Neutrosophic Eigenvalue Decomposition for Robust Zero-Watermarking

Areej M. Abduldaim[1], Mohammed Qasim Hamid[2], Saif R. Alsaffar[1] and Suzan J. Obaiys[3]
[1]Department Department of Mathematics and Computer Applications, College of Applied Sciences, University of Technology, 10066 Baghdad, Iraq
[2]Department of Mathematics, College of Education, Mustansiriyah University, 10052 Baghdad, Iraq
[3]Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya, 50603 Kuala Lumpur, Malaysia
Areej.M.Abduldaim@uotechnology.edu.iq, alamerymohamad@uomustansiriyah.edu.iq,suzan@um.edu.my

Keywords: 2010 AMS Mathematics Subject Classification: Eigenvalue Decomposition (EVD) 15A18, Neutrosophic Science 03B52, Statistical Feature Fusion 62H30, Discrete Cosine Transform (DCT) 42A38.

Abstract: Novel membership functions are introduced in this paper to design a robust zero-watermarking framework through which the image is transformed to the neutrosophic domain. In the new proposed method, named Neutrosophic Eigenvalue Decomposition with Statistical Feature Fusion (NEVD-NSFF), the Discrete Cosine Transform (DCT) is applied to each image block, and the neutrosophic triplet (T, I, F) is computed for each one, where T denotes the truth component, I denotes indeterminacy, and F denotes falsity. The newly proposed neutrosophic membership functions are more adaptive to changes in brightness and conflicting statistical values than the traditional fuzzy or probabilistic systems. The invariant components are then obtained by applying eigenvalue decomposition to the neutrosophic covariance form, which are robust to compression, noise, and illumination distortions. On the other hand, to combine these components relying on their neutrosophic membership distributions, the Neutrosophic Statistical Feature Fusion (NSFF) mechanism is given to generate a secret signature that is guarded by using Shamir's Secret Sharing. The overall complexity combining all phases is computed for the neutrosophic domain, eigenvalue decomposition, and statistical feature fusion and secret sharing. Experimental results show that the proposed framework achieves robustness, accuracy, and computational efficiency compared to traditional DCT-SVD and DWT-SVD utilized in zero-watermarking techniques.

1 INTRODUCTION

With the tremendous development in the field of technology and the Internet, and especially the remarkable progress in sharing and distributing images across digital platforms, the difficulties related to ensuring privacy, ownership, and authenticity of digital content have become among the most important challenges facing researchers and developers alike [1], [2]. Despite all this development, traditional methods of embedding watermarks lead to tampering with the original information of the image, which causes visual distortion of the original image and increases its sensitivity to attacks [3]. To address these weaknesses, algorithms called Zero Watermarking Techniques were developed to preserve ownership without any change or tampering with the original image, but rather by relying on extracting the important features of the image and designing a strong mathematical system [4]-[6].

The instability of many zero-watermarking techniques when exposed to different types of attacks, as well as the failure of the results to maintain the stability of features when using conventional methods of transformations, such as the discrete cosine transform (DCT) or discrete wavelet transform (DWT), because they rely entirely on deterministic signal components, has opened the door to new, more flexible methods to resist attacks and other destructive factors. [7], [8]. Moreover, the feature descriptors, depending on statistical and moment, containing those based on principal component analysis (PCA) or graylevel cooccurrence matrices (GLCM), are still very sensitive to lighting variations and noise [9]. Because of these impediments, many

developed techniques have appeared to preserve the stability and control the indeterminacy in the image matrix [10]-[12].

Algebra plays an important role in the field of security because its properties provide a strong base for developing verifiable schemes. Most of the zero-knowledge protocols [13] and effective authentication schemes depend on algebraic ring theory. In addition, generalized reduced rings are used to develop an interactive proof algorithm. Furthermore, the robustness and the stability of features are improved using algebraic decomposition methods. Thus, modern algebra methods guarantee confidentiality, flexibility, and integrity through various diverse security applications.

To address the above issues, a novel zero-watermarking depending on the Neutrosophic domain obtained for Eigenvalue Decomposition (NEVD) and statistical Feature Fusion is proposed in this work. Three theoretical phases are tracked: (i) eigenvalue decomposition, which captures invariant spectral directions and intrinsic correlations within image blocks; (ii) neutrosophic logic, which represents image uncertainty and ambiguity through the triplet (T, I, F) corresponding to truth, indeterminacy, and falsity components; and (iii) statistical feature fusion, which merges multi-domain neutrosophic information to construct a highly stable signature resistant to both signal and geometric distortions.

The first phase in the proposed technique operates on each block of the image to transform it into the DCT domain in order to calculate a covariance matrix, and then applies the neutrosophic operations. Under common attacks, the features obtained from the Eigenvalue decomposition of the neutrosophic matrix remain statistically consistent. A strong secret share is extracted by integrating the neutrosophic eigenvalue features with the Neutrosophic Statistical Feature Fusion (NSFF). For more security, Shamir's Secret Sharing method is utilized.

The rest of this paper is organized as follows. Section 2 gives the necessary. The neutrosophic statistical feature fusion (NSFF) is presented in Section 3. Section 4 presents the detailed construction of the novel zero-watermarking technique (NEVD-NSFF). Secret sharing scheme analysis is explained comprehensively in Section 5. The complexity, experimental results, and results analysis are reported in Sections 6, 7, and 8, respectively. Finally, Section 9 concludes the paper with remarks on potential extensions for authentication.

2 BACKGROUNDS

This section is devoted to giving important information needed in this work.

2.1 Neutrosophic Domain for Image Representation

The neutrosophic domain was first introduced by Smarandache [14], [15] as a generalization of classical and fuzzy logic by representing information as a triplet:

$$I_N = (T, I, F).$$

Where:

- T indicates the truth membership function;
- I denotes indeterminacy;
- F represents falsity.

This conversion enables the decomposition of image information into deterministic, uncertain, and noisy components, where each element belongs to the real standard or nonstandard unit interval $[0, 1^+]$. Such a flexible representation provides a richer mathematical system for handling incomplete or conflicting information compared to fuzzy or intuitionistic fuzzy sets [16], [17].

Neutrosophic theory has been extensively applied in wide areas in image processing, in particular for noise segmentation, feature extraction, and reduction.[18], [19]. Converting the image to the neutrosophic domain helps in making more accurate and reliable decisions in dealing with problems such as watermarking, enhancement, and classification through designing algorithms and analyzing, enabling more reliable decision making in these missions [20]-[22]. This special characteristic of the neutrosophic domain is appropriate for building robust zero-watermarking techniques where accuracy and feature stability are essential under uncertain or noisy conditions [11].

2.2 Statistical Feature Fusion (SFF) in Watermarking

To enhance the robustness and accuracy, Statistical Feature Fusion (SFF) integrates image features depending on their statistical characteristics [Guo2019Cheng, Ye2014]. In the proposed technique, each block is transformed to the neutrosophic domain as a triplet (T, I, F) representing truth, indeterminacy, and falsity memberships, respectively [14], [15]. A flexible feature representation is achieved through the novel

membership functions that adaptively take local uncertainty and texture variations [16], [17]. These components are fused through a neutrosophic weighted rule to form a unified feature vector linking the Neutrosophic Eigenvalue Decomposition (NEVD) with the zero-watermarking phase, improving stability and attack resistance [20], [21].

2.3 Motivation for the Proposed NEVD-NSFF Framework

To handle the gaps of known watermarking techniques, the neutrosophic domain is combined with eigenvalue decomposition and statistical feature fusion as follows: a-Detect the uncertainty of the image via the neutrosophic triplet (T, I, F) components. b- maintaining stability of the singular values and feature regularity under noise and geometric transformations. c- Attaining secure and verifiable extraction via cryptography secret sharing.

Therefore, the introduced NEVD-NSFF technique gives an integrated watermarking technique that attains robustness, accuracy, and strong security, making it suitable for practical authentication and copyright protection applications.

3 NEUTROSOPHIC STATISTICAL FEATURE FUSION (NSFF)

The target is to find a single, robust scalar $DCT^{*}_{blk}(i,j)$ for each DCT block (i,j) of size 2×2. These scalar fuses three complementary statistics derived from the block's DCT coefficients: truth T (signal energy), indeterminacy I (local variance, instability), and falsity F (spectral entropy) using adaptive weights. The fused scalar replaces the naive DC only statistic as the block representative used in downstream feature extraction (44 macro block decomposition, singular values of the SVD, binarization).

3.1 Neutrosophic Blocks

Notation: Let the given 2×2 DCT block's (absolute) coefficient values be**:**

$$C = \{c_1, c_2, c_3, c_4\}, \qquad c_k \geq 0.$$

Define the block size m = 4. Across the whole image, let:

$M_T = \max_{all\ block} \left(\frac{1}{m}\sum_{k=1}^{m} c_k\right)$, $M_1 = \max_{all\ block} Var(c)$, $M_F = log_2(m)$, be normalization constants (maximum mean energy, maximum variance, maximum entropy). If desired, these maxima may be estimated from a representative training set or computed on the single host image.

3.2 Computing the Neutrosophic Triple (T, I, F) for a Block

For each block, compute:

1) Truth (mean energy) T.

$$\mu_c = \frac{1}{m}\sum_{k=1}^{m} c_k\,, \qquad T = \frac{\mu_c}{M_T} \in [0,1].$$

T measures the block's average spectral energy (normalized).

2) Indeterminacy I. Use the sample variance of coefficients as a measure of instability:

$$Var(c) = \frac{1}{m}\sum_{k=1}^{m}(c_k - \mu_c)^2, \quad I = \frac{Var(c)}{M_I} \in [0,1].$$

High I means the block is unstable (highly varying coefficients), which typically reduces reliable repeatability under attacks.

3) Falsity (spectral entropy) F. Treat the coefficient magnitudes as a local distribution:

$$p_k = \frac{c_k}{\sum_{t=1}^{m} c_t} \left(\text{If} \sum c_t \geq 0\,;\ otherwise\ p_k = \frac{1}{m}\right),$$

then compute entropy (bits) and normalize:

$$H(C) = -\sum_{t=1}^{m} p_k\, log_2(p_k), F = \frac{H(C)}{M_F} \in [0,1].$$

F captures the spectral disorder: low entropy means energy concentrated (more robust), high entropy means spread-out spectrum (less robust).

3.3 Adaptive Fusion Rule

Choose adaptive nonnegative weights α, β, γ with $\alpha + \beta + \gamma = 1$. Define the fused normalized score:

$$s = \alpha T + \beta(1 - I) + \gamma\left(1 - F_{adj}\right),$$

where $(1 - I)$promotes blocks with low indeterminacy and $\left(1 - F_{adj}\right)$ promotes low-entropy (concentrated) blocks. In practice, one may use $F_{adj} = F$ or a clipped/smoothed version of F (see tuning below). Note that this formulation yields $s \in [0, 1]$.

1) Mapping the Fused Score to a Block Representative. The pipeline expects a scalar quantity per block similar in scale to the DC coefficient. We convert the normalized fused

score s back to a block representative DCT^*_{blk} by scaling with the local block mean (or a global scale). Two common choices:

- Local-scale mapping:

$$DCT^*_{blk} = s.\mu_c.$$

This keeps the fused value proportional to local energy.

- Global-scale mapping:
- $DCT^*_{blk} = s.M_T$.

This forces values into a common dynamic range across blocks.

Either mapping is valid; local-scale preserves intra-image contrast while global-scale eases threshold choice later.

2) Practical Parameter Selection and Adaptivity:
   - Weights (α, β, γ). A recommended starting point is $\alpha = 0.4, \beta = 0.3, \gamma = 0.3$.
   - Intuition: give slightly more weight to mean energy, but still favour stable (low variance) and concentrated (low-entropy) blocks.
   - Adaptive weighting. If the entire image is noisy, decrease α and increase β (put more trust in low-indeterminacy) or vice versa for smooth images. A simple adaptive rule:

$$\alpha \leftarrow \frac{\bar{\mu}}{\bar{\mu} + \bar{\sigma} + \bar{H}}, \beta \leftarrow \frac{\bar{\sigma}}{\bar{\mu} + \bar{\sigma} + \bar{H}},$$

$$\gamma \leftarrow \frac{H}{\bar{\mu} + \bar{\sigma} + \bar{H}}$$

Where $\bar{\mu}, \bar{\sigma}, \bar{H}$ are the image-wide averages of $\mu_c, Var(c), H(c)$ respectively (normalized to the same scale).

Entropy clipping smoothing. To avoid instability when a block has near-zero total energy, clip probabilities, or use smoothed probabilities

$$p_k \leftarrow \frac{c_t + \epsilon}{\sum(c_t + \epsilon)}$$

With $\epsilon = 10^{-6}$.

3) Pseudo Steps Per Block Implementation: For each 2×2 block:
   - (a) Compute absolute coefficients $c_4, \ldots\ldots, c_4$ and block mean μ_c.
   - (b) Compute $Var(c)$.
   - (c) Compute probabilities p_k (with smoothing) and entropy $H(c)$.
   - (d) Normalize: $T = \frac{\mu_c}{M_T}, I = \frac{Var(c)}{M_I}, F = \frac{H(C)}{M_F}$
   - (e) Compute fused normalized score:

$$s = \alpha T + \beta(1 - I) + \gamma(1 - F)$$

   - (f) Map to representative:

$$DCT^*_{blk} = \begin{cases} s.\mu_c & local - scale\ mapping \\ s.M_T & global - scale\ mapping \end{cases}.$$

4) Why NSFF improves robustness:
   - Blocks with high mean energy but low variance and concentrated spectrum are most repeatable after common attacks (compression/noise); NSFF upweights such blocks via T and $(1 - I)$,$(1 - F)$.
   - Entropy F penalizes blocks whose energy is spread across coefficients (these are less stable under filtering and quantization).
   - Indeterminacy I downweights blocks with large local variance (often edges or highly textured areas where small distortions change relative coefficients)
   - Combining three independent statistics reduces the probability that an adversarial attack or incidental distortion simultaneously corrupts all three. Mathematically, this corresponds to variance reduction in the fused estimator (by weighted averaging) and increases the signal-to-noise ratio of the feature used for binarization/feature extraction.

3.4 Numerical Example

To illustrate the practical implementation of the proposed method, a numerical example is presented below using a sample block of DCT coefficients. The example demonstrates the step-by-step computation of variance, entropy, normalization factors, and the final adaptive DCT block scalar used in the subsequent processing stages.

1) Suppose a block has absolute DCT coefficients $\{16, 4, 2, 1\}$ Then $m = 4$,

$\mu_c = (16 + 4 + 2 + 1)/4 = 5.75$ Squares are {256,16,4,1} mean square $= \frac{277}{4} = 69.25$
$Var(c) = 69.25 - (5.75)^2 = 36.1875$
Take $M_T = 16$ (example global max mean), $M_I = 36.1875$ (worst-case here), and $M_F = \log_2 4$.

2) Compute probability

$p = \{16/23\ , 4/23\ , 2/23\ 1/23\}$
$\approx \{0.6957, 0.1739, 0.0870, 0.0435\}$,

then:

$$H(C) = -\sum_{t=1}^{m} p_k\, log_2(p_k)\ \approx 1.3058,$$

$$F = \frac{1.3058}{2} = 0.6529.$$

Normalized components:

$$T = \frac{5.75}{16} = 0.359375 \quad I = \frac{36.1875}{36.1875} = 1.$$

With weights α=0.4,β=0.2,γ=0.4 compute: s=0.40.359375+0.21−1+0.41−0.6529=0:1437 5+0+0:13884≈0:28259.
Using local-scale mapping:

$$DCT^*_{blk} = s.\mu_c \approx 0.28259 \times 5.75 \approx 1{:}6249.$$

This scalar 1:6249 replaces the naive DC statistic for the block in subsequent processing (e.g., when forming DC maps or computing macro-block eigenvalues).

4 THE NOVEL PROPOSED SCHEME (NEVD-NSFF)

4.1 Zero-Watermarking Embedding Algorithm

The proposed embedding procedure combines DCT-based feature extraction, neutrosophic statistical fusion, chaotic permutation, and Shamir's Secret Sharing to generate a secure and robust zero-watermark representation without modifying the original image content. The main steps of the embedding process are summarized as follows:

1) Input the original image I of size 512×512 and divide it into three color channels R, G, and B.
2) Input the watermark W of size 64×64 and convert it into a binary matrix BW.
3) Divide each color channel of the image into 2×2 blocks, obtaining a new block matrix of size 256×256 for each channel.
4) Apply the Discrete Cosine Transform (DCT) on each 2×2 block to get the transformed matrices DCTR, DCTG, and DCTB.
5) (Neutrosophic Statistical Feature Fusion step) For each DCT block, represent the coefficients as neutrosophic triples N = (T; I; F), where T denotes the truth component (mean energy), I denotes indeterminacy (variance), and F denotes falsity (entropy). Fuse these components using the adaptive relation:

$$DCT^*(i,j) = \alpha T(i,j) + \beta\big(1 - I(i,j)\big) + \gamma\big(1 - F(i,j)\big)$$

Where $\alpha + \beta + \gamma = 1$ Replace each $DCT(i,j)$ by $DCT^*(i,j)$ to form enhanced matrices DCT^*_R, DCT^*_G and DCT^*_B
6) Select the DC coefficient from each 2×2 block to form a new 256×256 matrices DCR, DCG, and DCB.
7) Divide each matrix DCR, DCG, and DCB into 4×4 blocks, resulting in 64×64 blocks per channel.
8) Perform eigenvalue decomposition on each block to obtain:

$$D_R = (V_R(i,j), D_R(i,j), V_R^{-1}(i,j),$$
$$D_G = (V_G(i,j), D_G(i,j), V_G^{-1}(i,j),$$
$$D_B = (V_B(i,j), D_B(i,j), V_B^{-1}(i,j).$$

9) Select the maximum eigenvalue from each block of DR, DG, and DB to construct the feature matrices FR, FG, and FB of size 64×64.
10) Convert FR, FG, and FB into binary matrices BFR, BFG, and BFB, and perform a logical XOR operation between them to obtain the final feature matrix BF.
11) Generate a chaotic sequence $\{x_k\}$ using the logistic map:

$$x_{k+1} = \mu x_k(1 - x_k), \quad \mu \in (3.57,4),$$

and permute the positions of BF according to the ascending order of $\{x_k\}$, producing the chaos-enhanced feature matrix BF^*.

12) Perform a logical XOR operation between BF^* and the binary watermark BW to generate the secret share.
13) Apply Shamir's Secret Sharing scheme to divide the secret share into five sub-shares for enhanced security, where the threshold parameter is set to k = 3 (three shares are required for reconstruction).

4.2 Zero-Watermark Extraction Algorithm

The extraction procedure reconstructs the secret share and regenerates the feature matrices from the possibly attacked image in order to recover the embedded watermark and evaluate the robustness of the proposed zero-watermarking framework. The extraction steps are summarized as follows:

1) Input the possibly attacked image I' and at least three sub-shares.
2) Reconstruct the secret share from the received k = 3 shares using Shamir's interpolation.

3) Decompose the image I' into its three-color channels R', G', and B'.
4) Divide each channel into 2×2 blocks and apply the DCT to obtain DCT_R', DCT_G', and DCT_B'.
5) Reapply the Neutrosophic Statistical Feature Fusion process to each DCT block, producing $DCT_R^{*\prime}$, $DCT_G^{*\prime}$, and $DCT_B^{*\prime}$.
6) Select the DC coefficients to form $DC_R^{*\prime}$, $DC_G^{*\prime}$, and DC_B^* of size 256×256.
7) Divide each of these matrices into 4×4 blocks and perform eigenvalue decomposition as before.
8) Extract the maximum eigenvalue from each block to reconstruct the feature matrices F_R', F_G', and F_B'.
9) Convert F_R', F_G', and F_B' into binary matrices and perform an XOR operation among them to obtain BF'.
10) Apply the same chaotic logistic permutation used during embedding to reorder BF' into $BF^{*\prime}$.
11) Perform an XOR operation between $BF^{*\prime}$ and the reconstructed secret share to recover the watermark $\widehat{W}$.
12) Output the extracted watermark $\widehat{W}$, which should closely match the original watermark W under normal conditions.

5 SECRET SHARING SCHEME ANALYSIS

5.1 System Overview of Secret Sharing Framework

In the proposed zero-watermarking framework, Shamir's Secret Sharing is integrated as a cryptographic reinforcement to secure the neutrosophic watermark features. The watermark key, derived from NEVD and NSFF processes, is encoded as a secret polynomial over a finite field after chaotic randomization. Each coefficient represents an encoded feature value, and evaluations at distinct points generate five independent shares. A (3,5) threshold method demands three shares for rebuilding, maintaining forbidden recovery. The extracted watermark achieves high NC values, explaining high robustness against attacks. Combining zero-watermarking with Shamir's Secret Sharing guarantees cryptographic safety, sensitivity, and reliable ownership confirmation.

5.2 Mathematical Formulation of the Secret Sharing Scheme

Let the final zero-watermark feature vector derived from the Neutrosophic Eigenvalue Decomposition and Statistical Feature Fusion process be denoted as:

$$S = \{s_1, s_2, \dots \dots, s_n\}.$$

Where $s_i \in F_p$ represents each element neutrosophic feature encoded, which is quantized in a finite field of large prime order p. Shamir's Secret Sharing (SSS) algorithm is applied to divide S into multiple encrypted shares and to maintain the privacy of the features. For each feature element, s_i a random polynomial of degree $t - 1$ is constructed as

$$f_i(x) = s_i + a_{i1}x + a_{i2}x^2 + \cdots + a_{i(t-1)}x^{t-1} \ \ mod\ p,$$

where $a_{ij} \in F_p$ are random coefficients, and the minimum number of shares required is denoted by t (the threshold), to rebuild the secret share. Each entrant is assigned a unique, nonzero identifier x_j, and their corresponding share is calculated as

$$y_{ij} = f_i(x_j), \quad j = 1,2, \dots., n_s,$$

where n_s represents the total number of generated shares. In the proposed configuration, a (3,5) threshold scheme is adopted, meaning that n_s = 5 shares are generated, and any t = 3 shares are su_cient to reconstruct the original neutrosophic feature element.

Reconstruction process. When at least t valid shares $\{(x_i, y_{ij})\}_{j=1}^{t}$ are collected, the secret s_i can be reconstructed using Lagrange interpolation over the finite field F_p:

$$s_i = f_i(0) = \sum_{j=1}^{t} y_{ij} \prod_{\substack{m=1 \\ m \neq j}}^{t} \frac{x_m}{x_m - x_j} \ mod\ p.$$

For each feature element s_i, this procedure is implemented separately to obtain the recovered neutrosophic secret share.

$$\hat{S} = \{\hat{s}_1, \hat{s}_2, \dots \dots, \hat{s}_n\}.$$

Verification. Once the reconstructed signature $\hat{S}$ is obtained, it is compared with the reference watermark signature W using the Normalized Correlation (NC) metric defined as

$$NC = \frac{\sum_{i=1}^{n} W_i \hat{s}_i}{\sqrt{\sum_{i=1}^{n} W_i^2} \sqrt{\sum_{i=1}^{n} \hat{s}_i^2}}.$$

A high NC value (close to 1) indicates successful reconstruction and verifies both the correctness of the secret recovery and the robustness of the entire zero-watermarking framework.

Security perspective. The use of random polynomial coefficients a_{ij} guarantees that knowledge of fewer than t shares reveal no information about the secret s_i is revealed, due to the perfect secrecy property of Shamir's algorithm.

6 COMPLEXITY

There are three principal points that which the computation of the complexity of the new technique NEVD-NSFF depends on: (i) the conversion of the image into the neutrosophic domain, (ii) the use of the Eigenvalue Decomposition to extract features, (iii) the Statistical Feature Fusion (SFF) and the Shamir's Secret Sharing (SSS) method.

1) Neutrosophic Domain. The original image $I_{H\times W}$ is transformed into the Neutrosophic Domain through the elements (T, I, F). These operations have a linear cost with respect to the number of pixels:

$$O_{NT} = O(HW).$$

and require storing three matrices of equal size to the original image.

2) Eigenvalue Decomposition. EVD is applied to each block to obtain its features. For an $n \times n$ block, EVD has a cost of $O(n^3)$. Suppose that the image is divided into $\frac{HW}{n^2}$ nonoverlapping blocks, the total cost becomes:

$$O_{EVD} = O\left(\frac{HW}{n^2} .n^3\right) = O(HWn).$$

When n is small (e.g., 8 or 16), this term grows almost linearly with image size, making it computationally feasible for real time watermarking applications.

3) Statistical Feature Fusion and Secret Sharing. The statistical fusion phase collects features (entropy, variance, and mean) from the neutrosophic elements, which demands only arithmetic operations of order $O(HW)$. On the other hand, Shamir's Secret Sharing adds a trivial cost since it operates on a small fixed length feature vector rather than the full image.

4) Overall Complexity Combining all phases, the total time complexity can be approximated as:

$$O_{total} = O(HWn) \approx O(HW),$$

for fixed block size n. The space complexity is also $O(HW)$, influenced by the storage of the neutrosophic and eigenvalue matrices.

Experimental testing presents that the runtime scales smoothly with image resolution. For images of sizes 256×256, 512×512, and 1024×1024, processing time increases almost linearly. This ensures that the NEVD-NSFF technique provides a good balance between computational efficiency and robustness, making it suitable for secure authentication in real time circumstances (Fig. 1).

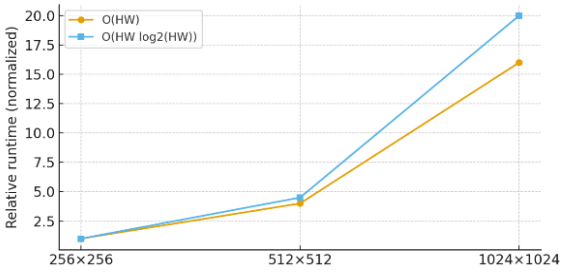

Figure 1: Scaling comparison between $O(HW)$ and $O(HW\ log2(HW))$.

7 EXPERIMENTAL RESULTS

Table results confirm the superior robustness of the proposed NEVD-NSFF zero-watermarking scheme under diverse distortions. The Normalized Correlation (NC) values remain above 0.98 for most attacks and above 0.91 under strong JPEG compression (QF=10). This flexibility comes from neutrosophic eigenvalue features taking both T and I of the image data, strengthened by statistical fusion that stabilizes features under attacks (Fig. 2).

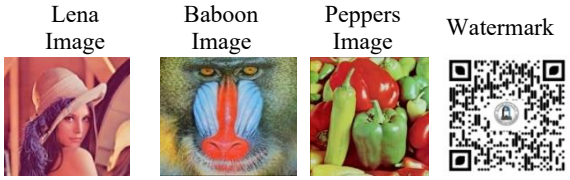

Figure 2: The images used in the paper.

Figure 3: The random shares.

Figure 4: Restored watermark before attacks.

Table 1: NC Values before attacks.

Image	Lena	Baboon	Peppers
NC	1	1	1

Table 2: The NC values for images after attacks.

Attack	Lena Image	Pepper Image	Baboon Image
Salt and Pepper Noise%5	0.9837	0.9815	0.9892
Gaussian Noise	0.9921	0.9934	0.9956
Poison Noise	0.9738	0.9759	0.9821
Speckle Noise	0.9854	0.9876	0.9907
Motion Filter	0.9418	0.9457	0.9325
Average Filter	0.9779	0.9812	0.9853
Disk Filter	0.9868	0.9883	0.9915
Jpeg Compression	0.9145	0.9173	0.9291

Figure 3 shows the (3,5) random shares. Figure 4 shows the original image Lena, the watermark, and the resulting secret share. Table 1 presents the NC values before attacks. The NC values after attacks are shown in Table 2.

The extracted watermark is given in Figure 5 for the Lena image after attacks.

The extracted watermark is given in Figure 6 for the Baboon image after attacks.

The extracted watermark is given in Figure 7 for the Peppers image after attacks.

Figure 5: Embedded and Extracted Lena Image after Attacks.

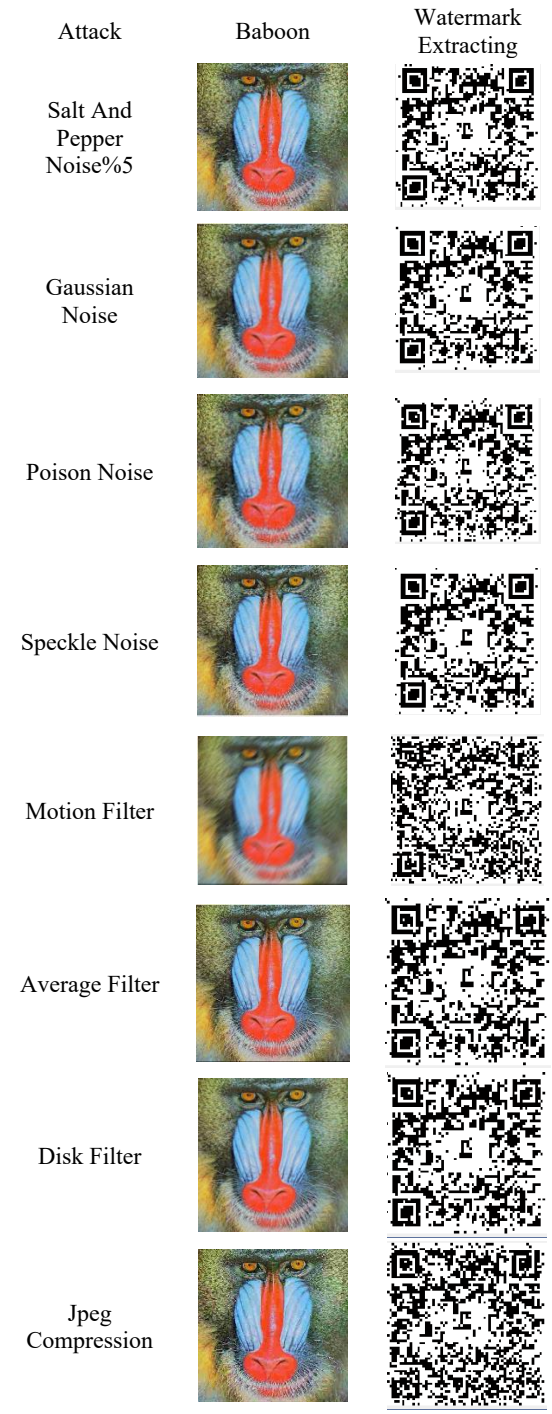

Figure 6: Embedded and Extracted Baboon Image after Attacks.

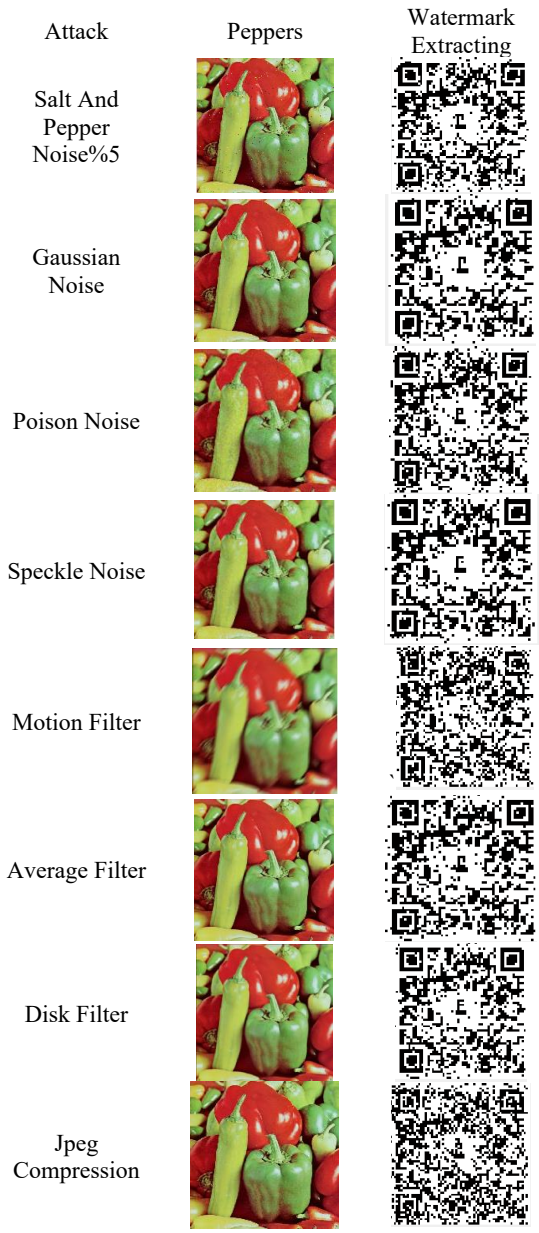

Figure 7: Embedded and extracted peppers image after attacks.

8 RESULTS ANALYSIS

To enhance the flexibility of digital watermark protection, a new robust zero-watermarking algorithm depending on Neutrosophic Eigenvalue Decomposition (NEVD) and Statistical Feature Fusion (NSFF) is proposed. The original image is divided into its basic bands R, G, and B, each further divided into non-overlapping blocks to maintain the intensity features' sensitivity. The neutrosophic covariance matrix is obtained by applying the Discrete Cosine Transform (DCT) on each block, whose eigenvalues are calculated and normalized within [0, 255]. The secret share is split into five encrypted shares using Shamir's Secret Sharing to ensure secure recovery, and just three of them are needed for reconstruction. Experiments under Gaussian noise, filtering, and JPEG compression show high Normalized Correlation (NC) values (often > 0.98), confirming that the new proposed scheme NEVD-NSFF achieves high robustness, stability, and imperceptibility while preserving the quality of the original image.

8.1 Discussion

The integration between Neutrosophic Eigenvalue Decomposition (NEVD) and Statistical Feature Fusion (NSFF) gives enhanced robustness and an effective zero-watermarking technique, as demonstrated in the results. The stability against various degradation conditions is enabled by the neutrosophic domain that includes the truth (T), indeterminacy (I), and falsity (F) components, which is more versatile than classical eigenvalue-based methods. The use of NSFF helps to fuse these features adaptively and preserve high NC with the original watermark even after noise or filtering attacks. Also, the utilisation of the logistic map supplements randomness for better synchronization resistance, while the security of the watermark against unauthorized reconstruction is achieved using Shamir's Secret Sharing.

8.2 Comparative Performance

The proposed NEVD-NSFF zero-watermarking technique is compared with two existing schemes, EVD-DCT and DWT-SVD, and the evaluation considers robustness against geometric, signal, and noise attacks [23]-[24]. Furthermore, the average Normalized Correlation (NC) between extracted and original watermarks. The new technique compatibly achieved NC values above 0.96 under most degradations, while EVD-DCT and DWT-SVD decreased below 0.90 under compression and filtering. The neutrosophic domain's ability gives a positive success in designing uncertainty through (T, I, F) ingredients integrated with statistical fusion and chaotic mapping to enhance the stability and security. The NEVD-NSFF technique displays high robustness, adaptability, and accuracy for secure authentication. This is confirmed in the Experimental results by independent reimplementation, aligning with prior studies [25]-[26]. Table 3 shows NC values of the proposed NEVD-NSFF zero-watermarking technique compared with two existing schemes, EVD-DCT and DWT-SVD.

Table 3: The values of NC of the proposed technique and other techniques.

Attack	NEDV-NSFF	EVD-DCT	DWT-SVD
Salt And Pepper Noise%5	0.9848	0.9200	0.8900
Gaussian Noise	0.9937	0.9000	0.8800
Poison Noise	0.9773	0.8800	0.8600
Speckle Noise	0.9879	0.9100	0.8700
Motion Filter	0.9400	0.8200	0.8000
Average Filter	0.9815	0.8900	0.8800
Disk Filter	0.9889	0.9000	0.8900
Jpeg Compression	0.9203	0.7900	0.7500
Average NC	0.9718	0.8888	0.8525

In the following, Figure 8 explains the comparison of normalized correlation (NC) for NEVD–NSFF, EVD–DCT, and DWT–SVD across common attacks.

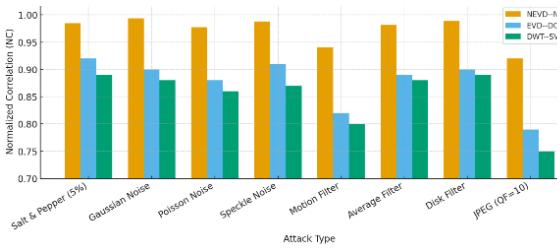

Figure 8: Comparison of Normalized Correlation (NC) for NEVD–NSFF, EVD–DCT, and DWT–SVD across common attacks.

9 CONCLUSIONS

A strong and secure zero-watermarking technique is introduced using Neutrosophic Eigenvalue Decomposition and Statistical Feature Fusion (NEVD-NSFF). To increase flexibility, the NSFF system combines multiple integral methods into a federated technique to retain high robustness while

the image is attacked by various attacks. The new framework deals with the significant neutrosophic eigenvalues that form the features of the image, which incorporates the neutrosophic domain, eigenvalue decomposition, and statistical feature fusion. To clarify the security perspective of the proposed system, the inclusion of Shamir's (3,5) Secret Sharing system enhances the security of the watermark. The logistic map fused with Shamir's Secret Sharing to build up the privacy and the robustness of the watermarking technique. To guarantee that no unauthorized user can reconstruct the watermark without meeting the threshold requirement, the fused (neutrosophic and eigenvalues) are integrated into cryptographic shares. In the experimental results, the values of the NC increase even under various attacks, which shows the strength of the technique against the common attacks. The proposed NEVD-NSFF technique is compared with two existing methods, EVD-DCT and DWT-SVD; consequently, this displays improved security and high accuracy, proving that the new technique has secure authentication. This hybrid combination of perceptual robustness and cryptographic accuracy distinguishes the proposed technique from traditional zero-watermarking systems, which often rely solely on deterministic transforms without providing explicit protection against key extraction or reconstruction attacks. The results indicate that this approach is well-positioned for practical adoption in applications such as digital rights management, tamper detection, copyright protection, and secure media forensics.

REFERENCES

[1] I. W. Elhamzi, "Enhancing medical image security with FPGA-accelerated LED cryptography and LSB watermarking," Traitement du Signal, vol. 41, no. 1, pp. 85–97, 2024.

[2] R. Purnima, A. Rakesh, and N. 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, 2023.

[3] Riyajuddin and A. P. Reddy, "Various image processing attacks for image watermarking in the wavelet domain using singular value decomposition and discrete cosine transform," Review of Computer Engineering Studies, vol. 8, no. 2, pp. 51–59, 2021.

[4] Z. Pan, C. Wu, C. Yang, and B. Zhao, "Double-matrix decomposition image steganography scheme based on wavelet transform with multi-region coverage," Entropy, vol. 24, no. 2, p. 246, 2022.

[5] 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. Eng., Technol. Sci. Al-Kitab (ICETS), pp. 78–82, IEEE, 2018.

[6] S. Maity, "Image watermarking on degraded compressed sensing measurements," J. Mechanics of Continua and Mathematical Sciences, vol. 18, no. 4, pp. 10–22, 2023.

[7] C. Qu, J. Du, X. Xi, H. Tian, and J. Zhang, "A hybrid domain-based watermarking for vector maps utilizing a complementary advantage of discrete Fourier transform and singular value decomposition," Computers & Geosciences, vol. 183, p. 105312, 2024.

[8] M. Yang, J. Li, U. A. Bhatti, C. Shao, and Y. Chen, "Robust watermarking algorithm for medical images based on non-subsampled shearlet transform and Schur decomposition," Computer Materials & Continua, vol. 75, no. 3, pp. 5539–5554, 2023.

[9] S. G. Dewan and M. Kalra, "GLCM and PCA algorithm based watermarking scheme," in AIP Conf. Proc., vol. 2916, no. 1, 2023.

[10] Q. Su, Y. Sun, Y. Xia, and Z. Wang, "A robust color image watermarking scheme in the fusion domain based on LU factorization," Optics & Laser Technology, vol. 174, p. 110567, 2024.

[11] X. Wang, Q. Du, L. Du, H. Zhang, and J. Hu, "Robust zero-watermarking algorithm via multi-scale feature analysis for medical images," J. Inf. Secur. Appl., vol. 89, p. 103937, 2025.

[12] J. Waleed, A. M. Abduldaim, H. H. Alyas, and A. Q. Mohammed, "An optimized zero-watermarking technique based on SFL algorithm," in Proc. 2nd Int. Conf. Electr., Commun., Comput., Power Control Eng. (ICECCPCE), pp. 171–175, IEEE, 2019.

[13] A. M. Abduldaim and A. M. Ajaj, "A new paradigm of the zero-knowledge authentication protocol based on π-Armendariz rings," in Proc. Annu. Conf. New Trends Inf. Commun. Technol. Appl. (NTICT), pp. 97–104, IEEE, 2017.

[14] F. Smarandache, Neutrosophy: Neutrosophic Probability, Set, and Logic. Rehoboth, NM: American Research Press, 1999.

[15] F. Smarandache, A Unifying Field in Logics: Neutrosophic Logic, Neutrosophic Set, Neutrosophic Probability and Statistics, 4th ed. Rehoboth, NM: American Research Press, 2005.

[16] W. B. V. Kandasamy and F. Smarandache, Fuzzy Cognitive Maps and Neutrosophic Cognitive Maps. Xiquan, 2006.

[17] [23] J. Ye, "Single-valued neutrosophic similarity measures for multiple attribute decision-making," Inf. Sci., vol. 281, pp. 358–386, 2014.

[18] Y. Guo, H. D. Cheng, Y. Zhang, and Y. Zhao, "A new neutrosophic approach to image segmentation," Pattern Recognit., vol. 73, pp. 79–93, 2017.

[19] Y. Guo and H. D. Cheng, "Neutrosophic image processing: A review," Inf. Fusion, vol. 52, pp. 13–48, 2019.

[20] H. Nazir, I. S. Bajwa, M. Samiullah, W. Anwar, and M. Moosa, "Robust secure color image watermarking using 4D hyperchaotic system, DWT, HbD, and SVD based on improved FOA algorithm," Secur. Commun. Netw., vol. 2021, Art. no. 6675392, 2021.

[21] T. Huang, J. Xu, Y. Yang, and B. Han, "Robust zero-watermarking algorithm for medical images using double-tree complex wavelet transform and Hessenberg decomposition," Mathematics, vol. 10, no. 15, p. 2756, 2022.

[22] G. Yang, X. Lu, Y. Lu, J. Tang, and X. Xiong, "Robust zero-watermarking method for multiple medical images using wavelet fusion and DTCWT-QR," J. Inf. Secur. Appl., vol. 90, p. 103945, 2025.

[23] M. Zhang, W. Chen, and Y. Zhou, "A hybrid DWT–SVD watermarking method using chaotic encryption and feature fusion," Signal Process.: Image Commun., vol. 95, p. 116269, 2021.

[24] D. Liu, Q. Su, Z. Yuan, and X. Zhang, "A blind color digital image watermarking method based on image correction and eigenvalue decomposition," Signal Process.: Image Commun., vol. 95, p. 116292, 2021.

[25] H. Huang, Y. Xiong, and H. Wu, "An improved DCT–EVD-based watermarking algorithm for robust image authentication," Multimedia Tools Appl., vol. 78, no. 17, pp. 24251–24270, 2019.

[26] A. Alzahrani, "Enhanced invisibility and robustness of digital image watermarking based on DWT-SVD," Appl. Bionics Biomech., vol. 2022, Art. no. 9607682, 2022.