



Enhancing Image Security through PCA-IWT-Based Nil Steganography under Distortion Scenarios

Areej M. Abduldaïm, Nadia M. G. Al-Saidi*, Anwar Khaleel Faraj, Saja A. Alameer Kahdim

ABSTRACT: Security has become a paramount concern across various fields of study today, with particular emphasis on steganography mechanisms as sought-after and promising research areas aimed at safeguarding multimedia data from unauthorized access. This study introduces a robust nil steganography technique that enhances its undetectable nature and resilience to various image processing attacks by combining Principal Component Analysis (PCA) with the Integer Wavelet Transform (IWT). The host image is converted to grayscale, the LL band is extracted using IWT, and the image is divided into non-overlapping 4×4 blocks as part of the concealment process. Principal features are then extracted from each block using PCA, and these are then XORed with the binary emblem to produce the confidential share. To produce the confidential share, three emblems are tested, and the XOR operation is performed to combine each emblem with the extracted features. According to experimental results, the system performs well in terms of Peak Signal-to-Noise Ratio (PSNR), Normalized Correlation (NC), and Bit Error Rate (BER) across various attack scenarios, including histogram equalization, Gaussian noise, and JPEG compression. In contrast to current techniques, the suggested method exhibits better imperceptibility and robustness. The algorithm can be considered suitable for real-world applications in secure image processing because it maintains a computational complexity of $O(N^2)$.

Key Words: Nil Steganography, Integer Wavelet Transform (IWT), Principal Component Analysis (PCA), image steganography, feature extraction, robustness and imperceptibility, image security, digital embedding techniques.

Contents

1 Introduction	1
2 Theoretical Background	3
2.1 Integer Wavelet Transform (IWT)	3
2.2 Block Partitioning of the LL Subband	3
2.3 Principal Component Analysis (PCA)	3
2.4 Construction of Feature Matrix	4
3 The proposed mechanism	4
3.1 The proposed algorithm for feature extraction	5
3.2 Retrieval Process	5
4 Results and Analysis	5
4.1 Stegavaluation	6
4.2 Steganalysis	15
4.3 The Complexity	16
4.4 Comparison	16
5 Conclusions	16

1. Introduction

Linear algebra techniques have garnered significant attention from researchers and are prevalent in numerous works within the field of computer science, particularly in image processing, signal analysis, and cybersecurity [1], which require efficient data representation and transformation. This can be attributed

* Corresponding author.

2010 *Mathematics Subject Classification*: 68U10, 94A08, 62H25.

Submitted September 12, 2025. Published October 16, 2025

to the inherent characteristics of these algebraic methods, particularly their capability to identify critical features within the data being processed. The robustness of most of these methods lies in their stability, often relying on the extraction of eigenvalues and eigenvectors, which are renowned for their strength and consistency. Signal processing, in particular, has extensively employed these methods, with image processing benefiting significantly from their advantages across various domains, including nil steganography techniques for hiding in images or videos [2,3]. Nil steganography mechanisms are categorized into two types based on the method employed to embed the emblem into the host image. In the nil steganography mechanism, essential information is extracted from the image and utilized in the embedding process, thereby preserving the quality of the host image. Conversely, in the traditional steganography mechanism, the emblem image is directly embedded into the image pixels, resulting in alterations to the host image quality.

The Hessenberg decomposition (Hess) has recently gained traction in various applications. Additionally, the widely employed algebraic decomposition method, singular value decomposition (SVD), holds particular significance due to its ability to identify unique singular values [4]. In the realm of steganography mechanisms, both decompositions are utilized in [5], which features double-matrix factorization and multi-region coverage to introduce the image steganography mechanism. This approach aims to address the challenge of poor extraction ability in images subjected to steganographic attacks or interference. Alternatively, optimization algorithms, such as those proposed in [6] and [7], have been explored for similar purposes. Moreover, nil steganography techniques have demonstrated effectiveness in medical imaging applications, employing methods such as the complex wavelet transform via double-tree and multilevel discrete cosine transform (MDCT) [8]. To enhance robustness and security, the Hess factorization is frequently optimized, either without any transformation in the YCbCr space, as demonstrated in [9], or without the use of optimization algorithms, as in [10,11]. Certainly, there are numerous possibilities for leveraging various algebraic methods alongside numerous mathematical tools, including optimization algorithms and ordinary transformations [12,13]. In [15], improved invisibility and robustness of digital image steganography are achieved through DWT-SVD, whereas in [14], enhancement is achieved through SVD applied to color image steganography via a combination of chaotic maps and IWT. The SVD is employed in [16] with a genetic algorithm but without utilizing any extra common transform. A new image watermarking method combines IWT, SVD, and chaos to address SVD's issues like false positives, low capacity, and security flaws [17]. On the other hand, authors in [18] devised an optimized steganography mechanism relying on the Generalized Singular Value Decomposition as a new method, alongside the Binary Gravitational Search optimization. Generally, PCA decomposition is not frequently employed in steganography mechanisms, particularly in nil steganography. In reversible steganography scenarios, the (GLCM), Gray-Level Cooccurrence Matrix, combined with PCA, is utilized to identify suitable bands for emblem embedding, leading to the design of a blind technique based on contourlet transform [19]. Regarding the COVID-19 images, in [20,21], to ensure ownership and copyright protection, PCA is implemented to hide and emblem images for medical data hiding techniques, thereby enhancing SecDH. The unique nil steganography technique was identified in [22], which employs PCA together with DWT to construct a robust nil steganography mechanism. Reciprocally, numerous ideas have been proposed, and various other algebraic decomposition methods have been explored.

Using Schur decomposition and fast finite Shearlet transform (FFST-Schur) and FrJFM (fractional-order JacobiFourier moments) in [23] to design a dual zero-watermarking algorithm and to address the problem that most zerowatermarking algorithms tend to be resistant to some attacks. A steganography mechanism is devised by combining the QR algebraic decomposition and Schur decomposition with the selected blocks to conceal the emblem bits [24]. Respecting fuzzy inference systems, the algebraic method LU has been successfully employed alongside the Mamdani FIS in [25] to extract a controlling item for balancing imperceptibility and robustness. Wu et al. [26] proposed a color nil steganography algorithm for multiple medical images based on FFST (fast finite Shearlet transform)-Schur decomposition and Tent mapping, effectively addressing the issue of the difficulty of centralized protection of these types of images, standard image processing, and geometric and combinatorial attacks.

The following contributions are accomplished in this work:

- To extract dominant image features from the LL band and enable high-fidelity embedding without visually altering the host image, a novel combination of Principal Component Analysis (PCA)

and Integer Wavelet Transform (IWT) is employed. The IWT's LL subband can be used to extract localized features because it is separated into 4×4 non-overlapping blocks. This block-level decomposition increases robustness, lessening sensitivity to noise and image distortion.

- To make a secure share that can be reversed, a unique method is proposed to generate a binary feature matrix from PCA components, which is then combined with the binary emblem using XOR.
- Numerous tests show that the suggested method outperforms similar methods in achieving high NC and PSNR values across a variety of attacks (such as JPEG compression, Gaussian noise, speckle noise, and histogram equalization). Moreover, the algorithm's computational complexity, $O(N^2)$, makes it suitable for large-scale or real-time applications in secure multimedia systems. When the technique is contrasted with a more recent PCADWT steganography method, it demonstrates superior BER performance in a range of attack scenarios, demonstrating its effectiveness.

The structure of this paper is as follows: The theoretical background for the utilized methods, with the Integration between them, is presented in Section 2. Section 3 introduces the implementation of nil steganography techniques, outlining the embedding and restoration steps for incorporating the emblem image. In Section 4, the results of some experiments and evaluator values are provided to evaluate the proposed technique in terms of robustness and imperceptibility. Moreover, this section discusses analysis and comparison to demonstrate the validity of the proposed method. Finally, Section 5 provides the conclusion of the work.

2. Theoretical Background

The proposed method is based on a two-step transformation procedure: dominant features are extracted from localized blocks using PCA after image features are first localized in the frequency domain using the IWT. This integration makes use of both transforms' advantages: PCA's feature decorrelation and IWT's localization.

2.1. Integer Wavelet Transform (IWT)

The grayscale image $I \in R^{N \times N}$, is decomposed into four subbands, such that:
 $IWT(I) = \{L L, L H, H L, H H\}$

- LL: represents the low-frequency, which is the subband that contains most of the image energy.
- LH, HL, HH: represent horizontal, vertical, and diagonal edges.

The LL is selected for further processing because it represents the core structure of the image.

2.2. Block Partitioning of the LL Subband

Divide the LL subband, where $LL \in R^{M \times M}$ ($M = N/2$) into $k \times k$ nonoverlapping blocks:

$$LL = \bigcup_{i=1}^B B_i, \quad B = \left(\frac{M}{k}\right)^2$$

Here, $k = 4$, leading to 4096 blocks for $M = 256$.

2.3. Principal Component Analysis (PCA)

For each block $B_i \in R^{4 \times 4}$, PCA is applied as follows:

1. Mean Centering: $\bar{B}_i = B_i - \mu_i$, where $\mu_i = \text{mean}(B_i)$
2. The Decomposition:

$$C_i v_j = \lambda_j v_j, j = 1, 2, \dots, k$$

The principal component, which captures the most variance in the block, is represented by the eigenvector v_1 that corresponds to the largest eigenvalue λ_1 .

2.4. Construction of Feature Matrix

A threshold comparison is used to extract the first column of the eigenvector matrix (v_1) from each block and assemble it into a global binary feature matrix $BZ \in \{0, 1\}^{64 \times 64}$:

Covariance Matrix: $C_i = \frac{1}{n-1} \bar{B}_i^T \bar{B}_i$

$$BZ_{i,j} = \begin{cases} 1, & \text{if mean } (v_1^{(i,j)}) > v_1^{(i,j)} \\ 0, & \text{otherwise} \end{cases}$$

3. The proposed mechanism

This paper proposes a new nil steganography method that combines Principal Component Analysis (PCA) and Integer Wavelet Transform (IWT). Robust features are extracted by using PCA on IWT-transformed blocks of the LL subband as it illustrated in Figure 1. This allows a binary emblem image to be securely embedded without substantially altering the host image. To confirm the robustness and imperceptibility of the suggested approach, it is thoroughly tested under various image attack scenarios.

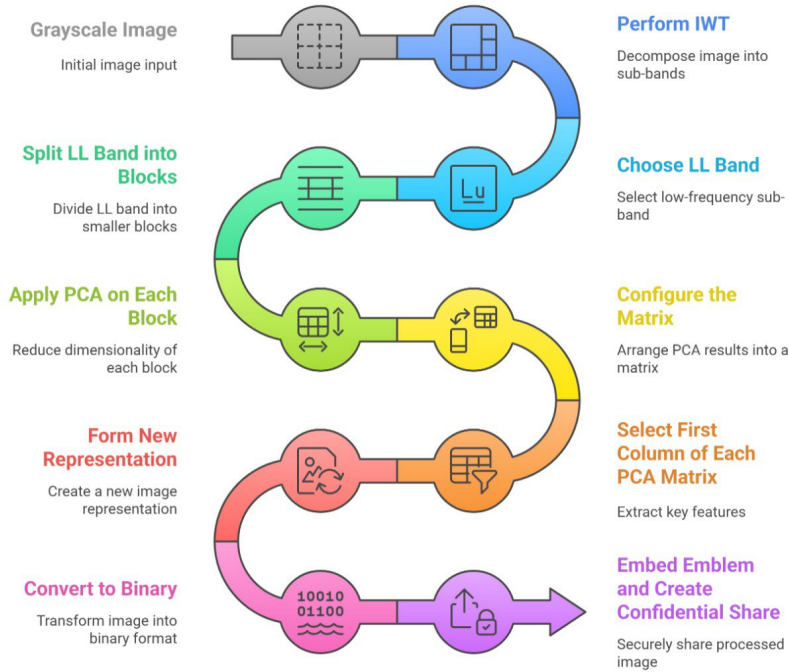


Figure 1: The diagram of the embedding process utilizing PCA with IWT

All images employed in this study have dimensions of 512×512 . Both the concealed images and the emblem undergo conversion from RGB space to luminance transformation. Subsequently, the IWT is conducted on the concealed image, with the LL Band subsequently subdivided into non-overlapping 4×4 blocks. The PCA is then applied to each block as an algebraic transformation to extract crucial information from the concealed images and generate the feature matrix bits.

3.1. The proposed algorithm for feature extraction

In the beginning, the IWT is conducted on the concealed image, followed by the application of the PCA to decompose each 4×4 block of the LL band to extract the eigenvector matrices V_i . Subsequently, to generate the features matrix and the confidential share, choose the first column from each V_i matrix and consider these columns as the principal components PC_i . The following algorithm explains the detailed steps:

- Algorithm 1 1: Insert the 512×512 concealment image I swap to grayscale.
 2: Implement IWT on I to find the 256×256 LL band.
 3: Divide the band LL into 4×4 nonoverlapping blocks (LL divided into 64×64 blocks).
 4: Implement the PCA on each block in step 3 to find the $V_{(i,j)}$ matrices, $1 \leq i \leq 64$ and $1 \leq j \leq 64$.
 5: Pick the first column from each $V_{(i,j)}$ to be the $PC_{(i,1)} = V_{(i,1)}$ (Each column is of size 4×1) and form the binary feature matrix BZ , such that each element of BZ corresponds to the block $V_{(i,j)}$, where $1 \leq i \leq 64$ and $1 \leq j \leq 64$.
 6: Configure the matrix BZ by comparing the average of each first column $V_{(i,1)}$ with the first element $V_{(i,1)}(1, 1)$ in the same column. This process is done for each block $V_{(i,j)}$ according to the following:

$$\begin{aligned} \text{avg}_{V_{(i,j)}} &= \left(\sum_{t=1}^4 V_{(i,j)}(t, 1) \right) / 4 \\ BZ(i, j) &= 1 \quad \text{if } \text{avg}_{V_{(i,j)}} \geq V_{(i,j)}(1, 1) \\ BZ(i, j) &= 0 \quad \text{otherwise} \\ &\text{where } 1 \leq i \leq 64 \text{ and } 1 \leq j \leq 64 \end{aligned}$$

- 7: Incorporate the emblem image E and swap to obtain the binary emblem matrix BE .
 8: The confidential share S is created by XORing BZ and BE matrices.

3.2. Retrieval Process

The exhaustive steps for image retrieval are given in the following algorithm:

- Algorithm 2 1: Insert the 512×512 concealment image I swap to grayscale.
 2: Implement IWT on I to find the 256×256 LL band.
 3: Divide the band LL into 4×4 nonoverlapping blocks (LL divided into 64×64 blocks).
 4: Implement the PCA on each block in step 3 to find the $V_{(i,j)}$ matrices, $1 \leq i \leq 64$ and $1 \leq j \leq 64$.
 5: Pick the first column from each $V_{(i,j)}$ to be the $PC_{(i,1)} = V_{(i,1)}$ (each column is of size 4×1) and form the binary feature matrix BZ , such that each element of BZ corresponds to the block $V_{(i,j)}$, where $1 \leq i \leq 64$ and $1 \leq j \leq 64$.
 6: Configure the matrix BZ by comparing the average of each first column $V_{(i,1)}$ with the first element $V_{(i,1)}(1, 1)$ in the same column. This process is done for each block $V_{(i,j)}$ according to the following:

$$\begin{aligned} \text{avr}_{V_{(i,j)}} &= \left(\sum_{t=1}^4 V_{(i,j)}(t, 1) \right) / 4 \\ BZ(i, j) &= 1 \quad \text{if } \text{avr}_{V_{(i,j)}} \geq V_{(i,j)}(1, 1) \\ BZ(i, j) &= 0 \quad \text{otherwise} \\ &\text{where } 1 \leq i \leq 64 \text{ and } 1 \leq j \leq 64 \end{aligned}$$

- 7: The binary emblem BE is restored by applying the confidential share S using XOR to BZ .

4. Results and Analysis

The experimental findings and performance assessment of the suggested nil steganography technique are shown in this section. A number of metrics, such as PSNR, NC, and BER, are employed to evaluate robustness and imperceptibility across multiple emblem images and under various distortion scenarios.

4.1. Stegavaluation

This section highlights the proposed method's impact and efficiency. It elucidates the outcomes obtained by applying the method before subjecting the images to attacks and the results observed after subjecting the same images to various attacks. This evaluation aims to assess the proposed method's robustness and imperceptibility.



Figure 2: The concealment images and the emblem A

The proposed nil steganography scheme is examined on four grayscale images of size 512×512 . A binary emblem image of size 64×64 is considered. The cover images and the emblem are shown in Figure 2. The NC value, with the absence of attacks, for each image in Figure 2, is equal to 1. This demonstrates that the suggested method can embed and extract data losslessly under optimal conditions. Additionally, the visual quality and robustness of the proposed mechanism are evaluated using PSNR, NC, and BER.

The PSNR, NC, and BER metrics are evaluated after the emblem A is retrieved. Table 1 (a, b, and c) presents the imperceptibility and robustness results tested against various attacks for the proposed mechanism. The retrieved emblem after three groups of attacks is shown in Figures 8, 9, and 10, respectively.

Table 1a: The PSNR values after attacks for emblem A

S	Lena	Girl	Baboon	Peppers
Salt&Pepper	27.011	26.217	27.115	26.985
JPEG Compression	61.305	61.287	60.684	60.933
Gaussian noise	37.64	37.675	37.66	37.652
Histequalization	1.985	10.096	16.369	20.56
Gaussian low Pass filter	34.068	38.137	31.327	34.277
Poisson noise	27.214	30.437	27.005	27.346
Speckle noise	35.66	41.092	35.501	35.715
Motion filter	26.036	28.352	23.921	25.502
Average filter	34.068	38.137	31.327	34.277
Median filter	31.721	35.401	30.439	31.512

Table 1b: The NC values after attacks for emblem A

S	Lena	Girl	Baboon	Peppers
Salt&Pepper	0.904	0.905	0.924	0.903
JPEG Compression	0.961	0.956	0.982	0.947
Gaussian noise	0.839	0.828	0.913	0.844
Histequalization	0.9	0.904	0.927	0.893
Gaussian low Pass filter	0.878	0.784	0.869	0.88
Poisson noise	0.767	0.784	0.834	0.774
Speckle noise	0.836	0.87	0.898	0.841
Motion filter	0.792	0.792	0.734	0.786
Average filter	0.878	0.881	0.689	0.88
Median filter	0.878	0.885	0.874	0.88

Table 1c: The BER values after attacks for emblem A

S	Lena	Girl	Baboon	Peppers
Salt&Pepper	0.166	0.165	0.132	0.169
JPEG Compression	0.068	0.077	0.031	0.093
Gaussian noise	0.271	0.289	0.152	0.262
Histequalization	0.137	0.167	0.129	0.185
Gaussian low Pass filter	0.209	0.535	0.224	0.206
Poisson noise	0.377	0.353	0.279	0.368
Speckle noise	0.275	0.222	0.177	0.268
Motion filter	0.377	0.342	0.424	0.352
Average filter	0.209	0.204	0.224	0.206
Median filter	0.209	0.197	0.216	0.207

The findings presented in Table 2 demonstrate that the proposed approach remains highly robust and imperceptible in a range of distortion scenarios. PSNR values remain within acceptable limits for visual quality, especially when JPEG compression is employed, which yields the highest PSNR scores. While BER is typically low, confirming dependable recovery, NC values regularly surpass 0.73 , suggesting a strong correlation between the original and restored emblems. The overall performance across all metrics validates the method's resilience and suitability for secure steganographic applications, despite the higher distortion introduced by filters like motion and Poisson.

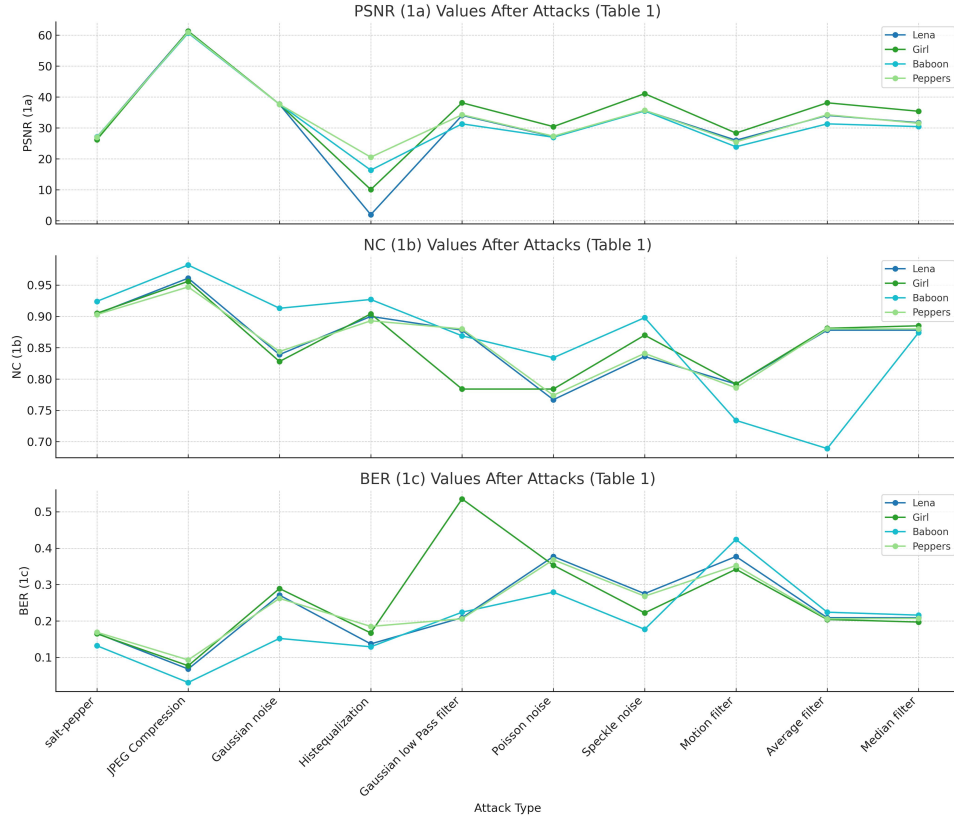


Figure 3: PSNR, NC, and BER values for emblem A

To test the proposed method with different emblems, two additional emblems, B and C, are adopted. The results obtained for the additional two emblems after the attacks closely resemble those achieved with the initial emblem, as detailed in Table 2(a, b, and c) and Table 3(a, b, and c). The Figures (3, 5, 7) show the line graph for the three different emblems (Figures 2, 4, and 6). The Bit Error Rate (BER), Normalized Correlation (NC), and Peak Signal-to-Noise Ratio (PSNR) values for four common test images-Lena, Girl, Baboon, and Peppers-under various image processing attacks are shown in these figures. The stability of PSNR and NC, as well as the reduction of BER values across attacks, can be used to evaluate the technique's robustness.

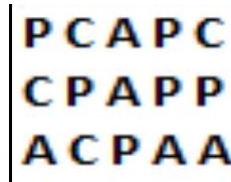


Figure 4: The emblem B

Table 2a: The PSNR values after attacks for emblem B

PCAPC CPAPP ACPAA	Lena	Girl	Baboon	Peppers
Salt&Pepper	0.177	26.012	27.230	26.95
JPEG Compression	61.305	61.287	60.684	60.933
Gaussian noise	37.675	37.682	37.643	37.674
Histequalization	18.985	10.096	16.369	20.56
Gaussian low Pass filter	34.068	38.137	31.327	34.277
Poisson noise	27.181	30.437	27.015	27.320
Speckle noise	35.671	41.075	35.527	35.734
Motion filter	26.036	28.352	23.921	25.502
Average filter	34.068	38.137	31.327	34.277
Median filter	31.721	35.401	30.439	31.512

Table 2b: The NC values after attacks for emblem B

PCAPC CPAPP ACPAA	Lena	Girl	Baboon	Peppers
Salt&Pepper	0.895	0.904	0.926	0.908
JPEG Compression	0.960	0.955	0.982	0.946
Gaussian noise	0.832	0.904	0.916	0.844
Histequalization	0.897	0.901	0.925	0.890
Gaussian low Pass filter	0.875	0.878	0.865	0.877
Poisson noise	0.751	0.780	0.826	0.768
Speckle noise	0.819	0.867	0.894	0.843
Motion filter	0.787	0.786	0.727	0.780
Average filter	0.875	0.878	0.865	0.877
Median filter	0.875	0.882	0.870	0.877

Table 2c: The BER values after attacks for emblem B

PCAPC CPAPP ACPAA	Lena	Girl	Baboon	Peppers
Salt&Pepper	27.125	0.163	0.126	0.156
JPEG Compression	0.068	0.077	0.031	0.093
Gaussian noise	0.276	0.290	0.144	0.258
Histequalization	0.173	0.167	0.129	0.185
Gaussian low Pass filter	0.209	0.204	0.224	0.206
Poisson noise	0.392	0.351	0.284	0.369
Speckle noise	0.295	0.222	35.527	0.259
Motion filter	0.342	0.342	0.424	0.352
Average filter	0.209	0.204	0.224	0.206
Median filter	0.209	0.197	0.216	0.207

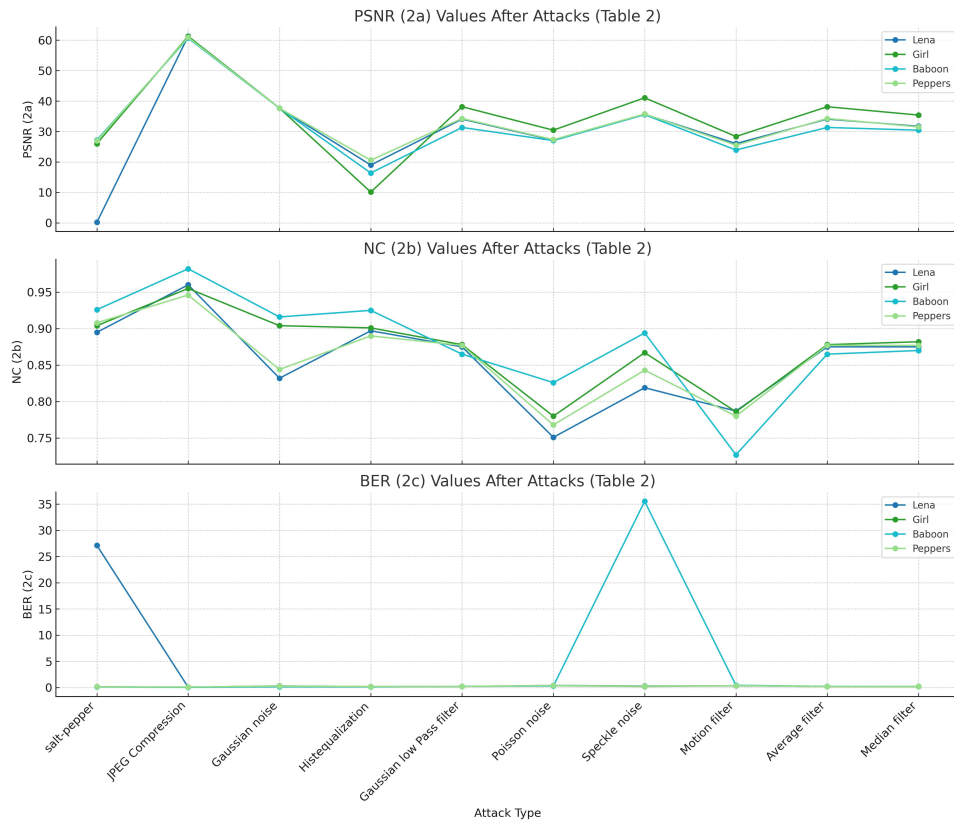


Figure 5: PSNR, NC, and BER values for emblem B

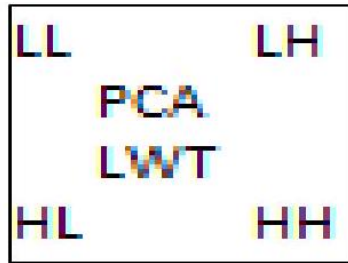


Figure 6: The emblem C

Table 3a: The PSNR values after attacks for emblem C

<div> <div>LL</div> <div>PCA</div> <div>LWT</div> <div>HL</div> <div>LH</div> <div>HH</div> </div>		Lena	Girl	Baboon	Peppers
	Salt and Pepper	26.920	26.375	27.040	27.042
	JPEG Compression	61.305	61.287	60.684	60.933
	Gaussian noise	37.679	37.698	37.655	37.653
	Histequalization	18.985	10.096	16.369	20.56
	Gaussian low Pass filter	34.068	38.137	31.327	34.277
	Poisson noise	27.199	30.455	27.016	27.315
	Speckle noise	35.647	41.082	35.518	35.723
	Motion filter	26.036	28.352	23.921	25.502
	Average filter	34.068	38.137	31.327	34.277
	Median filter	31.721	35.401	30.439	31.512

Table 3b: The NC values after attacks for emblem C

<div> <div>LL</div> <div>PCA</div> <div>LWT</div> <div>HL</div> <div>LH</div> <div>HH</div> </div>		Lena	Girl	Baboon	Peppers
	Salt&Pepper	0.900	0.909	0.927	0.907
	JPEG Compression	0.963	0.958	0.983	0.949
	Gaussian noise	0.854	0.840	0.915	0.853
	Histequalization	0.904	0.907	0.929	0.897
	Gaussian low Pass filter	0.882	0.886	0.873	0.884
	Poisson noise	0.766	0.796	0.839	0.786
	Speckle noise	0.840	0.881	0.905	0.846
	Motion filter	0.800	0.799	0.744	0.793
	Average filter	0.882	0.886	0.873	0.884
	Median filter	0.883	0.889	0.878	0.884

Table 3c: The BER values after attacks for emblem C

<div> <div>LL</div> <div>PCA</div> <div>LWT</div> <div>HL</div> <div>LH</div> <div>HH</div> </div>		Lena	Girl	Baboon	Peppers
	Salt and Pepper	0.180	0.165	0.133	0.168
	JPEG Compression	0.068	0.777	0.031	0.093
	Gaussian noise	0.257	0.279	0.153	0.258
	Histequalization	0.173	0.167	0.129	0.185
	Gaussian low Pass filter	0.209	0.204	0.224	0.206
	Poisson noise	0.391	0.347	0.281	0.363
	Speckle noise	0.279	0.212	0.171	0.270
	Motion filter	0.342	0.342	0.424	0.352
	Average filter	0.209	0.204	0.224	0.206
	Median filter	0.209	0.197	0.216	0.207

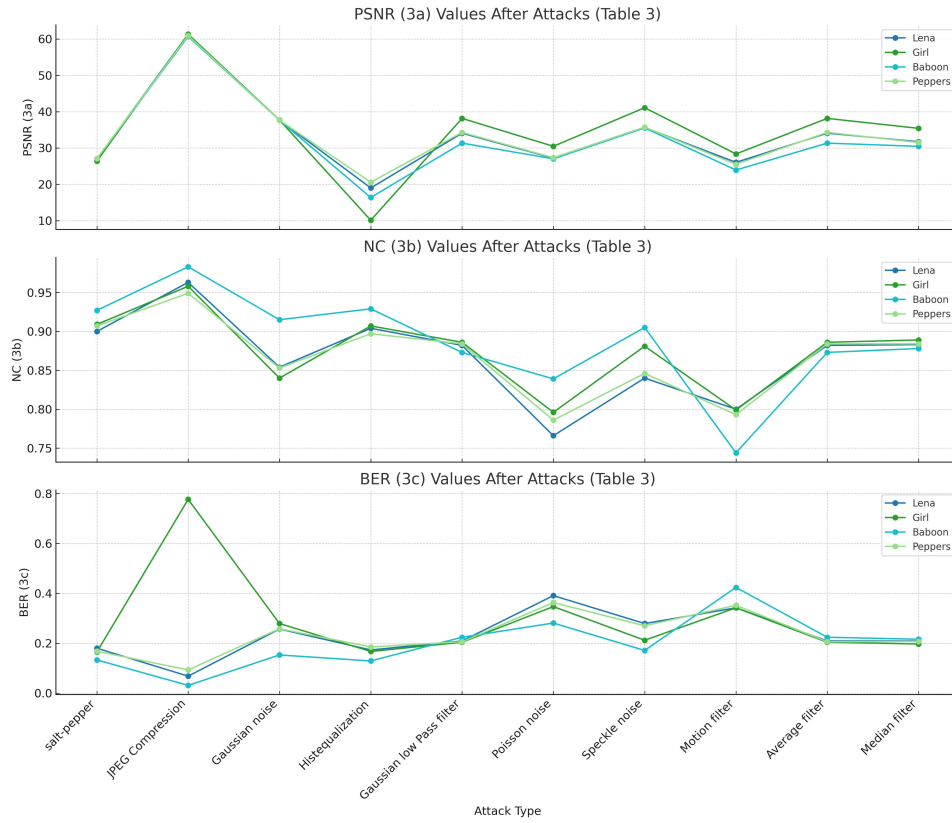


Figure 7: PSNR, NC, and BER values for emblem C

The robustness and consistency of the suggested PCA-IWT-based steganography method are further supported by the results in Tables 3 and 4, which use emblems B and C, respectively. High PSNR values indicate strong visual imperceptibility in both sets of results, particularly when JPEG compression is employed. In most situations, NC values remain above 0.75, indicating dependable symbol recovery, while BER values maintain acceptable bounds even when confronted with challenging distortions such as motion filtering and Poisson noise. These consistent results for various emblem patterns demonstrate the method's versatility, efficacy, and robustness for embedding safe and undetectable data. For the first emblem (A), the retrieved emblems (RE) are shown below, organized by attack type.

1. Noise Attacks: Introduce random variations in pixel values to simulate real-world distortions.













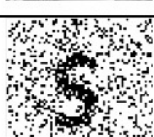

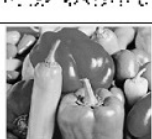



E (A)	-Lena-	-Girl-	-Baboon-	-Peppers-
S				
Gaussian low pass filter				
RE				
Motion filter				
RE				
Average filter				
RE				
Median filter				
RE				

Figure 8: The restoration of the emblem A after the Noise attacks

2. Filter Attacks: Apply smoothing or sharpening operations that can alter embedded emblem signals.

































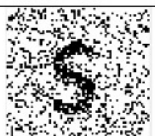
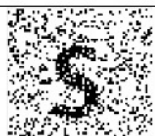

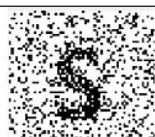
E (A)	-Lena-	-Girl-	-Baboon-	-Peppers-
S				
Gaussian low pass filter				
RE				
Motion filter				
RE				
Average filter				
RE				
Median filter				
RE				

Figure 9: The restoration of the emblem A after the Filter attacks

3. Geometric Attacks: Change the image structure or intensity distribution, potentially disrupting watermark alignment.










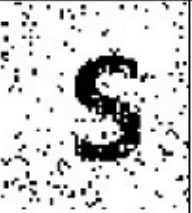
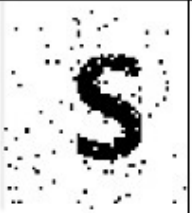






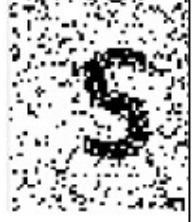


E (A)	Lena	Girl	Baboon	Peppers
S				
JPEG Compression				
RE				
Histequalization				
RE				

Figure 10: The restoration of the emblem A after Geometric attacks

4.2. Steganalysis

In general, any mathematical method is chosen to extract important information from the image matrix based on the characteristics of that method. Therefore, the stronger the method has the ability

to extract important areas from the matrix, the greater its impact on the accuracy of the results. Thus, the reason for applying the PCA on each block after dividing the LL channel, obtained using the IWT , into 4×4 nonoverlapping blocks $V_{(i,j)}$ is to separate each block into high frequencies represented by the principal components $PC_{(i,1)}$'s that consists of two parts: (i) the eigenvectors, which are represented by the first column of $V_{(i,j)}$ and correspond to the highest eigenvalues, and then construct the feature matrix BZ , and (ii) the lower frequencies, which are represented by the least important information in the image, and these are the eigenvectors that correspond to the lowest eigenvalues. Consequently, it is virtually certain that the included binary emblem BE can be restored without any change compared with the original emblem image. All of this demonstrates that the process of recovering the logo from the cover image yielded acceptable and satisfactory results, even after being subjected to various attacks.

4.3. The Complexity

To compute the total complexity of the algorithm, we'll analyze the time complexity of each step and then sum them up. The algorithm consists of two main parts: Share Creation and Emblem Restoration. We'll analyze both parts separately and then combine their complexities. To compute the complexity of the steps, we begin with the steps of converting the image to grayscale. The complexity of this step is: $O(512 \times 512) \approx O(N^2)$, where $N = 512$.

The complexity of performing is $O(512 \times 512) = O(N^2)$, as wavelet transforms typically require linear passes over the image. The complexity of dividing the LL Band into 4×4 Blocks is $O(1)$ per block (just partitioning), so total $O(4096) \approx O(M^2)$, where $M = 256$. The total complexity of PCA on each block, which involves eigenvalue decomposition is $O(4^3) = O(64)$ per block. Therefore, 4096 blocks $\times O(64) \approx O(4096 \times 64) = O(262,144)$. The complexity of the binary matrix BZ is equal to $O(4096)$.

Converting the emblem image to a binary matrix BE requires $O(64 \times 64) = O(4096)$, which is complex. As a result, algorithm one is performed with the total complexity: $O(262,144)(PCA) + O(262,144)(PCA) \approx O(524,288)$. In big O notation, this simplifies to $O(N^2)$, where $N = 512$ is the original image dimension. The total computational complexity of the algorithm is $O(N^2)$, where N is the side length of the input image (e.g., 512). This is primarily due to the PCA operations performed on all 4×4 blocks of the LL band.

4.4. Comparison

Table 4 illustrates the comparative performance of the proposed method with current methods, particularly in the presence of Gaussian noise and JPEG compression. The work is compared with Ref. [22] and Ref. [27], which utilized DWT with algebraic decomposition PCA under the BER metric. Overall, it maintains acceptable BER levels, demonstrating its robustness and practical reliability for secure image embedding, albeit marginally less effective against median filtering and salt & pepper noise.

Table 4: Comparison of our proposed technique with Ref. [22] and [26] under the BER metric

Attacks	Lena image		
	The proposed Technique	[22] Technique	[26] Technique
Salt&pepper	0.166	0.04	0.04
JPEG compression	0.068	0.0000	0.0336
Gaussian noise	0.271	0.07	0.28
Median filter	0.209	0.0049	0.2272

5. Conclusions

A technique of nil steganography, adopting the algebraic PCA method and the IWT, is proposed in this paper. The results are as follows:

1. In general, all the results obtained are acceptable and so close (if not better) to the optimal results achieved from using a popular transformation that extracts the image features optimally.

2. The proposed technique gave good flexibility against different types of common attacks.
3. The smallest value of the NC using emblem image A is (0.734) in the motion filter attack, and the biggest value is (0.982) in the JPEG compression attack.
4. The smallest value of the NC using emblem image B is (0.727) in the motion filter attack, and the biggest value is (0.982) in the JPEG compression attack.
5. The smallest value of the NC using emblem image C is (0.744) in the motion filter attack, and the biggest value is (0.983) in the JPEG compression attack.
6. Depending on the results obtained, it was found that the proposed method is effective and strong (resistant to the most tested attacks), i.e., having good robustness and imperceptibility.

Note that PCA has a general disadvantage, which is highly influenced by outliers in the data. So, to overcome this issue, many robust versions of PCA have been developed, including Randomized PCA, sparse PCA, etc.

References

1. M. H. Khudhur, J. Waleed, H. Hatem, A. M. Abduldaim, and D. A. Abdullah, An Efficient and Fast Digital Image Copy–Move Forensic Technique, in *Proc. 2nd Int. Conf. for Engineering, Technology and Sciences of Al-Kitab (ICETS)*, Kirkuk, Iraq, 2018, pp. 78–82.
2. Wajdi Elhamzi, Enhancing Medical Image Security with FPGA-Accelerated LED Cryptography and LSB Watermarking, *Traitement du Signal*, vol. 41, no. 1, pp. 85–97, Feb. 2024.
3. Purnima, Rakesh Ahuja, and Nidhi Gautam, Motion–Frames Based Video Watermarking Scheme for Copyright Protection Using Guided Filtering in Wavelet Domain, *Traitement du Signal*, vol. 40, no. 1, pp. 187–197, Feb. 2023.
4. A. Riyaduddin and A. Padmanabha Reddy, Countermeasures Against Image Processing Attacks for Image Watermarking in the Wavelet Domain Using Singular Value Decomposition and Discrete Cosine Transform, *Review of Computer Engineering Studies*, vol. 10, no. 2, pp. 51–57, 2023.
5. Z. Pan, W. C. Yang, and B. Zhao, Matrix Decomposition Image Steganography Scheme Based on Wavelet Transform with Multi–Region Coverage, *Entropy*, vol. 24, no. 246, pp. 1–21, 2022.
6. H. Nazir, I. S. Bajwa, M. Samidullah, A. Anwar, and M. Moosa, Robust Secure Color Image Watermarking Using 4D Hyperchaotic System, DWT, HbD, and SVD Based on Improved FOA Algorithm, *Hindawi: Security and Communication Networks*, 2021.
7. V. Kumar, V. Laddha, S. Aniket, and D. Yadav, Image and Text Steganography Using Convolutional Neural Network, *TECNICA ITALIANA–Italian Journal of Engineering Science*, vol. 65, no. 1, pp. 26–32, 2022.
8. Tongyuan Huang, Jia Xu, Yuling Yang, and Zhenyu Han, Robust Zero–Watermarking Algorithm for Medical Images Using Double–Tree Complex Wavelet Transform and Hessenberg Decomposition, *Mathematics*, vol. 10, no. 7, 1154, 2022.
9. N. S. Mohammed and A. M. Abduldaim, Algebraic Hessenberg Decomposition Method Optimized by Genetic Algorithm for Zero Watermarking Technique, *International Journal of Mathematics and Computer Science*, vol. 16, no. 4, pp. 1497–1514, 2021.
10. K. U. Singh, S. Y. Hsieh, C. Swarup, and C. Singh, Authentication of NIFTI Neuroimages Using Lifting Wavelet Transform, Arnold Cat Map, Z–Transform, and Hessenberg Decomposition, *Traitement du Signal*, vol. 39, no. 1, pp. 265–274, 2022.
11. Xiaochao Wang, Qiangian Du, Ling Du, Huayan Deng, and Jianping Hu, Robust Zero–Watermarking Algorithm via Multi–Scale Feature Analysis for Medical Images, *Journal of Information Security and Applications*, vol. 89, 2025, 103937.
12. Ali, Musrrat, and Sanoj Kumar, A Robust Zero–Watermarking Scheme in Spatial Domain by Achieving Features Similar to Frequency Domain, *Electronics*, vol. 13, no. 2, p. 435, 2024.
13. Yong Chen, Zhigang Jia, Hao Peng, and Yaxin Peng, Interpretable Feature Modeling for Robust Color Watermarking in the Quaternion Framework, *Expert Systems with Applications*, vol. 295, 2026, 128901.
14. W. H. Alshoura, Z. Zainol, and J. M. Alawida, An FPP–Resistant SVD–Based Image Watermarking Scheme Based on Chaotic Control, *Alexandria Engineering Journal*, vol. 61, no. 7, pp. 5713–5734, Jul. 2022.
15. A. Alzahrani, Enhanced Invisibility and Robustness of Digital Image Watermarking Based on DWT–SVD, *Applied Bionics and Biomechanics*, 2022.

16. N. S. Mohammed and A. M. Abduldaim, Algebraic Decomposition Method Utilized in Optimized Zero Watermarking Technique, *Proc. 1st Babylon Int. Conf. on Information Technology and Science*, 2021.
17. W. H. Alshoura and J. M. Alawida, Secure and Flexible Image Watermarking Using IWT, SVD, and Chaos Models for Robustness and Imperceptibility, *Scientific Reports*, vol. 15, p. 7231, 2025.
18. A. M. Abduldaim and A. K. Fara, 'Combining Algebraic GSVD and Gravitational Search Algorithm for Optimizing Secret Image Watermark Sharing Technique, *International Journal of Mathematics and Computer Science*, vol. 17, no. 2, pp. 753–774, 2022.
19. R. Thomas and M. Sucharitha, Reversible Color Image Watermarking Scheme Based on Contourlet Transform and Principal Component Analysis, *International Conference on Electrical Energy Systems*, 2021, pp. 641–644.
20. H. Natiq, N. M. Al-Saidi, S. J. Obaiys, M. N. Mahdi, and A. K. Farhan, Image encryption based on local fractional derivative complex logistic map, *Symmetry*, 14(9), 1874, 2022.
21. D. S. Ali, Nawras A. Alwan, and Nadia MG Al-Saidi, Image encryption based on highly sensitive chaotic system, *AIP Conference Proceedings-AIP Publishing LLC* 2183(1), 2019.
22. X. Leng, J. Xiao, and Y. Yang, A Robust Image Zero–Watermarking Algorithm Based on DWT and PCA, in *Communications in Computer and Information Science*, Springer, Berlin, Heidelberg, vol. 289, 2024.
23. Lu Yu, Lu Xh., Yang Gy., et al., Double Watermarking Algorithms Based on Fractional–Order Jacobi–Fourier Moments and FFST–Schur, *Circuits, Systems, and Signal Processing*, vol. 44, pp. 4796–4827, 2025.
24. Altay S. Y., Uluatag G., and Dogan N., Dual Watermarking Schemes Based on QR Decomposition and Schur Decomposition in the RIDWT Domain, *SiViP*, vol. 18, pp. 2783–2798, 2024.
25. R. I. Sabri and A. M. Abduldaim, Mamdani FIS Combined with LU Decomposition Method and Two–Level LWT for Image Watermarking Technique, *Proc. 3rd Int. Conf. on Engineering Applications*, 2022.
26. Yu Lu, Xinhui Lu, Guangyun Yang, Xiangqian He, A Robust Zero–Watermarking Algorithm for Multi–Medical Images Based on FFST–Schur and Tent Mapping, *Biomedical Signal Processing and Control*, vol. 96, 2024, 106557.
27. S. A. Kahdim and A. M. Abduldaim, Arbitrary Component Analysis for Zero Watermarking Technique, *International Journal of Mathematics and Computer Science*, vol. 18, no. 1, pp. 85–97, 2023.

Areej M. Abduldaim

College of Applied Sciences

University of Technology, Baghdad, Iraq.

E-mail address: areej.m.abduldaim@uotechnology.edu.iq

and

Nadia M. G. Al-Saidi

College of Applied Sciences

University of Technology, Baghdad, Iraq.

E-mail address: nadia.m.ghanim@uotechnology.edu.iq

and

Anwar Khaleel Faraj

College of Applied Sciences

University of Technology, Baghdad, Iraq.

E-mail address: Anwar.K.Faraj@uotechnology.edu.iq

and

Saja A. Alameer

Computer Technology Engineering, Al-Mustafa University, Baghdad, Iraq.

E-mail address: saja.alameer9@gmail.com