

Research Article

A Polar Complex Exponential Transform-Based Zero-Watermarking for Multiple Medical Images with High Discrimination

Wenbing Wang ^{1,2}, Yan Li ^{1,3} and Shengli Liu¹

¹School of Cyberspace Security, P. L. A. Strategic Support Force Information Engineering University, Zhengzhou 450001, China

²Software Engineering College, Zhengzhou University of Light Industry, Zhengzhou 450001, China

³Software Engineering College, Zhengzhou University, Zhengzhou 450001, China

Correspondence should be addressed to Yan Li; ly79@zzu.edu.cn

Received 9 December 2020; Revised 25 January 2021; Accepted 19 February 2021; Published 17 March 2021

Academic Editor: Jinwei Wang

Copyright © 2021 Wenbing Wang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Zero-watermarking is one of the solutions for image copyright protection without tampering with images, and thus it is suitable for medical images, which commonly do not allow any distortion. Moment-based zero-watermarking is robust against both image processing and geometric attacks, but the discrimination of watermarks is often ignored by researchers, resulting in the high possibility that host images and fake host images cannot be distinguished by verifier. To this end, this paper proposes a PCET- (polar complex exponential transform-) based zero-watermarking scheme based on the stability of the relationships between moment magnitudes of the same order and stability of the relationships between moment magnitudes of the same repetition, which can handle multiple medical images simultaneously. The scheme first calculates the PCET moment magnitudes for each image in an image group. Then, the magnitudes of the same order and the magnitudes of the same repetition are compared to obtain the content-related features. All the image features are added together to obtain the features for the image group. Finally, the scheme extracts a robust feature vector with the chaos system and takes the bitwise XOR of the robust feature and a scrambled watermark to generate a zero-watermark. The scheme produces robust features with both resistance to various attacks and low similarity among different images. In addition, the one-to-many mapping between magnitudes and robust feature bits reduces the number of moments involved, which not only reduces the computation time but also further improves the robustness. The experimental results show that the proposed scheme meets the performance requirements of zero-watermarking on the robustness, discrimination, and capacity, and it outperforms the state-of-the-art methods in terms of robustness, discrimination, and computational time under the same payloads.

1. Introduction

Medical images such as those obtained via ultrasound and magnetic resonance imaging (MRI) provide substantial evidence for clinical diagnosis, medical treatment, and research. High-speed mobile networks such as 5G and 6G have further accelerated the application of telemedicine and medical resource sharing. Under this circumstance, researchers are concerned with security issues such as copyright protection, ownership identification, and tamper detection. Robust watermarking, as a traditional tool that

establishes a security barrier for information transmitted over open networks, has application prospects in medical image research [1, 2].

Medical images display the details and lesions of tissues and organs and have extremely high requirements for quality; thus, the traditional robust watermarking which embeds watermarks by tampering with images is not suitable. Zero-watermarking, also known as lossless watermarking, does not require modifying image contents and maintains stability after attacks, thus becoming an effective method of medical image authentication.

To offer security without tampering with images, zero-watermarking was proposed by Wen et al. [3]. Zero-watermarking extracts robust features of images to construct a zero-watermark and stores it in a third-party authority together with potential side information. When ownership or integrity is disputed, the watermark generated based on the zero-watermark and robust features can be used as a proof. Robustness, discrimination, security, payload, and computational time are the essential properties of zero-watermarking. Among them, discrimination and robustness are two high-priority and conflicting properties, and a promising scheme achieves a trade-off between them.

Inspired by Wen et al., a large number of zero-watermarking schemes have appeared, and a substantial portion of them create robust features based on the frequency domain [4, 5] or hybrids of image transforms and decomposition [6–12]. Common image transforms such as the DCT (discrete cosine transform) [9, 10], DWT (discrete wavelet transform) [4, 7, 8, 11], DFT (discrete Fourier transform) [4], CAT (cellular automata transform) [5], FrFT (fractional Fourier transform) [6], and CT (contourlet transform) [12] have been applied to zero-watermarking. Utilizing the invariance of the significant values in decompositions such as SVD [6–9, 11–13] and QR [10] to further improve the robustness is common in zero-watermarking research. Zero-watermarking in the frequency domain or image decomposition is robust and widely used. However, the coefficients and significant values are susceptible to scaling and rotation attacks, placing the watermark at risk when these attacks occur.

Moments with geometrically invariant properties can be used to solve the issue and are widely applied to zero-watermarking [14]. However, these schemes have deficiencies, owing to the utilization of the relation between the moment magnitudes and a single reference value to construct robust features, which results in similar features among different images and insufficient discrimination. Low discrimination will degrade the verification credibility. To this end, this paper takes PCET (polar complex exponential transform) [15] magnitudes of the same order and PCET magnitudes of the same repetition as reference values and proposes a novel PCET-based zero-watermarking with discrimination, robustness, and low time cost for multiple medical images. The main contributions of this paper can be summarized as follows:

- (1) A novel robust feature generation location selection method is proposed, which constructs content-related features, improving the discrimination and reducing the possibility of false positives.
- (2) The proposed robust feature generation location selection method and the resistance of the PCET magnitudes to geometric attacks are successfully applied to zero-watermarking, and a zero-watermarking scheme with robustness, discrimination, and a low time cost is proposed.
- (3) The proposed scheme processes multiple medical images concurrently by overlapping their robust features. Finally, the efficiency and practicability of the scheme are obtained.

The rest of this paper is organized as follows. Section 2 describes the previous moment-based zero-watermarking schemes and summarizes their workflows. Section 3 presents a novel robust feature generation location selection method and analyses its feasibility. The framework and procedures of proposed scheme are presented in Section 4. Section 5 verifies the robustness, discrimination, and capacity of the proposed method and discusses the experimental results. Section 6 concludes the work.

2. Related Work

Moment-based zero-watermarking is the focus of this paper. This section briefly introduces the previous moment-based schemes and gives their frameworks, to illustrate the rationality of the proposed robust feature generation location selection method and zero-watermarking scheme.

Orthogonal moments are divided into discrete orthogonal moments and continuous orthogonal moments, among which continuous orthogonal moments are more effective in image representation [16]. Thus, this paper mainly studies continuous orthogonal moment-based zero-watermarking. Early continuous orthogonal moments such as Zernike [17] have a base function with factorial operations, and the zero-watermarking schemes based on these moments include Bessel Fourier moment-based scheme [14] and OFMM- (orthogonal Fourier-Mellin moments-) based scheme [18]. Factorial operations of moments may limit both computational efficiency and resistance to geometric attacks. Therefore, zero-watermarking that uses harmonic-based continuous orthogonal moments, such as PCET [19] and PHFM (polar harmonic Fourier moments) [20], has been developed. Considering the relation of the three channels of colour images, quaternion continuous orthogonal moments such as the QPHT (quaternion polar harmonic transform) [21] and QEM (quaternion exponential moment) [22] have been applied to zero-watermarking. Furthermore, the QPHFM-(quaternion polar harmonic Fourier moments-) based scheme by Xia et al. [23] utilizes wavelet numerical integration to improve the moment accuracy and robustness and uses QR codes to encode watermarks for large payload and security. Yang et al. [24] used the DFT to calculate QGPCET (quaternion generic polar complex exponential transform) moment to lower the computational complexity. Additionally, to solve the low discrimination issue, the scheme utilizes the characteristic of the GPCET in which the image areas highly described by the GPCET are adjustable by a parameter to mix up the GPCET magnitudes with the different parameters. Shao et al. [25] combined quaternion continuous orthogonal moments with visual cryptography to give a zero-watermarking model.

The above moment-based zero-watermarking schemes are different in their specific details, but their frameworks, as shown in Figure 1, are similar. First, these schemes construct the robust feature domain, mainly selecting an appropriate moment. Then, the geometric invariants and reference values are calculated as the robust feature generation location, which is crucial to the performance of zero-watermarking. Moment magnitudes are stable against attacks, making them the first choice for

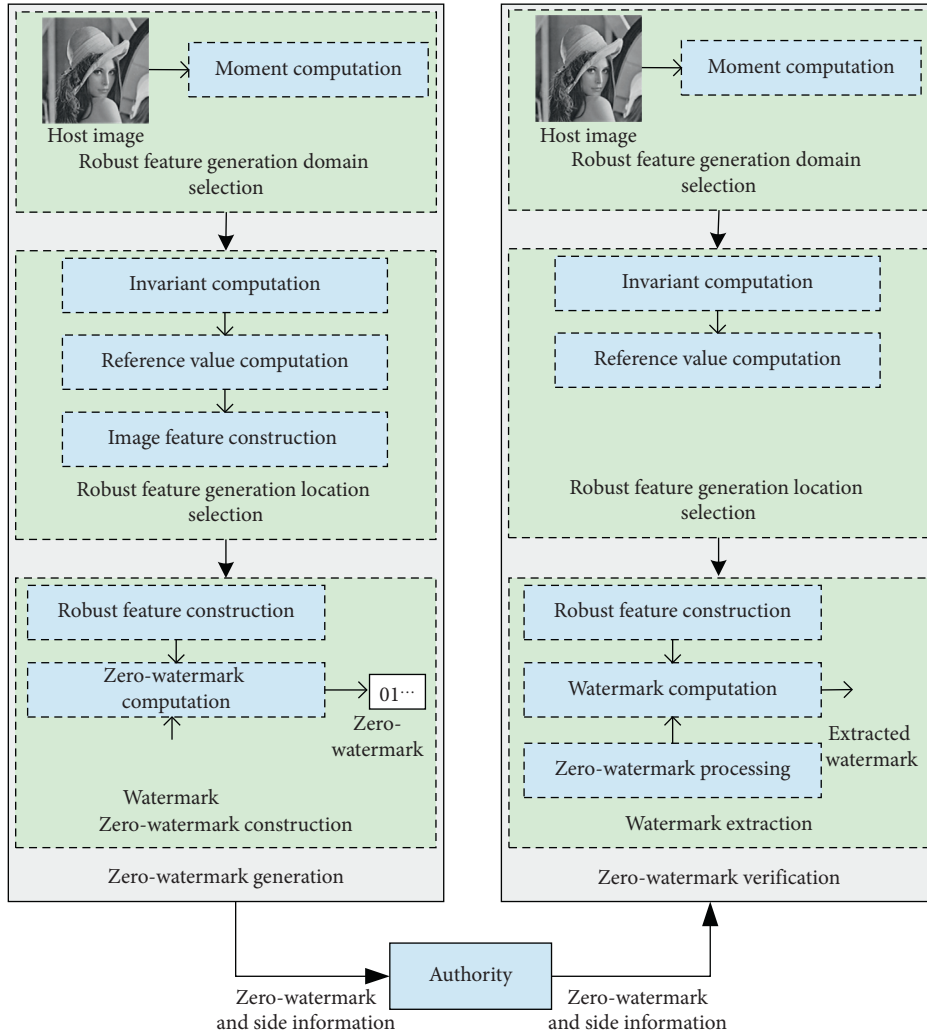


FIGURE 1: Framework of moment-based zero-watermarking.

geometric invariants. In the selection of the reference value, most schemes select one value as the reference value of all the geometric invariants. For example, [19–21, 23] select the mean of the geometric invariants, [14, 18, 24, 25] select the median of the geometric invariants, and [22] selects the Otsu threshold as the reference value (Table 1). With the invariants and reference value, schemes construct image features. Finally, a binary robust feature vector based on the image features is created and combines with a watermark to generate a zero-watermark. The verification is different from the construction in the third step, which uses the generated robust features and the zero-watermark stored in a third-party authority to recover the watermark.

It can be seen from Figure 1 that when the robust feature generation domain is known, the robust feature generation location, that is, the selection of geometric invariants and reference values, determines the robustness and discrimination. Although these existing zero-watermarking schemes have already achieved resistance to both image processing and geometric attacks, the characteristic that the value distributions of magnitudes have certain regularity results in insufficient discrimination. Therefore, to achieve both discrimination and robustness, this paper proposes a new

TABLE 1: Reference value selection methods.

Selection methods of reference values	Reference number
Median of magnitudes	[14, 18, 24, 25]
Mean of magnitudes	[19–21, 23]
Others	[22]

robust feature generation location selection method based on the stability of the relation between magnitudes of the same order and magnitudes of the same repetition and presents a novel PCET-based zero-watermarking scheme on this basis.

3. Proposed Robust Feature Generation Location Selection Method

3.1. Selection Procedure. Denote the moment of order n with repetition l as $m^{n,l}$. The flowchart of proposed robust feature generation location selection method is seen in Figure 2, and the steps are as follows:

- (1) Calculation of magnitudes and reference values: calculate the moment magnitudes and denote them

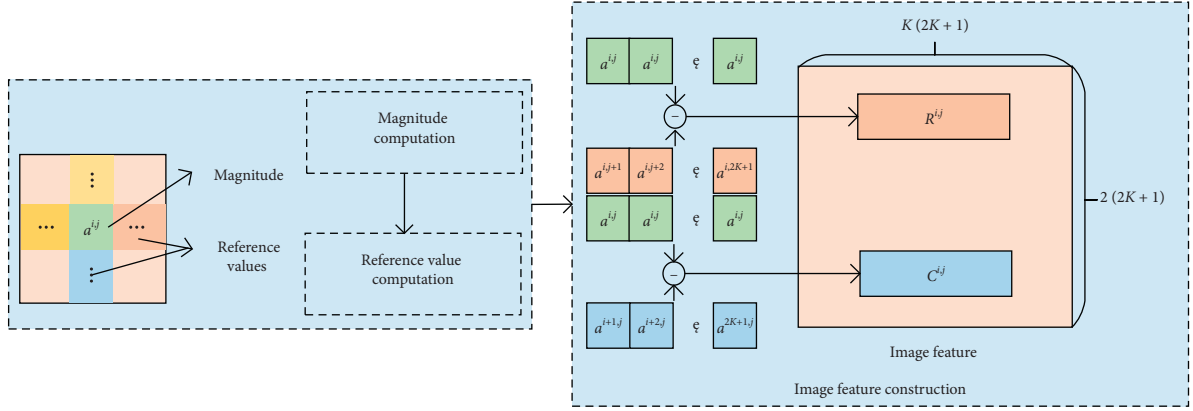


FIGURE 2: Workflow of proposed robust feature generation location selection.

as $M = \{|m^{n,l}| |n|, |l| \leq K\}$, which can be saved as matrix $A = (a^{i,j})_{(2K+1) \times (2K+1)}$, where $a^{i,j} = |m^{(i-K-1), (j-K-1)}|$. The reference values of $a^{i,j}$ are the magnitudes of column coordinates greater than j in its row and the magnitudes of row coordinates greater than i in its column, that is, $a^{i,j+1}, a^{i,j+2}, \dots, a^{i,2K+1}, a^{i+1,j}, a^{i+2,j}, \dots, a^{2K+1,j}$ are the reference values of $a^{i,j}$.

- (2) Image feature construction: $a^{i,j}$ ($1 \leq i \leq 2K+1, 1 \leq j < 2K+1$) subtracts its reference values with the same row coordinate; the result is a row vector $[a^{i,j} - a^{i,j+1} \ a^{i,j} - a^{i,j+2} \ \dots \ a^{i,j} - a^{i,2K+1}]$. Concatenate the $2K$ row vectors generated by the i th row of A into one row vector, and denote the row vector as R^i ($1 \leq i \leq 2K+1$) which has $2K^2 + K$ elements. Similar steps are performed on $a^{i,j}$ ($1 \leq i < 2K+1, 1 \leq j \leq 2K+1$) and its reference values with the same column coordinate, thereby a row vector C^i ($1 \leq i \leq 2K+1$) with $2K^2 + K$ elements is obtained. R^i and C^i compose an image feature matrix denoted as F :

$$F = (a^{i,j})_{(4K+2) \times (2K^2+K)} = \begin{bmatrix} R^1 \\ R^2 \\ \vdots \\ R^{2K+1} \\ C^1 \\ C^2 \\ \vdots \\ C^{2K+1} \end{bmatrix}. \quad (1)$$

- (3) Robust feature construction: binarize F by comparing each element with zero to get robust features $F_b = \{b^{i,j} | i = 1, 2, \dots, 2(2K+1), j = 1, 2, \dots, K(2K+1)\}$. The binarization process is

$$b^{i,j} = \begin{cases} 1, & d^{i,j} \geq 0, \\ 0, & \text{otherwise.} \end{cases} \quad (2)$$

3.2. Performance Comparison. Robust features of images should be stable against various attacks and closely relate to the image contents. Most existing moment-based zero-watermarking schemes choose the median or average of the moment magnitudes as the reference values, resulting in the low discrimination. To verify the performance of the proposed robust feature generation location selection method, this section designs three robust feature generation location selection methods based on the existing reference value selection methods (see Table 1) and compares them with the proposed method. The first method calculates the PCET magnitudes of images and uses the median of the magnitudes as the reference value to generate robust features; the second method also uses the PCET magnitudes as the geometric invariants, but the mean of the magnitude as the reference value; Inspired by Yang et al. [24], the third method calculates GPCET magnitudes with the parameter s of 0.5, 1, 2, and 3, and then uses the mean of medians of the four magnitude vectors as the reference value to construct the robust features. The robust features with sizes of 1000, 2000, 3000, and 4000 generated by the four methods are compared. The tested images are 2125 (1068 images with size of 128×128 , 204 images with size of 256×256 , 384 images with size of 160×128 , and 469 images with size of 512×512) medical images. Hamming distance is the quantitative measurement of the discrimination in this section, which is proportional to the discrimination. BER (bit error rate) and two attacks of the JPEG compression (QF = 30) and rotation (-5°) are used to measure the robustness. The comparative results of the Hamming distance and BER for the four methods are shown in Figures 3 and 4, and the formulas of Hamming distance and BER are seen in the following equations:

$$h = \sum_{i=1}^L (u_i \oplus v_i), \quad (3)$$

$$\text{BER} = \frac{\sum_{i=1}^L (u_i \oplus u_i^*)}{L}. \quad (4)$$

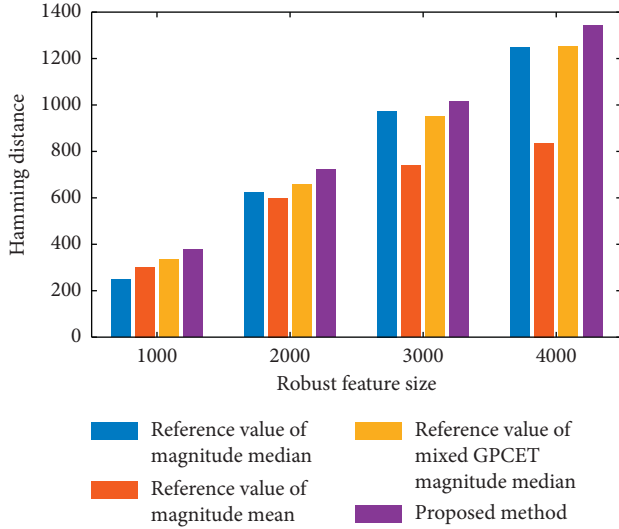


FIGURE 3: Hamming distance comparison of robust features.

Figure 3 shows the comparative results of the average Hamming distance. For the proposed method, the percentages of the Hamming distance to robust feature size are more than 30%, which are at least 6.1% higher than the average of the other three methods. Although the third method mixes GPCET magnitudes with different parameters to improve the discrimination, its average Hamming distance is 3.0% lower than that of the proposed method.

After compression and rotation attacks, the comparative results of the average BER are shown in Figure 4. As can be seen, compared with the other three methods, the BER values of the proposed method are low for both the JPEG compression and rotation. Specifically, the average BER for JPEG compression is 0.027, while the highest and lowest average BERs for the other three methods are 0.074 and 0.031, respectively; The average BER for rotation is 0.029, while the highest and lowest average BERs for the other three methods are 0.091 and 0.041, respectively. Therefore, the robustness of the proposed selection method is superior to the other three methods.

In summary, the proposed robust feature generation location selection method has both discrimination and

robustness. Its application in the moment-based zero-watermarking is presented in Section 4.

4. Proposed Zero-watermarking Scheme

To conserve the computational space and improve the practicability, the proposed scheme processes medical images in groups. Zero-watermark generation and verification for an image group are introduced in this section, and Figure 5 shows the framework of the zero-watermark generation process.

4.1. Zero-Watermark Generation. For the image group $A_{\text{set}} = \{A_t | A_t \in R_{M \times N}, 1 \leq t \leq T\}$ and binary watermark $W = \{w_i | 1 \leq i \leq L\}$, the steps of zero-watermark generation are as follows:

- (1) Robust feature generation domain selection. For the t th image, the PCET moments are calculated, and denote the moment of order n with repetition l as $m_t^{n,l}$.
- (2) Robust feature generation location selection
 - (2.1) Apply the proposed robust feature generation location selection method to each image of A_{set} . Extract the image features of each image and denote them as F_t , and the extraction steps can be seen in Section 3.
 - (2.2) Superposition of image features. Repeat step 2.1 to get the T image feature matrixes of A_{set} , and add them together based on the principle of matrix addition:
$$F = \sum_{t=1}^T F_t = (d^{i,j})_{(4K+2) \times (2K^2+K)}. \quad (5)$$
- (3) Construction of zero-watermark
 - (3.1) Robust feature generation. Binarize F by comparing each element with zero, and denote the resulting binary sequence as $F_b = \{b^{i,j} | i = 1, 2, \dots, 2(2K+1), j = 1, 2, \dots, K(2K+1)\}$. The specific binarization process is

$$b^{i,j} = \begin{cases} 1 & d^{i,j} \geq 0 \\ 0 & \text{otherwise} \end{cases}, \quad i = 1, 2, \dots, 2(2K+1), j = 1, 2, \dots, K(2K+1). \quad (6)$$

- (3.2) Robust feature scrambling and selection: set the initial value of a chaos systems such as the logistic map as x_1 to get a pseudorandom number sequence $\{x_i^1 | 1 \leq i \leq N\}$, where $N = 2K(2K+1)^2$. x_1 is adopted as the secret key Key_1 . The subscript sequence $I = \{o_i | 1 \leq i \leq N\}$ is obtained by sorting $\{x_i^1 | 1 \leq i \leq N\}$ in ascending or descending

order. F_b is transformed into an one-dimensional vector and then is sorted according to I . The first L elements of the sorted vector are the robust features of the image group and are denoted as $S = \{b_i | 1 \leq i \leq L\}$.

- (3.3) Watermark scrambling: set the initial value of the chaos system as x_2 to get a pseudorandom number sequence $\{x_i^2 | 1 \leq i \leq L\}$. x_2 is the secret

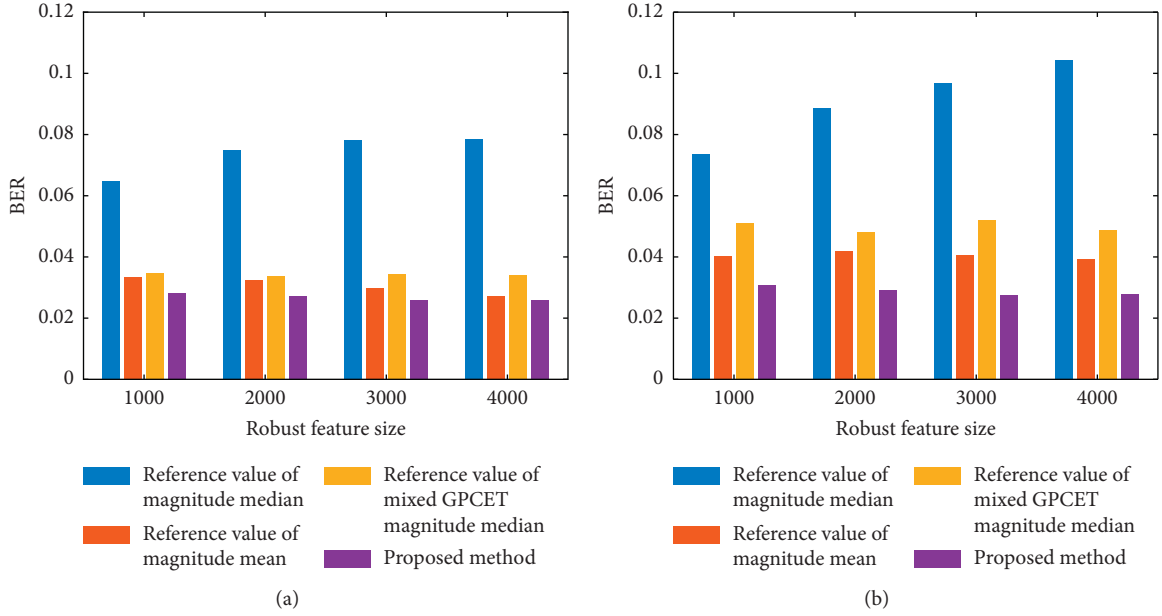


FIGURE 4: Robustness comparison of robust features. (a) JPEG compression (QF=30). (b) Rotation (-5°).

key *Key2*. Similar to Step 3.2, the binary watermark is scrambled according to the subscript sequence of sorted $\{x'_i | 1 \leq i \leq L\}$ and then is denoted as $W' = \{w'_i | 1 \leq i \leq L\}$.

- (3.4) Zero-watermark generation: perform the bitwise XOR operation on the robust features S and the watermark W' to get the final zero-watermark $W_{\text{zero}} = \{w_i^z | i = 1, 2, \dots, L\}$. The computation of the i th bit of zero-watermark is as follows:

$$w_i^z = b_i \oplus w'_i, \quad 1 \leq i \leq L. \quad (7)$$

- (4) W_{zero} is transmitted to a third-party authority together with the secret keys *Key1* and *Key2*.

4.2. Zero-Watermark Verification

- (1) Robust feature generation domain and location selection. They are same as Step 1 and Step 2 of the zero-watermark generation.
- (2) Watermark generation
 - (2.1) Robust feature generation and scrambling: with the secret key *Key1* obtained from the authority, the robust feature $S^* = \{b_i^* | 1 \leq i \leq L\}$ of the potentially distorted host images is generated. The generation method of robust feature can be seen in zero-watermark generation.
 - (2.2) Generation of scrambled watermark: perform the bitwise XOR on the zero-watermark obtained from the authority and S^* , and denote the resulting binary sequence as W'^* , where the i th bit is generated as follows:

$$w_i'^* = b_i^* \oplus w_i^z, \quad 1 \leq i \leq L. \quad (8)$$

- (2.3) Watermark recovery: use *Key2* obtained from the authority to recover W'^* , thereby a binary watermark for image authentication is obtained.

5. Experimental Results and Discussion

This section first comprehensively evaluated the robustness, discrimination, and capacity of the proposed scheme. Then, a comparison with other schemes is performed in terms of the discrimination, robustness, and computational efficiency.

5.1. Experimental Settings. The test images come from 10 grayscale medical images of 256×256 and 345 grayscale medical images of 512×512 in the TCIA library. The watermarks include 4 logo images and 8 randomly generated binary sequences. Both the discrimination and robustness can be measured using BER defined in (4). The PCET-based zero-watermarking [19], the QPHFM-based zero-watermarking [20], and the QGPCET-based zero-watermarking [24] are selected for a performance comparison. Because the performance of moment-based zero-watermarking is related to the maximum order of the moment, this section sets the maximum order K to the minimum allowed. When the watermark size is 64×64 , the minimums of K for scheme [19], scheme [20], scheme [24], and the proposed scheme are 37, 45, 16, and 8, respectively. The specific experimental parameters are shown in Table 2.

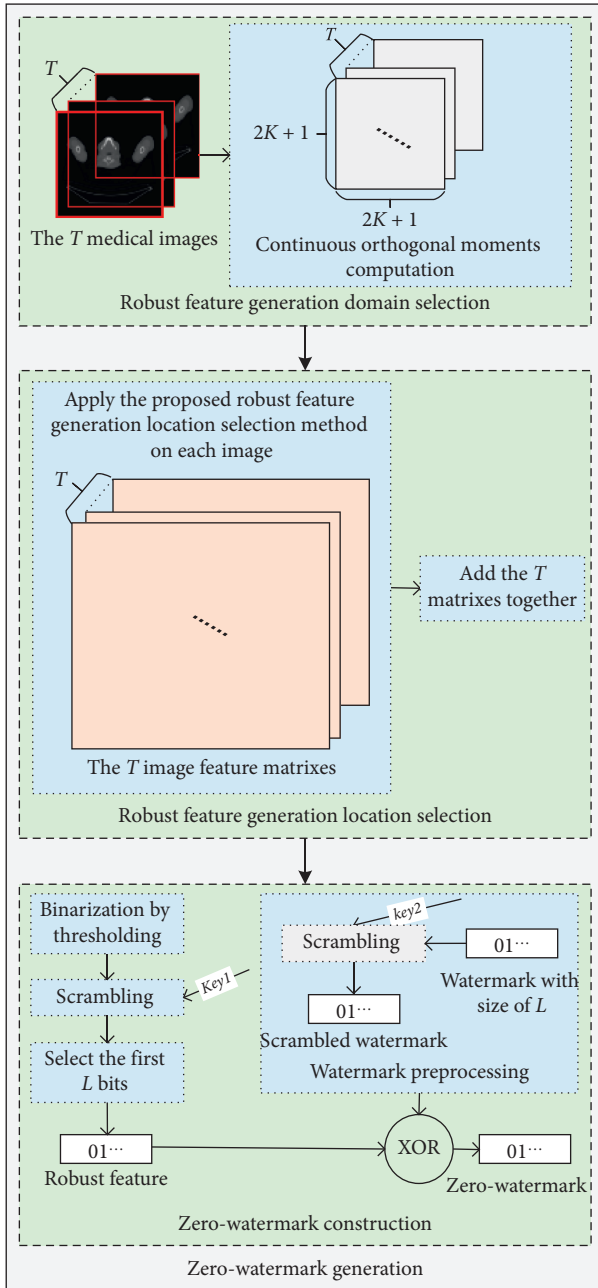


FIGURE 5: Framework of proposed zero-watermark generation.

5.2. *Robustness.* Robustness is one of the important properties of zero-watermarking and is inversely proportional to BER. To verify the robustness of the proposed scheme against both common image processing and geometric attacks, 130 images of 512×512 , 10 images of 256×256 , and 4 watermarks of 32×32 , 48×32 , 48×48 , and 64×64 are chosen to test the resistance against compression (QF = 30), rotation (-5°), scaling (1/2), and salt and peppers noise (0.01). Figures 6 and 7 show the correct extraction rate $R_c = N_c/N$ and BER of the extracted watermarks, respectively, where N_c is the number of correct watermark bits and N is the total number of watermark bits.

When 10 images of 512×512 and 10 images of 256×256 are divided into 10 groups (2 images in each group), the relationship between the correct extraction rate and the watermark size can be seen in Figure 6. As can be seen, the correct extraction rates are close to 1. Especially, the correct extraction rates of rotation and scaling are higher than 0.99. These data show that the proposed scheme maintains good resistance to different attacks under different payloads.

Figure 7 is the relationship between the average BER and the number T of images each group with a watermark of 64×64 and 120 images of 512×512 . The mean and standard deviation are 0.0132 and 0.0013 for compression, 0.0034 and 0.0003 for rotation, 0.0046 and 0.0005 for scaling, and 0.0121 and 0.0031 for salt and peppers, respectively. The highest point of the four curves corresponds to the salt and peppers noise and is 0.0178. Thus, the robustness of the proposed scheme is not affected by the number of images each group.

5.3. *Discrimination.* Another attribute of zero-watermarking is discrimination, which is proportional to the BER of the watermarks extracted from fake host images. To verify that the proposed scheme achieves significant discrimination, this section uses 10 images of 512×512 to construct 10 image groups numbered 1 to 10 and executes 10 zero-watermark generation processes and 10×10 zero-watermark verification process. The BERs obtained from the 10×10 verification process are presented in Table 3.

The row headings of Table 3 indicate the host image number, and the column headings are the image number in the verification process. When the generation and verification process are performed on the same image, the BERs (data on the diagonal line) are zero; when they are on different images, the average and minimum of BERs are 0.3631 and 0.2629, respectively. As can be seen, the proposed scheme can distinguish “true” and “false” images in the verification process.

5.4. *Capacity.* It is known that the robust features of the proposed scheme are generated by $2K(2K + 1)^2$ moments. Therefore, the number of robust feature bits is proportional to K , and theoretically unlimited capacity for the proposed scheme can be inferred. A scheme with extensive application prospective should achieve trade-off between capacity, robustness, and discrimination. To verify that the robustness and discrimination of the proposed scheme do not be degraded by high capacity, Figure 8 shows the relationship between the capacity and robustness and relationship between the capacity and discrimination based on 10 groups ($T = 1$) of 512×512 images and binary watermarks with different sizes.

Figure 8(a) presents BERs corresponding to four attacks of compression (QF = 30), rotation (-5°), scaling (1/2), and salt and peppers noise (0.01). Figure 8(b) shows the average BER when one group is regarded as the host image group, and the other 9 groups are used for the verification. The robustness decreases slightly as the capacity increases, and the maximum of BER is 0.0407. The discrimination increases slightly with the increasing capacity, and the minimum of

TABLE 2: Experimental settings.

Medical image database	TCIA [26]
Image size	512×512 , 256×256
Number of images	355
Watermark size	32×32 , 48×32 , 48×48 , 64×64 , 1000, 2000, 3000, 4000, 5000, 6000, 7000, 8000
Maximum order K of proposed scheme	8
Similar schemes	[19, 20, 24]

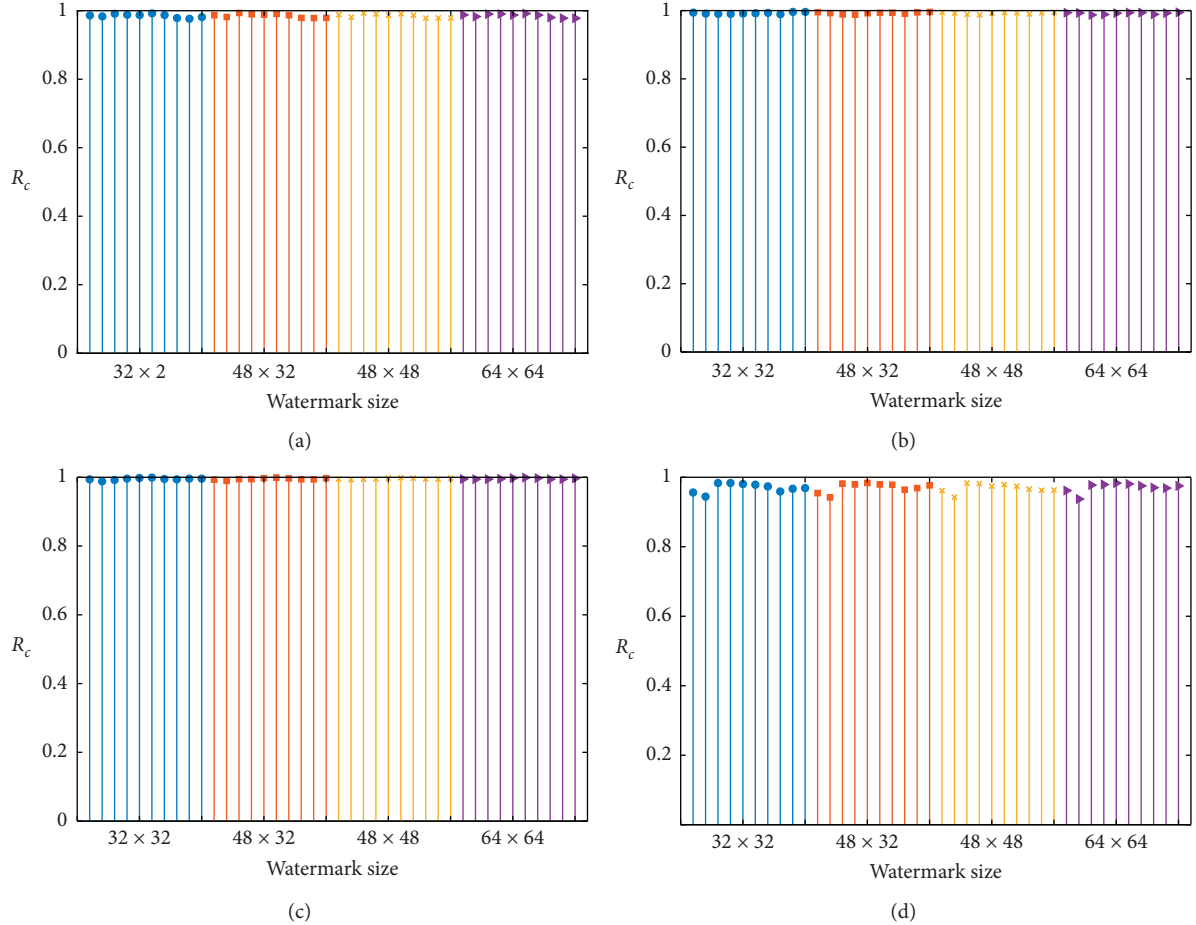


FIGURE 6: Relationship between watermark size and robustness. (a) JPEG compression (QF = 30). (b) Rotation (-5°). (c) Scaling (0.5). (d) Salt and peppers noise ($d=0.01$).

BER is 0.3218. These results demonstrate that the increasing of capacity does not degrade the robustness and discrimination.

5.5. Comparison with Other Schemes. This section will compare the performance of the proposed scheme with [19, 20, 24] based on 215 tested images in terms of robustness, discrimination, and computation time. For robustness, this section chooses 22 representative attacks which include common image processing such as compression, and geometric distortion such as rotation. The comparative results are presented in Tables 4–7. Because [20] takes 3 images as one group, its results come from 70 image groups. In addition, Table 8 presents the watermarks

generated by [20] and the proposed scheme when the 3 images of one group are rotated by 90° , 45° , and 0° , respectively. A zero-watermarking with high discrimination should distinguish not only original fake host images but also attacked fake host images. Table 9 presents the average BER when 210 attacked images are fake host images. Table 10 shows the computation time of the four schemes in the same software environments (MATLAB 2018) and hardware environments (2.90 GHz processor, 8 GB RAM). In the section 5, the moment calculation in the simulation experiments are based on ZOA (zeroth-order approximation) except for that of [24]. For the schemes that process images in groups, the computation time of an image is the result that the executing time of its group is divided by the number of images each group. The group size of the

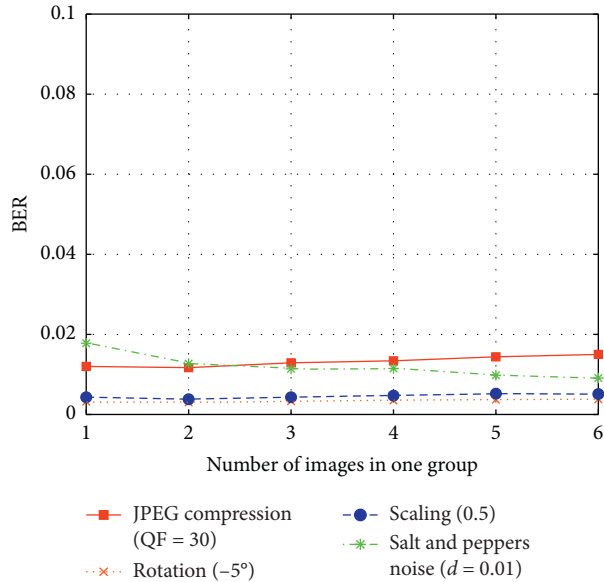


FIGURE 7: Relationship between number of images each group and robustness.

TABLE 3: Verification results among 10 image groups (BER).

Image no	1	2	3	4	5	6	7	8	9	10
1	0	0.3782	0.3799	0.3760	0.3508	0.4290	0.3494	0.4644	0.3142	0.2817
2	0.3782	0	0.3689	0.3870	0.4014	0.4019	0.3774	0.4563	0.3691	0.3523
3	0.3799	0.3689	0	0.2939	0.3313	0.4148	0.2815	0.4111	0.3240	0.3481
4	0.3760	0.3870	0.2939	0	0.3113	0.4080	0.2981	0.3438	0.2834	0.3472
5	0.3508	0.4014	0.3313	0.3113	0	0.3965	0.3335	0.4177	0.3003	0.3484
6	0.4290	0.4019	0.4148	0.4080	0.3965	0	0.3716	0.4094	0.3892	0.4138
7	0.3494	0.3774	0.2815	0.2981	0.3335	0.3716	0	0.3992	0.2939	0.2947
8	0.4644	0.4563	0.4111	0.3438	0.4177	0.4094	0.3992	0	0.4226	0.4497
9	0.3142	0.3691	0.3240	0.2834	0.3003	0.3892	0.2939	0.4226	0	0.2629
10	0.2817	0.3523	0.3481	0.3472	0.3484	0.4138	0.2947	0.4497	0.2629	0

proposed scheme is set to 1, 3, and 5, thereby the 210 tested images are divided into 210 groups, 70 groups, and 42 groups. The size of the watermark used in this section is 64×64 .

It can be seen from Tables 4–7 that the robustness of the proposed scheme is significantly higher than the other three schemes for most attacks. For example, BER of the proposed scheme is lower than 0.004 for counterclockwise rotation with 3° , while the minimum of the other three schemes is 0.0103. Although the four schemes are based on the harmonic-based continuous orthogonal moments, the proposed scheme assigns multiple reference values to each magnitude to build a one-many relationships between magnitudes and robust feature bits, which lowers the maximum order K of the moments involved in zero-watermarking. Therefore, the proposed scheme improves the robustness significantly by utilizing low-order moments to construct robust features.

Xia et al. [20] utilize the resistance of the quaternion moment magnitudes to construct QPHFM-based robust features for three images at the same time. However, binding three images together may affect its robustness

against rotation. In Table 8, when the three images of a group are rotated with 90° , 45° , and 0° , respectively, the BERs of the watermarks generated by the proposed scheme and [20] are 0.0017 and 0.1006. As can be seen, when the images of a group are rotated at different angles, the robustness of [20] is obviously degraded. [20] takes three images rotated with different degrees as the three imaginary parts of a quaternion to calculate a quaternion moment, destroying the stability of quaternion moment magnitudes. The proposed scheme calculates the moments for each image in a group separately before reconstructing the robust feature of the group; thus, it not only can change the group size but also maintains robustness when the images in one group are rotated at different angles.

To verify the discrimination of the proposed scheme, Table 9 gives the average BER of the watermarks obtained from the distorted fake host images. BER of the [19, 20] is significantly lower than that of the proposed scheme. Yang et al. [24] mixed QGPCET moments with different parameters to strengthen the correlation between robust features and host images, but the discrimination is still weaker

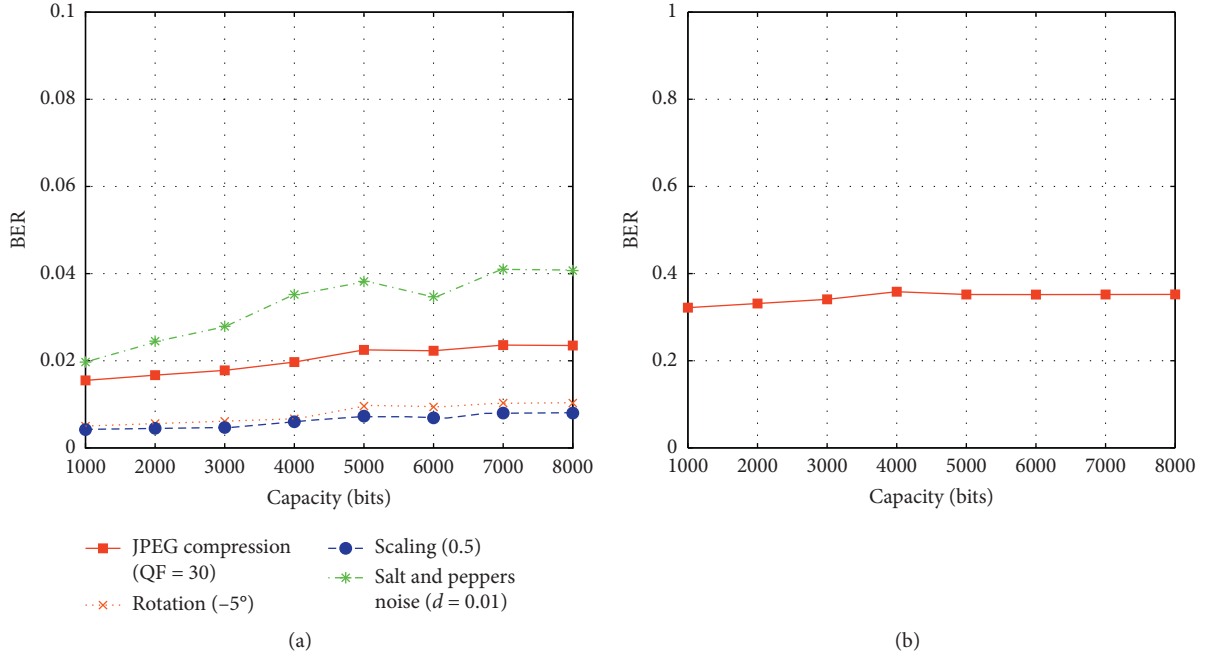


FIGURE 8: (a) Robustness and (b) discrimination under different payloads.

TABLE 4: Resistance comparison against JPEG compression (BER).

Attack type	Proposed scheme			Scheme [19]	Scheme [20]	Scheme [24]
	1 image each group	3 images each group	5 images each group			
JPEG compression (QF = 30)	0.0127	0.0122	0.0143	0.0095	0.0070	0.0156
JPEG compression (QF = 50)	0.0079	0.0074	0.0085	0.0062	0.0046	0.0103
JPEG compression (QF = 75)	0.0036	0.0031	0.0037	0.0036	0.0024	0.0058

TABLE 5: Resistance comparison against geometric attacks (BER).

Attack type	Proposed scheme			Scheme [19]	Scheme [20]	Scheme [24]
	1 image each group	3 images each group	5 images each group			
Rotation (-3°)	0.0043	0.0040	0.0048	0.0131	0.0103	0.0129
Rotation (-5°)	0.0034	0.0030	0.0033	0.0076	0.0080	0.0085
Rotation (-10°)	0.0043	0.0038	0.0042	0.0045	0.0048	0.0058
Scaling (0.5)	0.0045	0.0041	0.0044	0.0046	0.0084	0.0060
Scaling (2)	0.0027	0.0022	0.0025	0.0011	0.0017	0.0014

TABLE 6: Resistance comparison against noise attacks (BER).

Attack type	Proposed scheme			Scheme [19]	Scheme [20]	Scheme [24]
	1 image each group	3 images each group	5 images each group			
Salt&peppers noise ($d = 0.01$)	0.0190	0.0099	0.0090	0.0333	0.0187	0.0394
Salt and peppers noise($d = 0.02$)	0.0276	0.0142	0.0122	0.0480	0.0273	0.0571
Gaussian noise ($d = 0.001$)	0.0349	0.0194	0.0167	0.0142	0.0087	0.0220
Gaussian noise ($d = 0.005$)	0.0347	0.0189	0.0166	0.0304	0.0188	0.0476
Gaussian noise ($d = 0.01$)	0.0346	0.0191	0.0160	0.0434	0.0260	0.0671

TABLE 7: Resistance comparison against image filtering (BER).

Attack type	Proposed scheme			Scheme [19]	Scheme [20]	Scheme [24]
	1 image each group	3 images each group	5 images each group			
Average filtering (3×3)	0.0061	0.0057	0.0058	0.0123	0.0118	0.0087
Average filtering (5×5)	0.0105	0.0102	0.0099	0.0317	0.0309	0.0232
Average filtering (9×9)	0.0234	0.0233	0.0217	0.0751	0.0735	0.0655
Gaussian filtering (3×3)	0.0058	0.0054	0.0055	0.0118	0.0114	0.0084
Gaussian filtering (5×5)	0.0094	0.0090	0.0088	0.0269	0.0264	0.0195
Gaussian filtering (9×9)	0.0143	0.0141	0.0133	0.0458	0.0448	0.0359
Median filtering (3×3)	0.0056	0.0049	0.0055	0.0068	0.0071	0.0098
Median filtering (5×5)	0.0187	0.0167	0.0194	0.0223	0.0238	0.0298
Median filtering (9×9)	0.0652	0.0551	0.0596	0.0731	0.0755	0.0961

TABLE 8: Robustness comparison between proposed scheme and [20] when three images of a group are rotated by 90° , 45° , and 0° .

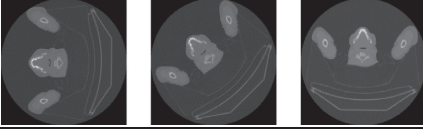


Group with 3 rotated images	Proposed scheme	Scheme [20]
		

TABLE 9: Discrimination comparison (BER).

Attack type	Proposed scheme			Scheme [19]	Scheme [20]	Scheme [24]
	1 image each group	3 images each group	5 images each group			
JPEG compression (QF = 20)	0.3315	0.3408	0.3283	0.1998	0.2232	0.3356
Rotation(-45°)	0.3314	0.3401	0.3276	0.1986	0.2229	0.3359
Scaling (0.3)	0.3408	0.3388	0.3241	0.1912	0.2280	0.3297
Scaling (3)	0.3310	0.3401	0.3275	0.1997	0.2237	0.3367
Salt and peppers noise ($d = 0.05$)	0.3323	0.3392	0.3281	0.2127	0.2249	0.3409
Gaussian noise($d = 0.005$)	0.3317	0.3393	0.3283	0.2317	0.2320	0.3491

TABLE 10: Computational time comparison (s).

1 image each group	Proposed scheme			Scheme [19]	Scheme [20]	Scheme [24]
	3 images each group	5 images each group				
11.98	12.18	11.90		269.52	186.65	18.36

than the proposed scheme for attacks other than Gaussian noise. Therefore, robust feature generation method based on the relationship between magnitudes of the same order and relationship between magnitudes of the same repetition is effective in improving the discrimination. In addition, the discrimination of the proposed scheme is independent of the number of images each group.

When the moments of an $M \times N$ image are calculated by ZOA, the time complexity for the PCET, GPHFM, and GPCET are all $O(MNK^2)$, where K is the maximum order. Therefore, their computation time is closely related to K . Table 10 shows that the proposed scheme is superior to the other schemes in terms of the computation time. The computation time of [19] is highest because its K is 37.

Although [20] can process three images at the same time, its quaternion PHFM moment calculation includes the calculation of PHFM moments with maximum order 45 for three image. Yang et al. [24] use DFT to reduce the computation time of GPCET moments, and its time efficiency is highest among the other three schemes. However, it is still lower than that of the proposed scheme. The proposed scheme set the maximum order of the moments to 8, which substantially lowers its time cost.

6. Conclusions

To solve the low discrimination issues that is common in previous moment-based zero-watermarking, this paper

proposed a new robust feature generation location selection method by regarding the magnitudes with the same order and magnitudes with the same repetition as the reference values of each magnitude, avoiding the low discrimination by assigning a single reference value to all the magnitudes and improving the robustness and computational efficiency by reducing the number of the magnitudes involved. Based on the proposed robust feature generation location selection method, this paper further proposed a PCET-based zero-watermarking scheme for multiple medical images. The experimental results indicate the significance of this work in terms of discrimination, robustness, capacity, and time cost. In the future, we will extend the robust feature construction method to other moments and apply it to other image processing domains.

Data Availability

The pseudocode used to support the findings of this study is available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Nos. 62002387 and 61872448) and the Science and Technology Innovation Talent Project of Henan Province (No. 184200510018).

References

- [1] C. Kumar, A. K. Singh, and P. Kumar, "A recent survey on image watermarking techniques and its application in e-governance," *Multimedia Tools and Applications*, vol. 77, no. 3, pp. 3597–3622, 2018.
- [2] A. Anand and A. K. Singh, "An improved DWT-SVD domain watermarking for medical information security," *Computer Communications*, vol. 152, pp. 72–80, 2020.
- [3] Q. Wen, T. F. Sun, and S. X. Wang, "Concept and application of zero-watermark," *Acta Electronica Sinica*, vol. 31, no. 2, pp. 214–216, 2003.
- [4] H.-H. Tsai, Y.-S. Lai, and S.-C. Lo, "A zero-watermark scheme with geometrical invariants using SVM and PSO against geometrical attacks for image protection," *Journal of Systems and Software*, vol. 86, no. 2, pp. 335–348, 2013.
- [5] T.-Y. Fan, H.-C. Chao, and B.-C. Chieu, "Lossless medical image watermarking method based on significant difference of cellular automata transform coefficient," *Signal Processing: Image Communication*, vol. 70, pp. 174–183, 2019.
- [6] S. Rawat and B. Raman, "A blind watermarking algorithm based on fractional Fourier transform and visual cryptography," *Signal Processing*, vol. 92, no. 6, pp. 1480–1491, 2012.
- [7] A. Dwivedi, A. Kumar, M. K. Dutta et al., "An efficient and robust zero-bit watermarking technique for biometric image protection," in *Proceedings of the International Conference on Telecommunications & Signal Processing*, Budapest, Hungary, July 2019.
- [8] X. L. Liu, B. J. Chen, and G. Coatrieux, "Color image zero-watermarking based on SVD and visual cryptography in DWT domain," in *Proceedings of the Eighth International Conference On Graphic And Image Processing*, Tokyo, Japan, October 2016.
- [9] X. Wu and W. Sun, "Robust copyright protection scheme for digital images using overlapping DCT and SVD," *Applied Soft Computing*, vol. 13, no. 2, pp. 1170–1182, 2013.
- [10] T. M. Thanh and K. Tanaka, "An image zero-watermarking scheme based on the encryption of visual map feature with watermark information," *Multimedia Tools and Applications*, vol. 76, no. 11, pp. 13455–13471, 2017.
- [11] X. B. Kang, G. F. Lin, Y. J. Chen et al., "Robust and secure zero-watermarking scheme for color images based on majority voting pattern and hyper-chaotic encryption," *Multimedia Tools and Applications*, vol. 79, pp. 1169–1202, 2020.
- [12] C. Kavitha and S. Sakthivel, "An effective mechanism for medical images authentication using quick response code," *Cluster Computing*, vol. 22, no. S2, pp. 4375–4382, 2019.
- [13] A. Rani and B. Raman, "An image copyright protection system using chaotic maps," *Multimedia Tools and Applications*, vol. 76, no. 2, pp. 3121–3138, 2016.
- [14] G. Gao and G. Jiang, "Bessel-fourier moment-based robust image zero-watermarking," *Multimedia Tools and Applications*, vol. 74, no. 3, pp. 841–858, 2015.
- [15] P. T. Yap, X. Jiang, and A. C. Kot, "Two-dimensional polar harmonic transforms for invariant image representation," *IEEE Transactions on Pattern Analysis & Machine Intelligence*, vol. 32, no. 7, pp. 1259–1270, 2010.
- [16] P. Kaur, H. Pannu, and A. K. Malhi, "Comprehensive study of continuous orthogonal moments—a systematic review," *ACM Computing Surveys*, vol. 52, no. 4, p. 30, 2019.
- [17] M. R. Teague, "Image-analysis via the general-theory of moments," *Journal of the Optical Society of America*, vol. 69, no. 8, p. 1468, 1980.
- [18] Z. Shao, Y. Shang, Y. Zhang, X. Liu, and G. Guo, "Robust watermarking using orthogonal fourier-mellin moments and chaotic map for double images," *Signal Processing*, vol. 120, no. 3, pp. 522–531, 2016.
- [19] C. P. Wang, X. Y. Wang, and X. J. Chen, "Robust zero-watermarking scheme based on polar complex exponential transform and logistic mapping," *Multimedia Tools and Applications*, vol. 76, pp. 26355–26376, 2017.
- [20] Z. Xia, X. Wang, X. Li et al., "Efficient copyright protection for three CT images based on quaternion polar harmonic Fourier moments," *Signal Processing*, vol. 164, pp. 368–379, 2019.
- [21] Z. Xia, X. Wang, W. Zhou, R. Li, C. Wang, and C. Zhang, "Color medical image lossless watermarking using chaotic system and accurate quaternion polar harmonic transforms," *Signal Processing*, vol. 157, pp. 108–118, 2019.
- [22] C.-P. Wang, X.-Y. Wang, Z.-Q. Xia, C. Zhang, and X.-J. Chen, "Geometrically resilient color image zero-watermarking algorithm based on quaternion Exponent moments," *Journal of Visual Communication and Image Representation*, vol. 41, pp. 247–259, 2016.
- [23] Z. Xia, X. Wang, M. Wang et al., "Geometrically invariant color medical image null-watermarking based on precise quaternion polar harmonic Fourier moments," *IEEE Access*, vol. 7, pp. 122544–122560, 2019.
- [24] H.-Y. Yang, S.-R. Qi, P.-P. Niu, and X.-Y. Wang, "Color image zero-watermarking based on fast quaternion generic polar complex exponential transform," *Signal Processing: Image Communication*, vol. 82, Article ID 115747, 2020.
- [25] Z. Shao, Y. Shang, R. Zeng, H. Shu, G. Coatrieux, and J. Wu, "Robust watermarking scheme for color image based on quaternion-type moment invariants and visual

- cryptography,” *Signal Processing: Image Communication*, vol. 48, pp. 12–21, 2016.
- [26] K. Clark, B. Vendt, K. Smith et al., “The cancer imaging archive (TCIA): maintaining and operating a public information repository,” *Journal of Digital Imaging*, vol. 26, no. 6, pp. 1045–1057, 2013.