
Research article

Fractional-order polar harmonic Fourier moments and 1D chaotic mapping for robust zero-watermarking of medical images

Abdallah Abdelaziz, Mohamed M. Darwish* and Mohamed A. Barakat

Department of Computer Science, University College of Alwajh, University of Tabuk, Al Wajh 48721, Saudi Arabia

* **Correspondence:** Email: M_darwish@ut.edu.sa.

Abstract: The continuous evolution of digital medical imaging underscores the critical importance of ensuring image security. Conventional watermarking techniques for robustness typically embed copyright details into the image, thereby altering its original form and making them unsuitable for domains such as the military and medicine, where absolute image fidelity is essential. To address this limitation, this paper proposes a robust zero-watermarking algorithm that enables copyright protection of medical images without modifying the host image. In this approach, fractional-order polar harmonic Fourier moments (FrPHFMs) were employed as invariant geometric descriptors in the construction of zero-watermarks. First, FrPHFMs were computed, and then the most accurate descriptors were selected to provide improved performance and strong geometric invariance. The extracted features are then integrated with a binary watermark using a 1D chaotic map (1D-RSS), formulated from reciprocal and squared sine functions and incorporating an exclusive or (XOR) operation, to construct the zero-watermark. Building on this design, a hybrid FrPHFM-chaos zero-watermarking algorithm was introduced, in which FrPHFMs ensure strong resilience to geometric distortions, while the chaotic map enhances security through its sensitivity to initial parameters. Experimental results demonstrated that the proposed algorithm exhibits high resistance to geometric distortions, conventional attacks, and combined attacks, outperforming existing methods. It achieves bit error rate (BER) < 0.001 and normalized correlation (NC) > 0.9 , confirming its superior robustness.

Keywords: zero-watermarking; chaotic mapping; fractional-order polar harmonic Fourier moments; medical images

Mathematics Subject Classification: 94A08

1. Introduction

With the continuous innovation of digital technology, the depth and breadth of the development of digital medical imaging technology have been significantly broadened [1]. The evolution of communication technologies has transformed healthcare, moving it from traditional diagnostic practices to telemedicine, thereby boosting the exchange and transfer of medical data such as X-ray, CT, and MRI images [2]. The digitization of medical imaging has revolutionized modern healthcare by enabling faster diagnostics, more efficient data sharing, and enhanced patient care. Medical images, as key outputs of digital hospitals, store private information such as patients' pathological characteristics and serve as a vital basis for doctors to diagnose their conditions [3, 4]. Nevertheless, during online storage or transmission, these images are vulnerable to various attacks, potentially leading to data leakage and misuse [5]. The easy access to powerful image editing tools increases the risk of malicious actions like medical identity theft, insurance fraud, and evidence tampering, with serious implications for individuals and society. As telemedicine and digital data transmission grow, safeguarding the integrity and confidentiality of medical images is vital. Unauthorized alterations can lead to misdiagnosis, privacy breaches, and legal issues. Additionally, rising medical data theft threatens public health systems, causing financial loss, compromising patient privacy, and disrupting daily life. Protecting and exchanging medical images in a secure manner is essential for safeguarding patient care and advancing medical collaboration and research [6]. Therefore, safeguarding medical information has become crucial, and rising concerns about patient privacy, data security, and the authenticity of medical images have highlighted the importance of innovative solutions such as digital watermarking to protect these critical assets [7].

The application of digital image watermarking has become widespread to safeguard the security and privacy of medical data. It not only helps protect sensitive patient information but also provides technical support for safeguarding data integrity. Additionally, watermarking is commonly applied for anti-counterfeiting certification and copyright protection of medical images [8,9].

Traditional approaches to watermarking protect digital images by embedding identifiers, such as digital signatures, into the image content [10–13]. Nevertheless, the embedding process inevitably alters the image, which can result in visual distortions and reduced diagnostic integrity in medical imaging.

Even minimal distortions caused by embedding a watermark can distort critical visual details, potentially impacting diagnostic accuracy and increasing the risk of medical errors or malpractice [14]. Therefore, such traditional techniques are generally unsuitable for use in this sensitive domain. To address the drawbacks of conventional watermarking, zero-watermarking has been introduced as an effective alternative that maintains image integrity and prevents distortion. Rather than embedding a watermark into the image, this approach derives unique features from the image and fuses them with copyright data to construct the watermark [15, 16]. This approach effectively ensures the security and authenticity of medical images without altering their content [17–19]. By relying on robustness and imperceptibility, zero-watermarking maintains the original visual and diagnostic quality of the images, making it highly suitable for clinical applications where accuracy and image integrity are critical, as well as for protecting the copyrights of medical images. Zero-watermarking plays an essential role in copyright protection for the healthcare sector. It verifies ownership and prevents the unauthorized distribution of critical data such as medical images, research findings, and patient reports. Consequently, this technique is highly effective at ensuring the integrity, authenticity, and overall

security of electronic medical data [20, 21]. Zero-watermark approaches offer key benefits, including high robustness against multiple attacks and superior imperceptibility [22]. Since the first introduction of the zero-watermarking solution [23], numerous algorithms of zero-watermarking have been developed; however, they still exhibit certain limitations when utilized for protecting the copyright of medical images [24–26].

Most of the current zero-watermarking algorithms exhibit limited robustness against complex attacks, with geometric transformations posing a particularly significant challenge. Additionally, medical images from the same modality often appear highly similar, reducing the discriminative power of the generated zero-watermarks. The limited discriminative capacity of medical image features results in increased false positives during copyright recognition, which diminishes the efficacy of existing zero-watermarking algorithms.

Watermarking research focuses on robustness, invisibility, and security, with robustness against geometric attacks remaining a key challenge. Addressing poor discrimination and weak resistance to geometric attacks is essential for improving the robustness and distinctiveness of zero-watermarks in medical images. In light of the existing limitations, this research aimed to develop a more straightforward algorithm while maintaining strong performance. Based on the importance of the fractional calculus field and the opportunities it provides to leverage the distinctive characteristics of various applications [27], fractional-order continuous orthogonal moments provide enhanced theoretical robustness and geometric invariance compared with their integer-order counterparts, improving resistance to geometric and signal processing attacks. Among them, FrPHFM, which extends polar harmonic Fourier moments (PHFM) and has been applied to quaternion polar harmonic Fourier moments (QPHFM), precise quaternion polar harmonic Fourier moments (PQPHFM) [28, 29], and accurate human parsing [30], introduces a fractional-order parameter that enhances feature representation and stability, improves robustness to geometric transformations including rotation, scaling, cropping, and aspect ratio changes as well as noise, and captures finer image details. PHFMs are a special case of FrPHFMs when the fractional parameter equals 1, making the FrPHFM a more flexible and general framework. Building on this, FrPHFMs are designed to address geometric distortions in watermarking. Their fractional orders offer greater flexibility in capturing fine details under severe distortions, making FrPHFMs highly effective for robust medical-image zero-watermarking. Based on this, the paper proposes a zero-watermarking algorithm that utilizes fractional orthogonal moment features to achieve robustness, security, and efficiency, thereby safeguarding the copyrights of medical images. The key contributions of this research can be outlined as follows:

- We introduce an FrPHFM-based zero-watermarking scheme for securing medical images.
- Encryption of the watermark image via a 1D-RSS chaotic map serves to enhance its overall security.
- The proposed method is evaluated using publicly accessible medical image datasets to demonstrate its practical effectiveness.
- Extensive experiments confirm that the suggested algorithm effectively achieves zero-watermark construction and verification, delivering satisfactory results and surpassing existing approaches in resisting conventional and geometric attacks, particularly geometric and combined ones.

This paper is structured as follows: Section 2 covers related work. Section 3 provides the theoretical background on FrPHFMs and 1D-RSS chaotic mapping. The proposed method is outlined in Section 4, with experimental results discussed in Section 5, and the conclusion presented in

Section 6.

2. Related works

In zero-watermarking, feature extraction is a crucial step for achieving robust and imperceptible copyright protection, especially in sensitive areas like medical imaging and digital forensics. It involves identifying key image information at the pixel level that remains invariant under geometric transformations and conventional attacks. Therefore, the success of zero-watermarking relies to a great extent on extracting geometrically invariant features from images. Although many algorithms have been proposed, the main challenge lies in reliably extracting features that can withstand diverse distortions and manipulations, especially geometric distortions. Since modifications to medical images are not allowed, zero-watermarking has attracted significant interest from researchers. This section presents several related zero-watermarking techniques, focusing on methods for feature image construction, such as moment-based and deep learning-based approaches, etc. Recently, significant attention has been directed toward zero-watermarking algorithms based on orthogonal moments, especially those with fractional order, due to their geometric invariance and stability, which enable effective extraction of distinctive image features. These methods enhance robustness to geometric manipulations, ensuring high accuracy in watermark recovery under transformations such as scaling and rotation, thereby motivating extensive research on zero-watermarking algorithms based on fractional orthogonal moments. Xia et al. [29] proposed a QPHFM-based zero-watermarking approach for color medical images. The incorporation of PQPHFM in feature image generation provides the method with notable stability and geometric invariance, enhancing robustness against geometric manipulations. Xia et al. [31] investigated an FoRHFM-based zero-watermarking algorithm aimed at ensuring grayscale medical-image copyright protection. In [32], Hosny and Darwish developed a zero-watermarking method for multi-color medical images that utilizes FrMGMs. Khafaga et al. [33] employed 1D Chebyshev chaos and MFrGHMs to introduce an algorithm of zero-watermarking for color medical images. A zero-watermarking framework utilizing QFPJFMs for color images was proposed by Wang et al. [34]. Xia et al. [35] presented a copyright verification method for colored medical images utilizing a lossless watermarking scheme that leverages accurate coefficients extracted through QPHTs. The algorithm developed by Wang et al. [36] incorporated the PCET to process grayscale images, including both standard and medical types. Wang et al. [37] presented a zero-watermarking approach using modified Zernike moments, enhancing robustness against geometric attacks and enabling copyright verification that preserves the original image data. A robust zero-watermarking approach utilizing QPHFMs, which allows simultaneous copyright protection of three CT images, was proposed by Xia et al. [38]. El-Khanchouli et al. [39] proposed a zero-watermarking method that uses fractional Racah moments to protect medical images. Recently, convolutional neural networks (CNNs) are increasingly employed in zero-watermarking, as they automatically derive robust, manipulation-invariant features, obviating manual feature design and offering improved robustness relative to traditional techniques. Fierro-Radilla [40] recently introduced a new research direction in zero-watermarking by proposing a technique based on CNNs. Utilizing CNNs, Liu et al. [41] proposed an approach of zero-watermarking. In this approach, the zero-watermark is generated by mapping the color style of the cover image onto the watermark. The VGG19 deep CNN was applied to propose effective zero-watermarking methods by Han et al. [42] and Darwish et al. [43]. Farhat et al. [44] introduced a zero-watermarking method for medical images that uses the ResNet50 model combined

with a logistic-Gaussian chaotic map, enabling resistance to geometric and conventional attacks. Huang et al. [45] developed a medical image zero-watermarking method that employs a pre-trained DO-VGG network. This network extracts high-dimensional robust features to construct a zero-watermark, ensuring reliable and imperceptible copyright protection. Han et al. [46] introduced an approach of zero-watermarking that employs a pretrained Swin transformer to extract multiscale depth features from host images for the construction of the zero-watermark. A zero-watermarking method combining deep learning and transform-domain techniques was proposed by Anand et al. [47], using AlexNet for robust feature extraction and integrating singular value decomposition (SVD) with non-sampled Shearlet transform to generate the zero-watermark image. A zero-watermarking approach based on DarkNet-53 was presented by Abdel-Aziz et al. [48], in which the Fibonacci Q-matrix is fused with the stationary wavelet transform for zero-watermark generation. A medical image zero-watermarking algorithm that integrates the discrete cosine transform with an improved NasNet-Mobile network was proposed by F. Dong et al. [49]. A residual-DenseNet-based medical image zero-watermarking technique was presented by C. Gong et al. [50] to achieve higher robustness. Xiang et al. [51] developed a ResNet-based medical image zero-watermarking approach, focusing on style feature extraction to reduce attack-induced data loss. The generator network produces the zero-watermark, while the detector network validates it. Sheng et al. [52] introduced an algorithm of zero-watermarking leveraging ResNet50 in combination with a discrete cosine transform (DCT) for improved robustness. A robust zero-watermarking method employing ResNet101, a discrete wavelet transform (DWT), and a DCT for feature extraction was presented by Nawaz et al. [53]. Yu, Fan et al. [54] developed a CNN-based zero-watermarking method employing Inception V3 and chaotic mapping, offering robustness against geometric manipulations but limited protection against conventional attacks. In [55], Zhang et al. trained a GoogLeNet network using transfer learning to extract features of the image and encrypt the watermark with a 2D Henon chaotic map, yielding a GoogLeNet-DCT algorithm highly resistant to geometric attacks. In [56], a two-stage framework named ConZWNNet was proposed by D. Tong et al., employing ConvNeXt with contrastive learning for robust feature extraction and a residual network with a multilayer perceptron (MLP) to fuse features for latent zero-watermark generation. A robust zero-watermarking method for medical imaging, based on a multi-branch CNN-transformer model, is introduced by Wang et al. [57].

3. Fundamental concepts

This section briefly introduces the basic theoretical components utilized in this study, encompassing integer-order PHFMs, FrPHFMs, and a one-dimensional chaotic map, 1D-RSS.

3.1. Integer-order PHFMs

The integer-order PHFMs, defined for an image $f(r, \theta)$ in the polar coordinate with moment order $p(p \geq 0)$ and repetition $q(|q| \geq 0)$, can be expressed as follows [28]:

$$F_{pq} = \frac{2}{\pi} \int_0^{2\pi} \int_0^1 f(r, \theta) [W_{pq}(r, \theta)]^* r dr d\theta = \frac{2}{\pi} \int_0^{2\pi} \int_0^1 f(r, \theta) T_p(r) e^{-iq\theta} r dr d\theta, \quad (1)$$

where F_{pq} denotes the PHFMs, $e^{-iq\theta}$ represents the angular Fourier component, and $T_p(r)$

corresponds to the integer-order radial polynomials, which are defined as follows [28]:

$$T_p(r) = \begin{cases} \frac{1}{\sqrt{2}}, & p = 0, \\ \cos(\pi p r^2), & p \text{ is even}, \\ \sin(\pi(p+1)r^2), & p \text{ is odd}. \end{cases} \quad (2)$$

$T_p(r)$ is orthogonal over the interval of $0 \leq r \leq 1$:

$$\int_0^1 T_p(r) T_o(r) r dr = \frac{1}{4} \delta_{po}, \quad (3)$$

while $e^{-iq\theta}$ is orthogonal in the range $0 \leq \theta \leq 2\pi$:

$$\int_0^{2\pi} e^{-iq\theta} e^{-il\theta} d\theta = 2\pi \delta_{ql}, \quad (4)$$

where δ denotes the Kronecker function.

The basis function $W_{pq}(r, \theta)$, defined by the radial polynomials and angular Fourier term, is orthogonal over the unit circle and satisfies:

$$\int_0^{2\pi} \int_0^1 W_{pq}(r, \theta) [W_{kl}(r, \theta)]^* r dr d\theta = \frac{\pi}{2} \delta_{pk} \delta_{ql}, \quad (5)$$

where $[W_{kl}(r, \theta)]^*$ denotes the conjugate of $W_{kl}(r, \theta)$.

An approximate reconstruction of the image $f(r, \theta)$ using a finite set of moments is given by:

$$\begin{aligned} f(r, \theta) &= \sum_{p=0}^{\infty} \sum_{q=-\infty}^{\infty} F_{pq} W_{pq}(r, \theta) \approx \sum_{p=0}^{\max} \sum_{q=-\max}^{\max} F_{pq} W_{pq}(r, \theta) \\ &= \sum_{p=0}^{\max} \sum_{q=-\max}^{\max} F_{pq} T_p(r) e^{iq\theta}. \end{aligned} \quad (6)$$

3.2. FrPHFMs

For an image $f(r, \theta)$, the FrPHFMs characterized by $p(p \geq 0)$ and a repetition of $q(|q| \geq 0)$ are examples of fractional continuous orthogonal moments that exhibit superior performance and strong global feature description ability, which are defined in a polar coordinate system [58] as:

$$F_{pq}^{(t)} = \frac{2}{\pi} \int_0^{2\pi} \int_0^1 f(r, \theta) [W_{pq}^{(t)}(r, \theta)]^* r dr d\theta = \frac{2}{\pi} \int_0^{2\pi} \int_0^1 f(r, \theta) T_p^{(t)}(r) e^{-iq\theta} r dr d\theta, \quad (7)$$

where $F_{pq}^{(t)}$ represents the FrPHFMs and $T_p^{(t)}(r)$ represents the fractional-order radial polynomials.

$T_p^{(t)}(r)$ of FrPHFMs is as follows [58]:

$$T_p^{(t)}(r) = \begin{cases} \frac{1}{\sqrt{2}}, & p = 0, \\ \sqrt{t}r^{t-1} \cos(\pi np), & p \text{ is even}, \\ \sqrt{t}r^{t-1} \sin(\pi(p+1)r^{2t}), & p \text{ is odd}, \end{cases} \quad (8)$$

where the parameter $t > 0$ represents the fractional order, and the basis function for the FrPHFMs is:

$$W_{pq}^{(t)}(r, \theta) = T_p^{(t)}(r)e^{iq\theta}. \quad (9)$$

Notably, defined over the domain $0 \leq r \leq 1$, the function $T_p^{(t)}(r)$ adheres to the orthogonal relationship:

$$\int_0^1 T_p^{(t)}(r)T_o^{(t)}(r)rdr = \frac{1}{4}\delta_{po}. \quad (10)$$

Owing to the properties of the radial polynomials and the angular Fourier factor, the basis function $W_{pq}^{(t)}(r, \theta)$ is orthogonal within the unit circle and satisfies the condition given below:

$$\int_0^{2\pi} \int_0^1 W_{pq}^{(t)}(r, \theta) [W_{kl}^{(t)}(r, \theta)]^* r dr d\theta = \frac{\pi}{2} \delta_{pk} \delta_{ql}, \quad (11)$$

where $[W_{kl}(r, \theta)]^*$ denotes the conjugate of $W_{kl}(r, \theta)$.

By considering FrPHFMs up to moment order $pmax$ and repetition $qmax$, the original image can be approximately reconstructed as shown below:

$$\begin{aligned} f(r, \theta) &= \sum_{p=0}^{\infty} \sum_{q=-\infty}^{\infty} F_{pq}^{(t)} W_{nm}^{(t)}(r, \theta) \approx \sum_{p=0}^{max} \sum_{q=-max}^{max} F_{pq}^{(t)} W_{pq}^{(t)}(r, \theta) \\ &= \sum_{p=0}^{max} \sum_{q=-max}^{max} F_{pq}^{(t)} T_p^{(t)}(r) e^{iq\theta}. \end{aligned} \quad (12)$$

3.3. Geometric invariance of FrPHFMs

FrPHFMs possess inherent geometric invariance properties that make them highly suitable for robust image analysis and zero-watermarking applications. These invariance characteristics stem from their orthogonal radial basis functions, which enables flexible representation of image structures.

3.3.1. Invariance to rotation

Consider an original image $f(r, \theta)$ that is rotated by an angle φ to produce $f'(r, \theta)$. Let the FrPHFMs of $f(r, \theta)$ and $f'(r, \theta)$, calculated via Eq (7), be $F_{pq}^{(t)}(f)$ and $F_{pq}^{(t)}(f')$, respectively.

These satisfy the following relationship: $F_{pq}^{(t)}(f') = F_{pq}^{(t)}(f)e^{-iq\varphi}$. Taking the magnitude of both sides yields $|F_{pq}^{(t)}(f')| = |F_{pq}^{(t)}(f)|$, demonstrating that the amplitude of FrPHFMs remains unchanged

under rotation, thereby confirming their rotation invariance.

3.3.2. Invariance to scaling

For FrPHFM computation, it is necessary to map the image onto the unit circle, allowing $f(r, \theta)$ to be normalized accordingly. By normalizing the image plane, FrPHFMs achieve scale invariance. This normalization process eliminates the dependency of the moments on the absolute size of the image, enabling consistent moment values for geometrically scaled versions of the same image, after normalization, the scaled image represents the same image function, which ensures that FrPHFMs are scale-invariant.

3.3.3. Invariance to length-width ratio changing

The change in length-width ratio (LWR) can be regarded as a generalized form of image scaling. To counter the effects of an LWR changing attack, an $M \times N$ rectangular image is first rescaled to a square of size $(M + N)/2 \times (M + N)/2$ before computing its FrPHFMs. Owing to the inherent scaling invariance of FrPHFMs, the moments derived from this process also exhibit invariance to LWR changes.

3.3.4. Invariance to cropping

The algorithm calculates FrPHFMs through inscribed circle mapping [58], ensuring that cropping the four corners of an image by a ratio smaller than $(2 - \sqrt{2})/4$ does not affect the FrPHFMs, as the inscribed circle retains the original content. However, if the cropping ratio exceeds $(2 - \sqrt{2})/4$, the inscribed circle's content is altered, which affects the computation of FrPHFMs and compromises invariance. Therefore, FrPHFMs can resist cropping attacks conditionally, depending on the severity of the crop.

3.4. Chaotic map

When developing chaotic maps for cryptographic purposes, it is essential to maintain a balance between unpredictability, wide chaotic ranges, sensitivity to initial conditions, and computational efficiency. This section details the 1D-RSS chaotic map, designed to balance chaotic characteristics and range. Its representation is defined mathematically as [59]:

$$x_{n+1} = \frac{4\alpha}{\sin(\alpha x_n) + 2} - \frac{3\beta}{(\sin(\beta x_n) + 2)^2}. \quad (13)$$

The parameters α and β are real numbers that, when integrated with x_n in both sections of the equation, enhance the complexity and unpredictability of the system. Dynamical system analyses, including bifurcation diagrams and Lyapunov exponent evaluation were performed on the 1D-RSS to assess and verify its chaotic behavior. 1D-RSS demonstrates complex chaotic dynamics across extensive α and β ranges, with a chaotic region covering almost the entire real number domain,

outperforming maps with limited chaotic ranges.

Bifurcation analysis is a widely used method for examining the stability, periodicity, and chaotic behavior of dynamical systems by showing their long-term states as a function of control parameters. For clarity and fairness, we used the bifurcation diagrams of the 1D-RSS from [59]. Figure 1 presents three bifurcation plots of the 1D-RSS under different parameter settings. In the first plot, β is set to 1000 while α varies; in the second, α is fixed at 1000 and β is varied; and in the third, both parameters change simultaneously. Unlike many traditional 1D chaotic maps whose outputs remain within narrow intervals such as $[-1, 1]$, the 1D-RSS produces values across a much wider and parameter-dependent range, indicating a strong and extensive chaotic region.

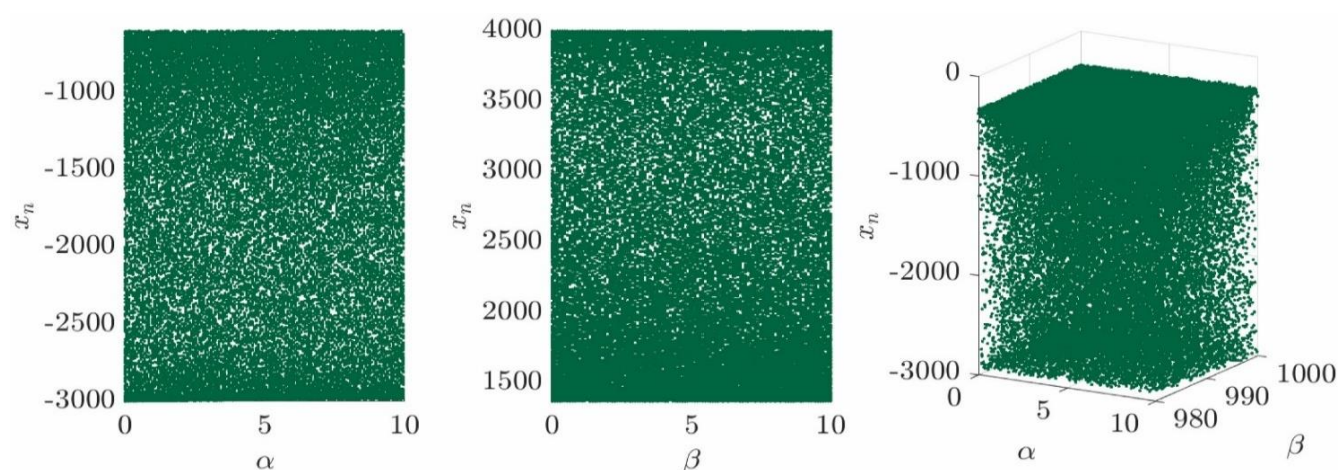


Figure 1. Bifurcation behavior plots for the 1D-RSS [59].

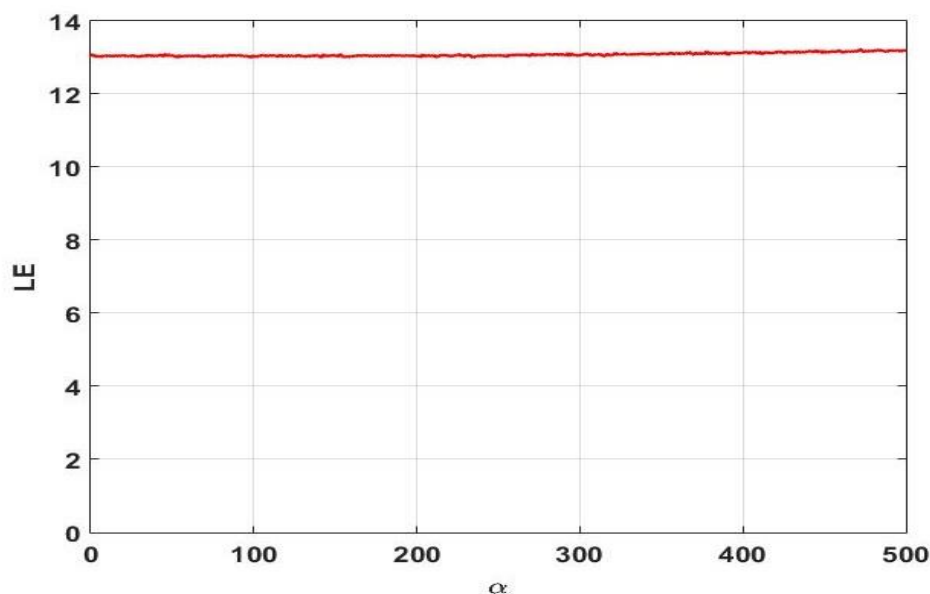


Figure 2. Comparison of Lyapunov exponents across varying α .

The Lyapunov exponent (LE) is a fundamental metric for characterizing chaos, quantifying

the rate at which trajectories diverge from close initial conditions. A positive LE confirms strong sensitivity and the presence of chaotic dynamics. The sensitivity of 1D-RSS was evaluated with $\beta = 1000$, as illustrated in Figure 2. The system consistently shows high positive Lyapunov exponent values up to 13 for all parameter settings, demonstrating persistent chaotic behavior.

4. Proposed zero-watermarking algorithm

The stability and accuracy of orthogonal moment coefficients are crucial for ensuring robust zero-watermarking. High-order moments of FrPHFM tend to suffer from numerical instability, lower accuracy, and greater sensitivity to noise, common image-processing, and geometric distortions. Therefore, the proposed method selects only low-order coefficients, which are known to be more stable and accurate. In addition, because some FrPHFM coefficients exhibit low accuracy, the algorithm selects coefficients from the precise set S to construct the zero-watermark, as described in Section 4.2. Consequently, low-order FrPHFM coefficients are therefore used to construct the feature image, enhancing the robustness of the algorithm. For convenience, denote the original medical image and watermark image sizes as $N \times N$ and $P \times Q$, respectively. Consider an original medical image represented as $F = \{f(i, j), 0 \leq i, j < N\}$, and a watermark image $L = \{l(i, j), 0 \leq i < P, 0 \leq j < Q\}$. The proposed method involves three key steps: encrypting the watermark image with a chaotic map, constructing the zero-watermark, and performing verification.

4.1. Watermark image encryption

To enhance security, the proposed algorithm employs the 1D-RSS [59] to chaotically encrypt the watermark image, as defined in Eq (13). Figure 3 presents a flowchart that illustrates the process for encrypting and decrypting a watermark image L of dimensions $P \times Q$, utilizing a private key, $K = (x_0, \alpha, \beta)$, consisting of the initial value of x_0 and the two parameters α, β from Eq (13). Only the encryption steps are presented here, as the decryption is simply the reverse of encryption. The complete encryption for the watermark image is described as follows.

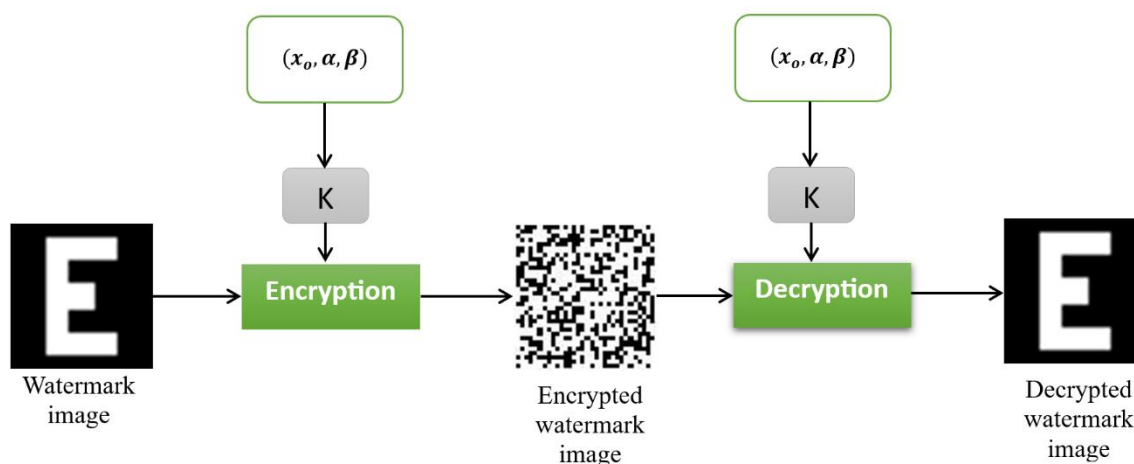


Figure 3. Process for encrypting and decrypting the watermark image.

Step 1: Chaotic sequence generation. The 1D-RSS map is initialized with the value K and iterated $P \times Q$ times to produce the chaotic sequence W_1 .

Step 2: Sorting the chaotic sequence. The $P \times Q$ sequence is organized in ascending order to produce the matrix $H_{P \times Q}$.

Step 3: Sequence binarization. The mean of all elements in $H_{P \times Q}$ is calculated and employed as a threshold to convert H into a binary matrix H' . Each value in the sequence is compared with the average, generating a binary chaotic sequence: coefficients greater than or equal to the mean are set to 1, and those below the mean are set to 0.

Step 4: XOR encryption. As XOR is reversible, it constitutes a crucial step in encryption. The watermark image L is XORed with H' to generate the encrypted watermark image L_C .

$$L_C = L \oplus H', \quad (14)$$

where \oplus represents the XOR operation.

4.2. Zero-watermarking generation

The stability and accuracy of FrPHFMs are vital to zero-watermarking robustness, as their precision in feature image construction directly impacts performance. Therefore, selecting precise coefficients is essential for reliable feature image construction. The following outlines the key steps of the proposed algorithm, and a flowchart depicting the zero-watermarking image construction approach is shown in Figure 4.

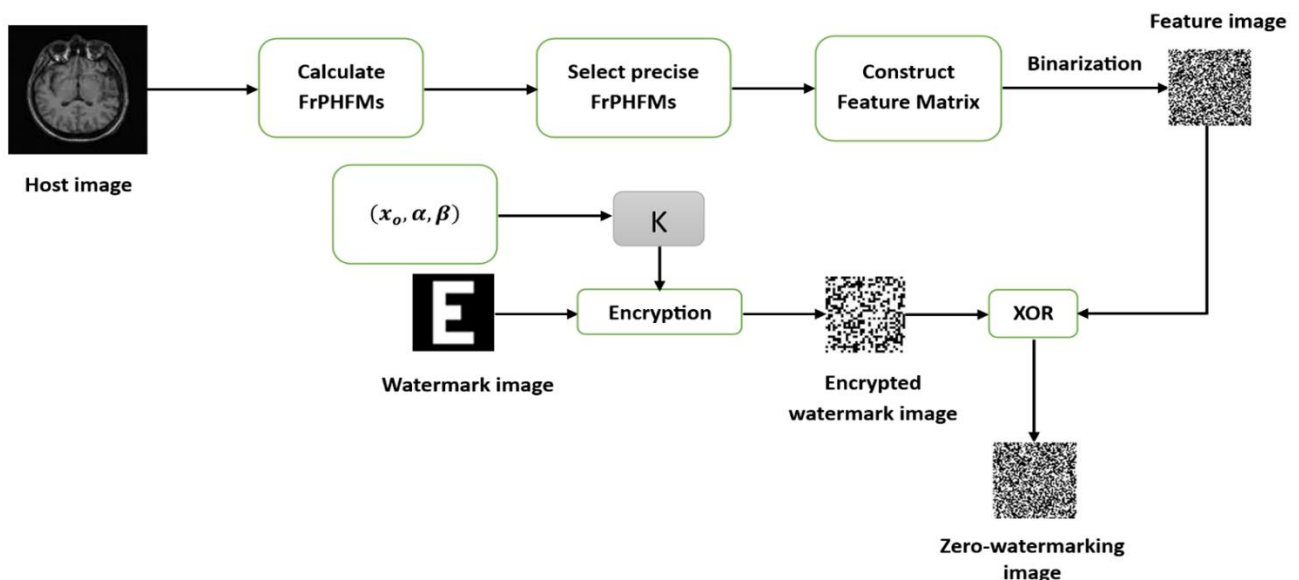


Figure 4. Zero-watermark generation.

Step 1: Calculation of FrPHFMs. For the original image F , FrPHFMs are calculated up to order p_{max} , resulting in $(p_{max} + 1)(2p_{max} + 1)$ moments.

Step 2: Selecting accurate coefficients for feature construction. To avoid inaccuracies in some FrPHFMs coefficients, only those belonging to the precise set $F_{pq}^{(t)}$ are used to build the zero-watermark. The precise coefficient set is given as follows:

$$S = \{F_{pq}^{(\alpha)}, q \neq 4i, i \in Z\}. \quad (15)$$

Step 3: Generating the amplitude sequence. The amplitudes of $(pmax + 1)(2pmax + 1)$ moments are repeatedly duplicated to build $P \times Q$ values, forming the amplitude sequence as:

$$A = \{a(i), 0 \leq i < P \times Q\}. \quad (16)$$

This sequence is then replicated as needed to generate the expanded amplitude sequence S of length $P \times Q$, matching the watermark size.

Step 4: Binary feature image construction. First, calculate the average A_{avg} of vector A and use it as the threshold for binarization. Map the sequence A to a $P \times Q$ feature image as:

$$B = \{b(i, j), 0 \leq i < P, 0 \leq j < Q\}, \quad (17)$$

then threshold B using A_{avg} to form the binary feature image as follows:

$$BF = \{bf(i, j), 0 \leq i < P, 0 \leq j < Q\}, \quad (18)$$

where

$$bf(i, j) = \begin{cases} 1, & \text{if } b(i, j) \geq A_{avg}, \\ 0, & \text{if } b(i, j) < A_{avg}. \end{cases} \quad (19)$$

Step 5: Watermark image encryption. The pre-processing method described in Section 4.1 is applied to encrypt the original watermark image, producing the encrypted watermark image L_C and thereby enhancing the overall security of the watermark.

Step 6: Zero-watermark image generation. For ease of operation, the 2D binary feature image BF and the encrypted watermark L_C are fused through an XOR operation, resulting in the generation of the binary zero-watermark ZW , which is the same size as the watermark and is defined as:

$$ZW = BF \oplus L_C. \quad (20)$$

The generated image ZW serves as the zero-watermark, verifying the copyright of the medical image and being securely stored within the intellectual property rights (IPR) database of a trusted third-party authority.

4.3. Verification of zero-watermarking

Similar to the construction stage in Figure 2, the flowchart outlines the verification procedure for the proposed approach, with the specific procedure outlined below as shown in Figure 5.

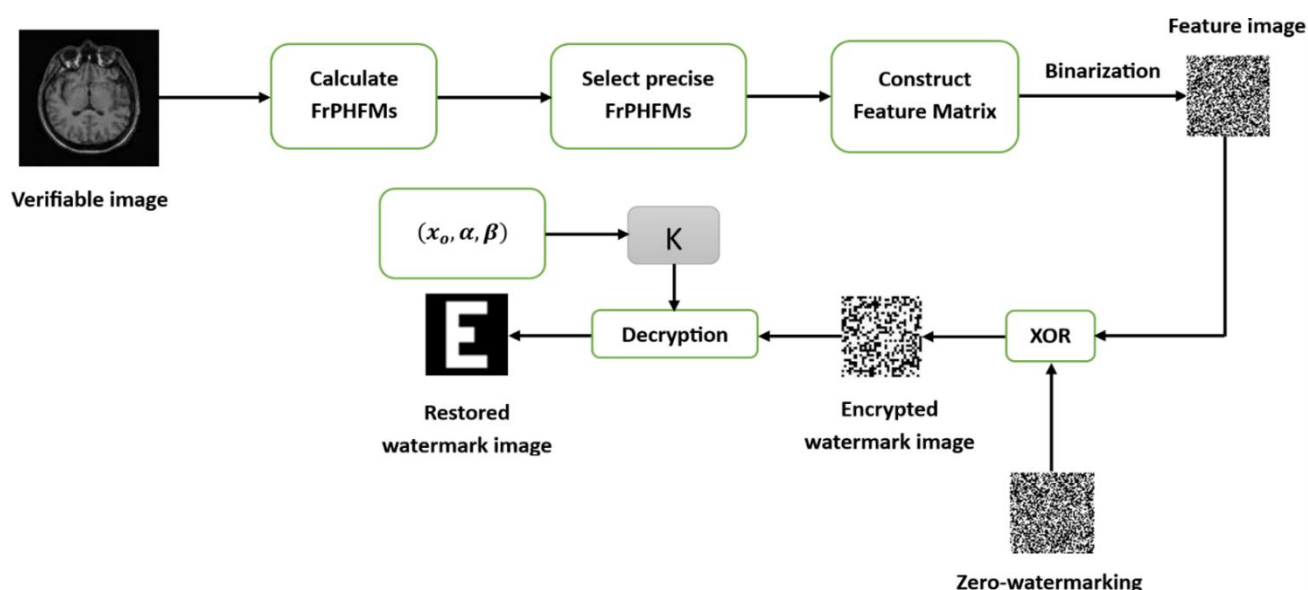


Figure 5. Zero-watermark verification.

Step 1: Feature image construction. The feature image BF' is obtained by performing steps 1–4 as specified in Section 4.2.

Step 2: Restore the encrypted watermark. Obtain the image ZW and generate an undecrypted watermark image L_C' with the help of Eq (21).

$$L_C' = BF' \oplus ZW. \quad (21)$$

Step 3: Retrieve the watermark image. Apply the 1D-RSS chaotic map with initial value K to chaotically decrypt L_C' , resulting in the decrypted watermark image L' . By comparing L' with the original watermark L , the authenticity of the image under verification can be confirmed.

5. Experimental results and analysis

This section provides a detailed evaluation of the proposed algorithm through various experiments, including details of the experimental setup, performance metrics, security analysis, robustness against potential attacks, and comparison with existing algorithms [18–20,24,39,49,57].

5.1. Experimental setup

All simulations to evaluate the proposed algorithm were performed using MATLAB (R2018b) on a laptop featuring a 1.9 GHz Intel Core™ i7 CPU, 8 GB RAM, and Windows 11. Figure 6 shows ten 512×512 CT, MRI, and X-ray medical image samples chosen from different datasets, while Figure 7 presents the 32×32 binary watermark image employed in the experiments.

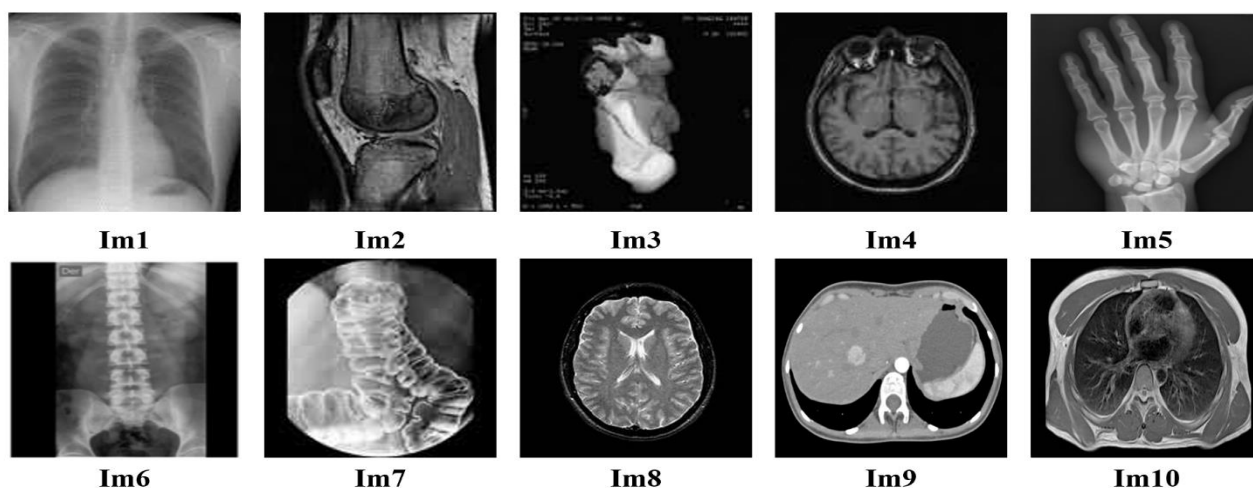


Figure 6. Sample medical images.

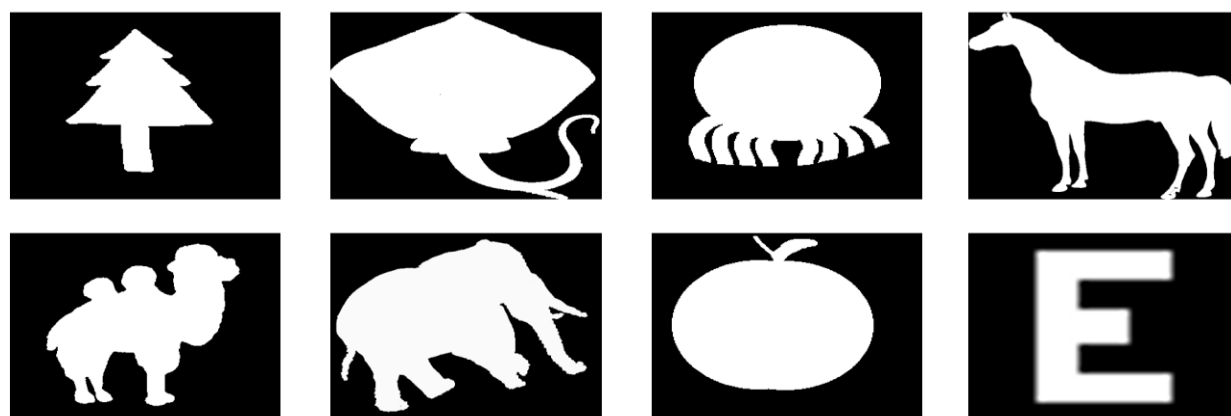


Figure 7. Examples of watermarks.

5.2. Influence of the fractional order on the stability of FrPHFM moments

We conducted an experiment to evaluate the numerical sensitivity of the fractional order of FrPHFMs, as it directly influences the stability and robustness of the watermarking system. In the experiment, ten medical images were resized to 256×256 , the maximum moment order was set to 10, and the fractional parameter t was varied from 0.1 to 1.0. For each value of t , the FrPHFM coefficients were computed for all original images and their corresponding attacked versions, including scaling ($1.5\times$), rotation (15°), cropping (30%), JPEG compression ($Q = 70$), Gaussian noise (0.03), and salt-and-pepper noise (0.03). The average mean squared error (MSE) between the FrPHFM coefficients of the original and attacked images was then calculated across all fractional orders to evaluate the sensitivity of the moments to variations in t . A higher MSE indicates lower numerical stability, whereas a lower MSE (approaching zero) indicates increased stability. As shown in Figure 8, the MSE reaches its minimum at $t = 0.6$, indicating that the fractional order plays a crucial role in the stability and robustness of the FrPHFM. The consistently lowest average MSE observed at $t = 0.6$ across all attacks confirms that this value is the optimal fractional order for generating stable and

reliable FrPHFM coefficients. Therefore, $t = 0.6$ is adopted in all subsequent experiments to assess the robustness of the proposed zero-watermarking algorithm.

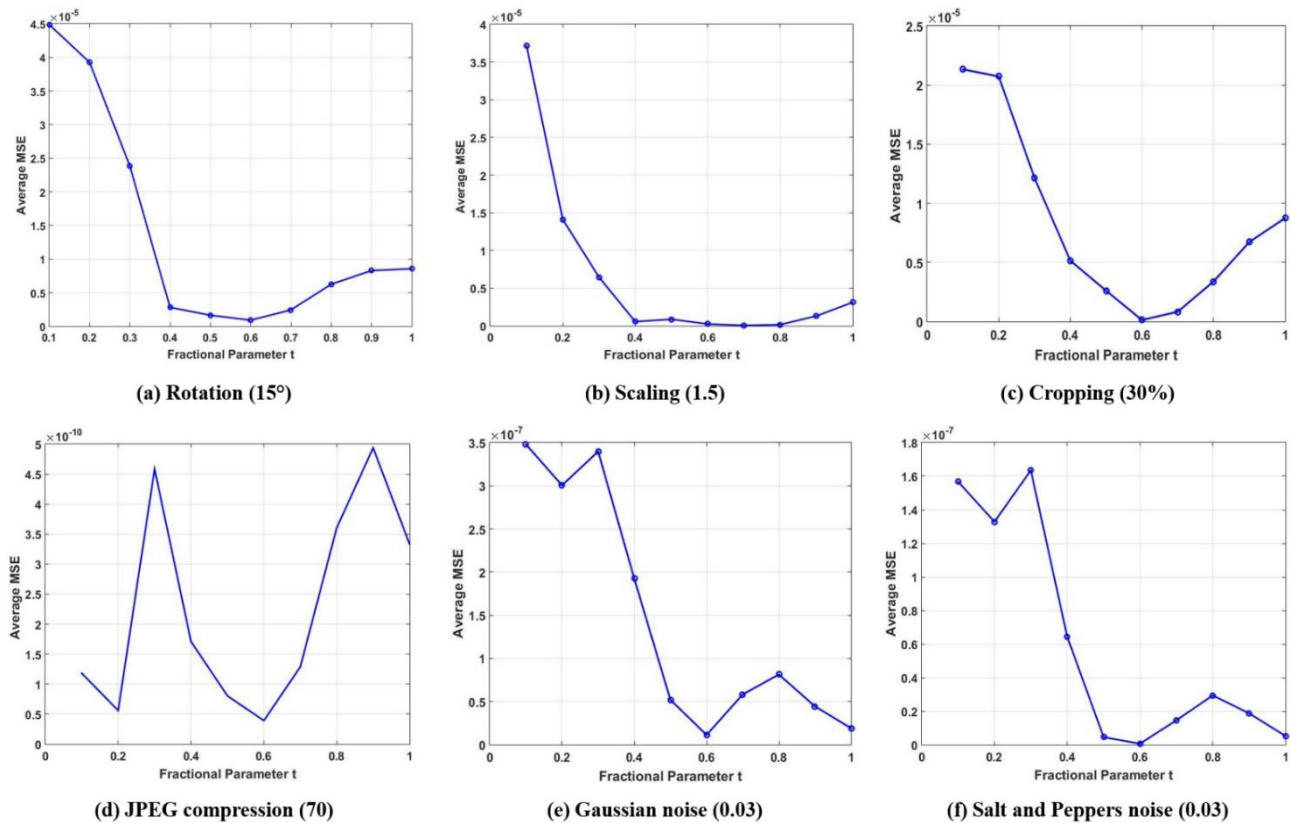


Figure 8. Influence of the fractional order on the stability of FrPHFM coefficients.

5.3. Evaluation metrics

Robustness: To objectively assess the performance and robustness of the algorithm against attacks, this study employs the NC and BER metrics. The metrics assess how closely the extracted watermark matches the original, with values between 0 and 1. NC values approaching 1 and BER values near 0 demonstrate strong similarity and confirm the algorithm's robustness. NC is computed as follows:

$$NC = \frac{\sum_{i=1}^m \sum_{j=1}^n [L(i,j) \times L^*(i,j)]}{\sum_{i=1}^m \sum_{j=1}^n [L(i,j)]^2}, \quad (22)$$

where L and L^* refer to extracted and original watermarks, of size $m \times n$, respectively. A higher NC value indicates greater robustness of the algorithm. The BER metric reflects the ratio of differing bits between the recovered and original watermark images. The BER can be calculated as follows:

$$BER(L, L^*) = \frac{1}{m \times n} \sum_{u=1}^m \sum_{v=1}^n [L(u,v) \oplus L^*(u,v)]. \quad (23)$$

Invisibility: The degree of image distortion resulting from an attack is assessed using the peak signal-to-noise ratio (PSNR), which is defined as follows:

$$PSNR = 10 \times \log_{10} \left(\frac{255^2}{MSE} \right), \quad (24)$$

$$MSE = \frac{1}{M \times N} \left(\sum_{i=1}^M \sum_{j=1}^N [f(i, j) - f'(i, j)]^2 \right), \quad (25)$$

where the original and attacked images, $f(i, j)$ and $f'(i, j)$, respectively, have dimensions $M \times N$. PSNR decreases as the distortion increases, and higher PSNR values correspond to lower distortion in the cover image.

5.4. Analysis of robustness

Table 1. NC and mean NC values for ten medical images under no attack and various types of attacks.

Attacks & Images	Im1	Im2	Im3	Im4	Im5	Im6	Im7	Im8	Im9	Im10	MeanNC
No Attack	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
JPEG 20	0.9946	0.9964	0.9952	0.9946	0.9969	0.9959	0.9965	0.9958	0.9947	0.9950	0.9956
JPEG 80	0.9982	1.0	0.9982	0.9990	0.9986	1.0	0.9988	0.9985	0.9990	0.9985	0.9989
Gaussian noise 0.01	1.0	0.9982	0.9990	0.9987	0.9990	1.0	1.0	0.9988	1.0	0.9980	0.9992
Salt-and-pepper noise 0.01	1.0	0.9990	1.0	0.9990	1.0	1.0	1.0	0.9990	1.0	0.9995	0.9996
Median filtering 3x3	0.9910	0.9920	0.9925	0.9915	0.9908	0.9910	0.9915	0.9922	0.9925	0.9915	0.9917
Average filtering 3x3	0.9946	0.9946	0.9959	0.9938	0.9940	0.9942	0.9945	0.9943	0.9945	0.9950	0.9945
Gaussian filtering 3x3	0.9964	0.9970	0.9968	0.9959	0.9975	0.9960	0.9965	0.9974	0.9970	0.9967	0.9962
Rotation 15	0.9982	0.9988	0.9978	0.9990	0.9982	0.9990	0.9985	0.9979	0.9984	0.9978	0.9984
Rotation 35	0.9946	0.9975	0.9959	0.9975	0.9965	0.9959	0.9965	0.9954	0.9948	0.9972	0.9962
Scaling 0.75	0.9982	0.9990	0.9985	0.9978	0.9990	0.9986	0.9984	0.9975	0.9988	0.9984	0.9984
Scaling 1.75	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
Length-width ratio (1.0,0.75)	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
Length-width ratio (0.5,1.25)	1.0	0.9982	0.9990	1.0	0.9990	0.9985	1.0	1.0	0.9990	1.0	0.9994
Cropping (20%)	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
Cropping (60%)	0.9946	0.9959	0.9965	0.9959	0.9945	0.9975	0.9970	0.9956	0.9948	0.9960	0.9958

This section assesses the robustness of the proposed algorithm toward various types of attacks, classified into conventional and geometric categories. To validate its performance, experiments are conducted using six medical images. The results, summarized in Table 1, include the NC values for each image under different attack scenarios, with the last column presenting the mean NC value across

all six images. The recovered watermarks exhibit mean NC values of 1 in the absence of attacks, indicating perfect extraction of the watermark information. Moreover, Table 1 demonstrates that the extracted watermarks maintain mean NC values above 0.99 even under multiple attacks, including noise, filtering, JPEG compression, and geometric operations like rotation, scaling (0.75), length–width ratio adjustments (0.5, 1.25), and 60% cropping. Notably, for certain geometric attacks such as scaling (1.75), length-width ratio (1.0, 0.75), and cropping (20%), the mean NC values remain at 1.0. Results reveal that the suggested approach is resilient to most conventional attacks, achieving high robustness and superior effectiveness, notably against geometric distortions.

The following subsections provide a detailed analysis illustrating the robustness and benefits of the suggested algorithm toward JPEG compression, noise, filtering, geometric, and combined attacks.









5.4.1. Conventional attacks

The primary goal of this subsection is to assess the ability of the suggested algorithm during conventional attacks through a series of experiments. A set of standard manipulations was applied to the original medical images, including common distortions such as JPEG compression, Gaussian noise addition, salt-and-pepper noise, Gaussian filtering, average filtering, and median filtering.

• Experiment on a JPEG compression attack

JPEG compression is a frequently employed technique for medical images transmitted over the Internet to reduce network load and improve transmission efficiency. However, as a lossy compression method, it inevitably causes some degradation in image quality. A common issue with JPEG compression is that it can alter certain image pixels, leading to artifacts or a reduction in overall image quality.

Table 2. The results after JPEG compression.

Attack	JPEG			
	30	50	70	90
Attacked image				
Detected Watermark				
PSNR	43.21 dB	46.09dB	48.56dB	52.98dB
BER	0.0020	9.7656e-04	0	0
NC	0.9964	0.9982	1	1


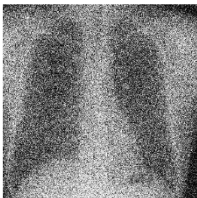

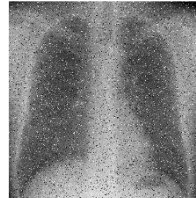




Accordingly, the JPEG compression attack is applied to the medical image at quality factors (QFs) of 30, 50, 70, and 90. Table 2 shows the PSNR results, the extracted watermarks, and their NC and BER metrics. From Table 2, it can be observed that the extracted watermarks closely resemble the original watermarks, with consistently high NC values and low BER values indicating strong

performance. After the images undergo JPEG compression, the NC values of the extracted watermarks remain above 0.99 at QF 30 and 50, and are equal to 1.0 at QF 70 and 90. Correspondingly, the BER values are near zero at QF 30 and 50, and exactly zero at QF 70 and 90, demonstrating the algorithm's strong robustness against JPEG compression.

• Experiment on noise attacks

Due to network transmission, medical images are susceptible to noise, resulting in unavoidable distortions. Noise attacks are simulated by introducing Gaussian noise and salt-and-pepper noise at varying intensities to the original medical image. The experiment assesses the robustness of the proposed algorithm under these noise attacks. Table 3 summarizes the PSNR values, the attacked medical images, the recovered watermark images, and their associated NC and BER metrics. As shown in Table 3, under salt-and-pepper noise (0.1) and Gaussian noise (0.1) attacks, the medical images become blurred. Despite the presence of speckles in the extracted watermarks, they remain clearly identifiable and do not affect practical interpretation. From Table 3, all NC values are above 0.99, and the BER values are near 0. Although PSNR values decline with increasing attack strength, resulting in significant image degradation at a noise level of 0.1, the algorithm remains highly robust. These findings demonstrate the suitability of the proposed algorithm for high-noise environments, providing a strong experimental foundation for safeguarding medical images. This resilience is likely due to the superior denoising performance of FrPHFMs.






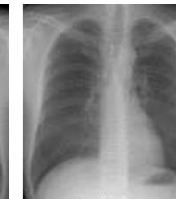






Table 3. The results after common different noise attacks.

Attack	Gaussian noise 0.05	Gaussian noise 0.1	Salt & peppers noise 0.05	Salt & peppers noise 0.1
Attacked Image				
Detected Watermark				
PSNR	18.63dB	15.61dB	13.53dB	11.24dB
BER	0.0029	0.0039	0.0010	0.0020
NC	0.9946	0.9927	0.9982	0.9964

• Experiment on filtering attacks

Filtering is commonly employed to reduce image noise and improve visual quality. In this experiment, median, average, and Gaussian filters with various window sizes were applied to the medical images. Table 4 summarizes the experimental results obtained under these filtering attacks. As observed, all NC values exceed 0.99, while BER values remain close to 0 under filtering attacks with the two tested window sizes. Even as the filter sizes increase, the watermark images can be completely extracted, highlighting the robustness of the suggested algorithm against different filtering attacks and confirming its strong anti-filtering capability.

Table 4. The results after common filter attacks.




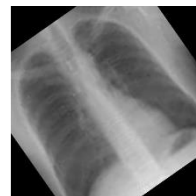
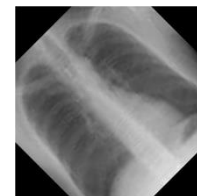





Attack	Median filtering		Average filtering		Gaussian filtering	
	3×3	5×5	33×	5×5	3×3	5×5
Attacked Image						
Detected Watermark						
PSNR	53.40dB	48.18-dB	54.47-dB	49.91-dB	72.63 dB	72.08-dB
BER	0.0049	0.0059	0.0029	0.0049	0.0020	0.0039
NC	0.9910	0.9892	0.9946	0.9910	0.9964	0.9928

5.4.2. Geometric attacks

Geometric distortions continue to be a critical issue in the field of image watermarking. Geometric transformations, such as rotation, scaling, and changes in the length-to-width ratio, may alter the image's structure, leading to information loss and severe degradation of the extracted watermark. If the attacked image cannot be properly aligned with the original, it may result in incomplete extraction of the watermark information. Accordingly, this section assesses the robustness of the proposed algorithm through experiments involving geometric attacks, including cropping, rotation, scaling, and changes in aspect ratio at various scales.

- **Experiment on rotation attacks**

Table 5. The results after a rotation attack.











Attack	Rotation				
	5	15	25	35	45
Attacked Image					
Detected Watermark					
PSNR	19.11dB	14.16 dB	12.36 dB	11.42dB	10.97dB
BER	0	9.7656e-04	0.0020	0.0029	0.0039
NC	1	0.9982	0.9964	0.9946	0.9928

Rotating an image slightly may result in distortions, and algorithms for feature extraction and verification can be easily affected as the global pixel structure is altered. A series of rotation attacks at 5° , 15° , 25° , 35° , and 45° was applied to the medical images. Table 5 presents the results corresponding to the images after rotation attacks. As observed, the NC value consistently remains above 0.99 and the BER below 0.0040; even under various rotation attacks, the proposed algorithm can still fully extract the watermarks. The extracted watermark image demonstrates high values of NC and low values of BER. This can be attributed to the rotational invariance of the feature matrix constructed using FrRHFMs, which enhances robustness against rotation attacks, as reflected by BER values near 0 and NC values close to 1. The experimental findings indicate that the proposed method is highly robust against rotation attacks.

- **Experiment on scaling attacks**

Image scaling can have a significant impact on image quality, as it often results in the loss of many pixels, which in turn affects accurate watermark extraction. We perform a scaling attack test with scaling factors 0.5, 0.75, 1.25, and 1.5 on medical images. Table 6 presents the results for images subjected to scaling attacks. As shown in Table 6, following various scaling attacks, the BER remains close to 0 while the NC exceeds 0.99. For scaling factors of 1.25 and 1.5, the BER is 0 and the NC remains at 1.0, demonstrating that the proposed algorithm can completely withstand scaling attacks. This is likely due to the high robustness and scaling invariance of FrPHFMs, which significantly enhances resistance to scaling attacks. It is to be noted that after scaling, since the dimensions of the attacked images differ from those of the original images, PSNR values cannot be calculated. Accordingly, PSNR is represented by ‘–’ in Table 6.

Table 6. The results after the scaling attack.











Attack	Scaling				
	0.25	0.5	0.75	1.25	1.5
Attacked Image					
Detected Watermark					
PSNR	--	--	--	--	--
BER	0.0039	0.0020	9.7656e-04	0	0
NC	0.9928	0.9964	0.9982	1	1

- **Experiment on cropping attacks**

Cropping an image may lead to the removal of important content. In this attack, specific regions of the medical image were deliberately removed to simulate partial data loss, which is a common threat in practical scenarios. In this experiment, we conduct a cropping attack test on medical images, as

listed in Table 7. A set of medical images was subjected to cropping, ranging from 10% to 50% of the upper-left image content being removed. Table 7 summarizes the NC and BER results obtained under different cropping ratios. From Table 7, as the cropping area increases and more image parts are lost, the extracted watermarks remain completely identifiable. Most NC values are 1.0 and BER values are 0, indicating that the proposed method can effectively resist cropping attacks, even with partial image removal.

Table 7. The results after the cropping attack.

Attack	Cropping				
	CR-1/4 (10%)	CR-1/8 (20%)	CR-1/16 (30%)	CR-1/32 (40%)	CR-1/64 (50%)
Attacked Image					
Detected Watermark					
PSNR	24.62dB	20.09 dB	15.95 dB	13.05	11.45
BER	0	0	0	9.7656e-04	0.0020
NC	1	1	1	0.9982	0.9964

This resilience is attributed to the fact that the watermark is not embedded in the image itself but is rather derived from robust features extracted through FrPHFMs, ensuring minimal distortion even under severe attacks. This may be attributed to the stability of the feature matrices constructed using FrPHFMs, which undergo minimal changes under attacks, thereby enhancing robustness against cropping.

The results demonstrate that the proposed method remains reliable even when large portions of the image are missing, which is vital for medical image authentication where integrity must be verifiable despite partial transmission losses or storage damage.











• Experiment on LWR changing attacks

The ability to resist LWR changes is particularly crucial for medical applications, where diagnostic images may be reformatted or rescaled without awareness of embedded security mechanisms. LWR changes can be treated as a generalized scaling operation on the image. We perform an LWR changing attack test on medical images, as listed in Table 8. The parameters for the LWR-changing attack included (0.25, 1.0), (0.5, 1.0), (0.75, 1.0), (1.0, 0.5), and (1.0, 1.5), representing vertical and horizontal scaling factors, respectively.

As shown in Table 8, following various LWR-changing attacks, the BER remains close to 0 and the NC of the extracted watermarks stays above 0.99. For three out of the five tested ratios, the BER is 0 and the NC is consistently 1.0, demonstrating that the proposed algorithm effectively resists LWR-changing attacks, ensuring reliable watermark recovery even under aspect ratio variations. It may be

because of the high robustness and LWR invariance of FrPHFMs, which greatly improves the robustness of LWR attacks. The experiment confirms that the method effectively safeguards watermark integrity under such transformations.

Table 8. The results after the LWR changing attack.

Attack	LWR				
	(0.25, 1.0)	(0.75, 1.0)	(1.25, 1.0)	(1.0, 0.5)	(1.0, 1.5)
Attacked Image					
Detected Watermark					
PSNR	--	--	--	--	--
BER	0.0020	0	0	9.7656e-04	0
NC	0.9964	1	1	0.9982	1

5.4.3. Combined attacks

Medical images are highly susceptible to various attacks while being transmitted, creating a significant challenge. Moreover, most zero-algorithms are evaluated against only a single type of attack, while the impact of combined attacks is often ignored. We conducted experiments on medical images subjected to various combinations of conventional and geometric attacks to assess the robustness of the proposed algorithm against combined attacks. From Table 9, it is evident that the recovered watermarks maintain NC values above 0.99 under multiple distortions, highlighting the proposed method's effectiveness in resisting complex combination attacks.

Table 9. NC and the mean NC results of the example images under combined attacks.

Attacks & Images	Im1	Im2	Im3	Im4	Im5	Im6	Im7	Im8	Im9	Im10	MeanN C
JPEG 80+ Scaling 1.75	1.0	1.0	1.0	0.9982	1.0	0.9982	1.0	0.9985	0.9985	0.9990	0.9992
Gaussian noise (0.02)+ Gaussian filtering 3×3	0.9928	0.9946	0.9928	0.9932	0.9946	0.9928	0.9947	0.9945	0.9928	0.9930	0.9936
Salt-and-pepper noise (0.02)+ Average filtering 3x3	0.9954	0.9956	0.9958	0.9946	0.9946	0.9956	0.9955	0.9950	0.9956	0.9946	0.9952
Rotation 15+Median filtering 3×3	0.9915	0.9910	0.9915	0.9920	0.9910	0.9915	0.9915	0.9925	0.9920	0.9920	0.9916
JPEG 80+ Rotation 35	0.9932	0.9946	0.9932	0.9942	0.9935	0.9932	0.9935	0.9940	0.9946	0.9935	0.9938
Cropping (1/8)+Scaling 1.5	1.0	1.0	0.9982	0.9982	1.0	0.9982	0.9985	1.0	0.9989	0.9982	0.9990
Cropping (1/8)+ Rotation 45	0.9946	0.9942	0.9928	0.9935	0.9935	0.9928	0.9930	0.9935	0.9928	0.9940	0.9935
Gaussian noise (0.02)+Length-width ratio (1.0,1.5)	0.9982	1.0	1.0	0.9982	1.0	1.0	0.9980	0.9985	0.9980	0.9982	0.9989
Length-width ratio (1.0,1.5)+ Median filtering 3×3	0.9910	0.9910	0.9920	0.9920	0.9915	0.9910	0.9922	0.9910	0.9915	0.9915	0.9915
Salt and peppers noise (0.02)+ Cropping (1/8)	1.0	0.9982	1.0	1.0	0.9982	0.9982	0.9985	1.0	0.9984	0.9982	0.9990

5.4.4. Comparison with the latest algorithms

For a comprehensive performance assessment, the suggested algorithm was compared with several recent zero-watermarking techniques [18-20, 24, 39, 49, 57]. For a fair comparison, the experiment was conducted using test medical images of size 512×512 and a watermark image of size 32×32 . The experimental results evaluating resistance to various attacks are summarized in Table 10, which compares the NC values of the proposed algorithm with those of existing approaches on medical images under different attack conditions. As reported in Table 10, the proposed method consistently achieves higher NC values compared to existing algorithms when medical images are subjected to various attack scenarios, demonstrating its superior performance and robustness, and confirming its effectiveness for practical medical image protection. Moreover, the experimental results indicate that the method remains highly effective even under severe distortions, further highlighting its reliability and robustness in zero-watermarking applications.

Table 10. NC experimental results comparison.

Attacks & Methods	[18]	[19]	[20]	[24]	[39]	[49]	[57]	Proposed
JPEG compression (QF = 10)	0.9990	0.982	0.974	0.981	0.9452	0.95	0.9995	0.9940
Median filtering (5×5)	0.999	0.991	0.988	0.992	0.9480	0.92	0.9950	0.9952
Salt & pepper noise (0.2)	0.9960	0.975	0.863	0.977	0.8680	0.85	0.9870	0.9968
Gaussian noise (0.2)	0.9970	0.984	0.943	0.982	0.8271	0.62	0.9852	0.9918
Scaling (2x)	1.000	0.998	0.996	1.000	0.9836	1.0	1.0	1.0
Rotation (15°)	0.987	0.964	0.965	0.922	0.9729	0.95	0.9950	0.9985
Cropping (Upper left 1/8)	0.985	0.974	0.987	0.955	0.9350	1.0	1.0	1.0

5.5. Computational complexity

Efficient execution is a critical requirement for zero-watermarking schemes applied to medical images, since these systems are often integrated into real-time clinical workflows or large-scale medical databases.

This section analyzes the time complexities of the suggested algorithm in comparison with other existing algorithms [18–20,24,39]. For the experiments, it was assumed that $M = N$ and $m = n$, where the cover image has dimensions $M \times N$ and the watermark image has dimensions $m \times n$. To ensure a fair evaluation of computational efficiency, the complexity of the suggested algorithm was derived and systematically compared with that of the existing algorithms. A summary of the time complexities for both the proposed and existing methods is presented in Table 11. The proposed algorithm consists of three steps: moments calculation, watermark image encryption, and zero-

watermarking generation. The core idea of the suggested algorithm is to leverage the FrPHFM for generating the feature image; therefore, the maximum computational cost of the proposed algorithm comes from the FrPHFM. Suppose $pmax$ order FrPHFM coefficients need to be calculated. Considering only multiplication, the complexity of directly computing the FrPHFM is $O((pmax + 1)(2pmax + 1) \times N^2)$ for an $N \times N$ image. Thus, the proposed zero-watermarking algorithm exhibits relatively low computational complexity, approximately $O((pmax + 1)(2pmax + 1) \times N^2) \cong O(pmax^2 \times N^2)$. Detailed calculations show that the complexity of each step can be estimated as $O((pmax + 1)(2pmax + 1) \times N^2)$, $O(n^2)$, and $O(n^2)$, respectively. Therefore, the overall computational complexity of the suggested method is roughly $O(pmax^2 \times N^2) + O(2 \times n^2)$, which can be approximated as $O(pmax^2 \times N^2)$.

Table 11. Time complexity comparison.

Algorithm	Time complexity
Algorithm [18]	$O\left(\frac{1025}{256} \times N^2\right) + O(2 \times n^2)$
Algorithm [19]	$O\left(\frac{1696}{256} \times N^2\right) + O(2 \times n^2)$
Algorithm [20]	$O\left(\frac{816}{256} \times N^2 + O(2 \times n^2)\right)$
Algorithm [24]	$O\left(\frac{2752}{256} \times N^2\right) + O(2 \times n^2)$
Algorithm [39]	$O(N^3)$
Proposed algorithm	$O(pmax^2 \times N^2)$

6. Conclusions

To protect medical images from information leakage and malicious tampering during transmission, this paper proposes a robust zero-watermarking framework based on fractional-order polar harmonic Fourier moments (FrPHFM) and chaotic mapping. FrPHFM extract rotation-, scaling-, and cropping-invariant features, ensuring strong resistance to geometric distortions. These features are then combined with a binary watermark using a one-dimensional chaotic encryption mechanism, which enhances both security and unpredictability. Experimental results demonstrate that the proposed method outperforms existing zero-watermarking schemes in robustness against common, geometric, and hybrid attacks. This approach provides a reliable solution for secure medical image transmission and copyright protection in digital healthcare. Future work will focus on extending the framework to color medical images, improving noise tolerance, optimizing computational efficiency, and integrating deep learning for more discriminative feature extraction.

Author contributions

Conceptualization, M. M. D.; methodology, M. M. D and M. A. B.; software, M. A. B. and M. M. D.; validation, A. A., M. A. B., and M. M. D.; formal analysis, A. A., M. A. B., and M. M. D.; investigation, A. A., M. A. B., and M. M. D.; resources, A. A., M. A. B., and M. M. D.; data curation, M. A. B. and M. M.D.; writing—original draft preparation, A.A., M.A.B., and M.M.D.; writing—review and editing, A.A., M.A.B., and M.M.D.; visualization, A.A., M.A.B., and M.M.D.; supervision, M.M.D.; project administration, M.M.D.; funding acquisition, A.A., M.A.B., and M.M.D. All authors have read and agreed to the published version of the manuscript.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

The authors extend their appreciation to the Deanship of Research and Graduate Studies at the University of Tabuk for funding this work through Research No. S-0264-2024.

Funding

This research was funded by the Deanship of Research and Graduate Studies at the University of Tabuk through Research No. S-0264-2024.

Conflict of interest

The authors declare that they have no conflicts of interest.

References

1. M. S. Moad, M. R. Kafi, A. Khaldi, A wavelet based medical image watermarking scheme for secure transmission in telemedicine applications, *Microprocess. Microsy.*, **90** (2022), 104490. <https://doi.org/10.1016/j.micpro.2022.104490>
2. A. F. Qasim, F. Meziane, R. Aspin, Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review, *Comp. Sci. Rev.*, **27** (2018), 45–60. <https://doi.org/10.1016/j.cosrev.2017.11.003>
3. S. P. Vaidya, Fingerprint-based robust medical image watermarking in hybrid transform, *Vis. Comput.*, **39** (2023), 2245–2260. <https://doi.org/10.1007/s00371-022-02406-4>
4. H. Shi, S. Zhou, M. Chen, M. Li, A novel zero-watermarking algorithm based on multi-feature and DNA encryption for medical images, *Multimed. Tools Appl.*, **82** (2023), 36507–36552. <https://doi.org/10.1007/s11042-023-15074-w>

5. M. M. Sayah, K. M. Redouane, K. Amine, Secure transmission and integrity verification for color medical images in telemedicine applications, *Multimed Tools Appl.*, **81** (2022), 43613–43638. <https://doi.org/10.1007/s11042-021-11791-2>
6. S. Gaur, V. Barthwal, An extensive analysis of digital image watermarking techniques, *Int. J. Intell. Syst. Appl. Eng.*, **12** (2023), 121–145.
7. S. Gull, S.A. Parah, Advances in medical image watermarking: a state of the art review, *Multimed Tools Appl.*, **83** (2024), 1407–1447. <https://doi.org/10.1007/s11042-023-15396-9>
8. Y. Shen, C. Tang, Z. Fan, T. Wu, Z. Lei, Blind watermarking scheme for medical and non-medical images copyright protection using the QZ algorithm, *Expert Syst. Appl.*, **241** (2024), 122547. <https://doi.org/10.1016/j.eswa.2023.122547>
9. O. P. Singh, K. N. Singh, A. K. Singh, A. K. Agrawal, H. Zhou, An improved robust algorithm for optimisation-based colour medical image watermarking, *Comput. Electr. Eng.*, **117** (2024), 109278. <https://doi.org/10.1016/j.compeleceng.2024.109278>
10. X. Zhang, Q. Su, Y. Sun, S. Chen, A robust and high-efficiency blind watermarking method for color images in the spatial domain, *Multimed. Tools Appl.*, **82** (2023), 27217–27243. <https://doi.org/10.1007/s11042-023-14479-x>
11. A. Soualmi A, L. Laouamer, A. Alti, A blind watermarking approach based on hybrid imperialistic competitive algorithm and SURF points for color images' authentication, *Biomed. Signal Proces.*, **84** (2023), 105007. <https://doi.org/10.1016/j.bspc.2023.105007>
12. K. M. Hosny, M. M. Darwish, Invariant image watermarking using accurate Polar harmonic transforms, *Comput. Electr. Eng.*, **62** (2017), 429–447. <https://doi.org/10.1016/j.compeleceng.2017.05.015>
13. C. Wang, Q. Zhang, X. Wang, L. Zhou, Q. Li, Z. Xia, et al., Light-field image multiple reversible robust watermarking against geometric attacks, *IEEE T. Depend. Secure*, **22** (2025), 5861–5875. <https://doi.org/10.1109/TDSC.2025.3576223>
14. K. Fares, A. Khaldi, K. Redouane, E. Salah, DCT & DWT based watermarking scheme for medical information security, *Biomed. Signal Proces.*, **66** (2021), 102403. <https://doi.org/10.1016/j.bspc.2020.102403>
15. F. Naz, A. Khan, M. Ahmed, M. I. Khan, S. Din, A. Ahmad, et al., Watermarking as a service (WaaS) with anonymity, *Multimed. Tools Appl.*, **79** (2020), 16051–16075. <https://doi.org/10.1007/s11042-018-7074-2>
16. A. Roček, M. Javorník, K. Slavíček, O. Dostál, Zero watermarking: Critical analysis of its role in current medical imaging, *J. Digit. Imaging*, **34** (2021), 204–211. <https://doi.org/10.1007/s10278-020-00396-0>
17. M. Magdy, N. I. Ghali, S. Ghoniemy, K. M. Hosny, Multiple zero-watermarking of medical images for internet of medical things, *IEEE Access*, **10** (2022), 38821–38831. <https://doi.org/10.1109/ACCESS.2022.3165813>
18. G. Yang, X. Lu, Y. Lu, X. Xiong, Robust zero-watermarking method for medical images based on FFST and Daisy descriptor, *J. Inf. Secur. Appl.*, **93** (2025), 104193. <https://doi.org/10.1016/j.jisa.2025.104193>
19. G. Yang, X. Lu, Y. Lu, J. Tang, X. Xiong, Robust zero-watermarking method for multiple medical images using wavelet fusion and DTCWT-QR, *J. Inf. Secur. Appl.*, **90** (2025), 104028. <https://doi.org/10.1016/j.jisa.2025.104028>

20. T. Huang, J. Xu, Y. Yang, B. Han, Robust zero-watermarking algorithm for medical images using double-tree complex wavelet transform and hessenberg decomposition, *Mathematics*, **10** (2022), 1154. <https://doi.org/10.3390/math10071154>
21. J. Yang, K. Hu, X. Wang, H. Wang, Q. Liu, Y. Mao, An efficient and robust zero watermarking algorithm, *Multimed. Tools Appl.*, **81** (2022), 20127–20145. <https://doi.org/10.1007/s11042-022-12115-8>
22. P. Meesala, D. M. Thounaojam, Integrating Fresnelet transform and spiking cortical model for robust medical image cryptosystem in zero-watermarking, *Comput. Electr. Eng.*, **118** (2024), 109371. <https://doi.org/10.1016/j.compeleceng.2024.109371>
23. Q. Wen, T. Sun, S. Wang, Concept and application of zero watermarking, *Acta Automat. Sinica*, **31** (2003), 214–216.
24. Y. Lu, X. Lu, G. Yang, X. Xiong, Robust zero-watermarking algorithm for multi-medical images based on FFST-Schur and Tent mapping, *Biomed. Signal Proces.*, **96** (2024), 106557. <https://doi.org/10.1016/j.bspc.2024.106557>
25. Y. Fang, J. Liu, J. Li, J. Chen, J. Hu, D. Yi, et al., Robust zero-watermarking algorithm for medical images based on SIFT and Bandelet-DCT, *Multimed. Tools Appl.*, **81** (2022), 16863–16879. <https://doi.org/10.1007/s11042-022-12592-x>
26. K. Hu, X. Wang, J. Hu, H. Wang, H. Qin, A novel robust zero-watermarking algorithm for medical images, *Vis. Comput.*, **37** (2021), 2841–2853. <https://doi.org/10.1007/s00371-021-02168-5>
27. M. A. Barakat, Comprehensive weighted newton inequalities for broad function classes via generalized proportional fractional operators, *Axioms*, **14** (2025), 234. <https://doi.org/10.3390/axioms14040234>
28. C. Wang, X. Wang, Y. Li, Z. Xia, C. Zhang, Quaternion polar harmonic Fourier moments for color images, *Inf. Sci.*, **450** (2018), 141–156. <https://doi.org/10.1016/j.ins.2018.03.038>
29. Z. Xia, X. Wang, M. Wang, S. Unar, C. Wang, Y. Liu, et al., Geometrically invariant color medical image null-watermarking based on precise quaternion polar harmonic Fourier moments, *IEEE Access*, **7** (2019), 122544–122560. <https://doi.org/10.1109/ACCESS.2019.2937985>
30. Y. Liu, C. Wang, M. Lu, J. Yang, J. Gui, S. Zhang, From simple to complex scenes: Learning robust feature representations for accurate human parsing, *IEEE T. Pattern Anal.*, **46** (2024), 5449–5462. <https://doi.org/10.1109/TPAMI.2024.3364951>
31. Z. Xia, X. Wang, C. Wang, C. Wang, B. Ma, Q. Li, et al., A robust zero-watermarking algorithm for lossless copyright protection of medical images, *Appl. Intell.*, **52** (2021), 1–15. <https://doi.org/10.1007/s10489-021-02324-x>
32. K. Hosny, M. Darwish, New geometrically invariant multiple zero-watermarking algorithm for color medical images, *Biomed. Signal Proces.*, **70** (2021), 103007. <https://doi.org/10.1016/j.bspc.2021.103007>
33. D. S. Khafaga, F. K. Karim, M. M. Darwish, K. M. Hosny, Robust zero-watermarking of color medical images using multi-channel Gaussian-Hermite moments and 1D Chebyshev chaotic map, *Sensors*, **22** (2022), 5612. <https://doi.org/10.3390/s22155612>
34. X. Wang, Y. Zhang, J. Tian, P. Niu, H. Yang, Accurate quaternion fractional-order pseudo-Jacobi-Fourier moments, *Pattern Anal. Appl.*, **25** (2022), 731–755. <https://doi.org/10.1007/s10044-022-01071-6>

35. Z. Xia, X. Wang, W. Zhou, R. Li, C. Wang, C. Zhang, Color medical image lossless watermarking using chaotic system and accurate quaternion polar harmonic transforms, *Signal Process.*, **157** (2019), 108–118. <https://doi.org/10.1016/j.sigpro.2018.11.011>
36. C. P. Wang, X. Y. Wang, X. J. Chen, C. Zhang, Robust zero watermarking algorithm based on polar complex exponential transform and logistic mapping, *Multimed. Tools Appl.*, **76** (2017), 26355–26376. <https://doi.org/10.1007/s11042-016-4182-1>
37. H. Wang, Y. Chen, T. Zhao, Modified Zernike moments and its application in geometrically resilient image zero-watermarking, *Circuits Syst. Signal Process.*, **41** (2022), 6844–6861. <https://doi.org/10.1007/s00034-022-02076-6>
38. Z. Xia, X. Wang, X. Li, C. Wang, S. Unar, M. Wang, et al., Efficient copyright protection for three CT images based on quaternion polar harmonic Fourier moments, *Signal Process.*, **164** (2019), 368–379. <https://doi.org/10.1016/j.sigpro.2019.06.025>
39. K. El-Khanchouli, H. Mansouri, N. E. Ghouate, H. Karmouni, N. E. Joudar, M. Sayyouri, et al., Protecting medical images using a zero-watermarking approach based on fractional Racah moments, *IEEE Access*, **13** (2025), 16978–17001. <https://doi.org/10.1109/ACCESS.2025.3532747>
40. A. F. Radilla, M. N. Miyatake, M. C. Hernandez, A robust image zero-watermarking using convolutional neural networks, In: *2019 7th International Workshop on Biometrics and Forensics (IWBF)*, 2019, 1–5. <https://doi.org/10.1109/IWBF.2019.8739245>
41. G. Liu, R. Xiang, J. Liu, R. Pan, Z. Zhang, An invisible and robust watermarking scheme using convolutional neural networks, *Expert Syst. Appl.*, **210** (2022), 118529. <https://doi.org/10.1016/j.eswa.2022.118529>
42. B. Han, J. Du, Y. Jia, H. Zhu, Zero-watermarking algorithm for medical image based on VGG19 deep convolution neural network, *J. Healthc. Eng.*, **2021** (2021), 5551520. <https://doi.org/10.1155/2021/5551520>
43. M. M. Darwish, A. A. Farhat, T. M. El-Gindy, Convolutional neural network and 2D logistic-adjusted-Chebyshev-based zero-watermarking of color images, *Multimed. Tools Appl.*, **83** (2023), 29969–29995. <https://doi.org/10.1007/s11042-023-16649-3>
44. A. A. Farhat, M. M. Darwish, T. M. El-Gindy, Resnet50 and logistic Gaussian map-based zero-watermarking algorithm for medical color images, *Neural Comput. Appl.*, **36** (2024), 19707–19727. <https://doi.org/10.1007/s00521-024-10121-5>
45. T. Huang, J. Xu, S. Tu, B. Han, Robust zero-watermarking scheme based on a depthwise overparameterized VGG network in healthcare information security, *Biomed. Signal Process.*, **81** (2023), 104478. <https://doi.org/10.1016/j.bspc.2022.104478>
46. B. Han, H. Wang, D. Qiao, J. Xu, T. Yan, Application of zero-watermarking scheme based on Swin transformer for securing the metaverse healthcare data, *IEEE J. Biomed. Health*, **28** (2024), 6360–6369. <https://doi.org/10.1109/JBHI.2023.3257340>
47. A. Anand, J. Bedi, A. Aggarwal, M. A. Khan, I. Rida, Authenticating and securing healthcare records: A deep learning-based zero watermarking approach, *Image Vis. Comput.*, **145** (2024), 104975. <https://doi.org/10.1016/j.imavis.2024.104975>
48. M. M. Abdel-Aziz, N. A. Lashin, H. M. Hamza, K. M. Hosny, ZWNet: Darknet53-based zero watermarking method for authentication of medical images inspired by Fibonacci Q-matrix and stationary wavelet transform, *Biomed. Signal Process. Control*, **100** (2025), 107044. <https://doi.org/10.1016/j.bspc.2024.107044>

49. F. Dong, J. Li, U. A. Bhatti, J. Liu, Y. W. Chen, and D. Li, Robust Zero Watermarking Algorithm for Medical Images Based on Improved NasNet-Mobile and DCT, *Electronics*, **12** (2023), 3444. <https://doi.org/10.3390/electronics12163444>
50. C. Gong, J. Liu, M. Gong, J. Li, U. A. Bhatti, J. Ma, Robust medical zero-watermarking algorithm based on residual-DenseNet, *IET Biometrics*, **11** (2022), 547–556. <https://doi.org/10.1049/bme2.12100>
51. R. Xiang, G. Liu, K. Li, J. Liu, Z. Zhang, M. Dang, Zero-watermark scheme for medical image protection based on style feature and ResNet, *Biomed. Signal Proces.*, **86** (2023), 105127. <https://doi.org/10.1016/j.bspc.2023.105127>
52. M. Sheng, J. Li, U. A. Bhatti, J. Liu, M. Huang, Y. W. Chen, Zero watermarking algorithm for medical image based on resnet50-DCT, *Comput. Mater. Contin.*, **75** (2023), 293–309. <https://doi.org/10.32604/cmc.2023.036438>
53. S. A. Nawaz, J. Li, M. U. Shoukat, U. A. Bhatti, M. A. Raza, Hybrid medical image zero watermarking via discrete wavelet transform-ResNet101 and discrete cosine transform, *Comput. Electr. Eng.*, **112** (2023), 108985. <https://doi.org/10.1016/j.compeleceng.2023.108985>
54. Y. Fan, J. Li, U. A. Bhatti, C. Shao, C. Gong, J. Cheng, et al., A multi-watermarking algorithm for medical images using inception V3 and DCT, *Comput. Mater. Contin.*, **74** (2023), 1279–1302. <https://doi.org/10.32604/cmc.2023.031445>
55. W. Zhang, J. Li, U. A. Bhatti, J. Liu, J. Zheng, Y. W. Chen, Robust multi-watermarking algorithm for medical images based on GoogLeNet and Henon map, *Comput. Mater. Contin.*, **75** (2023), 565–586. <https://doi.org/10.32604/cmc.2023.036317>
56. D. Tong, H. Hongxin, L. Can, W. Fengting, K. Weiling, R. Na, ConZWNNet: A contrastive learning-based zero-watermarking network for high robustness and distinguishability, *J. Inf. Secur. Appl.*, **93** (2025), 104139. <https://doi.org/10.1016/j.jisa.2025.104139>
57. J. Li, R. Wei, X. Xi, G. Zhang, Z. Yang, F. Zhang, Dual-branch cnn-transformer network for robust zero-watermarking of medical images, *Inf. Sci.*, **720** (2025), 122511. <https://doi.org/10.1016/j.ins.2025.122511>
58. C. Wang, H. Gao, M. Yang, J. Li, B. Ma, Q. Hao, Invariant image representation using novel fractional-order Polar harmonic Fourier moments, *Sensors*, **21** (2021), 1544. <https://doi.org/10.3390/s21041544>
59. M. A. Midoun, X. Cai, M. Z. Talhaoui, D. E. Mekkaoui, A. Smaili, Rotary combination permutation and image tiling to safeguard real-time image-based systems through a new 1D-chaotic map, *Expert Syst. Appl.*, **275** (2025), 126201. <https://doi.org/10.1016/j.eswa.2024.126201>



AIMS Press

© 2025 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (<https://creativecommons.org/licenses/by/4.0>)