

# Wave Atom-Based Perceptual Image Hashing Against Content-Preserving and Content-Altering Attacks

Fang Liu<sup>(✉)</sup> and Lee-Ming Cheng

Department of Electronic Engineering, City University of Hong Kong,  
83 Tat Chee Avenue, Kowloon Tong, Hong Kong  
f.liu@my.cityu.edu.hk, itlcheng@cityu.edu.hk

**Abstract.** This paper presents a perceptual image hashing algorithm based on wave atom transform, which can distinguish maliciously attacked images from content-preserving ones. Wave atoms are employed due to their significantly sparser expansion and better feature extraction capability than traditional transforms, like discrete cosine transform (DCT) and discrete wavelet transform (DWT). Thus, it is expected to show better performance in image hashing. Moreover, a preprocessing method based on Fourier-Mellin transform is employed to keep the proposed scheme against geometric attacks. In addition, a randomized pixel modulation based on RC4 is performed to ensure the security. According to the experimental results, the proposed scheme is sensitive to content-altering attacks with the resiliency of content-preserving operations, including image compression, noising, filtering, and rotation. Moreover, compared with some other image hashing algorithms, the proposed approach also achieves better performance even in the aspect of robustness, which is more important in some image hashing application, for example image database retrieval or digital watermarking.

**Keywords:** Image hashing · Authentication · Robustness · Wave atom transform

## 1 Introduction

Nowadays, the vigorous popularity of image processing techniques has resulted in an explosive growth of image illegal use, such as image forgery and unauthorized utilization. A traditional solution to deal with data illegal issues is to generate a hash using some standard cryptographic hash functions, like MD5 and SHA-1, and form a digital signature by some public key encryption algorithms [1]. This kind of hash functions achieves high sensitivity when applied to data authentication, where even one bit change in the message will result in significant changes in the hash value. Unfortunately, it is the sensitivity that makes these functions not applicable to digital images. Since images will also be considered as the identical one even if they have undergone some content-preserving manipulations, such as image compression, noising, and filtering.

Perceptual image hashing has been therefore presented to provide the content-based authentication, copyright verification and some other protections for digital images.

The core idea of perceptual image hashing is to construct the hash by extracting characteristics of human perception in images, and use this constructed hash to authenticate or retrieve an image without considering the various variables or formats of this image. This kind of schemes takes the changes of human perception into account and ignores the perceptually unnoticeable changes. They have drawn a lot of attention owing to the outstanding performance against common image processing operations. There are two important performance requirements for strong image hashing schemes, namely robustness and fragility, which influence each other mutually. Robustness is the degree to which an image hashing scheme is invariant to perceptually identical images, while fragility is the degree to which the scheme distinguishes the perceptually different images from the original ones. Consequently, it is expected that images which look like the same or very similar should have the same or very similar hash codes, while images which differ from each other should have distinct hash codes.

At present, many research studies have been carried out on perceptual image hashing based on various transformations, such as DWT [2–7], DCT [8, 9], Radon transform (RT) [10–12], discrete Fourier transform (DFT) [13–15], and others.

In 1998, a scale interaction model is used in wavelet domain to extract visually salient image feature points for image authentication [2]. Venkatesan et al. also extracted the invariant statistics characteristics of wavelet coefficients to construct robust hash in 2000 [3]. In the same year, an invariant relation of the parent and child pair nodes located at multiple scales in DWT decomposition is explored for hash generation as well [4]. Monga and Evans also exploited the features derived from the end-stop wavelet coefficients to detect visually significant feature points [5, 6]. Recently, Ahmed et al. [7] proposed a secure image hashing using both DWT and SHA-1.

Fridrich and Goljan [8] also took the advantage of that low frequency coefficients in DCT can represent the coarse information of a whole image and proposed a robust hash for digital watermarking. Lin and Chang [9] found a desired relation to construct their robust hash. This relation is based on the fact that DCT coefficients in the same position of different blocks are invariant before and after JPEG compression.

Since the Radon transform is also robust against image processing basic attacks and strong attacks, Lefebvre [10] first applied it to image hash. Further research has been taken by Roover [11] based on radial projection of the image pixels and is denoted the Radial hASHing (RASH) algorithm. A new approach is also proposed for image fingerprinting using the Radon transform to make the fingerprint robust against affine transformations by Seo et al. in [12].

There are lots of hashing schemes based on DFT as well. In [13], Swaminathan et al. developed an algorithm to generate a hash based on Fourier transform features and controlled randomization. In [14], a print-scan resistant image hashing algorithm is proposed based on the RT domain combining with DWT and DFT. In [15], moment features are extracted from the RT domain and the significant DFT coefficients of the moments are used to produce hashes.

Besides the transformations employed above, the matrix factorization is also prevalent in the field of perceptual image hashing [16–18]. Kozat et al. [16] proposed the hashing scheme based on matrix invariants as embodied by Singular Value Decomposition (SVD) and viewed images as well as attacks as a sequence of linear operators. Monga and Mihcak [17] first employed the low-rank decomposition of nonnegative

matrix factorization (NMF) with NMF of pseudo-randomly selected subimages to derive hashes. Tang et al. [18] explored the invariance relation existing in the NMF for constructing robust image hashes too. Recently, Tang et al. also proposed an efficient image hashing with a ring partition and a NMF, which is claimed with both the rotation robustness and good discriminative capability.

Moreover, there are many other significant methods for perceptual hashing as well. For instance, Lv and Wang [19] proposed a robust SIFT-Harris detector for selecting the most stable SIFT key points. The image hashes are then generated by embedding the detected local features into shape-contexts-based descriptors. And SIFT features are also used in the work of forensic hashing [20] to estimate geometric transform, while the block-based features are employed to detect and localize the image tampering. Khelifi and Jiang [21] proposed a robust and secure hash algorithm based on virtual watermarking detection which can detect the malicious changes in relatively large areas. Zhao et al. [22] employed Zernike moments representing the luminance and chrominance of an image as the global features, and position and texture information of salient regions as the local features to form their hashes.

However, compromise has always been made between robustness and fragility among those hashing schemes. Fortunately, it is expected that wave atom transform can achieve better performance than these conventional transforms in image hashing. Demanet and Ying introduced wave atom transform in 2007 [23], which are a recent addition to the repertoire of mathematical transforms of computational harmonic analysis. They have been proved to have a dramatically sparser expansion of wave equations than traditional transformations, which come either as an orthonormal basis or a tight frame of directional wave packets, and are particularly suitable for representing oscillatory patterns in images. Motivated by these attractive characteristics, this paper demonstrated the feasibility of wave atom transform applied in perceptual hashing based on our previous work [24]. In addition, a preprocessing image authentication method is proposed to further ensure the proposed scheme against geometric attacks using Fourier-Mellin transform.

The rest of this paper is structured as follows. Section 2 shows a brief overview and implementation of wave atom transform. The proposed algorithm is described in Sect. 3. The experimental analysis is presented in Sect. 4, whereas the conclusions are giving in Sect. 5.

## 2 Wave Atom Transform

Demanet and Ying introduced wave atoms as a variant of 2-D wavelet packets in 2007 [23], which can adapt to arbitrary local directions of a pattern, and can also sparsely represent anisotropic patterns aligned with the axes. Oscillatory functions and oriented textures in wave atoms have been proved to have a dramatically sparser expansion compared to some other fixed standard representations like Gabor filters, wavelets, and curvelets. Wave atoms interpolate precisely between Gabor atoms [25] and directional wavelets [26]. The period of oscillations of each wave packet is related to the size of essential support via parabolic scaling, i.e.  $wavelength \sim (diameter)^2$ .

Wave atoms can be constructed from tensor products of adequately chosen 1-D wave packets. Let  $\psi_{m,n}^j(x)$  represent a 1-D wave packet, where  $j, m \geq 0$ , and  $n \in \mathbb{Z}$ , centered in space around  $x_{j,n} = 2^{-j}n$  and centered in frequency around  $\pm w_{j,m} = \pm \pi 2^j m$  respectively, with  $C_1 2^j \leq m \leq C_2 2^j$ . The basis function is defined combining dyadic scaled and translated versions of  $\psi_m^0$  in the frequency domain as the following

$$\psi_{m,n}^j(x) = \psi_m^j(x - 2^{-j}n) = 2^{j/2} \psi_m^0(2^j x - n) \quad (1)$$

where

$$\psi_m^0(w) = e^{-iw/2} [e^{iz_m} g(\varepsilon_m(w - \pi(m + 1/2))) + e^{-iz_m} g(\varepsilon_{m+1}(w + \pi(m + 1/2)))] \quad (2)$$

with  $\alpha_m = \pi/2(m + 1/2)$ ,  $\varepsilon_m = (-1)^m$  and  $g$  a real-value  $C^\infty$  bump function is compactly supported on an interval of length  $2\pi$  such that  $\sum_m |\psi_m^0(w)|^2 = 1$ .

For each wave  $w_{j,m}$  at scale  $2^{-j}$ , the coefficient  $c_{j,m,n}$  is treated as a decimated convolution.

$$c_{j,m,n} = \int \psi_m^j(x - 2^{-j}n) u(x) dx = \frac{1}{2\pi} \int e^{i2^{-j}nw} \overline{\hat{\psi}_m^j(w)} \hat{u}(w) dw. \quad (3)$$

Discretize the sample  $u$  at  $x_k = kh$ ,  $h = 1/N$ ,  $k=1, \dots, N$ , and the discrete coefficients  $c_{j,m,n}^D$  are calculated by utilizing a reduced inverse FFT inside an interval of size  $2^{j+1}\pi$ , centered around the origin

$$c_{j,m,n}^D = \sum_{k=2\pi} (-2^j/2+1:2^j/2) e^{i2^{-j}nk} \sum_{p \in 2\pi\mathbb{Z}} \overline{\hat{\psi}_m^j(k + 2^j p)} \hat{u}(k + 2^j p). \quad (4)$$

There is a simple wrapping technique for implementation of 1-D wave packet as follows:

- (1) Perform a FFT of size  $N$  of the samples  $u(k)$ .
- (2) For each pair  $(j, m)$ , wrap the product  $\overline{\hat{\psi}_m^j} \hat{u}$  by periodicity inside the interval  $[-2^j\pi, 2^j\pi]$  and perform an inverse FFT of size  $2^j$  to obtain  $c_{j,m,n}^D$ .
- (3) Repeat step (2) for all pairs  $(j, m)$ .

The 2-D orthonormal basis functions with four bumps are formed by individually utilizing products of 1-D wave packets in the frequency plane. Let  $\mu = (j, m_1, m_2, n_1, n_2)$ , the basis function is modified as

$$\phi_\mu^+(x_1, x_2) = \psi_{m_1}^j(x_1 - 2^{-j}n_1) \psi_{m_2}^j(x_2 - 2^{-j}n_2). \quad (5)$$

A dual orthonormal basis can be established from the ‘‘Hilbert-transformed’’ wavelet packets as

$$\phi_{\mu}^{-}(x_1, x_2) = H\psi_{m1}^j(x_1 - 2^{-j}n_1)H\psi_{m2}^j(x_2 - 2^{-j}n_2). \quad (6)$$

By combining Eqs. (5) and (6), basis functions with two bumps are provided in the frequency domain, and directional wave packets oscillate in one single direction

$$\phi_u^{(1)} = (\phi_u^{+} + \phi_u^{-})/2, \quad \phi_u^{(2)} = (\phi_u^{+} - \phi_u^{-})/2 \quad (7)$$

where  $\phi_u^{(1)}$  and  $\phi_u^{(2)}$  are denoted as  $\phi_u$  together which form the wave atoms frame.

### 3 Proposed Algorithm

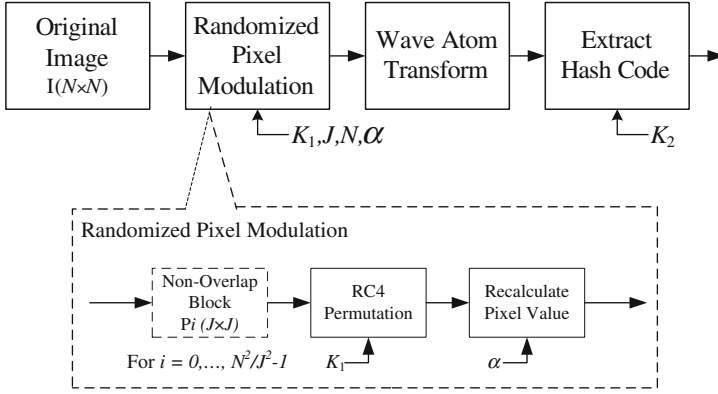
In this section, a compelling image hashing scheme is proposed based on wave atom transform, which satisfies both robustness and fragility for image hashing against content-preserving and content-altering attacks. Some initial work is presented in [24]. Wave atom transform is used since it can represent the image features better than other transforms. It has also been observed that the use of wave atom coefficients in the third scale band gives good robustness to common signal processing attacks except rotation manipulation, since rotation manipulation indeed changes an image perceptually to a certain extent. Consequently, a rotation-invariant preprocessing enhancement is presented in image authentication module to further ensure the robustness of our proposed algorithm against geometric attack. Besides, a randomized pixel modulation (RPM) [7] is used to enhance the security of our proposed scheme. Before applying wave atom transform, all pixels in the spatial domain are randomly modulated using a pseudo-random secret key stream based on RC4. The details of the proposed algorithm are shown below.

#### 3.1 Hash Generation Module

The detailed procedures of hash generation module shown in Fig. 1 are described as follows:

- (1) Let  $I$  denote the original input image of size  $N \times N$ .
- (2) Then, the RPM [7] is employed to  $I$  for the purpose of security. The details are described as follows:  
 Firstly, divide  $I$  into a number of non-overlapping blocks with dimension  $J \times J$  for each block. Thus,  $N^2/J^2$  blocks are generated. Denote  $P_i$  as the  $i$ -th block, where  $i = 0, \dots, N^2/J^2 - 1$ . And  $J$  is set to 16 in our implementation.

Secondly, the RC4 algorithm governed by a secret key  $K_1$  is employed to generate pseudo-random numbers for each block  $i$ . By sorting a  $J \times J$  generated number sequence in descending order, the indexes for all these numbers in the original sequence are marked. Let  $P_i(x, y)$  represent the gray value of the pixel at spatial domain location  $(x, y)$  in block  $P_i$ , and further reshaped to one dimension as  $S_i(m)$  where  $m = x + (y - 1) \times J$ . Then  $S_i(m)$  is permuted according to the marked indexes and denoted as  $S'_i(m)$ .



**Fig. 1.** Hash generation module

Finally, in order to make the image hash code dependent on the secret key, every pixel in each block is modulated as the following

$$P'_i(x, y) = P_i(x, y) + \alpha \times S'_i(m) \quad (8)$$

where  $P'_i(x, y)$  is the new pixel value and  $1 \leq x, y \leq J$  and  $m = x + (y - 1) \times J$ .

- (3) By performing wave atom transform to the image of new pixel values, several scale bands could be obtained, which has different frequencies. For each scale band, there are a number of sub-blocks which consists of different numbers of wave atom coefficients. Among these scale bands, the third scale band is selected to compute the hash code, since middle frequency scale coefficients are more robust than high frequency ones, and also more fragile than low frequency ones [26]. Since the energy of wave atom coefficients captures most information of main image features, the intermediate hash could be computed by exploring the mutual relationship of these sub-blocks.
- (4) Denote  $C(j, m_1, m_2, n_1, n_2)$  as wave atom coefficients, where  $j$  is the scale, and  $m_1, m_2, n_1, n_2$  represents the phase. Assign an index  $i$  for each sub-block in the third scale band. Let  $E_i$  be the energy of the  $i$ -th block. For all non-empty blocks in the third scale band

$$E_i = \sum_{q=1}^{l_2} \sum_{p=1}^{l_1} C(j, m_1, m_2, p, q)^2 \quad (9)$$

where  $l_1$  and  $l_2$  represent the length and width of the sub-block respectively.

To ensure that the extracted features used to generate the hash code cannot be exposed, a random sequence generated by RC4 is XORed with  $E_i$  to generate the new sequence  $E'_i$ . Let the total number of non-empty blocks in the third scale band be  $t$ . The energy difference between each two blocks is used to generate one hash bit. The intermediate hash can be calculated using this equation:

$$h^{(i)} = \begin{cases} 1, & \text{if } E'_i > E'_{i+1} \\ 0, & \text{Otherwise} \end{cases} \quad (10)$$

where  $i \in [1, \dots, t-1]$ .

To increase the security of hash code, a pseudo-random sequence generated by the secret key  $K_2$  is employed to XOR the intermediate hash  $h$  based on RC4 algorithm and generates the final hash  $H$ .

### 3.2 Image Authentication Module

To keep the robustness of the proposed scheme against common content-preserving attacks and geometric attacks, a rotation-invariant preprocessing is first presented in this section using Fourier-Mellin transform. Then the proposed authentication procedures are presented.

#### 3.2.1 Rotation-Invariant Preprocessing

It is well known that the Fourier-Mellin transform is invariant to rotation, translation and scaling manipulations, which is especially useful for image recognition [27]. In this paper, to ensure the proposed scheme robust to geometric attacks, the rotation-invariant property of Fourier-Mellin transform is employed in the proposed image hashing scheme.

Let  $I_1(x, y)$  denote an image, and  $I_2(x, y)$  is a translated and rotated replica of  $I_1(x, y)$  with translation  $(x_0, y_0)$  and rotation angle  $\varphi_0$ , then

$$I_2(x, y) = I_1(x \cos \varphi_0 + y \sin \varphi_0 - x_0, -x \sin \varphi_0 + y \cos \varphi_0 - y_0). \quad (11)$$

According to Fourier Transform and its properties, transforms of  $I_1$  and  $I_2$  are related by

$$F_2(u, v) = e^{-j2\pi(ux_0 + vy_0)} F_1(u \cos \varphi_0 + v \sin \varphi_0, -u \sin \varphi_0 + v \cos \varphi_0). \quad (12)$$

Denote  $M_1$  and  $M_2$  as the magnitudes of  $F_1$  and  $F_2$ , thus we have

$$M_2(u, v) = M_1(u \cos \varphi_0 + v \sin \varphi_0, -u \sin \varphi_0 + v \cos \varphi_0). \quad (13)$$

Using the polar coordinates, Eq. (13) can be rewritten as

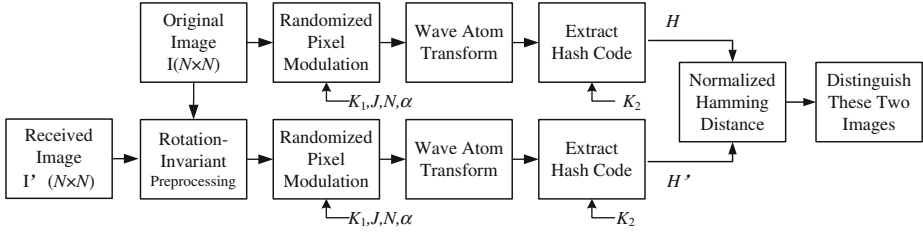
$$M_2(\rho, \varphi) = M_1(\rho, \varphi - \varphi_0). \quad (14)$$

Here, it is evident that there is only a same rotation which results from the image domain. The angle of rotation  $\varphi_o$  can be calculated using phase correlation.

Consequently, this preprocessing is provided using Fourier-Mellin transform which can estimate the rotated angle. And if the estimated angle is not zero, the translated and rotated image is rotated back. Otherwise, the image is not preprocessed.

### 3.2.2 Authentication Procedure

The image authentication module as illustrated in Fig. 2 is then employed to authenticate the received image. Using the same parameters  $N, K_1, K_2, \alpha$  and  $J$ , system can calculate the hash code of the received image and make the comparison with the original hash code in terms of normalized Hamming distance. The image authentication procedures are described as follows:



**Fig. 2.** Image authentication module

- (1) The received image goes through the rotation-invariant preprocessing as described in Sect. 3.2.1.
- (2) The output image undergoes the same steps as described in Sect. 3.1 in which the hash code  $H'$  is calculated.
- (3) Denote the  $i$ -th hash value of the original image and received image as  $H(i)$  and  $H'(i)$  respectively, the normalized Hamming distance  $d$  is therefore computed by

$$d(H, H') = 1/L \sum_{i=1}^L \delta(H(i), H'(i)) \quad (15)$$

where  $L$  is the length of hash and

$$\delta(H(i), H'(i)) = \begin{cases} 0, & H(i) = H'(i) \\ 1, & H(i) \neq H'(i) \end{cases} \quad (16)$$

- (4) Denote  $\vartheta$  as a threshold to decide whether the received image could be authenticated. If the calculated normalized Hamming distance is larger than  $\vartheta$ , the image  $I'$  is considered as a tampered or even a different one, which is unauthentic. Otherwise the image  $I'$  will be authenticated.

## 4 Experimental Analysis

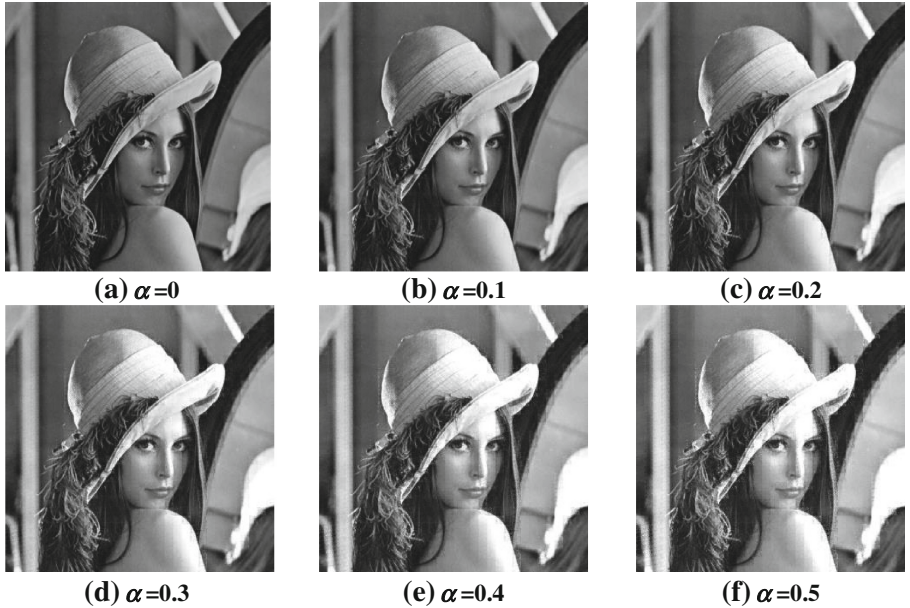
In order to test the performance of the proposed algorithm, 21 gray-scale images of size  $512 \times 512$  are used as the original test images, and the total numbers of images for content-preserving operations and content-altering attacks are 1113 and 442, respectively. Moreover, three image hashing algorithms are used for comparison in terms of robustness. The FAR versus FRR curve is also given to demonstrate the global



performance of our proposed algorithm where the normalized Hamming distance  $d$  is used as the metric.

#### 4.1 Content-Preserving Experimental Analysis and Comparisons

It is important to notice that a good perceptual image hashing scheme can authenticate perceptually identical images from the perceptually different images. In this section, some common content-preserving image processing operations conducted on Stirmark benchmark [28] are applied to illustrate the performance of our proposed scheme, including geometric operations. Table 1 shows the average normalized Hamming distance of the whole 21 original images under those operations based on different  $\alpha$ . Different versions of image Lena are also shown in Fig. 3 under different value of  $\alpha$  for example. The parameter  $\alpha$  in Eq. (8) is used to enhance the security of the hash code such that the new pixel value depends on both the original pixel value and the secret key. Without knowing the secret key, an attacker cannot extract the hash accurately, thus cannot create a forged image.



**Fig. 3.** Different versions of image Lena under different value of  $\alpha$

Note that the normalized Hamming distance is expected to approach zero for the perceptually identical images and approach 0.5 for different images. It can be also observed that the values of average normalized Hamming distance  $d$  between the hashes extracted from the original and processed images are all small under all manipulations, including geometric operations in Table 1, and with the increase of  $\alpha$ ,

**Table 1.** Average normalized Hamming distance under different image processing operations conducted on Stirmark benchmark

Image	Parameter	Average Normalized Hamming Distance $d$					
		$\alpha = 0$	$\alpha = 0.1$	$\alpha = 0.2$	$\alpha = 0.3$	$\alpha = 0.4$	$\alpha = 0.5$
JPEG compression	15	0.0145	0.0207	0.0166	0.0193	0.0207	0.0200
	20	0.0110	0.0186	0.0145	0.0193	0.0200	0.0186
	25	0.0069	0.0097	0.0110	0.0214	0.0166	0.0186
	30	0.0069	0.0124	0.0138	0.0186	0.0186	0.0138
	35	0.0076	0.0124	0.0117	0.0166	0.0173	0.0152
	40	0.0083	0.0124	0.0117	0.0145	0.0159	0.0152
	50	0.0062	0.0090	0.0055	0.0138	0.0152	0.0145
	60	0.0048	0.0076	0.0062	0.0145	0.0138	0.0131
	70	0.0028	0.0083	0.0062	0.0159	0.0124	0.0145
	80	0.0014	0.0055	0.0041	0.0138	0.0131	0.0131
	90	0.0014	0.0048	0.0041	0.0145	0.0110	0.0124
Noise addition	100	0.0000	0.0062	0.0041	0.0124	0.0124	0.0131
	0	0.0000	0.0055	0.0041	0.0124	0.0124	0.0124
	5	0.0462	0.0455	0.0366	0.0359	0.0380	0.0407
	10	0.1028	0.1049	0.0966	0.0897	0.0890	0.0973
	15	0.1656	0.1580	0.1504	0.1456	0.1366	0.1387
Median filtering	20	0.1656	0.1587	0.1539	0.1511	0.1463	0.1401
	$3 \times 3$	0.0193	0.0200	0.0248	0.0290	0.0311	0.0324
	$5 \times 5$	0.0290	0.0311	0.0276	0.0373	0.0331	0.0317
	$7 \times 7$	0.0393	0.0428	0.0373	0.0428	0.0373	0.0359
Convolution filtering	$9 \times 9$	0.0476	0.0449	0.0442	0.0483	0.0435	0.0449
	Gaussian	0.0849	0.1063	0.1104	0.1242	0.1235	0.1318
Affine transformation	Sharpening	0.0386	0.0386	0.0400	0.0380	0.0455	0.0490
	Y-shearing 1	0.0531	0.0559	0.0504	0.0518	0.0428	0.0455
	Y-shearing 2	0.0966	0.0959	0.0876	0.0911	0.0835	0.0814
	X-shearing 1	0.0518	0.0497	0.0545	0.0476	0.0476	0.0455
	X-shearing 2	0.1008	0.1001	0.0945	0.0925	0.0918	0.0939
	XY-shearing	0.0918	0.0835	0.0745	0.0801	0.0683	0.0718
	General 1	0.0856	0.0828	0.0745	0.0773	0.0697	0.0759
	General 2	0.0828	0.0725	0.0669	0.0732	0.0628	0.0642
	General 3	0.0759	0.0683	0.0635	0.0697	0.0676	0.0656
Rescaling	50	0.0014	0.0069	0.0069	0.0179	0.0207	0.0221
	75	0.0104	0.0117	0.0138	0.0166	0.0207	0.0179
	90	0.0145	0.0166	0.0145	0.0173	0.0200	0.0214
	110	0.0014	0.0062	0.0041	0.0159	0.0159	0.0159
	150	0.0097	0.0117	0.0090	0.0166	0.0159	0.0228
	200	0.0069	0.0076	0.0076	0.0159	0.0166	0.0200
Small random distortion	0.95	0.0621	0.0587	0.0504	0.0511	0.0476	0.0504
	1	0.0566	0.0573	0.0490	0.0476	0.0449	0.0455
	1.05	0.0594	0.0573	0.0483	0.0476	0.0455	0.0469
	1.1	0.0552	0.0552	0.0490	0.0497	0.0462	0.0469
Rotation	$-2^\circ$	0.1001	0.0966	0.0856	0.0883	0.0842	0.0870
	$-1^\circ$	0.0738	0.0752	0.0676	0.0676	0.0649	0.0725
	$1^\circ$	0.0828	0.0807	0.0683	0.0718	0.0656	0.0732
	$2^\circ$	0.0980	0.0897	0.0863	0.0828	0.0801	0.0794
Rotation with cropping	$-2^\circ$	0.0745	0.0732	0.0649	0.0635	0.0600	0.0649
	$-1^\circ$	0.0614	0.0566	0.0483	0.0538	0.0524	0.0504
	$1^\circ$	0.0573	0.0545	0.0524	0.0483	0.0504	0.0545
	$2^\circ$	0.0766	0.0752	0.0642	0.0656	0.0663	0.0773

(Continued)

**Table 1.** (Continued)

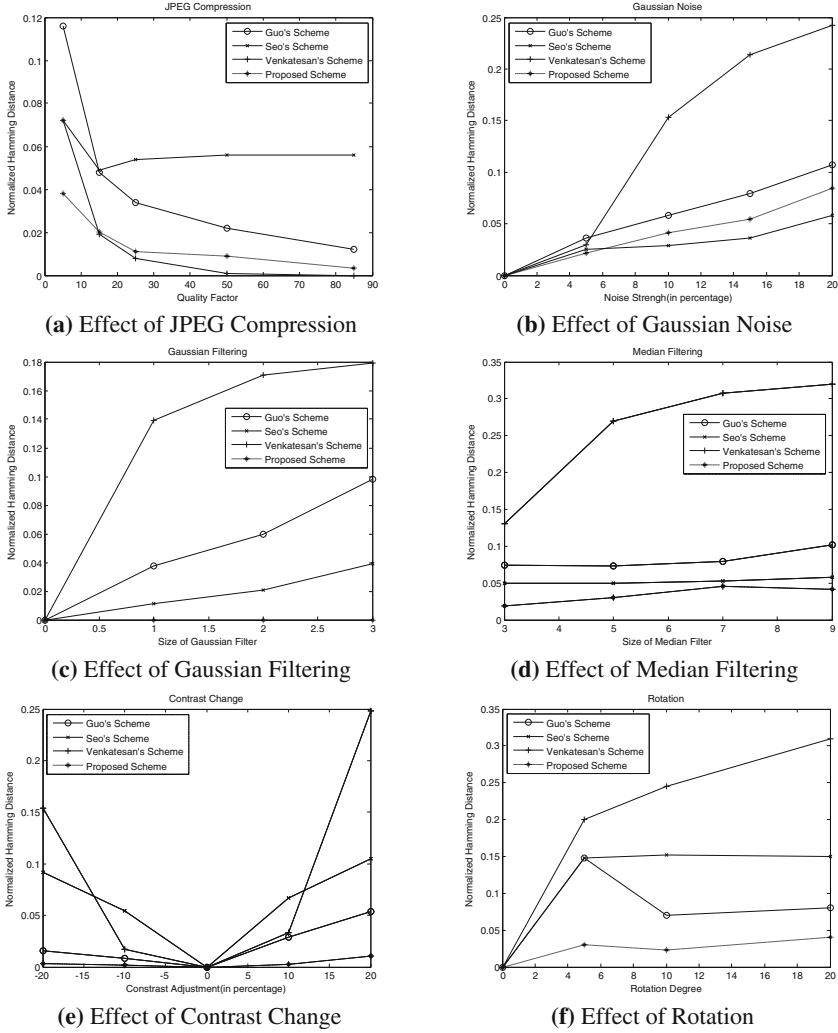
Image	Parameter	Average Normalized Hamming Distance $d$					
		$\alpha=0$	$\alpha=0.1$	$\alpha=0.2$	$\alpha=0.3$	$\alpha=0.4$	$\alpha=0.5$
Rotation with rescaling	$-2^\circ$	0.0821	0.0801	0.0690	0.0628	0.0656	0.0690
	$-1^\circ$	0.0690	0.0718	0.0594	0.0663	0.0656	0.0600
	$1^\circ$	0.0621	0.0649	0.0538	0.0566	0.0552	0.0621
	$2^\circ$	0.0794	0.0773	0.0656	0.0718	0.0676	0.0780

the values of  $d$  are a little increased. Since the coefficients in the third scale band of wave atom transform cannot be changed greatly without changing the content of image. Aware that the values of  $d$  under the parameters of 15 and 20 in Gaussian noise addition operations using Stirmark benchmark are a little larger than others. That's because under these two operations, there is much larger noise all over the images which affects the image quality more severely. By using the rotation-invariant pre-processing, the rotated images have been rotated back, while the non-rotated images have not been processed, thus there are not any perceptually different changes in images except the black background generated from the previous rotation operation, which results to a small  $d$ . Therefore, if the threshold  $\vartheta$  is selected probably, the proposed scheme can authenticate the images which go through all kinds of content-preserving operations conducted on Stirmark benchmark in Table 1.

Moreover, it is well known that image hashing can be used in various applications such as image retrieval or watermarking, in some of which the robustness is the most important standard. Hence, to demonstrate the great robustness of our proposed scheme, three image hashing algorithms proposed by Guo et al. [29], Seo et al. [12] and Venkatean et al. [3] have been compared with our scheme in which  $\alpha$  is chosen as 0.1. Guo et al. proposed a content-based image hashing scheme via wavelet and Radon transform, while Seo's scheme and Venkatean's scheme is based on the Radon transform and wavelet transform respectively. And here we employ the same parameters and the same operations as in other compared schemes on Matlab, such as Gaussian noise, Gaussian filtering, contrast change and rotation with cropping. Fig. 4 shows the performance of these image hashing schemes in terms of normalized Hamming distance.

As shown in Fig. 4(a), the robustness performance of proposed scheme is better than Guo's scheme and Seo's scheme but a little worse than Venkatean's scheme under JPEG compression, where the normalized Hamming distance of the proposed scheme is kept below 0.05. With the increase of Gaussian noise strength in Fig. 4(b), the proposed scheme keeps greater robustness than the scheme proposed by Guo and Venkatean, while a little worse than the scheme proposed by Seo. Considering the effect of Gaussian filtering, Median filtering and contrast change, the performance of our proposed method is better than the other three where the normalized Hamming distances are all below 0.05, whereas in other schemes, the normalized Hamming distance is above 0.1 in some cases. Moreover, the proposed scheme also performs the best and far better than others in geometric rotation manipulations.

In conclusion, the simulation results reveal that our scheme is superior to the schemes proposed by Guo et al., Seo et al. and Venkatean et al. The use of third scale band of wave atom transform enables the proposed algorithm to extract invariant



**Fig. 4.** Comparisons among different image hashing schemes in terms of normalized Hamming distance under different content-preserving manipulations

features from images, which are generally robust against content-preserving image manipulations.

## 4.2 Content-Altering Experimental Analysis

Although robustness is an important criterion for image hashing, fragility is also an indispensable considered factor. To prove the capability of image content-altering detection, 442 images are used to test in total, and only several tampered versions of image Lena have been shown in Fig. 5. Table 2 shows the normalized Hamming

distances between the hashes of Lena and tampered versions of Lena under different values of  $\alpha$ .



**Fig. 5.** Tampered versions of image Lena

It is observed that the distances  $d$  between the hashes of Lena and the tampered versions of Lena are normally larger than the distances between the original images and content-preserving processed ones. However, the distances decrease with the increase of  $\alpha$ . Note that the randomness is increased with the value of  $\alpha$ , but the capability of the tampering detection is also decreased. From Eq. (8), it can be seen that the new pixel value  $P'_I(x, y)$  is affected by the value of  $\alpha$  and increasing the value of  $\alpha$  will cause a large offset of  $P'_I(x, y)$ . In other words, the new pixel value  $P'_I(x, y)$  will be less influenced by the original pixel value  $P_I(x, y)$  of the original image itself. Therefore, the capability of tampering detection is degraded.

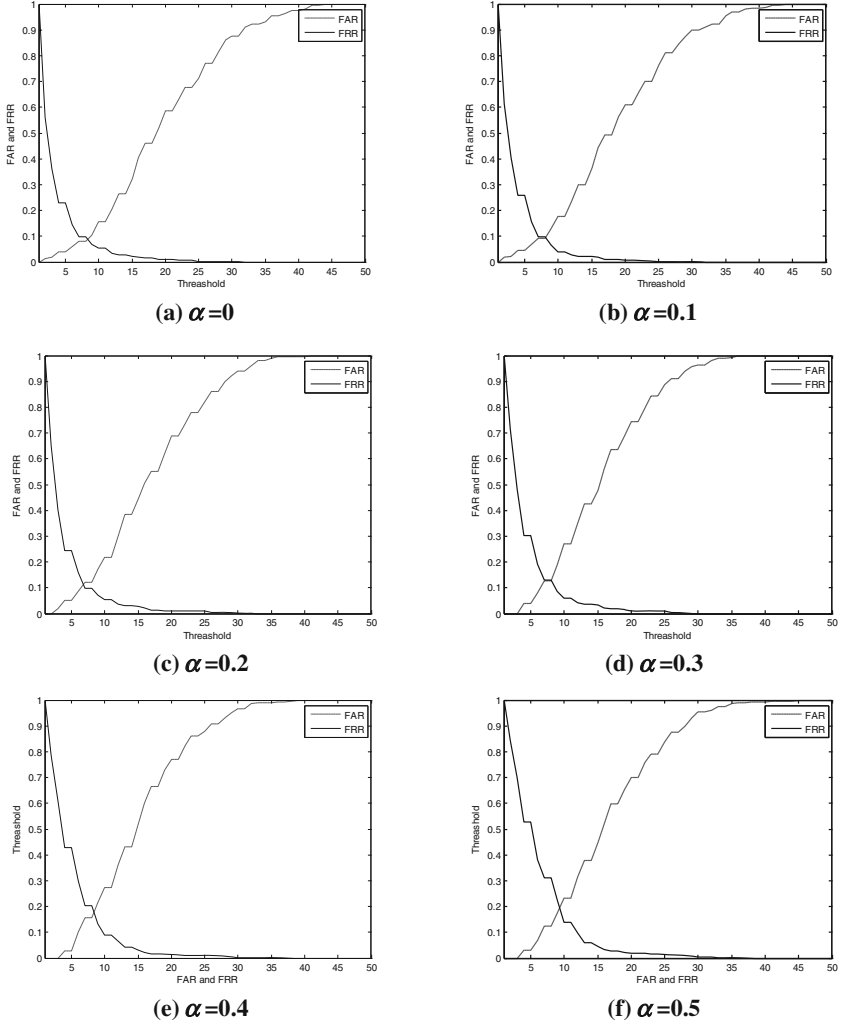
**Table 2.** Normalized Hamming distance against different tamperings

Image		Normalized Hamming Distance $d$					
		$\alpha = 0$	$\alpha = 0.1$	$\alpha = 0.2$	$\alpha = 0.3$	$\alpha = 0.4$	$\alpha = 0.5$
Malicious Attack	(a)	0.4058	0.3913	0.3333	0.3478	0.3043	0.2899
	(b)	0.1159	0.1014	0.0870	0.0870	0.0580	0.0580
	(c)	0.0870	0.1014	0.1159	0.0870	0.0725	0.0580
	(d)	0.1304	0.1594	0.1014	0.1304	0.1304	0.1449
	(e)	0.1159	0.1449	0.1159	0.1014	0.0870	0.0870
	(f)	0.1449	0.1304	0.1014	0.1014	0.1159	0.1449
	(g)	0.3043	0.3043	0.2464	0.1884	0.1739	0.1449
	(h)	0.1449	0.1304	0.0725	0.0725	0.0580	0.0725
	(i)	0.1739	0.1594	0.1739	0.1449	0.1159	0.1014

It is noteworthy that the threshold  $\vartheta$  is a tradeoff to evaluate the robustness and capability of the tampering detection. By comparing Tables 1 and 2, it can also be observed that when the value of  $\vartheta$  decreases, the capability to detect the malicious tampering will be increased, but the sensitivity of content-preserving operations becomes relatively higher.  $\vartheta = 0.1$  is found to be an optimal value to discriminate the content-preserving and content-altering attacks. Taking all criteria into consideration, we come to the conclusion that if  $\alpha$  and  $\vartheta$  are chosen as 0.1 and 0.1 respectively, the proposed algorithm is robust to most common image processing manipulations as shown in Table 1 and also able to detect all malicious tampered images as shown in Fig. 5. In addition, the security of the proposed scheme has also been guaranteed.

### 4.3 FAR versus FRR Curve

In this section, the false acceptance rate and the false rejection rate are calculated to evaluate the global performance of image hashing comprehensively in statistical analysis. The false acceptance rate (FAR) is the probability when the content altered images are identified as the genuine ones, which obtain the authentication. And the false rejection rate (FRR) is the probability when the genuine images are detected as the tampered ones, which cannot obtain the authentication. Determining whether or not the image is authentic is based on normalized Hamming distance. Hence, the distributions of FAR versus FRR can be obtained by varying the value of threshold under different value of  $\alpha$ , which are shown in Fig. 6. From Fig. 6, it is expected that the lower the equal error rate, the better the performance, and the scheme performs better when  $\alpha$  is smaller. However, it is a tradeoff among robustness, fragility and security. When we consider the security, which is the degree to which an image hashing scheme prevents the attacker from tricking the authentication system with a maliciously modified image,  $\alpha = 0.1$  is the optimal compromise in this scheme, while shows almost the same performance when RMP is not used. These experimental results show that the proposed scheme gives a comparable low equal error rate and performs well in both aspects of robustness and fragility in perceptual image hashing authentication.



**Fig. 6.** The distributions of FAR versus FRR under different value of  $\alpha$

## 5 Conclusion

In this paper, we have proposed a perceptual hashing scheme based on wave atom transform and randomized pixel modulation, which is appropriate for image content authentication, image database retrieval and so forth. The proposed algorithm can authenticate the images which have undergone common content preserved image processing operations conducted on Stirmark benchmark, such as compression, filtering, noise addition, affine transformation and also the geometric manipulation. It is simultaneously sensitive to malicious tampering with the guaranty of system security. Instead of using traditional transform like DWT, DCT or other transform, we propose



to employ wave atom transform for the sparser expansion and better characteristics to extract texture features when compared with others. The comparison results also show that the proposed scheme achieves better performance than the schemes proposed by Guo et al. [29], Seo et al. [12] and Venkatean et al. [3] even in the aspect of robustness.

## References

1. Schneier, B.: *Applied Cryptography*. John Wiley & Sons Inc, USA (1996)
2. Bhattacharjee, S., Kutter, M.: Compression tolerant image authentication. In: *Proceedings of International Conference on Image Processing*, vol. 4(7), pp. 435–438, Chicago, USA (1998)
3. Venkatesan, R., Koon, S.M., Jakubowski, M.H., Moulin, P.: Robust image hashing. In: *Proceedings of IEEE International Conference Image Processing*, vol. 3, pp. 664–666, Vancouver, BC, Canada (2000)
4. Lu, C.S., Liao, H.Y.M.: Structural digital signature for image authentication. *IEEE Trans. Multimedia* **5**, 161–173 (2003)
5. Monga, V., Evans, B.L.: Robust perceptual image hashing using feature points. *IEEE Int. Conf. Image Process.* **1**, 677–680 (2004)
6. Monga, V., Evans, B.L.: Perceptual image hashing via feature points: performance evaluation and tradeoffs. *IEEE Trans. Image Process.* **15**(11), 3452–3465 (2006)
7. Ahmed, F., Siyal, M.Y., Vali, U.A.: A secure and robust hash-based scheme for image authentication. *Signal Process.* **90**(5), 1456–1470 (2010)
8. Fridrich, J., Goljan, M.: Robust hash functions for digital watermarking. In: *Proceedings of IEEE International Conference Information Technology: Coding and Computing*, pp. 178–183 (2000)
9. Lin, C.Y., Chang, S.F.: A robust image authentication system distinguishing JPEG compression from malicious manipulation. *IEEE Trans. Circuits Syst. Video Technol.* **11**(2), 153–168 (2001)
10. Lefebvre, F., Macq, B., Legat, J.D.: RASH: Radon soft hash algorithm. In: *Proceedings of European Signal Processing Conference*, pp. 299–302 (2002)
11. Roover, C.D., Vleeschouwer, C.D., Lefebvre, F., Macq, B.: Robust video hashing based on radial projections of key frames. *IEEE Trans. Signal Process.* **53**(10), 4020–4036 (2005)
12. Seo, J.S., Haitisma, J., Kalker, T., Yoo, C.D.: A robust image fingerprinting system using the rado transform. *Signal Process. Image Commun.* **19**(4), 325–339 (2004)
13. Swaminathan, A., Mao, Y., Wu, M.: Robust and secure image hashing. *IEEE Trans. Inf. Forens. Sec.* **1**(2), 215–230 (2006)
14. Wu, D., Zhou, X., Niu, X.: A novel image hash algorithm resistant to print–scan. *Signal Process.* **89**(12), 2415–2424 (2009)
15. Lei, Y., Wang, Y., Huang, J.: Robust image hash in Radon transform domain for authentication. *Signal Process. Image Commun.* **26**(6), 280–288 (2011)
16. Kozat, S.S., Venkatesan, R., Mihcak, M.K.: Robust perceptual image hashing via matrix invariants. In: *Proceedings of IEEE International Conference on Image Processing*, pp. 3443–3446 (2004)
17. Monga, V., Mihcak, M.K.: Robust and secure image hashing via non-negative matrix factorizations. *IEEE Trans. Inf. Forens. Secur.* **2**(3), 376–390 (2007)
18. Tang, Z., Wang, S., Zhang, X., Wei, W., Su, S.: Robust image hashing for tamper detection using non-negative matrix factorization. *J. Ubiquitous Convergence Technol.* **2**(1), 18–26 (2008)



19. Lv, X., Wang, Z.J.: Perceptual image hashing based on shape contexts and local feature points. *IEEE Trans. Inf. Forensics Secur.* **7**(3), 1081–1093 (2012)
20. Lu, W., Wu, M.: Multimedia forensic hash based on visual words. In: *Proceedings of IEEE Conference Image Processing*, pp. 989–992, Hong Kong (2010)
21. Khelifi, F., Jiang, J.: Perceptual image hashing based on virtual watermark detection. *IEEE Trans. Image Process.* **19**(4), 981–994 (2010)
22. Zhao, Y., Wang, S., Zhang, X., Yao, H.: Robust hashing for image authentication using Zernike moments and local features. *IEEE Trans. Inf. Forensics Secur.* **8**(1), 55–63 (2013)
23. Demanet, L., Ying, L.: Wave atoms and sparsity of oscillatory patterns. *Appl. Comput. Harmonic Anal.* **23**(3), 368–387 (2007)
24. Liu, F., Cheng, L.-M.: Perceptual image hashing via wave atom transform. In: Shi, Y.Q., Kim, H.-J., Perez-Gonzalez, F. (eds.) *IWDW 2011. LNCS*, vol. 7128, pp. 468–478. Springer, Heidelberg (2012)
25. Mallat, S.: *A Wavelet Tour of Signal Processing*, 2nd edn. Academic Press, Orlando/San Diego (1999)
26. Antoine, J.P., Murenzi, R.: Two-dimensional directional wavelets and the scale-angle representation. *Signal Process.* **52**, 259–281 (1996)
27. Reddy, B.S., Chatterji, B.N.: An FFT-based technique for translation, rotation, and scale-invariant image registration. *IEEE Trans. Image Process.* **5**, 1266–1271 (1996)
28. Fair evaluation procedures for watermarking systems (2000). <http://www.petitcolas.net/fabien/watermarking/stirmark>
29. Guo, X.C., Hatzinakos, D.: Content based image hashing via wavelet and radon transform. In: Ip, H.H.-S., Au, O.C., Leung, H., Sun, M.-T., Ma, W.-Y., Hu, S.-M. (eds.) *PCM 2007. LNCS*, vol. 4810, pp. 755–764. Springer, Heidelberg (2007)

Transactions on Data Hiding and Multimedia Security X

Shi, Y.Q. (Ed.)

2015, IX, 107 p. 43 illus., Softcover

ISBN: 978-3-662-46738-1