Robust Hashing Based on Quaternion Gyrator Transform for Image Authentication

JUNLIN OUYANG1,2, XIAO ZHANG1, AND XINGZI WEN1

1School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China
2Hunan Software Vocational Institute, Xiangtan 411201, China

Corresponding author: Xiao Zhang (zhangxiaocoding@163.com)

This work was supported in part by the Natural Science Foundation of Hunan Province for Youths under Grant 2019JJ50168, in part by the Youth Fund For Humanities and Social Sciences Research of The Ministry Of Education under Grant 20YJCZH179, and in part by the Hunan Provincial Department of Education Innovation Platform Open Fund Project under Grant 19K035.

ABSTRACT Image hashing is one of the most effective methods in many image processing applications including image recognition or authentication, tampering detection, image retrieval, etc. In this paper, we propose a novel image hash method based on quaternion gyrator transform, which is more secure and compact in addition to its robustness and discriminative properties. In this proposed method, the quaternion gyrator transform (QGT), like the traditional quaternion Fourier transform which is a linear regular integral ratio transform is applied to effectively extract image features. Firstly, our hash function needs to scale all pictures to a fixed size. And the quaternion gyrator transform is used to transform each non-overlapping block in the original image for extracting the feature map of the source image. For each block, the inner product of the feature and a random weight is used to be one bit of the final image hash. Experiments with different image databases are conducted to test and verify the efficiency of our method. The result has proved that our method of constructing hash is robust to most of the content-preserving operations with a good distinction. Compared with some state-of-the-art hash algorithms, our algorithm is more excellent and has better performance in robustness and distinguishability.

INDEX TERMS Robust hashing, image authentication, quaternion gyrator transform, image feature.

I. INTRODUCTION

The continuous development and widespread popularity of mobile devices have brought convenience to people’s lives. However, many new problems were born at the same time. For example, the huge amount of data brings huge pressure to the server storage, especially the problem of insufficient storage caused by multiple users repeatedly storing the same pictures on the server. Meanwhile, a large number of ultra-high-definition pictures on the network may be damaged during transmitted. The attacker maliciously tampers with the image without changing the original semantic information of the picture. Therefore, it is very necessary to research and explore a new and effective technical method for image compression and image authentication.

In recent years, in order to solve the problem of image authentication, many solutions have been proposed, which have achieved good results under sufficient research. For image authentication, digital watermarking is one of effective solutions. Digital watermarking [1], [2] can be effectively embedded in the image with little change in the original picture. We authenticate the image by detecting the watermark to determine whether the image has been changed. However, some applications do not allow any small changes in image content and quality.

A more effective technical method is image hashing. The nature of image hashing can effectively reduce the pressure of storage and retrieval. For the image retrieval [3]–[9], experts design many adversarial hash learning models that receive good results. The hash algorithm also has some applications in video. Song et al. [10] propose a novel unsupervised video hashing framework dubbed Self-Supervised Video Hashing (SSVH). This algorithm adequately explores the temporal order of video frames in an end-to-end learning-to-hash fashion. Zhou et al. [11] propose a new entropy equilibrium optimization (EEO) methodology to enhance the coding performance of VR360 videos. Based on this method, he designs two algorithms, EEOA-ERP and...
EEOA-CMP, to enhance compression efficiency for the ERP and CMP pictures. Meanwhile, a good image hashing algorithm is robust and discriminative and can handle the problem of image authentication. Robustness means that image hashes of visually identity images should be the same or similar. In other words, image hashing is robust to resist different digit operations. This property guarantees that similar images can be retrieved faster, reducing the pressure of servers. Discrimination means that different images should produce different hashes. The image hash algorithm needs to be excellent in both characters.

Many researchers propose many efficient techniques to accelerate the development of image hashing. For example, the Radon transform is used to construct hashes. The characteristic of the Radon transform [12] determines that this scheme can resist small-angle image transformation problems. The discrete Fourier transform (DFT) based on the polar system and random key [13] ensures the security of hash. Quaternion discrete Fourier transform (QDFT) based on log-polar system [14] can effectively maintain the robustness of hashing. Tang et al. [15] propose a method based on visual attention and invariant moments, using a model presented by Itti et al. [16] to give weight to the LL sub-band of one level 2D discrete wavelet transformation (DWT), and using invariant moments to parse to improve the robustness and distinguishability of hash. Using the center-symmetric local binary patterns (CSLBP) to extract features and singular value decomposition (SVD) [17] has a good effect on resisting large-angle rotation and noise, contrast, brightness, compression. Tang et al. [18] utilize DWT and phase spectrum of Fourier transform (PFT) to collaboratively extract image features and ring partition to construct the final hash, which improves the distinguishing effect compared to other known methods. Quaternion singular value decomposition (QSVD) [19] is first applied to image hashing. After converting the image to the CIELab color domain, using QSVD to decompose each block to construct a hash, it also improves the discrimination ability and stability. Hamid et al. [20] exploit that the Laplacian pyramid is used to generate image hashing firstly. Two different pyramids can be generated by using different filters. The difference between the two Laplacian pyramids are calculated to obtain a unique and robust hash, which prevents non-malicious operations and detect minor tampering. One algorithm based on local color features [21] considers all the components of the color image and has a good distinction. Image hashing based on the color vector angle [22] divides the image into blocks to extract vector information and uses discrete wavelet transform to compress the feature matrix to form the image hash, which can resist normal digital operations. Laradji et al. [23] propose the quaternion Fourier transform (QFT) to calculate the hash. QFT hash improves discriminating ability, but its robustness is not good enough. Ouyang et al. [24] exploit that quaternion zernike moments (QZMs) offer a sound way to jointly deal with the three channels of color images without discarding chrominance information. This hash function based on QZMs provides a short hash and is robust to most common image content-preserving. Yan et al. [25] design the quaternion Fourier-Merlin transform to deal with localized tampering. Karsh et al. [26] extract global and local features through ring division and Markov probability to construct a hash for authentication. Qin et al. [27] exploit block truncation coding to design an image hashing algorithm with good perceptual robustness. Li and Guo [28] use sparse coding to construct an image hash for content recognition.

Since most of recent image hashing algorithms converted the color image into gray-scale one and lost the structure information of three color channels and the chrominance information, they didn’t reach satisfactory performances on processing color image. Focusing on the problems mentioned above, we utilize QGT to design an image hashing algorithm. Firstly, quaternions can obtain the important structural information of the color image and receive the optimal representation of the color. Many key issues have been well solved taking the advantage of this skill, such as image watermarking [29], image recognition [30], image quality assessment [31]. Secondly, QGT can be realized by phase modulation and quaternion discrete Fourier transform(QDFT). Accordingly, low-frequency coefficients of QGT embodies most information of image and important image features.

The contributions of our study are as follow: (1) We propose a robust image hash algorithm based on the QGT to convert images to binary codes for image authentication. This is the first method to capture the representation of image content by QGT. (2) Our method generates the binary codes in an unsupervised fashion. As a result, we address the problem that large amounts of data in supervised learning need to be labeled. (3) By performing QGT with a rotation angle of $\alpha$ on the color image, the security of our proposed hash algorithm can be guaranteed by it. Many experiments are conducted to verify the efficiency of our function, the result shows that our proposed algorithm building a novel and compact image hash has greatly improved on robustness to content-preserving operations and discrimination compared with other existing hash algorithms.

II. RELATED WORK

Quaternion [32], an extension of a complex number, is a hypercomplex number, which was first described in 1843 and defined in a four-dimensional space by Hamilton. The structure of the quaternion can well represent the color structure information of the color image. Based on this characteristic, the quaternion is widely used in image processing. From the perspective of mathematics, a quaternion $q$ is represented as:

$$\hat{q} = q_0 + q_1i + q_2j + q_3k$$

Among them, $q_0$, $q_1$, $q_2$, $q_3$ are real numbers, and $i$, $j$, $k$ are imaginary parts, which satisfy the following:

$$i^2 = j^2 = k^2 = ijk = -1, \quad ij = -ji = k$$
$$jk = -kj = i, \quad ki = -ik = j$$

(2)

At the same time, quaternions have the following operations:
conjunctive: \( \hat{q}^* \) of \( \hat{q} \): \( \hat{q}^* = q_0 - q_1i - q_2j - q_3k \)

- quaternion norm: \( |q| = \sqrt{q_0^2 + q_1^2 + q_2^2 + q_3^2} \)
- scalar multiplication: \( \lambda q = \lambda q_0 + \lambda q_1i + \lambda q_2j + \lambda q_3k \)

For color images, we can use pure quaternions to represent a pixel:

\[
Q = 0 + R(x, y)i + G(x, y)j + B(x, y)k
\]

where \( R, G, \) and \( B \) functions respectively represent the red, green, and blue channels of the RGB image at this point \((x, y)\). The Gyrator transform [33] originates from the first-order optical system for the free combination of generalized cylindrical lenses studied by the Spanish scholar Rodrigo et al. in 2006. Because the parameter of the transformation is the rotation angle, it is named Gyrator transformation.

Generalized the gyrator transform in two dimensions to the quaternion domain [34]:

\[
G_q^2[f(x, y)](u, v) = \iint f(x, y)K_q(u, v; x, y)dxdy
\]

\( f(x, y) \) is the RGB color image expressed by pure quaternion, \( K_q(u, v; x, y) \) is the kernel function of the transformation, and its expression is:

\[
K_q(u, v; x, y) = \frac{1}{|\sin \alpha|} \exp \left( \frac{\mu 2\pi (uv + xy) \cos \alpha - (uv + vx)}{\sin \alpha} \right)
\]

where \( \mu \) is a unit quaternion, \( \mu^2 = -1 \). At the same time, the quaternion gyrator transform and the quaternion Fourier transform have some relationship represented in this paper [34], that the quaternion gyrator transform with the rotation angle of \( f(x, y) \) is equivalent to a three-step operation, performing a phase modulation, undergoing a quaternion Fourier transform, and performing a phase modulation on this function.

\[
G_q^2[f(x, y)](u, v) = \frac{F_r\left[f(x, y)h(x, y)\left(\frac{v}{\sin \alpha}, \frac{x}{\sin \alpha}, \frac{u}{\sin \alpha}\right)\right]}{|\sin \alpha|} g(u, v)
\]

where \( h(x, y) \) and \( g(u, v) \) is:

\[
h(x, y) = e^{i2\pi \frac{xy \cot \alpha}{\sin \alpha}}
\]

\[
g(u, v) = e^{i2\pi \frac{uv \cot \alpha}{\sin \alpha}}
\]

### III. THE APPROACH

As is shown in Fig. 1, the image hash algorithm proposed in this article consists of three steps. In the first step, we will process the input image into a uniform size by bicubic interpolation, and divide the normalized image into image blocks that do not overlap each other. In the second step, the local block features map is extracted through the quaternion gyrator transform. In the third part, by compressing the feature map to a vector and inner product with the random vector, it is converted into the final hash by the binarization function. The difference between hashes will be calculated by the Euclidean distance. Our algorithm is described in detail below.

**FIGURE 1. The process of image hash.**

### A. PREPROCESSING

Since the actual pictures will have different sizes, we need to first unify the size of the input image through the bicubic interpolation method to ensure that the hash generated later is a fixed size. All input images are uniformly scaled to the size of \( M \times M \), and then the input image is divided into \( N \times N \) sub-blocks by non-overlapping blocks. Thus, the total number of sub-blocks is \( k \equiv (M/N)^2 \). For example, if the input image size is 64 \( \times \) 64 and the block size is 8 \( \times \) 8, the number of blocks is 64. Different block sizes will affect the robustness and distinguishability of the final hash, and we will verify the optimal block strategy through experiments. For each pixel of the input image, the color domain is converted to the quaternion domain by Eq. (1).

### B. FEATURE EXTRACTION

The feature extraction part uses the QGT transformation with angle \( \alpha \). The quaternion gyrator transformation can be realized by dividing the single-channel gyrator operation into three times [34]. We adopt another way to realize the quaternion gyrator transform through the quaternion Fourier transform.

\[
G_q^2[f(x, y)](u, v) = F_r^{-1}\left[F_r^2(f(u, v)F_r^2(u, v))\right] p(u, v)
\]

That is QGT can be realized by calculating the quaternion Fourier transformation twice. Suppose \( G(x, y) \) is the feature matrix of \( f(x, y) \) transformed by QGT. We get the feature matrix of the real domain by the following formula.

\[
\hat{G}(x, y) = \text{mod}(G(x, y))
\]

where ‘mod’ is the quaternion norm mentioned above.

For each block of the input picture \( B_i \), the above operations are performed. The features with a size of \( r \times r \) in the center area of the converted matrix are intercepted in each block and expanded to a one-dimensional vector to obtain the final feature vector \( C_i \) (\( i = 1, 2 \ldots k \)). We normalize the data of each vector.

\[
\hat{C}_i = \frac{c_j - u_i}{\delta_i + \lambda}, c_j \in C_i \left(i = 1, 2 \ldots r^2\right)
\]

where \( u_i, \delta_i \) are respectively the mean and standard deviation of \( C_i \) and defined as follows:

\[
u_i = \frac{1}{r^2} \sum_{j=1}^{r^2} c_j
\]

\[
\delta_i = \sqrt{\frac{\sum_{j=1}^{r^2} (c_j - u_i)^2}{r^2 - 1}}
\]
\( \lambda \) is a very small value to prevent division by zero. \( r \) means the size of the center of the blocks.

**C. HASH GENERATION**

For each normalized feature vector \( \hat{C}_i \), we use the following formula to get the approximate hash value of the first step:

\[
H_B(i) = \left[ \hat{C}_i * L + 0.5 \right]
\]

(13)

where \( L \) is a random vector of length \( r^2 \) generated by a positive integer key.

Next, we take the following binarization operation for each \( H_B(i) \):

\[
\hat{H}_B(i) = \begin{cases} 1, & \text{if } h_j > h_{j+1} \\ 0, & \text{if } h_j \leq h_{j+1} \end{cases} \quad h_j \in H_B(i)
\]

(14)

where \( j = 1, 2 \cdots k \).

**D. SIMILARITY EVALUATION**

The similarity between the pictures is calculated by the Euclidean distance of their corresponding hashes. For example, the hash vectors of two pictures are as follows: \( H_1, H_2 \), then the formula is as follows.

\[
d(H_1, H_2) = \sqrt{\sum_{l=1}^{N} [h_1(l) - h_2(l)]^2}
\]

(15)

where \( h_1(l) \) and \( h_2(l) \) are the \( l \)th element of hashes. We set a threshold \( T \). If the distance is greater than \( T \), it is a different image, otherwise, it is a similar image.

**IV. EXPERIMENTS**

In this experiment, we set \( M = 512, N = 64, k = 64, \alpha = \pi / 2, \lambda = 0.001 \) for the algorithm proposed above. As a result, we finally get an image hash, the length of which is 64 bits. We will discuss the robustness and discriminative of this algorithm separately in Section A and B. We will discuss in Section C whether rounding and binarization will reduce accuracy while reducing storage pressure. Section D gets the verification of hash security.

The receiver operating characteristics (ROC) [35] is to evaluate the effect of different thresholds. The x-axis is denoted by the false positive rate (PFPR) and the y-axis shows the true positive rate (PTPR). They indicate the ability of robustness and discrimination separately and are defined as follows:

\[
P_{TPR}(\lambda) = \frac{n_1(D_1 < \lambda)}{N_1}
\]

\[
P_{FPR}(\lambda) = \frac{n_2(D_1 < \lambda)}{N_2}
\]

(16)

We utilize the area under the ROC curve (AUC) [35] for quantitative comparison. The range of AUC is \([0, 1]\), and the value of AUC implies better performance if bigger.
FIGURE 3. The distribution of distances in different content-preserving operations. The red line represents the average Euclidean distance between the original hash of all images in the dataset and the hash of ones affected by the same noise type and the same parameter. The blue line represents the average Euclidean distance of all images hash in this dataset under the influence of all the different parameters of this type of noise.
A. ROBUSTNESS
We adopt the Kodak database [36] to verify the robustness of our hash algorithm. The image database contains 24 images, and its size is 512 $\times$ 768 or 768 $\times$ 512. Fig. 2 represents some images of this database. We employ content preservation operations to simulate robust attacks to generate additional image sets. The operations used include JPEG compression, Gaussian noise, Salt and Pepper noise, Gaussian filter, Median filter, Image scaling, Image rotation, Contrast adjustment, Brightness adjustment, etc. More details will be reflected in Table 1 in which there are 58 operations in total. In this case, the image collection of this experiment contains a total of $24 \times 59 + 24 = 1440$ images.

Fig. 3 shows the distribution of the Euclidean distance of different operations with different parameters, the x-axis is the parameter transformation, and the y-axis is the average distance of the 24 images from the original image under such operations. As shown in Fig.3.j, we set different parameters from 0.6 to 1.3 in the brightness adjustment. It can be seen that the mean values of normalized Euclidean distances of similar images under different parameter values fluctuate from 0.01 to 0.015. The blue line also means that the average Euclidean distance of all images hash in this dataset under all the different parameters is smaller than 0.02. In a word, the distance under all operations will not exceed 0.025. When we set the threshold to 0.022, our algorithm distinguishes whether it is a similar image with a probability of 99.9%. In a word, our algorithm performs well in robustness.

B. DISCRIMINATION
Here we use the UCID database [37] to verify the distinguishing effect of our algorithm. The image size of the data set is 384 $\times$ 512, or 512 $\times$ 384. The data set has 1338 color images in total, partly shown in Fig. 4. Each image hash will calculate Euclidean distance from other different image hashes, so we get 1338$\times$1337/2=894453 results. The total distribution is
shown in Fig. 5(b). At the same time, we copy the operation of the robust experiment and display its distribution diagram in Fig. 5(a). Among the two figures, the x-axis is the distance, and the y-axis is the frequency. As described in these two pictures, the minimum distance between different pictures is greater than 0.03, and the highest value is 0.093, the average value is 0.066, and the variance is 0.008. So the hash distance for different images is much larger than it of similar images. This also proves that our hash scheme is very effective in distinguishing. Table 2 shows that as the threshold changes,
the probability that similar pictures are judged to be similar is increasing, while the probability that different pictures are considered similar pictures is decreasing. It also told us that when the threshold $\theta = 0.022$, the error rate is the lowest. From the distribution histogram, we can also see that the 0.022 threshold is the most appropriate.

### C. EFFECT OF HASH LENGTH ON PERFORMANCE

In the algorithm, we have a rounding and binarization process for the hash. As shown in Fig. 6, the effect of the two aspects after rounding will be better than or approximately equal to that of the unrounding’s, and the effect after binarization is better than that without binarization. For unrounded matrices, the storage of a floating-point number generally consumes four bytes or eight bytes, one of which contains 8 bits. So the minimum per hash will occupy $64 \times 8 = 512$ bits. After rounding, the integer in all hash vector range from -8 to 16, which requires at least 5 bits to represent it, then a hash has $5 \times 64 = 320$ bits. For the binary hash, only 64 bits are needed to represent, greatly reducing the space consumed by hash storage. Meanwhile, there is no negative effect on robustness and discrimination.

### D. SECURITY

Color image Lena is selected as a test image to test the security of our image hashing. In the following steps, a group of secret keys is firstly used to control the hash generation of Lena. Then, another 100 different groups of secret keys are exploited to extract image hashes of Lena. Finally, the Euclidean distances between the first hash and the other 100 hashes are calculated. The results are presented in Fig. 7, where the x-axis is the index of wrong keys and the y-axis is the Euclidean distance. It is observed that the maximum and minimum ones are 0.39105 and 0.01408, the mean and standard deviation are 0.13468 and 0.09153 respectively. The mean distance is much bigger than most mean values of similar images. This illustrates the good security of our algorithm.

### V. PERFORMANCE COMPARISONS

To show the advantages of our algorithm, we select some excellent algorithms to compare. The selected algorithms include Random-walking hash algorithm [38], QSVD hash algorithm [19], SVD-CSLBP hash algorithm [17], Laplacian Pyramids hash algorithm [20], A hash algorithm based on deep convolutional neural network (DCNN) [39]. These algorithms above are hash algorithms recently published in journals or conferences. In order to show the fairness of the experiment, we uniformly set the image size to $512 \times 512$ to conduct the experiment. As shown in Fig. 8, we will compare
In this paper, we propose a robust hash algorithm based on quaternion gyrator transform for image authentication. After a lot of tests, experiments show that our algorithm is robust to JPEG compression, contrast adjustment, filtering, and other content-retention operations. The comparison of ROC curves shows that our proposed hash algorithm is superior to the existing methods in robustness and discrimination. Meanwhile, our hash code is more compact and shorter. Future work will be focused on two subjects. First, we will apply the idea of this hash algorithm to CBIR (Content-based image retrieval). Second, due to the excellent performance of our method in image processing, we will introduce a content-based model to video hashing.

**REFERENCES**

[1] B. Swapna, M. Kamalahan, S. Srinidhi, S. Sowmyia, S. Vasanth, and P. S. Divyabharathi, “Digital picture watermarking technique for security applications,” in *Proc. IOP Conf. Ser. Mater. Sci. Eng.*, vol. 872, no. 1, 2020, Art. no. 012001.

[2] J. Ouyang, G. Coatireux, B. Chen, and H. Shu, “Color image watermarking based on quaternion Fourier transform and improved uniform log-polar mapping,” *Comput. Electr. Eng.*, vol. 46, pp. 419–432, Aug. 2015.

[3] D. Wang, G. Song, and X. Tan, “Bayesian denoising for robust image retrieval,” *Pattern Recognit.*, vol. 86, pp. 134–142, Feb. 2019.

[4] M. Zhou, X. Zeng, and A. Chen, “Deep forest hashing for image retrieval,” *Pattern Recognit.*, vol. 95, pp. 114–127, Nov. 2019.

[5] D. Wu, Q. Dai, J. Liu, B. Li, and W. Wang, “Deep incremental hashing network for efficient image retrieval,” in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jan. 2019, pp. 9069–9077.

[6] X. Lu, W. Chen, and X. Li, “Discrete deep hashing with ranking optimization for image retrieval,” *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 31, no. 6, pp. 2052–2063, Jun. 2020.

[7] C. Liu, J. Ma, X. Tang, F. Liu, X. Zhang, and L. Jiao, “Deep hash learning for remote sensing image retrieval,” *IEEE Trans. Geosci. Remote Sens.*, early access, Jul. 17, 2020, doi: 10.1109/TGRS.2020.3007533.

[8] J. Yang, Y. Zhang, R. Feng, T. Zhang, and W. Fan, “Deep reinforcement hashing with redundancy elimination for effective image retrieval,” *Pattern Recognit.*, vol. 100, Apr. 2020, Art. no. 107116.

[9] J. Song, T. He, L. Gao, X. Xu, A. Hanjalic, and H. T. Shen, “Unified binary generative adversarial network for image retrieval and compression,” *Int. J. Comput. Vis.*, vol. 128, pp. 2243–2264, Feb. 2020.

[10] J. Song, H. Zhang, X. Li, L. Gao, M. Wang, and R. Hong, “Self-supervised video hashing with hierarchical binary auto-encoder,” *IEEE Trans. Image Process.*, vol. 27, no. 7, pp. 3210–3221, Jul. 2018.

[11] Y. Zhou, L. Tian, C. Zhu, X. Jin, and Y. Sun, “Video coding optimization for virtual reality 360-degree source,” *IEEE J. Sel. Topics Signal Process.*, vol. 14, no. 1, pp. 118–129, Jan. 2020.

[12] Y. L. Liu, G. J. Xin, and Y. Xiao, “Robust image hashing using radon transform and invariable features,” *Radioengineering*, vol. 25, no. 3, pp. 556–564, Sep. 2016.

[13] A. Swaminathan, Y. Yao, and M. Wu, “Robust and secure image hashing,” *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp. 215–230, Jun. 2006.

[14] J. Ouyang, G. Coatireux, and H. Shu, “Robust hashing for image authentication using quaternion discrete Fourier transform and log-polar transform,” *Digit. Signal Process.*, vol. 41, pp. 98–109, Jun. 2015.

[15] Z. Tang, H. Zhang, C.-M. Pun, M. Yu, C. Yu, and X. Zhang, “Robust image hashing with visual attention model and invariant moments,” *IEEE Image Process.*, vol. 14, no. 5, pp. 901–908, Apr. 2020.

[16] L. Itti, C. Koch, and E. Niebur, “A model of saliency-based visual attention for rapid scene analysis,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 20, no. 11, pp. 1254–1259, Nov. 1998.

[17] R. Darvazani, S. Mozaffari, and K. Yaghmai, “Perceptual image hashing using center-symmetric local binary patterns,” *Multimedia Tools Appl.*, vol. 75, no. 8, pp. 4639–4667, Apr. 2016.

[18] Z. Tang, Y. Yu, H. Zhang, M. Yu, C. Yu, and X. Zhang, “Robust image hashing via visual attention model and ring partition,” *Math. Biosci. Eng.*, vol. 16, no. 5, pp. 6103–6120, 2019.

[19] Z. Tang, M. Yu, H. Yao, H. Zhang, C. Yu, and X. Zhang, “Robust image hashing with singular values of quaternion SVD,” *Comput. J.*, Dec. 2019, doi: 10.1093/comjnl/bxz127.

[20] H. Hamid, F. Ahmed, and J. Ahmad, “Robust image hashing scheme using Laplacian pyramids,” *Comput. Electr. Eng.*, vol. 84, Jun. 2020, Art. no. 106468.

[21] Z. Tang, X. Zhang, X. Dai, J. Yang, and T. Wu, “Robust image hash function using local color features,” *AEU–Int. J. Electron. Commun.*, vol. 67, no. 8, pp. 717–722, Aug. 2013.

[22] Z. Tang, L. Huang, F. Yang, Y. Dai, and X. Zhang, “Robust image hashing via colour vector angles and discrete wavelet transform,” *IET Image Process.*, vol. 8, no. 3, pp. 142–149, Mar. 2014.

[23] I. H. Laradji, L. Ghouti, and E.-H. Khiari, “Perceptual hashing of color images using hypercomplex representations,” in *Proc. IEEE Int. Conf. Image Process.*, Sep. 2013, pp. 4402–4406.

[24] J. Ouyang, X. Wen, J. Liu, and J. Chen, “Robust hash based on quaternion Zernike moments for image authentication,” *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 12, no. 4s, pp. 1–13, Nov. 2016.

[25] C.-P. Yan, C.-M. Pun, and X.-C. Yuan, “Quaternion-based image hashing for adaptive tampering localization,” *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 12, pp. 2604–2677, Dec. 2016.

**TABLE 3. Performance comparisons among different algorithms.**

| Algorithm                  | AUC   | Average time(s) | Hash length |
|----------------------------|-------|-----------------|-------------|
| Random-walking hashing     | 0.94938 | 0.05             | 144 bits    |
| QVD                        | 0.99928 | 0.52             | 640 bits    |
| SVD-CLSBP                  | 0.8656 | 0.13             | 64 decimal digit |
| Laplacian Pyramids         | 0.90406 | 0.08             | 1024 decimal digit |
| DCNN                       | 0.97976 | 0.05             | 64 decimal digit |
| Our algorithm              | 0.99968 | 0.61             | 64 bits     |

**VI. CONCLUSION**

In this paper, we propose a robust hash algorithm based on quaternion gyrator transform for image authentication. The ROC curve of our algorithm is closer to the upper left corner of the hash algorithm than other comparison curves. Therefore, it can be intuitively concluded that our algorithm has better classification performance than the comparison algorithm. For quantitative analysis, the AUC of all hash algorithms is also calculated. Their AUC and ours are (0.949), (0.988), (0.996), (0.99928), (0.864), (0.904), (0.979) and (0.99968). At the same time, we use the same machine to measure the average time of hash generation by different algorithms. As shown in Table 3, the shortest hash length in our optimal case is only 64 bits. So our hash algorithm is better than other hash algorithms overall.
[26] R. K. Karsh, A. Saikia, and R. H. Laskar, “Image authentication based on robust image hashing with geometric correction,” *Multimedia Tools Appl.*, vol. 77, no. 19, pp. 25409–25429, 2018.

[27] Q. Qin, X. Chen, D. Ye, J. Wang, and X. Sun, “A novel image hashing scheme with perceptual robustness using block truncation coding,” *Inf. Sci.*, vol. 361–362, pp. 84–99, Sep. 2016.

[28] Y. Li and L. Guo, “Robust image fingerprinting via distortion-resistant sparse coding,” *IEEE Signal Process. Lett.*, vol. 25, no. 1, pp. 140–144, Jan. 2018.

[29] P.-P. Niu, L. Wang, X. Shen, S.-Y. Zhang, and X.-Y. Wang, “A novel robust image watermarking in quaternion wavelet domain based on superpixel segmentation,” *Multidimensional Syst. Signal Process.*, vol. 31, no. 2, pp. 1–22, Mar. 2020.

[30] J. Miao and K. I. Kou, “Quat.enion matrix regression for color face recognition,” 2020, arXiv:2001.10677. [Online]. Available: http://arxiv.org/abs/2001.10677

[31] Q. Sang, Y. Yang, L. Liu, X. Song, and X. Wu, “Image quality assessment based on quaternion singular value decomposition,” *IEEE Access*, vol. 8, pp. 75925–75935, 2020.

[32] W. R. Hamilton, “Theory of quaternions,” *Proc. Roy. Irish Acad.*, vol. 3, pp. 1–16, Jan. 1844.

[33] T. Alieva, J. A. Rodrigo, and M. L. Calvo, “Introduction to gyrator transform,” in *Proc. AIP Conf.*, 2007, pp. 256–263.

[34] S. Zhu-Hong, “A study on quaternion transforms for color image processing,” Ph.D. dissertation, School Comput. Sci. Eng., Southeast Univ., Dhaka, Bangladesh, 2015.

[35] T. Fawcett, “An introduction to ROC analysis,” *Pattern Recognit. Lett.*, vol. 27, no. 8, pp. 861–874, Jun. 2006.

[36] R. Franzen. (1999). *Kodak Lossless True Color Image Suite*. [Online]. Available: http://r0k.us/graphics/kodak

[37] G. Schaefer and M. Stich, “UCID: An uncompressed color image database,” in *Storage and Retrieval Methods and Applications for Multimedia*, vol. 5307, Bellingham, WA, USA: SPIE, 2004, pp. 472–480.

[38] X. Huang, X. Liu, G. Wang, and M. Su, “A robust image hashing with enhanced randomness by using random walk on zigzag blocking,” in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2016, pp. 14–18.

[39] C. Jiang and Y. Pang, “Perceptual image hashing based on a deep convolution neural network for content authentication,” *J. Electron. Imag.*, vol. 27, no. 4, 2018, Art. no. 043055.

---

**JUNLIN OUYANG** received the M.S. degree in computer application from Central South University, China, in 2007, and the Ph.D. degree in computer science from Southeast University, China, in 2015. He is currently a Lecturer with the School of Computer Science and Engineering, Hunan University of Science and Technology, China. His research interests include color image processing, information security and image retrieve, deep learning, image forensics, and so on.

**XIAO ZHANG** is currently pursuing the master’s degree with the School of Computer Science and Engineering, Hunan University of Science and Technology. His research interests include digital image technique, information security, deep learning, and so on.

**XINGZI WEN** received the M.S. degree in business administration, in 2007, and the Ph.D. degree in management science and engineering from Central South University, China, in 2014. She is currently a Lecturer with the Hunan University of Science and Technology, China. She is mainly engaged in research work in the software industry cluster, decision science, and complex networks.