mathematics

MDPI

Article

A Novel Reversible Image Camouflaging Method Based on Lossless Matrix Transformation

Gizem Dursun Demir and Ufuk Özkaya *

Department of Electrical-Electronics Engineering, Süleyman Demirel University, Isparta 32260, Türkiye; gizemdursun@sdu.edu.tr
* Correspondence: ufukozkaya@sdu.edu.tr

Abstract

Image encryption methods aim to transform a secret image into a noise-like, texture-like image. Since this behavior of the encrypted image indicates that it is encrypted, it provokes a large number of attacks. One of the most effective methods to counter this threat is to protect the information by transforming the original image into a new, meaningful image. The bottleneck of this approach is that the new image in which the information is embedded must have a high visual quality that is indistinguishable from the real image. Another critical requirement is obtaining the original image without loss. In this paper, we propose a reversible image camouflage method based on lossless matrix transformation and two-dimensional wavelet transformation. Random matrix perturbation is introduced and applied as an effective method for the lossless transformation of low-frequency or flat regions. The proposed method was applied to different datasets for performance analysis. The PSNR values of the plain/camouflage image pair are above 55 dB, and the SSIM values obtained by our method are very close to 0.9999 on these datasets. The experimental results demonstrate that the method's performance is independent of the content of the plain/target image and of the fragment size. Furthermore, in cases where the target image is specifically chosen, PSNR values exceed 58 dB. Additionally, the efficacy of the method in generating camouflage images has been demonstrated through histogram analysis and performance analysis in the low- and high-frequency regions.

Keywords: image camouflaging; matrix perturbation; wavelet transform

MSC: 94A08

1. Introduction

With the rapid advancement of multimedia technologies and cloud computing, data transmission and storage have gained significant importance for individuals and organizations. The security of sensitive data, such as confidential documents, medical and military images, and multimedia files that contain personal information, remains a major concern. To address the risks of unauthorized access and modification, researchers have introduced various security mechanisms. In particular, image encryption and data hiding techniques have been widely adopted as effective methods to protect information from interception and alteration.

Image encryption transforms a meaningful image into an encoded, noise-like format using a secret key, ensuring that only authorized users can decrypt and recover the original image. Various encryption techniques, such as Advanced Encryption Standard (AES) [1], chaotic systems [2,3], Fibonacci transformations [4], substitution-permutation networks

Check for updates

Academic Editor: Gintautas Dzemyda

Received: 4 February 2026
Revised: 20 March 2026
Accepted: 24 March 2026
Published: 26 March 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.

(SPNs) [5], DNA encoding [6,7], and neural networks [8,9] have been widely employed for this purpose. All these encryption methodologies mentioned transform the original image into a noise- or texture-like encrypted image by modifying pixel values and/or positions through specific mathematical models and operators. Consequently, these methodologies have the capacity to guarantee the secure transmission or protection of images. However, the fact that the encrypted image exhibits noise or texture-like behavior makes it readily distinguishable from meaningful images. This visual anomaly improves the detectability of the image for potential attackers, exposing it to a range of attacks and analyses that could compromise information security.

In order to overcome this drawback inherent in image encryption methods, image camouflage methods have been proposed as an alternative approach. Unlike image encryption methods, image camouflage methods transform a secret image into another meaningful image (camouflage image), whilst still prioritizing information security. A highly secure image camouflage method must ensure that the generated camouflage image contains minimal distortion and that the original image can be recovered from the camouflage image without loss or with minimal loss. In this regard, a number of image camouflage algorithms have been proposed to date. Mosaic-based image transformation techniques have evolved from database-dependent searches to autonomous color transformation schemes. Early methods, such as those proposed by Lai and Tsai [10], used secret-fragment-visible mosaic images and a greedy search algorithm that matched tile images based on a one-dimensional color scale conversion. However, these initial approaches were limited by the need for a large target image database to ensure security performance. To address this limitation, subsequent research [11] introduced methods for nearly reversible color transformation. This evolution enabled secret fragments to be transformed into any user-selected target image without the need for external databases. However, this approach necessitated a trade-off between tile size and reversibility performance.

To overcome the irreversibility of earlier mosaic-based schemes, recent research has shifted towards reversible image transformation (RIT) and camouflage methods. Hou et al. [12] and Zhang et al. [13] introduced frameworks that ensure full reversibility by employing clustering techniques, such as K-means and mean-shift, for block matching. While these methods significantly enhance visual quality, there is often a trade-off where minimizing block size to ensure lossless recovery results in an excessive increase in auxiliary data hiding capacity. Further refinements have integrated color difference channel transformations and prediction error expansion [14] to optimize visual output. However, managing the overhead of supplementary information remains a critical challenge in these concealment models [12,14].

To improve visual quality and matching efficiency further, image camouflage frameworks have been integrated with non-uniform clustering algorithms [15] and energy-function-based statistical features [16]. These advancements enable more precise block matching between the secret and target images, resulting in superior visual fidelity in the camouflaged and recovered outputs. Alongside these structural improvements, research has also focused on optimizing the embedding process to minimize auxiliary data. For example, reversible data hiding (RDH) combined with pixel shifting [17] and singular value decomposition (SVD)-based color transformations [18] have been used to protect the transformation parameters. By shifting from basic color scales to multidimensional feature sets and decomposition methods, these techniques aim to strike a balance between concealment quality and the volume of recovery information.

Visually meaningful encrypted images (VMEIs) have emerged as an alternative to noise-like ciphertext. They aim to generate encrypted images that retain the visual characteristics of a meaningful cover image [19]. The VMEI framework generally involves a

two-stage process: first, the secret image is pre-encrypted, and then data is embedded into a cover image [20]. The security and efficiency of VMEI have advanced through various pre-encryption techniques, ranging from simple pixel permutation [20,21] to robust 3D chaotic cat maps [22] and special encryption processes [23], which can also be scaled for multiple secret images [24]. In the data embedding stage, most work exploits the frequency domain by employing transformations such as the discrete wavelet transform (DWT) [21], lifting wavelet transform (LWT) [22,23], or Haar wavelet transform [20], placing hidden data in specific sub-bands. This approach focuses on computational efficiency [21] and incorporates human visual system models [23] to improve the visual fidelity of the resulting camouflaged image.

A persistent challenge for image embedding models is their limited capacity for data embedding; this has led to the development of various capacity optimization strategies. Recent developments include universal embedding models [25] that demonstrate superior performance in low-frequency flat regions and 2D compressive sensing methods [26] that are designed to maximize load while reducing storage and transmission bandwidth. To mitigate the visual degradation associated with fixed embedding, adaptive schemes based on texture analysis and information entropy [27] have emerged; however, these typically incur higher computational costs. Furthermore, multi-image embedding systems [28] have been developed to overcome capacity bottlenecks by processing multiple plaintext images simultaneously, effectively eliminating the need for main image data during decoding. Together, these methods represent a shift towards balancing computational efficiency and visual security with high-capacity embedding.

As previously stated, the concept of converting a hidden meaningful image into another meaningful image is intended to address the limitations and security risks of conventional image encryption methodologies. The methods proposed to date have significant limitations. Despite the implementation of extensive block-matching steps, mosaic image generation methods are unable to obtain the original image without loss. However, it should be noted that the efficacy of reversible data hiding methods is contingent upon the block (fragment) size. Decreasing the block size to achieve improved visual outcomes increases computational complexity. Furthermore, in certain instances, the disparities in the processing inherent in each block may result in the emergence of slight boundaries between them. The proposed VMEI methods are characterized by their inherent limited data embedding capacity. The proposed models to address this challenge result in an increase in the computational complexity of the methods, thereby restricting their effective use in real-time applications. Despite the recent proposal of numerous image camouflage and visually meaningful image transformation methods, the majority of extant approaches rely on block matching strategies or complex embedding procedures to preserve visual consistency between images. It is frequently observed that such techniques are characterized by two principal limitations. Firstly, these techniques are often accompanied by high computational complexity. Secondly, the techniques exhibit limited embedding flexibility.

In this work, we propose a novel approach by integrating random matrix perturbation into the existing image camouflage framework. The proposed approach diverges from conventional methodologies in that it does not seek visually similar blocks. Rather, it constructs a transformation matrix that maps the original image to a distorted target representation. The normalized representation of this matrix is implicitly embedded within the wavelet coefficients of the camouflage image, thereby enabling the recovery of the original image through a matrix inversion process.

To the best of our knowledge, the integration of random matrix perturbation with wavelet-domain information embedding for meaningful image camouflage has not been previously explored. This design eliminates the necessity for block matching operations

while preserving the capacity to accurately reconstruct the original image. It is therefore evident that the proposed framework provides a novel and computationally efficient alternative to existing camouflage generation methods. This method ensures both the generation of a camouflage image with minimum distortion and lossless recovery of the plain image. The proposed method has the potential to be used in a computationally feasible way for secure offline data transmission. In comparison with state-of-the-art methods, the proposed technique has been shown to yield superior visual outcomes. The main contributions of this work are as follows:

- A transformation matrix was established to bilaterally map the spatial information between the original and the target fragment images. The random matrix perturbation method, which has been demonstrated to achieve lossless transformation even in low-frequency and flat regions of the images, was introduced.
- The transformation data between the original image and the target image has been normalized and embedded into the high-frequency components in a manner that preserves the fidelity of the camouflage image to the target image.
- The proposed method is independent of fragment size. The efficacy of the method is unaffected by fragment size and consistently yields successful visual outcomes.

The rest of this paper is organized as follows. The Section 2 describes the proposed method rigorously. In the Section 3, the experiments, analysis parameters, and the numerical and visual results are represented. These results are also supplemented with comparative analyses and a discussion of the results in Section 4. The Section 5 gives a concise conclusion and overall evaluation of this work.

2. Proposed Method

In this section, the proposed image camouflaging method is explained in a rigorous way. The proposed method generates a camouflage image by transforming a plain image into a target image with minimum distortion. Moreover, the proposed method enables lossless recovery of the original image from the camouflage image. As demonstrated in Figure 1, the proposed methodology comprises two phases. In the first phase, the primary objective is to generate the transformation matrix that facilitates the transformation between the corresponding fragment images of the source and target images. This process ultimately yields the optimal transformation matrix that provides the transformation between the two images. The subsequent phase is the data hiding phase, which involves embedding the transformation matrix and the vector containing the transformation information in the target image. Although the flowchart of the method was represented on a single color channel (represented as a grayscale image) for simplicity, the method is fully compatible with color images. For RGB plain and target images, the transformation is performed concurrently between the corresponding color channels of the plain and target images. Specifically, the R, G, and B channels are processed independently as distinct layers, and the resulting single-channel camouflage components are then combined to create the final color camouflage image.

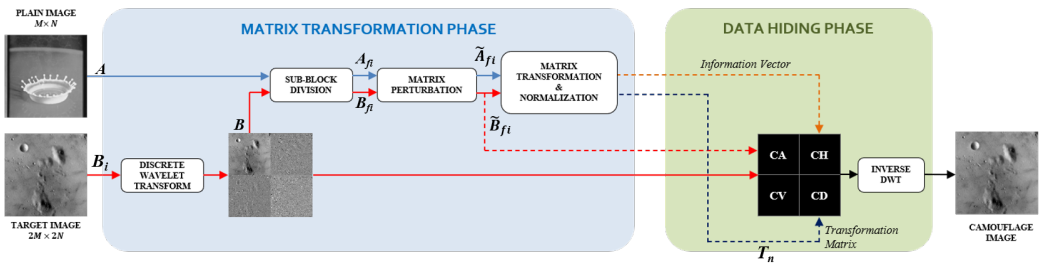


Figure 1. The flowchart of the proposed image camouflaging method for grayscale images.

2.1. Matrix Transformation Phase

In this phase, the main goal is to generate a transformation matrix that provides a lossless bidirectional transformation between a plain image and a target image. Let the plain image (A) and the initial target image (B_i) be grayscale images with the size of $M \times N$ and $2M \times 2N$, respectively. To produce a transformation matrix of the same size as the plain image, an approximate image is obtained by applying a discrete wavelet transform (DWT) to the initial target image. Here, Daubechies 1 (Haar) wavelet was used to get the approximate image. To guarantee optimal reversibility, the integer-to-integer Haar discrete wavelet transform (DWT) was implemented using a lifting scheme. To ensure a fully reversible transformation, an integer-to-integer lifting scheme is used for the DWT. Unlike conventional convolution-based DWTs, the lifting scheme maintains the integrality of both the approximation and detail coefficients by incorporating rounding operations within the lifting steps. This ensures that reconstruction of the secret image remains lossless and free from rounding errors. At the end of this transform process, the approximate image was then assigned as the target image (B).

2.1.1. Sub-Block Division

In the sub-block division step, the plain and target images were divided into non-overlapping square fragment images, called A_f and B_f, respectively. The dimensions of the fragment image can be calculated in accordance with the dimensions of both the original and target images, taking into account the following considerations:

- If the plain and target images are square ($N \times N$), the size of the square fragment images can be calculated as a multiplier of the original image size. Furthermore, in this case, the size of the fragment can be determined to be equivalent to the original image size, thus eliminating the need for a sub-block division process.
- If the plain and target images are rectangular ($M \times N$), the size of the fragment can be determined as the highest common factor (HCF) value of the values of the rows and columns of the images or as a multiplier of the HCF value.

At the end of the sub-block division process, the plain and target images are divided into the same number of square fragment images.

2.1.2. Matrix Perturbation

Following the sub-block division process, the transformation matrix between corresponding fragment images of plain and target images is obtained by Equation (1):

$$B_{f_i} = T_{f_i} A_{f_i},\ i = 1, 2, 3, \ldots, K \tag{1}$$

where, A_{f_i} and B_{f_i} represent ith fragments of the plain and target image, respectively. T_{f_i} is the transformation matrix and K is the number of fragments. In order to transform the A_{f_i} matrix to B_{f_i} and also recover A_{f_i} matrix from B_{f_i} matrix without any loss of information, the T_{f_i} matrix must be invertible. The primary factor that threatens the condition of the transformation matrix being invertible is the presence of low-frequency regions within the fragment images, which exhibit similar pixel behavior. The low-frequency (smooth) regions cause the transformation matrix to be ill-conditioned and result in losses during the image reconstruction phase. Here, to ascertain whether the transformation matrix is ill-conditioned, the condition number of the matrix is calculated as follows (Equation (4)):

$$B_{f_i} = T_{f_i} A_{f_i} \iff T_{f_i} = B_{f_i} A_{f_i}^{-1} \tag{2}$$

$$A_{f_i} = T_{f_i}^{-1} B_{f_i} \iff T_{f_i}^{-1} = A_{f_i} B_{f_i}^{-1} \tag{3}$$

$$\kappa(T_{f_i}) = \|T_{f_i}\|\|T_{f_i}^{-1}\| \tag{4}$$

As seen from Equations (2) and (3), to ensure that the transformation matrix has a low condition number, it is inevitable that the corresponding fragment matrices of both plain and target images must also be invertible matrices with low condition numbers. So, to ensure that the transformation matrix has a low condition number and is thus invertible, both fragment matrices are perturbed using a random noise matrix [29] as follows:

$$\tilde{A}_{f_i} = A_{f_i} + n_1(x, y) \tag{5}$$

$$\tilde{B}_{f_i} = B_{f_i} + n_2(x, y) \tag{6}$$

Here, $n_1(x, y)$ and $n_2(x, y)$ depict the random noise matrices with uniform distribution, the elements of which vary between 0 and 1, added to the fragment matrices. Moreover, given that each fragment image comprising the plain and target images will possess a distinct textural property, employing random matrices generated with a fixed seed will not serve the purpose of lossless transformation. It is therefore essential to generate different noise matrices during the camouflage image generation stage for each fragment pair to ensure lossless recovery of the plain image. Because, these noise matrices ensure that the transformation matrix becomes fully invertible by reducing its condition number.

2.1.3. Matrix Transformation and Normalization

In the final stage of the matrix transformation phase, the transformation matrix is obtained for each pair of perturbed matrices as given in Equation (7):

$$T_{f_i} = \tilde{B}_{f_i}\tilde{A}_{f_i}^{-1} \tag{7}$$

The fragment transformation matrices for each pair of fragment matrices are acquired and concatenated to produce the overall transformation matrix. This transformation matrix is then normalized between [0.1–0.9] to embed it in the approximation image.

2.2. Data Hiding Phase

In this stage, the main goal is the embedding of the transformation matrix within the camouflage image. This provides the original image to the camouflage image with minimum distortion, and then the original image is recovered from the camouflage image without any loss.

The following operations are performed to produce the camouflage image that contains the transformation matrix:

- The perturbed fragment target images are concatenated and, therefore, the perturbed target image ($\tilde{B}$) is produced. The perturbed target image is overwritten with the approximate image (CA).
- The normalized transformation matrix (T_n) is overwritten on the diagonal detail image matrix (CD) according to the following equation:

$$CD(x, y) = CD(x, y) + T_n(x, y) \tag{8}$$

- An information vector including numerical data, such as fragment size, maximum and minimum value of the transformation matrix, is embedded into the horizontal detail image matrix by LSB encoding. The T_{min}, T_{max}, and fragment size values are stored as 64-bit double-precision floating-point scalars. A total of 192 bits are allocated within the information vector and embedded into the least significant bits (LSBs) of the CH sub-band.

- The camouflage image is derived through the implementation of an inverse wavelet transform on the modified target image, after the execution of these sequential operations.

2.3. Recovery of the Plain Image

By means of the processes explained above, the original image is transformed into a meaningful and predefined camouflage image with minimum distortion. On the other hand, a series of processes is employed to ensure the recovery of the original image from the camouflage image without any loss. The operations performed in this step involve the execution of the processes utilized to generate the camouflage image, executed in reverse order. The algorithm for original image recovery is described as follows:

- **Input:** Camouflage image
- **Output:** Original image
- **Step 1:** Discrete wavelet transform is applied to the camouflage image.
- **Step 2:** The perturbed target image ($\tilde{B}$) is extracted from the approximation image (CA).
- **Step 3:** The information vector (includes fragments size, maximum and minimum value of original transformation matrix) is extracted from horizontal detail image (CH).
- **Step 4:** The normalized transformation matrix (T_n) is extracted from the diagonal detail image (CD) by Equation (9):

$$T_n(x,y) = CD(x,y) - \lfloor CD(x,y) \rfloor \tag{9}$$

  where, $\lfloor . \rfloor$ is the floor operator. Then, the normalized matrix is denormalized to the original transformation matrix (T).
- **Step 5:** The perturbed target image and the transformation matrix are both divided into square fragments, with each fragment being of a predefined fragment size in the information vector. Then the perturbed original fragment images are calculated by Equation (10):

$$A_{f_i} = T_{f_i}^{-1} \tilde{B}_{f_i} \tag{10}$$

- **Step 6:** In the subsequent stage of the process, the fragmented images are concatenated in order to obtain the perturbed original image matrix. In the final stage, the original image is obtained by flooring the perturbed image matrix.

In the following section, the numerical and visual results will be presented to demonstrate the efficacy of the proposed method. The datasets utilized, performance analysis metrics, and performance analyses will be presented rigorously.

3. Experimental Results

This section presents the numerical and visual results of the proposed method. The performance of the method is evaluated under various scenarios, and its advantages are highlighted. The method is applied to a collection of color images from various datasets, and the performance of the camouflage image generation and original image recovery is investigated. The created data set comprises both square [30] and rectangular [31] images. Whilst some of the square images were originally of the size of 256×256, 512×512, and 1024×1024, some were obtained by resizing the original rectangular images to these values. For rectangular images, the original size and halved-size versions were utilized.

The proposed method was conducted on the dataset mentioned above, and the root mean square error (RMSE), color peak signal-to-noise ratio (CPSNR), and structural similarity index measure (SSIM) metrics were utilized to evaluate its performance. Furthermore, the computation times for different fragment sizes have been obtained to demonstrate the

method's real-time camouflage image generation and original image recovery times. The values of RMSE, CPSNR, and SSIM are computed as:

$$RMSE = \sqrt{\frac{\sum_{C\in\{R,G,B\}}\sum_{x=1}^{M\times N}(B_i(x)-C_i(x))^2}{3\times M\times N}} \tag{11}$$

$$CPSNR = 10\log_{10}\frac{255^2\times 3\times M\times N}{\sum_{C\in\{R,G,B\}}\sum_{x=1}^{M\times N}(B_i(x)-C_i(x))^2} \tag{12}$$

$$SSIM = \frac{(2\mu_{B_i}\mu_{C_i}+C_1)(2\sigma_{B_iC_i}+C_2)}{(\mu_{B_i}^2+\mu_{C_i}^2+C_1)(\sigma_{B_i}^2+\sigma_{C_i}^2+C_2)} \tag{13}$$

Here, B_i and C_i represent the original target image and the camouflage image, respectively.

SSIM and CPSNR metrics are utilized together to determine the degree to which the generated camouflage image approximates the original image. SSIM is a measure of structural similarity between two images by analyzing luminance, contrast, and texture. The SSIM metric ranges from -1 to 1, with 1 indicating a perfect match. CPSNR is an objective metric, expressed in decibels (dB), that is utilized for the purpose of evaluating the quality of both the generated camouflage image and the recovered image. It is widely accepted that a higher CPSNR value is indicative of superior image quality. The CPSNR values of two images that are a perfect match diverges infinite values [32,33].

On the other hand, these metrics also have some drawbacks. SSIM is a step ahead of basic metrics like CPSNR, but suffers from issues regarding geometric sensitivity. Even slight pixel shifts or rotations cause identical images to fluctuate in score. It also uses computationally heavier sliding window calculations. SSIM can also become unstable in low-contrast areas and generally ignores color differences, which makes it less reliable for high-precision tasks like medical imaging or professional color correction [34]. Although CPSNR is a popular benchmark due to its simplicity of calculation, its most significant shortcoming is its inability to replicate the visual perception of humans. The CPSNR is based exclusively on pixel-by-pixel intensity disparities. Consequently, it does not take into account the manner in which the human visual system perceives image quality. Furthermore, CPSNR is less effective at capturing structural distortions, texture changes, and perceptual artifacts, which limits its reliability for evaluating perceptual image quality.

3.1. Performance Evaluation on Square Image Dataset

In the first scenario, the plain images of size $N \times N \times 3$ were camouflaged with the target images of size $M \times M \times 3$ as $N = \{256, 512\}$ and $M = \{512, 1024\}$. Here, to analyze the performance of the method, it was applied to a total of 624 different image pairs. As illustrated in Figure 2, the camouflage image obtained for different fragment sizes is presented, along with the specific zoomed images and the performance results obtained. Moreover, the overall performance of our method in transforming plain images of size $256 \times 256 \times 3$ into target images of size $512 \times 512 \times 3$ is demonstrated in Figure 3. As seen in the figures, the proposed method generates high-quality camouflage images that are devoid of any distortion, irrespective of the size of the fragment.

3.2. Performance Evaluation on Rectangular Image Dataset

In the second scenario, the proposed method was evaluated on rectangular color images. The original size values of these images are $768 \times 1024 \times 3$ and $1024 \times 768 \times 3$. These original images and their halved-size versions were utilized as target and plain images, respectively. Here, to analyze the performance of the method, it was applied to a total of 150 different image pairs. The performance metrics obtained for rectangular camouflage images are given in Table 1. As is evident from the qualitative results, analogous to results

for the square ones, the performance metrics demonstrate a high image camouflaging performance, irrespective of fragment size.

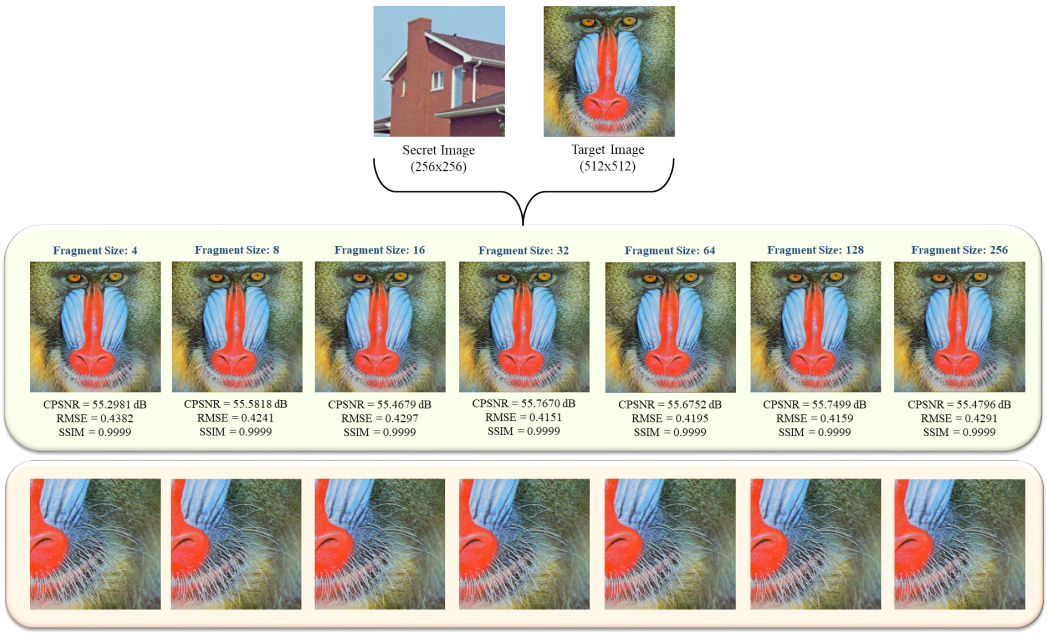


Figure 2. The camouflage images for different fragment sizes.

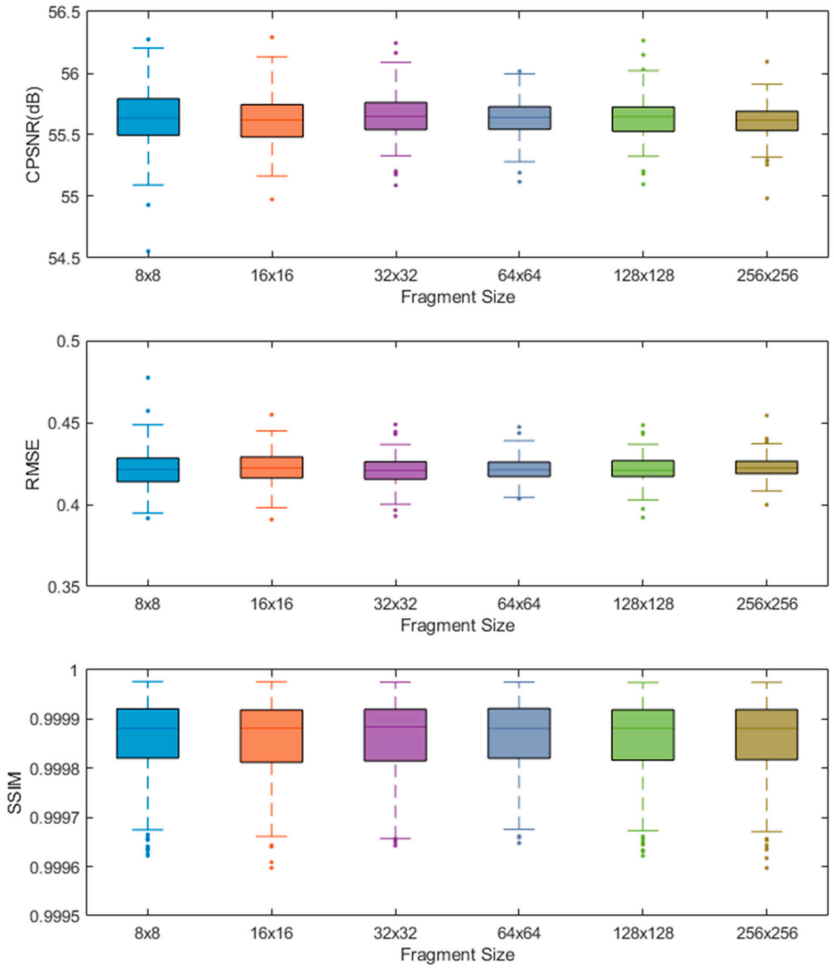


Figure 3. *Cont*.

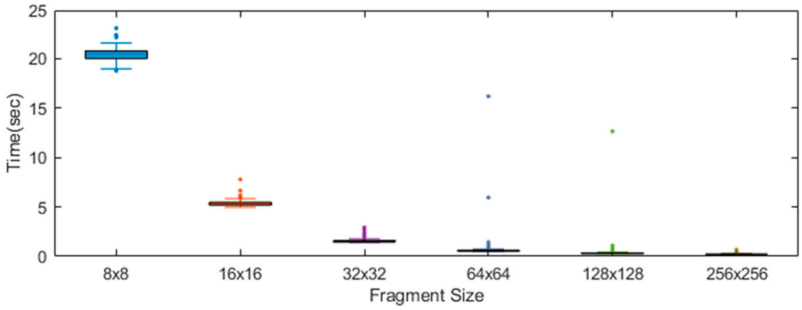


Figure 3. The overall performance of our method for different fragment size values (plain image size: $256 \times 256 \times 3$ and target image size: $512 \times 512 \times 3$).

Table 1. Obtained performance metrics on rectangular images for various fragment sizes.

Fragment Size	CPSNR (dB) ↑	SSIM ↑	RMSE ↓
4	$55.6627 \pm 17.89 \times 10^{-2}$	$0.9999 \pm 6.23 \times 10^{-5}$	$0.4202 \pm 8.7 \times 10^{-3}$
8	$55.6358 \pm 18.03 \times 10^{-2}$	$0.9999 \pm 5.48 \times 10^{-5}$	$0.4215 \pm 8.7 \times 10^{-3}$
16	$55.6370 \pm 15.15 \times 10^{-2}$	$0.9999 \pm 5.51 \times 10^{-5}$	$0.4215 \pm 7.3 \times 10^{-3}$
32	$55.6401 \pm 14.59 \times 10^{-2}$	$0.9999 \pm 5.52 \times 10^{-5}$	$0.4213 \pm 7.1 \times 10^{-3}$
64	$55.6371 \pm 14.01 \times 10^{-2}$	$0.9999 \pm 5.54 \times 10^{-5}$	$0.4214 \pm 6.8 \times 10^{-3}$
128	$55.7023 \pm 17.95 \times 10^{-2}$	$0.9999 \pm 6.00 \times 10^{-5}$	$0.4183 \pm 8.6 \times 10^{-3}$

3.3. Visual Quality Analysis

In addition to the numerical results, the success of the proposed method in generating camouflage images has been demonstrated through histogram analysis and performance analysis in low- and high-frequency regions. A fundamental approach employed in the analysis of images to ascertain their natural or camouflage state involves the examination of the image's histogram. Therefore, from an information security perspective, the camouflage image must exhibit a histogram behavior that is indistinguishable from that of the natural image. The results of the histogram analysis are presented in Figure 4. Here, the first column displays the plain image, and the next two columns depict the target image and the camouflage image, respectively. The last three columns illustrate the histogram displays obtained for the red, green, and blue channels, respectively. As demonstrated by the histogram graphs, the generated camouflage image displays behavior that is almost identical to the target image's histogram, exhibiting no abnormal characteristics when subjected to rigorous histogram analysis.

As a secondary analysis of the qualitative results, the pixel behavior of both the target image and the camouflage image was examined within both the low-frequency and high-frequency regions. Additionally, the consistency of the transitions between these regions was analyzed for both images in Figure 5. Here, the initial row comprises plain images, the subsequent row contains target images, and the final row encompasses the generated camouflage images. In the medial segment, zoomed versions of fragment images (shown with red squares on the original images) comprising low-frequency and high-frequency pixel regions of the target and camouflage images are presented. The camouflage image does not produce any artifacts in either frequency region. Furthermore, there is no visual difference between the camouflage image and the target image.

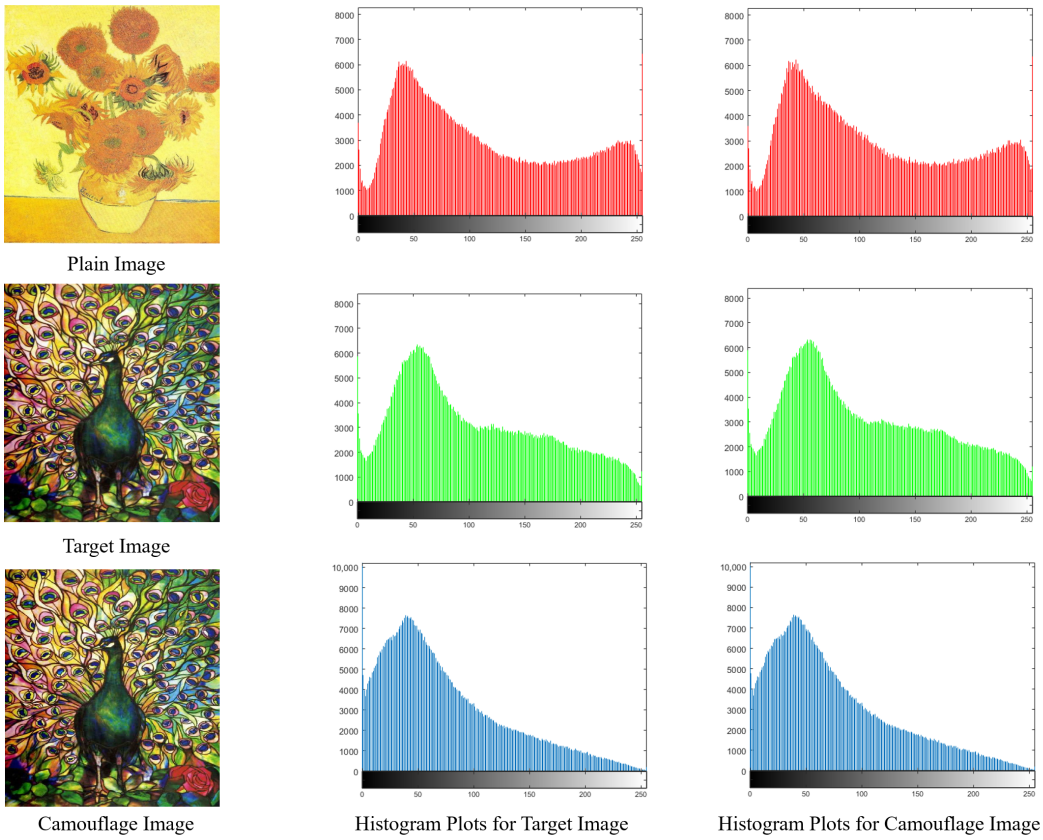


Figure 4. The visual results for histogram analysis.



Figure 5. Visual comparison between the target and camouflage images for low-frequency and high-frequency pixel regions. (First Row: Plain images, second row: target images and their zoomed fragment images, third row: camouflage images and their zoomed fragment images).

3.4. Comparative Analysis

In this section, we compare our results with those obtained by other state-of-the-art methods. To ensure fair comparison, we evaluated our method on a combined image dataset including all test images used in reference works. As our study does not include

an encryption model, the comparison is based solely on the visual quality metrics of the generated camouflage image. As demonstrated in Table 2, the proposed method exhibits a marked superiority in terms of visual quality performance.

Table 2. Comparison of the visual quality metrics for the camouflage image.

Work	Reversibility	CPSNR (dB) ↑	SSIM ↑
Ref. Work [22]	Nearly Reversible	41.2106	0.9987
Ref. Work [23]	Nearly Reversible	36.4277	0.9978
Ref. Work [20]	Nearly Reversible	40.0594	0.9459
Ref. Work [26]	Nearly Reversible	48.7666	0.9839
Ref. Work [27]	Nearly Reversible	43.5174	0.9990
Ref. Work [25]	Fully Reversible	45.3263	0.9882
Ref. Work [12]	Fully Reversible	33.2894	0.9413
Ref. Work [13]	Fully Reversible	34.3812	0.9508
Our work	Fully Reversible	55.2532	0.9999

3.5. Ablation Study

This section presents a series of ablation studies that demonstrate the significant contribution of random matrix perturbation—the original approach in our work—to the generation of camouflage images, as well as its importance in losslessly recovering the original image.

The first study analyzed the effect of random matrix perturbation on reducing the condition number of the transformation matrix. Due to the strong correlation in image matrices, a sharp decrease in the condition number cannot always be expected when these matrices are perturbed with random matrices. Nevertheless, the ability to reduce the condition number to a range where lossless transformation is guaranteed is the fundamental motivation behind the study.

As Figure 6 clearly shows, the condition numbers of the seven different fragment matrices before the perturbation process are extremely high, indicating that a lossless transformation is impossible. Conversely, the perturbation process has significantly reduced the condition numbers in fragments where lossless inversion was impossible, as well as in all other fragments. The condition numbers of all fragments have been reduced to values at which lossless inversion can be achieved. Here, the condition number values are plotted on a logarithmic scale to clearly illustrate this change.

In the second study, the effect of random matrix perturbation on reducing the condition number and, consequently, on the lossless recovery of the original image was investigated. In this analysis, the proposed random matrix perturbation process was not applied to the plain and target images. In the second stage, the recovered image obtained by applying a random matrix perturbation. The resulting recovered images are given in Figure 7. As shown in Figure 7, the recovered image obtained without perturbation exhibits singular behavior in the transformation matrix because one or both of the fragment matrices contain low-frequency regions. Consequently, information is lost when the corresponding fragment images are recovered. However, the perturbation process enables even previously lost fragments to be recovered without loss.

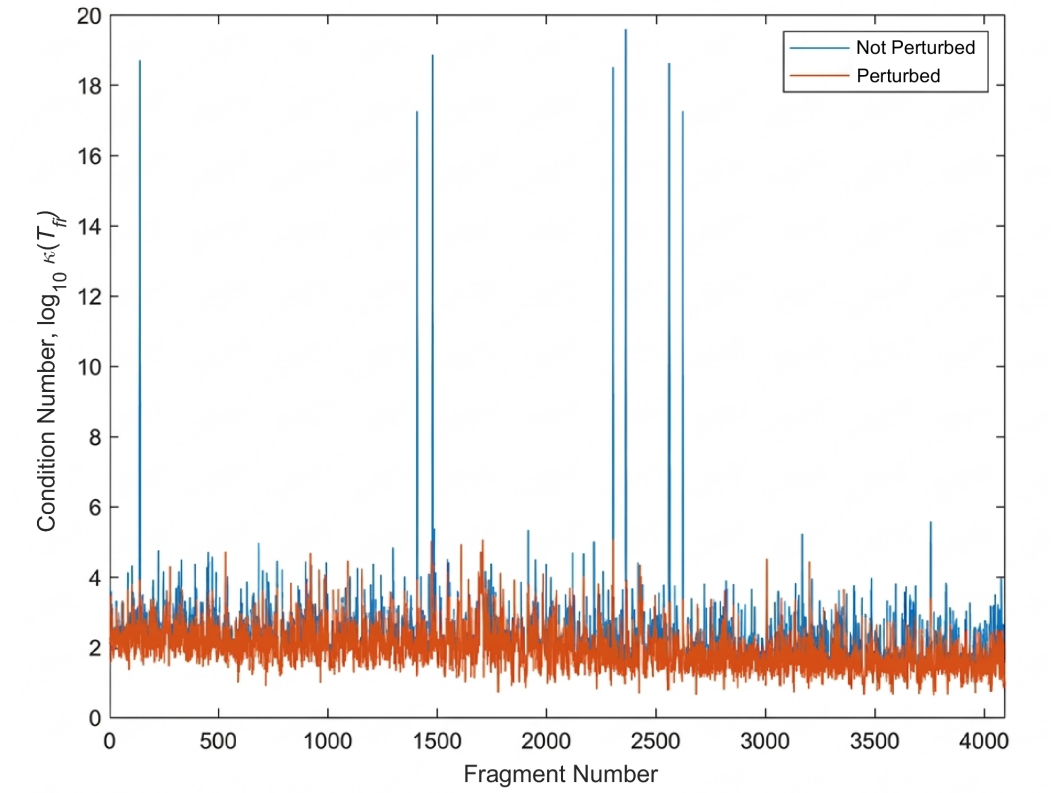


Figure 6. Condition numbers of transformation matrix fragments before and after random matrix perturbation.

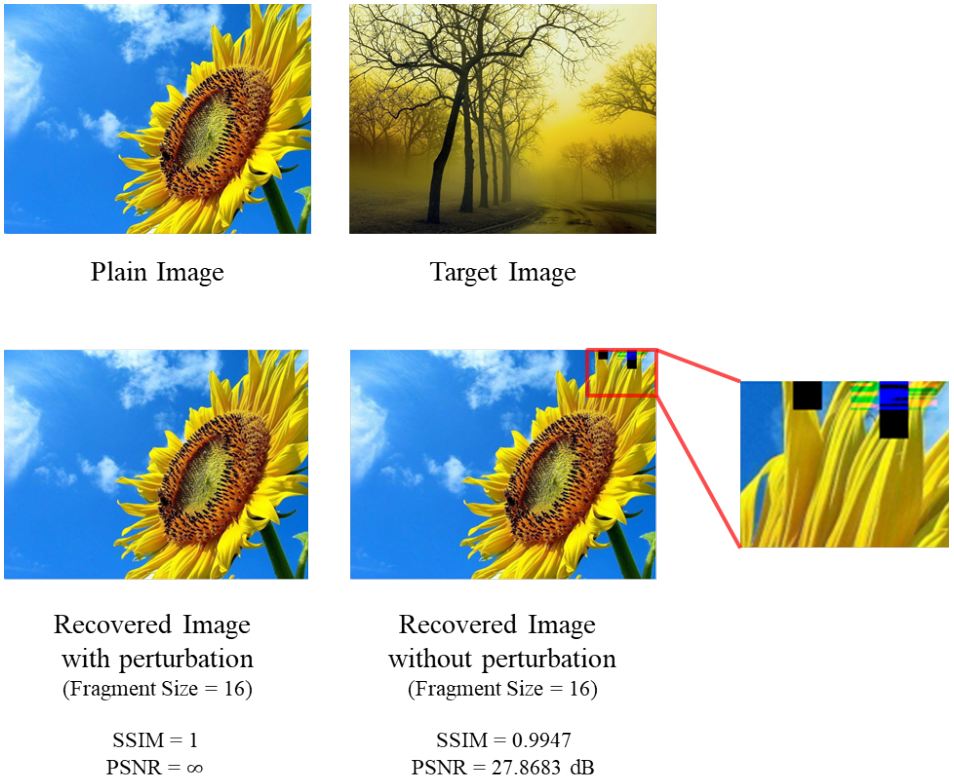


Figure 7. Recovered Images with/without random matrix perturbation.

3.6. Steganalysis of the Method

In addition to the numerical and visual analyses and ablation studies conducted to demonstrate the effectiveness of our method, we also evaluate its reliability from an in-

formation security perspective using steganalysis tools. For this purpose, the StegExpose tool [35] is used to evaluate the reliability of the information hiding in our method. StegExpose analyzes whether pixel changes in an image file are too small to be detected by the human eye. Rather than relying on a single analysis method, StegExpose combines several statistical tests (Chi-Square Test, RS (Relative Steering) Analysis, Sample Pairing Analysis, and Primary Sets) to provide a more reliable result. The performance of these detectors is measured using the area under the ROC curve (AUC). Here, an AUC value of around 0.50 indicates that the detector performs no better than random guessing, meaning that the embedding scheme is highly secure. The AUC values obtained from steganalysis for 40 test images are shown in Figure 8. Combining all the detectors to represent the total detection capacity produced a Fusion AUC value of 0.4950. This nearly ideal value strongly indicates the overall security of the proposed framework. It suggests that, on average, the blind multi-class steganalysis tool is unable to distinguish between camouflaged images and natural images reliably.

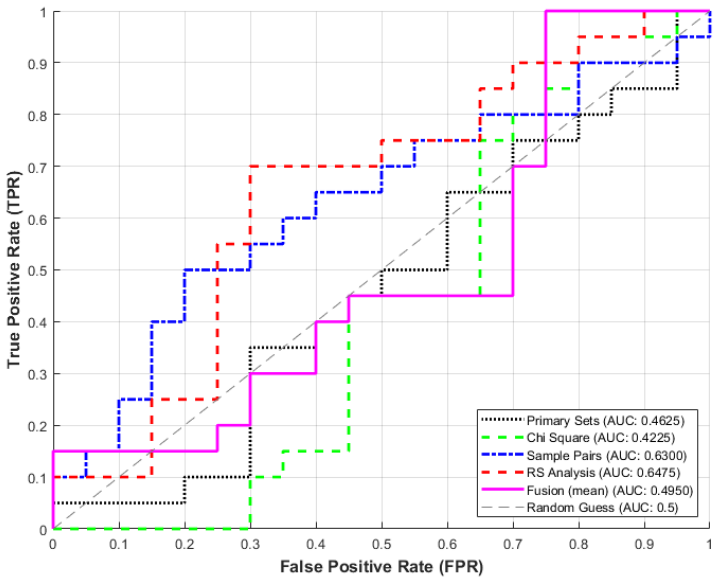


Figure 8. Resulting AUC graphs and values of steganalysis.

4. Discussion

In this work, we have proposed a reversible image camouflaging method based on lossless matrix transformation. The primary motivation underlying our research endeavors was to generate a camouflage image with minimal distortion, whilst ensuring the recovery of the original image without loss. Our method ensures lossless image recovery because we ensure the reversibility of the transformation matrix through random matrix perturbation, and because the wavelet transform is also an invertible method. Moreover, to analyze the extent to which our method, consisting of lossless matrix transformation and data embedding stages, meets generating a camouflage image with minimum distortion, it was tested on two data sets that are commonly used in the literature. The findings of experimental studies demonstrate the potential for the production of camouflage images at a level that is almost indistinguishable from target images. It is noteworthy that the attainment of this visual performance is not contingent upon the fulfillment of any specific visual criteria pertaining to the plain image or the target image. High-quality camouflage images are consistently produced for any given plain-target image pair (Figures 2–5). Moreover, the experimental findings demonstrate that the efficacy of the method is not contingent on the selected fragment size (Figure 3). However, the following points may still be considered when selecting the fragment size:

- As the fragment size increases, the time required to generate the camouflage image decreases dramatically. Inversely, as fragment size increases, the total execution time decreases despite the $O(f^3)$ complexity per inversion. This is because the total number of matrices (K) decreases quadratically, significantly reducing the overhead of iterative matrix perturbations and function calls in our implementation. Therefore, there is a trade-off about the selection of fragment size.
- When the fragment size is small, it is more likely that fragment matrices will contain low-frequency regions or flat regions. By perturbing these matrices, it is easier to reduce the condition number of the transformation matrix to lower values, but this will increase the processing time. In such cases, the problem can be solved by reducing the fragment size. However, if the images have large low-frequency or flat pixel regions, the problem is solved again by matrix perturbation. However, it may not be possible to achieve low condition number values with low fragment sizes.

Another aspect related to the effective use of the method is the selection of the target image. In the experimental studies conducted, the method was applied to a varying number of randomly selected plain-target image pairs. However, while the plain image to be camouflaged appears naturally due to the nature of the task, the user can choose which target image to use for camouflage. Therefore, the content of the selected target image is decisive for the visual quality of the generated camouflage image. In the event that the target image contains low-frequency regions, it is imperative to perturb it to ensure lossless transformation. Since the resulting perturbed image matrix is overwritten in the approximation matrix, the camouflage image is constructed using the updated matrix. Conversely, if the target image is free from any perturbation, the approximation matrix remains unaltered, thereby producing a camouflage image that exhibits a greater degree of similarity to the original. The effect of the selected target image on the visual quality of the generated camouflage image is shown in Figure 9. The results given by green dots were obtained for target images that have large low-frequency regions and need to be perturbed. The remaining results were obtained for target images devoid of any regions requiring perturbation. Here, the fragment size is set to 64. As clearly shown in Figure 9, in the absence of a low-frequency region within the target image that necessitates perturbation, as dictated by the selected fragment size, a substantial enhancement is evident in the CPSNR and SSIM values of the generated camouflage image.

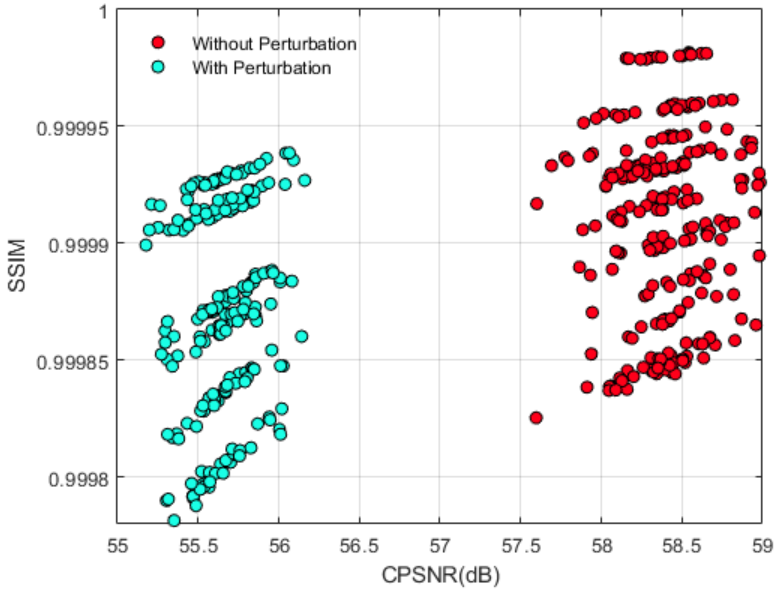


Figure 9. The effect of the target image perturbation on the visual quality of camouflage image.

5. Conclusions

This paper proposes a reversible image camouflaging method based on lossless matrix transformation. To ensure that the camouflaged image contains minimal distortion and that the plain image can be recovered from the camouflaged image without loss, the random matrix perturbation method is proposed in this study. The low-frequency (flat) regions in the images pose a significant bottleneck for lossless matrix transformation operations. By reducing the rank of the transformation matrix defined between the square fragment matrices of the plain and target images using random matrix perturbation, a lossless transformation between the two image spaces has been achieved. Thus, a lossless transformation between any two images has been achieved without the need for any block matching or optimal mapping process. Subsequently, the normalized transformation matrix defined between the two fragment matrices was embedded into the detail coefficient matrix of the target image with the lowest energy via wavelet transformation. Here, a lifting scheme was employed in the wavelet transformation to ensure the normalized transformation matrix is obtained losslessly without any rounding errors.

The performance of the proposed method was evaluated on two different datasets. Metrics such as RMSE, CPSNR, and SSIM were analyzed for different fragment sizes. The results of the experimental studies show that our method consistently produces superior results for different fragment sizes and is not affected by fragment size. Additionally, to demonstrate the visual quality of the generated camouflage image, histogram analyses and image analysis procedures in low- and high-frequency regions were performed. Ablation studies were performed to observe the dominant effect of the random matrix perturbation process on the number of conditions and to demonstrate its importance in obtaining the plain image without loss. Finally, steganalysis was performed on the camouflage images generated using the StegExpose tool.

According to the experimental results obtained from all the analyses conducted, the proposed method generates high-quality camouflaged images for any pair of plain and target images and can recover the original image without loss. It is particularly noteworthy that the method maintains high performance even in images containing extensive low-frequency regions, such as medical and document images.

The most important constraint of this method, which must be taken seriously, is that the ratio between the size of the plain image and the size of the target image must be 1:4. The main reason for this is that the generated transformation matrix is naturally the same size as the plain image. From a practical standpoint, it is not feasible to require an image four times larger than the plain image to securely store or transmit it. Improving current methods to achieve the performance metrics demonstrated in this work using a 1:1 transformation has been identified as a priority for future work. In this context, the development of generative models—such as autoencoders that can represent images in a lower-dimensional latent space and synthesize high-quality images—is among the most significant innovative methods with the potential to overcome the limitations discussed in this work.

Author Contributions: Conceptualization, G.D.D. and U.Ö.; Methodology, U.Ö.; Software, G.D.D.; Validation, G.D.D. and U.Ö.; formal analysis, G.D.D. and U.Ö.; investigation, G.D.D.; resources, G.D.D.; writing—original draft preparation, G.D.D.; writing—review and editing, U.Ö.; visualization, G.D.D. and U.Ö.; supervision, G.D.D. and U.Ö. 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 author.

Acknowledgments: The authors would like thank Zeynep Sırma Alparslan Gök for her helpful suggestions in developing the model of the work.

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

References

1. Dworkin, M.J.; Barker, E.; Nechvatal, J.R.; Foti, J.; Bassham, L.E.; Roback, E.; Dray, J.F. *Advanced Encryption Standard (AES)*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2001. [CrossRef]
2. Pekerti, A.A.; Sasongko, A.; Indrayanto, A. Secure end-to-end voice communication: A comprehensive review of steganography, modem-based cryptography, and chaotic cryptography techniques. *IEEE Access* **2024**, *12*, 75146–75168. [CrossRef]
3. Acharya, B.; Sravan, J.V.; Potnuru, D.J.R.; Patro, K.A.K. MIE-SPD: A New and Highly Efficient Chaos-Based Multiple Image Encryption Technique with Synchronous Permutation Diffusion. *IEEE Access* **2025**, *13*, 62773–62797. [CrossRef]
4. Hazzazi, M.M.; Rehman, M.U.; Shafique, A.; Aljaedi, A.; Bassfar, Z.; Usman, A.B. Enhancing image security via chaotic maps, Fibonacci, Tribonacci transformations, and DWT diffusion: A robust data encryption approach. *Sci. Rep.* **2024**, *14*, 12277. [CrossRef]
5. Dhall, S.; Yadav, K. Cryptanalysis of substitution-permutation network based image encryption schemes: A systematic review. *Nonlinear Dyn.* **2024**, *112*, 14719–14744. [CrossRef]
6. Qiqieh, I.; Alzubi, J.; Alzubi, O. DNA cryptography based security framework for health-cloud data. *Computing* **2025**, *107*, 35. [CrossRef]
7. Huang, L.; Ding, C.; Bao, Z.; Chen, H.; Wan, C. A DNA Encoding Image Encryption Algorithm Based on Chaos. *Mathematics* **2025**, *13*, 1330. [CrossRef]
8. Pham, D.H.; Vu, M.T. Takagi-Sugeno–Kang Fuzzy Neural Network for Nonlinear Chaotic Systems and Its Utilization in Secure Medical Image Encryption. *Mathematics* **2025**, *13*, 923. [CrossRef]
9. Wang, C.; Zhang, Y. A novel image encryption algorithm with deep neural network. *Signal Process.* **2022**, *196*, 108536. [CrossRef]
10. Lai, I.-J.; Tsai, W.-H. Secret-Fragment-Visible Mosaic Image—A New Computer Art and Its Application to Information Hiding. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 936–945. [CrossRef]
11. Lee, Y.-L.; Tsai, W.-H. A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations. *IEEE Trans. Circuits Syst. Video Technol.* **2014**, *24*, 695–703. [CrossRef]
12. Hou, D.; Zhang, W.; Yu, N. Image camouflage by reversible image transformation. *J. Vis. Commun. Image Represent.* **2016**, *40*, 225–236. [CrossRef]
13. Zhang, W.; Wang, H.; Hou, D.; Yu, N. Reversible Data Hiding in Encrypted Images by Reversible Image Transformation. *IEEE Trans. Multimed.* **2016**, *18*, 1469–1479. [CrossRef]
14. Yao, H.; Liu, X.; Tang, Z.; Hu, Y.-C.; Qin, C. An Improved Image Camouflage Technique Using Color Difference Channel Transformation and Optimal Prediction-Error Expansion. *IEEE Access* **2018**, *6*, 40569–40584. [CrossRef]
15. Hou, D.; Qin, C.; Tang, Z.; Yu, N.; Zhang, W. Reversible visual transformation via exploring the correlations within color images. *J. Vis. Commun. Image Represent.* **2018**, *53*, 134–145. [CrossRef]
16. Yin, J.; Ou, B.; Liu, X.; Peng, F. Mosaic secret-fragment-visible data hiding for secure image transmission based on two-step energy matching. *Digit. Signal Process.* **2018**, *81*, 173–185. [CrossRef]
17. Zhong, H.; Chen, X.; Tian, Q. An Improved Reversible Image Transformation using K-Means Clustering and Block Patching. *Information* **2019**, *10*, 17. [CrossRef]
18. Lama, R.K.; Han, S.J.; Kwon, G.R. SVD based improved secret fragment visible mosaic image generation for information hiding. *Multimed. Tools Appl.* **2014**, *73*, 873–886. [CrossRef]
19. Jing, S.; Li, J. An overview of visually meaningful ciphertext image encryption. *Multimed. Tools Appl.* **2025**, *84*, 13617–13652. [CrossRef]
20. Armijo-Correa, J.O.; Murguía J.S.; Mejía-Carlos, M.; Arce-Guevara, V.E.; Aboytes-González, J.A. An improved visually meaningful encrypted image scheme. *Opt. Laser Technol.* **2020**, *127*, 106165. [CrossRef]
21. Bao, L.; Zhou, Y. Image encryption: Generating visually meaningful encrypted images. *Inf. Sci.* **2015**, *324*, 197–207. [CrossRef]
22. Kanso, A.; Ghebleh, M. An algorithm for encryption of secret images into meaningful images. *Opt. Lasers Eng.* **2017**, *90*, 196–208. [CrossRef]
23. Yao, H.; Liu, X.; Tang, Z.; Qin, C.; Tian, Y. Adaptive image camouflage using human visual system model. *Multimed. Tools Appl.* **2019**, *78*, 8311–8334. [CrossRef]
24. Dolendro Singh, L.; Manglem Singh, K. Visually meaningful multi-image encryption scheme. *Arab. J. Sci. Eng.* **2018**, *43*, 7397–7407. [CrossRef]
25. Yang, Y.-G.; Wang, B.-P.; Yang, Y.-L.; Zhou, Y.-H.; Shi, W.-M.; Liao, X. Visually meaningful image encryption based on universal embedding model. *Inf. Sci.* **2021**, *562*, 304–324. [CrossRef]

26. Wang, Y.; Chen, J.; Wang, J. Visually meaningful image encryption based on 2D compressive sensing and dynamic embedding. *J. Inf. Secur. Appl.* **2023**, *78*, 103613. [CrossRef]
27. Wang, X.; Liu, C.; Jiang, D. A novel visually meaningful image encryption algorithm based on parallel compressive sensing and adaptive embedding. *Expert Syst. Appl.* **2022**, *209*, 118426. [CrossRef]
28. Hu, L.-L.; Chen, M.-X.; Wang, M.-M.; Zhou, N.-R. Visually meaningful triple images encryption algorithm based on 2D compressive sensing and multi-region embedding. *Knowl.-Based Syst.* **2025**, *324*, 113804. [CrossRef]
29. Vu, V.H.; Tao, T. The condition number of a randomly perturbed matrix. In Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing, San Diego, CA, USA, 11–13 June 2007; pp. 248–255. [CrossRef]
30. USC-SIPI Database. Available online: https://sipi.usc.edu/database/database.php?volume=misc (accessed on 24 December 2024).
31. Lee, Y.L.; Tsia, W.H. Related Images of the Experiments. Available online: https://people.cs.nycu.edu.tw/~yllee/yllee&whtsai_sfv.html (accessed on 16 January 2025).
32. Kusuma, M.R.; Panggabean, S. Robust digital image watermarking using DWT, Hessenberg, and SVD for copyright protection. *Int. J. Adv. Comput. Inform.* **2026**, *2*, 41–52. [CrossRef]
33. Lakasek, S.B.; Elhadi, H. A Robust Image Watermarking Technique Using NSST-HD-SVD. *Int. J. Adv. Comput. Inform.* **2026**, *2*, 115–126. [CrossRef]
34. Pambrun, J.F.; Noumeir, R. Limitations of the SSIM quality metric in the context of diagnostic imaging. In Proceedings of the IEEE International Conference on Image Processing (ICIP), Quebec City, QC, Canada, 27–30 September 2015; pp. 2960–2963. [CrossRef]
35. Boehm, B. Stegexpose—A tool for detecting LSB Steganography. *arXiv* **2014**, arXiv:1410.6656. [CrossRef]

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.