Efficient copyright protection for three CT images based on quaternion polar harmonic Fourier moments

Zhiqiu Xia, Xingyuan Wang, Xiaoxiao Li, Chunpeng Wang, Salahuddin Unar, Mingxu Wang, Tingting Zhao

*Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116023, China
School of Information, Qilu University of Technology (Shandong Academy of Sciences), Jinan 250353, China
School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China
 Liaoning Energy Investment (Group) Co., Ltd, Shenyang 110136, China
College of Information, Shenyang Institute of Engineering, Shenyang 110136, China

ABSTRACT

The current zero-watermarking scheme mainly offers the copyright protection to one image. Although the scheme can be used for many images repeatedly, the repeat operation requires a lot of time and large storage space. Using the quaternion polar harmonic Fourier moments (QPHFM), the paper considers three CT images as a whole to construct the key image and proposes a robust zero-watermarking algorithm offering the copyright protection to three CT images simultaneously, improving the efficiency of watermarking system and saving the storage space. The algorithm first considers the three CT images as three imaginary parts of an array of pure quaternion and calculates their QPHFM and then constructs the watermark image using the amplitude of QPHFM, and finally makes the chaotic scrambling to the feature image and then the XOR operation to the feature image and watermark image to generate key image. Experiment results prove the proposed scheme can resist common image processing attacks and geometric attacks effectively and thus can be well applied to the copyright protection of three images.

© 2019 Elsevier B.V. All rights reserved.

1. Introduction

Nowadays the medical digital information construction of hospital is accelerating, in which case digital medical images, such as computed tomography (CT), ultrasonic imaging (US) and nuclear magnetic resonance imaging (NMRI), have become the important reference for doctors to determine patients' physical conditions. The images may be intercepted during the network transmission and thus face security problems. How to enhance the medical digital information system's robustness, especially effectively ensuring medical images' reliability, availability and confidentiality, has become an urgent problem. Some techniques are proposed to resolve the image security issues in recent years, including image encryption technology [1,2] and digital watermarking technology [3–5], etc. In which digital watermarking technology is mainly used to achieve the copyright protection of digital images. It embeds featured or significant digital information into medial images. Its unique robustness and security ensures that the watermark can be extracted reliably and completely from the image after data processing, and thus achieves the expected result of copyright protection, completeness certification, and so on. However, the watermark information embedded may destroy the completeness of medical image. The medical image contains some important pathological information and any change may affect the doctor's pathological judgment. Therefore, designing a lossless medical image copyright protection scheme is very crucial.

In 2001, Wen et al. [6] proposed the concept of zero-watermarking. The zero-watermarking means constructing the watermark information using the image's key features without changing the image. It's theoretical basis is each image has different features, so each image has its watermark information different from that of other images. The zero-watermarking technology has the following advantages: (1) it does not change the original image, i.e., having the good imperceptibility; (2) it has the strong robustness, i.e., the zero-watermarking technology balances the robustness of digital watermark algorithm, the amount of embedded information of watermark, and the imperceptibility perfectly. The advantages above decide the zero-watermarking's applicability to medical images, because the technology ensures images' completeness while protecting the copyright effectively.
The research on zero-watermarking method has made great progress in recent years, but current zero-watermarking scheme mainly offers the copyright protection to one image. Although it can be used to many images repeatedly, the repeat operation requires a lot of time and large storage space. However, in CT images, the same part of body is generally collected with many images, so how to realize the simultaneous copyright protection of many CT images of the same part of body is crucial. In this case, the paper considers three CT images as a whole using QPHFM and proposes a zero-watermarking scheme realizing the simultaneous copyright protection of three CT images. The scheme first considers the three CT images as three imaginary parts of an array of pure quaternion and calculates their QPHFM and then constructs feature image using the amplitude of QPHFM, and finally makes the chaotic scrambling to the feature image and then the XOR operation to the feature image and watermark image to generate key image. The scheme realizes the copyright protection of three images simultaneously, improves the efficiency of watermarking system and saves storage space. The experiment results show the scheme can resist common image processing attacks and geometric attacks effectively and thus can be well applied to the copyright protection of three images.

The rest of the paper is organized as follows: Section 2 expands the related works of zero-watermarking technology; Section 3 introduces the QPHFM of three different images; Section 4 describes the zero-watermarking scheme proposed in details; Section 5 analyzes a series of experiments verifying the performance of the scheme; finally, Section 6 summarizes the paper.

2. Related works

Zero-watermarking was first proposed by Wen et al. [6]. They constructed the zero-watermark image using feature information after the digital images’ discrete cosine transform (DCT), overcame statistical attacks and verified the feasibility of zero-watermarking algorithm. Later, they proposed constructing the zero-watermark using the high-order cumulants in scheme [7]. The scheme made a comparative analysis on the two methods constructing zero-watermark using DCT and the high-order cumulants respectively. The analysis results show that constructing zero-watermark using the high-order cumulants has the better robustness than constructing zero-watermark using DCT in terms of common signal processing like noise and filtering and small-angle rotations. Chen et al. [8] proposed a wavelet-domain-based image copyright protection algorithm applied to public copyright certification. The algorithm extracts the original image’s feature matrix from the low-frequency range of wavelet domain and considers the matrix as the watermark matrix, and then sends the watermark matrix and cryptographic parameters to a reliable third-party certification authority TA and adds a timestamp. The algorithm can effectively resist interpretation attacks and shows the strong robustness to common image processing attacks and geometric attacks. Chang and Lin [9] improved the feature extraction method based on the algorithm, made the Sobel edge detection to the low-scale approximate image of host image and extracted the feature matrix, getting a good result. Boyer et al. [10] proposed a distortion compensated-quantization index modulation (DC-QIM) zero-watermarking algorithm, used the large deviation theory to evaluate the performance of algorithm through the receiver operating feature (ROC) and the total probability of detection error. In the comparison with quantized projection (QP) and spread spectrum (SS), the DC-QIM method showed its superiority. Tsai et al. [11] proposed an effective zero-watermarking algorithm based on the α-trimmed mean algorithm and the support vector machine (SVM). The algorithm uses the α-trimmed mean algorithm to remove noise to enhance the precision of feature selection, and records the relationship between feature information and watermark using a well-trained SVM model. Basing on [11], they [12] proposed a geometric-attack-resistant zero-watermarking algorithm based on the SVM and the particle swarm optimization (PSO) resisting image rotation, scaling and translation attacks effectively. Rawat and Raman [13] proposed a zero-watermarking scheme based on the fractional Fourier transform (FrFT) and the visual cryptography (VC). The scheme constructs the master share and the ownership share using the visual secret sharing. The master share is expressed with the image features extracted through singular value decomposition. The ownership share can be obtained by processing the master share and a significant secret image using the VC technology. Then, the ownership share is sent to TA for storage. Basing on the Bessel-Fourier moments (BFMs), Gao and Jiang [14] proposed a robustness visual zero-watermarking algorithm. The algorithm first makes the translation and scaling normalization of image and calculates the BFM of normalized image, and then converts the amplitude into a binary feature image and makes the XOR operation to the image and the logo image to generate a verification image, and finally stores the verification image in TA. The algorithm can resist many kinds of attacks and its performance is better than other visual zero-watermarking algorithms and the algorithm based on Zernike moment. Sun et al. [15] proposed a space domain zero-watermarking algorithm based on the generalized Arnold transform (GAT). The algorithm first scrambles the original logo image using the GAT and then gets the binary feature matrix from the original image according to quantization embedding rules, and finally gets the key image by making the XOR operation to the scrambled logo image and feature matrix using the spread spectrum technology. Based on the quaternion Exponent moments (QEMs) and the polar complex exponential transform (PCET), Wang et al. [16,17] proposed two kinds of robust zero-watermarking algorithms for color images and grayscale images to resist various geometric attacks and conventional image processing attacks effectively. Shao et al. [18] proposed a double-image robust zero-watermarking scheme based on the orthogonal Fourier–Mellin moments (OFMM) and the chaotic map and realized the simultaneous copyright protection of two images. The scheme uses the invariant of OFMM to construct the feature image and adds the scrambling watermark to generate a verification image, and improves the security of system using chaotic mapping. Thanh and Tanaka [19] proposed a robustness zero-watermarking algorithm based on the visual map feature (VMF) and the permuted visual map feature (PVMF). The algorithm’s main idea is combining the QR decomposition with the one-dimension DCT to extract the features of image’s robustness. The algorithm improves the robustness of zero-watermarking and reduces calculation cost using the proposed VMF and PVMF. Liu et al. [20] proposed an improved vector-map zero-watermarking scheme. The scheme solves the problem of interpretation attack by adding a timestamp to watermark image sequence and shows the good robustness for geometric attacks. Kavitha and Sakhivel [21] proposed two zero-watermarking algorithms specific for medical image certification and discussed the two algorithms based on the singular value decomposition (SVD) and the contourlet transform-singular value decomposition (CT-SVD). The two algorithms have good security and robustness and are applicable to the copyright protection of medical images effectively.

3. Quaternion polar harmonic Fourier moments

According to the quaternion theory, we can consider three CT images of the same size as three imaginary parts of an array of pure quaternion. Therefore, we can express the three CT images in the form of an array of pure quaternion:

\[ f(r, θ) = f_1(r, θ)i + f_2(r, θ)j + f_3(r, θ)k. \]  

(1)
where \( f_1(r, \theta), f_2(r, \theta) \) and \( f_3(r, \theta) \) are three CT images. In this way, we can consider the three images as a vector and describe them as a whole.

Because the multiplication of quaternions is not commutative, the quaternion polar harmonic Fourier moments (QPHFM) [22] of \( f(r, \theta) \) with the order of \( n = 0, 1, \ldots, \infty \) and the repetition of \( m|m| = 0, 1, \ldots, \infty \) has two forms:

\[
P_{nm}^p = \frac{2}{\pi} \int_0^{2\pi} \int_0^1 T_n(r) \exp(-\mu m\theta) f(r, \theta) r dr d\theta, \tag{2}
\]

\[
P_{nm}^q = \frac{2}{\pi} \int_0^{2\pi} \int_0^1 T_n(r) f(r, \theta) \exp(-\mu m\theta) r dr d\theta, \tag{3}
\]

where \( \mu = \alpha i + \beta j + \gamma k \) is a unit pure quaternion. In this paper, \( \mu \) is set to \( \mu = (i + j + k)/\sqrt{3} \), unless otherwise specified. In the two forms above, the Fourier factor \( \exp(-\mu m\theta) \) is placed on the left and right side of \( f(r, \theta) \), so \( P_{nm}^p \) and \( P_{nm}^q \) are called the left QPHFM and the right QPHFM respectively. Taking the left QPHFM as an example, QPHFM of \( f(r, \theta) \) can be obtained from the PHFM of three images \( f_1(r, \theta), f_2(r, \theta) \) and \( f_3(r, \theta) \):

\[
P_{nm}^p = A_{nm} + iB_{nm} + jC_{nm} + kD_{nm} \tag{4}
\]

With

\[
A_{nm} = -\alpha \text{Im}(P_{nm}(f_1)) - \beta \text{Im}(P_{nm}(f_2)) - \gamma \text{Im}(P_{nm}(f_3))
\]

\[
B_{nm} = \text{Re}(P_{nm}(f_1)) + \beta \text{Im}(P_{nm}(f_2)) - \gamma \text{Im}(P_{nm}(f_3))
\]

\[
C_{nm} = \text{Re}(P_{nm}(f_2)) + \alpha \text{Im}(P_{nm}(f_1)) - \gamma \text{Im}(P_{nm}(f_3))
\]

\[
D_{nm} = \text{Re}(P_{nm}(f_3)) + \alpha \text{Im}(P_{nm}(f_1)) + \beta \text{Im}(P_{nm}(f_2)).
\]

where \( \text{Re}(p) \) and \( \text{Im}(p) \) are the real part and the imaginary part of complex number \( p \) respectively.

According to the principle of orthogonal function, the image can be reconstructed with the infinite orthogonal function sequence [23]. Therefore, after getting the QPHFM, we can reconstruct \( f(r, \theta) \) approximately using finite QPHFM. The reconstruction formulas using the left QPHFM and the right QPHFM are as follows:

\[
f'(r, \theta) = \sum_{n=0}^{n_{\max}} \sum_{m=-m_{\max}}^{m_{\max}} T_n(r) \exp(\mu m\theta) P_{nm}^p. \tag{6}
\]

\[
f'(r, \theta) = \sum_{n=0}^{n_{\max}} \sum_{m=-m_{\max}}^{m_{\max}} T_n(r) P_{nm}^p \exp(\mu m\theta). \tag{7}
\]

Taking the left QPHFM as an example, the reconstruction of \( f(r, \theta) \) can be obtained from the reconstruction of three images \( f_1(r, \theta), f_2(r, \theta) \) and \( f_3(r, \theta) \):

\[
f'(r, \theta) = f_1' f_1(r, \theta) + f_2' f_2(r, \theta) + f_3' f_3(r, \theta) + k f_3'(r, \theta) \tag{8}
\]

With

\[
f_1'(r, \theta) = \text{Re}(A'_{nm}) - \alpha \text{Im}(B'_{nm}) - \beta \text{Im}(C'_{nm}) - \gamma \text{Im}(D'_{nm})
\]

\[
f_2'(r, \theta) = \alpha \text{Im}(A'_{nm}) + \beta \text{Im}(B'_{nm}) - \gamma \text{Im}(C'_{nm})
\]

\[
f_3'(r, \theta) = \beta \text{Im}(A'_{nm}) + \alpha \text{Im}(B'_{nm}) - \gamma \text{Im}(C'_{nm})
\]

\[
(f_3'(r, \theta) = \gamma \text{Im}(A'_{nm}) - \alpha \text{Im}(B'_{nm}) + \beta \text{Im}(C'_{nm}). \tag{9}
\]

where \( f_1'(r, \theta), f_2'(r, \theta) \) and \( f_3'(r, \theta) \) are reconstructed three images, \( A'_{nm}, B'_{nm}, C'_{nm} \) and \( D'_{nm} \) are the reconstructed matrices with PHFM [22] from \( A_{nm}, B_{nm}, C_{nm} \) and \( D_{nm} \) and \( f_3'(r, \theta) = 0 \).

Fig. 1 gives the three CT images’ reconstruction images of QPHFM with the maximum order of 50 and the corresponding reconstruction error images. Results show that after the QPHFM reconstruction, the three images are very close to the original images, indicating the QPHFM theory of three different images is entirely feasible.

\[\text{Fig. 1. Three medical images’ QPHFM reconstruction images with the maximum order of 50 and the corresponding reconstruction error images.}\]

\[\text{4. Proposed scheme}\]

Suppose \( f_1(r, \theta), f_2(r, \theta) \) and \( f_3(r, \theta) \) are three grayscale CT images with the size of \( N \times N \). \( W \) is a watermark image with the size of \( P \times Q \). The proposed scheme consists of two stages: watermark embedding and watermark extraction. In watermark embedding, the QPHFM of original three CT images are computed, then the QPHFM amplitudes are used to construct feature image, and finally the watermark image is embedded by applying an exclusive OR operation between watermark image and scrambled feature image. Watermark extraction is the inverse process of watermark embedding, which is mainly used to validate copyright of three CT images. Different from conventional watermarking methods, there are three roles in our scheme: Embedder, Extractor and Intellectual Property Rights (IPR) Center. The embedder constructs the key image of the original image, the IPR center stores the constructed hash value from embedder, and the extractor checks the copyright of the original image.

\[\text{4.1. Watermark embedding}\]

The watermark embedding process mainly aims to construct the key image and store the key image in the copyright certification protection center. The embedding procedure is composed of seven steps:

\[\text{Step 1: Calculate the QPHFM.}\]

Consider the three original three CT images \( f_1(r, \theta), f_2(r, \theta) \) and \( f_3(r, \theta) \) as the three imaginary parts of pure quaternion and calculate the three CT images’ QPHFM with the
maximum order of $n_{\text{max}}$ using Eq. (2), and obtain $(n_{\text{max}} + 1)(2n_{\text{max}} + 1)$ moments.

**Step 2: Random select moments.**
Select $P \times Q$ moments $M = (m_i, 0 \leq i < P \times Q)$ randomly from the $(n_{\text{max}} + 1)(2n_{\text{max}} + 1)$ moments above according to a pseudo random sequence using the secret key $K_1$.

**Step 3: Generate the two-dimension feature matrix.**
Calculate the amplitude of $M$ and obtain $P \times Q$ amplitudes $A = (a_i, 0 \leq i < P \times Q)$ as image features, and then raise it to the two-dimension feature matrix $V = (v_{i,j}, 0 \leq i < P, 0 \leq j < Q)$.

**Step 4: Construct the perceptual hash sequence.**
Calculate the matrix $V$ column by column to get the mean of amplitude and compare each amplitude in the column vector with the mean to determine the sequence element. The amplitude element equal or greater than the mean is recorded as 1; otherwise, the amplitude element is recorded as 0. In this way, all elements obtained are scanned into sequences and then form the perceptual hash sequence $H = (h_{i,j}, 0 \leq i < P, 0 \leq j < Q)$.

**Step 5: Logistic scrambling encryption.**
Encrypt perceptual hash sequence to enhance the security of our scheme [24]. Use logistic mapping [25] with the initial value of $x_0$ to generate the chaotic sequence $L$ with the length of $P \times Q$. The definition of logistic mapping is as follows:

$$x_{i+1} = \lambda x_i(1-x_i), \quad i = 0, 1, 2, \ldots , \quad (10)$$

where $x_i$ is a number between 0 and 1, $0 \leq \lambda < 4$ is the control parameter of logistic system. Most values of $\lambda$ beyond 3.5699456 exhibit chaotic behavior. In this paper, $\lambda = 4$.

Then convert the chaotic sequence $L$ into the binary sequence $L'$:

$$L' = \begin{cases} 0, & L \leq \text{Threshold} \\ 1, & L > \text{Threshold} \end{cases} \quad (11)$$

in which Threshold is the mean of $L$. Make the XOR operation to binary sequence $L'$ and $H$ to get the chaotic sequence $H'$:

$$H' = L' \oplus H. \quad (12)$$

**Step 6: Watermark embedding.**
Make the XOR operation to chaotic sequence $H'$ and watermark $W$ and finally generate the key image $K = (k_{i,j}, 0 \leq i < P, 0 \leq j < Q)$. The owner of original host image has the management right of key image and can extract the watermark. In the algorithm, the watermark is connected to the host image and stored as the secret key for watermark extraction rather than being embedded into the host image.

$$K = H' \oplus W. \quad (13)$$

**Step 7: Hash operation.**
To further enhance the security of the scheme, we employ hash operation on the key image $K$, secret key $K_1$ and initial value of logistic mapping $x_0$, and obtain the hash value $HV$:

$$HV = HF(K, K_1, x_0), \quad (14)$$

where $HF$ is the one-way hash function. Then the hash value $HV$ is stored in intellectual property rights (IPR) center for copyright protection.

4.2. Watermark extraction

Suppose $f_1(r, \theta)$, $f_2(r, \theta)$ and $f_3(r, \theta)$ are three CT images to be verified with the size of $N \times N$. The watermark extraction process mainly aims to determine the ownership of copyright of the image to be verified. The extraction procedure consists of six steps: Calculate the QPHFM, Random select moments, Generate the two-dimension feature matrix, Construct the perceptual hash sequence, Logistic scrambling encryption and Watermark extraction. The specific process of watermark extraction is as follows:

**Step 1: Calculate the QPHFM.**
Consider the three CT images to be verified as the three imaginary parts of an array of pure quaternion and calculate the three CT images’ QPHFM with the maximum order of $n_{\text{max}}$, and then get $(n_{\text{max}} + 1)(2n_{\text{max}} + 1)$ moments.

**Step 2: Random select moments.**
Select $P \times Q$ moments $\hat{M} = (\hat{m}_i, 0 \leq i < P \times Q)$ randomly from the $(n_{\text{max}} + 1)(2n_{\text{max}} + 1)$ moments above according to a pseudo random sequence using the secret key $K_1$.

**Step 3: Generate the two-dimension feature matrix.**
Calculate the amplitude of $\hat{M}$ and obtain $P \times Q$ amplitudes $\hat{A} = (\hat{a}_i, 0 \leq i < P \times Q)$ as image features, and then raise it to the two-dimension feature matrix $\hat{V} = (\hat{v}_{i,j}, 0 \leq i < P, 0 \leq j < Q)$.

**Step 4: Construct the perceptual hash sequence.**
Calculate the matrix $\hat{V}$ column by column to get the mean of amplitude and compare each amplitude in the column vector with the mean to determine the sequence element. The amplitude element equal or greater than the mean is recorded as 1; otherwise, the amplitude element is recorded as 0. In this way, all elements obtained are scanned into sequences and then the perceptual hash sequence $\hat{H} = (\hat{h}_{i,j}, 0 \leq i < P, 0 \leq j < Q)$ is formed.

**Step 5: Logistic scrambling encryption.**
Use logistic mapping with the initial value of $x_0$ to generate the chaotic sequence $\hat{L}$ with the length of $P \times Q$, and then convert the chaotic sequence generated into the binary sequence $\hat{L}'$ and make the XOR operation to binary sequence
selected amplitude 5.1. on images.

5. Experiment results

The paper uses 99 CT images of the size of 512 × 512 from database The Cancer Imaging Archive (TCIA) [26] as the original host images. In the experiments, the images are divided into 33 groups of which 4 groups are shown in Fig. 3. We use a binary image of 32 × 32 as the watermark image.

5.1. Selection of the order of QPHFM

The algorithm constructs the zero-watermark using the amplitude of QPHFM. The algorithm’s watermark capacity depends on the number of moments, and the number of moments is decided by the maximum order of moment, i.e. $N_{QPHFM} = (\text{max} + 1)(2n_{\text{max}} + 1)$, so the watermark capacity is decided by the maximum order of moment, as shown in Fig. 4. In the paper, the size of watermark image is 32 × 32, so the maximum order of QPHFM selected is 25.

5.2. Robustness

5.2.1. Robustness to various attacks

The section uses the first group of test images to measure the algorithm’s robustness to various attacks. The peak signal-to-noise ratio (PSNR) [27,28] is used to measure the degree of distortion of image attacked. The smaller the PSNR is, the bigger the degree of distortion of image attacked is. After various attacks, the three CT images’ PSNR values are expressed with PSNR1, PSNR2 and PSNR3. We use the accuracy rate (AR) to measure the robustness of algorithm. The higher the AR is, the closer the watermark extracted is to the original watermark, i.e., the better the robustness is. The AR is defined as follows:

$$\text{AR} = \frac{\text{Number of correct retrieved bits}}{\text{Number of logo image bits}} \times 100\%.$$  

The algorithm uses three images $f_1(r, \theta)$, $f_2(r, \theta)$ and $f_3(r, \theta)$ simultaneously to construct the key image, so when testing its robustness, the attacks to images can be divided into the following seven cases: the attack to $f_1$ alone, the attack to $f_2$ alone, the attack to $f_3$ alone, the attack to both $f_1$ and $f_2$, the attack to both $f_1$ and $f_3$, the attack to both $f_2$ and $f_3$, and the attack to $f_1$, $f_2$ and $f_3$ simultaneously.

(1) JPEG compression

To test the algorithm’s ability of resistance to JPEG compression, we make JPEG compression attacks with compression quality factors (Q) 10%, 30%, 50% and 70% to the images. Fig. 5 shows the images after JPEG compression attacks. Table 1 shows the robustness. The experimental results in Table 1 show that the ARs of watermarks extracted from images after the JPEG compression are all greater than 0.98, indicating the algorithm has a good ability of resistance to JPEG compression.

(2) Noise attacks

We add the Gaussian noise and the salt & pepper noise with different variances to the images respectively to test whether the algorithm can resist noise attacks effectively. Fig. 6 shows the images after noise attacks. Table 2 shows the corresponding robustness results. The experimental data in Table 2 shows that with the increase in the noise variance, the AR of watermark extracted decreases. However, the ARs of watermarks extracted from test images under different Gaussian noise and salt & pepper noise are all greater than 0.96, indicating the algorithm has the strong robustness to noise attacks.

![Fig. 3. Four groups of original images.](image-url)
Table 1
AR to JPEG compression attacks.

<table>
<thead>
<tr>
<th>Attack</th>
<th>$f_1$</th>
<th>$f_2$</th>
<th>$f_3$</th>
<th>$f_1, f_2$</th>
<th>$f_1, f_3$</th>
<th>$f_2, f_3$</th>
<th>$f_1, f_2, f_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>JPEG 10%</td>
<td>0.9912</td>
<td>0.9873</td>
<td>0.9912</td>
<td>0.9873</td>
<td>0.9898</td>
<td>0.9883</td>
<td>0.9844</td>
</tr>
<tr>
<td>JPEG 30%</td>
<td>0.9971</td>
<td>0.9941</td>
<td>0.9951</td>
<td>0.9941</td>
<td>0.9932</td>
<td>0.9951</td>
<td>0.9922</td>
</tr>
<tr>
<td>JPEG 50%</td>
<td>0.9980</td>
<td>0.9980</td>
<td>0.9980</td>
<td>0.9961</td>
<td>0.9971</td>
<td>0.9951</td>
<td>0.9932</td>
</tr>
<tr>
<td>JPEG 70%</td>
<td>0.9971</td>
<td>0.9971</td>
<td>0.9980</td>
<td>0.9961</td>
<td>0.9971</td>
<td>0.9961</td>
<td>0.9961</td>
</tr>
</tbody>
</table>

Fig. 5. PSNR to JPEG compression attacks.

Table 2
AR to noise attacks.

<table>
<thead>
<tr>
<th>Attack</th>
<th>$f_1$</th>
<th>$f_2$</th>
<th>$f_3$</th>
<th>$f_1, f_2$</th>
<th>$f_1, f_3$</th>
<th>$f_2, f_3$</th>
<th>$f_1, f_2, f_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaussian noise 0.02</td>
<td>0.9844</td>
<td>0.9795</td>
<td>0.9883</td>
<td>0.9736</td>
<td>0.9863</td>
<td>0.9795</td>
<td>0.9746</td>
</tr>
<tr>
<td>Gaussian noise 0.03</td>
<td>0.9805</td>
<td>0.9775</td>
<td>0.9844</td>
<td>0.9727</td>
<td>0.9776</td>
<td>0.9697</td>
<td>0.9717</td>
</tr>
<tr>
<td>Salt &amp; pepper noise 0.02</td>
<td>0.9844</td>
<td>0.9902</td>
<td>0.9883</td>
<td>0.9854</td>
<td>0.9834</td>
<td>0.9834</td>
<td>0.9824</td>
</tr>
<tr>
<td>Salt &amp; pepper noise 0.03</td>
<td>0.9834</td>
<td>0.9873</td>
<td>0.9863</td>
<td>0.9805</td>
<td>0.9805</td>
<td>0.9805</td>
<td>0.9697</td>
</tr>
</tbody>
</table>

Fig. 6. PSNR to noise attacks.

(3) Image filtering

This part makes three filtering attacks to the images, including the average filtering, the Gaussian filtering and the median filtering. Fig. 7 shows the images after filtering attacks. Table 3 shows the results of watermarks extracted. We can see from the table that the median filtering has a great influence on the algorithm, of which the minimum AR is 0.9463; the ARs in the cases of Gaussian filtering and mean filtering are greater than 0.99 and 0.96, respectively. The results indicate the algorithm has a good ability of resistance to filtering attacks as a whole.

(4) Image rotation

This part rotates the test images to test the algorithm's resistance to rotation attacks. We set the rotation angles to be 5°, 15°, 30° and 45°. Fig. 8 shows that images after rotation attacks. Table 4 shows the robustness results. It can be seen that the ARs of watermarks extracted from $f_1$, $f_2$ and $f_3$ after rotations are all greater than 0.99, indicating the algorithm has a good ability of resistance to rotation attacks. However, the ARs of watermarks extracted in the case of attacks to only one image or two images are poor, and the minimum AR is 0.90. The reason is that rotating only one or
**Table 3**

AR to filtering attacks.

<table>
<thead>
<tr>
<th>Attack</th>
<th>$f_1$</th>
<th>$f_2$</th>
<th>$f_3$</th>
<th>$f_1, f_2$</th>
<th>$f_2, f_3$</th>
<th>$f_1, f_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Median filtering 3 x 3</td>
<td>0.9912</td>
<td>0.9863</td>
<td>0.9873</td>
<td>0.9873</td>
<td>0.9824</td>
<td>0.9834</td>
</tr>
<tr>
<td>Median filtering 5 x 5</td>
<td>0.9785</td>
<td>0.9638</td>
<td>0.9775</td>
<td>0.9600</td>
<td>0.9629</td>
<td>0.9570</td>
</tr>
<tr>
<td>Gaussian filtering 3 x 3</td>
<td>0.9900</td>
<td>0.9951</td>
<td>0.9971</td>
<td>0.9961</td>
<td>0.9971</td>
<td>0.9951</td>
</tr>
<tr>
<td>Gaussian filtering 5 x 5</td>
<td>0.9900</td>
<td>0.9951</td>
<td>0.9971</td>
<td>0.9961</td>
<td>0.9971</td>
<td>0.9951</td>
</tr>
<tr>
<td>Average filtering 3 x 3</td>
<td>0.9951</td>
<td>0.9873</td>
<td>0.9922</td>
<td>0.9873</td>
<td>0.9883</td>
<td>0.9873</td>
</tr>
<tr>
<td>Average filtering 5 x 5</td>
<td>0.9863</td>
<td>0.9746</td>
<td>0.9863</td>
<td>0.9756</td>
<td>0.9805</td>
<td>0.9688</td>
</tr>
</tbody>
</table>

**Table 4**

AR to image rotation.

<table>
<thead>
<tr>
<th>Attack</th>
<th>$f_1$</th>
<th>$f_2$</th>
<th>$f_3$</th>
<th>$f_1, f_2$</th>
<th>$f_2, f_3$</th>
<th>$f_1, f_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rotation 5</td>
<td>0.9541</td>
<td>0.9395</td>
<td>0.9414</td>
<td>0.9463</td>
<td>0.9492</td>
<td>0.9404</td>
</tr>
<tr>
<td>Rotation 15</td>
<td>0.9209</td>
<td>0.9053</td>
<td>0.9036</td>
<td>0.9092</td>
<td>0.9082</td>
<td>0.9063</td>
</tr>
<tr>
<td>Rotation 30</td>
<td>0.9316</td>
<td>0.9170</td>
<td>0.9229</td>
<td>0.9297</td>
<td>0.9160</td>
<td>0.9395</td>
</tr>
<tr>
<td>Rotation 45</td>
<td>0.9316</td>
<td>0.9180</td>
<td>0.9063</td>
<td>0.9082</td>
<td>0.9219</td>
<td>0.9248</td>
</tr>
</tbody>
</table>

Fig. 7. PSNR to filtering attacks.

Fig. 8. PSNR to image rotation.
two images may destroy the inner links of three images and then reduce the QPHFM accuracy calculated, thus causing the poor robustness.

(5) Image scaling

This part makes a scaling test to the images. The scaling in the paper means scaling the image by some factors and then resuming the original size. We attack the images in the form of scaling by the factor of 0.5, 0.75, 1.25 and 1.5, respectively. Fig. 9 shows the images after scaling attacks. Table 5 shows the extracted watermarks’ ARs to image scaling. The table shows that the ARs of watermarks extracted are all greater than 0.97, i.e., the algorithm has the strong robustness to image scaling.

(6) Image cropping

The image cropping is one of the most common geometric attacks, directly cropping the image to remove some part of the image and thus causing an incomplete image. A large area of cropping may cause the difficulty in watermark extraction and then affect the quality of watermark directly. This section makes cropping attacks to images to different degrees (the left corner: cropping 1/16, 1/8, 1/4 and 1/2). Fig. 10 shows the images after cropping. The ARs of watermarks extracted are shown in Table 6. We can see that the algorithm can extract watermark information perfectly when cropping 1/16 or 1/8. When the cropping degree is 1/4 or 1/2, the extracted watermark information deteriorates. The reason is that the QPHFM used in the scheme is based on the inscribed circle, and the cropping of image corners does not change the content of inscribed circle when the cropping degree is lower than $1 - \sqrt{2}/4$. Once the cropping degree exceeds $(2 - \sqrt{2})/4$, the content of the inscribed circle is destroyed, resulting in inaccurate calculation of QPHFM, thus affecting the extracted watermark information. In summary, the proposed scheme can resist a certain degree of image cropping on the four corners of the image. For large degree of cropping on the four corners or the cropping on the image center, the robustness of the proposed scheme will deteriorate. In the future work, we will try our best to solve this problem so that it can resist the cropping attack of all positions and degrees.

(7) Multiple attacks

Images are vulnerable to multiple attacks during transmission. Here we add multiple attacks to the image to further test the robustness of the algorithm. The images after multiple attacks are shown in Fig. 11, and the AR results of the extracted watermarks are shown in the last column of Table 7, in which the robustness is measured with the AR of watermark extracted in the case of the simultaneous attack to $f_1$, $f_2$ and $f_3$. Moreover, Table 7 also shows the AR results of the scheme subjected to a single attack, column 5–8 corresponds to Attack1–Attack4, respectively. It can be seen from Table 7 that the result of suffering multiple attacks is slightly worse than that of suffering single attack. However, all the ARs are greater than 0.96. This means the proposed scheme can resist multiple attacks very well, which further verifies the good performance of the proposed scheme.

5.2.2. Comparison of watermark performance

To show the superiority of the scheme proposed, we compare the scheme with five excellent image watermarking schemes
Fig. 10. PSNR to image cropping.

(a) Cropping 1/16: PSNR1=24.08, PSNR2=24.08, PSNR3=24.08
(b) Cropping 1/8: PSNR1=18.06, PSNR2=18.06, PSNR3=18.06
(c) Cropping 1/4: PSNR1=12.04, PSNR2=12.78, PSNR3=12.04
(d) Cropping 1/2: PSNR1=6.51, PSNR2=8.75, PSNR3=6.53

Fig. 11. PSNR to multiple attacks.

(a) JPEG (30%)+Gaussian noise (0.03)
(b) JPEG (50%)+Gaussian filtering (3×3)
(c) Average filtering (3×3)+Gaussian filtering (3×3)
(d) Gaussian filtering (3×3)+Rotation (30)
(e) Salt & pepper noise (0.03)+Scaling (1.25)
(f) Rotation (30)+Scaling (0.75)
(g) JPEG (30%)+Gaussian noise (0.02)+Median filtering (3×3)
(h) Salt & pepper noise (0.02)+Gaussian filtering (3×3)+Rotation (15)
(i) Average filtering (3×3)+Rotation (5)+Scaling (1.25)
(j) Rotation (45)+Scaling (0.75)+Gaussian noise (0.02)+JPEG (30%)
in which [8,9] are two representative zero-watermarking schemes. [16] is an image moment-based zero-watermarking scheme, [29] is a quaternion theory-based color image watermarking scheme and [30] is a robustness lossless medical image watermarking scheme applicable to electronic healthcare with the embedded factors $K = 10$ and $K = 20$. In the comparison experiments, the results are obtained by averaging the ARs of 33 groups of images. The comparison results with schemes [8,9,16] are shown in Table 8, and the comparison results with schemes [29,30] are shown in Table 9. It should be noted that the robustness of the scheme proposed is measured with the AR of watermark extracted in the case of the simultaneous attack to $f_1$, $f_2$ and $f_3$. In Table 8, we can see that the ARs in the proposed scheme are higher than the ARs in the schemes [8,9,16], which illustrates that the proposed scheme provides better robustness than schemes [8,9,16]. Table 9 shows that the proposed scheme provides the significantly better performance than schemes [29,30] under various attacks. For Gaussian noise and histogram equalization, the scheme proposed has small improvements in the robustness than schemes [29,30]. However, for salt & pepper noise, JPEG compression and image filtering, the robustness improves a lot. To sum up, the scheme proposed has the excellent robustness.

### 5.3 Efficiency analysis

In this section, we analyze in detail the efficiency of the proposed scheme and other schemes. We use the above 6 schemes to achieve copyright protection for 30 images. The PC used for the experiment has a 2.90 GHz Processor with 4 GB RAM and the operation system is Microsoft Windows 7 Ultimate. The experiment is conducted using MATLAB version 8.6. The average running time of 30 images is shown in Table 10, which shows the proposed scheme costs the least time. This is because the proposed scheme can achieve the copyright protection of three images at one time, and other algorithms need to be performed three times repeatedly. That is to say the proposed scheme can effectively shorten the running time and improve the efficiency.

In addition, from the perspective of space, the proposed scheme only generates one key image for three original images, while other algorithms need to generate three key images. Therefore, this

---

**Table 7** AR to multiple attacks.

<table>
<thead>
<tr>
<th>Attack</th>
<th>PSNR1</th>
<th>PSNR2</th>
<th>PSNR3</th>
<th>Attack1</th>
<th>Attack2</th>
<th>Attack3</th>
<th>Attack4</th>
<th>Multiple</th>
</tr>
</thead>
<tbody>
<tr>
<td>JPEG (30%) + Gaussian noise (0.03)</td>
<td>16.88</td>
<td>16.15</td>
<td>16.81</td>
<td>0.9902</td>
<td>0.9717</td>
<td>N/A</td>
<td>N/A</td>
<td><strong>0.9639</strong></td>
</tr>
<tr>
<td>JPEG (50%) + Gaussian filtering (3 x 3)</td>
<td>30.41</td>
<td>27.57</td>
<td>30.17</td>
<td>0.9932</td>
<td>0.9941</td>
<td>N/A</td>
<td>N/A</td>
<td><strong>0.9912</strong></td>
</tr>
<tr>
<td>Average filtering (3 x 3) + Gaussian filtering (3 x 3)</td>
<td>25.72</td>
<td>23.95</td>
<td>25.45</td>
<td>0.9854</td>
<td>0.9941</td>
<td>N/A</td>
<td>N/A</td>
<td><strong>0.9805</strong></td>
</tr>
<tr>
<td>Gaussian filtering (3 x 3) + Rotation (30)</td>
<td>14.30</td>
<td>12.02</td>
<td>13.81</td>
<td>0.9941</td>
<td>0.9941</td>
<td>N/A</td>
<td>N/A</td>
<td><strong>0.9902</strong></td>
</tr>
<tr>
<td>Salt &amp; pepper noise (0.031) + Scaling (1.25)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0.9897</td>
<td>0.9941</td>
<td>N/A</td>
<td>N/A</td>
<td><strong>0.9609</strong></td>
</tr>
<tr>
<td>Rotation (30) + Scaling (0.75)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0.9941</td>
<td>0.9912</td>
<td>N/A</td>
<td>N/A</td>
<td><strong>0.9814</strong></td>
</tr>
<tr>
<td>JPEG (30%) + Gaussian noise (0.02) + Median filtering (3 x 3)</td>
<td>23.17</td>
<td>21.90</td>
<td>23.19</td>
<td>0.9902</td>
<td>0.9746</td>
<td>0.9785</td>
<td>N/A</td>
<td><strong>0.9697</strong></td>
</tr>
<tr>
<td>Salt &amp; pepper noise (0.02) + Gaussian filtering (3 x 3) + Rotation (15)</td>
<td>14.75</td>
<td>13.20</td>
<td>14.80</td>
<td>0.9824</td>
<td>0.9941</td>
<td>0.9951</td>
<td>N/A</td>
<td><strong>0.9814</strong></td>
</tr>
<tr>
<td>Average filtering (3 x 3) + Rotation (5) + Scaling (1.25)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0.9854</td>
<td>0.9941</td>
<td>N/A</td>
<td>N/A</td>
<td><strong>0.9775</strong></td>
</tr>
<tr>
<td>Rotation (45) + Scaling (0.75) + Gaussian noise (0.02) + JPEG (30%)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0.9941</td>
<td>0.9912</td>
<td>0.9746</td>
<td>0.9902</td>
<td><strong>0.9629</strong></td>
</tr>
</tbody>
</table>

**Table 8** Comparison of the robustness (AR) between the proposed scheme and similar zero-watermarking schemes [8,9,16].

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>JPEG compression (30)</td>
<td>0.9932</td>
<td>0.9891</td>
<td>0.9916</td>
<td>0.9725</td>
</tr>
<tr>
<td>JPEG compression (70)</td>
<td>0.9973</td>
<td>0.9932</td>
<td>0.9952</td>
<td>0.9766</td>
</tr>
<tr>
<td>Rotation 5</td>
<td>0.9966</td>
<td>0.8175</td>
<td>0.6680</td>
<td>0.9794</td>
</tr>
<tr>
<td>Rotation 45</td>
<td>0.9932</td>
<td>0.8294</td>
<td>0.6845</td>
<td>0.9765</td>
</tr>
<tr>
<td>Scaling 0.25 and resizing to original size</td>
<td>0.9893</td>
<td>0.9908</td>
<td>0.9883</td>
<td>0.9562</td>
</tr>
<tr>
<td>Scaling 4 and resizing to original size</td>
<td>0.9961</td>
<td>0.9944</td>
<td>0.9912</td>
<td>0.9832</td>
</tr>
<tr>
<td>Median filtering (3 x 3)</td>
<td>0.9852</td>
<td>0.9836</td>
<td>0.9822</td>
<td>0.9751</td>
</tr>
<tr>
<td>Gaussian filtering (3 x 3)</td>
<td>0.9950</td>
<td>0.9925</td>
<td>0.9908</td>
<td>0.9759</td>
</tr>
<tr>
<td>Gaussian noise (0.01)</td>
<td>0.9756</td>
<td>0.9715</td>
<td>0.9715</td>
<td>0.9656</td>
</tr>
<tr>
<td>Salt &amp; pepper noise (0.03)</td>
<td>0.9971</td>
<td>0.9535</td>
<td>0.9302</td>
<td>0.9554</td>
</tr>
<tr>
<td>Upper left corner cropping (1/16)</td>
<td>1.0000</td>
<td>0.8902</td>
<td>0.8257</td>
<td>1.0000</td>
</tr>
<tr>
<td>Upper left corner cropping (1/8)</td>
<td>1.0000</td>
<td>0.8742</td>
<td>0.7744</td>
<td>1.0000</td>
</tr>
</tbody>
</table>

**Table 9** Comparison of the robustness (AR) between the proposed scheme and schemes [29,30].

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaussian noise (0.0001)</td>
<td>0.9997</td>
<td>0.8495</td>
<td>0.9200</td>
<td>0.9554</td>
</tr>
<tr>
<td>Salt &amp; pepper noise (0.003)</td>
<td>0.9791</td>
<td>0.9523</td>
<td>0.9624</td>
<td>0.9676</td>
</tr>
<tr>
<td>Salt &amp; pepper noise (0.005)</td>
<td>0.9912</td>
<td>0.9358</td>
<td>0.9402</td>
<td>0.9402</td>
</tr>
<tr>
<td>Median filtering (3 x 3)</td>
<td>0.9852</td>
<td>0.8206</td>
<td>0.9404</td>
<td>0.9502</td>
</tr>
<tr>
<td>Average filtering (3 x 3)</td>
<td>0.9950</td>
<td>0.9973</td>
<td>0.9346</td>
<td>0.9453</td>
</tr>
<tr>
<td>Gaussian filtering (3 x 3)</td>
<td>0.9963</td>
<td>0.9243</td>
<td>0.9597</td>
<td>0.9676</td>
</tr>
<tr>
<td>JPEG compression (40%)</td>
<td>0.9966</td>
<td>0.9432</td>
<td>0.8840</td>
<td>0.8945</td>
</tr>
<tr>
<td>JPEG compression (70%)</td>
<td>0.9973</td>
<td>0.9854</td>
<td>0.9002</td>
<td>0.9049</td>
</tr>
<tr>
<td>Rotation 1</td>
<td>0.9961</td>
<td>0.9824</td>
<td>0.9678</td>
<td>0.9741</td>
</tr>
<tr>
<td>Rotation 5</td>
<td>0.9966</td>
<td>0.9654</td>
<td>0.9643</td>
<td>0.9711</td>
</tr>
<tr>
<td>Rotation 10</td>
<td>0.9954</td>
<td>0.9473</td>
<td>0.9397</td>
<td>0.9679</td>
</tr>
<tr>
<td>Sharpening attack</td>
<td>0.9941</td>
<td>0.9799</td>
<td>0.9879</td>
<td>0.9918</td>
</tr>
<tr>
<td>Histogram equalization</td>
<td>0.9961</td>
<td>0.9886</td>
<td>0.9920</td>
<td>0.9964</td>
</tr>
</tbody>
</table>
algorithm can effectively reduce storage space and save resources. In a word, our method is more efficient compared to the other five methods in terms of time and space.

5.4. The effect of watermark size on robustness

As can be seen from Section 5.1, the watermark capacity of the proposed scheme depends on the maximum order of QPHFM. As the maximum order of QPHFM increases, the size of the embeddable watermark image will gradually increase accordingly. However, the increase of the maximum order of QPHFM brings two problems: (1) The time of QPHFM computation becomes longer as the number of moments increases, as shown in Fig. 12, which leads to the decrease of the scheme’s efficiency. (2) In the computation of higher-order moment, various errors may cause the moment’s numerical calculation distortion or even divergence [31,31]. Therefore, in the zero-watermarking algorithm, the order too big will affect the algorithm’s robustness. To illustrate the higher-order moment’s influence on the robustness, we embed the watermark image with size 64 × 64 (maximum order is 50) in the QPHFM and compare the scheme with the original scheme. Fig. 13 shows the comparison results, in which the robustness is measured with the AR of watermark extracted in the case of the simultaneous attack to $f_1$, $f_2$ and $f_3$. The attack 1 to 12 are JPEG 10, JPEG 50, Gaussian noise 0.03, Salt and pepper noise 0.03, median filtering $3 \times 3$, Gaussian filtering $3 \times 3$, Average filtering $3 \times 3$, Rotation 5, Rotation 45, Scaling 0.5, Scaling 1.5 and Cropping 1/8, respectively. It should be noticed that the curves are obtained from the mean of 33 groups of experiment. The comparison results show that the algorithm’s AR obtained with the $32 \times 32$ watermark image (maximum order is 25) is bigger than the AR obtained with the $64 \times 64$ watermark image (maximum order is 50). It means the AR of watermark extracted decreases as size of watermark image increases. Therefore, when selecting the watermark size, it is necessary to consider the compromise between the performance and the watermark size.

6. Conclusions

The paper proposes a QPHFM-based robustness zero-watermarking scheme for three CT images, realizing the copyright protection for three CT images simultaneously. The algorithm first considers the three CT images as three imaginary parts of an array of pure quaternion and calculates their QPHFM, and then constructs the feature image using the QPHFM, and finally makes the XOR operation to the feature image after chaotic scrambling and the watermark image to get the key image. The experiment results show that the scheme proposed can resist common image processing attacks sand geometric attacks effectively and thus is very applicable to the copyright protection of three images. The scheme proposed has the following innovation points: (1) it first realizes the simultaneous copyright protection for three images, improves the algorithm’s efficiency effectively and saves storage space; (2) it first constructs the QPHFM of three different images; (3) it does not change the original CT images and thus ensures the completeness of CT images. Therefore, the scheme proposed has important theoretical values for the simultaneous copyright protection of three images. The future work is combining the hypercomplex theory with the multi-image processing to propose a copyright protection scheme for multiple images.

Conflict of interest

None.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (nos. 61802212, 61672124, and 61371015), Shandong Provincial Natural Science Foundation (no. ZR2019BF017), the Password Theory Project of the 13th Five-Year Plan National Cryptography Development Fund (no. MM[2017]0203), a Project of Shandong Province Higher Educational Science and Technology Program (JJ18KA331), Basic scientific research Project of Colleges and Universities in Liaoning Province (WQ20170707). Data used in this publication were generated by the National Cancer Institute Clinical Proteomic Tumor Analysis Consortium (CPTAC).

References