A Robust Image Hashing Algorithm Resistant Against Geometrical Attacks

YuLing LIU, Yong XIAO

College of Information Science and Engineering, Hunan University, Changsha, 410082, China

yuling_liu@126.com, xiao_yongemail@163.com

Abstract. *This paper proposes a robust image hashing method which is robust against common image processing attacks and geometric distortion attacks. In order to resist against geometric attacks, the log-polar mapping (LPM) and contourlet transform are employed to obtain the low frequency sub-band image. Then the sub-band image is divided into some non-overlapping blocks, and low and middle frequency coefficients are selected from each block after discrete cosine transform. The singular value decomposition (SVD) is applied in each block to obtain the first digit of the maximum singular value. Finally, the features are scrambled and quantized as the safe hash bits. Experimental results show that the algorithm is not only resistant against common image processing attacks and geometric distortion attacks, but also discriminative to content changes.*

Keywords

Image hashing, LPM, contourlet transform, SVD.

1. Introduction

With the rapid development of network and multimedia technology, an increasing amount of digital multimedia content is widely used in various fields. However, it is still difficult for users to discriminate the authentic images from the counterfeits because of the easy reproduction and distribution, so there is an urgent need for an effective method that is able to solve the problem of the copyright protection. Digital watermarking technology is a new method that can effectively solve the problem, but one common issue of the traditional image watermarking algorithms is that they modify the content of the carrier image and thus introduce content distortion. As such, the image hashing algorithm is now widely applied for image authentication because it does not change the content of the original image. It differs from the traditional watermarking method which has the contradiction of robustness and invisibility. Image hashing algorithm is based on image content and can support various applications such as image authentication and retrieval. This method is also known as perceptual hashing, robust hashing and etc., and it has received much attention of researchers over the recent years.

The traditional cryptographic hash functions, such as MD5 and SHA [1-6], have been used for data authentication. Although cryptographic hash functions are effective to ensure data integrity, they are not feasible for multimedia information which emphasizes the perceptual information retention rather than the bit change. Moreover, the traditional hash functions are quite sensitive to data change, that is, changing one bit of the input data will lead to a significant change of the output hash. Image hashing algorithm mainly emphasizes the robustness of image features. It should be invariant to incidental modifications such as JPEG compression, geometric distortion, addition of noise and other similar operations. Another requirement for the image hashing algorithm is the ability to distinguish the visually distinct images. Image hashing achieves image authentication by comparing the similarity of two image hashes that are extracted from the original image and the suspicious image.

A typical image hash algorithm is composed of two main stages: feature extraction and hash generation. Feature extraction is the crucial step in the algorithm, and it is mainly based on spatial domain and transform domain at present. Schneider proposes the first image hashing method based on the gray histogram for image authentication. He partitions the image into a set of image blocks, then constructs a gray histogram for each block and encrypts the histograms by the secret key, generating the final hash values [7]. Venkatesan et al. propose a hashing method based on statistic features of wavelet sub-band image [8]. Blocks of wavelet image are randomly generated for extracting features and generating the hashing sequences. Lin proposes an authentication method based on DCT transformation for robustness against JPEG compression [9]. Wen proposes a hashing algorithm based on DCT and PCA [10].These methods mainly construct the hash sequence with the means or variances of image luminance, DCT coefficients, histogram statistics and etc. [11-16]. These algorithms have low complexity of computations but they are not able to resist geometric attacks.

There are some schemes based on matrix factorization [17]. Kozat proposes a hash algorithm based on SVD decomposition [18] where the most significant vectors of random images are used to generate the hashing values. This algorithm is robust to geometric attacks, but has high rate of false-classification. Xu et al. [19] describe an image

hashing algorithm using discrete curvelet transform. Although it achieves satisfactory robustness to common attacks, it is vulnerable to geometric attacks. Other algorithms are based on Radon and DWT [20]. F. Lefebvre et al. [21-23] propose a robust image hash algorithm for digital image signature. This algorithm takes full use of the radon transform and principal component analysis to generate robust image characteristics as signature, and this algorithm can resist against geometrical attacks to some extent. These algorithms have some robustness against geometric attacks; however, they are time-consuming and have poor performance for simple texture images. Swaminathan [24] suggests that the use of Fourier-Mellin transform can be helpful for resisting affine transformation, but their algorithm has high computational complexity. Ricardo introduces an image hashing based on image normalization and SVD [25], which has good robustness against geometric attacks but with poor performance to other normal attacks. Qin et al. [26] present an image hashing method based on DFT domain and non-uniform sampling, which can resist against geometric attacks. The global or local features can also be used to form the features of image content. A content-based hashing scheme is proposed [27], in which Harris corner detector is used to extract the salient feature points. Then these feature points can be used to generate the hashes. However, the robustness of the scheme depends on the accuracy and capacity of Harris detector. There are also some image hashing algorithms based on geometric features and target character [28-30]. Although these algorithms can resist against some attacks, they are not ideal to attacks combined various geometric attacks with common image processing attacks. Due to the reason that geometric attacks usually change the synchronization of images, the traditional methods are difficult to accurately extract image features. The difficulties of hashing algorithms become how to effectively combine image general features with image detail features and resist against geometric attacks.

This paper presents a new robust image hashing algorithm to resist against geometric attacks. We focus mainly on the robustness and discrimination of image hashing. The normalization of image translation and log-polar mapping (LPM) are used to resist against geometric attacks. Then the DCT and SVD are used to generate image hashing values. Finally, standardized hamming distance is used to measure the similarity between images. Experimental results show that our algorithm is robust not only to common content-preserving attacks, but also to robust geometric attacks. Also, it has good performance of distinction.

The rest of this paper is organized as follows. Section 2 introduces the related work. Section 3 describes the details of hashing generation and hashing authentication. Experimental results and analysis are presented in Sec tion 4. Section 5 concludes briefly with our future work.

2. Related Work

2.1 LPM and Invariant Centroid Algorithm

The log-polar mapping is an image transformation method that transforms the Cartesian coordinate system into log-polar coordinate system, as shown in Fig. 1, γ and θ represent the polar axis and the polar angle respectively. The position of image pixel can be presented by Cartesian coordinate (x, y) and log-polar coordinate (ρ, θ), shown as (1) and (2). Assuming that the origin of coordinate is $O(x_0,y_0)$, the two coordinates satisfy the following relationship between them.

$$\rho = \sqrt{(x-x_0)^2 + (y-y_0)^2}\,, \tag{1}$$

$$\theta = \arctan\left(y - y_0 / x - x_0\right)\,. \tag{2}$$

Then we obtain the log-polar coordinate plane as follows: $\xi = \log\rho, \psi = \theta$. One of the important nature properties of log-polar coordinate is that it converts the scaling in the Cartesian coordinate to translation in the log-polar coordinate because

$$\xi_1 = \log(k * \rho) = \log(k) + \log(\rho) = \log(k) + \xi\,. \tag{3}$$

It is to say that the up and down translation in the radial direction can be applied to represent scaling. It is the same in angle, when the image is rotated by L angle,

$$\psi_1 = \psi + L\,. \tag{4}$$

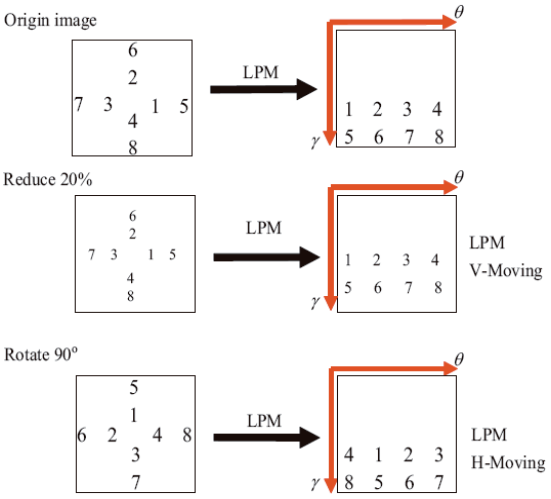


Fig. 1. Graph to illustrate LPM transformation.

That is to say that the right and left translation in the angular direction can be used to represent angle rotation. This is the invariant of scaling and rotation of log-polar coordinate system.

The invariant centroid algorithm can be used to correct the translation of the image. Calculating the invariant centroid of distorted image as $C_t = (c_{xt}, c_{yt})$, and the amount of translation can be represented as: $\Delta x = c_{xt} - c_x$, $\Delta y = c_{yt} - c_y$, then translation of the mapping image along the x and y axes is employed to correct the translation-attacked image.

2.2 Contourlet Transform

Contourlet transform is a new extension of the wavelet transform, which is an image analysis method being widely used in the field of image processing. The comparison of this transform and wavelet transform is shown in Fig. 2. This transform method has strong signal analysis capabilities. It uses the Laplacian pyramid decomposition (LP) and direction of the filter bank (DFB) to achieve a multi-resolution, local and multi-directional image analysis method. The Laplacian pyramid is used to decompose an image into a number of radial sub-bands, and the directional filter banks decomposes each LP detail sub-band into a number of directional sub-bands. It is a way to capture the geometric structure of the two-dimensional signal, and it can achieve decomposition on arbitrary direction of arbitrary scale. The method can be employed for image feature extraction.

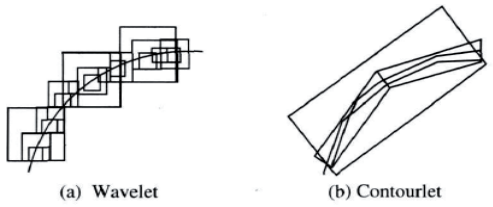


Fig. 2. Comparison of wavelet transform and contourlet transform.

2.3 SVD Decomposition

The singular value decomposition is a common matrix decomposition method, which can do matrix diagonalization operation. The singular values of image matrix represent the internal characteristics of the image rather than visual characteristics. Because singular values own strong stability, there is no significant change to carrier image after slight modifications. And singular values contain intrinsic properties (luminance information is contained in singular values, whereas geometric information is maintained by corresponding singular vectors). So this decomposition method is usually used in digital watermarking, image processing, signal processing and statistics, etc.

Considering the image as a non-negative matrix, and the following formula is used to represent the singular value decomposition:

$$A = USV^T \ . \tag{5}$$

$A \in R_{m*m}$ (R represents the set of real numbers) represents an image matrix, U represents the left-orthogonal matrix and V represents the right-orthogonal matrix, both of them are part of real number domain. S=diag($\lambda_1, \lambda_2, \lambda_3, ..., \lambda_n$) presents a diagonal matrix, and the non-diagonal elements are zero. S is uniquely determined in accordance with the matrix A, the diagonal elements are the singular values of image decomposition, $\lambda_1 \geq \lambda_2 \geq \mathrm{L} \geq \lambda_r > \lambda_{r+1} = \mathrm{L} = \lambda_n = 0$.

r represents the rank of the matrix A and also indicates the number of non-zero singular values. λ_i (i=1 , 2 , … , n) expresses the singular values of matrix A and also means the square of the eigenvalues of AA^T .

Singular value decomposition has the advantage of no requirement on the size of the transformation matrix, which can be a square or long matrix. Also it owns good stability and the ability to resist geometric attacks. This method contains good performance in the representation of image features.

3. Proposed Hashing Algorithm

Image hashing algorithm especially emphases on: robustness and discrimination. This means that we can still extract the same hashing values to confirm the authentication information of the image after conventional attacks. This needs us to extract some deep-level characteristics of the image. These features need to be enough to express the basic content of the image and have strong stability. Also these features need to have the ability of distinguishing the maliciously attacked image or perception significantly different image from the original image. Moreover, the obtained hashing values should be different and random. In other words, the hashing values are statistically independent.

In order to resist geometric attacks, LPM can be used to convert the rotation and scaling of the original image to translation in the angular and radial direction on log-polar coordinates. The geometric correction of the image can be done through cyclic translation and comparison. Invariant centroid theory has also been used as the method for translation correction, and the distance of invariant centroid can be used to correct the image. Contourlet transform can be applied to obtain the low frequency sub-band image in order to produce relatively stable features. The low frequency sub-band image can better represent content features of the image, and the chaos theory is employed to scramble the features to increase their security. The hashing sequence can be generated through adaptive blocking and SVD operation.

The image hashing algorithm is mainly robust to common image processing attacks, but sensitive to images after malicious attacks and visually distinct images. Fig. 3 shows the image authentication procedure using image hashing.

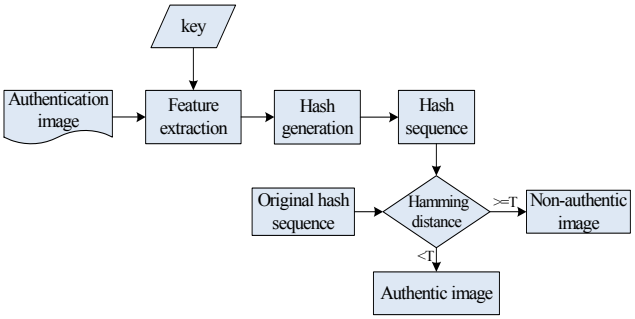


Fig. 3. Structure of hashing algorithm.

3.1 Image Hashing Generation

The main purpose of the algorithm is to resist the geometric attacks. The flow diagram of this algorithm is shown in Fig. 4 and the main steps of the algorithm are as follows. Firstly contourlet transform operation is applied to image. The low frequency sub-band image can be selected and divided into blocks, followed by performing DCT to each image block. The low-mid frequency DCT coefficients show the main energy distribution of the image, and both the low frequency sub-band image and the maximum singular value have good stability, so the generated hashing values own good robustness and can resist against various common attacks. The algorithm is also able to distinguish different images or images after malicious tempering from original images. And we need to correct geometric attacks and extract the hashing values for image authentication.

The specific steps are as follows:

1. Calculate the invariant centroid $C(c_x, c_y)$ of original image H, and then conduct log-polar transformation after low-pass filtering. The number of sampled polar axis and the polar angle is 512*512 and the image H_1 can be obtained, which can be used for the geometric correction in certification processing.

2. Adaptive contourlet transform is conducted to image H_1 and the low-frequency sub-band image can be obtained, and then the image is partitioned into blocks of adaptive size, such as the size of 8*8.

3. The logistic chaotic system is applied to scramble the blocks and the initial value can be saved as the secret key to ensure the security of the image hashing.

4. The low-mid frequency coefficients (4*4) of each block can be obtained through DCT operation and zigzag scanning. Then the coefficients are arranged as a two-dimensional array.

5. For low-mid frequency coefficients of each block, we perform SVD to them and obtain the maximum singular value of each block. The hashing values will be generated according to the relationship of the maximum singular value B_i of each block and the mean value (avg) of all maximum values, that is,

$$w_i = \begin{cases} 1, B_i \geq avg \\ 0, B_i < avg \end{cases} \tag{6}$$

$1 \leq i \leq N$, and N represents the number of blocks.

6. The hashing values of each block are organized and arranged and the final image hashing sequence $W(i)$ can be generated accordingly.

7. The hashing sequence is attached to original image and transmitted to the receiver finally.

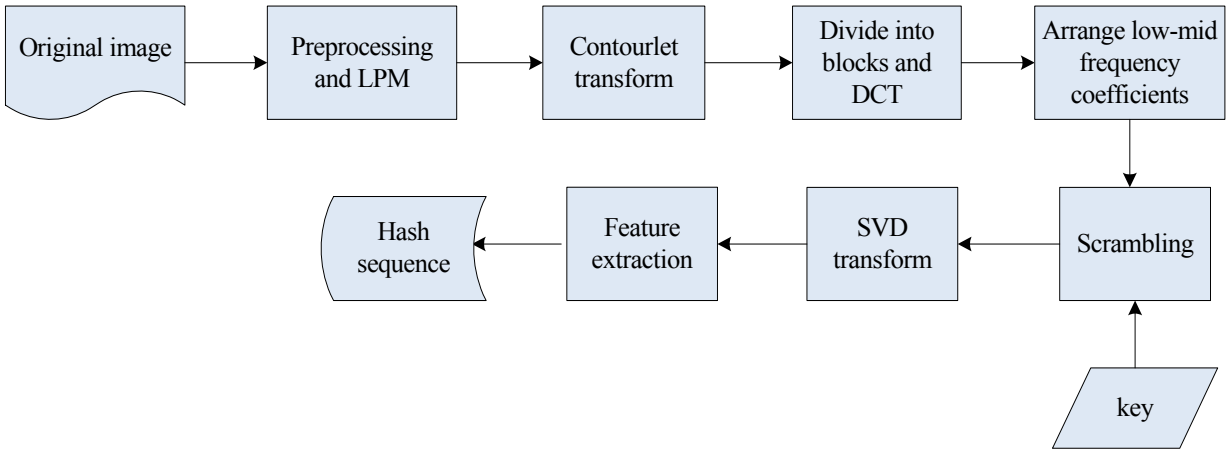


Fig. 4. Hash generation.

3.2 Image Authentication Algorithm

The hashing sequence of image can be obtained in the receiver side. The authentication can be achieved by comparing the similarity of the received hashing sequence and the hashing sequence generated from the received image. Then the authenticity of the image can be judged according to the threshold. In the process of image authentication, we first need to detect the geometric distortion. If the image is distorted, then the geometric correction will be performed, otherwise the hashing features will be extracted directly. The flow chart is shown in Fig. 5 and the steps of image authentication algorithm are as follows:

1. The invariant centroid method is applied to detect the translation of the received image I. Then we can obtain the average coordinate of invariant centroids of different radiuses. If translation attacks exist, we can estimate the translation parameters and correct the attacks. The corrected image is saved as I_1.

2. Generate the hashing values of image I_1 in accordance with the steps (2-6) of the hashing generation algorithm, and the hashing values are saved as $W_1(i)$.

3. Calculate the normalized hamming distance between the received hashing $W(i)$ and $W_1(i)$ as $D(W,W_1)$. Let *sim* represents the similarity of them. The normalized hamming distance and similarity can be expressed as follows:

$$D(W,W_1)=\frac{1}{L}\sum_{k=1}^{L}|w(k)-w_1(k)|, \quad (7)$$

$$sim=1-\frac{1}{L}\sum_{k=1}^{L}|w(k)-w_1(k)|. \quad (8)$$

L represents the length of hashing sequence, and k represents the bit number of hashing sequence.

4. Threshold T can be set through running a lot of experiments. If $D(W,W_1)\le T$, the hashing values of two images match and the image is authentic, otherwise cyclic comparison. Also we can set a threshold T_1, if $sim \ge T_1$, the image is authentic, otherwise cyclic comparison. T and T_1 are the thresholds to distinguish images after malicious tampering or different images from common attacked images.

5. Cyclic comparison: If the normalized hamming distance is larger than the threshold T, cyclic translation is performed in the radial and angular direction of the log-polar coordinates. Then we generate the hashing sequence and compare the normalized hamming distance of the two hashing sequences with threshold T. If the radial direction and angular direction are shifted to the end, it means that the image is different.

4. Experimental Results and Analysis

The experiment is run in Windows XP and implemented with MATLAB 7.0, and the standard test images of 512*512 size are used, such as 'Lena', 'Baboon', 'Barbara' and 'Pepper', etc. We use these test images under common image attacks and malicious tampering to analyze the experimental results.

The image hashing values are obtained by extracting key features of images. Security shows that the secret key is important for hashing generation. Robustness means that the hashing values are not changed after conventional attacks, which ensures the normal image authentication. Discrimination means that the hashing values will be different when the image is different or is maliciously tamped, which reflects the integrity of the certification.

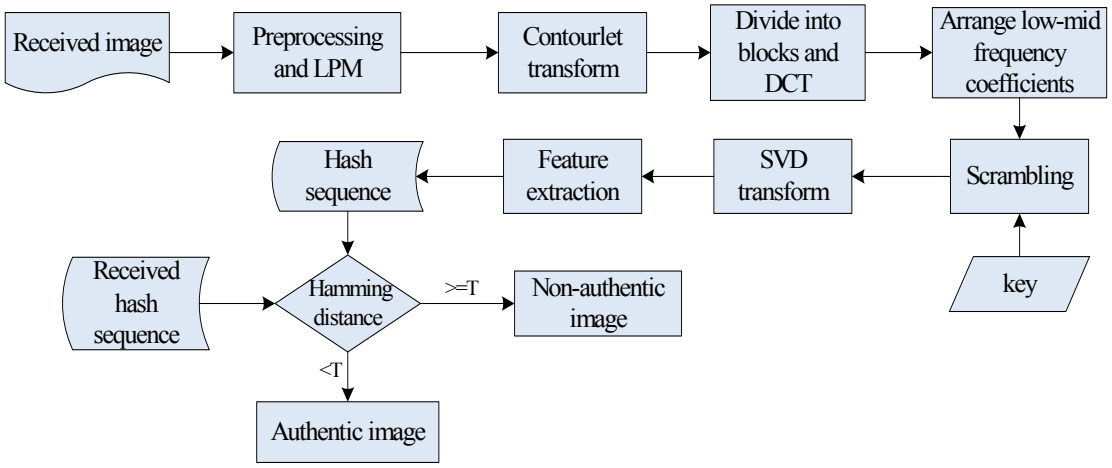


Fig. 5. Image authentication.

4.1 Security Analysis

Due to the addition of logistic scrambling in hashing generation, the secret key is needed in the hashing generation. Since the logistic system is very sensitive to initial values, even a small change may cause significant distinction. Thus only the user with the right key can generate right hashing sequence. If the key is different, the hashing values will be greatly changed. This may ensure the security of image hashing method.

Logistic chaotic system is non-periodic and non-convergence. The values obtained by iterative generation are in a state of pseudo-random distribution. The model seems very simple and deterministic, but has a very complex dynamic behavior. Generally the parameter μ is set as 4 because the performance is better compared with other values. Fig. 6 shows the logistic sequence of 2000 points generated with this condition: $\mu = 4$, $x_0 = 0.4$. The below figure shows the difference of the sequences generated by

different initial values such as 0.4, 0.4000001, 0.40000002, and the number 1 represents the difference of 0.4 and 0.4000001, number 2 shows the difference of 0.4 and 0.40000002, number 3 shows the difference of 0.4000001 and 0.40000002. The result demonstrates that these points are randomly distributed and sensitive to small change of initial value.

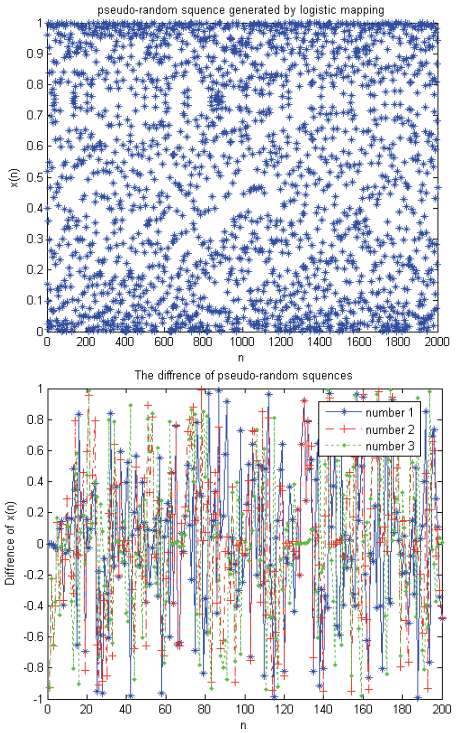


Fig. 6. Security analysis of logistic chaotic mapping.

4.2 Robustness Analysis

Robustness focuses mainly on the non-malicious attacks. When the image is attacked with common processing, the resulting hashing values should be similar to the values generated from the image before attack. Usually these attacks include JPEG compression, Gaussian noise, salt and pepper noise addition, median filtering, cropping, etc. Also, some geometric attacks such as rotation, scaling, translation, etc. are generally considered as common image processing that will not exert significant impact on image quality. The experiment shows that this algorithm is resistant not only to common content-preserving attacks, but also to geometric attacks.

In term of resisting common attacks, experimental results show that the normalized hamming distance of this algorithm will not be greater than 0.2. Based on this observation, the algorithm fixes the threshold at 0.2. This algorithm extracts features with good robustness and strong ability to resist attacks including noise addition, filtering, etc. Experimental data is shown in Tab. 1.

It can be seen from Tab. 1 that the proposed algorithm has good robustness to common content-preserving attacks, such as JPEG compression, Gaussian noise addition, Salt and pepper noise addition, Median filtering and etc. This is all for the reason that the algorithm only extracts the robust and stable features. Because the DCT and SVD are applied to represent the stable and internal energy of image, the robustness can be achieved with this.

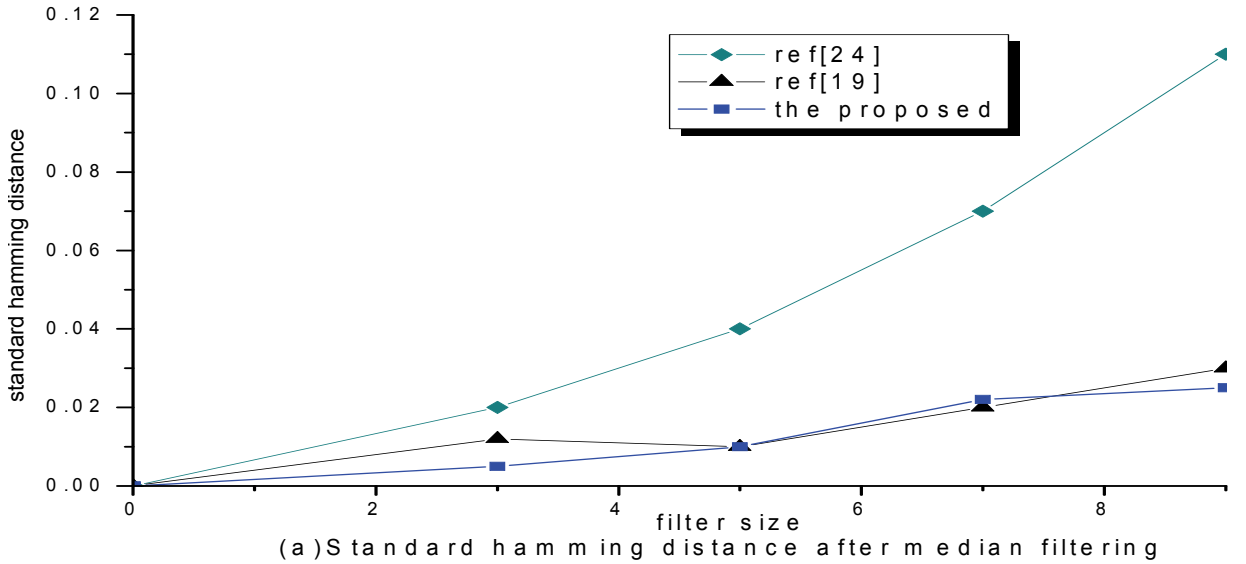
Image operation		Normalized hamming distance
JPEG compression	80%	0.0026
	60%	0.0029
	40%	0.0068
Gaussian noise	0.01	0.0186
	0.02	0.027
	0.03	0.0143
Salt and pepper noise	0.02	0.0143
	0.05	0.0235
	0.07	0.0332
Median filtering	3*3	0.005

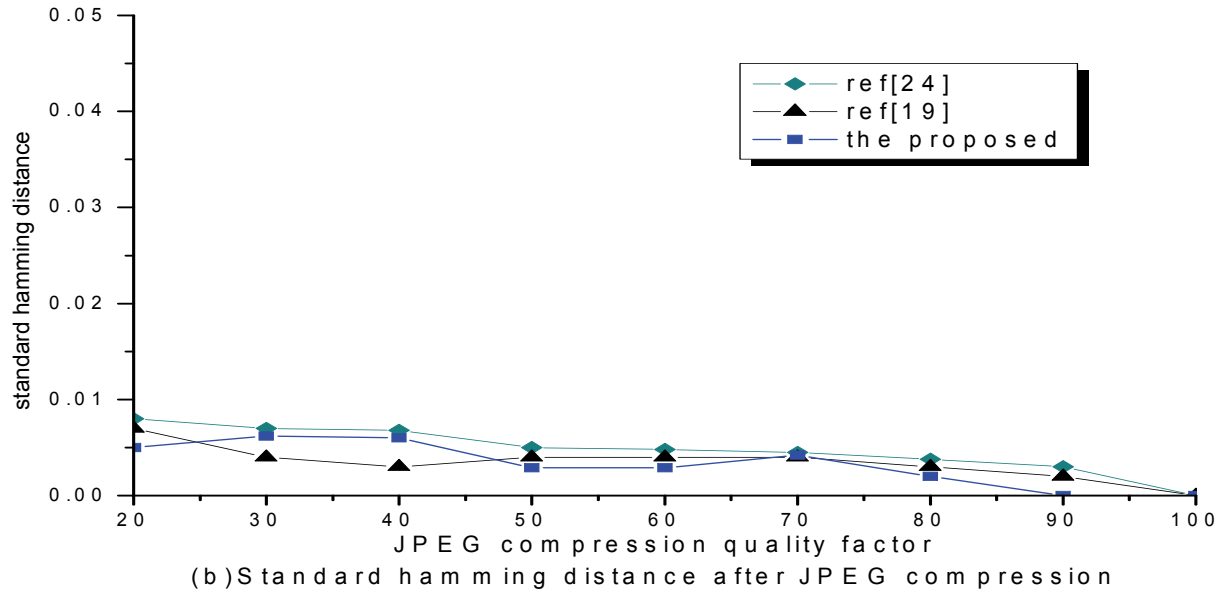
Tab. 1. Image conventional attacks and normalized hamming distance.

Compared with reference [19] and reference [24], the proposed algorithm has better robustness. Reference [19] and [24] are not able to defend geometric attacks. In the experiments, we conduct some common attacks in order to measure the performance of the proposed algorithm and of reference [19] and [24] respectively. The comparison results are shown in Fig. 7.

From Fig. 7 we can conclude a conclusion that the robustness of the proposed algorithm is better than that of reference [19]. We can learn that our algorithm is better than reference [19] when the size of median filter is under about 5*5, and the performance is nearly similar when the size of median filter is large. The experimental results of JPEG compression show that our algorithm achieves satisfactory robustness when the quality factor is larger than 47. It is clearly shown that reference [19] owns better performance than reference [24], so the proposed algorithm is also better than reference [24], which is shown clearly in Fig. 7. We can obtain a conclusion that the proposed algorithm has smaller normalized hamming distance compared with reference [19] and reference [24].

Since it can resist geometric attacks and reference [19] does not have the ability nearly, the proposed algorithm has better performance than reference [19]. We conduct some experiments to geometric attacks such as rotation, scaling, translation, etc. and compare the results with reference [25], and show the results in Tab. 2. The results demonstrate that the proposed algorithm owns better robustness against geometric attacks compared with reference [25]. This is due to the factor that the log-polar mapping and centroid algorithm are employed for image restoration. The robustness for geometric attacks is still acceptable.





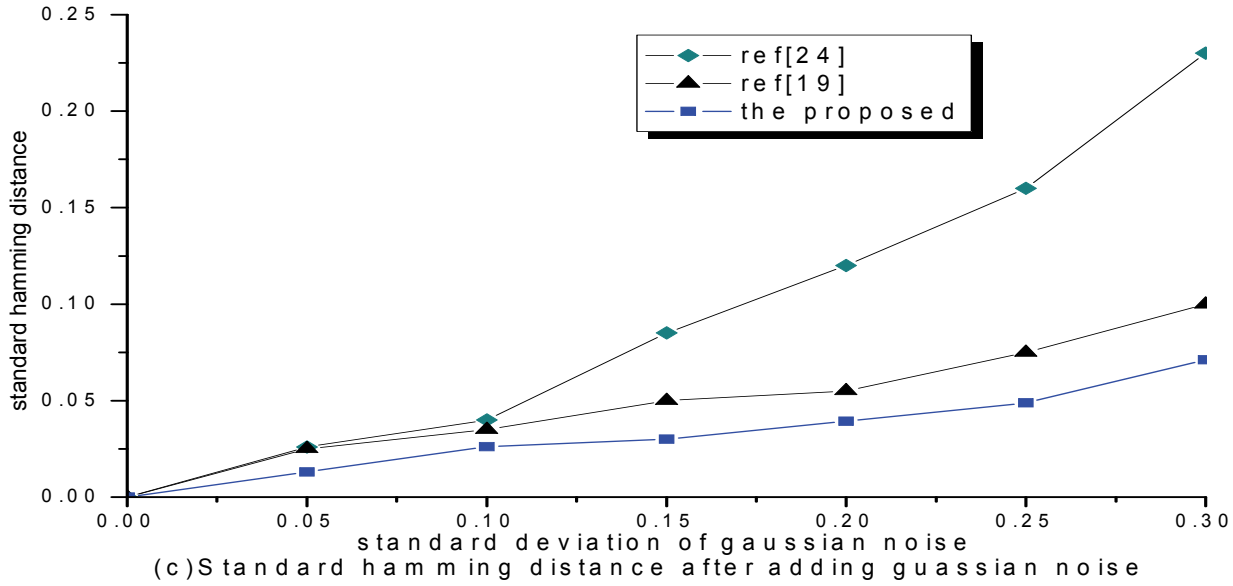


Fig. 7. Comparison of conventional attacks.

Geometric attacks	Normalized hamming distance	
	The proposed	Ref[25]
Rot15+cropping	0.0107	0.039
Rot30+cropping	0.0132	0.02
Rot45+cropping	0.0137	0.068
Scaling1.5	0.0608	0.13
Scaling1.2	0.0277	0.12
Scaling0.8	0.0407	0.13
Translation 20*20	0.0319	--
Translation 40*40	0.0317	--

Tab. 2. Geometric attacks and normalized hamming distance.

4.3 Discrimination Analysis

The normalized hamming distance can be applied to analysis of the discrimination of image hashes. The larger the normalized hamming distance is, the higher the discrimination. According to the comparative experiments of different standard test images in Tab. 3, the normalized hamming distance is basically about 0.21, so this algorithm can distinguish different images or maliciously attacked images.

When the image is maliciously tampered, it can be detected. That is the normalized hamming distance of hashing sequence is larger than threshold T, which is shown in Fig. 8.

(a) D=0.2227 (b) D=0.3408 (c) D=0.5830

Fig. 8. Experimental results of malicious tampering.

The random number generator can be applied to obtain 299 different binary sequences, which are with the same length as the image hashing sequence. The discrimination and randomness can be tested according to the distance comparison of the true hash and 299 different hashing sequences. The hashing sequence of 150th is set as the true hashing sequence. From Fig. 9 we can see that the standard Hamming distance is substantially about 0.5, and 0.2 can be used as the threshold.

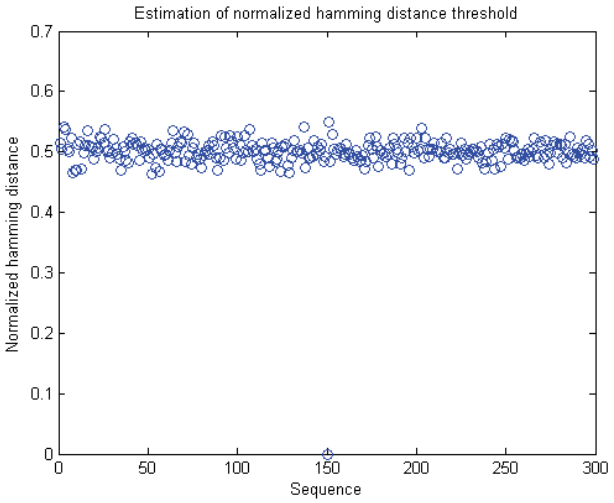


Fig. 9. Distances between the hash sequence and random uniform {0, 1} sequences.

We also obtain 100 different images from image database, where image sizes range from 256*256 to 3072*2048. These images should be converted to gray images. Then the proposed algorithm is applied to obtain the hashing sequence of each image. We calculate the normalized hamming distance between each pair of hashes, and then obtain 4950 results. Fig. 10 is the distribution of these 4950 results, where the abscissa is the normalized hamming distance and the ordinate can represent the frequency of normalized hamming distance. It can be learn that the distribution of the normalized hamming distance is like Gaussian distribution and the peak value is almost 0.5. So the normalized hamming distances of different images are big enough. It is clear that small threshold can improve the performance of discrimination, but it will result in negative impact on the robustness relatively. Therefore, we should select a suitable threshold in terms of the practical application. And the threshold is set to be 0.2 which is reasonable in practical applications. The results show that this algorithm is of good performance.

Image	Lena	Barbara	Pepper	Fullgold	Airplane
Lena	0	0.2139	0.4023	0.5986	0.3008
Barbara	0.2139	0	0.3428	0.5938	0.2139
Pepper	0.4023	0.3428	0	0.3213	0.4629
Fullgold	0.5986	0.5938	0.3213	0	0.6396
Airplane	0.3008	0.2139	0.4629	0.6396	0

Tab. 3. Normalized Hamming distance test of different standard images.

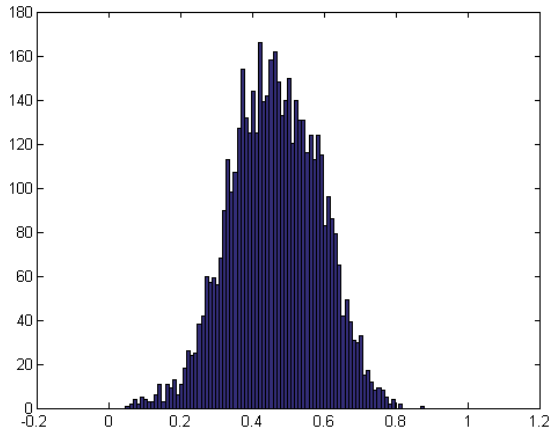


Fig. 10. Distribution of hamming distance between different images.

5. Conclusion

Image hashing algorithms are widely used in various applications including authentication, watermarking and image retrieval, where robustness, discrimination and security are the three most important characteristics. This paper proposes an effective hashing method for image authentication. The log-polar coordinate transform and invariant centroid algorithm can be applied for geometric correction. Theoretical analysis demonstrates that the proposed feature is robust to the some geometrical attacks, such as translation, scaling, rotation, etc. The experimental results show that the new algorithm can not only tolerate the perceptually similar manipulations, such as JPEG compression, low-pass filtering, median filtering, Gaussian noise, etc., but also can distinguish two visually distinct images. Compared with other well-known algorithms, the proposed algorithm owns better performance. It owns good robustness and discrimination and can be applied to practical application.

This algorithm only extracts features from log-polar coordinate system and is not very accurate for small-scale tampering. More research can be done for increasing the ability of forgery detection in the future so as to improve the performance of hashing algorithm.

Acknowledgements

This work was partially supported by National Basic Research Program 973 (No. 2011CB311808), National Natural Science Foundation of China (No. 61103215, 61232016, 61173141, 61173142, 61173136, 61073191, 61070196, 61202496, 61373132, 61373133), Science and Technology Program of Changsha City (No. K1009003-11), Hunan Provincial Natural Science Foundation of China (No. 13JJ2031) and Youth Growth Plan of Hunan University.

References

[1] CORON, J. S., DODIS, Y., MALINAUD, C., PUNIYA, P. Merkle-Damgard revisited: how to construct a hash function. *International Association for Cryptologic Research*, 2005, vol. 3621, p. 430 - 448.

[2] STEVENS, M., SOTIROV, A., APPELBAUM, J., LENSTRA, A., MOLNAR, D., OSVIK, D. A., WEGER, B. Short chosen-prefix collisions for MD5 and the creation of a rogue CA certificate. *International Association for Cryptologic Research*, 2009, vol. 5677, p. 55 - 69.

[3] WANG, X. Y., LAI , X. J., FENG, D. G., CHEN, H., YU, X. Y. Cryptanalysis of the hash functions MD4 and RIPEMD. *Advances in Cryptology-EUROCRYPT 2005*, 2005, vol. 3494, p. 1 - 18.

[4] MIRONOV, L., ZHANG, L. T. Applications of SAT solvers to cryptanalysis of hash functions. *Theory and Application of Satisfiability Testing – SAT 2006*, 2006, vol. 4121, p. 102 - 115.

[5] BURR, W. E. Cryptographic hash standards: where do we go from here? *Security and Privacy*, 2006, vol. 4, p. 88 - 91.

[6] WANG, M. Y., SU, C. P., HUANG, C. P., WU, C. W. An HMAC processor with integrated SHA-1 and MD5 algorithms. In *Proceedings of the 2004 Asia and South Pacific Design Automation Conference*, 2004, p. 456 - 458.

[7] SCHNEIDER, M., CHANG, S. F. A robust content based digital signature for image authentication. In *Proceedings of 1996 IEEE ICIP*. Lausanne (Switzerland). USA: IEEE, 1996, p. 227 - 230.

[8] VENKATESAN, R. , KOON, S. M., JAKUBOWSKI, M. H., MOULIN, P. Robust image hashing. In *Proceedings of IEEE International Conference on Image Processing*. Vancouver BC (Canada), 2000, p. 664 - 666.

[9] LIN, C. Y., CHANG, S. F. A robust image authentication system distinguishing JPEG compression from malicious manipulation. *IEEE Transactions Circuit and Systems for Video Technology (S1051-8215)*, 2001, vol. 11, no. 2, p. 153 - 168.

[10] WEN, Z. K., ZHU, W. Z., OUYANG, J., LIU, P. F., DU, Y. H., ZHANG, M., GAO, J. H. A robust and discriminative image perceptual hash algorithm. In *Proceedings 2010 International Conference on Genetic and Evolutionary Computing*. ShenZhen (China), 2010, p. 709 - 712.

[11] FRIDRICH, J., GOLJAN, M. Robust hash functions for digital watermarking. In *Proceedings of 2000 IEEE International Conference on Information Technology: coding and computing*. Las Vegas-Nevada (USA), 2000, p. 178 - 183.

[12] SEBE, N., QI, T., LOUPIAS, E., LEW, M. S., HUANG, T. S. Color indexing using wavelet-based salient points. In *Proceedings of 2000 IEEE Workshop on Content-based Access of Image and Video Libraries*. Washington DC (USA), 2000, p. 15 – 19.

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

[14] AHMED, F., SIYAL, M. Y., ABBAS, V. U. A secure and robust hash-based scheme for image authentication. *Signal Processing*, 2010, vol. 90, no. 5, p. 1456 - 1470.

[15] HU, Y. Y., NIU, X. M. DWT based robust image hashing algorithm. In *Proceedings of 6th International Conference on Networked Computing (INC 2010)*. Gyeongju (Korea), 2010, p. 1 - 4.

[16] 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.

[17] 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.

[18] KOZAT, S. S., MIHCAK, M. K., VENKATESAN, R. Robust perceptual image hashing via matrix invariants. In *Proceedings of 2004 IEEE Conference on Image Processing (ICIP)*. Singapore, 2004, p. 3443 - 3446.

[19] XU, W. J., YI, B. Image hash algorithm based on discrete curvelet transforms. *Journal of Image and Graphics*, 2011, vol. 16, no. 8, p. 1374 - 1378.

[20] 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.

[21] LEFEBVRE, F., MACQ, B., LEGAT, J. D. RASH: Radon soft hash algorithm. In *Proceedings of IEEE International Conference on European Signal Processing*. Toulouse (France), 2002.

[22] 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*. Barcelona (Spain), 2003, p. 495 - 498.

[23] DE ROOVER, C., DE VLEESCHOUWER, C., LEFEBVRE, F., MACQ, B. Robust image hashing based on radical variance of pixels. In *Proceedings of IEEE International Conference on Image Processing*. Genoa (Italy), 2005, p. 77 - 80.

[24] 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.

[25] HERNANDEZ, R. A. P., MIYATAKE, M. N., KURKOSKI, B. M. Robust image hashing using image normalization and SVD decomposition. In *Proceedings 2011 International Midwest Symposium on Circuits and Systems (MWSCAS)*. Seoul (Korea), 2011, p. 1 - 4.

[26] 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.

[27] MONGA, V., EVANS, B. L. Perceptual image hashing via feature points: Performance evaluation and tradeoffs. *IEEE Transactions on Image Processing (S1057-7149)*, 2006, vol. 15, no. 11, p. 3453 to 3466.

[28] HU, Y. Y., NIU, X. M., ZHANG, H. A novel perceptual image hashing method via geometric features and distance invariant. In *Proceedings 2009 International Congress on Image and Signal Processing (CISP)*. Tianjin (China), 2009, p. 1 - 5.

[29] ZHANG, B., XIN, Y., NIU, X. X. Image perceptual hash algorithm based on target character. In *Proceedings 2011 International Congress on Communication Technology (ICCT)*. Jinan (China), 2011, p. 397 - 401.

[30] LIU, F., CHENG, L. M., LEUNG, H. Y., FU, Q. K. Wave atom transform generated strong image hashing scheme. *Optics Communications*, 2012, vol. 285, p. 5008 - 5018.

About Authors ...

YuLing LIU was born in Hunan, China, 1980. She received her B.S. and Ph.D. degree from Hunan University, China, in 2003 and 2008. Since 2008, she is a lecturer. Her research interests include information hiding, information security, digital watermarking and natural language processing. She has more than 20 international journal and conference papers in scientific review.

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