nevertheless, it should be emphasized that the evaluation of any steganographic method must be performed on a diverse set of images. For this purpose, we utilize the NRCS [35] image database, which is commonly employed for testing steganographic techniques. In our research, we selected a sample of 530 1200×1200 pixel images in lossless PNG format and assessed the method according to several criteria:

1. Reliability of perception of the stego-images;
2. Robustness against attacks on the embedded message;
3. Resistance to steganalysis techniques;
4. Computational complexity of the embedding and extraction processes.

3.1. Reliability of Perception of the Stego-Images

The perceptual reliability in steganographic methods is a highly nontrivial issue, as it largely depends on the characteristics of the human visual system. To date, there is no universally accepted mathematical model that accurately quantifies human perception in this context, making it challenging to rigorously evaluate the perceptual reliability of embedded information.

Nevertheless, differential measures are widely accepted as practical indicators of how much a container changes as a result of steganographic embedding. One of the most commonly used measures is the Peak Signal-to-Noise Ratio (PSNR), which quantifies the difference between the original and the stego-image. PSNR is defined as

$$PSNR = 20log_{10}\left(\frac{255}{\sqrt{MSE}}\right), \tag{23}$$

where MSE (Mean Squared Error) is calculated as the average squared difference between corresponding pixels in the original and stego-images

$$MSE = \frac{1}{nm}\sum_i \sum_j |X(i,j) - M(i,j)|^2, \tag{24}$$

where n, m are the dimensions of the image, X is the container matrix, and M is the steganographically modified image.

Higher PSNR values indicate smaller perceptual changes and, therefore, higher perceptual reliability of the stego-image.

Unlike the classical code-controlled steganographic method, in the proposed adaptive approach, the energy of each codeword is chosen based on the robustness of the corresponding block. As a result, the PSNR can vary from one image to another, reflecting the adaptive embedding strategy that balances reliability of perception and robustness.

To further investigate the perceptual reliability of the proposed adaptive steganographic method, we perform an empirical experiment on a set of 530 real images from the NRCS database in PNG format. In this experiment, additional information was embedded

into the images, and the resulting PSNR value was computed for each stego-image. This approach allows us to assess the variation in perceptual quality across different images, taking into account the adaptive selection of codeword energies for each block. The distribution of PSNR values over the sample is visualized as a histogram for values $QF_{target} = 50$, and $QF_{target} = 20$, which is presented in Figure 4, providing a clear overview of the method's impact on image quality.

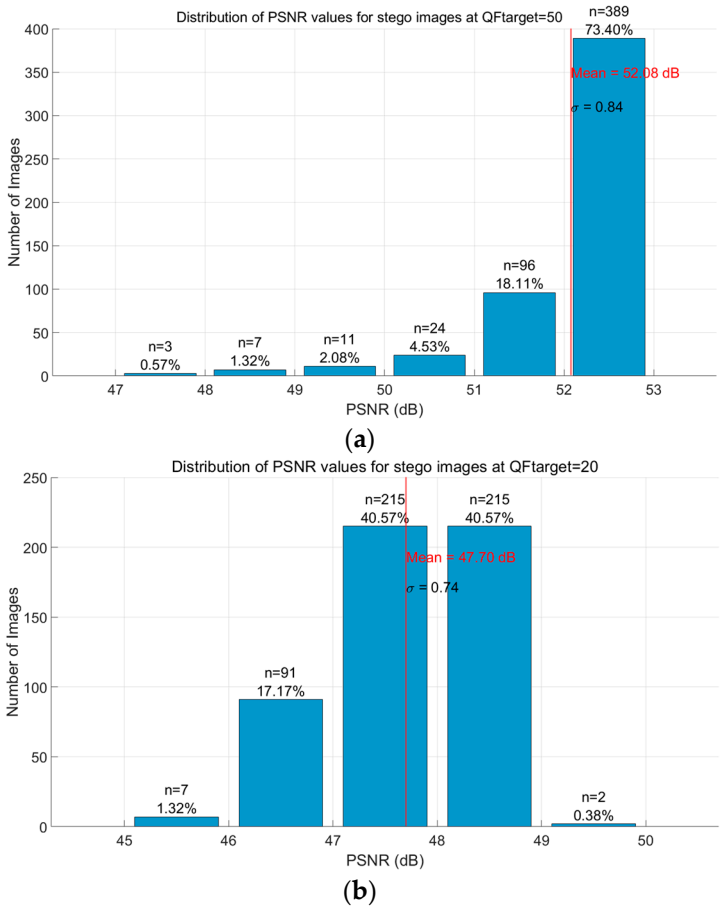


Figure 4. Histogram of PSNR values for steganographic images at $QF_{target} = 50$ (**a**) and $QF_{target} = 20$ (**b**).

For $QF_{target} = 50$, the proposed adaptive method demonstrates more pronounced improvements when compared with the classical code-controlled method: PSNR values range from 47.40 dB to 52.83 dB, with a significantly higher average of 52.07 dB. This clear increase in perceptual quality highlights the importance of adapting the embedding energy to the expected attack level. The obtained results demonstrate that the proposed adaptive approach not only enhances robustness against compression attacks, as will be shown, but also significantly improves perceptual reliability compared to the classical code-controlled method.

For $QF_{target} = 20$, the obtained PSNR values lie in the range from 45.43 dB to 49.40 dB, with an average value of 47.7 dB. It is worth emphasizing that even the classical code-controlled steganographic method demonstrates a PSNR of approximately 48.1 dB under comparable conditions. Therefore, despite operating in a more challenging regime with stronger robustness requirements, the proposed adaptive approach achieves perceptual reliability that is fully comparable to the original method. This confirms that the gain in robustness obtained through adaptive energy selection does not come at the expense of noticeable degradation in visual quality.

Finally, in the best-case reliability of perception scenario corresponding to $QF_{target} = 100$, the proposed method achieves a PSNR of up to 54.15 dB. This result confirms the high perceptual reliability of the method when robustness constraints are minimal and further demonstrates the flexibility of the proposed adaptive framework across a wide range of operating conditions.

3.2. Robustness Against Attacks on the Embedded Message

The robustness of the proposed steganographic method against attacks on the embedded message is evaluated as follows. First, the additional information is embedded into the image container using the proposed algorithm. Next, the stego-image is subjected to a selected attack. After the attack, the embedded information is extracted from the distorted image. Finally, robustness is quantified by measuring the percentage of incorrectly decoded bits, i.e., the bit error rate (BER), which serves as an objective metric of the method's resistance to attacks on the embedded message.

A wide variety of attacks on the embedded message are known, including compression attacks, geometric transformations, additive noise attacks, and other forms of signal manipulation. Among these, compression attacks remain the most prevalent in practice. This is primarily due to the widespread use of lossy compression algorithms in modern digital communication and storage systems. For example, images transmitted via messaging applications, social networks, or cloud services are almost invariably subjected to JPEG compression with medium to high compression ratios. Consequently, ensuring robustness against compression attacks addresses the most common and practically relevant threat scenario for steganographic methods today, making it a critical benchmark for evaluating method reliability. While other distortion types (e.g., additive noise, filtering, geometric transformations) are also relevant in certain application contexts, their comprehensive analysis falls beyond the scope of the present study, which focuses on JPEG compression as the primary and most widespread attack vector in contemporary communication channels.

In Figure 5, we present the graph showing the dependence of the bit error rate (BER) on the JPEG quality factor (QF) for the proposed adaptive method, as well as for the classical code-controlled steganographic method.

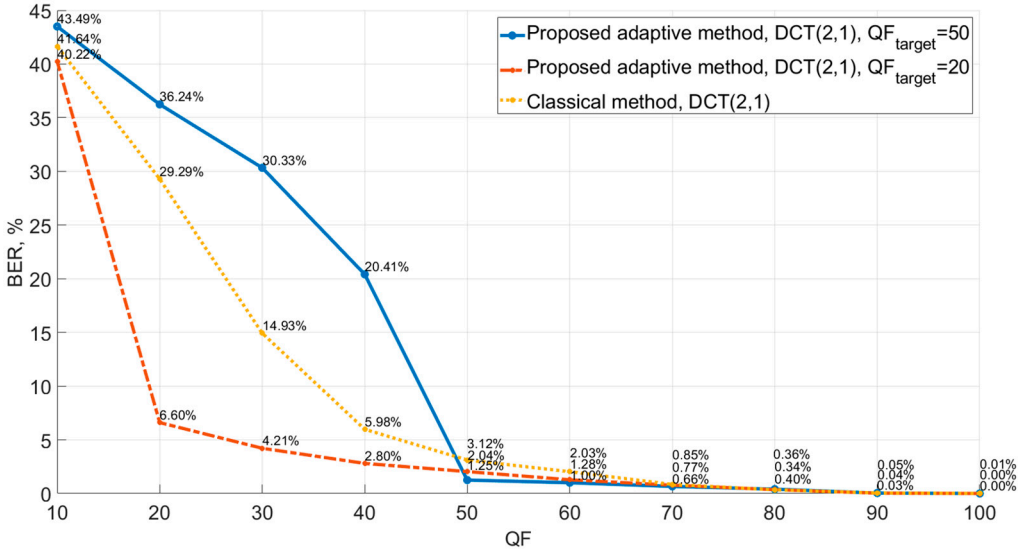


Figure 5. The graph showing the dependence of the BER on the JPEG QF for the proposed adaptive method and the classical code-controlled steganographic method.

Figure 5 illustrates the BER dependence on the JPEG quality factor (QF) for the proposed adaptive embedding method with $QF_{target} = 50$, $QF_{target} = 20$ and for the classical steganographic method based on code control.

For the case $QF_{target} = 50$, it can be observed that the adaptive method demonstrates very good robustness against JPEG compression attacks for attack strengths with $QF \geq 50$. Moreover, the advantage of the adaptive approach over the classical method becomes more pronounced as the attack strength increases. In particular, at $QF = 70$, which corresponds to the most commonly used compression settings in practical applications, the adaptive method achieves a BER that is 0.19% lower than that of the classical approach. As the compression strength further increases, this gap widens: at $QF = 50$, the adaptive method exhibits a reduction in the error rate of 1.86% compared to the classical method.

As expected, for compression attack levels with $QF < 50$, the effectiveness of the adaptive method decreases sharply. This behavior is a direct consequence of the fact that the energy adaptation is performed with $QF_{target} = 50$ and is therefore optimized for attack strengths corresponding to $QF \geq 50$. When the compression becomes stronger than the target level, the predefined energy distribution is no longer sufficient to guarantee the same level of robustness, which leads to a noticeable increase in the bit error rate.

A particularly remarkable behavior is observed for $QF_{target} = 20$. In this case, the performance gain of the adaptive method under strong compression attacks becomes highly pronounced. Specifically, for an attack with $QF = 20$, the adaptive approach demonstrates a reduction in the bit error rate of 22.68% compared to the classical code-controlled method. This constitutes a very strong result and is of substantial practical importance for communication channels subjected to severe compression attacks against the embedded message.

It should also be emphasized that at the attack level $QF = 50$, the adaptive scheme configured with $QF_{target} = 50$ achieves 0.79% fewer bit errors compared to the adaptive scheme optimized for $QF_{target} = 20$. This result clearly demonstrates the importance of adapting the embedding strategy to the expected compression conditions. In other words, while adaptation to lower quality factors provides substantial robustness against strong attacks, optimal performance at moderate compression levels is achieved only when the adaptation target matches the actual attack strength.

While the robustness evaluation presented above considers a single JPEG compression operation, real-world scenarios in social media and messaging applications often involve multiple re-compression cycles. For instance, an image may be compressed when uploaded, re-compressed when forwarded, and compressed again when saved or shared across different platforms. Understanding how the proposed method performs under such conditions is therefore important for practical deployment.

To evaluate the resilience of the proposed adaptive method to multiple compression cycles, we conducted an additional experiment in which stego-images were subjected to two consecutive JPEG compressions. The experiment was performed on 530 PNG images for the proposed method with $QF_{target} = 20$. For comparison, we first evaluated single compression at $QF = 80$, yielding a bit error rate of 0.35%. Subsequently, we applied a double compression scenario with $QF = 90$ followed by $QF = 70$, which simulates a typical use case where an image is first compressed by a social media platform (e.g., at high quality) and then re-compressed during forwarding or storage. Under this double compression scenario, the bit error rate increased to 1.99%.

This increase in error rate under double compression highlights the additional challenges posed by cascaded distortions, which can be more severe than a single compression at the final quality factor alone. The results suggest that while the proposed adaptive method provides a degree of resilience to re-compression, particularly given its design for

a target quality factor of 20, further improvements may be necessary for applications where multiple compression cycles with varying quality factors are common. A comprehensive investigation of multiple re-compression cycles, including scenarios with more than two compressions and varying quality factor sequences, remains an important direction for future research.

3.3. Resistance to Steganalysis Techniques

A key characteristic of any steganographic method is its robustness against possible steganalysis attacks. The classical code-controlled steganographic method has already been researched [36] for its robustness against major steganalysis attacks, and the results were impressive. The most well-known detection methods have proven largely ineffective both in revealing the embedded information and in detecting its presence through steganalysis when code control is employed. This effect can be explained by the fact that the impact on individual pixels of the container is strictly controlled and minimal. Within each block, the numbers of positive and negative modifications are balanced, and given statistically equiprobable message symbols across the entire container, the overall embedding does not significantly alter the primary statistical characteristics of the container itself.

This, in turn, motivated the search for new theoretical foundations and practical approaches for detecting codeword-based embedding. Currently, such methods are still in the developmental stage.

One of the classical and widely studied statistical steganalysis techniques is RS steganalysis. RS steganalysis operates by dividing an image into groups of pixels and analyzing how controlled modifications of least significant bits affect the resulting statistical noise within these groups. By classifying groups as "regular" or "singular" based on the change in noise patterns after bit flipping, RS steganalysis can detect hidden information that alters the natural pixel statistics of the container. This method is particularly effective at identifying steganographic embedding that utilizes least significant bit modifications and related statistical perturbations, making it an important benchmark for evaluating the detectability of steganographic schemes. Because RS steganalysis targets inherent statistical consistencies in natural images, passing RS detection is widely regarded as a significant indicator of a method's resilience to statistical attack scenarios.

To evaluate the steganalytic security of the proposed adaptive steganographic method, a dedicated experimental study was performed. A dataset consisting of 530 digital images from the NRCS database in PNG format was used, into each of which additional information was embedded in all image blocks using the proposed adaptive embedding scheme. The target compression quality factor was set to $QF_{target} = 20$, which corresponds to a deliberately challenging scenario. This choice was made to maximize the embedding impact on the container and thus to analyze the method's behavior under the most adverse conditions from a steganalysis perspective. After embedding, all stego-images were stored in the PNG format to avoid any additional distortions caused by compression. Subsequently, RS steganalysis was applied to the resulting stego-dataset. The obtained detection results are presented in Figure 6.

Analysis of the results presented in Figure 6 shows that only 8 out of 530 stego-images (approximately 1.51%) are classified by the RS steganalysis method as belonging to the Moderate embedding risk region. The remaining images are assessed as either safe or indistinguishable from cover images, indicating the absence of reliable steganographic evidence.

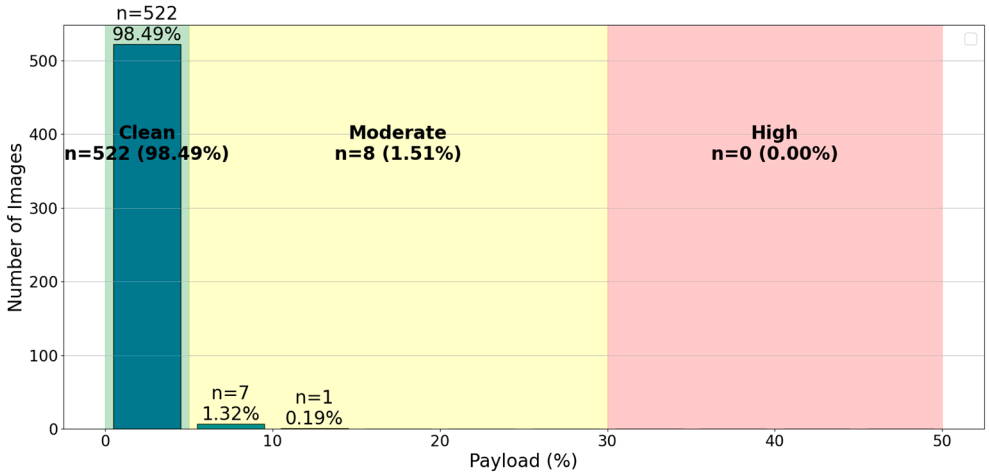


Figure 6. RS steganalysis results for images embedded using the proposed adaptive steganographic method (histogram with risk regions).

These results demonstrate the low effectiveness of RS steganalysis against the proposed adaptive steganographic method, even under deliberately unfavorable conditions, where the embedding process was optimized for a strong attack scenario with $QF_{target} = 20$. Despite the increased embedding impact required to ensure robustness under severe compression, the majority of stego-images remain statistically close to their corresponding covers from the perspective of RS analysis.

From a practical standpoint, this confirms that the proposed adaptive method preserves the fundamental statistical properties of the container, rendering classical RS steganalysis largely ineffective. Consequently, RS analysis cannot be considered a reliable detection tool for the proposed method, highlighting its strong resistance to one of the most widely used and established steganalytic techniques.

Chi-square (χ^2) analysis is a widely used statistical method in steganalysis that evaluates the likelihood of hidden information in digital images. The technique is based on examining the distribution of pixel values, especially focusing on pairs of values that are expected to appear with similar frequency in natural images. When a message is embedded into the image using a steganographic method, these distributions are slightly altered, and the χ^2 test can detect these deviations.

Performing experiments using χ^2 analysis is important because it provides a quantitative measure of detectability for the embedded information. In our study, we perform χ^2-based experiments to evaluate how detectable the hidden message is, particularly under strong embedding conditions.

In this research, we do not apply the χ^2 test in its raw form. Instead, we calibrate it using a control group of clean, unmodified images. This calibration involves computing the mean and standard deviation of Chi-square values across the clean set and then normalizing the test results of target images relative to these statistics, producing Z-scores. The reason for this approach is that natural images, even without steganographic content, often exhibit significant deviations in pixel pair distributions, which can lead to high raw Chi-square values and false positives. By referencing a baseline derived from clean images, we can more accurately distinguish between normal variations in natural images and anomalies likely caused by steganographic embedding. This method ensures that detection thresholds reflect the inherent statistical properties of the image set, improving both the reliability and interpretability of the results.

Figure 7 shows a histogram summarizing the results of the Chi-square analysis with calibration. The chart illustrates the distribution of images across three detection zones:

low (green), medium (yellow), and high (red) Z-scores, highlighting how many images fall into each category. This visualization provides a clear overview of the steganography detection outcomes relative to the baseline established from the clean image set.

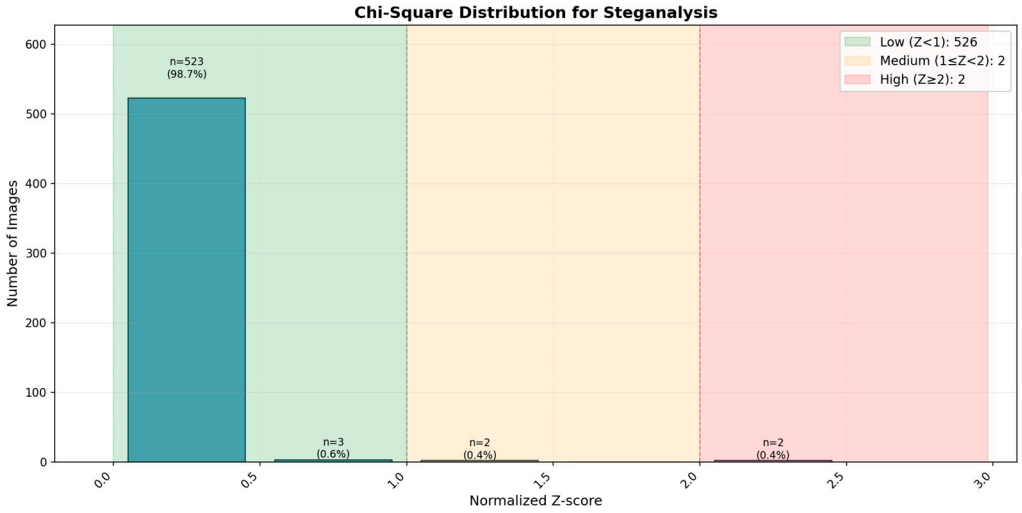


Figure 7. Distribution of images across Chi-square detection zones calibrated on clean images.

Analysis of Figure 7 demonstrates the high robustness of the proposed adaptive steganographic method against χ^2 steganalysis. Out of 530 images with embedded messages, only 2 images fell into the yellow zone and 2 into the red zone, corresponding to a very low detectability rate of less than 1%. This clearly indicates that the adaptive method effectively minimizes statistical artifacts in the container, making the hidden information nearly invisible to this type of attack. Overall, these results confirm the efficiency of the proposed approach in maintaining stealthiness while embedding data in all blocks.

Another important class of steganalytic attacks is Simple Pair Analysis (SPA), which is designed to detect subtle correlations introduced by embedding in adjacent pixel pairs. SPA is particularly sensitive to local dependencies and statistical irregularities in image blocks, making it a complementary method to RS steganalysis. Investigating the performance of our proposed adaptive method against SPA is crucial to verify its resistance to a broader range of attacks. Therefore, we will perform experiments using the same set of 530 images and embedding parameters as previously described to assess the detectability of hidden messages under SPA.

Figure 8 presents a histogram illustrating the detection of steganographic messages in the set of 530 images using SPA. The figure highlights the regions of detection confidence, allowing us to visually assess the robustness of the proposed adaptive embedding method against SPA.

Analysis of Figure 8 shows that SPA failed to detect a single steganographic message among the 530 images embedded with the proposed adaptive method. This result demonstrates the extremely high resistance of our method against SPA, indicating that even standard statistical pair-based attacks are unable to reveal the presence of hidden information. Such robustness confirms the effectiveness of the adaptive energy distribution strategy in minimizing detectable distortions in the container.

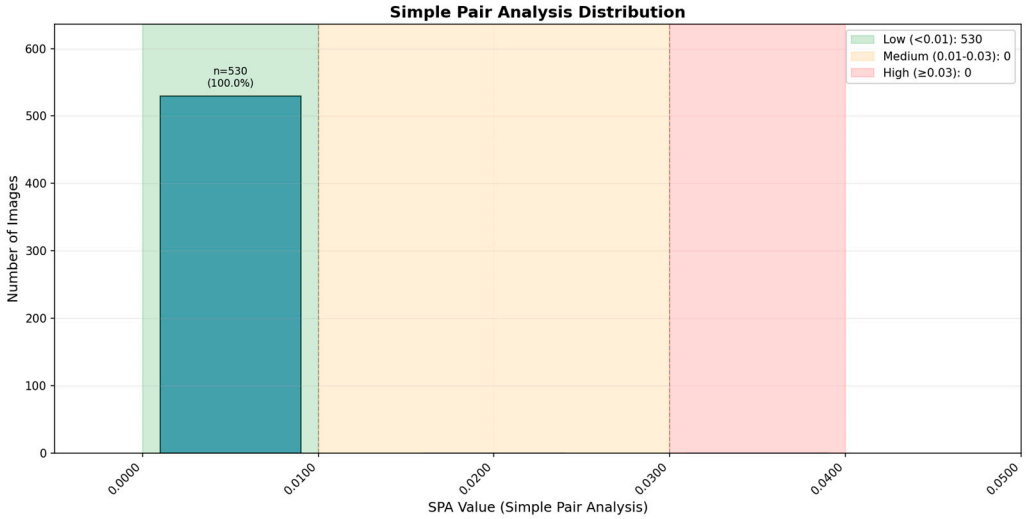


Figure 8. Histogram of SPA-based detection results.

In addition, we applied StegExpose, a practical tool that integrates multiple modern steganalytic tests, to the set of 530 images containing embedded messages. Remarkably, StegExpose did not detect any steganographic content in a single image, further confirming the robustness of the proposed adaptive method. This demonstrates that even advanced, real-world detection tools are unable to reveal the hidden information, highlighting the practical security of our approach.

3.4. Computational Complexity of the Embedding and Extraction Processes

Assessing the computational complexity of steganographic algorithms is inherently challenging. This is due to the fact that the execution time and efficiency of these algorithms heavily depend on the specific implementation and the platform on which they are executed. Minor differences in coding practices, memory management, or software optimizations can significantly affect performance metrics.

To provide a fair and practical comparison, we adopted the following approach for evaluating computational efficiency: we measured the time required for both embedding and extracting hidden information in images of size 1200 × 1200 pixels. All experiments were performed in MATLAB R2023b, executed on a workstation equipped with an AMD Ryzen 5 7500F CPU, 32 GB DDR5 RAM, and an NVIDIA GeForce RTX 3050 GPU.

This setup ensures that the reported performance metrics reflect realistic computational requirements for typical laboratory environments and provide a reliable basis for comparing the efficiency of different steganographic methods.

Table 2 presents the measured times for embedding and extracting hidden information, as well as the total processing time for a 1200 × 1200 pixel PNG image. The table includes the proposed adaptive steganographic algorithm, the classical LSB algorithm, the SVD-UV-based algorithm, and the DCT-based algorithm. These measurements allow a clear comparison of the computational efficiency of different methods under the same experimental conditions, highlighting the practical feasibility of the proposed approach.

The results presented in Table 2 reveal that, although the proposed adaptive method incurs a higher embedding time of 5.85 s, compared to classical code-controlled methods and other traditional techniques, the extraction time remains remarkably low at just 0.11 s. This is a crucial advantage, as extraction is often performed on resource-constrained devices, where efficiency and speed are paramount.

Table 2. Computational performance comparison of different steganographic algorithms on 1200 × 1200 PNG images.

Algorithm	Proposed Method	Classical Code-Controlled	LSB-R	SVD UV Method	Koch-Zhao DCT Method
Embedding time, s	5.85	0.01	0.88	148.16	1.90
Extraction time, s	0.11	0.05	0.58	0.33	0.96
Total time, s	5.96	0.06	1.46	148.49	2.86

In other words, the adaptive method's trade-off can be explained: longer embedding time is balanced by rapid extraction, ensuring that the overall performance is well-suited for real-world applications. Moreover, the adaptive embedding significantly enhances robustness against attacks on the embedded message, improving the reliability of information recovery while maintaining low extraction time. Consequently, the proposed method not only provides strong protection of hidden data but also preserves practical usability, making it both robust and efficient in real-world settings.

3.5. Qualitative Evaluation on Standard Test Images

To facilitate a comparison with existing steganographic methods and to provide a qualitative assessment of perceptual reliability, we present visual results from three standard test images widely used in the steganography literature: Barbara, Cameraman, and Baboon. These images were selected because they exhibit distinct textural characteristics, Barbara contains fine periodic patterns, Cameraman features smooth gradients and edge structures, and Baboon is characterized by high-frequency texture and complex details. Evaluating the proposed method on such diverse content allows for a comprehensive assessment of its perceptual impact across different image types.

For this experiment, we embedded a random binary message into each test image using the proposed adaptive code-controlled method with $QF_{traget} = 50$. The embedding was performed in the Y channel (only channel for the case of grayscale images) with an 8 × 8 block size, resulting in an embedding capacity of 1/64 bit per pixel. The original images, their stego versions after embedding, and the corresponding difference maps are presented in Figure 9.

As observed in Figure 9, the differences between the original and stego-images are visually imperceptible to the human eye across all three test images. The difference maps reveal that the embedding modifications are spatially distributed and exhibit block-wise variation in intensity, which is a direct consequence of the proposed adaptive energy selection mechanism. Notably, regions with complex textures, such as the baboon's fur and the patterned fabric in Barbara, receive stronger embedding energy due to their higher robustness characteristics, whereas smooth regions, such as the sky in Cameraman, receive weaker modifications to preserve perceptual quality.

To quantify the perceptual impact, we computed the PSNR values for each stego-image: Barbara achieved 50.8 dB, Cameraman achieved 50.7 dB, and Baboon achieved 49.4 dB. These values are close to 50 dB for all test images, which is generally considered an excellent level of perceptual quality, indicating virtually indistinguishable differences from the original images. These results confirm that the proposed adaptive method maintains high visual reliability across diverse image content.

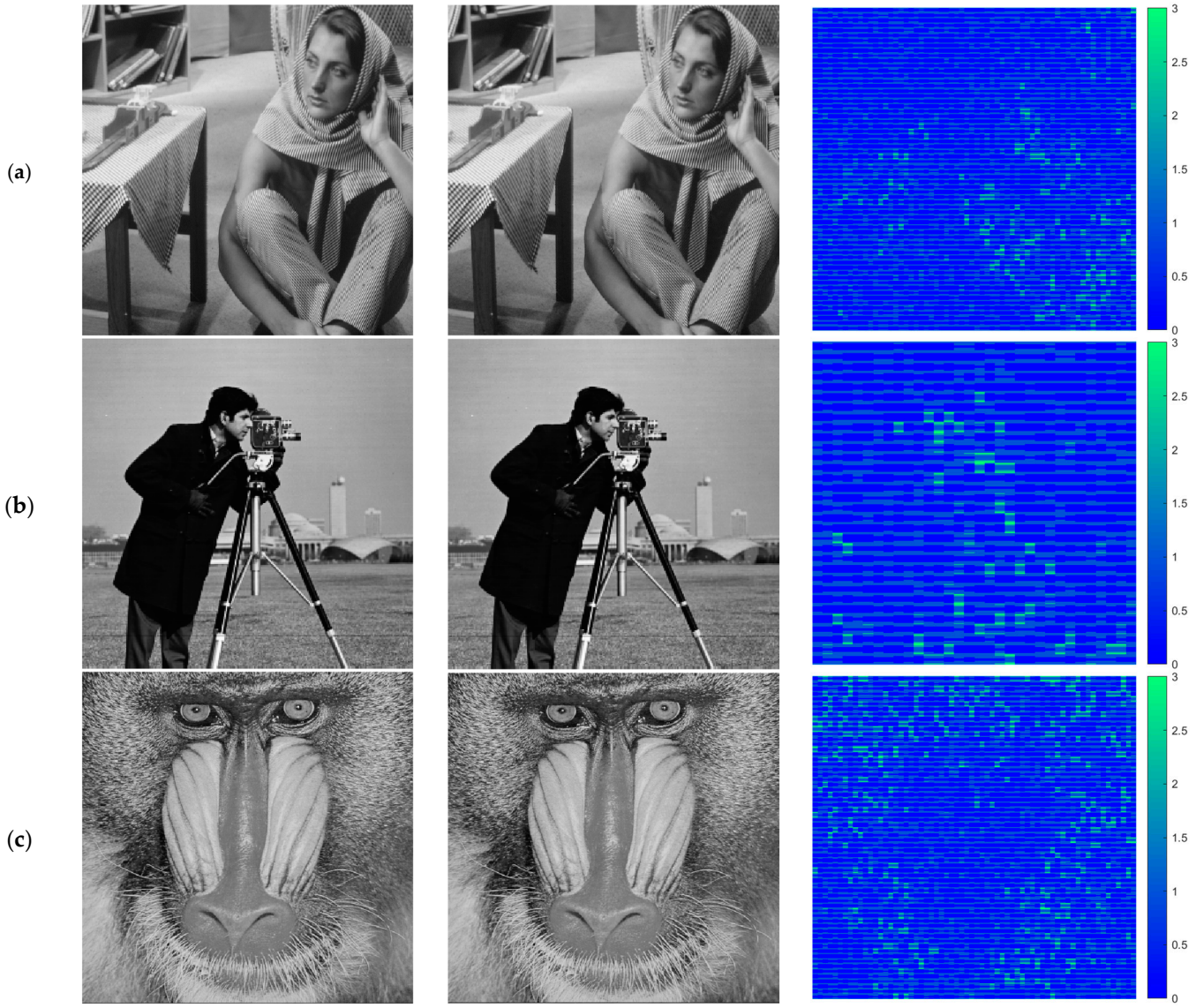


Figure 9. Visual comparison on standard test images. From left to right: original image, stego-image after adaptive embedding ($QF_{target} = 50$), and difference map. Rows: (**a**) Barbara, (**b**) Cameraman, (**c**) Baboon.

For completeness, we also evaluated the robustness of the embedded message against JPEG compression attack on these test images. The results demonstrate consistent robustness for $QF_{target} = 50$. At the commonly used compression level of $QF = 70$, the bit error rates are 1.3% for Barbara, 1.6% for Cameraman, and 3.8% for Baboon, confirming reliable message recovery under realistic transmission conditions. Slightly higher error rates observed for Baboon at low quality factors can be attributed to its high-frequency content, which is more susceptible to compression artifacts. Nevertheless, the overall performance confirms the reliability of the proposed method across diverse image types.

While the primary experimental evaluation in this study is conducted on the NRCS dataset, which consists of natural landscape images, we have supplemented our analysis with results from three standard test images (Barbara, Cameraman, Baboon) that exhibit diverse textural characteristics. The consistent performance across these distinct image types provides preliminary evidence that the proposed adaptive method generalizes beyond a single image domain. Nevertheless, a comprehensive investigation across more specialized

image categories, such as medical images or AI-generated content, remains an important direction for future work.

4. Discussion

4.1. Comparative Analysis and Practical Implications

To provide a comprehensive evaluation of the proposed adaptive steganographic method, this section presents a comparative analysis with several well-known and widely used steganographic techniques reported in the literature. The comparison is focused on key performance criteria that are essential for practical steganographic systems, including robustness against compression attacks, perceptual reliability, and embedding capacity. The selected reference methods represent different embedding paradigms and are commonly used as baselines in steganographic research, which allows for an objective assessment of the proposed approach. The quantitative results of this comparison are summarized in Table 3 and discussed in detail below.

Table 3. The results of the comparative analysis of the proposed adaptive steganographic method with the best-known analogs.

Algorithm/Method	% of Errors at a Given Level of *QF*										PSNR, dB	R	Domain
	10	20	30	40	50	60	70	80	90	100			
Proposed adaptive steganographic method													
$QF_{target} = 50$	43.48	36.23	30.33	20.41	1.25	1	0.65	0.4	0.04	0	52.07	1/64	S
$QF_{target} = 20$	40.21	6.6	4.21	2.8	2.04	1.27	0.77	0.35	0.03	0	47.7	1/64	S
Steganographic method with code control of additional information embedding [28]													
$T_{(5,1)}$	41.63	29.2	14.93	5.98	3.11	2.03	0.84	0.34	0.04	0	48.1	1/64	S
$T_{(5,4)}$	50	50	49.04	45.56	40.56	29.90	5.60	0.70	0	0	48.1	1/64	S
Modern analogs													
Li, 2021, [27]	—	—	0.02	—	0.02	—	0.01	—	0.01	0.01	~27.1	0.01	NN
Wang, 2021, [8]	—	—	0	—	0	—	—	0	—	0	~38.5	0.01	DCT
Zhu, 2019, [9]	—	—	—	—	—	—	33.9	7.4	0.3	—	~45	<1/8	DCT
Chanu, 2014, [17]	—	—	—	—	23.88	14.1	2.76	0.08	0.08	—	~32.7	1/16	SVD
Melnik, 2012, [19]	13	7	5	4	2	2	2	2	2	—	~34.7	1/64	SVD
Chang, 2007, [18]	—	—	—	—	24.7	14.4	2.71	0.2	0.1	—	~32.7	1/64	SVD

The comparative analysis presented in Table 3 demonstrates the strong performance of code-controlled steganographic methods, which consistently exhibit low error rates and high perceptual reliability. The proposed adaptive steganographic method further enhances these strengths by adjusting the embedding energy according to the robustness of each block. Specifically, when $QF_{target} = 50$, the method is optimized for maximal perceptual realibility while maintaining strong resilience against compression attacks with $QF \geq 50$, ensuring minimal error rates even under significant attack conditions. In contrast, when $QF_{target} = 20$, the adaptive method exhibits phenomenal robustness, surpassing the original code-controlled method in terms of error reduction while still preserving high PSNR values, indicating excellent perceptual quality. Overall, these results highlight that the proposed adaptive approach achieves a superior balance between resistance to steganalysis, robustness against attacks, and reliability of perception, outperforming both classical code-controlled methods and modern analogs across multiple metrics.

To provide a broader perspective on the positioning of the proposed method within the landscape of modern steganographic techniques, Table 4 presents a comparative analysis structured by embedding domains. Unlike the detailed numerical comparison in Table 3, which focuses on quantitative performance metrics under specific attack conditions, Table 4 offers a qualitative overview of the principal advantages and limitations inherent to each methodological family. This complementary view helps to illustrate the trade-offs that steganographic systems must navigate, balancing robustness, perceptual quality, computational efficiency, and embedding capacity, and highlights how the proposed adaptive code-controlled method occupies a distinct and advantageous position within this design space.

Table 4. Comparative overview of methodological families in steganography and positioning of the proposed adaptive code-controlled method.

Domain	Representative Methods	Key Advantages	Key Limitations	Robustness to JPEG	Perceptual Quality (PSNR, dB)	Capacity (bpp)
DCT-based	[4–9]	Good robustness to JPEG compression; exploitation of frequency-domain energy compaction; well-established theoretical foundation	Moderate computational complexity; block artifacts may appear at high embedding strength; careful coefficient selection required	High (BER ~0% at QF $\geq$ 70)	~38–45	~0.01–0.1
DWT-based	[10–12]	Multi-resolution analysis; good spatial-frequency localization; robust to various signal processing operations	Higher computational complexity due to multi-level decomposition; parameter tuning required	Moderate to High	~40–48	~0.01–0.05
SVD-based	[13–19]	Excellent numerical stability; good resistance to geometric attacks; singular values are robust to perturbations	High computational complexity for large-scale images due to matrix decomposition; potential reconstruction artifacts; sensitivity to improper modification of singular values, leading to visual degradation	Moderate (BER ~2–24% at QF = 50)	~35–45	~0.015–0.06
Arnold Transform-based	[20,21]	Enhanced security via pixel scrambling; improved resistance to statistical detection	Typically combined with other transforms; scrambling alone does not ensure robustness; an additional embedding step is required	Moderate	~38–42	~0.01–0.03
Spatial-domain	[22–25]	Low computational complexity; direct pixel manipulation; suitable for real-time and IoT applications	Low robustness to compression and filtering; vulnerable to statistical steganalysis	Low to Moderate	~45–52	up to 0.1–0.5 (highly detectable at the upper bound)
AI-based (GAN, NN)	[26,27]	Adaptive embedding; excellent imperceptibility; potential for learning-based optimization	High computational resources required; limited real-time applicability; training data dependency	Moderate to High	~40–55	~0.01–0.1
Code-controlled	[28–30]	Combines spatial efficiency with spectral control; balanced robustness and speed; blind decoding support	Fixed block size limits capacity; requires codeword precomputation	High (BER ~3.11% at QF = 50)	~48–52	$1/64 \approx 0.0156$

Table 4. *Cont.*

Domain	Representative Methods	Key Advantages	Key Limitations	Robustness to JPEG	Perceptual Quality (PSNR, dB)	Capacity (bpp)
Proposed Adaptive Code-controlled	This work	Block-wise adaptive energy selection; superior robustness–imperceptibility trade-off; fast extraction; strong steganalysis resistance	Increased embedding time compared to non-adaptive version; target QF must be predefined	Very High (BER ~1.25% at QF = 50; 6.6% at QF = 20)	47.7–54.15	$1/64 \approx 0.0156$

The comparative analysis presented in Tables 3 and 4 highlights several important observations. First, transform-domain methods (DCT, DWT, SVD) generally offer good robustness to JPEG compression but often at the cost of higher computational complexity and, in some cases, moderate perceptual quality. For instance, SVD-based methods achieve PSNR values around 35–45 dB, which is noticeably lower than the 47.7–54.15 dB range achieved by the proposed adaptive method. Second, traditional spatial-domain methods provide excellent computational efficiency and high PSNR but suffer from poor robustness under compression attacks. Third, while AI-based methods demonstrate promising adaptive capabilities, their practical deployment is constrained by high computational demands and the need for extensive training data.

The code-controlled steganographic family, including the proposed adaptive method, occupies a unique position in this landscape. By operating in the spatial domain while exerting spectral control via structured codewords, these methods achieve a compelling balance: they combine the low extraction complexity of spatial methods with robustness approaching that of transform-domain techniques. The proposed adaptive extension further enhances this balance by introducing block-wise energy selection, which reduces unnecessary distortions in robust blocks while reinforcing embedding in vulnerable regions. As a result, the proposed method achieves up to 22.68% reduction in bit error rate compared to the classical code-controlled method under strong compression (QF = 20), while maintaining PSNR values above 47 dB, a level of perceptual quality that is competitive with or superior to most transform-domain alternatives.

4.2. The Role of Cover Image in Steganographic System Design

In any steganographic system, the cover image (or container) plays a fundamental role that extends beyond merely serving as a carrier for hidden information. The selection and characteristics of the cover image directly influence the achievable trade-offs between the three core criteria of steganography: reliability of perception, robustness, and capacity. From a signal processing perspective, the cover image defines the available "embedding space" and determines how modifications will be perceived by the human visual system or detected by steganalysis tools.

Natural images possess inherent statistical properties that steganographic methods must preserve to remain undetectable. For instance, smooth regions with gradual intensity variations are highly sensitive to any modification, as even minor pixel changes can introduce visible artifacts. Conversely, textured regions with high-frequency content can accommodate stronger embedding without perceptible distortion due to the masking effect of the human visual system. This property is exploited in the proposed adaptive method through block-wise robustness assessment, which identifies regions that can tolerate higher embedding energy.

The choice of cover image also affects robustness against compression attacks. Images with rich textures and high-frequency components tend to retain more of their structural

information after JPEG compression, whereas smooth images are more susceptible to quality degradation. In the proposed adaptive framework, this relationship is captured by the robustness functional $R(B_i)$, which is evaluated experimentally for each block to determine the minimal codeword energy required for reliable extraction under a predefined target compression level.

Moreover, the cover image determines the maximum achievable embedding capacity. In the proposed block-based method, capacity is directly tied to the number of available blocks and the block size. However, not all blocks are equally suitable for embedding; some may require excessive energy to achieve robustness, potentially compromising imperceptibility. The adaptive approach addresses this by selecting the minimal necessary energy for each block, effectively optimizing the use of the available embedding space.

In the experimental evaluation, we employed a diverse set of 530 images from the NRCS database to ensure that the proposed method's performance is not biased toward specific image characteristics. Additionally, we presented results from standard test images (Barbara, Cameraman, Baboon) with distinct textural properties to demonstrate the method's consistent behavior across different cover types. The results confirm that the adaptive strategy successfully accounts for cover image variability, maintaining high perceptual reliability and robustness regardless of the underlying image structure.

4.3. Generalizability to Specialized Image Domains

While the experimental validation in this study is primarily based on natural images from the NRCS database, the proposed adaptive code-controlled method is not inherently limited to this domain. Understanding its performance on other image types, such as medical images, satellite imagery, or AI-generated content, is important for assessing its practical applicability across diverse real-world scenarios.

Medical images, for instance, present unique challenges for steganography. In applications such as secure transmission of patient data or digital watermarking for tamper detection, preserving diagnostically relevant features is paramount. The proposed method's adaptive energy selection mechanism, which minimizes embedding distortion by allocating energy only where necessary, is particularly well-suited to such sensitive applications. The block-wise robustness assessment ensures that modifications are concentrated in regions that can tolerate them without compromising diagnostic quality. Preliminary evidence from our experiments on images with varying texture complexity (e.g., smooth gradients in Cameraman, high-frequency details in Baboon) suggests that the method successfully adapts to different structural characteristics, which bodes well for its applicability to medical imagery.

AI-generated content represents another emerging domain where steganographic methods may find application, for example, in provenance tracking or content authentication of synthetic media. However, the statistical properties of AI-generated images differ from those of natural photographs, which may affect both the imperceptibility of embedding and the robustness of extraction. The proposed method's reliance on block-wise robustness assessment, which is determined experimentally for each image, offers a degree of automatic adaptation to the specific characteristics of the input data. Nevertheless, the systematic evaluation of AI-generated datasets remains an open question and constitutes a promising direction for future research.

In summary, while the current study establishes the effectiveness of the proposed adaptive method on natural images, its application to specialized domains, while conceptually feasible, requires dedicated investigation. We hope that the discussion provided here will serve as a foundation for such future work.

5. Conclusions

This paper has presented and thoroughly investigated an adaptive code-controlled steganographic method aimed at improving the robustness of embedded information while preserving high perceptual reliability and acceptable computational efficiency. Unlike conventional spatial-domain and transform-domain approaches, the proposed method successfully combines their key advantages by enabling spectrally controlled embedding within the spatial domain, without explicit transformation of the container.

The core contribution of the proposed approach lies in the adaptive selection of codeword energy at the block level, based on the robustness characteristics of individual image blocks. This strategy eliminates the inefficiency of uniform embedding and enables stronger embedding in vulnerable regions while minimizing unnecessary distortions in structurally robust areas. As a result, the proposed method achieves a significantly improved trade-off between imperceptibility and robustness compared to the classical code-controlled steganographic scheme.

Extensive experimental evaluation on large image datasets confirms the effectiveness of the proposed adaptive method. The results demonstrate a substantial reduction in bit error rate under JPEG compression attacks, particularly in scenarios involving strong compression, while maintaining PSNR values that correspond to visually imperceptible distortions. In several attack regimes, the proposed adaptive approach significantly outperforms the classical code-controlled method.

For moderate compression attacks (QF = 50), it achieves a bit error rate as low as 1.25% while maintaining a high perceptual quality of 52.07 dB PSNR. Under stronger attack conditions (QF = 20), the method preserves robustness with 6.6% bit errors at 47.7 dB PSNR.

Overall, adaptive energy selection provides up to 22.68% fewer errors or up to 6.05 dB higher PSNR compared to the classical code-controlled steganographic method, demonstrating its practical effectiveness in attack-resilient communication scenarios.

A key outcome of this research is the high resistance of the proposed method to statistical steganalysis. Experimental analysis using RS steganalysis, calibrated χ^2 analysis, Simple Pair Analysis, and the StegExpose framework shows that the adaptive method remains largely undetectable even under deliberately unfavorable embedding conditions. These results indicate that the proposed scheme preserves the fundamental statistical properties of the container, making classical and practical steganalytic techniques ineffective.

From a computational perspective, although the adaptive embedding procedure increases the overall embedding time, the extraction process remains extremely fast, which is a critical advantage for resource-constrained receivers. This asymmetry between embedding and extraction complexity makes the method particularly suitable for practical applications where decoding efficiency is essential.

In summary, the results obtained in this work demonstrate that adaptive code-controlled steganography represents a promising and practically viable direction for modern information hiding systems. By jointly achieving high robustness, strong resistance to steganalysis, and excellent perceptual reliability, the proposed approach outperforms both classical code-controlled methods and several state-of-the-art alternatives.

It should be noted, however, that the experimental evaluation in this study primarily focuses on JPEG compression attacks, which constitute the most common and practically relevant distortion in modern digital communication channels. Other types of distortions, such as additive noise, filtering, cropping, rotation, and scaling, while important in certain scenarios, were not systematically evaluated within the scope of this work.

Future research directions include automatic robustness estimation using machine learning techniques, extension of the adaptive framework to video and audio containers, and further optimization of the embedding strategy for diverse attack models and real-time

communication scenarios, as well as a comprehensive investigation of robustness against a broader range of signal processing operations and geometric distortions and systematic evaluation of the proposed method on specialized image domains, including medical images and AI-generated content.

It is important to note that the experimental validation presented in this study is limited to still images, which represent a fundamental container type in steganography. While the proposed adaptive code-controlled method is conceptually generalizable to other media types, such as video and audio, this extension requires careful consideration of the specific characteristics of each medium. For video, the method can be applied on a frame-by-frame basis, with additional constraints to ensure temporal consistency and avoid flickering artifacts. For audio, the one-dimensional Walsh–Hadamard transform can be employed, with codewords designed to target perceptually significant frequency components in the audio spectrum. These extensions, however, lie beyond the scope of the present work and are left for future investigation.

Author Contributions: Conceptualization, A.S. and N.K.; methodology, D.Y.; software, A.S. and K.M.; validation, A.S., N.K. and B.S.; formal analysis, A.S. and R.S.; investigation, N.K. and K.M.; resources, A.S.; data curation, R.S. and K.M.; writing—original draft preparation, A.S.; writing—review and editing, A.S. and R.S.; visualization, B.S.; supervision, N.K.; project administration, A.S.; funding acquisition, R.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding authors.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

DCT	Discrete Cosine Transform
SVD	Singular Value Decomposition
JPEG	Joint Photographic Experts Group
QF	JPEG Quality Factor
PSNR	Peak Signal-to-Noise Ratio
IoT	Internet of Things
SSIM	Structural Similarity Index Measure
MSE	Mean Squared Error
IWT	Integer Wavelet Transform
DWT	Discrete Wavelet Transform
QIM	Quantization Index Modulation
DTCWT	Dual-Tree Complex Wavelet Transforms
CNN	Convolutional Neural Network
ILWT	Integer Lifting Wavelet Transform
GAN	Generative Adversarial Networks
LSB	Least Significant Bit
WHT	Walsh–Hadamard Transform
BER	Bit Error Rate
SPA	Simple Pair Analysis

References

1. Apau, R.; Asante, M.; Twum, F.; Hayfron-Acquah, J.B.; Peasah, K.O. Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review. *PLoS ONE* **2024**, *19*, e0308807. [CrossRef] [PubMed]

2. Abdulla, A.A. Digital image steganography: Challenges, investigation, and recommendation for the future direction. *Soft Comput.* **2024**, *28*, 8963–8976. [CrossRef]
3. Yahya, A. *Steganography Techniques for Digital Images*; Springer: Berlin/Heidelberg, Germany, 2018; 122p. Available online: https://link.springer.com/book/10.1007/978-3-319-78597-4 (accessed on 10 March 2026).
4. Ramyashree; Venugopala, P.S.; Raghavendra, S.; Kubihal, V.S. Enhancing secure medical data communication through integration of LSB and DCT for robust analysis in image steganography. *IEEE Access* **2024**, *13*, 1566–1580. [CrossRef]
5. Al Ali, I.A.J.; Abdulazeez, Z.A.; Aljubouri, R.M. JPEG-Resistant DCT Steganography for Secure Communication. *Fusion Pract. Appl.* **2026**, *21*, 245–264.
6. Jiao, Y.; Zhang, Z.; Yang, X.; Li, Y.; Mei, F.; Li, Z. A robust coverless image steganography based on DCT-SVD. In *Proceedings of the 3rd International Conference on Computer Science and Blockchain (CCSB), Shenzhen, China, 17–19 November 2023*; IEEE: New York, NY, USA, 2023; pp. 59–63. Available online: https://ieeexplore.ieee.org/document/10398826 (accessed on 10 March 2026).
7. Lan, Y.; Shang, F.; Yang, J.; Kang, X.; Li, E. Robust image steganography: Hiding messages in frequency coefficients. *Proc. AAAI Conf. Artif. Intell.* **2023**, *37*, 14955–14963. [CrossRef]
8. Wang, S.; Zheng, N.; Xu, M. A Compression Resistant Steganography Based on Differential Manchester Code. *Symmetry* **2021**, *13*, 345. [CrossRef]
9. Zhu, Z.; Zheng, N.; Qiao, T.; Xu, M. Robust Steganography by Modifying Sign of DCT Coefficients. *IEEE Access* **2019**, *7*, 168613–168628. [CrossRef]
10. Durafe, A.; Patidar, V. Development and analysis of IWT-SVD and DWT-SVD steganography using fractal cover. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 4483–4498. [CrossRef]
11. Pramanik, S. An adaptive image steganography approach depending on integer wavelet transform and genetic algorithm. *Multimed. Tools Appl.* **2023**, *82*, 34287–34319. [CrossRef]
12. El-den, B.M.; Raslan, W. A reversible and robust hybrid image steganography framework using radon transform and integer lifting wavelet transform. *Sci. Rep.* **2025**, *15*, 15687. [CrossRef]
13. Liu, J.; Song, X.; Li, G.; Han, K. Robust JPEG image steganography using wavelet domain SVD and adaptive QIM. In *Proceedings of the 8th International Conference on Signal and Image Processing (ICSIP), Wuxi, China, 8–10 July 2023*; IEEE: New York, NY, USA, 2023; pp. 434–438. Available online: https://ieeexplore.ieee.org/document/10270839 (accessed on 10 March 2026).
14. Khandelwal, J.; Sharma, V.K. Extensive dual tree complex wavelet transform-based image steganography using SVD and CNN subspace. *J. Discret. Math. Sci. Cryptogr.* **2023**, *26*, 617–627. [CrossRef]
15. Teoh, Y.J.; Ling, H.C.; Wong, W.K.; Basuki, T.A. A hybrid SVD-based image watermarking scheme utilizing both U and V orthogonal vectors for robustness and imperceptibility. *IEEE Access* **2023**, *11*, 51018–51031. [CrossRef]
16. Kumari, M.R.R.; Kumar, V.V.; Naidu, K.R. Digital image watermarking using DWT-SVD with enhanced tunicate swarm optimization algorithm. *Multimed. Tools Appl.* **2023**, *82*, 28259–28279. [CrossRef]
17. Chanu, Y.J.; Singh, K.M.; Tuithung, T. A Robust Steganographic Method based on Singular Value Decomposition. *Int. J. Inf. Comput. Technol.* **2014**, *4*, 717–726.
18. Chang, C.C.; Lin, C.C.; Hu, Y.S. An SVD oriented watermark embedding scheme with high qualities for the restored images. *Int. J. Innov. Comput. Inf. Control* **2007**, *3*, 609–620.
19. Melnik, M.A. Compression-resistant steganographic algorithm. *Inf. Secur.* **2012**, *2*, 99–106.
20. Pattanayak, S.; Samanta, S.; Dey, D.; Sarkar, A.; Bhattacharyya, S. An Image Steganography Approach Using Arnold Transformation. In *Novel Research and Development Approaches in Heterogeneous Systems and Algorithms*; IGI Global: Hershey, PA, USA, 2023; pp. 217–235. Available online: https://www.irma-international.org/viewtitle/320132/?isxn=9781668475249 (accessed on 10 March 2026).
21. Nipanikar, S.; Nipanikar, R.; Kulkarni, M. Steganography in Colour Images with Proposed Arnold Chaotic Map and Optimized Curvelet Transform. In *Information and Communication Technology for Competitive Strategies (ICTCS 2022)*; Intelligent Strategies for ICT; Springer Nature: Singapore, 2023; pp. 297–310. Available online: https://link.springer.com/chapter/10.1007/978-981-19-9304-6_29 (accessed on 10 March 2026).
22. Septinaputri, G.S.; D'Layla, A.W.C.; De La Croix, N.J.; Ahmad, T. Enhanced Spatial Domain Image Steganography for Improved IoT Security and Privacy Applications. In *Proceedings of the IEEE 21st International Conference on Mobile Ad-Hoc and Smart Systems (MASS), Seoul, Republic of Korea, 23–25 September 2024*; IEEE: New York, NY, USA, 2024; pp. 635–640. Available online: https://ieeexplore.ieee.org/document/10723401 (accessed on 10 March 2026).
23. Milosav, P.; Milosavljević, M.; Banjac, Z. Steganographic method in selected areas of the stego-carrier in the spatial domain. *Symmetry* **2023**, *15*, 1015. [CrossRef]
24. Sulong, G.B.; Wimmer, M.A. Image hiding by using spatial domain steganography. *Wasit J. Comput. Math. Sci.* **2023**, *2*, 25–29. [CrossRef]

25. Wahono, D.; Rahman, H.; Syarif, H.; De La Croix, N.J.; Ahmad, T. Enhancing Data Security Using Steganography in Spatial Domain Images. In *Proceedings of the Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE), Vellore, India, 22–23 February 2024*; IEEE: New York, NY, USA, 2024; pp. 1–6. Available online: https://ieeexplore.ieee.org/document/10493831 (accessed on 10 March 2026).
26. Sushma, R.B.; Manjula, G.R.; Belavagi, M. A Mellin transform based video steganography with improved resistance to deep learning steganalysis for next generation networks. *MethodsX* **2024**, *13*, 102887. [CrossRef] [PubMed]
27. Li, Z.; Zhang, M.; Liu, J. Robust image steganography framework based on generative adversarial network. *J. Electron. Imaging* **2021**, *30*, 023006. [CrossRef]
28. Kobozeva, A.A.; Sokolov, A.V. Robust Steganographic Method with Code-Controlled Information Embedding. *Probl. Energeticii Reg.* **2021**, *4*, 115–130. [CrossRef]
29. Kobozeva, A.A.; Sokolov, A.V. Steganographic Method with Code Control of Information Embedding Based on Multi-level Code Words. *Radioelectron. Commun. Syst.* **2023**, *66*, 173–189. [CrossRef]
30. 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. *Probl. Reg. Energetics* **2024**, *62*, 121–137. [CrossRef]
31. Ahmed, N.; Rao, K.R. *Walsh-Hadamard Transform, Orthogonal Transforms for Digital Signal Processing*; Springer: Berlin/Heidelberg, Germany, 1975; pp. 99–152. Available online: https://ieeexplore.ieee.org/document/4309466 (accessed on 10 March 2026).
32. 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. *Probl. Energeticii Reg.* **2022**, *54*, 84–100. [CrossRef]
33. Ahmed, N.; Natarajan, T.; Rao, K.R. Discrete cosine transform. *IEEE Trans. Comput.* **2006**, *100*, 90–93. [CrossRef]
34. Kobozeva, A.A.; Sokolov, A.V. Efficient Coding of the Embedded Signal in Steganographic Systems with Multiple Access. *Probl. Energeticii Reg.* **2021**, *2*, 101–113. [CrossRef]
35. Natural Resources Conservation Service (NRCS), United States Department of Agriculture. Available online: https://www.nrcs.usda.gov (accessed on 10 March 2026).
36. Lanovska, O.O.; Sokolov, A.V. Steganalysis of a method with code-controlled information embedding in the Walsh-Hadamard transform domain. *Inform. Math. Methods Simul.* **2024**, *14*, 273–283.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.