University of Baghdad
College of Engineering
JE
JOURNAL OF ENGINEERING

Journal of Engineering

journal homepage: www.jcoeng.edu.iq

Volume 32 Number 6 June 2026

Robust Zero-Watermarking Scheme for Medical Images Using DT-CWT and Blind Geometric Correction

Ali Nasif Jasim [1], **Sadiq H. Abdulhussain** [1,*], **Abir Hussain** [2]

[1]Department of Computer Engineering, College of Engineering, University of Baghdad, Baghdad, Iraq
[2]Department of Electrical Engineering, University of Sharjah, Sharjah 27272, United Arab Emirates

ABSTRACT

Protecting medical images in medical applications is considered a delicate task and needs to be carefully managed. Generally, the demand is to protect the data of the patient without changing the content of the actual diagnostic data. Zero-watermarking (ZWM) technique provides an elegant solution as it logically links copyright information to essential image properties instead of hiding it in the image pixels themselves. However, there is a trade-off in performance; this is because the existing methods fail to handle image rotation attacks. For example, a small tilt of the image can render the watermark ineffective due to a drop in the feature extraction process. In this paper, the proposed method tackles the aforementioned challenge using Dual-Tree Complex Wavelet Transform (DT-CWT) to generate stable, shift-invariant features from the low-frequency components. Then, the extracted features are processed with Improved Differential Entropy (IDE) to resist common attacks. In addition, the most important part is the blind geometric correction system, where it automatically detects and corrects rotation or reflection by analyzing statistical moments and image distortion, which is performed without the need for the comparison of original image. Finally, the security is enhanced using Arnold scrambling and logistic mapping before mapping the watermark to the extracted features. The developed method is resilient to noise, filtering, JPEG compression, and crucially, geometric attacks. The results show that the Normalized Correlation (NC) scores above 0.99 under different attacks including heavy rotation, solving a long-standing vulnerability in ZWM research. For medical image protection, this developed method is considered reliable, secure, and practical for telemedicine applications.

Keywords: Zero-watermarking, Arnold scrambling, Feature fusion, Blind geometric correction.

1. INTRODUCTION

The rapid growth of online image sharing, cloud storage, and social platforms increases the demand for protecting digital media ownership and integrity, which is a critical requirement

*Corresponding author
Peer review under the responsibility of University of Baghdad.
https://doi.org/10.31026/j.eng.2026.06.12

Article received: 26/02/2026
Article revised: 12/05/2026
Article accepted: 13/05/2026
Article published: 01/06/2026

for both commercial and scientific applications. Digital watermarking is widely used for copyright protection, authentication, and traceability. These actions are performed by linking ownership information with multimedia content so that the owner is able to establish authenticity or resolve disputes **(Sharma et al., 2024)**. Classical watermarking, however, embeds data into the host signal, and this leads to some level of distortion (even if it is imperceptible). Sometimes, this distortion is considered unacceptable, particularly in scenarios where the original content must remain untouched, such as medical imaging, forensics, and legal evidence.

The aforementioned limitations can be bypassed by zero-watermarking (ZWM), which is also called oblivious watermarking **(Meenakshi et al., 2019).** ZWM was developed as a lossless alternative to classical watermarking. In classical watermarking, the watermark bits are embedded into the host image. However, in ZWM, robust features are extracted from the host original image and then bind these features with watermark information such as logo, ID, or hash. This will generate a ZWM key, or ownership key, that is stored externally in database, trusted authority, or blockchain. In this case, the original image is kept unchanged while it is still able to perform copyright verification and ownership authentication **(Liu et al., 2018; Khan et al., 2019)**. Notably, the effectiveness of zero-watermarking depends primarily on the stability and discriminative power of the extracted features. These features should remain consistent under common attacks (compression, filtering, noise, scaling, rotation) and remain sufficiently distinct to avoid confusion between different images or owners.

ZWM is attractive in different applications such as medical applications. This is because diagnostic images demand strict integrity requirements, and any pixel modification may be deemed risky or unacceptable. For example, fundus and tele-ophthalmology imaging contain fine structures that are particularly sensitive to changes under low-resolution acquisition, image compression or poor illumination conditions. This has led to the development of watermarking approaches that avoid embedding as well as preserve diagnostic quality and have the capability for supporting ownership verification **(Singh and Dutta, 2020; Moad et al., 2022)**. Consequently, many modern ZWM systems emphasize robust feature extraction (regularly in transform domains such as DWT/DCT/DTCWT) and secure binding (often encryption, scrambling, chaotic maps) to enhance robustness against both signal-processing and geometric distortions **(Wu et al., 2023; Lebcir et al., 2024)**.

The protection of medical images using ZWM is considered a key research area. This trend becomes increasingly demanded to protect copyright, data integrity, as well as to ensure trust of information in healthcare systems. When compared to traditional embedded watermarking, ZWM maintains the original image signal untouched. Simultaneously, ZWM enables the verification of ownership and the detection of tamper, both of which are considered crucial requirements for medical data. Accordingly, various ZWM methods have been proposed. These methods utilize transform domain features, chaotic encryption, descriptors based on moments, and recently, deep learning representations are used to enhance robustness and security.

A ZWM framework based on Fractional Racah Moments (FrROMs) was proposed by (**El-Khanchouli et al., 2025)**. In this framework, a new family of discrete fractional orthogonal moments was derived using spectral decomposition of Racah polynomials. The design tackled the issue of instability that occurs at high-order moments. In the reconstruction process, the framework avoids the data embedding in the image and obtained a low mean squared error (MSE $\approx 10^{-22}$). This framework is robust against compression, noise, cropping,

and rotation attacks. It also steadily outperforms moments based on discrete Racah polynomials in terms of NC and BER, especially for fractional orders γ in the range (0, 0.1].
(Wu et al., 2023) developed a zero-watermarking (ZWM) scheme for color medical images utilizing the Dual-Tree Complex Wavelet Transform (DT-CWT), which will hereafter be referred to as ZWDC method. This scheme combines DT-CWT with an Improved Differential Entropy (IDE) model. Stable sub-blocks were selected based on variance. In addition, to enhance distortion resistance, IDE combined singular values and their mean. Moreover, Arnold scrambling and logistic mapping were used to improve security. This scheme achieved an average NC of 0.9928.
A secure ZWM method was proposed by **(Yuan et al., 2024)** for encrypted medical images. The method combines a multi-level Discrete Wavelet Transform (DWT), Daisy descriptors, DCT, and logistic chaotic mapping. First, the input image is encrypted using DWT-DCT and chaotic sequences. Then, Daisy descriptors are extracted from the LL3 sub-band to provide stable, rotation-invariant features. Finally, the extracted features are transformed with DCT, hashed, and re-encrypted using logistic mapping. This method maintained NC values above 0.8 even with rotation attack up to 70°. In addition, this method shows low computational complexity, where the embedding and extraction process is under 0.5 seconds. Therefore, this method is considered suitable for telemedicine applications.
More recently, in zero-watermarking, the researchers have moved from handcrafted feature engineering toward deep learning–based feature extraction. This is due to the aim of learning features that are simultaneously robust and discriminative across diverse attacks. Deep-learning-based algorithms have been used to generate relatively stable hash-like representations or robust feature vectors for medical image protection. This is performed to improve the algorithm performance under geometric attacks when compared with handcrafted features **(Gong et al., 2022; Hosny et al., 2024)**. Other studies integrate CNN-based feature learning with classical transforms, such as Discrete Cosine Transform (DCT), to benefit from both learned semantic stability and well-known frequency-domain robustness **(Dong et al., 2023)**. Practical approaches are also being used to develop effective spatial-domain constructs to minimize complexity while maintaining sufficient robustness for real-world applications, as a result of complexity and time consumption **(Ali and Kumar, 2024)**. But despite reducing the computational overhead, the spatial domain methods show vulnerabilities to geometric distortions. Their performance degrades greatly under rotation and complex non-scaling geometric attacks, and this limits their overall reliability when compared to robust frequency domain alternatives.
In conclusion, ZWM is regarded as a crucial path for copyright protection in situations where the original media must be completely unaltered. Particularly in fields like healthcare and telemedicine, the current research trends center on (i) strengthening security of the stored ownership key, (ii) improving discriminability to prevent ownership ambiguity, and (iii) improving robustness against geometric distortions **(Singh and Dutta, 2020; Wu et al., 2023; Gong et al., 2022; Dong et al., 2023; Li et al., 2024; Taj et al., 2024)**.
The aforementioned methods demonstrate the development from handcrafted features (orthogonal moments and wavelet coefficients) towards hybrid transform-domain techniques. Although this research has claimed robust performance of the presented algorithms, they still require further investigation. These methods exhibit poor performance when the image is subjected to geometric distortions. They show limited resistance to translation and rotation in certain diagrams. Furthermore, some methods are characterized by high computational complexity in the feature extraction and encryption phases. While

recent advancements in overlapping block processing have successfully reduced some of these extraction bottlenecks **(Abdulhussain et al., 2022)**, balancing this speed with robustness against geometric distortions remains a challenge. Finally, there is a lack of standardized evaluation protocols across different datasets and attack scenarios.

In this paper, a robust ZWM framework is proposed specifically for medical images. It must be noted that the proposed method is built on the work of **(Wu et al., 2023).** While previous works demonstrated strong performance, they show poor performance when the image is exposed to geometric distortions, showing limited resistance to translation and rotation. Currently a tradeoff exists in ZWM designs where methods that are highly resilient to a comprehensive range of distortions (such as the geometric transformations, noise, filtering and JPEG compression) often require heavy computational resources which makes them impractical for fast telemedicine applications. The proposed method bridges this gap between geometric resilience and computational efficiency. This balance is achieved by combining a Blind Geometric Correction module that is based on statistical image moments with a 1st level Dual-Tree Complex Wavelet Transform (DT-CWT) that secures shift invariance without sacrificing spatial resolution. In order to address the gaps of existing methodologies under geometric distortions, this framework introduces these mechanisms along with several other enhancements to the standard ZWM pipeline, supported by experimental results that maintain Normalized Correlation (NC) scores above 0.99 under various attacks.

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

- **Blind Geometric Correction via Image Moments:** An automated module is implemented that can calculate second order and third order statistical central moments to detect and correct image rotation and flipping. This normalization process is performed blindly which means the original host image is not required for comparison during verification. Unlike standard ZWM techniques that fail and lose synchronization under rotational attacks, this method is highly effective because it independently realigns the image to a canonical orientation before feature extraction, ensuring near perfect retrieval even under severe geometric distortion.
- **Redundancy & Majority Voting**: A robust error correction approach is introduced to minimize the Bit Error Rate (BER) during the extraction phase. It works by repeating every bit of the encrypted watermark multiple times (using a redundancy factor) across different feature blocks. While this redundancy expands the required feature vector size and adds marginal computational complexity during the matching and voting phase, the trade-off is highly favorable. The majority voting procedure guarantees precise retrieval even when significant regions of the host image are heavily distorted or cropped.
- **One Level of Decomposition DT-CWT**: In order to achieve shift invariance without sacrificing the spatial resolution of the feature grid, a first level decomposition of the DT-CWT is used to extract the low pass approximation sub band. This can act as an optimization over deep, multi level decompositions that balance computational efficiency with structural stability.
- **Middle-upper Variance block selection**: To construct a highly stable feature vector, the algorithm divides the sub band into non-overlapping 8x8 blocks. The variance of every block is calculated, and the blocks are numerically sorted. The algorithm dynamically determines the selection threshold by isolating the middle to upper range of values of this sorted list. This adaptively filters out unstable flat regions (low variance) and noisy edges (extreme high variance) which significantly enhances the discriminative power of the extracted features.

2. PRELIMINARIES

In this section, the basic concepts and mathematical notations required to understand the proposed ZWM method are presented. The mathematical representation of digital images, and feature extraction principles used for watermark registration and verification are explained. In addition, this section outlines the security mechanisms applied in watermarking systems. Moreover, its common attacks are delivered. Finally, the performance evaluation metrics utilized in this paper are introduced.

2.1 Feature Extraction

Feature extraction is the method used to represent the image as well as to reduce computational complexity. This process utilizes a compact set of descriptors instead of using raw pixels to capture the image structural scene, which creates a compact set for more stable and distinctive watermarking purposes **(Sharma et al., 2024)**. In this paper, the extraction process is constructed using DT-CWT and IDE **(Wu et al., 2023; Ying et al., 2019)**.

The DT-CWT decomposes the image into multi-scale sub-bands. Traditional wavelet transforms exhibit an issue of significant change in transform coefficients, as well as an absence of directional information when a slight shift occurs in the input image.

On the other hand, DT-CWT tackles both limitations by providing near shift invariance and enhanced directional information. Consequently, the DT-CWT provides robust low frequency coefficients that serve as a reliable foundation for generating structural features that are resilient to minor spatial shifts **(Wu et al., 2023)**.

However, wavelet transform coefficients alone are not highly robust against strong signal attacks. To enhance this robustness, a hybrid approach combining Singular Value Decomposition (SVD) and an IDE transformation is used. In the proposed method, the extracted coefficients from the selected sub-blocks are first processed by using SVD to capture their dominant structural properties Eq. (4) and then subjected to a logarithmic entropy transformation Eq. (5).

This subsequent processing is designed to stabilize the final feature distribution and reduce sensitivity to sudden intensity changes caused by noise, filtering, or JPEG compression. Thus, the resulting hybrid features remain highly discriminative for distinguishing between images, while demonstrating improved resilience to geometric attacks and common image degradations.

2.2 Cryptography and Security

In ZWM systems, security represents the protection of the watermark information and its associated registration data from threats. Because the host image is not altered, security mechanisms can be applied directly to the watermark before it gets bound with the extracted features **(Sharma et al., 2024)**. This can provide a distinct performance advantage highly correlated with ZWM architecture because the encryption targets only the compact binary watermark rather than the high resolution medical image and the computational overhead remain low, and this introduces no degradation to the host image's quality or the extraction speed of the algorithm.

In this paper, when compared to traditional cryptographic standards like AES or RSA which are computationally heavy and can disrupt dimensional arrays, chaos-based techniques are used in order to enhance the watermark confidentiality. Specifically, a 1D Logistic Map is used to generate a pseudorandom sequence Eq. (8). This uses an initial condition x_0 as a

secret seed and a control parameter r in order to ensure a fully chaotic regime. This continuous sequence is thresholded into a binary mask with a string length exactly equal to the total size of the watermark vector. The core encryption mechanism is then executed via a highly efficient bitwise XOR ($\oplus$) operation between the watermark and the generated chaotic mask Eq. (10). It is noteworthy that the logistic map produces sequences that are difficult to predict without prior knowledge of the secret key **(Panday et al., 2024; Çelik and Doğan, 2023)**. In addition, to spatially permute the watermark pattern, the Arnold transform is utilized. The Arnold Transform is a periodic, geometric mapping matrix that scrambles the 2D pixel coordinates Eq. (6). In this scheme, the spatial scrambling is applied for a fixed parameter of k iterations **(Wang et al., 2024)**. And because the transform is periodic and deterministic, it is perfectly reversed during the verification stage by applying the inverse mapping matrix for the exact same number of k iterations Eq. (7).
The combined utilization of chaotic encryption and spatial scrambling provides lightweight and effective security, which is considered suitable for large-scale and high-resolution image verification scenarios **(Panday et al., 2024; Çelik and Doğan, 2023; Wang et al., 2024)**.
Finally, in order to maintain system integrity, strict key management is used. The secret parameters that are necessary for reconstruction (specifically the initial condition x_0, the control parameter r, the Arnold iteration count k, the watermark dimensions and the selected host feature indices) are securely stored in an external trusted database alongside the generated Master Zero Watermark (ZW) key.

3. METHODOLOGY

In this section, the methodology and the steps of the proposed method are thoroughly described. In practice, the methodology is divided into two stages, the registration stage, and the verification stage. The two stages are explored to examine and clarify the fundamental concepts underlying the practical implementation in their most basic form, as well as to identify the prerequisites required prior to initiating the proposed method.

3.1 Major Techniques

This section describes the principal computational techniques that are used in the proposed ZWM method.

3.1.1 Blind Geometric Correction via Image Moments

To address the sensitivity of ZWM to rotation and flipping without requiring the original cover image, the proposed method implements a blind geometric correction module based on statistical image moments. This process normalizes the image orientation before feature extraction. The raw two dimensional image moments M_{ij} are defined as follows **(Gonzalez and Woods, 2018)**:

$$M_{ij} = \sum_x \sum_y x^i y^j I(x, y) \quad (1)$$

Where x and y represent the spatial pixel coordinates, and I(x,y) represent the grayscale intensity value of the pixel at those coordinates. Using the central moments μ_{ij}, the orientation angle θ is derived to determine the principal axis of the image **(Gonzalez and Woods, 2018)**:

$$\theta = \frac{1}{2} arctan\left(\frac{2\mu_{11}}{\mu_{20} - \mu_{02}}\right) \quad (2)$$

Where $\mu_{11}, \mu_{20}, and\ \mu_{02}$ represent the second order central moments of the image. In order to check if the image is upside down, a third order moment (μ_{30}) is calculated. These values are calculated to define the mathematical limits by summing across the entire image grid, from its width ($x = 0\ to\ M - 1$) to its height ($y = 0\ to\ N - 1$). If the resulting value is negative, then the image is flipped 180°. Lastly, an affine transformation which is simply a standard 2D rotation around the image's center, turns the image back to its normal, upright position. We use a smoothing method called cubic interpolation to ensure the feature grid stays perfectly aligned no matter how the image was originally rotated.

3.1.2 Dual-Tree Complex Wavelet Transform (DT-CWT)

In the proposed ZWM method, and for feature extraction, DT-CWT is employed. The standard Discrete Wavelet Transform (DWT) is a powerful tool for multi-resolution analysis; however, it suffers from two major limitations. These limitations affect the DWT effectiveness of ZWM: shift variance and lack of directional selectivity **(Wu et al., 2023)**. This is because small spatial changes in the input image causes significant variations in the wavelet coefficients. As a result, this sensitivity breaks the synchronization required for ZWM.

The aforementioned limitations are tackled when DT-CWT is used. This is because DT-CWT utilizes two parallel DWT trees. The DWT tree is one for the real part and other for the imaginary part. This structure of the dual tree provides near shift-invariance and directional selectivity in six distinct orientations, which are ±15°, ±45°, and ±75°. This makes it more robust to geometric distortions than traditional wavelets.

In the proposed ZWM method, we implement DT-CWT to focus on Low-Pass Approximation Sub band derived from the 1st level decomposition.

First, the decomposition level: The input image $I(x, y)$ is decomposed at level $L = 1$. To preserve the spatial resolution of the feature grid, deep multi-level decomposition (e.g., L = 3 or L = 4) is avoided. In the 1st-level of decomposition, the dimension of the image is reduced to half (512×512 to 256×256). This provides a sufficient number of 8×8 blocks to support the high redundancy factor ($R = 4$) required for the error correction mechanism.

Second, the low-pass feature extraction: The high-frequency sub bands contain directional edge information, which are often subject to high-frequency noise attacks such as Gaussian noise, and speckle noise. On the other hand, the low-pass sub band captures the stable as well as structural approximation of the image content.

The transform provides a complex coefficient output, but for robust feature, we extract the magnitude of the low-pass coefficients as described by **(Wu et al., 2023)**, as follows:

$$C_{low} = DT - CWT_{level=1}^{lowpass}(I_{norm}) \quad (3)$$

This low-pass approximation C_{low} will serve as the robust domain from which the stable blocks are selected and processed using Hybrid SVD and IDE. The watermark is anchored to the low-frequency structural components. This is performed to ensure that the generated ZWM remains retrievable even after significant degradation or geometric warping to the image.

Choosing the first level of decomposition ($L = 1$) is a strategic balance between robustness and capacity. While deeper levels (such as $L = 2$ or $L = 3$) can offer more stability, they significantly shrink the image size and leave too few blocks for feature extraction. By staying at $L = 1$, the subband is kept large enough (256×256) to provide the high number of 8×8 blocks that are required for the $R = 4$ redundancy and majority voting system. This ensures the watermark remains retrievable even if the image is heavily warped or degraded.

3.1.3 Adaptive Block Selection and Hybrid SVD-IDE

To construct the feature vector, we employ a hybrid approach combining variance-based selection: SVD, and IDE **(Wu et al., 2023)**. First, the low-pass sub band is divided into non-overlapping 8×8, and to present the selection of unstable flat regions, i.e. low information, or noisy edges, the blocks are sorted by variance. The method selects the best stable blocks from the middle-upper variance range.
Second, for each selected block, SVD is applied to obtain the singular values S. A weighted singular value σ_ω is computed using the first three largest singular values (S_1, S_2, and S_3) to capture dominant structural features as follows **(Wu et al., 2023)**:

$$\sigma_\omega = 0.6S_1 + 0.3S_2 + 0.1S_3 \tag{4}$$

Third, to linearize the distribution and enhance robustness against gain attacks, the weighted singular values are transformed using a logarithmic entropy formula as follows **(Ying et al., 2019; Wu et al., 2023)**:

$$v_{ide} = 0.5log(2\pi e(\sigma_\omega^2) + \mu_s + C) \tag{5}$$

Where e is Euler's number (approximately 2.718), μ_s is the mean of the singular values and C is a stabilizing constant, which is set to 1.0.

3.1.4 Arnold Transform for Image Scrambling and Unscrambling

To scramble the spatial correlation of the watermark and render it to become visually unrecognizable, the Arnold Transform is used. This is performed by applying it as a secondary security layer following the chaotic encryption. In this process, the pixel coordinates are geometrically permuted in order to ensure that the stored ZWM reveals no intelligible patterns. The scrambling and subsequent restoration processes are executed as follows:

First, the forward scrambling (registration): The binary watermark image is processed iteratively. In each iteration, the pixel coordinates (x, y) are mapped to new coordinates (x', y') using a specific modulo transformation matrix. This operation gets repeated for a fixed number of iterations ($k = 10$) so that it achieves a fully scrambled state **(Panday et al., 2024; Wang et al., 2024)**.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \ mod N \tag{6}$$

Where N is the representation of the width and height dimensions of the square watermark image.

Second, the inverse unscrambling (verification): In the watermark recovery phase, the original spatial structure is restored by applying the inverse transformation. This step reverses the geometric permutation by using the same iteration count ($k = 10$) but with the inverse mapping matrix **(Panday et al., 2024; Wang et al., 2024)**.

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} mod N \tag{7}$$

Since both transformations are modular and deterministic, they form a perfect reversible pair.

3.1.5 Logistic Map for Chaotic Sequence Generation

In order to ensure the confidentiality of the watermark data, a chaos-based encryption layer is applied prior to spatial scrambling. This process generates a pseudo-random binary mask that is mathematically linked to a secret seed, which prevents unauthorized recovery even if the scrambling pattern is known **(Çelik and Doğan, 2023; Riaz et al., 2024)**. The encryption process is executed in three steps:

First, the sequence generation. A chaotic sequence is initialized by using a secret seed value (x_0) and Logistic Map recurrence relation. The control parameter (r) is set to 3.9999 in order to ensure that the system operates in a fully chaotic regime, producing a non-repeating trajectory **(Çelik and Doğan, 2023; Riaz et al., 2024)**.

$$x_{n+1} = r x_n (1 - x_n) \tag{8}$$

Where x_n is the current state value of the sequence, and x_{n+1} is the next generated value. Second, the binary mask construction. The continuous chaotic sequence gets converted into a binary cryptographic mask (Mc). A thresholding operation is applied where values exceeding the threshold ($\tau = 0.5$) are mapped to 1, and all others to 0 **(Çelik and Doğan, 2023; Riaz et al., 2024)**.

$$M_c(i) = \begin{cases} 1, & if\ x_i > 0.5 \\ 0, & otherwise \end{cases} \tag{9}$$

Where x_i represents the continuous value of the chaotic sequence at index i. Third, the bitwise encryption: The binary watermark image is encrypted by performing a bitwise XOR operation (denoted by the $\oplus$ symbol) with the generated mask. It is noteworthy that this operation effectively randomizes the bit distribution of the watermark while maintaining the computational cost efficiency and fully reversible for the verification stage **(Çelik and Doğan, 2023; Riaz et al., 2024)**.

$$W_{masked} = W \oplus M_c \tag{10}$$

3.2 Registration Stage

The registration stage is the foundational phase of the ZWM process. In this phase, the system extracts a robust feature set from the host medical image using the DT-CWT and IDE. Simultaneously, the watermark is processed via redundancy and chaotic encryption. A ZWM

key is then generated by logically linking these two data streams without altering a single pixel of the original medical image. The registration phase has the following steps:

Step 1: Parameter initialization at the beginning of the process. The algorithm initializes the needed cryptographic and image processing parameters.
- Host & Watermark Paths: These are the locations of the cover and watermark images.
- Block Size ($N \times N$): It's the size of the sub-blocks used for feature extraction.
- Redundancy Factor (R): It represents the factor that can determine how many times each watermark bit is repeated to ensure robustness.
- Arnold Iterations (k): The number of rounds that are used for spatial scrambling.
- Logistic Parameters (x_0, r): The initial seed and control parameter for the chaotic generator.
- IDE Constant (C): The stabilization constant for the entropy calculation.

Step 2: Image Loading and Blind Geometric Correction. The host image is loaded and converted to grayscale to reduce computational complexity. In order to ensure that the features are extracted from a standardized orientation, the image is normalized to its canonical orientation using the statistical moments and affine warping described previously in the Blind Geometric Correction section:

$$I_{norm} = GeometricCorrection(I_{host}) \tag{11}$$

Step 3: DT-CWT Decomposition
The normalized host image I_{norm} is decomposed using the DT-CWT.
- Only one decomposition level is considered to extract the low-low approximation sub band (LL).
- This sub band captures the components in the low-frequency (stable structural information) of the image while filtering out high-frequency noise **(Wu et al., 2023)**.

$$LL_{coeffs} = DT - CWT_{level=1}(I_{norm}) \tag{12}$$

Step 4: Adaptive Block Selection and Feature Generation
To construct the binary feature vector F_{host}, the LL subband is processed according to the following criteria:
- Block Partitioning: The sub band is partitioned into non-overlapping blocks with a size of $N \times N$.
- Variance-Based Selection: In order to avoid unstable flat regions or noisy edges, the variance of every block is calculated. After the blocks are sorted, a subset of "stable" blocks (from the middle-upper variance range) is selected. The indices of these blocks are stored.
- Hybrid SVD-IDE Extraction: For each of the selected blocks, the SVD is applied. The singular values S are weighed and transformed by using the IDE logarithmic formula which is defined in Eq. (5).
- Binarization: To form the final feature vector F_{host} of the host, the resulting entropy values are binarized by using their median value as follows **(Wu et al., 2023)**:

$$F_{host}(i) = \begin{cases} 1, v_{ide}(i) \geq median(v_{ide}) \\ 0, otherwise \end{cases} \tag{13}$$

Step 5: The binary watermark image W is processed to enhance security and robustness:

- Arnold Scrambling: The watermark is spatially scrambled for k iterations to disperse pixel correlations **(Panday et al., 2024; Wang et al., 2024)**.

$$W_{scrambled} = Arnold(W, k) \quad (14)$$

- Redundancy Expansion: To resist local distortions, each bit of the scrambled watermark is repeated R times. This step expands the watermark vector size so that it matches the number of selected host features.

$$W_{expanded} = repeat(W_{scrambled}, R) \quad (15)$$

Step 6: Chaotic Encryption, a pseudo-random binary sequence K_{chaos} is generated using the Logistic Map with the secret keys x_0 and r. In this process, the expanded watermark is encrypted via a bitwise XOR operation **(Çelik and Doğan, 2023; Riaz et al., 2024)**:

$$W_{encrypted} = W_{expanded} \oplus K_{chaos} \quad (16)$$

Step 7: ZWM Construction The final "Zero-Watermark" (or Master Share) is generated by logically combining the extracted host features with the encrypted watermark bits. This step creates the ownership link with no effect to the host image **(Sharma et al., 2024)**:

$$ZW = F_{host} \oplus W_{encrypted} \quad (17)$$

Step 8: Registration Data Storage To enable future verification, the system outputs and stores the following secret parameters. The original image is also not required for verification, only these keys:
- Zero-Watermark Vector (ZW)
- Selected Block Indices: The specific coordinates of the stable blocks used for feature extraction.
- Logistic Parameters (x0,r): For regenerating the decryption key.
- Watermark Dimensions: The shape of the original binary watermark.
- Arnold Iterations (k): For inverse scrambling.

Fig. 1 illustrates the updated process flow of the registration stage.

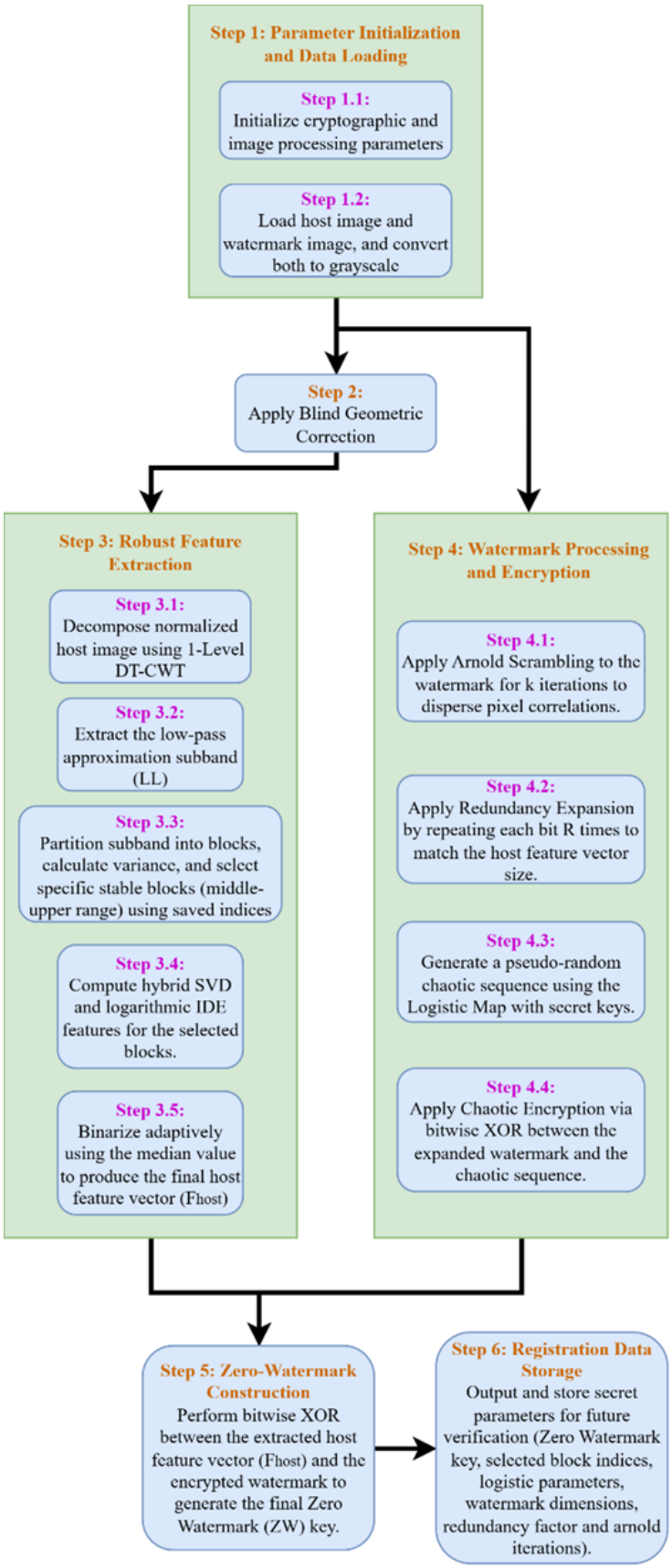

Figure 1. Process flow of the Registration Stage

3.3 Verification Stage

The verification stage is the complementary phase to the registration. Its purpose is to validate ownership and evaluate the watermark robustness when the watermarked image has been subjected to attacks. And unlike traditional methods, this stage doesn't need the original cover image, only the secret keys that are generated during registration.

Step 1: Loading data and pre-verification checks. The verification phase begins by loading the attacked image, which may have undergone filtering, compression, geometric distortion, or other signal processing attacks. It should be noted that the essential registration data stored previously are also loaded by the system, which is shown below in **Table 1**.

Table 1. Registration Data for the Verification Stage.

Data	**Variable / Description**
Zero-Watermark Key Z_w	The Essential key
Selected Block Indices	The coordinates of stable blocks used in the host image.
Logistic Parameters (x_0, r)	To regenerate the decryption key.
Original Watermark Dimensions	To reshape the recovered bitstream.
Arnold Iterations (k)	For inverse scrambling.

Step 2: Geometric Scaling and Blind Correction before feature extraction, the system ensures the attacked image matches the canonical geometry used during registration.
- Scaling Correction: If the attacked image dimensions are different from the original size (due to scaling or cropping or something else), then it gets resized to the standard resolution (512×512) by using linear interpolation.
- Blind Geometric Correction: The image is processed to correct rotation and flipping.

Step 3: Robust Feature Extraction. Once the image geometry is normalized, the features are extracted using the same protocol as the registration stage.

- Decomposition: The image is decomposed by using 1-level DT-CWT to retrieve the low pass approximation subband (LL).
- Feature Generation: The system retrieves the specific 8×8 blocks which are defined by the stored selection block indices. These blocks go through the same SVD and IDE transformation sequence (Eq. 5) that is used in the registration. Afterwards, the values are binarized to produce the extracted feature vector $F_{attacked}$.

Step 4: Watermark Reconstruction (Majority Voting) The extracted features are used to recover the encrypted watermark bits:
- XOR Retrieval: The extracted feature vector is XORed with the stored Zero-Watermark Key (ZW) to retrieve the encrypted watermark stream.

$$W'_{encrypted} = F_{attacked} \oplus ZW \tag{18}$$

- Chaotic Decryption: The pseudo-random chaotic sequence K is regenerated using the stored logistic parameters (x_0, r). The retrieved stream is XORed with this key to remove the chaotic encryption.

$$W'_{expanded} = W'_{encrypted} \oplus K \tag{19}$$

- Majority Voting: Since the watermark was expanded by a redundancy factor R, the system groups the bits and applies a majority vote to determine the final value of each bit.

$$W'_{scrambled}(i) = \begin{cases} 1 & if \ \sum_{i=1}^{R} b_i > R/2 \\ 0 & otherwise \end{cases} \quad (20)$$

where b_i represents the individual recovered bits within the redundancy group of size R.

Step 5: inverse scrambling and the final output. The recovered bitstream gets reshaped into a 2D matrix that matches the original watermark dimensions. Finally, the Inverse Arnold Transform is applied for k iterations in order to reverse the spatial scrambling and restore the original visual structure of the watermark.

$$W_{recovered} = InverseArnold(W'_{scrambled}, k) \quad (21)$$

Step 6: Performance Evaluation. Once the watermark is recovered, multiple metrics are computed to evaluate the fidelity and robustness of the watermarking scheme. **Table 2** shows the metrics that were used and what their formula and description are.

Table 2. Evaluation Metrics that are used in the proposed method.

Metric	Symbol	Formula	Description
Normalized Correlation	**NC**	$NC = \frac{\sum(W \cdot \widehat{W})}{\sqrt{\sum W^2 \sum \widehat{W}^2}}$	Similarity between original and recovered watermark
Bit Error Rate	**BER**	$BER = \frac{B_e}{B}$	Error rate between total number of watermark bits and the number of bits that were extracted with errors
Execution Time	**T_{reg}, T_{ver}**	$T = t_{end} - t_{start}$	Measures algorithmic efficiency. T_{reg} refers to registration duration and T_{ver} to verification duration. Lower time indicates higher computational efficiency.

Fig. 2 shows the process flow of the verification stage.

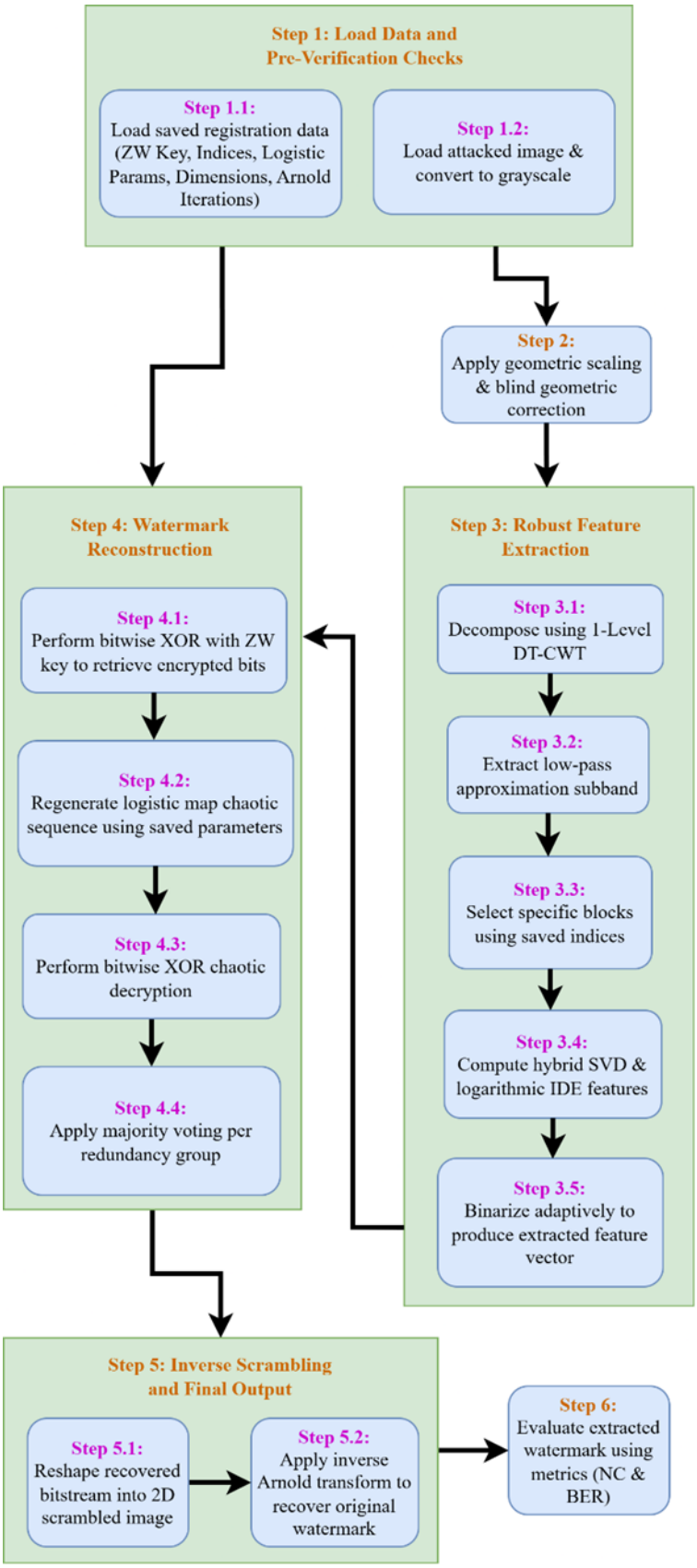

Figure 2. Process Flow of the Verification Stage.

4. RESULTS AND DISCUSSION

Before demonstrating the experimental results, it is important to establish the testing framework that was used to evaluate the proposed zero watermarking method. The robustness of the scheme is measured against various image modifications that aim to degrade or desynchronize the embedded data **(Sharma et al., 2024).** These involve signal level distortions such as image processing operations like filtering and compression **(Sharma and Kumar, 2018)** and removal attacks such as noise injection **(Song et al., 2010).** Additionally, the method is tested against geometric and desynchronization attacks such as rotation, scaling and translation, which disrupt spatial alignment **(Su et al., 2022; Xi et al., 2024).** To assess the proposed method's resilience and efficiency under these conditions, Normalized Correlation (NC) is used in order to measure watermark similarity **(Alomoush et al., 2023),** Bit Error Rate (BER) evaluates the accuracy of recovery **(Basnayaka and Jia, 2023)** and execution time determines the computational cost of the registration and verification phases **(Kalarikkal Pullayikodi et al., 2017).**

The next part in this section presents the experimental results that were obtained from the implementation of the proposed ZWM method. The performance of the system is evaluated in terms of robustness and accuracy of watermark retrieval under various image processing attacks, which include filtering, compression, noise addition, and geometric distortions.

Quantitative measures like NC and BER are used to evaluate the effectiveness of the proposed approach. **Tables 3 to 8** and **Table 10** below show the performance test against the state-of-the-art method of ZWDC that shares a similar transform domain foundation but also lacks some mechanisms such as blind geometric correction module or a redundancy factor that is implemented in this study.

The proposed method will also be tested against the approach by **(Xia et al., 2021)** on **Table 9,** which utilizes polar harmonic transforms and chaotic encryption but exhibits significantly higher bit error rates under complex distortions.

All experiments were conducted on a PC running Windows 11 Pro, equipped with an Intel Core i7-8700 CPU, 32 GB RAM, and an NVIDIA GeForce GTX 1080 GPU. The implementation also utilized a number of programming libraries such as Matplotlib for data visualization and plotting, NumPy for array manipulation and numerical computation, OpenCV for image processing and blind geometric corrections, time libraries that measure execution times, and dtcwt that perform DT-CWT decomposition.

The tests are done using 5 different watermarks, noted as (W1-W5).

The proposed method in this paper outperforms the previous work and shows improvement in almost all listed parameters. **Table 3** shows a performance results table with the previously mentioned study on noise attacks.

Table 3. Performance table comparison with related work on noise attacks using NC metric.

	Attack					
Method	**Gaussian Noise 2%**	**Gaussian Noise 4%**	**Salt & Pepper 2%**	**Salt & Pepper 4%**	**Speckle Noise 2%**	**Speckle Noise %4**
(Wu et al., 2023) (W1)	0.9990	0.9980	0.9990	1.0000	1.0000	1.0000
(Wu et al., 2023) (W2)	1.0000	0.9970	0.9985	0.9985	1.0000	0.9985
(Wu et al., 2023) (W3)	0.9953	0.9988	0.9988	1.0000	1.0000	0.9988
(Wu et al., 2023) (W4)	0.9962	0.9962	1.0000	0.9981	1.0000	1.0000

(Wu et al., 2023) (W5)	0.9980	0.9987	1.0000	0.9993	1.0000	1.0000
Proposed method (W1)	1.0000	1.0000	1.0000	0.9988	1.0000	1.0000
Proposed method (W2)	1.0000	1.0000	1.0000	0.9988	1.0000	1.0000
Proposed method (W3)	1.0000	1.0000	1.0000	0.9989	1.0000	1.0000
Proposed method (W4)	1.0000	1.0000	1.0000	0.9989	1.0000	1.0000
Proposed method (W5)	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000

Table 3 compares the proposed method with ZWDC under various noise attacks. The proposed framework demonstrates a noticeable robustness compared to existing works. When Gaussian noise with an intensity level of 2% and 4% are applied and tested, an NC score of 1.0000 across all five watermarks is achieved. However, while the ZWDC method is still performing well, it showed some inconsistency with scores ranging from 0.9953 to 1.0000.

The same pattern is observed when Salt and Pepper are applied and tested. At 2% density, the proposed method maintained perfect NC scores of 1.0000 for every watermark. Even when the noise was increased to 4%, the NC scores show a noticeably remarkable value between 0.9988 and 1.0000. It is clear that when compared to the existing method, the NC score reduced as low as 0.9981 under similar conditions.

The proposed method showed a near-perfect robustness against Speckle noise, achieving perfect NC scores of 1.0000 for all watermarks at both 2% and 4% variance levels. ZWDC held up well at 2%; however, their performance decreased at 4%, with some watermarks dropping to 0.9985.

To sum up, these results make a compelling case, where the hybrid feature extraction and redundancy mechanisms built into the proposed method deliver a more reliable and stable defence against noise-based signal degradation than the current state-of-the-art alternative. **Table 4** shows a performance results table with the related study on filtering attacks.

Table 4. Performance table with related work on image filtering attacks using NC metric.

	Attack					
Method	**Median Filtering (7x7)**	**Median Filtering (9x9)**	**Average Filtering (7x7)**	**Average Filtering (9x9)**	**Weiner Filtering (7x7)**	**Weiner Filtering (9x9)**
(Wu et al., 2023) (W1)	1.0000	1.0000	0.9990	0.9990	0.9990	0.9990
(Wu et al., 2023) (W2)	1.0000	1.0000	0.9985	0.9985	0.9985	0.9985
(Wu et al., 2023) (W3)	1.0000	1.0000	0.9988	0.9988	0.9988	0.9988
(Wu et al., 2023) (W4)	1.0000	1.0000	0.9981	0.9981	0.9981	0.9981
(Wu et al., 2023) (W5)	1.0000	1.0000	0.9993	0.9993	0.9993	0.9993
Proposed method (W1)	1.0000	0.9988	1.0000	0.9994	1.0000	1.0000
Proposed method (W2)	1.0000	0.9988	1.0000	0.9994	1.0000	1.0000
Proposed method (W3)	1.0000	0.9989	1.0000	1.0000	1.0000	1.0000
Proposed method (W4)	1.0000	0.9989	1.0000	1.0000	1.0000	1.0000
Proposed method (W5)	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000

The filtering attack results shown in **Table 4** is similar, specifically against linear filtering. Whether facing Average or Wiener filtering, the proposed method achieves NC scores values of 1.0000, which is greater than that of ZWDC. The NC score of the existing method is between 0.9981 and 0.9993. Both methods demonstrate resilience against the Median filtering effectively, though at the larger mask size. The proposed method showed a marginal

reduction to 0.9988 compared to the related work which stayed optimal. Nevertheless, that retrieval quality exceeds above the required threshold for reliable medical image authentication.

To sum up, the results depict that the hybrid feature extraction method achieves enhanced robustness against signal processing attacks, particularly in preserving watermark integrity under high-intensity noise and linear blurring conditions.

Table 5 shows a performance results table with the related study on JPEG compressions attacks.

Table 5. Performance table with related work on JPEG compression attacks using NC metric.

Method	Attack				
	JPEG (QF=5)	**JPEG (QF=25)**	**JPEG (QF=45)**	**JPEG (QF=65)**	**JPEG (QF=75)**
Wu et al. (2023) (W1)	0.9980	0.9990	1.0000	1.0000	1.0000
Wu et al. (2023) (W2)	0.9970	0.9985	1.0000	1.0000	1.0000
Wu et al. (2023) (W3)	0.9977	0.9988	1.0000	1.0000	1.0000
Wu et al. (2023) (W4)	0.9962	0.9981	1.0000	1.0000	1.0000
Wu et al. (2023) (W5)	0.9987	0.9993	1.0000	1.0000	1.0000
Proposed method (W1)	0.9980	1.0000	1.0000	1.0000	1.0000
Proposed method (W2)	0.9982	1.0000	1.0000	1.0000	1.0000
Proposed method (W3)	0.9989	1.0000	1.0000	1.0000	1.0000
Proposed method (W4)	0.9989	1.0000	1.0000	1.0000	1.0000
Proposed method (W5)	1.0000	1.0000	1.0000	1.0000	1.0000

Table 5 shows how the proposed watermarking method is robust for JPEG compression attacks at different Quality Factors (QF) compared with Wu et al. (2023). The method proves notably more resilient, especially for a high compression ratio. At QF=5, where significant compression artifacts appear, the proposed method shows NC values between 0.9980 and 1.0000 across all five watermarks. On the other hand, the ZWDC method shows a noticeable drop and has reduced blow the value 0.9962.

At QF=25, the proposed method shows perfect recovery with NC scores of 1.0000 for all watermarks. The related work on the other hand still shows minor deviations, with NC values between 0.9981 and 0.9993. At higher quality factors of 45, 65 and 75, both methods maintain optimal performance with NC score values of 1.0000 across all watermarks.

This indicates that the proposed method achieves performance comparable to state-of-the-art methods at standard quality levels, while providing enhanced robustness under low-bandwidth or high-compression conditions. This represents a notable advantage in practical scenarios, where image quality is frequently compromised. **Table 6** shows the performance results of the proposed and existing methods on image scaling attacks.

Table 6. Performance table with related work on image scaling attacks using NC metric.

Method	Attack				
	SC (SF=0.5)	**SC (SF=0.75)**	**SC (SF=1.25)**	**SC (SF=1.75)**	**SC (SF=2)**
Wu et al. (2023) (W1)	1.0000	1.0000	1.0000	1.0000	1.0000
Wu et al. (2023) (W2)	1.0000	1.0000	1.0000	1.0000	1.0000
Wu et al. (2023) (W3)	1.0000	1.0000	1.0000	1.0000	1.0000
Wu et al. (2023) (W4)	1.0000	1.0000	1.0000	1.0000	1.0000

Wu et al. (2023) (W5)	1.0000	1.0000	1.0000	1.0000	1.0000
Proposed method (W1)	1.0000	1.0000	1.0000	1.0000	1.0000
Proposed method's (W2)	1.0000	1.0000	1.0000	1.0000	1.0000
Proposed method's (W3)	1.0000	1.0000	1.0000	1.0000	1.0000
Proposed method's (W4)	1.0000	1.0000	1.0000	1.0000	1.0000
Proposed method's (W5)	1.0000	1.0000	1.0000	1.0000	1.0000

Table 7 shows the proposed watermarking scheme against the ZWDC method under image scaling attacks, with Scaling Factors (SF) ranging from 0.5 to 2. Both approaches demonstrate robustness against geometric resizing. For all tests, whether reducing images to half size (SF = 0.5) or enlarging them to double size (SF = 2), all five watermarks maintained perfect NC scores of 1.0000. This shows that the proposed method may bring novel geometric correction techniques for rotation and translation, but it hasn't sacrificed the strong scaling stability that transform-domain approaches like DT-CWT are known for. In this particular area, it performs comparably to the related work's established benchmark. **Table 7** presents the performance results of the proposed method in comparison with related studies under rotation attacks.

Table 7. Performance table with related work on rotation attacks using NC metric.

	Attack				
Method	**RO (angle = 5°)**	**RO (angle = 10°)**	**RO (angle = 45°)**	**RO (angle = 90°)**	**RO (angle = 135°)**
Wu et al. (2023) (W1)	1.0000	1.0000	0.9990	1.0000	0.9990
Wu et al. (2023) (W2)	1.0000	1.0000	0.9985	1.0000	0.9985
Wu et al. (2023) (W3)	1.0000	1.0000	0.9988	1.0000	0.9988
Wu et al. (2023) (W4)	1.0000	1.0000	0.9981	1.0000	0.9981
Wu et al. (2023) (W5)	1.0000	1.0000	0.9993	1.0000	0.9993
Proposed method (W1)	1.0000	1.0000	0.9994	1.0000	0.9994
Proposed method (W2)	1.0000	1.0000	0.9994	1.0000	0.9994
Proposed method (W3)	1.0000	1.0000	0.9989	1.0000	0.9989
Proposed method (W4)	1.0000	1.0000	0.9989	1.0000	0.9989
Proposed method (W5)	1.0000	1.0000	0.9973	1.0000	0.9973

Table 7 demonstrates robust performance for both the ZWDC method and the proposed method against rotation attacks, with NC values remaining near-perfect across all tested angles. Both techniques achieve perfect scores of 1.0000 for small rotations of 5° and 10° as well as for the orthogonal rotation of 90°, indicating complete watermark preservation under these conditions. While performance decreases at diagonal angles of 45° and 135°, the values remain very high, ranging between 0.9973 and 0.9994 across all watermarks. The proposed method performs comparably to the baseline and exhibits slight improvements in specific instances, such as achieving 0.9994 with Watermarks 1 and 2 compared to ZWDC's respective 0.9990 and 0.9985, although it decreases slightly with Watermark 5. Overall, the data indicates that both watermarking strategies are highly effective and virtually indistinguishable in their resilience to geometric rotation distortions.
Table 8 presents the performance results of the proposed method in comparison with related studies under translation attacks.

Table 8. Performance table with related work on translation attacks using NC metric.

Method	Attack					
	TSL ([-5,0])	**TSL ([5,0])**	**TSL ([0,-5])**	**TSL ([0,5])**	**TSL ([-5,5])**	**TSL ([5,-5])**
Wu et al. (2023) (W1)	0.9960	0.9970	0.9990	0.9960	0.9891	0.9950
Wu et al. (2023) (W2)	0.9940	0.9955	0.9985	0.9940	0.9834	0.9925
Wu et al. (2023) (W3)	0.9953	0.9965	0.9988	0.9953	0.9871	0.9941
Wu et al. (2023) (W4)	0.9924	0.9943	0.9981	0.9924	0.9791	0.9905
Wu et al. (2023) (W5)	0.9974	0.9980	0.9993	0.9974	0.9928	0.9967
Proposed method (W1)	0.9994	0.9976	1.0000	1.0000	0.9945	0.9939
Proposed method (W2)	0.9994	0.9976	1.0000	1.0000	0.9946	0.9940
Proposed method (W3)	0.9989	0.9957	1.0000	1.0000	0.9904	0.9993
Proposed method (W4)	0.9989	0.9954	1.0000	1.0000	0.9897	0.9986
Proposed method (W5)	0.9973	0.9973	1.0000	1.0000	0.9858	0.9828

Table 8 shows that the results for translation attacks indicate that the proposed method generally outperforms the ZWDC method. It demonstrates superior robustness, particularly in vertical displacements. The proposed method achieves perfect NC scores of 1.0000 across nearly all watermarks for vertical shifts TSL [0, -5] and TSL [0, 5], whereas the related and baseline method consistently exhibit slight degradation in these scenarios, with values ranging from approximately 0.9924 to 0.9993. This advantage is also observed in the horizontal shifts TSL [-5, 0], where the proposed method maintains near-perfect scores of around 0.9994 compared to the baseline's average of approximately 0.9960. While both methods experience a minor performance reduction during complex diagonal translations such as TSL [5, -5], the proposed method remains highly competitive, demonstrating strong capability in preserving watermark integrity under geometric displacement.
Table 9 presents the proposed method's performance evaluated by BER in comparison to the scheme by **(Wu et al., 2023; Xia et al., 2021)** under various attacks.

Table 9. Performance table with related works on various attacks using NC and BER metric.

Attack Type	Proposed methods					
	Wu et al. (2023)		**Xia et al., (2021)**		**Proposed Method**	
	NC	**BER**	**NC**	**BER**	**NC**	**BER**
Gaussian Noise %3	0.9922	0.6191	0.8048	16.4337	1.0000	0.0000
Salt and Pepper Noise %3	0.9962	0.2994	0.8052	16.3682	0.9994	0.0000
Speckle Noise %3	0.9957	0.3365	0.8048	16.4020	1.0000	0.0000
Median Filtering (5x5)	0.9996	0.0352	0.8062	16.2690	1.0000	0.0000
Gaussian Filtering (5x5)	0.9999	0.0068	0.8052	16.3653	1.0000	0.0000
JPEG Compression (QF=20)	0.9957	0.3340	0.8042	16.4510	0.9988	0.0020
Crop (1/16)	0.9811	1.5020	0.7948	17.2790	0.9980	0.2111
Scaling Factor (SF=0.5)	0.9998	0.0156	0.8049	16.3869	1.0000	0.0000
Scaling Factor (SF=2.5)	1.0000	0.0000	0.8044	16.4365	1.0000	0.0000
Scaling Factor (SF=4)	1.0000	0.0000	0.8045	16.4286	1.0000	0.0000
Rotation (Angle=5°)	0.9919	0.6357	0.8050	16.3790	0.9951	0.0078
Rotation (Angle=10°)	0.9788	1.6787	0.8050	16.3818	0.9910	0.0283
Translation ([-5,0])	0.9846	1.2148	0.7813	18.4436	0.9989	0.0596
Translation ([-5,5])	0.9769	1.8340	0.7742	19.0782	0.9904	0.9993

Table 9 shows a comprehensive evaluation of the proposed method's robustness by measuring both NC and BER against the schemes proposed by **(Wu et al., 2023; Xia et al., 2021)** by using different attacks. Under noise injection such as 3% Gaussian, Salt and Pepper and Speckle noise, the proposed method shows stability by achieving perfect or near perfect NC scores of up to 1.0000 and a BER of 0.0000, whereas Wu et al. shows slight degradations and Xia et al. struggles greatly with BERs exceeding 16.3. The proposed method also proves to be highly resilient to data loss and compression artifacts. For example, under heavy JPEG compression (QF=20) maintains an NC of 0.9988 and a minimal BER of 0.0020, and under a 1/16 cropping attack it achieves an NC of 0.9980 and a BER of 0.2111, outperforming both other methods. Moreover, the framework's robustness is validated under complex geometric distortions by achieving great recovery across varying scaling factors (SF=0.5 to 4) and maintaining higher similarity values and lower error rates during attacks like translation and rotation such as achieving 0.0283 BER under a 10° rotation while Wu et al.'s method experiences a substantial error spike to 1.6787.

Table 10 presents the proposed method's NC in comparison to the ZWDC scheme along with the execution time in both the registration and verification stages under the most complex and extreme attacks, which are referred to as combined attacks, in order to demonstrate the proposed method's effectiveness and practicality.
Combinations of attacks at once involve geometric data removal, like cropping paired with scaling, are the most dominant and difficult attacks. While the proposed method easily filters out signal level distortions like noise or compression, extreme cropping can delete the stable image blocks that watermarking systems rely on. This structural loss leaves less raw data to reconstruct the watermark which explains the slight performance drop in those specific scenarios.

Table 10. Performance table with related work on combined attacks and the proposed method's execution times

	Attack			
Attack	**Wu et al. (2023) NC**	**Proposed method NC**	**Proposed method Registration Time (T_{reg}) in seconds (s)**	**Proposed method Verification Time (T_{ver}) in seconds (s)**
SN(3%)+JPEG(QF=60)	0.9883	1.0000	0.288808	0.171253
SPN(3%)+GF(5 × 5)	0.9865	0.9982	0.295022	0.173540
SC(SF=2.5)+Crop(1/16) (W3)	0.9934	0.9684	2.185601	0.337559
RO(angle=90°)+MF(5 × 5)	0.9644	0.9957	0.293869	0.170926
GN(3%)+TSL([-5,0])	0.9702	0.9994	0.702106	0.166325

Based on the results in **Table 10**, the proposed method demonstrates superior robustness compared to related work in four out of five combined attack scenarios and achieving great NC scores of up to 1.0000. Although the scaling and cropping attack results in a slightly lower NC and increased registration time (2.18s), the scheme proves highly resilient against complex rotation and noise combinations. Furthermore, the consistently fast verification times (averaging ~0.17s) highlight the algorithm's computational efficiency and suitability for real-time applications.

In standard telemedicine and clinical workflows, an authentication process requiring less than 1 second is generally classified as real time as it introduces almost no loading delay for a physician retrieving medical images.

Fig. 3 below illustrates different watermarks in their original state, and after they were extracted from an attacked host image.

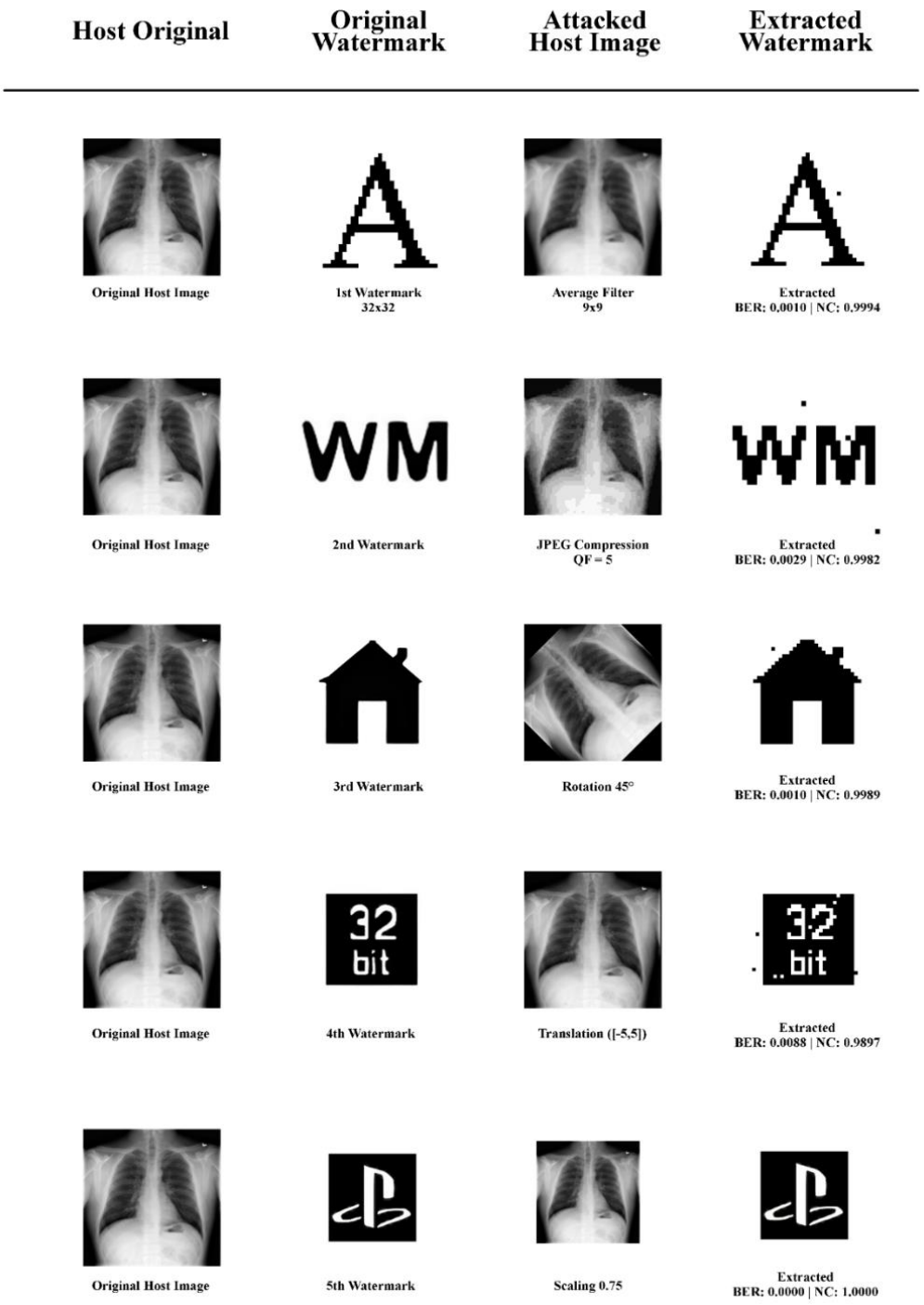

Figure 3. Visual demonstration of the extracted watermarks

5. CONCLUSIONS

Feature extraction plays a fundamental role in ZWM, as it directly enhances the robustness and reliability of watermark extraction algorithms. This paper presents a robust ZWM method to address the geometric vulnerability of medical image authentication. Different from traditional methods which struggle with synchronization during rotation or displacement, the proposed method integrates DT-CWT with a novel Blind Geometric Correction module. By using statistical image moments to compute the principal axis and skewness, the proposed method successfully normalizes image orientation before feature extraction. This effectively neutralizes rotation and flipping attacks without requiring the original cover image. In addition, the feature extraction process is more stabilized through a hybrid approach combining SVD and IDE. This ensures that the extracted signatures remain distinct and robust to common signal-processing attacks (filtering, sharpening, and compression). To ensure the confidentiality and integrity of patient data, the watermark is secured using a dual-layer encryption mechanism involving Logistic Map chaotic sequences and Arnold Scrambling, rendering the hidden information statistically undetectable to unauthorized users. Experimental evaluation shows that the proposed method outperforms the state-of-the-art methods on a wide range of distortions, which include:

- Geometric Attacks: demonstrating exceptional resilience to rotation, scaling, and translation.
- Signal Degradation: maintaining high fidelity under different noisy environments as well as aggressive JPEG compression ($QF = 5$).

While verification is fast, registration is computationally heavy under extreme combined attacks. Further validation is required for 3D volumetric medical images, and severe cropping can break the redundancy mechanism ($R = 4$).

To sum up, this method provides a secure, non-intrusive solution for medical copyright protection. It balances computational efficiency with high robustness, making it suitable for real-time telemedicine applications as well as the protection of sensitive diagnostic imagery. Future work will focus on extending this blind geometric correction capability to 3D medical image volumes for healthcare applications.

NOMENCLATURE

Symbol	Description	Symbol	Description
BER	Bit Error Rate	NC	Normalized Correlation.
CNN	Convolutional Neural Network.	QF	Quality Factor.
DCT	Discrete Cosine Transform.	RO	Rotation.
DT-CWT	Dual-Tree Complex Wavelet Transform.	SC	Scaling.
DWT	Discrete Wavelet Transform.	SF	Scaling Factor.
FrROMs	Fractional Racah Moments.	SN	Speckle Noise.
GF	Gaussian Filtering.	SPN	Salt & Pepper Noise.
GN	Gaussian Noise.	SVD	Singular Value Decomposition.
IDE	Improved Differential Entropy.	T_{reg}	Registration Time, s.
LL	Low-Pass Approximation Subband.	TSL	Translation.
MF	Median Filtering.	T_{ver}	Verification Time, s.
MSE	Mean Squared Error.	ZWM	Zero-watermarking.

Acknowledgements

The authors would like to thank the University of Baghdad for general help and support.

Credit Authorship Contribution Statement

Ali Nasif Jasim: Writing original draft, Writing – review & editing, Methodology, Software, and Validation. Sadiq H. Abdulhussain: Writing – original draft, Writing – review & editing, Methodology, Supervision, and proofreading. Abir Hussain: Writing – original draft, Writing – review & editing, and proofreading.

Declaration of Competing Interest

The authors declare that they have no known competing financial or personal interests that could have appeared to influence the work reported in this paper.

REFERENCES

Abdulhussain, S.H., Mahmmod, B.M., Flusser, J., AL-Utaibi, K.A. and Sait, S.M., 2022. Fast overlapping block processing algorithm for feature extraction. *Symmetry*, 14(4), pp. 715–715. https://doi.org/10.3390/sym14040715

Aberna, P. and Agilandeeswari, L., 2024. Digital image and video watermarking: methodologies, attacks, applications, and future directions. *Multimedia Tools and Applications*, 83(2), pp. 5531–5591. https://doi.org/10.1007/s11042-023-15806-y.

Ali, M. and Kumar, V., 2024. A robust zero-watermarking scheme in spatial domain by achieving features similar to frequency domain. *Electronics*, 13(13), P. 2935. https://doi.org/10.3390/electronics13020435

Alomoush, W., Khashan, O.A., Alrosan, A., Attar, H.H., Almomani, A., Alhosban, F. and Makhadmeh, S.N., 2023. Digital image watermarking using discrete cosine transformation based linear modulation. *Journal of Cloud Computing*, 12(1), P. 96. https://doi.org/10.1186/s13677-023-00468-w

Basnayaka, D.A. and Jia, J., 2023. Bit error rate performance and diversity analysis for mediumband wireless communication. *2023 IEEE Virtual Conference on Communications (VCC)*, pp. 224–229. https://doi.org/10.1109/vcc60689.2023.10474832

Çelik, H., and Doğan, N., 2024. A hybrid color image encryption method based on extended logistic map. *Multimedia Tools and Applications*, 83(5), pp. 12627-12650. https://doi.org/10.1007/s11042-023-16215-x

Dong, F., Li, J., Bhatti, U.A., Liu, J., Chen, Y.-W., Li, D., 2023. Robust zero watermarking algorithm for medical images based on improved NasNet-Mobile and DCT. *Electronics*, 12(16), P. 3444. https://doi.org/10.3390/electronics12163444

El-Khanchouli, K., Mansouri, H., El Ghouate, N., Karmouni, H., Joudar, N.-E., Sayyouri, M., Askar, S.S., Abouhawwash, M., 2025. Protecting medical images using a zero-watermarking approach based on fractional Racah moments. *IEEE Access*, 13, pp. 16978-17001. https://doi.org/10.1109/ACCESS.2025.3532747

Gong, C., Liu, J., Gong, M., Li, J., Bhatti, U.A., Ma, J., 2022. Robust medical zero-watermarking algorithm based on Residual-DenseNet. *IET Biometrics*, 11(6), pp. 547-556. https://doi.org/10.1049/bme2.12100

Gonzalez, R.C. and Woods, R.E., 2018. *Digital image processing*. 4th ed. New York, NY: Pearson.

Hosny, K.M., Magdi, A., Osama ElKomy and Hanaa M. Hamza, 2024. Digital image watermarking using deep learning: A survey. *Computer Science Review*, 53, pp. 100662–100662. https://doi.org/10.1016/j.cosrev.2024.100662

Jasim, A. and Abdulhussain, S., 2025. A comprehensive review of digital watermarking techniques: applications, characteristics, classification, and related aspects. *Journal of Information Hiding and Multimedia Signal Processing*, 16(4). https://www.jihmsp.org/2025/vol16/N4/09.JIHMSP-250704.pdf

Kalarikkal Pullayikodi, S., Tarhuni, N., Ahmed, A. and Shiginah, F., 2017. Computationally efficient robust color image watermarking using Fast Walsh Hadamard transform. *Journal of Imaging*, 3(4), P. 46. https://doi.org/10.3390/jimaging3040046

Khan, M.F., Monir, S.M.G., Naseem, I., 2019. A novel zero-watermarking based scheme for copyright protection of grayscale images. *Mehran University Research Journal of Engineering & Technology*, 38(3), pp. 627-640. https://doi.org/10.22581/muet1982.1903.09

Lebcir, M., Awang, S. and Benziane, A., 2024. Robust blind image watermarking scheme using a modified embedding process based on differential method in DTCWT-DCT. *Multimedia Tools and Applications*, 83(22), pp. 61379–61405. https://doi.org/10.1007/s11042-024-18185-0

Li, C., Sun, H., Wang, C., Chen, S., Liu, X., Zhang, Y., Ren, N., Tong, D., 2024. Zwnet: A deep-learning-powered zero-watermarking scheme with high robustness and discriminability for images. *Applied Sciences*, 14(1), P. 435. https://doi.org/10.3390/app14010435

Liu, F., Ma, L., Liu, C., Lu, Z.-M., 2018. Zero watermarking scheme based on U and V matrices of quaternion singular value decomposition for color images. *J. Inf. Hiding Multim. Signal Process.*, 9(3), pp. 629-640. https://www.jihmsp.org/~jihmsp/2018/vol9/JIH-MSP-2018-03-013.pdf

Meenakshi, K., Swaraja, K., Kora, P. and Kumari, U.C., 2019. Texture feature based oblivious watermarking with slant transform using fuzzy logic. *In: 2019 IEEE 5th International Conference for Convergence in Technology (I2CT)*. pp. 1–5. https://doi.org/10.1109/I2CT45611.2019.9033613.

Moad, M.S., Kafi, M.R. and Khaldi, A., 2022. Medical image watermarking for secure e-healthcare applications. *Multimedia Tools and Applications*, 81(30), pp. 44087–44107. https://doi.org/10.1007/s11042-022-12004-0

Panday, S.P., Manandhar, S., Shakya, A., Joshi, B., Year. Hybrid color watermarking technique with Arnold scrambling. *In Proceedings of the 2024 6th International Conference on Image Processing and Machine Vision*, pp. 94-99. https://doi.org/10.1145/3645259.3645275

Rani, A., Bhullar, A.K., Dangwal, D., Kumar, S., 2015. A zero-watermarking scheme using discrete wavelet transform. *Procedia Computer Science*, 70, pp. 603-609. https://doi.org/10.1016/j.procs.2015.10.046

Riaz, M., Dilpazir, H., Naseer, S., Mahmood, H., Anwar, A., Khan, J., Benitez, I.B. and Ahmad, T., 2024. Secure and fast image encryption algorithm based on modified logistic map. *Information*, [online] 15(3), P. 172. https://doi.org/10.3390/info15030172

Sharma, S. and Kumar, V., 2018. Performance evaluation of 2D face recognition techniques under image processing attacks. *Modern Physics Letters B*, 32(19), P. 1850212. https://doi.org/10.1142/s0217984918502123

Sharma, S., Zou, J.J., Fang, G., Shukla, P., Cai, W., 2024. A review of image watermarking for identity protection and verification. *Multimedia Tools and Applications*, 83(11), pp. 31829-31891. https://doi.org/10.1007/s11042-023-16843-3

Singh, A., and Dutta, M.K., 2020. A robust zero-watermarking scheme for tele-ophthalmological applications. *Journal of King Saud University-Computer and Information Sciences*, 32(8), pp. 895-908. https://doi.org/10.1016/j.jksuci.2017.12.008

Song, C., Sudirman, S., Merabti, M. and Llewellyn-Jones, D., 2010. Analysis of Digital Image Watermark Attacks. *2010 7th IEEE Consumer Communications and Networking Conference*, pp. 1–5. https://doi.org/10.1109/ccnc.2010.5421631

Su, Q., Liu, D. and Sun, Y., 2022. A robust adaptive blind color image watermarking for resisting geometric attacks. *Information Sciences*, 606, pp. 194–212. https://doi.org/10.1016/j.ins.2022.05.046

Taj, R., Tao, F., Kanwal, S., Almogren, A., Altameem, A., Ur Rehman, A., 2024. A reversible-zero watermarking scheme for medical images. *Scientific Reports*, 14(1), P. 17320. https://doi.org/10.1038/s41598-024-67672-9

Wang, G., Ye, X. and Zhao, B., 2024. A novel remote sensing image encryption scheme based on block period Arnold scrambling. *Nonlinear Dynamics*, 112(19), pp. 17477–17507. https://doi.org/10.1007/s11071-024-09953-6

Wang, X., Wen, M., Tan, X., Zhang, H., Hu, J. and Qin, H., 2022. A novel zero-watermarking algorithm based on robust statistical features for natural images. *The Visual Computer*, 38(9-10), pp. 3175–3188. https://doi.org/10.1007/s00371-022-02544-9

Wu, D., Li, L., Wang, J., Ma, P., Wang, Z., Wu, H., 2023. Robust zero-watermarking scheme using DT CWT and improved differential entropy for color medical images. *Journal of King Saud University-Computer and Information Sciences*, 35(8), P. 101708. https://doi.org/10.1016/j.jksuci.2023.101708

Xi, X., Zhang, J., Du, J. and Yang, Z., 2024. Desynchronization attacks resistant watermarking for remote sensing images based on DWT-SVD and normalized feature domain. *Transactions in GIS*, 28(8), pp. 2705–2721. https://doi.org/10.1111/tgis.13262

Xia, Z., Wang, X., Han, B., Li, Q., Wang, X., Wang, C. and Zhao, T., 2021. Color image triple zero-watermarking using decimal-order polar harmonic transforms and chaotic system. *Signal Processing*, 180, pp. 107864–107864. https://doi.org/10.1016/j.sigpro.2020.107864

Ying, Q., Lin, J., Qian, Z., Xu, H., Zhang, X., 2019. Robust digital watermarking for color images in combined DFT and DT-CWT domains. *Mathematical Biosciences and Engineering*, 16(5), P. 4788. https://doi.org/10.3934/mbe.2019241

Yuan, Y., Li, J., Liu, J., Bhatti, U. A., Liu, Z. and Chen, Y., 2024. Robust zero-watermarking algorithm based on discrete wavelet transform and daisy descriptors for encrypted medical image. *CAAI Transactions on Intelligence Technology*. https://doi.org/10.1049/cit2.12282

Zhang, F., Wang, H., He, M. and Xia, J., 2024. Robust blind symmetry-based watermarking in the frequency domain against social network processing and desynchronization attacks. *IEEE Transactions on Circuits and Systems for Video Technology*, pp. 1–1. https://doi.org/10.1109/tcsvt.2024.3395802

Zhong, X., Das, A., Alrasheedi, F. and Tanvir, A., 2023. A brief, in-depth survey of deep learning-based image watermarking. *Applied Sciences*, [online] 13(21), p.11852. https://doi.org/10.3390/app132111852

خطط قوي للعلامة المائية الصفرية للصور الطبية باستخدام تحويل المويجات المركبة مزدوجة الشجرة (DT-CWT) والتصحيح الهندسي الأعمى

علي نصيف جاسم[1]، صادق حبيب عبد الحسين[1]، *، عبير جعفر حسين[2]

[1]قسم هندسة الحاسبات, كلية الهندسة, جامعة بغداد, بغداد, العراق.
[2]قسم الهندسة الكهربائية، جامعة الشارقة، الشارقة، الإمارات العربية المتحدة.

الخلاصة

إن حماية الصور الطبية في التطبيقات الطبية هي عملية توازن دقيقة. فهناك حاجة لحماية بيانات المرضى دون المساس بالمحتوى التشخيصي الفعلي. تقدم العلامة المائية الصفرية (Zero-watermarking) حلاً أنيقاً من خلال ربط معلومات حقوق النشر منطقياً بالسمات المتأصلة في الصورة بدلاً من دفنها في البيكسلات نفسها. ومع ذلك، هناك مقايضة؛ حيث تفشل معظم الطرق الحالية عندما يقوم شخص ما ببساطة بتدوير الصورة. حتى الميل الطفيف يكسر عملية استخراج الميزات، مما يجعل العلامة المائية عديمة الفائدة. يتناول نهج هذه الورقة هذه المشكلة بشكل مباشر باستخدام تحويل المويجات المركبة مزدوجة الشجرة (DT-CWT) لاستخراج ميزات مستقرة وغير متغيرة للإزاحة من المكونات منخفضة التردد، ثم معالجتها باستخدام الإنتروبيا التفاضلية المحسنة (IDE) لمقاومة هجمات معالجة الإشارات الشائعة. قبل ربط العلامة المائية بهذه الميزات، نقوم بتشفيرها باستخدام خلط أرنولد (Arnold scrambling) بالإضافة إلى التخطيط اللوجستي (logistic mapping) لمزيد من الأمان. تصمد هذه الطريقة أمام الضوضاء، والترشيح (الفلترة)، وضغط JPEG، والأهم من ذلك، الهجمات الهندسية. وبفضل التصحيح المعتمد على العزم، تحقق الدراسة درجات ارتباط تطبيعي (Normalized Correlation) تزيد عن 0.99 في ظل معظم الهجمات بما في ذلك التدوير الشديد، مما يحل نقطة ضعف طويلة الأمد في أبحاث العلامة المائية الصفرية. بالنسبة لحماية الصور الطبية، يعني هذا حلاً موثوقاً وآمناً وعملياً لتطبيقات التطبيب عن بعد في العالم الحقيقي.

الكلمات المفتاحية: العلامة المائية الصفرية، خلط أرنولد، دمج الميزات، التصحيح الهندسي الأعمى.