Circuits Syst Signal Process (2018) 37:5441–5462
https://doi.org/10.1007/s00034-018-0822-8

Robust Color Image Hashing Using Quaternion Polar Complex Exponential Transform for Image Authentication

Khalid M. Hosny[1] · **Yasmeen M. Khedr**[1] · **Walid I. Khedr**[1] · **Ehab R. Mohamed**[1]

Received: 26 September 2017 / Revised: 19 April 2018 / Accepted: 21 April 2018 /
Published online: 26 April 2018

Abstract Image hashing is one of the multimedia protection techniques. In this paper, a new method for robust image hashing based on quaternion polar complex exponential transform (QPCET) is proposed. The proposed method targets two goals. The first goal is the robustness against geometric and common signal processing attacks. The second one is authenticating color images without conversion which keeps their color information. In the proposed method, the input color image is normalized by the bicubic interpolation and then the interpolated image passes to Gaussian low-pass filter. QPCET moments are used to extract features. Finally, the hash value is calculated using the extracted features. On the sender side, a secret key is utilized to increase the protection of the hash value before transmitting it. The hash value is attached with the transmitted color image. On the receiver side, the authenticity of the received image is checked by decrypting the hash value. Euclidean distance is used to check the similarity between different hashes. Results of the conducted experiments prove the robustness of proposed hash against different geometric and signal processing attacks. Also, it preserves the content of the transmitted color image. Hashing different images has a very low collision probability which ensure the suitability of the proposed method for

✉ Khalid M. Hosny
k_hosny@yahoo.com

Yasmeen M. Khedr
eng_yasmeenkh@yahoo.com

Walid I. Khedr
khedrw@yahoo.com

Ehab R. Mohamed
ehab.rushdy@gmail.com

[1] Department of Information Technology, Faculty of Computers and Informatics,
Zagazig University, Zagazig 44519, Egypt

Birkhäuser

image authentication. Comparison with the existing methods ensures the superiority of the proposed method.

Keywords Quaternion polar complex exponential transform moment · Image hashing · Image authentication · Geometric attacks · ROC

1 Introduction

Image hashing technique is a useful tool used in protecting the content of color images. The available image editing tools such as PhotoScape, Adobe Photoshop and Photopad could be used to manipulate and alter the content of the color images. In addition to the image authentication, robust image hashing could be utilized in detecting image forgery and tampering. Traditional hash techniques such as SHA-1 and MD-5 [12] are sensitive to very small changes in the image. Therefore, these techniques are not suitable for image authentication. This drawback makes these techniques unsuitable for image authentication. Robust image hashing provides a short sequence from image and can tolerate content-preserving modifications [18]. Previous studies refer to the role of robust image hashing for image authentication. There are two types of image hashing methods. The first type is devoted to gray images or one channel of color images such as a luminance, while the second one handles the color images.

Swaminathan et al. [19] constructed a new method that used Fourier transform. Experimental results showed that this method has good capabilities and is flexible to different operations. Unfortunately, this method could not preserve the content of the image. Monga and Mihcak [14] used nonnegative matrix factorization (NMF) for image hashing. Ahmed et al. [1] presented a new wavelet-based image authentication method. This method could not achieve the robustness against geometric attacks. Zhao et al. [25] utilized the corrected phases of Zernike moments and the rotation invariants to construct an image hash. This method is robust against most content-preserving attacks and has low collision probability.

Weng and Preneel [23] proposed a new image hashing algorithm for image content authentication. They divided the image into blocks and extract the features of each block using the coefficients of the discrete Fourier transform (DFT). This method achieved a marginal success in securing the content of image blocks. Lei et al. [13] constructed a robust image hash where the features of the image were extracted using the Radon transform. Their results showed robustness against JPEG compression, blur and noise attacks. Zhao [24] used the magnitudes of Zernike moments to construct the image hash. This method improved the robustness against attacks. Unfortunately, the hash is sensitive to filtering. Qin et al. [17] presented a robust image hashing scheme using a non-uniform sampling in the discrete Fourier domain. Their results showed low probability and robustness against content-preserving manipulations.

Tang et al. [21] used the coefficients of the dominant discrete cosine transform (DCT) to construct the image hash where their results showed robustness against different attacks. Chen et al. [2] proposed a robust image hashing scheme using invariants of Tchebichef moments. The random gray code was applied to enhance the expected discriminability. Their results showed robustness against content-preserving manipulations. Tang et al. [20] proposed a perceptual hash for color images. This hash was constructed by computing the invariant moments of Hu for each channel and concatenating them where the L2 norm was used to evaluate the similarity between image hashes. Since Hu moment invariants are not accurate, this method could not achieve the desirable robustness against different attacks. All aforementioned methods were used to construct image hash for gray or single channel color images.

On the other side, Ghouti [4] utilized the quaternion singular value decomposition (QSVD) to construct the perceptual hash for color images. Ouyang et al. [15] proposed a new hash for color images. They used quaternion discrete Fourier transform to extract features of the image. To achieve the rotation invariance, they utilized the log polar transform. This method is relatively robust against the popular content-preserving operations. Ouyang et al. [16] proposed a new hash for authenticating color images. They used the quaternion Zernike moments (QZMs) to extract the features of the color images. In their work, Ouyang and his co-authors utilized the Zero-approximation method to calculate the Zernike moments which results in a set of inaccurate features and inaccurate scaling and rotation moment invariants. In addition to this significant weakness point, the extracted features by Zernike moments are sensitive to different kinds of noises. Unfortunately, none of the aforementioned hashing methods achieve the optimal image hash. This shortage motivates the authors to propose a new method to construct a robust image hash for color image authenticate.

In the proposed method, a robust image hash is constructed where the highly accurate and fast QPCET moments and their rotations, scaling and translation invariants are used to extract highly accurate features from color images. The Euclidean distance is used to measure the similarity between the image hashes. Experimental results clearly show that the proposed method is robust against the scaling and rotation attacks with different scaling factors and a wide range of rotation angles. Also, it is robust against the common signal processing attacks such as salt and peppers noise, white Gaussian noise, speckle noise, JPEG compression, average filtering, brightness and contrast adjustment with different parameters. A set of numerical experiments is performed to test the validity of the proposed method. A comparison with the existing methods, Ghouti [4] and Ouyang et al. [16], ensures the superiority of the proposed method.

The rest of the paper is organized as follows: A detailed description of the proposed scheme is presented in Sect. 2. The process of image authentication is presented in Sect. 3. The description of the conducted numerical experiments and the analysis of the obtained results are presented in Sect. 4. The conclusion of this work is presented in Sect. 5.

2 Proposed Hashing Scheme

The proposed method is divided into three main steps as illustrated in Fig. 1. Each step will be described in a separate subsection. The first subsection is devoted to the image preprocessing step. The detailed process of extracting the features is presented in the second subsection. Finally, the process of hash construction is presented in the third subsection.

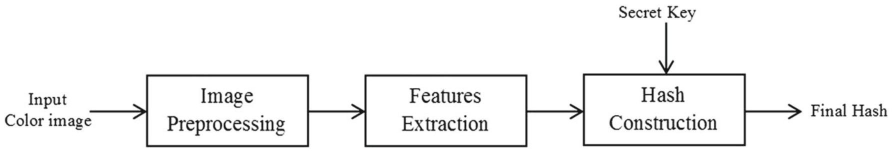


Fig. 1 Proposed image hashing scheme

2.1 Image Preprocessing

The preprocessing of the color images is performed through two successive steps. Firstly, the input color image is rescaled to a fixed size $M \times M$ using bicubic interpolation. This resizing process aims to unifying the size of hashes of all images. Secondly, the rescaled color image is filtered. In this process, the rescaled color image is filtered by the Gaussian low-pass filter to improve the robustness of the extracted features against noise and decrease the high frequency components. The size of the kernel/window of the Gaussian low-pass filter must increase with increasing the value of the standard deviation, σ, to maintain the Gaussian nature of the filter. Three different windows are tested, 3×3 with $\sigma = 1$; 5×5 with $\sigma = 3$ and 7×7 with $\sigma = 5$. The obtained results are close to each other. The window size 3×3 with standard deviation $\sigma = 1$ will be used in the performed experiments.

2.2 Feature Extraction

Highly accurate QPCET moments are computed for the input color image to extract highly accurate features. These accurate features are the cornerstone in constructing the robust image hash. Quaternion representation of color images and the QPCET moments are discussed in the following subsections.

2.2.1 Quaternion of Color Image

Hamilton [5] introduced the quaternion as a generalized mathematical complex number. A quaternion consists of one real part and three imaginary parts. It can be expressed as follows:

$$q = w + xi + yj + zk \tag{1}$$

where $w, \ x, \ y$ and z are real numbers, and i, j and k are three imaginary units which are defined according to the following equations:

$$\begin{aligned} i^2 &= j^2 = k^2 = -1 \\ i &= jk = -kj \\ j &= ki = -ik \\ k &= ij = -ji \end{aligned} \tag{2}$$

If the real part $w = 0$, q is called a pure quaternion. The conjugate q^* and modulus of a quaternion $|q|$ are defined as follows:

$$q^* = w - xi - yj - zk, \qquad |q| = \sqrt{w^2 + x^2 + y^2 + z^2} \tag{3}$$

A color image with the image intensity function $f(x, y)$ could be represented as an array of pure quaternions [22] as follows:

$$f(x, y) = f_{\mathrm{R}}(x, y)\, i + f_{\mathrm{G}}(x, y)\, j + f_{\mathrm{B}}(x, y)\, k \tag{4}$$

where $f_{\mathrm{R}}(x, y)$, $f_{\mathrm{G}}(x, y)$, $f_{\mathrm{B}}(x, y)$ represent the red-, green- and blue-channels, respectively.

2.2.2 QPCET Moments

The right-side QPCET moments of order p and repetition q for the RGB color image with image intensity $f(r, \theta)$ are defined in the polar coordinates over a unit circle as follows [22]:

$$\Phi_{pq} = \frac{1}{\pi} \int_0^{2\pi} \int_0^1 f(r, \theta) \exp\left(-\mu 2\pi p r^2\right) \exp(-\mu q \theta)\, r \mathrm{d}r \mathrm{d}\theta \tag{5}$$

where $\mu = (i + j + k)/\sqrt{3}$ is called a unit pure quaternion. Hosny and Darwish [8] introduced a novel highly accurate, fast and numerically stable method for computing the QPCET moments. This method is summarized using the following equations.

$$\Phi_{pq} = \frac{1}{\pi} \sum_i \sum_j \hat{f}\left(r_i, \theta_{i,j}\right) D_{pq}\left(r_i, \theta_{i,j}\right) \tag{6}$$

where

$$D_{pq}\left(r_i, \theta_{i,j}\right) = K_p(r_i)\, L_q\left(\theta_{i,j}\right) \tag{7}$$

$$K_p(r_i) = \int_{U_i}^{U_{i+1}} \mathrm{e}^{-\mu 2\pi p r^2} r \mathrm{d}r \tag{8}$$

$$L_q\left(\theta_{i,j}\right) = \int_{U_i}^{V_{i,j+1}} \mathrm{e}^{-\mu q \theta} \mathrm{d}\theta \tag{9}$$

Since the QPCET moments are defined and computed in the polar coordinates, the image intensity function in Cartesian coordinates, $f(x, y)$, must be mapped to polar coordinates. All details of this process are presented in [6, 9]. The function $\hat{f}\left(r_i, \theta_{i,j}\right)$ represents the discrete color image in polar coordinates.

2.3 Hash Construction

The magnitude values of the computed QPCET moments represent the extracted features which are stored in a vector E. For a maximum order $n = 5$, the total number of features is 21 elements. Therefore, the hash length is $21 \times 8 = 168$ bits. Optimal image hashing must achieve two criteria, robustness and security. An image hashing is said to be robust, when using the same secret key between the sender and the receiver, the similar images must produce the similar hash [19]. To enhance the security, the image hash is scrambled by using a secret key, K. The secret key is randomly generated and represented in a vector. The similarity between image hashes is measured by the Euclidean distance [7]:

$$d\left(h_1, h_2\right) = \sqrt{\sum_{l=1}^{L} \left(E_1\left(l\right) - E_2\left(l\right)\right)^2} \tag{10}$$

where h_1 and h_2 are two image hashes and L is the length of hash vector.

3 Image Authentication

Robust image hashing is one of the techniques for image authentication [12]. Robust image hashing is the target of this paper. At the sender's side, the preprocessing operations are applied to the input color image, and then QPCET moments are computed. The extracted features are sorted in a 1D vector called 'the hash vector' which is attached with the image to be sent. A secret key is utilized to encrypt the hash value before executing the sending operation. At the receiver side, the received hash is decrypted using the same secrete key and generates the hash from the received image in same way as the sender did. Finally, the generated hash and the attached one are compared to determine the image authenticity. An illustration of the main steps of image authentication is displayed in Fig. 2. A threshold value, T, is used to decide whether the two images are similar or not. If hash distance value d is smaller than the threshold, T, then the two images are similar. Otherwise, the two images are different.

4 Numerical Results

To evaluate the performance of the proposed method, 660 original TIF format color images of size 786×576 from different datasets [11] were used. The first dataset contains color images of flowers, while the second dataset contains a man-made color images. The third dataset contains color images of animals. In the performed experiments, 143, 418 and 99 color images are selected randomly from the first, second and the third datasets, respectively. Samples from these color images are displayed in Fig. 3. In all experiments, the following parameters are defined as follows: The size of normalized image $M = 256$; the order of QPCET moments is $L = 5$ (numbers

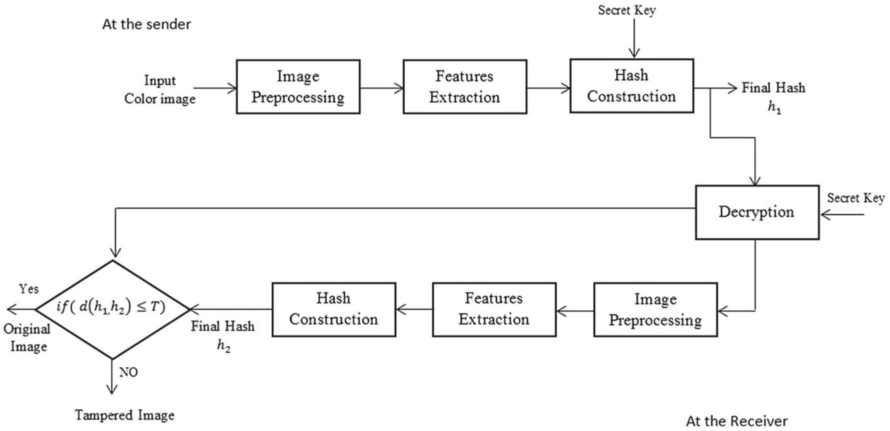


Fig. 2 Image authentication scheme

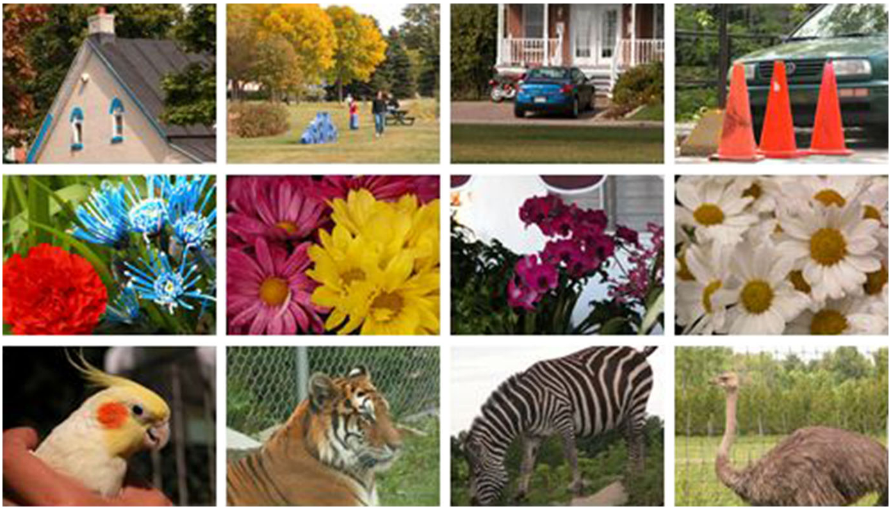


Fig. 3 Samples of different color images from flowers, man-made and animals datasets [11] (Color figure online)

of moments are 21) where the hash length of the proposed method is $21 \times 8 = 168$ bits. The robustness of the hash is tested against content-preserving attacks such as rotation, scaling, salt and peppers noise, speckle noise, white Gaussian noise, JPEG compression, average filter, brightness and contrast adjustment.

To ensure the validity of the proposed method, robustness tests and uniqueness hash test have been performed and the obtained results are shown in Sect. 4.2. To ensure the superiority of the proposed method, ROC curves [3] are used in comparing the proposed method with the existing methods, QSVD [4] and QZM [16]. The comparison between different methods is presented in Sect. 4.3.

Table 1 Parameters used in the robustness experiment

Attack	Description	Parameter value
Average filter	Window size	3, 5, 7, 9, 11
JPEG compression	Quality factor	10, 30, 50, 70, 90%
Contrast adjustment	Ratio	− 20, − 10, 10, 20
Brightness adjustment	Ratio	0.85, 0.9, 0.95, 1.05, 1.1
Scaling	Factor	0.6, 0.8, 1.2, 1.5, 2
Rotation	Angle in degrees	2°, 10°, 30°, 45°, 210°
White Gaussian noise	Noise level	0.002, 0.004, 0.006,0.008, 0.01
Salt and peppers noise	Noise level	0.01, 0.02, 0.04, 0.06, 0.08
Speckle noise	Noise level	0.01, 0.02, 0.04, 0.06

4.1 Robustness Test

In the conducted experiments, 660 color images are used where each color image is attacked by 43 attacks. The attacks and the different values of the parameters are shown in Table 1. After that, the similarity between the original and attacked images is measured using the Euclidean distance. It is concluded that the total numbers of identical image pairs are $660 \times 43 = 28{,}380$. Figure 4 illustrates the probability distribution of identical images. It is observed that most preserving operations are less than threshold, T, value equal to 3 and only few image pairs which exceed this threshold. Additional experiment is performed using 4 standard color images, ‘F16,’ ‘Lena,’ ‘Mandrill’ and ‘Pepper’ which selected from the dataset [10]. These images as displayed in Fig. 5 are used in testing the robustness against different attacks. The proposed method is applied to these standard color images where the obtained results are plotted and displayed in separate figures.

The robustness of the hash against the average filter and the JPEG compression are displayed in Fig. 6a and b, respectively. It is observed that the values of the hash distances for average filter with common small window size, 3×3 and 5×5, are very small and these values slightly increased as the window size increased such as 7×7, 9×9 and 11×11. For the JPEG compression attack, very small values of the hash distances are obtained with high-quality factors.

The hash distances for contrast and brightness adjustments are displayed in Fig. 7a and b, respectively. The results in these figures show that the two attacks produce very small values for the hash distance where these values do not override 0.04 which ensure the robustness of the proposed method against both attacks.

Scaling factors < 1 refer to image reduction, while scaling factors > 1 refer to image magnification. The hash distances are computed for scaling factors ranging from 0.4 to 2.2 with constant step 0.2 and counterclockwise rotation angles ranging from 0° to 210° with constant angle increment equal to 30°. The hash distances for rotation and scaling with different parameters are displayed in Fig. 8a and b, respectively. It is clear that very small values of the hash distances are obtained for scaling factors > 1 and acute rotation angles.

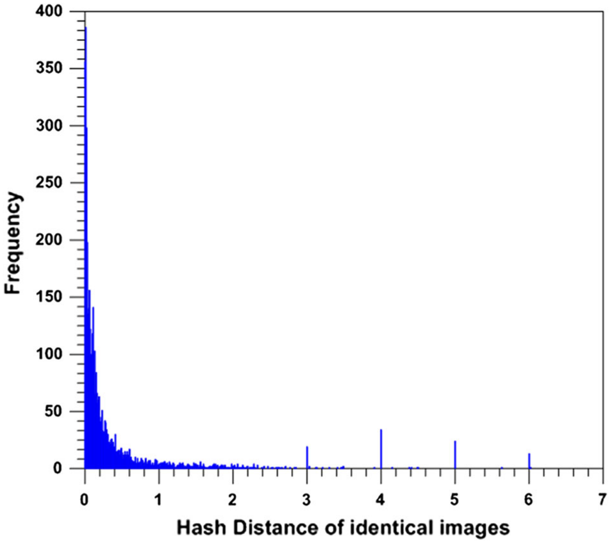


Fig. 4 Probability distributions of identical images

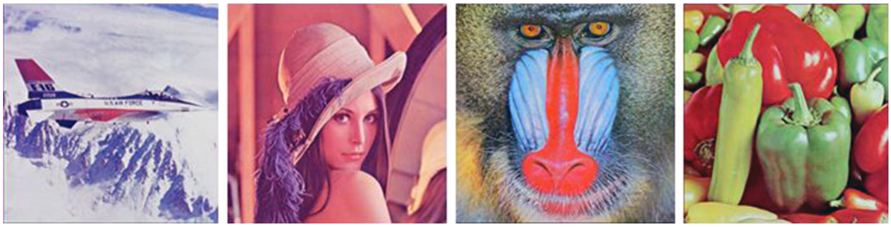


Fig. 5 Standard color images (Color figure online)

The robustness against common noises such as Gaussian noise, salt and pepper noise and speckle noise with different level of contamination is evaluated and displayed in Fig. 9a, b and c, respectively. The values of the hash distances for all geometric and signal processing attacks slightly change along the change of the parameters. Generally, in all cases, the values of the hash distances are not exceeding the specified value of the threshold T which ensures the robustness of the hash constructed by the proposed method against all geometric and signal processing attacks.

In image authentication using a hash distance, two color images are considered different when the hash distance is higher than the value of the threshold, T [1]. Based on the obtained results, some statistical calculations are performed using the different hash distances of the proposed method for the 43 different attacks. The average hash distance for each one of the nine attacks, average filter, JPEG compression, contrast adjustment, brightness adjustment, scaling, rotation, white Gaussian noise, salt and peppers noise and speckle noise, are shown in Table 2. None of the statistical average values exceeded the value of the threshold. These results ensure the robustness of the proposed hashing method against all kind of attacks. Also, these results are consistence

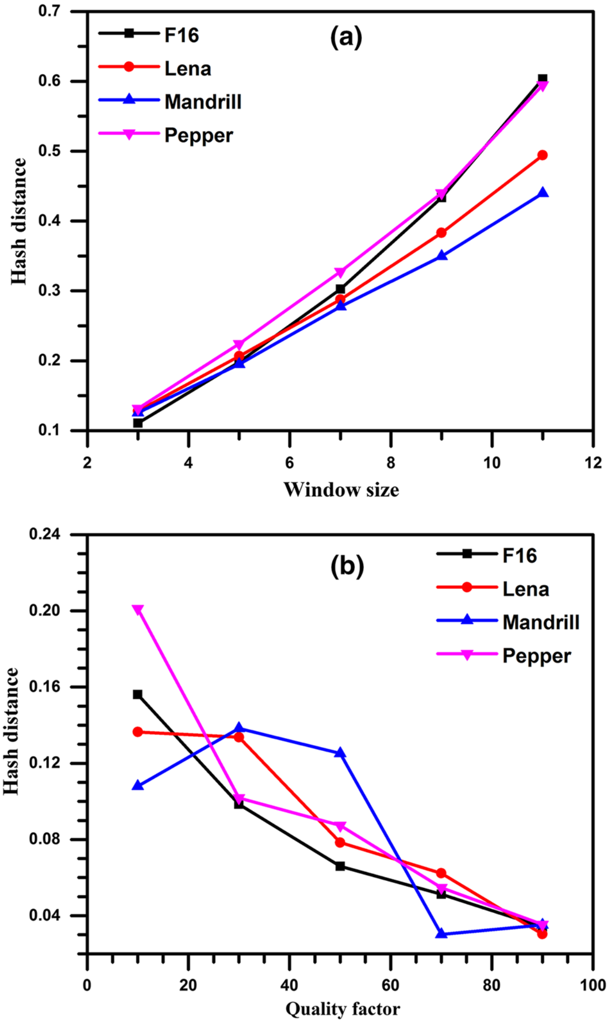


Fig. 6 Robustness performances for average filter and JEPG compression, **a** average filter, **b** JPEG compression

with the probability distribution of identical images as displayed in Fig. 4 which ensure that $T = 3$ is the best choice to judge the similarity.

4.2 Uniqueness Hash

If the hash sequences of dissimilar images are distinct, this means that the hash is unique. We download 300 images from man-made dataset [11] to form different images database. Figure 10 clarifies that the Euclidean distance probability distributions that computed from the relation $C_{300}^2 = 88450$ hash pairs with 300 different images.

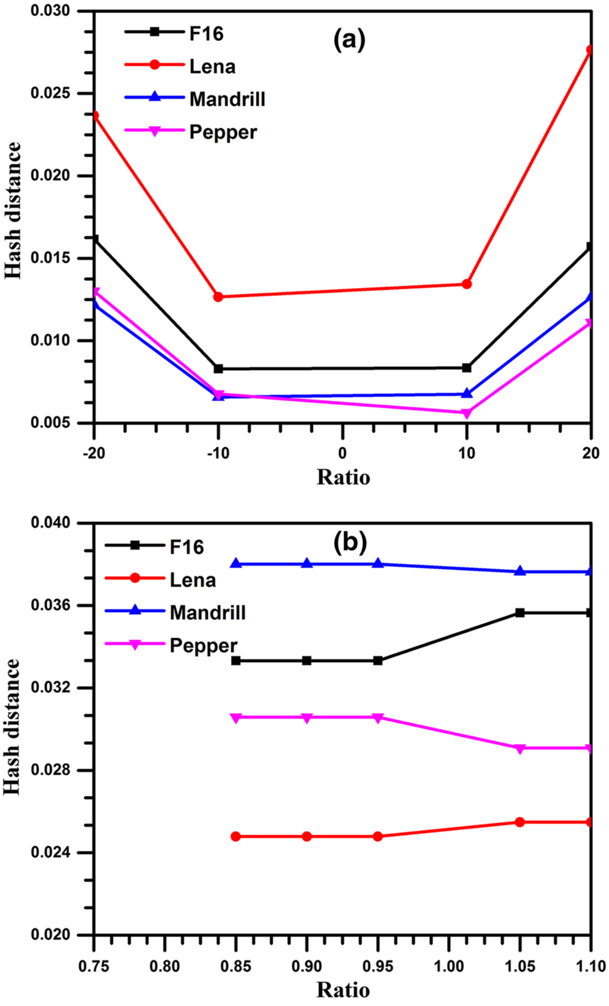


Fig. 7 Robustness performances for contrast and brightness adjustment, **a** contrast adjustment, **b** brightness adjustment

Overall, we observed that the hashing distance of most different image pairs is more than $T = 3$. If two dissimilar images have identical hash values with the Euclidean distance less than T value, this can be called probability of collision (P_C) [26]. P_C can be calculated using Eq. 11. Thereby, these results prove the uniqueness and robustness of the proposed hashing method.

$$P_\mathrm{C} = \frac{\text{Number of different images judged as similar images}}{\text{Total number of different images}} \tag{11}$$

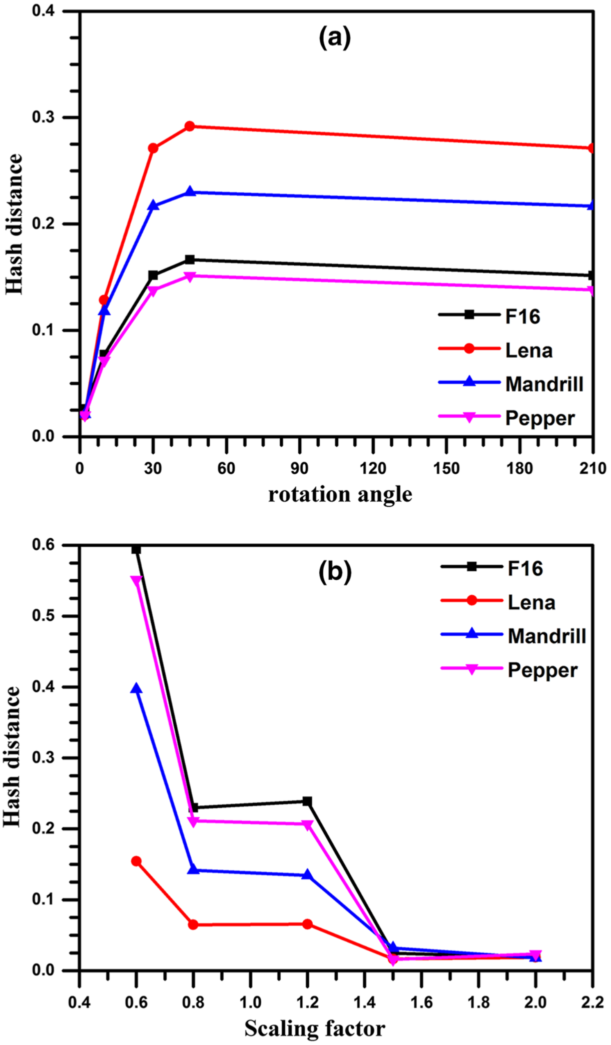


Fig. 8 Rotation and scaling hash distances. **a** Rotation, **b** scaling

4.3 Performance Comparisons

The performance of the proposed hashing method is compared with the existing methods, QSVD-based method of Ghouti [4] and the QZM-based method of Ouyang et al. [16]. For fair and accurate comparison, the same color images from the dataset in [11] are used in the comparison. The receiver operating characteristics (ROC) is a good and reliable qualitative measure. The ROC curves [3] are used for visualizing the classification performances. For fair comparison, the ROC curve is computed and plotted for each attack using the method of Ghouti [4], the method of Ouyang et al. [16] and the proposed method. The true positive rate (TP rate) and the false positive rate (FP rate) of the two compared methods are defined as follows:

Fig. 9 Robustness for some noise **a** Gaussian noise, **b** salt and pepper noise, **c** speckle noise

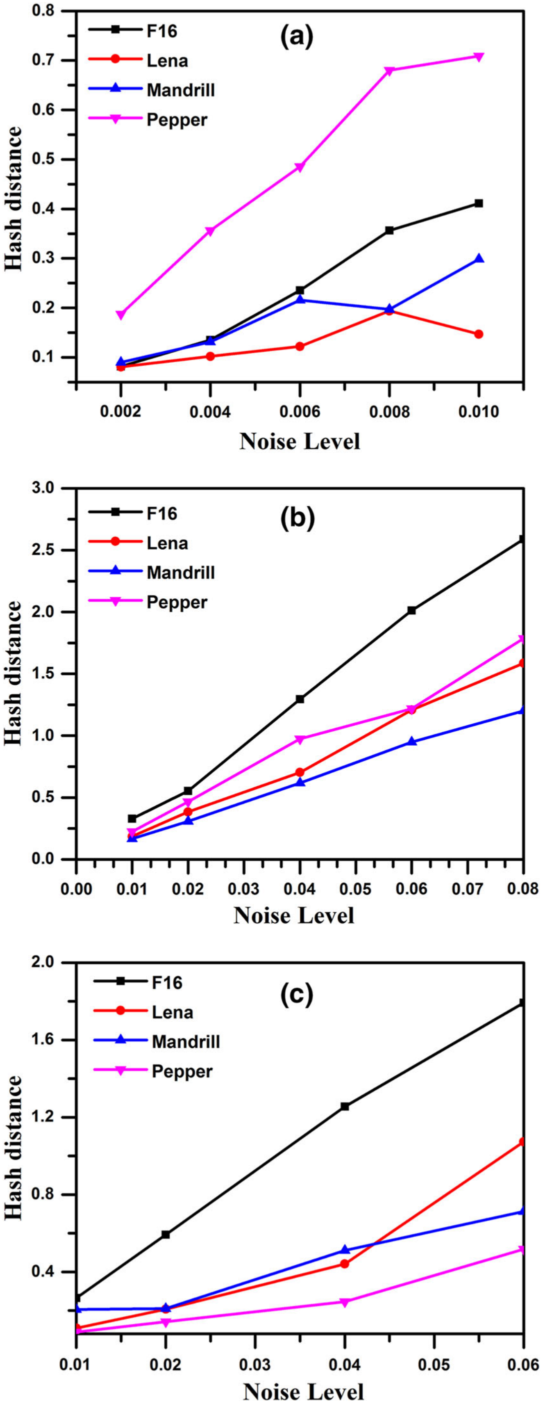


Table 2 Statistics of hash distances for the proposed method

Attacks	Maximum	Minimum	Average
Average filter	0.603586	0.110792	0.312709
JPEG compression	0.201139	0.030213	0.088206
Contrast adjustment	0.027657	0.005632	0.012536
Brightness adjustment	0.038007	0.024787	0.03179
Scaling	0.594366	0.016047	0.157936
Rotation	0.291804	0.020163	0.153646
White Gaussian noise	0.708716	0.080655	0.260803
Salt and peppers noise	2.587835	0.166826	0.937869
Speckle noise	1.792617	0.088713	0.523109

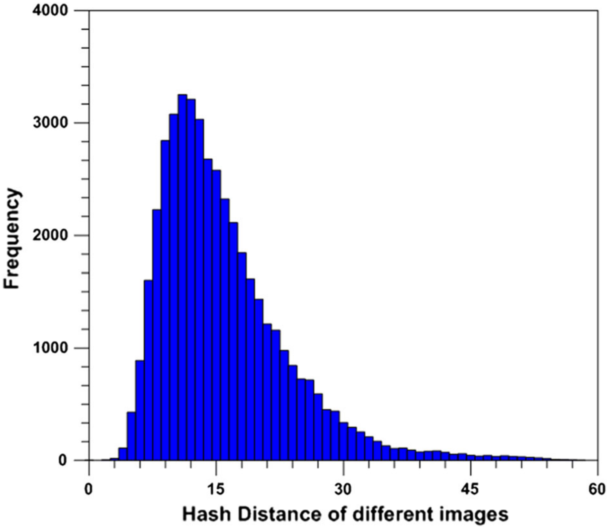


Fig. 10 Probability distribution of different image hashing

$$\text{TP rate} = \frac{x}{X}$$

$$\text{FP rate} = \frac{y}{Y}$$

where x is number of the pairs of identical images considered as similar images, X is the total pairs of identical images, y is number of the pairs of different images considered as similar images, and Y is number of the total pairs of different images. To compute ROC curve for each method, different thresholds are selected in order to

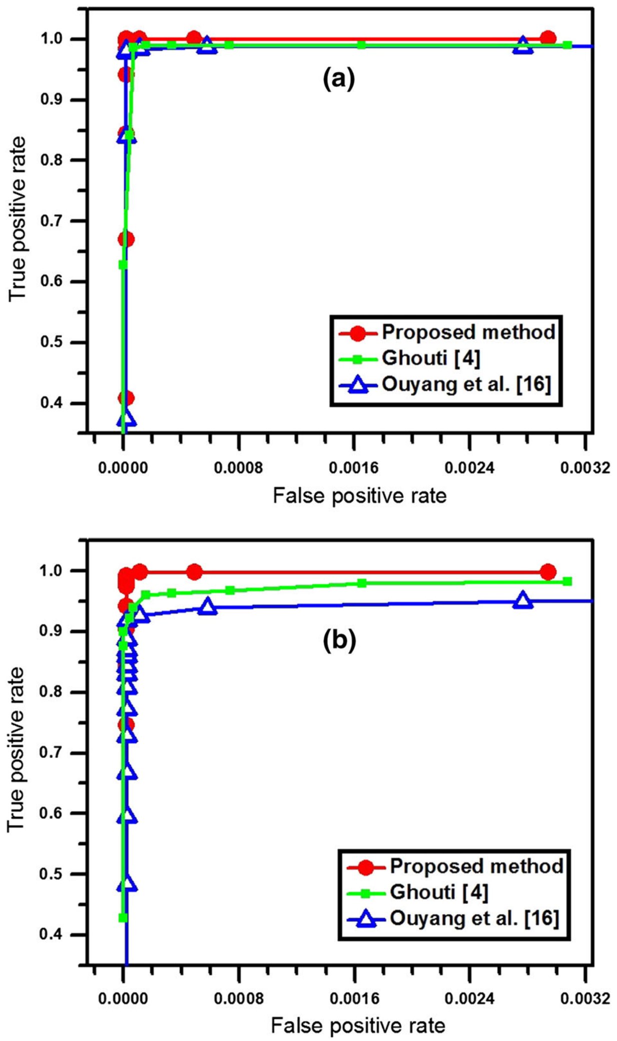


Fig. 11 ROC curve for an average filter and JPEG compression respectively, **a** average filter, **b** JPEG compression

compare the proposed, Ghouti [4] and Ouyang et al. [16] methods. Different values of the thresholds are selected to be close to the specific threshold of each method. For the proposed method, the specific threshold is 3, so the selected values are 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1, 2, 3 and 4. For the method of Ghouti [4], the specific threshold is 200, so the selected values are 10, 40, 50, 70, 100, 120, 150, 200, 250, 300, 350 and 400. Finally, the specific threshold Ouyang et al. [16] is 12, so the selected values are 0.4, 0.6, 0.8, 1, 3, 6, 10, 12, 15, 20, 30 and 40.

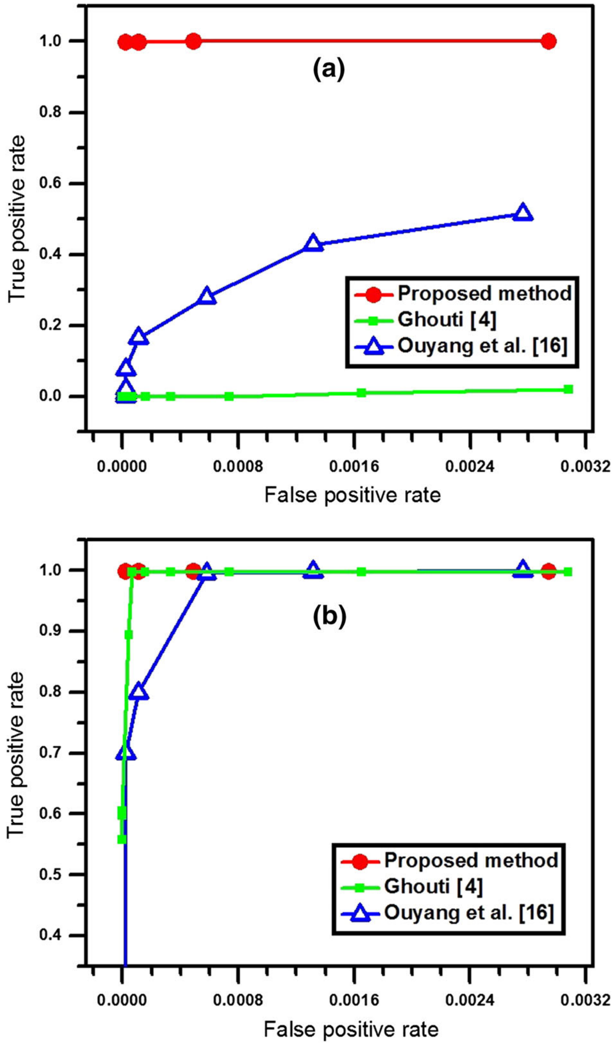


Fig. 12 ROC curve for **a** contrast adjustment, **b** brightness adjustment

The ROC curves for the average filter and JPEG compression are presented in Fig. 11a and b, respectively. It is observed that the proposed method is much robust to average filter and JPEG compression attacks.

The ROC curve for the contrast adjustment attack is displayed in Fig. 12a. It is clear that, the proposed method is perfect where it reached to 1 by a small false positive rate. On the other hand, the method of Ghouti [4] is sensitive to contrast adjustment, while the performance of the method of Ouyang et al. [16] is extremely bad. The ROC curve for the brightness adjustment attack is displayed in Fig. 12b. The performance of the proposed method is much better than the performance of the other methods [4] and [16].

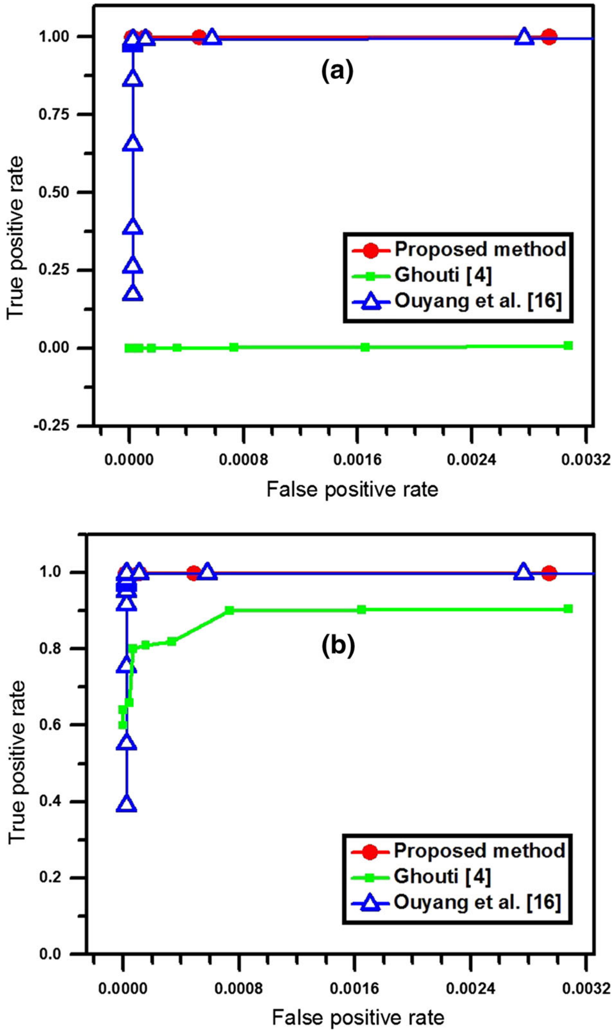
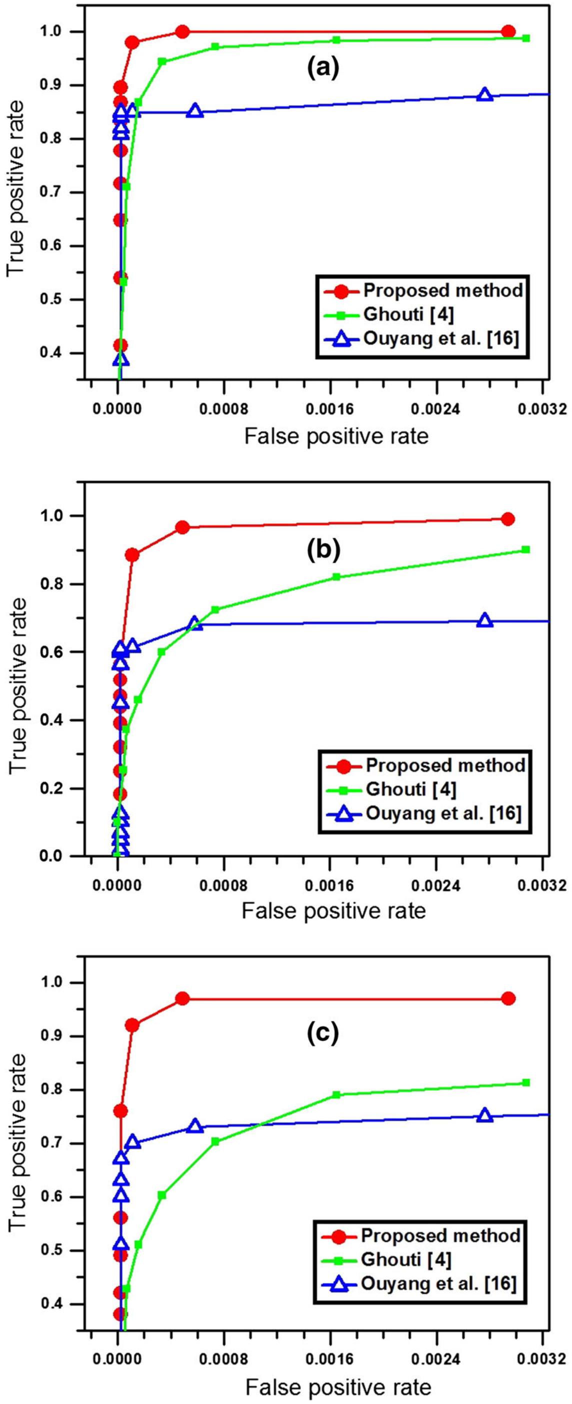


Fig. 13 ROC curve for geometric attacks **a** rotation, **b** scaling

For geometric attacks, the ROC curves for the rotation and scaling attacks are displayed in Fig. 13a and b, respectively. These figures clearly show that the proposed method is robust against rotation and scaling attacks due to the high accuracy of the QPCET moments. The method of Ghouti [4] is highly sensitive to rotation and scaling attacks.

Speckle noise is very important in medical images so we need to test the robustness against this noise. Robust to this kind of noise is very attractive characteristics. Despite the importance of this attack in the field of images, it was not applied before by Ghouti [4] and Ouyang et al. [16]. Therefore, in the current work we used this attack. Figure 14a, b and c shows ROC curves of some attacks related to noise such as Gaussian noise, salt and pepper and speckle noise.

Fig. 14 ROC curve for **a** Gaussian noise, **b** salt and pepper noise, **c** speckle noise



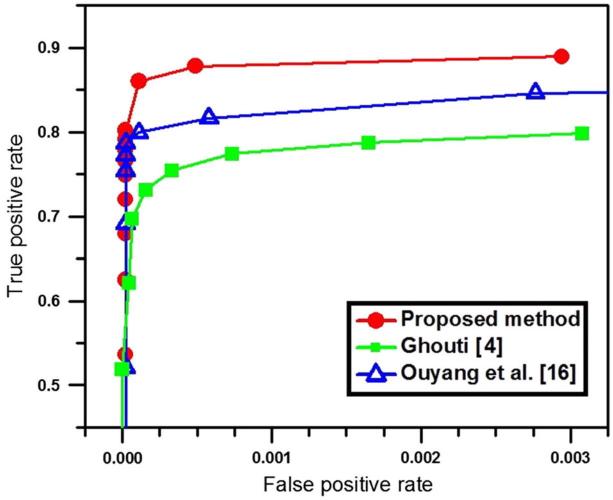


Fig. 15 ROC curve between a proposed, Ghouti [4] and Ouyang et al. [16]

The obtained results confirm the robustness of the proposed method. On the other side, the method of Ghouti [4] is sensitive to the three kinds of noises. The method of Ouyang et al. [16] is very sensitive, and its performance is very bad. Finally, Fig. 15 shows a ROC curve for general comparison between a proposed method, Ghouti [4] and Ouyang et al. [16]. All plotted ROC curves show that the proposed method achieved the best performance where the true positive rate is very close to 1 for all attacks.

The robustness to different attacks could be evaluated quantitatively. Additional set of experiments is performed where the Euclidean distance is used as an explicit quantitative measure. The 4 standard color images are attacked by the nine attacks with few different parameters. The comparison between the proposed method and the existing methods [4] and [16] is performed using hash distance values. For different values of the threshold, T, of each method the hash distance is tested and determined if this value is less than the threshold or not. The method is robust if the hash distance is less than the threshold, T, otherwise the method is not robust.

The threshold of the proposed method, $T = 3$, the hash distance for all attacks is less than T. So, the robustness is achieved against all attacks. For a threshold, $T = 200$, the method of Ghouti [4] failed in the test of rotation and contrast adjustment attacks. For a threshold, $T = 12$, the method of Ouyang et al. [16] failed in the test of contrast and brightness adjustments attacks.

The obtained results of hash distance for different attacks as shown in Table 3 are consistent with the previously obtained results and confirm the robustness of the proposed method. Overall, it is clear that the proposed QPCET-based hashing method is robust against different attacks with different parameters. Moreover, the proposed QPCET-based hashing method is anti-collision and short hash length.

Table 3 Comparison between hash distance results using the proposed method, the methods of Ghouti [4] and the method of Ouyang et al. [16]

Attacks	Parameter	F16			Lena			Mandrill			Peppers		
		Ghouti [4]	Ouyang et al. [16]	Proposed method	Ghouti [4]	Ouyang et al. [16]	Proposed method	Ghouti [4]	Ouyang et al. [16]	Proposed method	Ghouti [4]	Ouyang et al. [16]	Proposed method
Salt and peppers noise	0.01	30.692	0.8925	0.328679	69.39592	0.5865	0.185657	36.54702	0.663	0.166826	45.44019	0.8415	0.224036
	0.08	62.701	7.1655	2.587835	138.3695	4.896	1.586556	76.5735	5.457	1.200393	88.4986	6.528	1.785778
White Gaussian noise	0.002	8.088	0.1275	0.081881	5.4776	0.1785	0.080655	9.636117	0.255	0.090047	28.42839	0.5865	0.187264
	0.01	17.146	1.6575	0.411	8.262748	0.357	0.146902	15.34435	0.9435	0.298639	46.1946	1.8105	0.708716
Speckle noise	0.01	39.334	1.397184	0.265222	10.6004	0.19691	0.10887	29.67515	0.680877	0.205709	7.599357	0.152334	0.088713
	0.06	78.091	7.289144	1.792617	32.84525	3.403109	1.073567	78.86363	3.327907	0.712944	10.74599	1.699714	0.517927
Rotation	10	611	0.2888	0.077324	883.0672	0.5033	0.128498	660.487	0.3594	0.117925	580.4682	0.2426	0.071749
	45	2605	0.4766	0.166377	4039.24	0.7359	0.291804	2690.263	0.5845	0.229836	2228.062	0.4225	0.151271
Scaling	0.6	19.5526	1.2495	0.594366	7.774281	0.663	0.154351	7.319673	0.5865	0.396938	16.71748	1.2495	0.551602
	2	7.259178	0.0255	0.018918	2.837827	0.0765	0.018759	3.032626	0.0255	0.018051	7.250002	0.051	0.023533
JPEG compression	10%	26.83267	0.1785	0.156026	15.01032	0.5865	0.136455	25.53956	0.255	0.107907	32.7201	0.459	0.201139
	90%	21.43583	0.051	0.03414	25.55264	0.1275	0.03036	34.00355	0.102	0.035103	23.5251	0.153	0.035375
Brightness adjustment	0.85	2.367861	12.3165	0.033317	2.508259	12.8265	0.024787	2.51602	11.1945	0.038007	3.790434	21.2415	0.030578
	1.1	2.367861	14.6115	0.035645	2.508259	10.6335	0.025486	2.51602	11.7045	0.037644	3.790434	23.9955	0.029087
Average filter	3	15.24527	0.816	0.110792	25.18081	0.867	0.128247	26.60599	1.122	0.125614	23.66545	0.5355	0.13147
	11	33.88674	2.4225	0.603586	51.60265	2.8305	0.49413	47.92845	3.1365	0.439891	49.06899	1.5555	0.594903
Contrast adjustment	− 20	1163.314	19.12	0.016158	2520.405	41.29	0.023656	1369.612	36.42	0.012185	1708.388	32.04	0.013008
	20	619.6791	11.32	0.015704	1356.733	33.43	0.027657	742.1249	41.73	0.01265	897.1967	33.53	0.011104

5 Conclusion

In this work, a new method for color image hashing is proposed. The utilization of the QPCET moments achieves three contributions. First, the QPCET moments are used to extract highly accurate features of the input color image and then construct a highly accurate hash values. Second, the QPCET rotation and scaling moment invariants are highly accurate which protect the constructed hash from the rotational and scaling attacks. Third, the QPCET moments are robust to different types of noises.

The input color images are attacked by nine, rotation, scaling, JPEG compression, average filter, contrast and Brightness adjustment, speckle noise, salt and peppers noise, and Gaussian noise, attacks with different parameters. The QPCET moments are used to extract the features of the original and attacked images, and then, the hash values are computed. The obtained results are tested by using quantitative and qualitative approaches where these results clearly show the robustness of the proposed method. The proposed method achieves the uniqueness of the hash by achieving a very low collision probability. Therefore, it is concluded that the proposed method is suitable for color image authentication.

References

1. F. Ahmed, M. Siyal, V. Uddin Abbas, A secure and robust hash-based scheme for image authentication. Signal Process. **90**(5), 1456–1470 (2010)
2. Y. Chen, W. Yu, J. Feng, Robust image hashing using invariants of Tchebichef moments. Optik **125**(19), 5582–5587 (2014)
3. T. Fawcett, An introduction to ROC analysis. Pattern Recognit. Lett. **27**(8), 861–874 (2006)
4. L. Ghouti, Robust perceptual color image hashing using quaternion singular value decomposition, in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, (2014). http://doi.org/10.1109/ICASSP.2014.6854311
5. W.R. Hamilton, *Elements of Quaternions* (Longmans Green, London, 1866)
6. K.M. Hosny, Accurate circular moment invariants of gray-level images. J. Comput. Sci. **7**(5), 715–722 (2011)
7. K.M. Hosny, New set of Gegenbauer moment invariants for pattern recognition applications. Arab. J. Sci. Eng. **39**(10), 7097–7107 (2014)
8. K.M. Hosny, M.M. Darwish, Highly accurate and numerically stable higher order QPCET moments for color image representation. Pattern Recognit. Lett. **97**(1), 29–36 (2017)
9. K.M. Hosny, M.A. Shuman, H.M. Abdel Salam, Fast computation of orthogonal Fourier–Mellin moments in polar coordinates. J. Real-Time Image Process. **6**(2), 73–80 (2011)
10. http://sipi.usc.edu/database/database.php?volume=misc
11. http://tabby.vision.mcgill.ca/html/browsedownload.html
12. S. Jothimani, P. Betty, A survey on image authentication techniques. IJETT **7**(4), 184–186 (2014)
13. Y. Lei, Y. Wang, J. Huang, Robust image hash in Radon transform domain for authentication. Signal Process. Image Commun. **26**, 280–288 (2011)
14. V. Monga, M. Mihcak, Robust and secure image hashing via non-negative matrix factorizations. IEEE Trans. Inf. Forensics Secur. **2**(3), 376–390 (2007)
15. J. Ouyang, G. Coatrieux, H. Shu, Robust hashing for image authentication using quaternion discrete Fourier transform and log-polar transform. Digit. Signal Process. **41**, 98–109 (2015)
16. J. Ouyang, X. Wen, J. Liu, Robust hashing based on quaternion zernike moments for image authentication. ACM Trans. Multimed. Comput. Commun. Appl. **12**(4s), 1–13 (2016)
17. C. Qin, C. Chang, P. Tsou, Robust image hashing using non-uniform sampling in discrete fourier domain. Digit. Signal Process. **23**(2), 578–585 (2013)
18. L. Sebastian, A. Varghese, T. Manesh, Image authentication by content preserving robust image hashing using local and global features. Procedia Comput. Sci. **46**, 1554–1560 (2015)

19. A. Swaminathan, Y. Mao, M. Wu, Robust and secure image hashing. IEEE Trans. Inf. Forensics Secur. **1**(1), 215–230 (2006)
20. Z. Tang, Y. Dai, X. Zhang, Perceptual hashing for color images using invariant moments. Appl. Math. Inf. Sci. **6**(2s), 643S–650S (2012)
21. Z. Tang, F. Yang, L. Huanga, X. Zhang, Robust image hashing with dominant DCT coefficients. Optik **125**, 5102–5107 (2014)
22. X. Wang, W. Li, H. Yang, P. Wang, Y. Li, Quaternion polar complex exponential transform for invariant color image description. Appl. Math. Comput. **256**, 951–967 (2015)
23. L. Weng, B. Preneel, A secure perceptual hash algorithm for image content authentication. IFIP Int. Fed. Inf. Process. **7025**, 108–121 (2011)
24. Y. Zhao, Perceptual image hash using texture and shape feature. J. Comput. Inf. Syst. **8**(8), 3519–3526 (2012)
25. Y. Zhao, S. Wang, G. Feng, Z. Tang, A robust image hashing method based on Zernike moments. J. Comput. Inf. Syst. **6**(3), 717–725 (2010)
26. Y. Zhao, Y. Yuan, W. Wei, Extraction of shape feature for image hash. J. Comput. Inf. Syst. **7**(16), 5660–5667 (2011)