Journal of Computational Information Systems6:3(2010) 717-725
Available at http://www.Jofcis.com

A Robust Image Hashing Method Based on Zernike Moments

Yan ZHAO[1,2], Shuozhong WANG[1,†], Guorui FENG[1], Zhenjun TANG[3]

[1] *School of Communication and Information Engineering, Shanghai University, Shanghai 200072, P. R. China*
[2] *School of Computer and Information Engineering, Shanghai University of Electric Power, Shanghai 200090, P. R. China*
[3] *Department of Computer Science, Guangxi Normal University, Guilin 541004, P. R. China*

Abstract

Image hashing maps an image to a short binary sequence representing the image's characteristics. This paper proposes a new image hashing method using Zernike moments that are an effective means for extracting robust features from an image. The method is based on rotation invariance of magnitudes and corrected phases of Zernike moments. Similarity between hashes is measured with the Hamming distance. Experimental results show that the scheme is robust against most content-preserving attacks. Hashes between pairs of different images have low collision probability. The Zernike moment based image hash can be used to detect forged images containing inserted foreign areas.

Keywords: Image Hashing; Zernike Moments; Image Authentication

1. Introduction

People can now use various image processing tools to change images for different purposes. This leads to problems such as copyright infringement and hostile tampering to the image contents. Recently, image authentication techniques have been developed rapidly to verify content integrity and prevent forgery. Image hashing is an important method for image authentication. The concept of image hashing is derived from cryptographic hashing. A cryptographic hash is extremely sensitive to the input data: even one bit change in the input will change the output hash dramatically. For an image, however, after normal manipulations such as brightness/contrast adjustment, small-angle rotation and JPEG compression, it is considered as the same image in terms of human vision, and therefore should have the same (or similar) hash as the original. On the other hand, hashes of two different images should be totally different.

In [1], Monga divided the problem of image hashing into two steps, as illustrated in Fig. 1. An image feature vector is extracted to form an intermediate hash, which should capture the perceptual qualities of the image. Then the intermediate hash is compressed to produce the final hash in the second step.

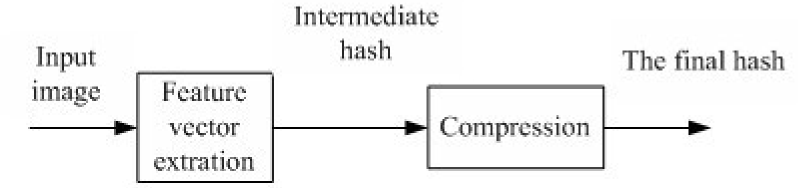


Fig. 1 Block Diagram of Monga's Image Hashing Scheme

In recent years, various image hashing methods have been proposed. These schemes can be classified

[†] Corresponding author.
Email addresses: shuowang@shu.edu.cn (Shuozhong WANG).

into two types: space domain methods and transform domain methods. Methods used in the space domain include histogram [2], singular value decomposition (SVD) [3], and non-negative matrix factorization (NMF) [4-6]. Transforms used for generating image hashes include discrete wavelet transform (DWT) [1, 7-8], discrete cosine transform (DCT) [9-11], Radon transform [12], and Fourier-Mellin transform [13]. Xiang et al. [2] propose a robust image hashing method based on the fact that the shape of an image histogram is invariant to geometric deformation. In [6], Tang et al. propose a lexicographical framework for image hashing. The image hash is formed using “words” taken from an evolutional dictionary. The scheme can resist normal content-preserving manipulations and has a very low collision probability. In [8], a wavelet-based hashing scheme is proposed, which can tackle robustness, security and tamper detection issues.

In image processing, orthogonal rotation-invariant moments (ORIMs) are important features. These moments can effectively catch important information in an image, and are invariant to rotation. Zernike moments (ZM) is a well-known ORIM originally proposed in [14], and has been studied extensively ever since. Because digitization of images compromises orthogonality of the moments, digital ZM cannot represent subtle details in an image. In [15], Lin et al. propose to use a numerical optimization technique to improve numerical accuracy of Zernike moments. In [16], Li et al. propose a new shape descriptor combining both magnitude and phase coefficients of ZM, which is invariant to rotation. In [17], Chen and Sun present a new distinctive image descriptor to represent the normalized region which comprises the Zernike moment phase information, and an accurate and robust estimation of the rotation angle between a pair of normalized regions.

In this paper, we develop a new method to construct robust and secure image hashes using Zernike moments, which is based on rotation invariance of magnitudes and corrected phases of ZM. The degree of similarity between hashes is measured by Hamming distance. Simulation results show that the scheme is robust against JPEG compression, additive noise, watermark embedding, scaling, brightness and contrast adjustments, gamma correction, Gaussian filtering, and rotation. Hashes between a pair of different images have low collision probability. In addition, we will show that the proposed hash scheme is capable of detecting forged images containing inserted foreign objects.

The paper is organized as follows. Section 2 briefly introduces the concept of Zernike moments and presents expressions to be used in this work. Section 3 describes the proposed image hashing method using ZM, with experimental results and analyses on the performance of the ZM-based hashes given in Section 4. Section 5 concludes the paper.

2. Zernike Moments

Zernike polynomials of order *n* and repetition *m* in a polar coordinate system can be defined as [14-17]

$$V_{n,m}(\rho,\theta) = R_{n,m}(\rho)e^{jm\theta} \tag{1}$$

where $n = 0, 1, \dots, 0 \le |m| \le n$, $n - |m|$ is even. $R_{n,m}(\rho)$ are real-valued radial polynomials defined as

$$R_{n,m}(\rho) = \sum_{s=0}^{(n-|m|)/2} (-1)^s \frac{(n-s)!}{s!\left(\frac{n+|m|}{2}-s\right)!\left(\frac{n-|m|}{2}-s\right)!}\rho^{n-2s} \tag{2}$$

The orthogonal property of $V_{n,m}(\rho,\theta)$ can be indicated by

$$\int_0^{2\pi}\int_0^1 V_{n,m}^*(\rho,\theta)V_{p,q}(\rho,\theta)\rho d\rho d\theta = \frac{\pi}{n+1}\delta_{n,p}\delta_{m,q} \tag{3}$$

where the superscript $*$ denotes complex conjugate and $\delta_{a,b}$ satisfies

$$\delta_{a,b} = \begin{cases} 1, a = b \\ 0, a \neq b \end{cases} \tag{4}$$

So the Zernike polynomials $V_{n,m}(\rho,\theta)$ are orthogonally defined on a unit disc.

The Zernike moments of order *n* and repetition *m* of a continuous image $f(\rho,\theta)$ are defined as

$$Z_{n,m} = \frac{n+1}{\pi}\int_0^{2\pi}\int_0^1 f(\rho,\theta)V_{n,m}^*(\rho,\theta)\rho d\rho d\theta = \frac{n+1}{\pi}\int_0^{2\pi} e^{-im\theta}\int_0^1 f(\rho,\theta)R_{n,m}(\rho)\rho d\rho d\theta \cdot \tag{5}$$

For digital images, the integrals are replaced with summations:

$$Z_{n,m} = \frac{n+1}{\pi}\sum_{(\rho,\theta)\in unit\ disk}\sum f(\rho,\theta)V_{n,m}^*(\rho,\theta) \tag{6}$$

Suppose *α* is a rotation angle, and $Z_{n,m}$ and $Z_{n,m}^r$ are ZM of the original and the rotated images respectively. We have

$$Z_{n,m}^r = Z_{n,m}e^{-jm\alpha} \tag{7}$$

Thus, $Z_{n,m}^r = \left|Z_{n,m}^r\right|e^{j\varphi_{n,m}^r}, Z_{n,m} = \left|Z_{n,m}\right|e^{j\varphi_{nm}}$, $\left|Z_{n,m}^r\right| = \left|Z_{n,m}\right|, \varphi_{n,m}^r = \varphi_{n,m} - m\alpha$. The amplitudes of ZM are invariant to rotation, while the phases are not. To reduce the influence of rotation, ZM is multiplied by an exponent:

$$Z_{n,m}^{'} = Z_{n,m}e^{-jm\varphi_{s,1}} \tag{8}$$

where $\varphi_{s,1}$ is the phase of $Z_{s,1}$ of the image, and *s* is an odd number. So we can get

$$\varphi_{n,m}^{r'} = \varphi_{n,m}^r - m\varphi_{s,1}^r = \varphi_{n,m}^r - m\left(\varphi_{s,1} - 1\alpha\right) = \varphi_{n,m} - m\varphi_{s,1} = \varphi_{n,m}^{'} \tag{9}$$

This way, phases of the changed ZM, $Z_{n,m}^{'}$, are also rotation-invariant. We choose *s* = 3 for simplicity.

3. Image Hashing Using Zernike Moments

A block diagram of the proposed image hashing method is shown in Fig. 2, and the steps are as follows.

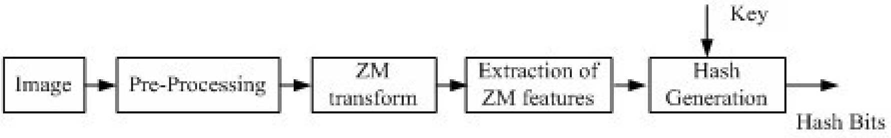


Fig. 2 Block Diagram of the Proposed Image Hashing Method

(1) The image is first pre-processed. The pre-processing steps include re-sizing using bi-linear interpolation, color space conversion, and low-pass filtering. The aim of re-sizing is to change the image into a fixed size, *M*×*M*, to ensure that the generated image hash has a fixed length. As the luminance component contains most structural and textural information of an image, we do not consider colors in the present work. A color image is converted to monochrome and then passed through a low-pass filter to produce the pre-processed image. Low-pass filtering can enhance robustness of the image hash against normal image processing.

(2) Zernike moments of the inscribed circle of the pre-processed square image are calculated. Because the shape features can be obtained from a small number of low frequency coefficients, the order *n* does not need to be large. We choose *n* = 10. Further, since $Z_{n,-m} = Z_{n,m}$, only $Z_{n,m}$ ($m \geq 0$) is used as the image feature. Table 1 lists the ZM features from orders 0 through 10. So we have 36 Zernike moments in total.

Table 1 List of Zernike Moments for Different Orders

Order *n*	Zernike moments	Number of the moments	Cumulative number
0	$Z_{0,0}$	1	1
1	$Z_{1,1}$	1	2
2	$Z_{2,0}$, $Z_{2,2}$	2	4
3	$Z_{3,1}$, $Z_{3,3}$	2	6
4	$Z_{4,0}$, $Z_{4,2}$, $Z_{4,4}$	3	9
5	$Z_{5,1}$, $Z_{5,3}$, $Z_{5,5}$	3	12
6	$Z_{6,0}$, $Z_{6,2}$, $Z_{6,4}$, $Z_{6,6}$	4	16
7	$Z_{7,1}$, $Z_{7,3}$, $Z_{7,5}$, $Z_{7,7}$	4	20
8	$Z_{8,0}$, $Z_{8,2}$, $Z_{8,4}$, $Z_{8,6}$, $Z_{8,8}$	5	25
9	$Z_{9,1}$, $Z_{9,3}$, $Z_{9,5}$, $Z_{9,7}$, $Z_{9,9}$	5	30
10	$Z_{10,0}$, $Z_{10,2}$, $Z_{10,4}$, $Z_{10,6}$, $Z_{10,8}$, $Z_{10,10}$	6	36

(3) To reduce the influence of rotation, the Zernike moments are multiplied by an exponent $e^{-jm\varphi_{s,1}}$. Amplitudes and phases of corrected Zernike moments, $Z'_{n,m}$, are obtained to form the ZM features. Each of the amplitudes and phases of the modified ZMs is then encoded into 3 bits to form the intermediate hash. Thus the hash length is 36×2×3=216 bits.

(4) The final hash sequence is obtained by pseudo-randomly permuting the binary sequence obtained in the previous step.

4. Experiments and Hash Performance

In the experiment, the image size was normalized to 128×128. The resized images were low-pass filtered with a 3×3 Gaussian low-pass mask with standard deviation = 1. As stated in Section 3, the hash length was 216 bits. We use Hamming distance to measure similarity between hashes:

$$D(H_1, H_2) = \sum_{k=1}^{K} \left| H_1(k) - H_2(k) \right| \tag{10}$$

where *K* is the length of the image hash.

Four standard images sized 512×512 were used in the experiment: Airplane, House, Lena, and Baboon. To test robustness of the hash, StirMark 4.0 [18] was used to perform attacks including JPEG coding, additive noise contamination, watermark embedding and image scaling. In addition, brightness adjustment, contrast adjustment and rotation using Adobe Photoshop, and gamma correction and 3×3 Gaussian filtering using MATLAB are also tested. The types of attacks and the parameters used are listed in Table 2. The indices in the left-most column correspond to the abscissa of Fig. 3.

4.1. Comparison of Methods Using ZM and Modified ZM

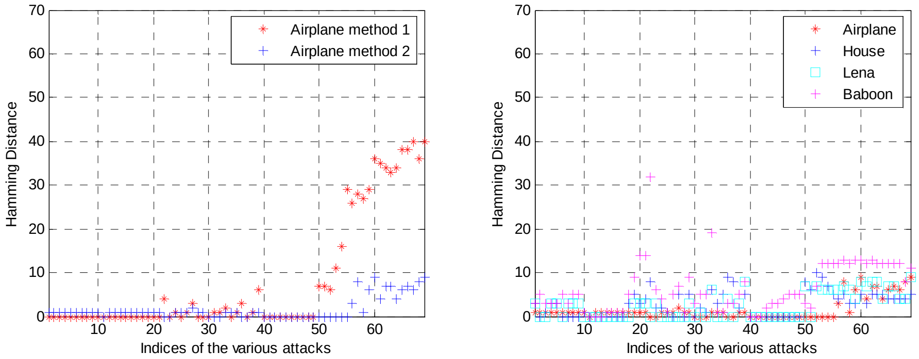
Two hashing methods are compared in Fig. 3(a). Method 1 uses amplitudes and phases of ZM to derive the image hashing, and Method 2 uses the amplitudes and phases of modified ZM. It is observed that Method 1 is robust against JPEG compression, additive noise, watermark embedding, scaling, brightness and contrast adjustments, gamma correction, and Gaussian filtering, but is not robust against rotation, indicated by the large Hamming distances. Method 2 is robust against all these content-preserving attacks.

4.2. Robustness Test

Distances between hashes of the original and attacked images are calculated. The results are presented in Fig. 3(b). We observe that most Hamming distances are no more than 20, with a few exceptions corresponding to manipulations that cause significant changes in the image intensity. Thus, we can safely set a threshold at, say, 30, to judge whether or not two images can be considered visually identical. If the Hamming distance is greater than the threshold, the two images are considered different.

Table 2 Parameters Used in the Robustness Experiment

Indices	Attack	Description	Parameter value
1-9	JPEG compression	Quality factor	20, 30, … , 100
10-11	Additive noise	Level	1, 2
12-21	Watermark embedding	Strength	10, 20, … , 100
22-27	Scaling	Ratio	0.5, 0.75, 0.9, 1.1, 1.5, 2.0
28-31	Brightness adjustment	Photoshop's brightness scale	10, 20, -10, -20
32-35	Contrast adjustment	Photoshop's contrast scale	10, 20, -10, -20
36-39	Gamma correction	γ	0.75, 0.9, 1.1, 1.25
40-49	3×3 Gaussian filtering	Standard deviation	0.1, 0.2, ... , 1.0
50-69	Rotation	Angle in degrees	1, 2, … , 20



(a) Comparison of two methods

(b) Robustness against attacks

Fig. 3 Performance of ZM-based Image Hashing. Indices in the Abscissa Correspond to Attacks as Listed in Table 2.

4.3. Uniqueness of Hashes

Uniqueness means that two hash sequences from two different images should be sufficiently different. Fig. 4 shows the probability distributions of the Hamming distance calculated from $C_{2112}^{2} = 2229216$ hash pairs with 2112 different images and that of the Hamming distance calculated from 13511 pairs of similar images. In these different images, 8 are well-known benchmark images, 1715 downloaded natural images from the Internet, and 389 captured with digital cameras. The mean and standard deviation of different images' distribution is 57.18 and 8.03 respectively. The mean and standard deviation of similar images' distribution is 5.45 and 9.73 respectively.

To evaluate performance of the proposed hashing scheme, we calculate probabilities of the two types of errors: P_C and P_E. P_C is the probability of collision, meaning that two different images have similar hash values with the Hamming distance less than a threshold, while P_E is the probability of false collision between two similar images.

Probabilities of these errors vary with a different threshold value as shown in Table 3. We can see that a threshold value 30 gives a very low collision probability and an acceptable false collision probability, which conforms to Fig. 3(b). This is considered an acceptable trade-off between robustness, forgery detection capability (as will be seen in the next sub-section) and security of the system.

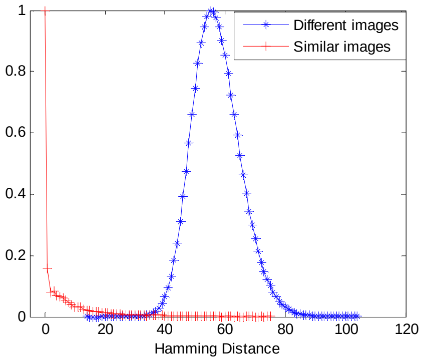


Fig. 4 Distribution of Hamming Distance

Table 3 Relationship Between Threshold Value and Error Probabilities

Threshold	20	25	30	35	40	45	50
P_{C}	$1.79\times10\text{-}^{6}$	9.87×10^{-6}	7.22×10^{-5}	8.67×10^{-4}	9.45×10^{-3}	5.88×10^{-2}	0.204
P_{E}	0.078	0.054	0.039	0.028	0.018	0.011	0.0057

4.4. Forgery Detection Capability

In this experiment, anti-forgery performance of the proposed method was tested with a total of 2112 uncompressed images that were processed with content-preserving operations, and 2112 forged images. Some of the forged images were produced using Photoshop to give a natural look, while most generated automatically by running a program that simply pasted a foreign block into the image. The pasted area was 10% of the host. To measure the forgery detection performance, the false negative and false positive probabilities are calculated:

$$P_{\mathrm{FN}} = \frac{\text{Number of forged images judged as natural images}}{\text{Total number of forged images}} \tag{11}$$

$$P_{\mathrm{FP}} = \frac{\text{Number of natural images judged as forged images}}{\text{Total number of natural images}} \tag{12}$$

Fig. 5 gives four ROC curves corresponding to three types of content-preserving processing: gamma correction (γ=1.1 and 1.15), rotation by 20°, and JPEG compression with $Q = 30$. It is seen that the hash has good ability in distinguishing rotation and JPEG coding from copy-move forgery, and it is reasonably good for gamma correction.

Table 4 gives some examples, with original and forged images, and the Hamming distances. The first six original images are taken from [19] and the next two downloaded from Internet. The forged versions of these eight images were produced with Photoshop. The last two forged images were generated by running a MATLAB program, in which the replaced blocks are outlined by white rectangles.

We observe from the experiment that tampering strong enough is detectable. Hamming distance of the first image pair (Peppers) is relatively small since the Zernike moments are calculated on a unit circle, and most of the tampered area is outside the circle as shown in Fig. 6.

In general, the proposed hashing method is sensitive to changes in the shape and profile of objects, but not the fine details. For detection of image tampering that affects fine details, further studies are needed.

5. Conclusions

In this paper, an image hashing method is proposed based on rotation invariance of magnitudes and modified phases of Zernike moments, which are multiplied by an exponent. Each of the amplitudes and phases of the modified ZM is encoded into 3 bits to form an intermediate hash. The final hash sequence is obtained by pseudo-randomly permuting the intermediate hash. Similarity between hashes is measured by Hamming distance. Experimental results show that the method is robust against most content-preserving image manipulations such as JPEG compression, watermark embedding and rotation. Hashes between a pair of different images have very low collision probability. Image forgery involving structural modifications may be detected using the ZM-based image hash.

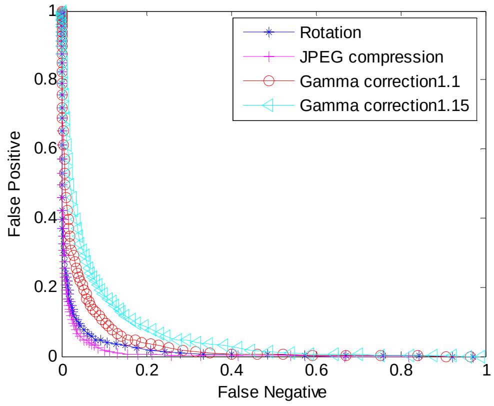
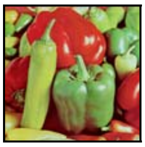
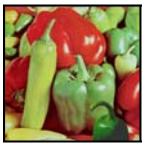
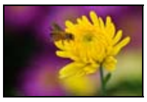
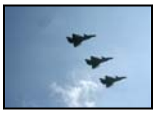
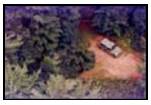
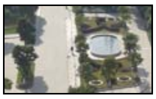
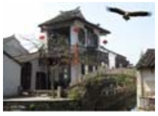
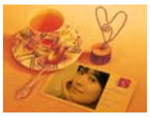
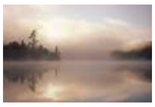
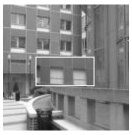
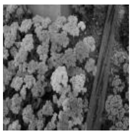
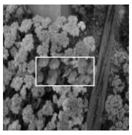


Fig. 5 ROC Curve of the Proposed Method

Table 4 Hamming Distance *D* between Original and Forged Images

Original	Forged	Image size	*D*	Original	Forged	Image size	*D*
		512×512	26			600×399	40
		570×395	43			482×319	49
		540×319	40			600×430	54
		700×525	59			289×432	55
		128×128	51			128×128	55

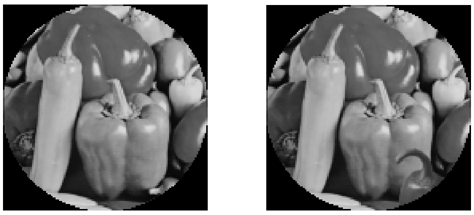


Fig. 6 Original and Tampered Images in the Unit Circle

In the proposed scheme, Zernike moment is calculated from the inscribed circle of a normalized square image, inevitably leading to loss of information in the image corners and reducing sensitivity of the hash to tampering. This may be overcome by mapping a rectangular image to a circle instead of taking the inscribed circle for Zernike moment calculation so that contents in corners is preserved. In addition, further study is needed to enhance sensitivity of hashes to tampering in small regions involving fine details.

Acknowledgement

This work was supported by the Natural Science Foundation of China (60773079, 60872116, 60832010)

References

[1] V. Monga, A. Banerjee and B. L. Evans, A clustering based approach to perceptual image hashing[J], IEEE Transactions on Information Forensics and Security, 2006, 1(1): 68-79

[2] S. Xiang, H. J. Kim and J. Huang, Histogram-based image hashing scheme robust against geometric deformations[C], Proc. of the ACM Multimedia and Security Workshop, ACM Press, 2007, pp. 121-128

[3] S. S. Kozat, K. Mihcak and R. Venkatesan, Robust perceptual image hashing via matrix invariants[C], Proc. of IEEE Conference on Image Processing (ICIP'04), Singapore, Oct. 24-27, 2004, pp. 3443-3446

[4] V. Monga and M. K. Mihcak, Robust and secure image hashing via non-negative matrix factorizations[J], IEEE Transactions on Information Forensics and Security, 2007, 2(3): 376-390

[5] Z. Tang, S. Wang, X. Zhang, W. Wei and S. Su, Robust image hashing for tamper detection using non-negative matrix factorization[J]. Journal of Ubiquitous Convergence and Technology, 2008, 2(1): 18-26

[6] Z. Tang, S. Wang, X. Zhang, W. Wei and Y. Zhao, Lexicographical framework for image hashing with implementation based on DCT and NMF, Multimedia Tools and Applications[J], 2010, DOI: 10.1007/s11042-009-0437-y

[7] V. Monga and B. L. Evans, Perceptual image hashing via feature points: performance evaluation and trade-offs[J], IEEE Transactions on Image Processing, 2006, 15(11): 3453-3466

[8] F. Ahmed, M.Y. Siyal and V. U. Abbas, A secure and robust hash-based scheme for image authentication[J], Signal Processing, 2010, 90 (5): 1456-1470

[9] J. Fridrich and M. Goljan, Robust hash functions for digital watermarking[C], Proc. of IEEE International Conference on Information Technology: Coding and Computing (ITCC'00), Las Vergas, USA, Mar. 27-29, 2000, pp. 178-183

[10] Y. Lin and S. F. Chang, A robust image authentication system distinguishing JPEG compression from malicious manipulation[J]. IEEE Transactions on Circuits System and Video Technology, 2001, 11(2):,153-168

[11] C. D. Roover, C. D. Vleeschouwer, F. Lefebvre and B. Macq, Robust video hashing based on radial projections of key frames[J], IEEE Transactions on Signal Processing, 2005, 53(10): 4020-4036

[12] F. Lefebvre, B. Macq and J.-D. Legat, RASH: Radon soft hash algorithm[C], Proc. of European Signal Processing Conference (EUSIPCO'02), Toulouse, France, Sep. 3-6, 2002, pp.299-302

[13] A. Swaminathan, Y. Mao and M. Wu, Robust and secure image hashing[J], IEEE Transactions on Information Forensics and Security, 2006, 1(2): 215-230

[14] F. Zernike, Beugungstheorie des schneidenverfahres und seiner verbesserten form[J], der phasenkontrastmethode, Physica, 1934, 1, pp.689-704

[15] H. Lin, J. Si, Glen P. Abousleman, Orthogonal rotation-invariant moments for digital image processing[J], IEEE

Transactions On Image Processing, 2008, 17(3): 272-282

[16] S. Li, M.C. Lee, C.M. Pun, Complex Zernike moments features for shape-based image retrieval[J], IEEE Transactions On Systems, Man, and Cybernetics-part A: Systems and Humans, 2009, 39(1): 227-237

[17] Z. Chen, S. K. Sun, A Zernike moment phase based descriptor for local image representation and matching[J], IEEE Transactions on Image processing, 2010, 19(1): 205-219

[18] F. A. P, Petitcolas (2000) Watermarking schemes evaluation[J], IEEE Signal Processing Magazine,17(5): 58-64

[19] Z. Tang, Perceptual Image Hashing: Framework, Methods, and Performance Evaluation, PhD dissertation, Shanghai University, 2009, pp.59-60