A Hybrid Image Zero-Watermarking Technique Based on Sigmoid-Neutrosophic Domain and SVD

Hussein Kadhim Abdali[1], Areej M. Abduldaim[1(✉)], and Matheel E. Abdulmunim[2]

[1] Department of Mathematics and Computer Applications, College of Applied Sciences, University of Technology, 10001 Baghdad, Iraq
Areej.M.Abduldaim@uotechnology.edu.iq

[2] Multimedia and Digital Media Department, College of Computer Sciences, University of Technology, 10001 Baghdad, Iraq

Abstract. This paper aims to devise a robust hybrid image zero watermarking scheme using the concept of a neutrosophic set. It proposes to extend the traditional neutrosophic domain by introducing a new definition of neutrosophic membership functions used to construct this domain, with particular emphasis on the T function, which is used to extract stable local image features and enhance the representation of distinctive features. The image is converted to a neutrosophic form with three components: T (Truth), I (Indeterminacy), and F (False), to maximize the opportunity to select concentrated features, combining the novel neutrosophic domain and singular value decomposition (SVD) to verify image authenticity. The proposed T transforms raw pixel intensities into locally normalized structural descriptors that are highly sensitive to local tampering, which allows for resistance to common attacks by extracting robust image features that are stable and distinctive. Using the proposed membership functions, the cover image is transformed into the neutrosophic form, then the main exporter is utilized to extract features, being the component T. To obtain robust features, divide T into nonoverlapping blocks and then apply the SVD to each block. Three strategies are adopted to extract features and investigate the density effect of these features on watermarking performance. The resulting features and the watermark are integrated through an XOR logic operation to produce the zero watermark. Experimental results on standard paradigm images demonstrate strong robustness against common attacks. The findings show that the proposed T plays a key role in improving feature stability and overall authentication performance.

Keywords: Sigmoid function · Truth membership function · Neutrosophic domain · SVD · Image Zero watermarking

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2027
O. Gervasi et al. (Eds.): ICCSA 2026 Workshops, LNCS 16758, pp. 344–364, 2027.
https://doi.org/10.1007/978-3-032-30497-1_21

1 Introduction

As technology advances, so too do digital image transmission methods in medical diagnostics, intelligent decision making systems, communications, and surveillance. This expansion in image usage has increased the risks of illegal manipulation, redistribution, and forgery, making intellectual property protection and reliable image verification increasingly important objectives [1]. Based on the above, the mechanism of zero watermarking technology, which ensures the preservation of essential image characteristics without altering the original data, makes it the most suitable for sensitive applications that require maintaining image accuracy, unlike traditional watermarking approaches that rely on changing spatial information in the original image [2].

Florentin Smarandache in [3] generalized fuzzy logic and introduced two new concepts neutrosophy which is the study of neutralities as an logic extension; and its derivative neutrosophic, such as neutrosophic logic, neutrosophic set, neutrosophic probability, and neutrosophic statistics and thus new approaches beganing in scientific research for four areas: set theory, probabilityand statistics, logics, and philosophy. Early works [4] and [5] in image processing each pixel represents using three independent components called the membership functions: T (the truth), I (the indeterminacy), and F (the falsity). This gives richer features compared to classical or fuzzy forms. Next studies extended these concepts to clustering [7] edge detection [6] and classification [8]. A neutrosophic fuzzy clustering method depending on non local information is introduced in [9, 10] to develop an edge detection process and denoising of the image segmentation algorithm.

Decompositions such as GSVD [11] and Hessenberg [12] have been used effectively in many papers for sharing images securely and achieving zero watermarking algorithms. Moreover, SVD [1] is particularly effective due to the robustness of its singular values to common signal processing operations. Optimization algorithms further emphasize the importance of stable feature selection for improving watermark resilience [13, 14].

The difficulty in ensuring ownership, authenticity, and privacy has become a reality due to the constant development of new and sophisticated digital technologies, as well as the ease of sharing images online [15, 16]. Conventional watermarking methods embed information directly into images, often introducing distortion and increasing vulnerability to attacks [17]. In rapid progress, and to overcome the limitations of existing technologies, image zero watermarking techniques were developed, relying on methods that extract the features with high precision and secure mathematical modeling to preserve ownership without manipulating the real image [18, 19].

The widespread use of DCT and DWT in image zero watermarking techniques has not made them entirely robust against various attacks because they depend on image features that are sensitive to distortion [20]. From the same perspective, the statistical methods like PCA and GLCM for extracting features are also sensitive to noise and illumination variations [21, 22]. Depending on this shortcoming, more robust methods are motivated to be developed to enhance the stability of the extracted features, in addition to addressing valuably uncertainty in the image [23, 24].

To provide a neutrosophic environment and find effective image features, converting images to a neutrosomatic domain and finding the T component is a more reliable step that efficiently handles image enhancement, watermarking, and classification. For robust

zero watermarking, a neutrosophic form becomes the most satisfactory and flexible under noisy and uncertain various conditions, which is essential to stability and accuracy.

The limitations of the previous techniques motivate the proposal of a hybrid zero-watermarking technique that combines a neutrosophic domain and SVD to extract features using the idea of a sigmoid membership function. The difference between traditional functions and the proposed membership function is that the proposed T-function focuses on features specific to the block itself, rather than on image features in general, and simultaneously reduces noise-sensitive variations through the inclusion of local mean and deviation in a nonlinear functionThis makes the choice among the features better and more stable, especially under common image processing operations, which gives a successful equilibrium between sensitivity and robustness.

The remainder of the paper is ordered as follows. Section 2 provides the background information needed. Section 3 identifies the materials and methods to construct the new image neutrosophic domain and design the image watermarking scheme. In Sect. 4, the experimental results for three cases of feature extraction before and after attacks are given. Section 5 demonstrated the methodology analysis of the proposed algorithms and experimental results. In Sect. 6, the conclusion is included.

2 Background

In this section, existing concepts and methods related to the image neutrosophic domain are provided.

2.1 Neutrosophic Domain Structure

The neutrosophic framework represents any proposition, event, or set-membership using an ordered triple $(\boldsymbol{T}, \boldsymbol{I}, \boldsymbol{F})$, where $\boldsymbol{T}$ denotes the degree of truth, $\boldsymbol{I}$ the degree of indeterminacy, and $\boldsymbol{F}$ the degree of falsity. Each component is defined as a real subset of the interval $[-\mathbf{0}, +\mathbf{1}]$, and the three components are mutually independent—there is no requirement that $\boldsymbol{T} + \boldsymbol{I} + \boldsymbol{F} = 1$. This independence allows the model to characterize incomplete, inconsistent, and indeterminate information more flexibly than classical and fuzzy approaches [25].

The Neutrosophic image is the way in which each pixel, $P(x, y)$, in the image is interpreted such that three membership functions represent it $T(x, y), I(x, y)$, and $F(x, y)$ where these membership functions represent membership in the bright pixel set, the indeterminate set, and the non-bright pixel set, respectively [26].

A neutrosophic image P_{NS} is characterized by three membership sets T, I, and F [4].

The pixel $P(i, j)$ in the image domain is transformed into the neutrosophic domain. $P_{NS}\ (i, j) = T(i, j), I(i, j), F(i, j)$. The functions $T(i, j), I(i, j)$ and $F(i.j)$ are the membership values defined as

$$T(i, j) = \frac{\overline{g}(i, j) - \overline{g}_{\min}}{\overline{g}_{\max} - \overline{g}_{\min}},$$

where $\overline{g}(i,j) = \frac{1}{w \times w} \sum_{m=i-w/2}^{i=w/2} \sum_{n=j-w/2}^{j+w/2} g(m,n)$

$$I(i,j) = \frac{\delta(i,j) - \delta_{\min}}{\delta_{\max} - \delta_{\min}}$$

where $\delta(i,j) = |g(i,j) - \overline{g}(i,j)|$

$$F(i,j) = 1 - T(i,j)$$

where $g(i,j)$ is the intensity value of the pixel (i,j), $\overline{g}(i,j)$ is the local mean value of $g(i,j)$ (e.g., window average), $\delta(i,j)$ is the absolute value of the difference between intensity $g(i,j)$ and its local mean value $\overline{g}(i,j)$.

2.2 Normalization and Mapping Functions:

To define a neutrosophic domain, a set of statistical mapping functions, including Z-score normalization, Gaussian weighting, and sigmoid transformation, is needed to stabilize the extracted image features.

Sigmoid Function. The sigmoid function, also called the sigmoidal curve or logistic function, is defined as a mathematical equation that produces outputs ranging between 0 and 1, resulting in an S-shaped graph [27]. It is commonly used in artificial neural networks to align outputs with standard probability situations, machine learning, image processing, optimization, and normalization tasks. It is the function:

$$y = \frac{1}{1 + e^{-x}}$$

where $x \in R$ and $y \in (0,1)$.

Score Normalization. The Z- score normalization converts the data to have a mean = 0 and a standard deviation = 1. This operation adjusts the values of the data according to how far they deviate from the mean, and it measured in units of standard deviation. Because of the different scales they have, the significance of this process is to avoid the dominance of certain features over others. Consequently, this affects the achievement of machine learning designs.

$$z = \frac{p - \mu}{\sigma}$$

where p is the value of the data point, μ is the mean of the dataset, σ is the standard deviation of the dataset.

Gaussian Function. In mathematics, a Gaussian function, often simply referred to as a Gaussian, is a function of the base form

$$f(x) = \exp(-x^2)$$

and with parametric extension

$$f(x) = a\left(-\frac{(x - b^2)}{2c^2}\right)$$

for arbitrary real constants a, b, and non-zero c.

A Gaussian weighting function is a mathematical tool that assigns weights to data points based on their distance from a central point, using a bell-shaped curve formula to give higher importance to nearby data and lower importance to distant data.

2.3 Singular Value Decomposition (SVD)

Let $A \in \mathbb{R}^{m\times n}$(or $\mathbb{C}^{m\times n}$). Then there exist orthonormal (unitary) matrices $U \in \mathbb{R}^{m\times m}$, $V \in \mathbb{R}^{n\times n}$, and a diagonal matrix $\Sigma = \text{diag}(\sigma_1, \ldots, \sigma_p)$, $p = \min(m, n)$, with non-negative entries $\sigma_1 \geq \cdots \geq \sigma_p \geq 0$, such that

$$A = U\Sigma V^T.$$

where σ_i are the singular values of A, Columns of U and V are the left and right singular vectors, respectively. If $\text{rank}(A) = r$, then $\sigma_1, \ldots, \sigma_r > 0$ and the remaining singular values are zero. Equivalently, $A = \sum_{i=1}^{r} \sigma_i u_i v_i^T$.

Moreover, for any $k \leq r$, the truncated sum of the first k terms gives the best rank-k approximation to A in the least-squares sense [28].

3 Materials and Methods

This section describes the materials and methodology used to evaluate the proposed watermarking scheme. First, the dataset and experimental environment employed in the experiments are presented. Then, the main steps of the proposed algorithms are described, including image preprocessing, feature extraction, zero watermark (secret share) generation, and authentication procedures (zero-watermark construction). Finally, the evaluation metrics and attack models used to assess the performance of the system are introduced.

3.1 Experimental Materials

The materials used in this work comprise the experimental paradigm test images, the watermark images, and the implementation environment.

Paradigm Images and Implementation Environment. The experiments were conducted using four paradigm images, which are commonly used in image processing and watermarking literature (Baboon, Peppers, Girl, and Village Road) of size 256 × 256, obtained from the USC-SIPI Image Database, University of Southern California, which is widely available and a standard paradigm dataset in image processing research. All experiments were performed using MATLAB R2023a software on a computer with an Intel Core i5 processor and 8 GB RAM in Windows 10. These paradigm images allow fair comparison with existing methods. These paradigm images allow fair comparison with existing methods (Fig. 1).

Watermark Images. Three binary watermark images of size 256 × 256,128 × 128 and 64 × 64 were used in the experiments. Each watermark image is converted into a binary sequence before generating the zero watermark. The watermark is generated for the link to the University of Technology website: https://uotechnology.edu.iq/en/ (Fig. 2)


Baboon Peppers Girl Village Road

Fig. 1. The images used in this work



Fig. 2. The QR watermark images used in this paper

3.2 The Proposed Theoretical Methods and Algorithms

In this section, new membership functions are proposed and proved suitable for designing a new neutrosophic domain, and, as an application of this new domain, a zero watermarking technique is proposed to construct a zero-watermark and recover a watermark image.

The Proposed Membership Functions of the Improved Neutrosophic Domain. To enhance feature representation, the image is transformed into a new neutrosophic domain, which represents pixels using the three proposed membership components $T(i,j)$, $I(i,j)$ and $F(i,j)$.

Truth Membership Function T. Suppose that

$$Z(i,j) = \frac{I(i,j) - \mu_L}{\sigma_L + \epsilon}$$

where $I(i,j)$ is the pixel intensity, μ_L is the local mean (computed in a window around the pixel), σ_L is the local standard deviation, $\varepsilon > 0$ is a small stabilizer to avoid division by zero for numerical stability, and k contrast sensitivity controlle Let $x = kZ(i,j)$, then

$$T(i,j) = \frac{1}{1 + e^{-k\frac{I(i,j)-\mu_L}{\sigma_L+\epsilon}}} = \frac{1}{1+e^{-x}}$$

is a membership function.

Proof: To prove that $T(i,j)$ is a membership function, showing each of the three functions takes values in the interval [0,1]. Since

$$x = k\frac{I(i,j) - \mu_L}{\sigma_L + \varepsilon}$$

which is a finite real number because the denominator > 0 and $k, I(i,j), \mu_L$ are finite. The logistic function

$$T(i,j) = \frac{1}{1 + e^{-k\frac{I(i,j)-\mu_L}{\sigma_L+\epsilon}}} = \frac{1}{1+e^{-x}}$$

has the well-known range $0 < T(i,j) < 1$ for every finite real x. Therefore,
$0 < T(i,j) < 1$. Hence $T(i,j) \in [0,1]$.

Indeterminacy Membership Function I. Classical neutrosophic indeterminacy is commonly defined based on the normalized deviation from the local mean [Guo and Cheng, 2009]. In the proposed neutrosophic representation, an improved indeterminacy membership function is introduced based on a logarithmic nonlinear transformation of the truth membership $T(i,j)$.

Let $T(i,j) \in [0, 1]$ denote the truth-membership value obtained from the sigmoid-based normalization. We define the preliminary function:

$$f(T(i,j)) = -\log(T(i,j) + \varepsilon) + (1 - T(i,j))\log(1 - T(i,j) + \varepsilon),$$

where $\varepsilon > 0$ is a small constant to ensure numerical stability.

Since $f(T(i,j))$ does not necessarily lie in the interval [0, 1], it cannot be directly used as a valid membership function. Therefore, we propose the following normalized indeterminacy membership function:

$$I_N(i,j) = \frac{f(T(i,j)) - f_{min}}{f_{mix} - f_{min}}$$

Where

$$f_{min} = min_{r\in[0,1]} f(T), \quad f_{mix} = mix_{r\in[0,1]} f(T)$$

Based on the monotonic decreasing behavior of $f(T)$ the extrema occur at the boundary points.

$$f_{mix} = f(0) = -\log(\varepsilon) + \log(1 + \varepsilon)$$

$$f_{mix} = f(1) = -\log(1 + \varepsilon),$$

Thus, the proposed indeterminacy membership function can be written explicitly as:

$$I_N(i,j) = \frac{-\log(T(i,j) + \varepsilon) + (1 - T(i,j))\log(1 - T(i,j) + \varepsilon) + \log(1 + \varepsilon)}{-\log(\varepsilon) + 2\log(1 + \varepsilon)}$$

The function $I_N(i,j)$ is a valid membership function, i.e.,

$$I_N(i,j) \in [0, 1], \quad \forall (i,j)$$

Proof
Let $T(i,j) \in [0, 1]$ and define

$$f(T) = -\log(T + \varepsilon) + (1 - T)\log(1 - +\varepsilon),$$

Since the logarithmic function is continuous on $(0, \infty)$ and $\varepsilon > 0$, it follows that $f(T)$ is continuous on the closed interval [0, 1]. Therefore, by the extreme value theorem, $f(T)$ attains its minimum and maximum values on [0, 1], denoted by f_{min} and f_{mix}, respectively.

Thus, for all $T \in [0, 1]$,

$$f_{min} \leq f(T) \leq f_{mix}$$

Subtracting f_{min} from all sides yields.

$$0 \leq f(T) \leq f_{min} \leq f_{mix} - f_{min}$$

Since $f_{mix} - f_{min} > 0$, dividing both sides by $f_{mix} - f_{min}$ gives:

$$0 \leq \frac{f(T) - f_{min}}{f_{mix} - f_{min}} \leq 1$$

By definition,

$$I_N(i, j) = \frac{f(T(i, j)) - f_{min}}{f_{mix} - f_{min}}$$

Hance

$$0 \leq I_N(i, j) \leq 1$$

Therefore, $I_N(i, j))$ satisfies the fundamental condition of a membership function.

$$I_N(i, j) \in [0, 1]$$

Classical neutrosophic indeterminacy component $I(i, j)$ is a deviation-based (linear, symmetric), while the improved indeterminacy membership function $I_N(i, j)$ is logarithmic, asymmetric, and information-driven.

Falsity Membership Function F. It is clear that

$$F(i, j) = 1 - T(i, j)$$

is a membership function.

This transformation allows the algorithm to separate deterministic information from uncertainty, improving watermark robustness.

Comparative Justification with Classical Neutrosophic Membership Functions
Compared to classical neutrosophic models, the proposed membership functions provide a more adaptive and discriminative representation. The truth membership $T(i, j)$ uses a nonlinear sigmoid mapping based on local mean and deviation, enhancing structural contrast and suppressing noise. Including a nonlinear transformation, the indeterminacy $I(i, j)$ membership function is defined for feature extraction and fragility to thin variations. The falsity $F(i, j) = 1 - T(i, j)$ benefits indirectly from the improved definition of $T(i, j)$. Overall, the proposed formulation better captures local structures and balances robustness and sensitivity.

Interpreting the convenience of the Proposed Membership Function T for Zero-Watermarking

The truth membership function $T(i,j)$ constitutes the core component of the proposed framework. Unlike conventional mappings based on raw or globally normalized intensities, $T(i,j)$ encodes the locally normalized deviation of a pixel from its neighborhood $Z(i,j)$. Specifically, values of $T(i,j)$ close to 1 or 0 correspond to locally dominant or recessive structures, whereas values near 0.5 indicate structurally neutral regions. The proposed formulation offers the following advantages: (i) The local adaptivity, which means that the utilization of μ_L and σ_L permits the function to adapt to local image statistics, preserving structural frequency and reducing sensitivity to illumination changes. (ii) Bounded and stable output since $0 < T(i,j) < 1$, then it is easy to use in feature extraction phase and recovery phase. (iii) The control sensitivity parameter k keeps balance between sharpening and smoothness, this implies the function is flexible making robust, semi-fragile, or fragile. Whenever k increasing, then the robust sensitivity increases.

Using the proposed truth membership function T makes edge regions produce strong changes in $T(i,j)$, homogeneous regions yield values close to 0.5; textured regions exhibit moderate variations. Consequently, the image is transformed into a structure-aware statistical representation, which is more informative for feature extraction than raw intensity values.

The Zero Watermark Construction Algorithm. The zero watermark construction utilizing the SVD is given below and demonstrated in Fig. 3a.

The algorithm outlines the steps of the Zero Watermark Construction for embedding watermarks into images. It begins by converting the original 256-by-256 image to grayscale, then adding three binary watermarks of different sizes. The image is transformed into a neutrosophic domain, which represents pixels using the three proposed membership components $T(i,j)$, $I(i,j)$ and $F(i,j)$. The truth membership function $T(i,j)$ constitutes the core component of the proposed framework; the matrix uses a sigmoid function as a base with specified parameters. The T component is divided into 64 by 64 blocks of size 4 by 4. Singular Value Decomposition is applied to each block, producing three matrices per block. Three cases are tested to create feature matrices of sizes 256-by-256, 128-by-128, or 64-by-64, depending on feature richness (the diagonal matrix $\Sigma_{(i,j)}$). The chosen feature matrix is binarized, and an XOR operation is performed between this matrix and the binary watermark to produce a secret share M. This process ensures robust watermark embedding by combining image features with multiple watermark sizes.

The Zero Watermark Construction Algorithm

Start

Step 1. Enter the original image of size 256×256 and transform it into a gray-level form.

Step 2. Enter the three binary watermarks of size 256×256, 128×128, 64×64.

Step 3. Convert the original image to the neutrosophic domain using the membership functions introduced in 3.1 to obtain the matrix of the neutrosophic component T.

$$T(i,j) = \frac{1}{1 + e^{-k\frac{I(i,j)-\mu_L}{\sigma_L+\epsilon}}}$$

Epsilon = $1e-6$,, Sigmoid Gain (k) =5

Step 4. Select the $T-component$ of the original image and divide it into 64×64 blocks, each of size 4×4.

Step 5. Apply the Singular Value Decomposition method (SVD) on each block in Step 4, and get 3 matrices for each block $U_{(i,j)} \cdot \Sigma_{(i,j)} \cdot V^T{}_{(i,j)}$

Step 6. Three cases are tested for all blocks to create a new matrix to be the matrix of features:

Case 1. (Richer features): Choose the matrices $\Sigma_{(i,j)}$ and construct a new matrix of size 256×256 to be the feature matrix C.

Case 2. (Less rich, partially compact**):** Choose the main diagonal of each $\Sigma_{(i,j)}$ and construct a new matrix of size 128×128 to be the feature matrix C.

Case3. (Most compact features**):** Choose the maximum number of each $\Sigma_{(i,j)}$ and construct a new matrix of size 64×64 to be the feature matrix C.

Step 7. Binarize the matrix C to obtain the feature matrix K where $1 \leq i \leq n$
where: case1: n = 256 case2: n = 128 case3: n = 64**.**

Step 8. Perform an XOR operation between the binary features of the original image K and the binary watermark W to get M (secret share).

End

In the authentication phase, the original image is not required. Instead, the verification process is performed using the test (suspected) image and the stored secret share generated during the zero-watermark construction stage.

The Watermark Recovery Algorithm. The watermark recovery utilizing the SVD is given below and demonstrated in Fig. 3b.

The algorithm outlines the steps of a watermark recovery for a 256-by-256 suspected image. It starts by converting the image to gray-level, then uses three stored zero watermarks. The image is transformed into a neutrosophic domain matrix using a specific formula involving parameters epsilon and sigmoid gain. The T-component of the image matrix is divided into 64-by-64 blocks of size 4-by-4. Singular Value Decomposition is applied to each block, producing three matrices. Three cases are tested to create a feature matrix C of varying sizes: 256-by-256 for richer features, 128-by-128 for less rich features, and 64-by-64 for the most compact features. The matrix C is binarized to form matrix K, with size depending on the case. Finally, an XOR operation between K and secret shares M reconstructs the zero-watermark. These steps are important as it clearly presents the sequential process and decision points in recovering a watermark from an image.

The Watermark Recovery Algorithm

Start

Step 1. Enter the suspected image I' of size 256×256 transform it into a gray-level form.

Step 2. Enter the three stored zero watermarks M.

Step 3. Convert the original image to the neutrosophic domain using the membership functions introduced in 3.1 to obtain the matrix of the neutrosophic component T.

$$T(i,j) = \frac{1}{1 + e^{-k\frac{I(i,j)-\mu_L}{\sigma_L+\epsilon}}}$$

Epsilon = $1e-6$, Sigmoid Gain (k) =5

Step 4. Select the $T-component$ of the original image and divide it into 64×64 blocks, each of size 4×4.

Step 5. Apply the Singular Value Decomposition method (SVD) on each block in Step 4 get 3 matrices $U_{(i,j)} \cdot \Sigma_{(i,j)} \cdot V^T{}_{(i,j)}$

Step 6. Three cases are tested for all blocks to create a new matrix to be the matrix of features:

Case 1. (Richer features): Choose the matrices $\Sigma_{(i,j)}$ and construct a new matrix of size 256×256 to be the feature matrix C.

Case 2. (Less rich, partially compact): Choose the main diagonal of each $\Sigma_{(i,j)}$ and construct a new matrix of size 128×128 to be the feature matrix C.

Case3. (Most compact features): Choose the maximum number of each $\Sigma_{(i,j)}$ and construct a new matrix of size 64×64 to be the feature matrix C.

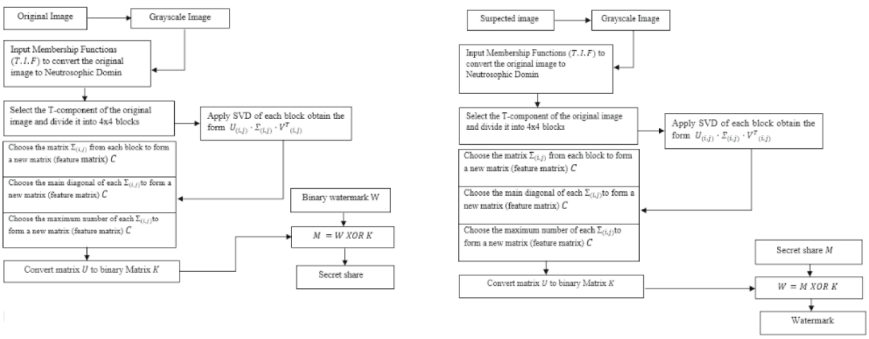
Step 7. Binarize the matrix C to obtain the feature matrix K where $1 \le i \le n$

where: case1: n = 256 case2: n = 128 case3: n = 64**.**

Step 8. Apply the XOR operation between the binary features K and the secret shares M to construct the zero-watermark.

End

The extracted watermark is compared with the original watermark stored at the ownership authority. A high similarity indicates authenticity, while deviations indicate possible tampering.



(a) (b)

Fig. 3. (a) The diagram of the zero-watermark construction and **(b)** The diagram of the authentication procedure

Evaluation Metrics

a-Watermark similarity. The performance of the proposed scheme is evaluated using Normalized Correlation (NC).
b-For recovery accuracy. BER measures the percentage of incorrectly recovered watermark bits.

Attacks Simulation. To evaluate robustness, the original images were subjected to common image processing attacks, and the NC and BER are reported after each attack. Common attacks include: Noise attacks (Gaussian noise, Salt & pepper noise, Speckle noise, Poisson noise), Filtering attacks (Median filter, Average filter, Motion filter, Gaussian lowpass filter), and Image-Processing attacks (JPEG Compression, Histogram Equalization).

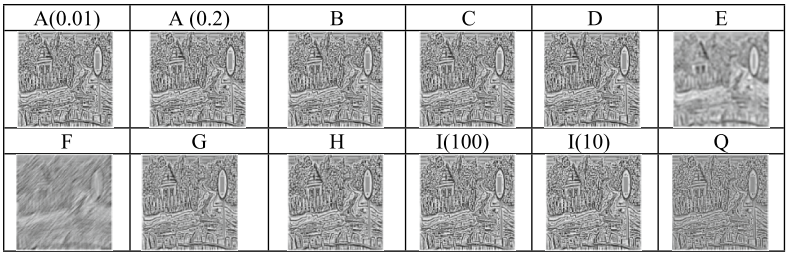


Fig. 4. The Village Road image after the attacks

The Village Road image after the attacks : Attacked Village Road image compares the detailed structures of samples labeled A through Q, with some labels indicating differ-ent conditions or concentrations. Depending on the behavior of each attack, most im-ages sometimes show a consistent pattern of layered and fibrous textures, suggesting similar structural features across samples A(0.01), A(0.2), B, C, D, G, H, I(100), I(10), and Q. And different patterns at other times, sample E and F differ noticeably, with E showing a less defined structure and F appearing more blurred or less organized. This comparison highlights how different attacks or processing operations affect image structures and extracted features, which is essential for assessing the robustness and reliability of the proposed method under various experimental conditions.

4 The Results

This section presents the experimental results obtained from the proposed zero-watermarking method using the improved neutrosophic domain. The performance of the algorithms is evaluated on several paradigm test images and various image processing attacks.

For the three cases, the performance of the watermark recovery is measured using the Normalized Correlation (NC) and BER between the original and recovered watermark (Table 1).

Table 1. The NC and BER Values with no Attacks for the three cases

Images	Baboon	Peppers	Girl	Village Road
NC	1	1	1	1
BER	0	0	0	0

4.1 Noise Attacks

Table 2 presents three cases, each used to constrain a feature matrix for different attack types: Salt and pepper noise, Gaussian noise, Poisson noise, and Speckle noise. The matrices correspond to four images: Baboon, Peppers, Girl, and Village Road. Each image has two columns labeled NC and BER, representing numerical values for each attack and image. The first case shows values mostly close to 1 for NC and lower values for BER across all attacks and images, indicating strong constraint performance. The second case has lower NC values and higher BER values, especially for Gaussian noise, suggesting less effective constraints. The third case shows intermediate values between the first two images. The table highlights how each image performs differently depending on the noise type and image, generally providing the best results in maintaining feature integrity under noise attacks. This Table helps understand which case is most effective for resisting specific noise types in various image settings.

Table 2. NC and BER values after applying a noise attack to the images

Case 1: The diagonal matrices $\Sigma_{(i,j)}$ were selected to construct the feature matrix								
Attacks	**Baboon**		**Peppers**		**Girl**		**Village Road**	
	NC	**BER**	**NC**	**BER**	**NC**	**BER**	**NC**	**BER**
Salt and pepper Noise (0.01)	1	0	1	0	1	0	1	0
Salt and pepper Noise (0.2)	0.999	4.57764e-05	0.999	3.05176e-05	0.999	1.52588e-05	0.999	1.52578e-05
Gaussian Noise	0.999	9.15527e-05	1	0	0.999	4.57764e-05	0.999	4.577
Poisson noise	1	0	1	0	1	0	1	0
Speckle noise	1	0	1	0	1	0	1	0
Case 2: the main diagonal of the matrices $\Sigma_{(i,j)}$ were selected to construct the feature matrix								
Attacks	**Baboon**		**Peppers**		**Girl**		**Village Road**	
	NC	**BER**	**NC**	**BER**	**NC**	**BER**	**NC**	**BER**
Salt and pepper Noise (0.01)	0.970	0.0306	0.968	0.0326	0.969	0.0322	0.972	0.0316
Salt and pepper Noise (0.2)	0.946	0.2899	0.943	0.3068	0.939	0.3050	0.942	0.2945
Gaussian Noise	0.944	0.0635	0.917	0.0931	0.916	0.095	0.912	0.1058
Poisson noise	1	0	1	0	1	0	0.992	0.0067
Speckle noise	0.942	0.0604	0.922	0.0927	0.924	0.0858	0.916	0.0901
Case 3: the maximum singular value of the matrices $\Sigma_{(i,j)}$ (i.e., the element in the location (1, 1)) were selected to construct the feature matrix								
Attacks	**Baboon**		**Peppers**		**Girl**		**Village Road**	
	NC	**BER**	**NC**	**BER**	**NC**	**BER**	**NC**	**BER**
Salt and pepper Noise (0.01)	0.983	0.0178	0.988	0.0151	0.986	0.0139	0.981	0.0244
Salt and pepper Noise (0.2)	0.832	0.1826	0.843	0.1372	0.865	0.1535	0.838	0.1752
Gaussian Noise	0.993	0.0009	0.994	0.00091	0.993	0.0085	0.981	0.0183
Poisson noise	1	0	1	0	1	0	0.991	0.0092
Speckle noise	0.986	0.0202	0.990	0.0124	0.986	0.0146	0.971	0.0314

4.2 Filter Attacks

Table 3 below presents three different cases for selecting features to construct a feature matrix, evaluated across the four above. For each image, two metrics are shown: NC and BER, under four attack types: Gaussian low-pass filter, Motion filter, Average filter, and MED filter. Case 1 shows perfect scores with NC equal to 1 and BER equal to 0 for all attacks and images, indicating ideal performance when diagonal matrices are used. Case 2 presents lower NC values around 0.67 to 0.74 and BER values between 0.28 and 0.35, showing moderate performance when only the main diagonal of the matrices is used. Case 3 shows improved NC values ranging from about 0.61 to 0.88 and lower BER values from approximately 0.13 to 0.42, indicating better results when the maximum singular value of the matrices is selected. Overall, the table highlights how different matrix feature selection methods affect the accuracy (NC) and bit error rate (BER) of image processing

under various filter attacks, with Case 1 performing best, Case 3 showing good results, and Case 2 performing moderately.

Table 3. NC and BER values after applying a filter attack to the images

Case 1: The diagonal matrices $\Sigma_{(i,j)}$ were selected to construct the feature matrix								
Attacks	**Baboon**		**Peppers**		**Girl**		**Village Road**	
	NC	**BER**	**NC**	**BER**	**NC**	**BER**	**NC**	**BER**
Gaussianlowpassfilte	1	0	1	0	1	0	1	0
Motion filter	1	0	1	0	1	0	1	0
Average filter	1	0	1	0	1	0	1	0
MED filter	1	0	1	0	1	0	1	0
Case 2: the main diagonal of the matrices $\Sigma_{(i,j)}$ were selected to construct the feature matrix								
Attacks	**Baboon**		**Peppers**		**Girl**		**Village Road**	
	NC	**BER**	**NC**	**BER**	**NC**	**BER**	**NC**	**BER**
Gaussianlowpassfilte	0.703	0.3199	0.735	0.2833	0.730	0.2904	0.726	0.2944
Motion filter	0.678	0.3480	0.687	0.3240	0.687	0.3372	0.692	0.3304
Average filter	0.703	0.3199	0.735	0.2833	0.730	0.2904	0.726	0.2944
MED filter	0.695	0.3281	0.731	0.2875	0.718	0.3026	0.718	0.3018
Case 3: the maximum singular value of the matrices $\Sigma_{(i,j)}$ (i.e., the element in the location (1, 1)) were selected to construct the feature matrix								
Attacks	**Baboon**		**Peppers**		**Girl**		**Village Road**	
	NC	**BER**	**NC**	**BER**	**NC**	**BER**	**NC**	**BER**
Gaussianlowpassfilte	0.840	0.1745	0.871	0.1411	0.879	0.1333	0.855	0.1599
Motion filter	0.646	0.3828	0.645	0.3825	0.611	0.4167	0.629	0.3999
Average filter	0.840	0.1735	0.871	0.1411	0.879	0.1333	0.855	0.1599
MED filter	0.831	0.1840	0.869	0.1428	0.874	0.1389	0.848	0.1674

4.3 Image-Processing Attacks

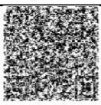
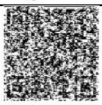
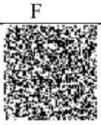
Table 4 presents three cases for constructing a feature matrix—using diagonal matrices, main diagonal elements, and maximum singular values—across four image sets named Baboon, Peppers, Girl, and Village Road. For each case, it shows two metrics: NC (normalized correlation) and BER (bit error rate), under three attack conditions: JPEG compression at quality 100, JPEG compression at quality 90, and histogram equalization. Higher NC values close to 1 and lower BER values close to 0 indicate better per-formance. The first case, using diagonal matrices, consistently achieves near-perfect NC values around 0.999 and very low BER values near zero for all images and attacks, showing the best robustness. The second case, using only the main diagonal, shows lower NC values and higher BER, indicating weaker performance. The third case, using maximum singular values, performs better than the second but not as well as the first, with NC values mostly above 0.9 and moderate BER values. This table highlights that selecting the full diagonal matrices for feature construction provides the most reliable results against these image attacks.

The following Table 5 shows the recovered watermark images for the three cases, Village Road See Table 4:

Table 4. NC and BER values after applying an image-processing attack to the images

Case 1: The diagonal matrices $\Sigma_{(i,j)}$ were selected to construct the feature matrix								
Attacks	**Baboon**		**Peppers**		**Girl**		**Village Road**	
	NC	**BER**	**NC**	**BER**	**NC**	**BER**	**NC**	**BER**
JPEG Compression Quality (100)	0.999	0.00021	0.999	6.10353e-05	0.999	0.00021	0.999	0.00051
JPEG Compression Quality (90)	0.999	0.00071	0.998	0.00123	0.999	0.00115	0.998	0.00195
Histogram Equalization	1	0	1	0	1	0	1	0
Case 2: the main diagonal of the matrices $\Sigma_{(i,j)}$ were selected to construct the feature matrix								
Attacks	**Baboon**		**Peppers**		**Girl**		**Village Road**	
	NC	**BER**	**NC**	**BER**	**NC**	**BER**	**NC**	**BER**
JPEG Compression Quality (100)	0.986	0.0148	0.979	0.0223	0.977	0.0250	0.973	0.0296
JPEG Compression Quality (90)	0.929	0.2478	0.895	0.2302	0.899	0.2505	0.900	0.2759
Histogram Equalization	0.805	0.2106	0.828	0.1857	0.827	0.1878	0.817	0.1983
Case 3: the maximum singular value of the matrices $\Sigma_{(i,j)}$ (i.e., the element in the location (1, 1)) were selected to construct the feature matrix								
Attacks	**Baboon**		**Peppers**		**Girl**		**Village Road**	
	NC	**BER**	**NC**	**BER**	**NC**	**BER**	**NC**	**BER**
JPEG Compression Quality (100)	0.998	0.0019	0.999	0.0004	0.999	0.0004	0.990	0.0100
JPEG Compression Quality (90)	0.995	0.0053	0.997	0.0490	0.994	0.0058	0.987	0.0144
Histogram Equalization	0.924	0.0837	0.956	0.0485	0.957	0.0471	0.933	0.0734

Table 5. Recovered watermark images for the three cases for the Village Road image

Case 1: The diagonal matrices $\Sigma_{(i,j)}$ were selected to construct the feature matrix						
attack	A(0.01)	A(0.2)	B	C	D	E
Recovered Watermark						
attack	F	G	H	I(100)	I(10)	O
Recovered Watermark						
Case 2: the main diagonal of the matrices $\Sigma_{(i,j)}$ were selected to construct the feature matrix						
attack	A(0.01)	A(0.2)	B	C	D	E
Recovered Watermark						
attack	F	G	H	I(100)	I(10)	O
Recovered Watermark						
Case 3: the maximum singular value of the matrices $\Sigma_{(i,j)}$ (i.e., the element in the location (1, 1) were selected to construct the feature matrix						
attack	A(0.01)	A(0.2)	B	C	D	E
Recovered Watermark						
attack	F	G	H	I(100)	I(10)	O
Recovered Watermark						

Recovered watermark images for the three cases for the Village Road image: Table 5 recovered watermarks after different types of attacks using three cases for con-structing the feature matrix: Case 1 uses diagonal matrices, Case 2 uses the main di-agonal of matrices, and Case 3 uses the maximum singular value at position (1, 1). Each case shows two rows of Recovered QR code Watermark images under various attack types labeled A with values 0.01 and 0.2, B, C, D, E, F, G, H, I with values 100 and 10, and O. The table highlights how the watermark recovery varies depending on the matrix construction case and attack type, illustrating differences in watermark clar-ity and integrity across cases and attacks.

4.4 Comparison

The proposed system is adaptable to the image environment, enabling it to control the balance between robustness and sensitivity based on the chosen image feature extraction methods. While most image zero watermarking methods are designed for either a fragile or robust case, the proposed technique operates as a tamper-sensitive, semi-fragile, or robust system depending on the selected control factor.

Table 6. Compared the proposed zero watermarking scheme with previous methods

Method	Technique	Watermark Type	NC (Typical under Attacks)	BER	Robustness	Image Distortion
Proposed Method	Netrsophic + SVD	Zero-watermark	0.998 1.000	≈ 0	Very High	No
Ref [23]	GLC + PCA	Embedded	0.80 – 0.93	Moderate –High	Moderate	Yes
Ref [18]	DWT-DCT–SVD	Embedded	0.90 – 0.98	Moderate	Moderate–High	Yes
Ref [22]	PCA-based	Zero/Hybrid	0.85 – 0.95	Moderate	Moderate (noise sensitive)	No/Low
Ref [1]	DWT–SVD	Embedded	0.95 – 0.99	Low–Moderate	High (but degrades under noise)	Yes

Table 6 presents four methods, in addition to the proposed technique, based on techniques used, watermarking type, NC target, bit error rate (BER), robustness, and image distortion. Methods include GLC and PCA [22] and using PCA-based [21] with a 256x256 watermark and very low distortion; using DCT and SVD with a 64x64 watermark and low distortion [17], using OWT-SVD [1]. Robustness varies from low to high, with some methods resistant to JPEG compression and noise. The table highlights differences in watermark size, robustness, and image distortion among the methods.

5 Methodology Analysis of the Proposed Algorithms and Experimental Results

This section provides a comprehensive analysis of the proposed hybrid zero watermarking paradigm based on the neutrosophic domain and singular value decomposition (SVD). The role of the proposed membership function $T(i, j)$ used in the steps of feature extraction is analyzed to evaluate the impact of the scheme designed.

5.1 Analysis of Feature Extraction Strategies

Three feature extraction strategies are investigated in the proposed scheme, depending on the richness of the features.

The first case utilizes the whole diagonal matrix features of the SVD, preserving a dominant feature from the structural information of each block, resulting in highly stable watermark recovery. The second case utilizes only diagonal elements to reduce

the feature size, making the features more sensitive to distortions. The third case utilizes only the dominant singular value, capturing the primary energy of each block. This approach significantly reduces structural information, increasing sensitivity to attacks.

5.2 Robustness Analysis Under Attacks

According to the experimental results above, the robustness of the proposed zero watermarking scheme is depending on the case of choosing the features.

Under the noise attacks, Gaussian, salt-and-pepper, speckle, and Poisson noise, in the first case, since NC ≈ 1 and BER ≈ 0, then the scheme achieves at most the perfect performance and consequently indicates strong robustness. While in the second case, notice a degradation, especially under higher noise levels. The third case keeps balanced robustness, although it retreats under strong noise. This attitude guarantees flexibility when using richer features, but the compact features increase the effects of confusion.

Under filtering attacks, Gaussian, median, average, and motion filtering, the first case shows high stability, and this displays that this case was not affected (NC $= 1$). In case two, the NC ≈ 0.68–0.73, which indicates a big decline in robustness. While the third case shows moderate degradation (NC ≈ 0.64–0.87). Filtering attacks smooths the overall image, so the features are changed immediately hardly than richer features.

Under compression and intensity attacks**,** JPEG compression and histogram equalization, in the first case, the NC ≈ 0.998–1 keeps high values, and the second case shows substantial degradation, especially at lower quality levels. While the third case is still sensitive but better than the second case.

These results indicate that the proposed T form effectively normalizes global intensity variations, contributing to robustness against such attacks.

5.3 Role of the Proposed Membership Functions

The behavior of the proposed scheme is related directly to the introduced membership function $T(i, j)$: emphasizes local structural contrast rather than absolute intensity, reduces sensitivity to brightness, contrast (for example) distortions, and enhances feature stability across different environments.

6 Conclusion

This technique is designed to be able to extract stable and significant features that have the ability and capacity to attack resistance. The robustness against common attacks achieved under the recent proposed scheme is NC almost 1 and Ber 0. Furthermore, this technique is more flexible and reliable compared with existing approaches because it integrates strong feature stability, with no deformation, and high sensitivity.

The consolidation between the neutrosophic representation of the image and utilizing the SVD on the blocks shows that the proposed scheme attains high-powered interaction truth modeling and algebraic stability. The obtained model achieves a blind authentication technique and keeps the cover image unchanged; consequently, it is regarded as the most suitable for high-integrity applications. The experimental results represent the

near-perfect recovery of the input watermark under different types of attacks, significantly outperforming reduced features, and stands out the significant impact of feature richness.

Moreover, the systematic analysis of various feature extraction techniques releases a principal trade-off between sensitivity and robustness, which gives a good perception to construct a flexible zero watermarking scheme. More than that, depending on the obtained results It is being explored that the proposed design is considered as an adaptable system, not just an important approach for robust zero watermarking that can be tuned for semi-fragile authentication schemes.

Overall, the method can be characterized as a robust zero-watermarking scheme with tunable sensitivity, making it suitable for both copyright protection and authentication applications.

References

1. Alzahrani, A.: Enhanced invisibility and robustness of digital image watermarking based on DWT-SVD. Appl. Bion. Biomech. **2022**, Article 9607682 (2022)
2. Qu, C., Du, J., Xi, X., Tian, H., Zhang, J.: A hybrid domain-based watermarking for vector maps utilizing a complementary advantage of discrete Fourier transform and singular value decomposition. Comput. Geosci. **183**, 105312 (2024)
3. Smarandache, F.: Neutrosophy: Neutrosophic Probability, Set, and Logic: Analytic Synthesis & Synthetic Analysis. American Research Press, Rehoboth (1998)
4. Guo, Y., Cheng, H.D.: New neutrosophic approach to image segmentation. Pattern Recogn. **42**(5), 587–595 (2009)
5. Cheng, H.D., Guo, Y., Zhang, Y.: A novel image segmentation approach based on neutrosophic set and improved fuzzy C-means algorithm. New Math. Nat. Comput. **7**(1), 155–171 (2011)
6. Guo, Y., Sengür, A.: A novel image edge detection algorithm based on neutrosophic set. Comput. Electr. Eng. **40**(8), 3–25 (2014)
7. Yu, B., Niu, Z., Wang, L.: Mean shift-based clustering of neutrosophic domain for unsupervised constructions detection. Optik **124**(21), 4697–4706 (2013)
8. Salama, A.A., Eisa, M., Fawzy, A.E.: A neutrosophic image retrieval classifier. Int. J. Comput. Appl. **170**(9), 1–6 (2017)
9. Wen, J., Xuan, S., Li, Y., Peng, Q., Gao, Q.: Image segmentation algorithm based on neutrosophic fuzzy clustering with non-local information. IET Image Proc. **14**(3), 576–584 (2020)
10. Xu, G., Wang, S., Yang, T., Jiang, W.: A neutrosophic approach based on TOPSIS method to image segmentation. Int. J. Comput. Commun. Control **13**(6), 1047–1061 (2018)
11. Abduldaim, A.M., Faraj, A.K.: Combining algebraic GSVD and gravitational search algorithm for optimizing secret image watermark sharing technique. Int. J. Math. Comput. Sci. **17**(2), 753–774 (2022)
12. Mohammed, N.S., Abduldaim, A.M.: Algebraic Hessenberg decomposition method optimized by genetic algorithm for zero watermarking technique. Int. J. Math. Comput. Sci. **16**(4), 1497–1514 (2021)
13. Waleed, J., Abduldaim, A.M., Alyas, H.H., Mohammed, A.Q.: An optimized zero-watermarking technique based on SFL algorithm. In: 2nd International Conference on Electrical Communication Computer Power and Control Engineering (ICECCPCE), pp. 171–175 (2019)

14. Yang, G., Lu, X., Lu, Y., Tang, J., Xiong, X.: Robust zero-watermarking method for multiple medical images using wavelet fusion and DTCWT-QR. J. Inform. Secur. Appl. **90**, 103945 (2025)
15. Elhamzi, I.W.: Enhancing medical image security with FPGA-accelerated LED cryptography and LSB watermarking. Traitement du Signal **41**(1), 85–97 (2024)
16. Purnima, R., Rakesh, A., Gautam, N.: Motion-frames based video watermarking scheme for copyright protection using guided filtering in wavelet domain. Traitement du Signal **40**(1), 187–197 (2023)
17. Riyajuddin, R., Reddy, A.P.: Various image processing attacks for image watermarking in the wavelet domain using singular value decomposition and discrete cosine transform. Rev. Comput. Eng. Stud. **8**(2), 51–59 (2021)
18. Pan, Z., Wu, C., Yang, C., Zhao, B.: Double-matrix decomposition image steganography scheme based on wavelet transform with multi-region coverage. Entropy **24**(2), 246 (2022)
19. Maity, S.: Image watermarking on degraded compressed sensing measurements. J. Mech. Continua Math. Sci. **18**(4), 10–22 (2023)
20. Yang, M., Li, J., Bhatti, U.A., Shao, C., Chen, Y.: Robust watermarking algorithm for medical images based on non-subsampled shearlet transform and Schur decomposition. Comput. Mater. Continua **75**(3), 5539–5554 (2023)
21. Kahdim, S.A., Abduldaim, A.M.: Principal component analysis for zero watermarking technique. Int. J. Math. Comput. Sci. **18**(1), 85–97 (2023)
22. Dewan, S.G., Kalra, M.: GLCM and PCA algorithm based watermarking scheme. In: AIP Conference Proceedings, vol. 2916 (2023)
23. Su, Q., Sun, Y., Xia, Y., Wang, Z.: A robust color image watermarking scheme in the fusion domain based on LU factorization. Opt. Laser Technol. **174**, 110567 (2024)
24. Wang, X., Du, Q., Du, L., Zhang, H., Hu, J.: Robust zero-watermarking algorithm via multi-scale feature analysis for medical images. J. Inform. Secur. Appl. **89**, 103937 (2025)
25. Smarandache, F.: A Unifying Field in Logics: Neutrosophy, Neutrosophic Set. American Research Press, Neutrosophic Probability and Statistics (2001)
26. Azad, R., Sengur, A.: A novel image segmentation algorithm based on neutrosophic similarity clustering. Appl. Soft Comput. **25**, 391–398 (2014)
27. von Seggern, D.H.: CRC standard curves and surfaces with mathematica, 2nd edn. CRC Press, Boca Raton (2007)
28. Eckart, C., Young, G.: The approximation of one matrix by another of lower rank. Psychometrika **1**(3), 211–218 (1936)