Robust Image Hashing Using Radon Transform and Invariant Features

Yuling LIU[1], Guojiang XIN[2], Yong XIAO[1]

[1]College of Computer Science and Electronic Engineering, Hunan University, 410082 Changsha, China
[2]College of Management and Information Engineering, Hunan University of Chinese Medicine, 410208 Changsha, China

yuling_liu@hnu.edu.cn

Manuscript received October 12, 2015

Abstract. *A robust image hashing method based on radon transform and invariant features is proposed for image authentication, image retrieval, and image detection. Specifically, an input image is firstly converted into a counterpart with a normalized size. Then the invariant centroid algorithm is applied to obtain the invariant feature point and the surrounding circular area, and the radon transform is employed to acquire the mapping coefficient matrix of the area. Finally, the hashing sequence is generated by combining the feature vectors and the invariant moments calculated from the coefficient matrix. Experimental results show that this method not only can resist the normal image processing operations, but also some geometric distortions. Comparisons of receiver operating characteristic (ROC) curve indicate that the proposed method outperforms some existing methods in classification between perceptual robustness and discrimination.*

Keywords

Image hashing, radon transform, invariant centroid, invariant moments

1. Introduction

In the information era, copying and distribution of the multimedia data have become increasing convenient. However, the illegal tampering and usage of the image is a serious issue. In order to solve this problem, the traditional hash functions in cryptography and digital fragile watermarking techniques have been proposed. The hash functions such as SHA-1 and MD5 are extremely sensitive to the input data, because a bit change will result in large changes in the hash result [1]. In the digital fragile watermarking schemes, the original image will be modified for embedding the fragile watermark, which may undermine the perceived characteristics of the original image [2]. Therefore, image hashing is developed for image authentication.

Image hashing can transform an original image into a short sequence to represent its content, which is widely used in image authentication, copy detection, image retrieval, etc. Even though the original image is processed by normal image processing which do not affect the perceptual content in transmission, the extracted hash sequence remains unchanged for image authentication. As we know, perceptual robustness and discrimination are the two key issues of image hashing. Perceptual robustness requires that image hashing should be invariant to content-preserving operations. Discrimination claims that image hashing have the ability to distinguish the visually distinct images.

A variety of image hashing schemes have been proposed in recent years, including the schemes based on various transformations, the schemes based on matrix factorization, and the schemes based on invariant features. Various transformations have been applied to image hashing generation. Monga and Evans propose an image hashing method using discrete wavelet transform (DWT), but the method cannot resist contrast adjustment, gamma correction and large-angle rotation [3]. Lin and Chang develop a hashing method based on discrete cosine transform (DCT) of non-overlapping image blocks, but the method is not tolerant to geometric distortions [4]. Lefebvre et al. propose an image hashing method using the important features extracted in radon transform, which owns good robustness but lacks the ability to resist some conventional attacks [5], [6]. Lei et al. describe a robust scheme using the radon transform and moments for generating hashing sequence [7]. The scheme can resist geometric transform due to the invariant moments of the radon domain. Wu, Zhou and Niu suggest a robust hashing method based on the radon and wavelet transform which can resist the print-scan attacks, but the method doesn't own good key-dependent security [8]. Other improved radon-based hashing methods using image normalization and the key-dependent secure hashing methods based on radon transform also have been proposed [9], [10]. These methods are robust to small angle rotation, but their discriminations are not desirable. Swaminathan, Mao and Wu utilize the Fourier coefficients for hashing generation, but the scheme can only resist some common attacks [11]. Xiang, Kim and Huang present a method using the invariant shape features of histogram, but the method isn't sensitive to the changes of

image content [12]. Qin, Chang and Tsou [13] propose a hashing method based on non-uniform sampling.

Some other methods using the matrix factorization have been proposed. Kozat, Mihcak and Venkatesan divide the image into blocks and conduct the singular value decomposition (SVD) in each one for image hashing generation [14]. The non-negative matrix factorizations (NMF) are utilized to form image hashing, but these algorithms are sensitive to watermark embedding [15], [16]. A hashing method using the compressive sensing (CS) is proposed, but its discrimination is limited [17]. Tang et al. develop a dictionary framework to generate the image hash sequence, but its computational complexity and the tamper detection capability need to be improved [18].

There are also some methods using invariant features. Zhao et al. propose some hashing methods that combine the local texture features and Zernike moments for image hashing generation, which can't resist high strength noise addition and some geometric attacks, e.g. cropping [19], [20]. Tang et al. describe some robust hashing methods based on the invariant features. But these algorithms also can't resist noise addition and some geometric attacks [21], [22]. Liu, Cheng and Leung employ the wave atom transform in the hashing method, but the method doesn't own good performance of resisting geometric attacks such as scaling and translation [23]. Most of the aforementioned hashing methods are sensitive to geometric attacks. Although some methods are robust against geometric transform, but their discriminative capabilities are not desirable.

In our previously published paper, we proposed a hashing method based on log-polar mapping (LPM) and contourlet transform. The sub-band image is divided into non-overlapping blocks, and low and middle DCT frequency coefficients are selected from each block. The singular value decomposition (SVD) is applied to obtain the first digit of the maximum singular value. Finally, the features are scrambled and quantized as the safe hash bits [24]. However, in this paper, we propose a new image hashing method based on radon transform and invariant features, which is robust to ordinary image processing operations including JPEG compression, filtering, noise contamination, scaling, translation and rotation. The invariant centroid point and the circular area around the invariant point are helpful to resist geometric attacks. The radon transform is employed to obtain the rotation invariant property [7]. And then the final image hashing sequence can be generated in the radon domain. Secret key is introduced in the feature extraction. The method can satisfy the robustness against normal image processing and geometric distortions, and also have good discrimination for perceptual different images.

The rest of this paper is organized as follows. Section 2 introduces some useful tools and concepts. Section 3 describes the details of the proposed scheme. Experimental results are presented in Sec. 4. Finally, conclusions are drawn in Sec. 5.

2. Brief Description of Useful Tools and Concepts

2.1 Radon Transform

Radon transform is an effective method to analyze the signal between the spatial domain and its projection space. Let $g(r, \theta)$ denote the radon transform of a two-dimension image $f(x, y)$, which is defined as its linear integral along the line inclined at an angle θ from the x -axis and a distance r from the origin. The mathematical expression can be written as $g(r, \theta) = R\{f(x, y)\} = \iint f(x,y)\delta(r - x\cos\theta - y\sin\theta)\mathrm{d}x\,\mathrm{d}y$, where $\delta(\cdot)$ is the pulse function, $r = x\cos\theta + y\sin\theta$, and $0 \le \theta < 2\pi$. Radon transformation has excellent properties for the geometric transformations, i.e. translation, scaling and rotation.

2.2 Invariant Moments

Invariant moments, firstly introduced by Hu [25], are invariant to translation, scaling and rotation. The aim of choosing invariant moments as image features is to make the hash resilient to image rotation. Let $f(x, y)$ be gray value of a pixel in a digital image sized $m \times n$, where $0 \le x \le m$ and $0 \le y \le n$. Thus, the seven invariant moments are defined as follows:

$$\phi_1 = \eta_{20} + \eta_{02}, \tag{1}$$

$$\phi_2 = (\eta_{20} - \eta_{02})^2 + 4\eta_{11}^2, \tag{2}$$

$$\phi_3 = (\eta_{30} - 3\eta_{12})^2 + (3\eta_{21} - \eta_{03})^2, \tag{3}$$

$$\phi_4 = (\eta_{30} + \eta_{12})^2 + (\eta_{21} + \eta_{03})^2, \tag{4}$$

$$\begin{aligned}\phi_5 = {} & (\eta_{30} - 3\eta_{12})(\eta_{30} + \eta_{12})\left[(\eta_{30} + \eta_{12})^2 - 3(\eta_{21} + \eta_{03})^2\right] \\ & + (3\eta_{21} - \eta_{03})(\eta_{21} + \eta_{03})\left[3(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2\right],\end{aligned} \tag{5}$$

$$\begin{aligned}\phi_6 = {} & (\eta_{20} - \eta_{02})\left[(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2\right] \\ & + 4\eta_{11}(\eta_{30} + \eta_{12})(\eta_{21} + \eta_{03}),\end{aligned} \tag{6}$$

$$\begin{aligned}\phi_7 = {} & (3\eta_{21} - \eta_{03})(\eta_{30} + \eta_{12})\left[(\eta_{30} + \eta_{12})^2 - 3(\eta_{21} + \eta_{03})^2\right] \\ & - (\eta_{30} - 3\eta_{12})(\eta_{21} + \eta_{03})\left[3(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2\right]\end{aligned} \tag{7}$$

where $\eta_{pq}(p, q = 0,1,2,\ldots)$ are the normalized central moments defined as:

$$\eta_{pq} = \frac{\mu_{pq}}{\mu_{00}^{\gamma}} \tag{8}$$

in which γ is determined by:

$$\gamma = \frac{p+q}{2} + 1, \quad p+q = 2,3,\cdots \tag{9}$$

and μ_{pq} are the central moments calculated by:

$$\mu_{pq} = \sum_{x=0}^{m}\sum_{y=0}^{n}(x-\bar{x})^p (y-\bar{y})^q \mathrm{f}(x,y) \tag{10}$$

where

$$\bar{x} = \frac{M_{10}}{M_{00}}, \quad \bar{y} = \frac{M_{01}}{M_{00}} \tag{11}$$

and M_{pq} are the $(p + q)$-th order moments:

$$M_{pq} = \sum_{x=0}^{m}\sum_{y=0}^{n} x^p y^q \mathrm{f}(x,y) \,. \tag{12}$$

3. Image Hashing Scheme

Generally, the image hashing scheme is mainly composed of two parts: feature extraction and hash generation. Image feature extraction is the crucial stage of the hashing scheme. The important robust features are extracted to represent the main contents of the original image. Then these features will go through some quantitative procedures to form the final hash sequence. The image hashing sequence can meet the robustness to some perceptually similar operations, and have the ability to distinguish the visually distinct images.

3.1 Image Preprocessing

In order to obtain a normalized image, the original image is rescaled to a fixed size $k \times k$ with bilinear interpolation. This is based on the consideration that the real images with different sizes can generate their hashes with a fixed length and have the same computation complexity. This step can also ensure that the proposed hashing can resist image rescaling to a certain extent. We choose $k = 512$ in the experiment.

3.2 Invariant Centroid Algorithm and the Circular Area Extraction

Invariant centroid algorithm is a method to extract an invariant feature point of an image. The point will remain unchanged even if the image undergoes some normal image processing and some geometric transforms. Thus the extraction of the invariant centroid point is crucial to the robustness of the hashing scheme. Through applying an iterative approach, we can obtain the invariant centroid point, which is close to the center point of the image. Assume that the invariant centroid point of the original image F(x,y) is calculated as follows:

$$C_x = \frac{\sum_x\sum_y \mathrm{F}(x,y)x}{\sum_x\sum_y \mathrm{F}(x,y)}, \quad C_y = \frac{\sum_x\sum_y \mathrm{F}(x,y)y}{\sum_x\sum_y \mathrm{F}(x,y)} \tag{13}$$

where $x, y \in M \times N$, that is to say that they belong to the entire image. The main steps of the scheme are as follows.

- Calculate a centroid point of the original image as C_0, which is regarded as the initial value C_b of the invariant centroid, $C_b = C_0$.
- Taking C_b as the center point, extract the centroid point C_r in the circular area with the radius r_i. If $C_b = C_r$, C_r is the invariant centroid point of the image, otherwise set $C_b = C_r$.
- Set C_b as the center point and r_i as the radius, and extract the centroid point. This procedure will end until that the centroid points of two extracting are the same. The final point is the invariant centroid point, and the one near the center point is applied to obtain the circular area.
- After the extraction of the invariant centroid, the point can be set as the center of the circle and a circular area can be obtained around the point, where R is set as the radius of the circular area.

Usually, R should be a bit smaller than the length and width of the original image in order to keep the area unchanged after the translation, cropping and rotation. The image hashes can be obtained by extracting the important robust features in the circular area finally.

3.3 Image Feature Extraction

1) Local Feature Extraction

For the local features, four feature values, including zero-order moment, variance, singular value and DC component of DCT, are obtained from the selected rows, and then these values are formed a feature vector. These features all own good performance of resisting normal image processing and geometric distortions.

When the recycling translation happens on the θ axis, assuming that the rotation angle is ϕ, the zero-order moment function is defined as follows:

$$\mathrm{Z}(r) = \int_0^{2\pi} \mathrm{g}(r,\theta)\mathrm{d}\theta \,. \tag{14}$$

Thus the following relationship will be generated when the rotation happens:

$$\mathrm{Z}_1(r) = \int_0^{2\pi} \mathrm{g}(r,\theta+\phi)\mathrm{d}\theta = \int_0^{2\pi} \mathrm{g}(r,\theta')\mathrm{d}\theta' = \mathrm{Z}(r) \,. \tag{15}$$

The zero-order moment of radon coefficient line can be regarded as an invariant feature. And the variance of the corresponding line can also be used as a feature value.

$$m = \frac{1}{len}\sum_{j=1}^{len} \mathrm{g}_i(j) \,, \tag{16}$$

$$\sigma = \frac{1}{len-1}\sum_{j=1}^{len}\left[\mathrm{g}_i(j) - m\right]^2 \tag{17}$$

where i and j respectively represent the number of line and the number of coefficient in each line. *len* represents the length of a line, m indicates the mean value, and $g_i(j)$ expresses the coefficient values of each line. Since the SVD decomposition owns good performance of resisting geometric attacks [14], the maximum singular value of each line is considered as a feature value. We apply the discrete Fourier transform to each line for resisting translation attacks since the generated coefficients remain constant. Because the real parts of coefficients have more stability, and the imaginary parts can easily be changed by some common attacks, the real parts of the coefficients are extracted to compose another matrix which owns good performance of resisting ordinary attacks. All of the elements are the real parts of coefficients, which are not sensitive to changes caused by ordinary attacks. Then DCT is conducted to the matrix, and the direct coefficient (DC) is considered as a feature value, that is because the DCT can well present the energy of the image and the DC can remain stable.

2) Global Feature Extraction

For the global features, the invariant moments of the radon coefficient matrix are firstly extracted, and then the HU moments in Sec. 2.2 are applied here. The global hashes are obtained by combining the seven HU moments together. The global features can well represent the image content and resist the geometric attacks, and have the desirable stability.

3.4 Image Hash Construction

A robust image hashing method is not only able to resist normal image processing, such as JPEG compression, noise addition, filtering and other manipulations, but also can resist geometric distortions such as rotation, scaling and translation. Therefore, the hashing sequences extracted from perceptually the same images, should be same or similar. And the hashing sequences extracted from the perceptually different images should be significantly different. The distance of similarity between two different images should be great enough.

The proposed hashing generation algorithm can be described as Fig. 1. The steps of the algorithm are as follows.

Input: the original image I, the key K

Output: the hashing sequence H

Begin:

(1) Image preprocessing.

(2) Extract the invariant centroid region.

(3) Extract the circular area around the invariant centroid.

(4) Apply radon transform to the circular area.

(5) Generate the random sequences using the logistic chaotic system based on K, which it is applied to select 15 coefficient lines. For each coefficient line, compute the zero-order moment, variance, singular value, DC component of DCT to obtain the local features.

(6) Extract the invariant moments of the radon coefficient matrix to obtain the global features.

(7) Combine the local features and the global features to concatenate the final hash sequence H.

(8) Append H to the original image I, and then transmit it to the receiver.

End

The final hashing sequence H can be formed by combining local hashes with global hashes. The hash length L is 67 ($67 = 4 \times 15 + 7$) decimal digits.

3.5 Image Authentication

In the image authentication stage, hash H_1 is first generated from the suspect image with the same process as the original hash H. Then H_1 is compared with the original H with the Euclidean distance. The Euclidean distance is defined as follows:

$$d\left(H, H_1\right) = \sqrt{\sum_{i=1}^{L}\left[H\left(i\right) - H_1\left(i\right)\right]^2} \tag{18}$$

where $H(i)$ and $H_1(i)$ represent the i-th value of the original hashing sequence and the extracted hashing sequence, respectively. By comparing the hash distance d, generally the distance of perceptually similar images is small, and the distance of the perceptually different images is relatively

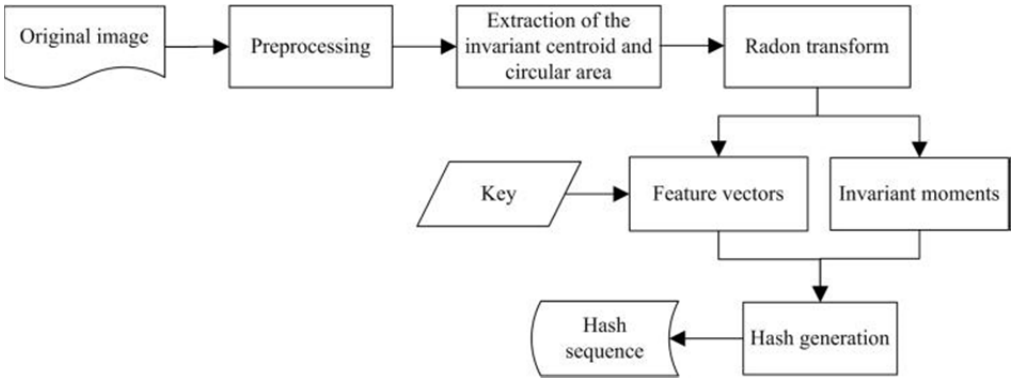


Fig. 1. Block diagram of the hash generation.

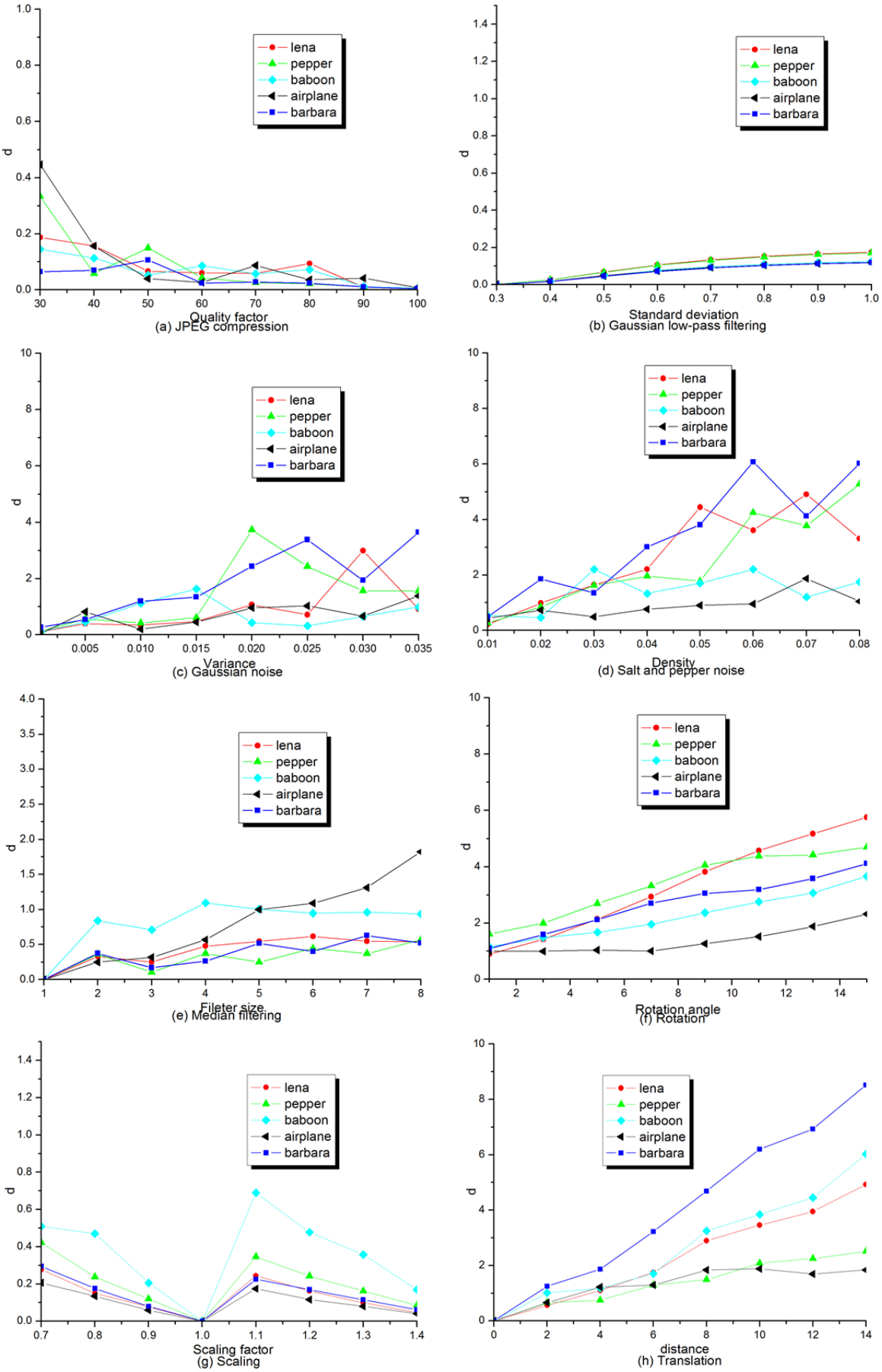


Fig. 2. The results of resisting different attacks.

great. A threshold T can be set according to the experiments, if $d \le T$, the image is authentic and the two images are visually similar, otherwise the two images are perceptually different.

4. Experimental Results

The proposed scheme is run in Windows 7 and realized with Matlab2012a. Several standard test images with the size of 512×512 are used, such as 'lena', 'baboon', 'barbara', 'fullgold', 'airplane' and 'pepper'. The image database of Columbia University is also used for the overall analysis of performance. We use these test images under the commonly used image manipulations and malicious tampering to analyze the experimental results.

Robustness means that the hashing values are not changed significantly after ordinary image processing and geometric distortions, which can ensure the image authentication. Discrimination means that the hashing values are different when the images are perceptually distinct or maliciously tampered, which reflects the image integrity. Here, we mainly validate the robustness and discrimination of the proposed hashing

4.1 Security Analysis

During the process of the image hash generation, the logistic chaotic scrambling encryption step is introduced, and hence it is necessary to have the corresponding key. Moreover, the chaotic system is sensitive to the initial value, so that even small difference can vary widely, which means that if the key is correct, the right hash sequence can be obtained; if the key is not correct, the extracted hash sequence is different. Thus the proposed hash sequence has better security.

4.2 Robustness Analysis

The experiments of robustness analysis are mainly aimed at the robustness against the content-preserving attacks. The hashing values should remain similar when these attacks happen, including the ordinary image processing operations such as JPEG compression, Gaussian noise, salt and pepper noise, median filtering, Gaussian filtering, also including some geometric distortions such as scaling, translation and rotation. We extracted image hashes of the original images and their distorted versions, and then calculated their distances. For space limitation, only the results of five standard color images sized 512×512, including Lena, Peppers, Baboon, Airplane and Barbara, are taken for example. The experiments demonstrate that the proposed scheme not only can resist the ordinary image processing, but also the geometric attacks. The used manipulations and corresponding parameters for robustness experiments are listed in Tab. 1. The results are shown in Fig. 2.

Manipulation	***Description***	***Parameter values***
JPEG compression	Quality factor	30, 40, ..., 100
3×3 Gaussian low-pass filtering	Standard deviation	0.3, 0.4, ..., 1.0
Gaussian noise	Deviation	0.001, 0.005, ..., 0.035
Salt and pepper noise	Density	0.01, 0.02, ..., 0.08
Median filtering	Filter size	1, 2, ..., 8
Rotation	Rotation angle	1, 3, ..., 15
Scaling	Scaling factor	0.7, 0.8, ..., 1.4
Translation	Distance	0, 2, ..., 14

Tab. 1. The used manipulations and their parameter values.

Manipulation	**Maximum**	**Minimum**	**Mean**	**Standard deviation**
JPEG compression	0.4463	0.0042	0.0752	0.08
3*3Gaussian filtering	0.1746	0.0016	0.0842	0.05
Gaussian noise	3.7263	0.0449	1.0998	0.97
Salt and pepper noise	6.0742	0.2206	2.1595	1.63
Median filtering	1.8205	0	0.5372	0.39
Rotation	5.7560	0.8945	2.6090	1.31
Scaling	0.6892	0	0.1873	0.15
Translation	8.5170	0	2.3566	2.03

Tab. 2. Maximum, minimum and mean Euclidean distance of different manipulations and their standard deviations.

Due to the preprocessing, the original images will go through an image normalization procedure. The sizes of the images will be the same, which can resist the scaling distortion. Due to the extraction of the invariant centroid and the circular areas, the proposed scheme can resist the translation and rotation attacks. Figure 2 also shows the performances of resisting geometric attacks. The image hashes of the original image and the distorted versions are extracted, and then, their similarities are calculated using Euclidean distance. The y-axis d is the Euclidean distance of the image hashes, and the x-axis represents the parameter values of different operations. Table 2 presents the minimum, maximum and mean distance of each manipulation and its standard deviation. It can be seen that all the Euclidean distances are less than 10.

4.3 Discrimination Analysis

Discrimination means that the proposed scheme should be able to distinguish different images and the malicious operations from the content-preserving ones. In the paper, the Euclidean distance is applied to analyze the discrimination of image hashing. The greater the Euclidean distance between images, the better the discrimination.

Here, we randomly select 200 images from the image database of Columbia University for the discrimination analysis. These images contain (but not limited to) different categories including people, buildings, landscapes and so on. The sizes of these images range from 256×256 to 2048×1536. We mainly extract the hash sequences of different images and calculate the Euclidean distances between each pair of the hashes. Then the 19900 results are obtained and the distribution is shown in Fig. 3.

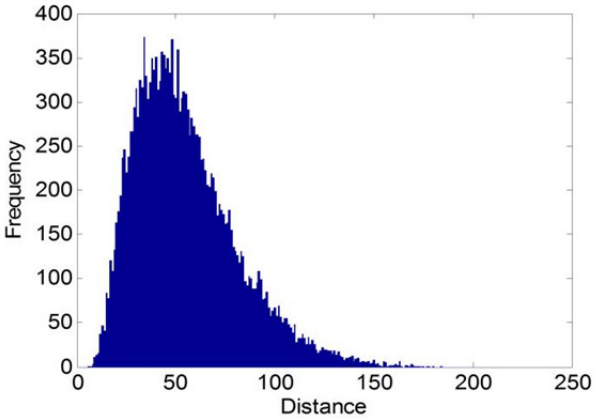


Fig. 3. Distribution of the Euclidean distances between different image hashes.

The x-axis is the Euclidean distance and the y-axis represents the number of image pairs. The minimum, maximum, mean and standard deviation of hash distances are 6.40, 184.01, 55.01, and 25.97, respectively. As shown in Fig. 3, it is clear that a small threshold can improve discrimination performance, but it may simultaneously influence the perceptual robustness. Therefore, we should select a suitable threshold in the practical applications. When the threshold equals 8.0, almost not any two different images are falsely identified as similar images. When the threshold reaches 10, only 0.12% different images are mistakenly classified as visually identical images. If the Euclidean distance between hashes is greater than the threshold, we can easily distinguish perceptual different images; otherwise we fail to detect the image. For example, we choose the threshold $T = 10$ for image authentication, which will show excellent detection performance.

According to the comparative experiments of different images in Tab. 3, the Euclidean distances of different images are all greater than 10. Thus the proposed scheme has the ability of distinguishing different images.

To further demonstrate the performance of the proposed scheme to content changing attacks, we consider the four examples of cut-and-paste image editing as shown in Fig. 4. It can be seen that the Euclidean distances of image hashes between the original images and their distorted versions are greater than 10. Moreover, we also use the above 200 images as the original images. And then we create 200×7 tampered images, where the regions of malicious operations are from 10% to 70% with a step 10% of the original image size. Experimental results show that when the percentage of malicious operations is more than 30%, the Euclidean distances of image hashes between the

Image	*Lena*	*Pepper*	*Baboon*	*Fullgold*	*Airplane*	*Barbara*
Lena	0	20.935	40.206	20.677	42.353	11.927
Pepper	20.935	0	30.795	24.848	42.505	27.091
Baboon	40.206	30.795	0	51.144	28.933	49.480
Fullgold	20.677	24.848	51.144	0	52.205	22.302
Airplane	42.353	42.505	28.933	52.205	0	51.549
Barbara	11.9274	27.091	49.480	22.302	51.549	0

Tab. 3. Euclidean distances of different standard images.

(a) $d = 35.8391$ (b) $d = 12.0733$

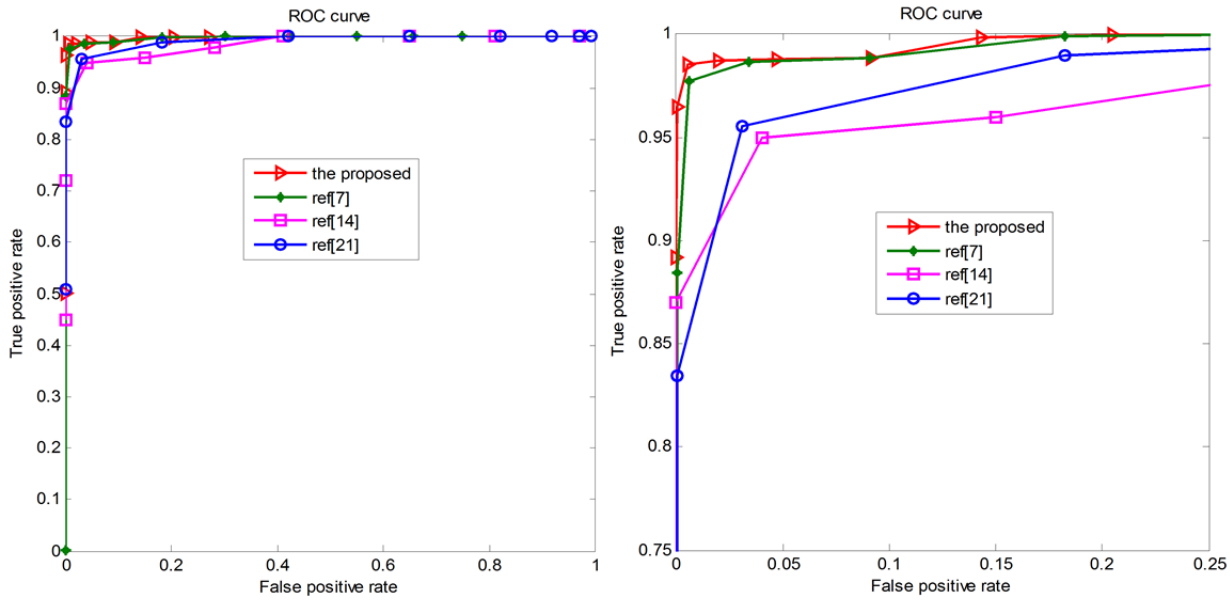
(c) $d = 17.5422$ (d) $d = 31.3445$

Fig. 4. Experimental results of malicious tampering.

original images and their distorted versions are greater than 10, thus we can correctly declare it inauthentic. When the percentage of malicious operations is less than 30%, we are concerned about the malicious attacks on small region since they are rational attacks. To some degree, we can claim that the proposed scheme is able to distinguish the malicious operations from the content-preserving ones.

4.4 Performance Comparisons

In this subsection, we mainly compare the proposed scheme with several reported hashing methods. Zhao, Wang and Zhang [20] proposed a method that also combines the local features and the global features for image hashing, but the method cannot resist high strength noise addition for the reason that the noise may influence the extraction of the salient regions. And the method is not robust against cropping and rotation distortion with large angle. Since our features are extracted from the radon domain, the method proposed by Lei, Wang and Huang [7] is selected for comparison. Moreover, the proposed scheme uses the SVD and invariant moments, thus the methods proposed by Kozat et al. [14] and Tang et al. [21] are also selected for comparison. The proposed scheme mainly aims at the grayscale images. All the color images are converted to the grayscale images in the experiments. The same Euclidean distance computing is also applied to the analysis. We obtain the similar images with eight content-preserving operations on 200 original images of the above database, and take the different content images and the forged images by pasting a foreign block, which the size is more than 30%, into the 200 original images as perceptually distinct images. The receiver operating characteristics (ROC) is a useful tool for visualizing classification perfor-



(a) ROC curve (b) Zoomed-in view of the ROC curve

Fig. 5. ROC curve comparisons among different methods.

mances between robustness and discrimination. The true positive rate (*TPR*) and the false positive rate (*FPR*) are calculated firstly. *TPR* and *FPR* are defined as follows, respectively.

$$TPR = n_1 / N_1, \tag{19}$$

$$TPR = n_2 / N_2. \tag{20}$$

Here n_1 is the number of the pairs that the visually identical images are considered as the similar images, N_1 is the total pairs of visually identical images, n_2 is the number of the pairs that the different images are considered as similar images, and N_2 is the total pairs of different images. It is clear that *TPR* and *FPR* indicate robustness and discrimination respectively. If two methods have the same *TPR*, the one with a low *FPR* outperforms that with a high *FPR*. Similarly, if they have the same *FPR*, the one with a high *TPR* is better than that with a low *TPR*. In order to obtain the experimental comparisons of the proposed scheme and the methods in reference [7], [14], [21], we set different threshold values and calculate the *TPR*s and *FPR*s of different methods. We repeat this process with different thresholds and obtain the ROC graph as shown in Fig. 5, with *TPR* and *FPR* as *y* axis and *x* axis, respectively.

The method in reference [7] uses the invariant moments and DFT for image hashing generation, which can resist some geometric distortions. The method in reference [14] uses the SVD-SVD, and the method in reference [21] uses the invariant moments, which can resist rotation distortion. But they only use the global features of the image and cannot balance the robustness with discrimination well. The proposed scheme combines the local features with the global features for hashing which can outperform these methods. As shown in Fig. 5, we can know that the ROC curve of the proposed scheme is above the curves of other methods, and the area under the ROC curve is larger than the curves of other methods, which means that the proposed scheme is superior to the other three methods in terms of classification performance.

5. Conclusions

In this work, an image hashing method is developed, which not only owns good robustness against the typical content-preserving operations, such as JPEG compression, filtering, noise contamination, scaling, translation and rotation, but also good discrimination for perceptually distinct images. The key contribution of this work is using radon transform and invariant features, which means combining the local features and the global features. However, the success of the proposed scheme depends on the multiple transformations to a large extent, so that the computational complexity is not desirable enough. Meanwhile, the hashing length is not the shortest among the state-of-art work. The further research is desired to extract the features that better represent the image contents, and it also maintains short hash length and low computational complexity.

Acknowledgments

This work was partially supported by the National Natural Science Foundation of China (No. 61103215, 61373132, 61373133and 61402162), the Hunan Provincial Natural Science Key Foundation of China (No. 13JJ2031), the National Social Science Fund Projects (No. 13CJY007), the Youth Growth Plan of Hunan University, Ministry of Education, Humanities and Social Sciences Research Projects (No. 12YJAZH216).

References

[1] STEVENS, M., SOTIROV, A., APPELBAUM, J., et al. Short chosen-prefix collisions for MD5 and the creation of a rogue CA certificate. In *Proceedings of CRYPTO*, 2009, LNCS 5677, p. 55 to 69. DOI: 10.1007/978-3-642-03356-8_4

[2] LIU, S. H., YAO, H. X., GAO, W., et al. An image fragile watermark scheme based on chaotic image pattern and pixel-pairs. *Applied Mathematics and Computation*, 2007, vol. 185, no 2, p. 869–882. DOI: 10.1016/j.amc.2006.07.036

[3] MONGA, V., EVANS, B. L. Perceptual image hashing via feature points: performance evaluation and tradeoffs. *IEEE Transactions on Image Processing,* 2006, vol. 15, no. 11, p. 3452–3465. DOI: 10.1109/TIP.2006.881948

[4] LIN, C. Y., CHANG, S. F. A robust image authentication method distinguishing JPEG compression from malicious manipulation. *IEEE Transactions on Circuits and Systems for Video Technology*, 2001, vol. 11, no. 2, p. 153–168. DOI: 10.1109/76.905982

[5] LEFEBVRE, F., MACQ, B., LEGAT, J. D. RASH: radon soft hash algorithm. In *Proceedings of the 11th European Signal Processing Conference.* Toulouse (France), 2002, p. 299–302.

[6] LEFEBVRE, F., CZYZ, J., MACQ, B. A robust soft image hash algorithm for digital image signature. In *Proceedings of IEEE International Conference on Image Processing ICIP'2003*. Barcelona (Spain), September 2003, vol. 3, p. 495–498. DOI: 10.1109/ICIP.2003.1246725

[7] LEI, Y. Q., WANG, Y. G., HUANG, J. W. Robust image hash in radon transform domain for authentication. *Signal Processing: Image Communication*, 2011, vol. 26, no. 6, p. 280–288. DOI: 10.1016/j.image.2011.04.007

[8] WU, D., ZHOU, X. B., NIU, X. M. A novel image hash algorithm resistant to print-scan. *Signal Processing.* 2009, vol. 89, no. 12, p. 2415-2424. DOI: 10.1016/j.sigpro.2009.05.016

[9] OU, Y., RHEE, K. H. A key-dependent secure image hashing scheme by using radon transform. In *Proceedings of the International Symposium on Intelligent Signal Processing and Communication System*. Kanazawa (Japan), January 2009, p. 595-598. DOI: 10.1109/ISPACS.2009.5383770

[10] RAMIREZ-GUTIERREZ, K., NAKANO-MIYATAKE, M., PEREZ-MEANA, H. Improvement of radon-based image hashing using image normalization. In *Processing of Conference on Electronics, Robotics and Automotive Mechanics CERMA*. Cuernavaca (Mexico), November 2011, p. 173–177. DOI: 10.1109/CERMA.2011.34

[11] SWAMINATHAN, A., MAO, Y. N., WU, M. Robust and secure image hashing. *IEEE Transactions on Information Forensics and Security*, 2006, vol. 1, no. 2, p. 215–230. DOI: 10.1109/TIFS.2006.873601

[12] XIANG, S. J., KIM, H. J., HUANG, J. W. Histogram-based image hashing scheme robust against geometric deformations. In *Proceedings of the 9th workshop on Multimedia and Security*. Dallas (TX, USA), September 2007, p. 121–128. DOI: 10.1145/1288869.1288886

[13] QIN, C., CHANG, C. C., TSOU, P. L. Robust image hashing using non-uniform sampling in Discrete Fourier Domain. *Digital Signal Processing,* 2012, vol. 23, no. 2, p. 578–585. DOI: 10.1016/j.dsp.2012.11.002

[14] KOZAT, S. S., VENKATESAN, R., MIHCAK, M. K. Robust perceptual image hashing via matrix invariants. In *Proceedings of IEEE International Conference on Image Processing ICIP'2004*. Singapore, October 2004, p. 3443–3446. DOI: 10.1109/ICIP.2004.1421855

[15] MONGA, V., MIHCAK, M. K. Robust and secure image hashing via non-negative matrix factorizations. *IEEE Transactions on Information Forensics and Security*, 2007, vol. 2, no. 3, p. 376–390. DOI: 10.1109/TIFS.2007.902670

[16] TANG, Z. J., WANG, S. Z., ZHANG, X. P. Robust image hashing for tamper detection using non-negative matrix factorization. *Journal of Ubiquitous Convergence Technology*, 2008, vol. 2, no. 1, p. 18–26.

[17] KANG, L.W., LU, S. C., HSU, Y. C. Compressive sensing-based image hashing. In *Proceedings of the 16th IEEE International Conference on Image Processing ICIP 2009*. Cairo (Egypt), November 2009, p. 1285–1288. DOI: 10.1109/ICIP.2009.5413606

[18] TANG, Z. J., WANG, S. Z., ZHANG, X. P., et al. Lexicographical framework for image hashing with implementation based on DCT and NMF. *Multimedia Tools and Application*, 2011, vol. 52, no. 2-3, p. 325–345. DOI: 10.1007/s11042-009-0437-y

[19] ZHAO, Y. Perceptual image hash using texture and shape feature. *Journal of Computational Information Systems*, 2012, vol. 8, no. 8, p. 3519–3526.

[20] ZHAO, Y., WANG, S. Z., ZHANG, X. P., et al. Robust hashing for image authentication using Zernike moments and local features. *IEEE Transactions on Information Forensics and Security,* 2013, vol. 8, no. 1, p. 55–63. DOI: 10.1109/TIFS.2012.2223680

[21] TANG, Z. J., DAI, Y. M., ZHANG, X. Q. Perceptual hashing for colour images using invariant moments. *Applied Mathematics and Information Sciences*, 2012, vol. 6, no. 2S, p. 643–650.

[22] TANG, Z. J., ZHANG, X. Q., DAI, X., et al. Robust image hash function using local colour features. *International Journal of Electronics and Communications (AEÜ)*, 2013, vol. 67, no. 8, p. 717–722. DOI: 10.1016/j.aeue.2013.02.009

[23] LIU, F., CHENG, L. M., LEUNG, H. Y., et al. Wave atom transform generated strong image hashing scheme. *Optics Communications*, 2012, vol. 285, no. 24, p. 5008–5018. DOI: 10.1016/j.optcom.2012.08.007

[24] LIU, Y. L., XIAO, Y. A robust image hashing algorithm resistant against geometrical attacks. *Radioengineering,* 2013, vol. 22, no. 4, p. 1072–1082.

[25] HU, M. K. Visual pattern recognition by moment invariants. *IRE Transactions on Information Theory*, 1962, vol. IT-8, no. 2, p. 179–187. DOI: 10.1109/TIT.1962.1057692

About the Authors...

Yuling LIU (corresponding author) was born in Hunan, China, 1980. She received her B.S. and Ph.D. degree from Hunan University in 2003 and 2008. She is an associated professor in Hunan University now. Her research interests include information security, information hiding and digital watermarking. She has more than 30 international journal and conference papers in scientific review.

Guojiang XIN was born in Liaoning, China, 1979. He is an associated professor at Hunan University of Chinese Medicine. He received his Ph.D. degree in Computer Science from Central South University in 2013. His main research interest is image processing.

Yong XIAO was born in Hunan, China, 1989. He is currently pursuing his M.S. degree in Computer Science and Technology at the College of Computer Science and Electronic Engineering, Hunan University, China. His main research interests include information security, image hashing and digital watermarking.