Content-based image hashing using wave atoms

Liu Fang(刘 芳)[a)†], Leung Hon-Yin(梁瀚贤)[a)],
Cheng Lee-Ming(郑利明)[a)], and Ji Xiao-Yong(季晓勇)[b)]

[a)] *Department of Electronic Engineering, City University of Hong Kong, Hong Kong SAR, China*
[b)] *School of Electronic Science and Engineering, Nanjing University, Nanjing* 210093, *China*

(Received 2 June 2011; revised manuscript received 1 November 2011)

It is well known that robustness, fragility, and security are three important criteria of image hashing; however how to build a system that can strongly meet these three criteria is still a challenge. In this paper, a content-based image hashing scheme using wave atoms is proposed, which satisfies the above criteria. Compared with traditional transforms like wavelet transform and discrete cosine transform (DCT), wave atom transform is adopted for the sparser expansion and better characteristics of texture feature extraction which shows better performance in both robustness and fragility. In addition, multi-frequency detection is presented to provide an application-defined trade-off. To ensure the security of the proposed approach and its resistance to a chosen-plaintext attack, a randomized pixel modulation based on the Rényi chaotic map is employed, combining with the nonliner wave atom transform. The experimental results reveal that the proposed scheme is robust against content-preserving manipulations and has a good discriminative capability to malicious tampering.

Keywords: image hashing, authentication, wave atom transform, chaotic system

PACS: 02.70.–c, 05.45.Gg, 42.30.Va, 43.60.Hj **DOI:** 10.1088/1674-1056/21/4/040204

1. Introduction

Along with the rapid development of internet and multimedia technologies, digital data is widely being created, replicated, and disseminated. The easy accessibility of digital data gives rise to the enormous growth of manipulation tools. Digital forgery and unauthorized utilization consequently have become more prevalent, which makes the security of data very challenging.

In this situation, hash functions are employed mainly for cryptography authentication. In the traditional way of authenticating digital messages, the hash is calculated using some standard cryptographic hash functions such as MD5 or SHA1 and a digital signature is formed using some public key encryption algorithms like RSA.[1] This kind of cryptographic hash function possesses high key and plaintext sensitivity; even one bit disturbance in the message will lead to significant changes of the hash value. However, it is not suitable for image security applications due to this sensitivity to all image manipulations, even non-malicious ones, such as JPEG compression or filtering.

Recently many content-based image hashing schemes have been proposed, which are invariant to acceptable manipulations and also able to authenticate an image consisting of visually unnoticeable changes, while cryptographic hashing cannot be achieved.[2,3] They have drawn a lot of attention owing to their outstanding performances compared to some signal processing manipulations. The state-of-the-art techniques are mainly classified into four approaches: image statistics based approach,[4–6] relation based approach,[7,8] image feature extraction approach,[9–12] and preservation of coarse image representation approach.[13–15]

The approaches used in Refs. [4]–[6] construct the hashes by selecting the invariant statistics characteristics from images, such as mean, variance, and higher moments of intensity values of image blocks. As a result, great robustness can be obtained. In relation based schemes,[7,8] the invariant relationships of transformation coefficients are used to generate hash codes. Unfortunately, the scheme is a little sensitive to some perceptually insignificant changes. Approaches based on image feature extraction[9–12] usually extract hash features by detecting the salient image feature points, and possess good robustness. Approaches based on preservation of coarse image representation extract hash features using the coarse information about the whole image, such as the coefficients of low frequency

†Corresponding author. E-mail: f.liu@student.cityu.edu.hk
© 2012 Chinese Physical Society and IOP Publishing Ltd

in discrete cosine transform (DCT)[13] and Fourier transform,[14] and also the low-rank decomposition of nonnegative matrix factorization (NMF).[15] These schemes achieve great robustness, and sensitivity to malicious tampering is also considered at the same time.

In this paper, wave atom transform[16] is used to analyse the image characteristics in different scale bands and a novel approach is found to construct a hash that can be robust against content-preserving manipulations while resisting malicious attacks better than traditional ones. Even though there are plenty of image hashing schemes based on wavelet transform, DCT or other transforms, which aim to obtain great robustness by exploring the characteristics of transforms, unfortunately the robustness is pursued at the expense of fragility. In addition, how to construct a good feature extraction scheme which is strong in robustness, fragility, and attack resistance is still a challenging problem. However, it is worthwhile mentioning that wave atom transform is expected to outperform other transforms both in robustness and in fragility, since it has a good characteristic to extract texture features by using few coefficients and it captures the coherence of the pattern along and across the oscillations compared with other transforms. It also shows great performance in image de-noising, which makes the proposed hashing scheme more robust against insignificant modifications.

Wave atoms are a recent addition to the repertoire of mathematical transforms of computational harmonic analysis, 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. Since there have been few studies exploring the potential capability of wave atoms in image hashing, in this paper, motivated by the characteristics of wave atoms, we propose a novel scheme to represent the image information more precisely. Moreover, the Rényi chaotic map is utilized for three-layer protection. It is known that one characteristic of a chaotic system is the sensitivity to initial conditions, which makes the system particularly suitable to serve as the pseudo-random number generator (PRNG) as shown in Refs. [17] and [18], moreover it supports high key sensitivity. The combination of the chaotic map based randomized pixel modulation and the nonlinear wave atom transform can ensure the security of this system. The experimental results demonstrate that the proposed scheme achieves a better trade-off between the robustness and fragility requirements.

The rest of this paper is structured as follows. In Section 2 a brief overview of wave atom transform is given. The details of the proposed scheme are presented in Section 3. The experimental results are shown in Section 4, where multi-frequency detection is also given. Security is analysed in Section 5, and conclusions are drawn in Section 6.

2. Wave atom transform

Introduced by Demanet and Ying,[16] wave atoms are a variant of two-dimensional (2D) wavelet packets, which obey the parabolic scaling law wavelength $\sim$ (diameter)^2. Wave atom transform can adapt to the arbitrary local direction 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 than some other fixed standard representations like Gabor filters, wavelets, and curvelets. Wave atoms interpolate accurately between Gabor atoms[19] and directional wavelets,[20] and the period of oscillation of each wave packet (wavelength) is related to the size of the essential support via parabolic scaling.

2.1. Definition of wave atoms

Function $\varphi_\mu(x)$ is employed to describe the wave atoms with subscript $\mu = (j, \boldsymbol{m}, \boldsymbol{n}) = (j,\, m_1,\, m_2,\, n_1,\, n_2)$ where j, m_1, m_2, n_1, n_2 are all integers. A point (x_μ, ω_μ) is indexed in phase-space as

$$x_\mu = 2^{-j}\boldsymbol{n}, \quad \omega_\mu = \pi 2^j \boldsymbol{m}, \quad C_1 2^j \leq \max_{i=1,2} |m_i| \leq C_2 2^j, \tag{1}$$

where C_1 and C_2 are two positive constants, x_μ is the position vector and the centre of $\varphi_\mu(x)$, ω_μ is the wave vector which determines the centre of both bumps of $\hat{\varphi}_\mu(\omega)$ as $\pm\omega_\mu$.

2.2. One-dimensional discrete wave atom implementation

Wave atoms are constructed from the tensor products of adequately chosen one-dimensional (1D) wave packets in practice. Let $\psi^j_{m,n}(x)$ represent a 1D wave packet, where $j \geq 0$, $m \geq 0$, and $n \in Z$ are centred around $x_{j,n} = 2^{-j}n$ in space and $\pm\omega_{j,m} = \pm\pi 2^j m$

in frequency with $C_1 2^j \leq m \leq C_2 2^j$. The basis function can be defined when combining dyadic scaled and translated versions of $\hat{\psi}_m^0$ in the frequency domain as follows:

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

where $\hat{\psi}_m^0(\omega)$ is defined as

$$\begin{aligned}\psi_m^0(\omega) = {} & \mathrm{e}^{-\mathrm{i}\omega/2}[\mathrm{e}^{\mathrm{i}\alpha_m} g(\varepsilon_m(\omega - \pi(m+1/2))) \\ & + \mathrm{e}^{-\mathrm{i}\alpha_m} g(\varepsilon_{m+1}(\omega + \pi(m+1/2)))] \quad (3)\end{aligned}$$

with $\alpha_m = \frac{\pi}{2}(m+1/2)$, $\varepsilon_m = (-1)^m$ and g being a real-value compactly supported C^∞ bump function such that $\sum_m |\psi_m^0(\omega)|^2 = 1$.

For each wave $w_{j,m,n}$ at scale 2^{-j}, the coefficient $c_{j,m,n}$ can be treated as a decimated convolution. By discretizing the sample u at $x_k = kh$, $h = 1/N$, $k = 1, \ldots, N$, the discrete coefficients $c_{j,m,n}^{\mathrm{D}}$ are computed using a reduced inverse fast Fourier transform (FFT) inside an interval of size $2^{j+1}\pi$, centred about the origin, as

$$\begin{aligned}c_{j,m,n}^{\mathrm{D}} = {} & \sum\nolimits_{k=2\pi(-2^j/2+1:1:2^j/2)} \mathrm{e}^{\mathrm{i}2^{-j}nk} \\ & \times \sum\nolimits_{p\in 2\pi Z} \overline{\hat{\psi}_m^j(k+2^j p)}\hat{u}(k+2^j p). \quad (4)\end{aligned}$$

2.3. Two-dimensional discrete wave atom implementation

By individually taking the products of 1D wave packets, two-dimensional (2D) orthonormal basis functions with four bumps can be formed in the frequency plane. The 2D wave atoms are indexed using $\mu = (j, \boldsymbol{m}, \boldsymbol{n}) = (j, m_1, m_2, n_1, n_2)$ and the basis function is modified as

$$\varphi_\mu^+(x_1, x_2) = \psi_{m1}^j\left(x_1 - 2^{-j}n_1\right)\psi_{m2}^j\left(x_2 - 2^{-j}n_2\right). \quad (5)$$

A dual orthonormal basis can be defined from the "Hilbert-transformed" wavelet packets as

$$\begin{aligned}\varphi_\mu^-(x_1, x_2) = {} & H\psi_{m1}^j\left(x_1 - 2^{-j}n_1\right) \\ & \times H\psi_{m2}^j\left(x_2 - 2^{-j}n_2\right). \quad (6)\end{aligned}$$

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

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

$\varphi_\mu^{(1)}$ and $\varphi_\mu^{(2)}$ are jointly denoted as φ_μ and form the wave atoms frame. The wave atom transform algorithm is based on the apparent generalization of the 1D wrapping strategy to the 2D case. Figures 1(a) and 1(b) show the elements of wave atoms in the spatial domain and the frequency domain, respectively.

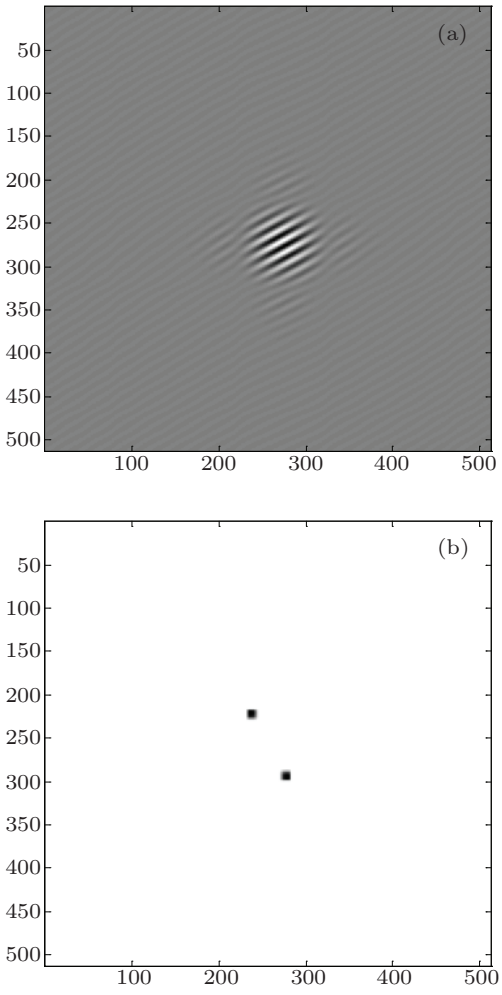


Fig. 1. Elements of wave atoms in (a) the spatial domain and (b) the frequency domain, respectively.

3. Proposed scheme

In this section, a novel wave atom based image hashing scheme is proposed. In order to enhance the security of the proposed scheme, randomized pixel modulation (RPM)[21] is used with the wave atom transform. To ensure randomization and key sensitivity, a chaotic map is employed instead of the original RC4 algorithm. The details of the proposed method are shown below.

3.1. Hash generation

The block diagram of hash generation is shown in Fig. 2. The proposed hash generation scheme is described as follows:

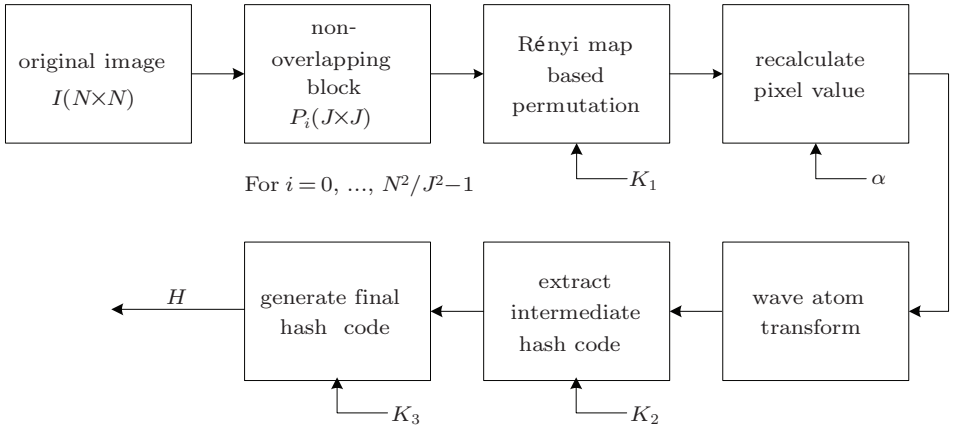


Fig. 2. Hash generation procedure.

Step 1 Suppose that I denotes the input image of size $N \times N$. Divide the image I into a number of non-overlapping blocks, each with dimension $J \times J$. Let P_i denote non-overlapping blocks, where $i = 0, \ldots, N^2/J^2 - 1$. In this implementation, J is set to be 16 and each block is divided into 16×16 pixels.

Step 2 In this step, the Rényi map[22] is employed. Compared with other chaotic maps, the Rényi map shows a remarkable performance in efficiency and security. It can be described as

$$f(x) = (q2^{n-i}x + \lfloor 2^{-j}x \rfloor) \bmod 2^n, \tag{8}$$

where q is an odd positive integer, i, j are selected positive integers, and n is the length of the sequence. This generator can be easily implemented with a multiplier, an adder and two bit-shift operations. In this scheme, the secret key K_1 is used as the initial value x serving as the seed for this PRNG.

Let $P_i(x, y)$ represent the gray value of a pixel in spatial domain (x, y) corresponding to the block P_i, and S_i represents the 1D sequence of $P_i(x, y)$. Denote p_i as the permutation sequence obtained from sorting the $J \times J$ bits pseudo-random numbers generated by the Rényi map. The new permutated sequence of each block is governed by the following equation:

$$S'_i(m) = S_i(p(m)), \tag{9}$$

where i is the block index and m is the index of a particular element S_i.

Step 3 In order to make the image hash code sensitive to the secret key, the RPM transform is employed. All the pixels in each block are preprocessed as follows:

$$P'_i(x, y) = P_i(x, y) + \alpha \times S'_i(m), \tag{10}$$

where $0 \le x, y \le J - 1$, and $m = J \times x + y$.

Step 4 Wave atom transform is then applied to the preprocessed image. By performing the wave atom transform described in Section 2, the image is decomposed into five scale bands and figure 3 shows the wave atom tiling of the frequency plane.

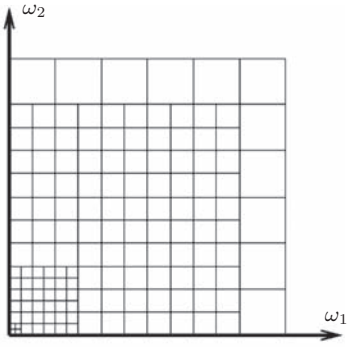


Fig. 3. Wave atom tiling of the frequency plane (only the first quadrant is shown).

For each scale band, there are a number of sub-blocks which consist of a great number of wave atom coefficients. From among these scale bands, the third scale band is selected to compute the hash code, since the coefficients in this scale band will not change greatly unless some content-based modification occurs. Experiments are conducted to investigate the changes of the coefficients in all scale bands under content-preserving and content-modification manipulations. Table 1 shows the statistical percentage of the changed value of coefficients based on 100 gray-scale images of size 512×512. The results show that the coefficients in the third scale band are more robust than high frequency ones, and are more fragile than low frequency ones. Since the energy of wave atom coefficients captures most information about the image features, the intermediate hash is computed by exploring the mutual relationship between these sub-blocks. Such a design can ensure the robustness of this system.

Table 1. The changed percentages of wave atom transform coefficients in various scale bands.

Manipulation	Changed percentage of wave atom transform coefficients				
	Scale band 1	Scale band 2	Scale band 3	Scale band 4	Scale band 5
Content-preserving	1.4012%	4.6825%	35.3513%	161.4571%	893.2834%
Content-modification	85.9983%	174.8729%	197.0968%	185.0298%	845.1677%

Step 5 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 represent the phases. For all non-empty blocks in the third scale band, the energy of the i-th wave atom block E_i is computed by

$$E_i = \sum_{q=1}^{l_2} \sum_{p=1}^{l_1} C(j, m_1, m_2, p, q), \tag{11}$$

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

To make sure that the intermediate hash code does not reveal information about the original mutual relationship of the wave atom blocks, a random permutation governed by the secret key K_2 is applied to E_i using the same method based on the Rényi map. Denote the new sequence as E'_i, and the difference between two new continuous blocks is used to generate one hash bit. Let the total number of non-empty blocks in the third scale band be r. The i-th bit of the intermediate hash h can be expressed as

$$h^{(i)} = \begin{cases} 1, & \text{if } E'_i > E'_{i+1}, \\ 0, & \text{otherwise}, \end{cases} \tag{12}$$

where $i \in [1, \ldots, r-1]$.

Step 6 A pseudo-random sequence generated by the secret key K_3 based on the Rényi map is applied to XOR the intermediate hash h in order to form the final hash H.

3.2. Image authentication

The image authentication module is employed to authenticate the received image I'. By utilizing system parameters N, J, K_1, K_2, K_3, and α, the receiver calculates the hash of the received image and compares it with the hash of original image H. The detailed procedures are described as follows.

Step A The received image goes through the steps as described in Subsection 3.1 to obtain the hash H'.

Step B The normalized hamming distance d between these two hash codes is then computed for authentication. Denote the i-th values of H and H' as $H(i)$ and $H'(i)$ respectively, and L as the length of the image hash, i.e.,

$$d(H, H') = \frac{1}{L} \sum_{i=1}^{L} \delta(H(i), H'(i)), \tag{13}$$

where

$$\delta(H(i), H'(i)) = \begin{cases} 0, & H(i) = H'(i), \\ 1, & H(i) \neq H'(i). \end{cases} \tag{14}$$

Step C Define θ as a discriminative threshold to distinguish whether the received image is authenticated using the following two rules:

(i) $\forall\, I, I'$ if $d(H, H') > \theta$ then $I \neq I'$;

(ii) $\forall\, I, I'$ if $d(H, H') \leq \theta$ then $I \approx I'$.

If d is larger than the threshold, the received image is considered to be a tampered one or even as being a different image. Otherwise the received image will be authenticated.

4. Experimental results

In order to test the proposed scheme, 100 gray-scale images of size 512×512 are used as the original test images, and the total numbers of images for content-preserving manipulations and malicious attacks are 3100 and 10000, respectively. The proposed image hashing algorithm is implemented in MATLAB on a personal computer with an Intel(R) Core(TM) i7 (2.80 GHz) CPU (DDR 4 G).

4.1. Robustness against content-preserving manipulation

Robustness is a measure of the degree to which an image hashing scheme is invariant to perceptually identical images. In this subsection, some common signal processing manipulations which do not change the content of the image significantly are used to verify the robustness. The normalized hamming distance d is used for authenticating which is supposed to approach to zero for similar images and approach to 0.5 for disparate ones. Table 2 shows the average normalized hamming distance of 100 original images under certain manipulations based on different values of α.

Table 2. Average normalized hamming distances under different content-preserving manipulations.

Image	System parameter	Normalized hamming distance			
		$\alpha = 0$	$\alpha = 0.5$	$\alpha = 1$	$\alpha = 1.5$
JPEG (quality factor)	5	0.0648	0.0642	0.0746	0.0812
	15	0.0225	0.0261	0.0297	0.0361
	25	0.0148	0.0157	0.0199	0.0264
	50	0.0074	0.0074	0.0106	0.0149
	85	0.0028	0.0028	0.0049	0.0061
Gaussian noise (standard variance)	5	0.0094	0.0101	0.0104	0.0159
	10	0.0114	0.0174	0.0225	0.0270
	15	0.0245	0.0268	0.0310	0.0414
	20	0.0323	0.0383	0.0433	0.0578
Salt and pepper noises addition (noise density)	0.02	0.0364	0.371	0.0420	0.0399
	0.04	0.0417	0.0503	0.0535	0.0581
	0.06	0.0558	0.0545	0.0690	0.0712
	0.08	0.0651	0.0712	0.0801	0.0787
Gaussian low pass filtering (standard variance, window)	0.5,3	0.0114	0.0667	0.1343	0.1846
	0.5,5	0.0117	0.0667	0.1346	0.1846
	1.5,3	0.0338	0.0790	0.1409	0.1875
	1.5,5	0.0517	0.0916	0.1491	0.1916
Median filtering (filter size)	3×3	0.0228	0.0270	0.0293	0.0303
	5×5	0.0410	0.0468	0.0446	0.0500
	7×7	0.0620	0.0674	0.0593	0.0638
	9×9	0.0871	0.0861	0.0781	0.0819
Contrast change	10%	0.0049	0.0100	0.0048	0.0117
	20%	0.0174	0.0220	0.0159	0.0314
	–10%	0.0012	0.0091	0.0010	0.0132
	–20%	0.0013	0.0164	0.0019	0.0313
Laplacian sharpening (operator)	0.2	0.0058	0.0709	0.1400	0.1913
	0.4	0.0058	0.0697	0.1390	0.1910
Rotation	5°	0.2857	0.3119	0.3316	0.3478
	10°	0.4333	0.4255	0.4343	0.4333
	15°	0.4817	0.4846	0.4801	0.4832
	20°	0.4977	0.4972	0.4972	0.4980

From Table 2, it can be observed that the values of d between the hash of the original image and the hash of the processed image are small for all cases, except the rotation manipulations. Since rotation manipulations destroy the correlation of the wave atoms, the wave atom coefficients after such a manipulation will be changed greatly, which leads to a large hamming distance. Note that the parameter α in Eq. (10) is used to enhance the security of the hash such that d depends on both image pixels and the secret key. This RPM transform will destroy the characteristics of the original image, which reduces the robustness of wave atom transform and leads to a larger hamming distance.

Furthermore, some relevant schemes proposed by Guo and Hatzinakos,[23] Seo *et al.*[24] and Venkatesan *et al.*[5] have been compared with the proposed scheme in the robustness test. Guo and Hatzinakos

proposed a content based image hashing scheme via wavelet and Radon transform, while Seo's scheme and Venkatean's scheme are based only on Radon transform and wavelet transform, respectively. Figure 4 shows the performances of these image hashing schemes in terms of the normalized hamming distances.

As shown in Fig. 4(a), the performance of robustness in our proposed scheme is better than those of the schemes given by Guo *et al.* and Seo *et al.*, while a little worse than Venkatean's one under JPEG compression. With the increase of Gaussian noise strength in Fig. 4(b), the proposed scheme always performs the best among all the methods, due to the capability of wave atom transform in image de-noising. Considering the effect of Gaussian filtering and contrast change manipulations, the performance of our proposed method is also better than those of other three where the normalized hamming distances are all below 0.02, while in other schemes, the normalized hamming distance is above the threshold of 0.1 in some cases. The comparison results reveal that the proposed scheme is superior to the schemes proposed by Guo *et al.*, Seo *et al.*, and Venkatean *et al.* The use of the third scale band of wave atom transform enables the proposed approach to extract invariant features from the image which shows great robustness against common image processing manipulations.

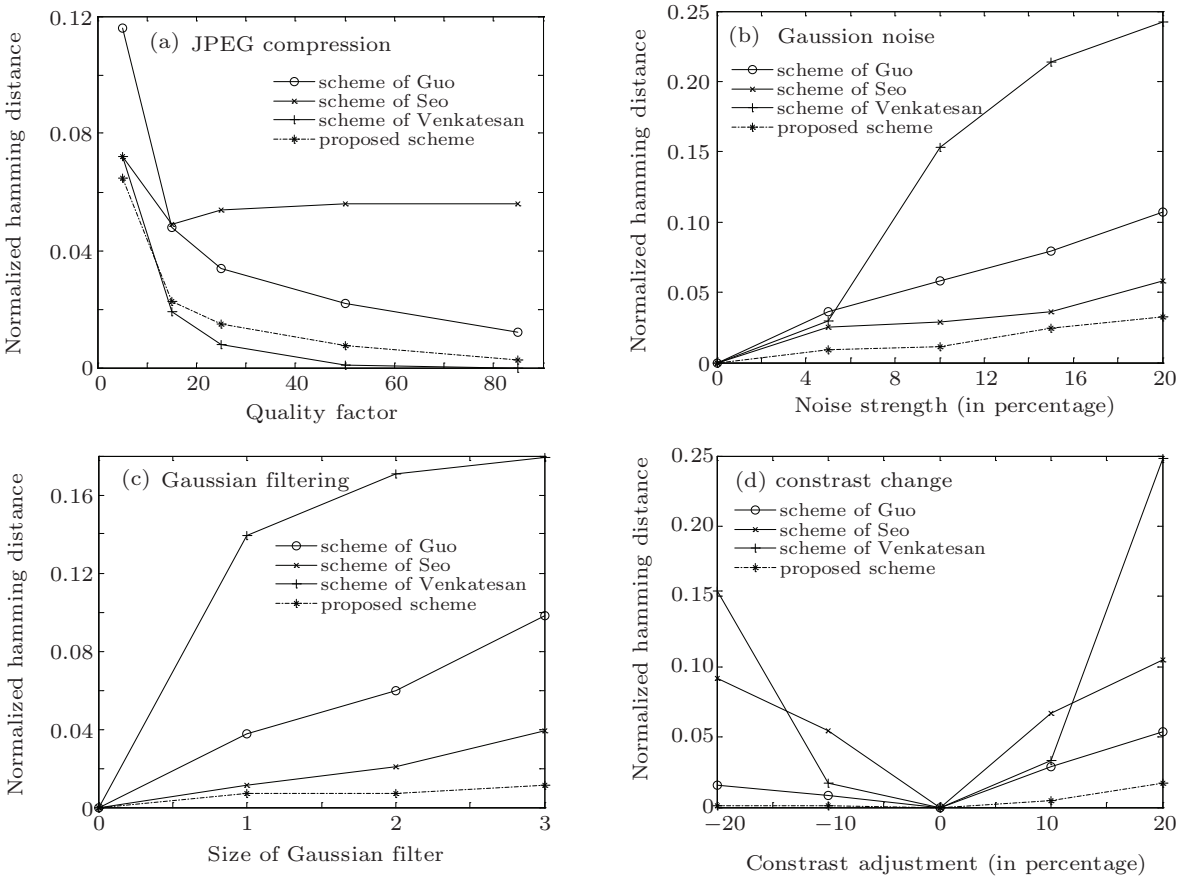


Fig. 4. Comparison of robustness among different schemes. (a) Effect of JPEG compression, (b) effect of Gaussian noise, (c) effect of Gaussian filtering, and (d) effect of contrast change.

4.2. Fragility against malicious attacks

Unlike some traditional schemes in which only robustness is considered, the scheme proposed in this paper also additionally takes the characteristic of fragility into account. Fragility is the degree to which an image hashing scheme distinguishes the perceptually different images from the original ones. To demonstrate the capability of malicious tamper detection, 10000 attacked images are tested, and only three tampered versions of images are shown in Fig. 5. Table 3 shows the normalized hamming distances between the original images and the tampered versions in Fig. 5 and also the average normalized hamming distances of 10000 test images.



Fig. 5. Examples of tampered images.

Table 3. Normalized hamming distances under different malicious attacks.

Image		Normalized hamming distance			
		$\alpha = 0$	$\alpha = 0.5$	$\alpha = 1$	$\alpha = 1.5$
Malicious attacks	(a)	0.3043	0.3333	0.3188	0.3043
	(b)	0.2319	0.1594	0.2464	0.2609
	(c)	0.3333	0.3768	0.4493	0.4783
	average	0.2429	0.2503	0.2622	0.2816

It is observed from Table 3 that the normalized hamming distance d values between the hash of original images and the hash of tampered versions are normally larger than the distances between the hash of original images and the hash of non-maliciously processed ones. The average normalized hamming distances of the 10000 attacked images are 0.2429, 0.2503, 0.2622, and 0.2816, respectively, when the values of α are equal to 0, 0.5, 1, and 1.5.

The threshold θ is a trade-off between the robustness and the fragility; the increase of θ will increase the robustness of the proposed algorithm while reducing the fragility to malicious tampering. Moreover, the increased value of α will reduce the robustness performance but increase the system security. The receiver operation characteristic (ROC) curve is employed as a fair way to evaluate both the robustness and the fragility. The ROC curve is used to demonstrate the receiver's performance by classifying the received image into one of the two hypotheses which are described as follows:

i) H_1: image is authentic;

ii) H_2: image is unauthentic.

The false acceptance rate (FAR) is the probability that hypothesis H_2 is accepted when H_1 is true; while the false rejection rate (FRR) is the probability that hypothesis H_1 is accepted when H_2 is true. ROC curve is a plot of the probability of detection 1-FAR for the false alarm probability FRR as threshold θ is varied. In this experiment, over ten thousand images are used to obtain the ROC curve as shown in Fig. 6.

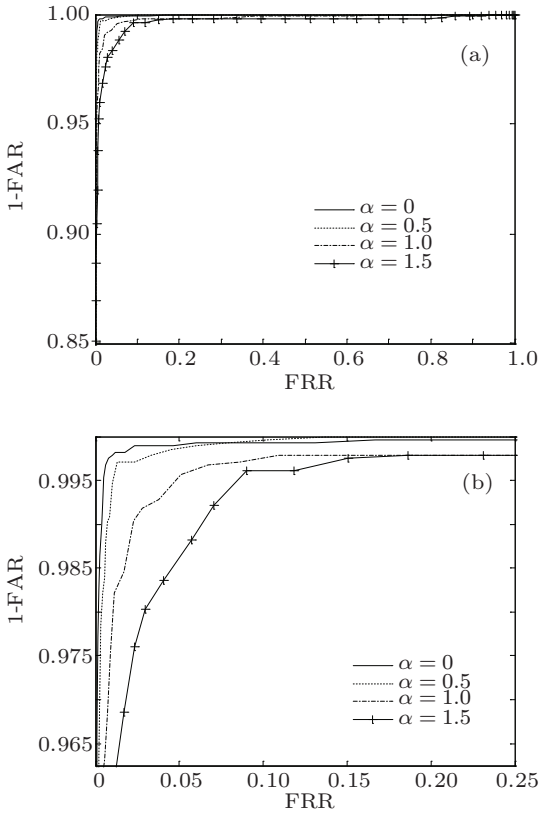


Fig. 6. ROC curves of different values of α: (a) the original curve and (b) the magnified version.

From Fig. 6, it can be observed that a very high acceptance rate is obtained at a fairly low false rejection rate. Note that the randomness in the image is increased with the value of α, and the characteristics

of the image itself are destroyed more seriously. The randomized image represented by wave atom transform is not so good as its original one in the sense of effectiveness because of the destroyed characteristics of image itself, and the coefficients cannot reflect the malicious changes of image so well from the non-malicious processed one either. Hence, the boundary of the hamming distance between the malicious attacks and the non-malicious manipulations is fuzzier with the increased α. It can also be noticed in Fig. 6 that the scheme obtains the best results when RPM is not employed. However the security of the system will be weakened. Fortunately, the performance of the ROC curve is still excellent when α is chosen as 0.5, though the performance is a little worse than the one when α is equal to 0. By considering the image hashing criteria, the optimal trade-off needs to be made when α and θ are chosen as 0.5 and 0.1 respectively, and the proposed algorithm is robust against common signal processing manipulations but fragile to the maliciously tampered images. In addition, the security of the proposed scheme is also guaranteed.

4.3. Multi-frequency detection

It is well known that image hashing schemes can be adopted in many applications including image authentication, content-based retrieval from databases, image and video watermarking, anti-piracy searches, and so forth. Different situations may need different performance trade-offs between the robustness and fragility. To meet the stricter demand and improve accuracy, multi-frequency detection is proposed in this paper, which increases the capability of fragility and further prevents hash collisions. According to the user's demand, which is actually an application-defined trade-off, the images will be chosen whether they undergo the detection based on the normalized hamming distance d calculated in Section 3.2 or not. In this paper, the image is chosen to process the detection when $d \in [0.05, 0.1]$ or $d = 0$.

The new detection is based on the fact that the coefficients in the second scale band are robust against content-preserving manipulations but fragile to content-modification manipulations. The detection scheme goes through the steps as described in Subsection 3.1, with the exception of Step 5. Instead of using the mutual relationship between sub-blocks, a 4-bit quantization is used to quantize the energy of sub-blocks for better fragility in Step 5. The experimental results show that the parameter d which is below 0.1 under malicious tampered attacks in the original proposed scheme increases to 0.2500 on average, while the parameter d which is above 0.05 under JEPG compression, Gaussian noise, and salt and pepper addition noise manipulations in the original proposed scheme becomes 0.0201 on average and 0.1344 under other non-malicious attacks. And the probability of hash collision decreases to $1/2^{(69+24)}$. Figure 7 shows the normalized hamming distance of 500 different images. It can be observed that the distance between hashes of different images is around 0.5, and the collision does not exist in this experiment. Hence, the multi-frequency detection achieves better performance on tamper detection and collision prevention.

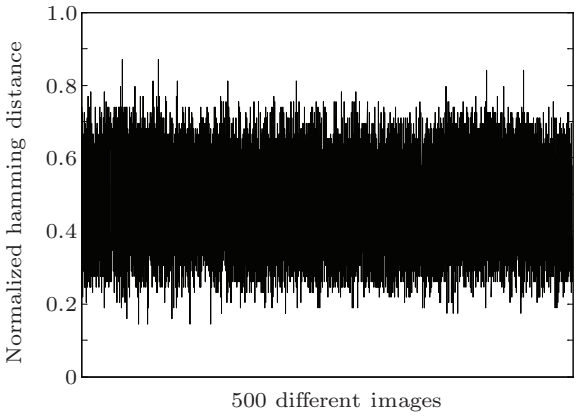


Fig. 7. Normalized hamming distance of 500 different images.

5. Security analysis

In order to evaluate the practicality of the proposed approach, the following security aspects are discussed.

5.1. Key complexity of the Rényi map

In this scheme, a 32-bit PRNG which combines two dynamical systems is employed based on the Rényi map. The secret key is used as the initial value of the 32-bit seed for the combined PRNG, where the parameters of each system are chosen as $n = 15$, $i = 14$, $q = 623$, and $n = 17$, $i = 15$, $q = 5599$, respectively. Since $2^{17}-1$ and $2^{15}-1$ are relatively prime, the combined generator has a period length of $\approx 2^{32}$ bits. And it has been validated that the generated pseudo-random sequence has passed all the NIST SP800-22

standard suite tests and has a maximum period.[22] The advantage of employing the combined PRNG is the possibility of achieving a global period equal to the product of the periods of the single systems, which can enlarge the key space and further ensure the security of the approach.

5.2. Three-layer combined protection

In the proposed scheme, the utilization of RPM governed by the secret keys J, α, and K_1, changes all the pixels in the original image by using the weighted random permuted pixel values. The nonlinear wave atom transform is then used to obtain the key-dependent coefficients. K_2 is used to randomly permute the obtained block energy, based on which the hash is generated. The final hash is generated by XOR the intermediate hash using the random stream governed by K_3. In this approach, three different Rényi map-based PRNGs governed by secret keys K_1, K_2, and K_3 respectively are employed, and Fig. 8 shows the architecture of the proposed approach, which is a three-layer system. Since all the secret keys are independent of each other, the whole complexity of this system is equal to 96-bit. To launch a brute force attack, an adversary must try all possibilities.

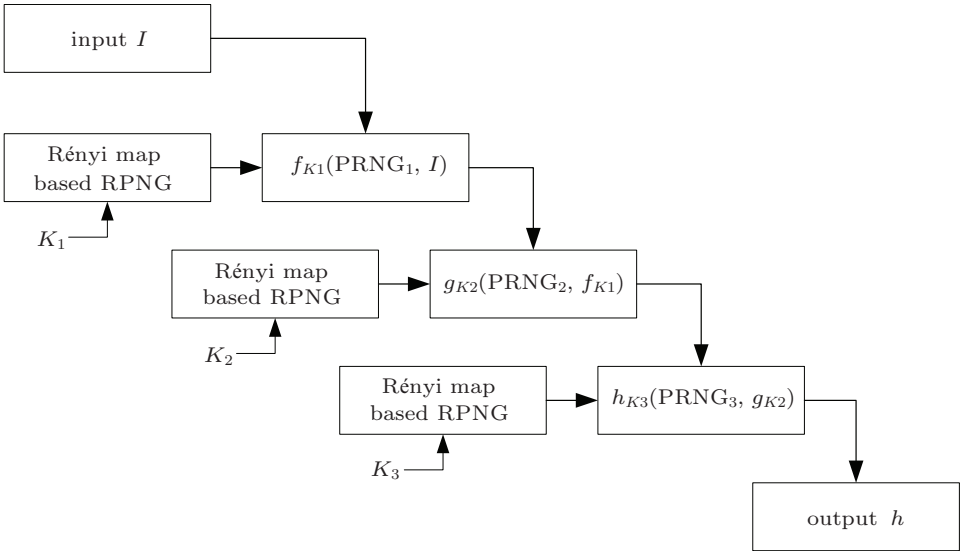


Fig. 8. Architecture of the proposed approach.

5.3. Key sensitivity

It is well known that a chaotic system is sensitive to initial conditions; hence the Rényi map can keep the proposed scheme sensitive to the secret keys. Figure 9 shows the effect of the change in secret keys. It can be observed that the change in the secret keys significantly changes the image hash and results in a large normalized hamming distance, which demonstrates that the proposed scheme has high key sensitivity.

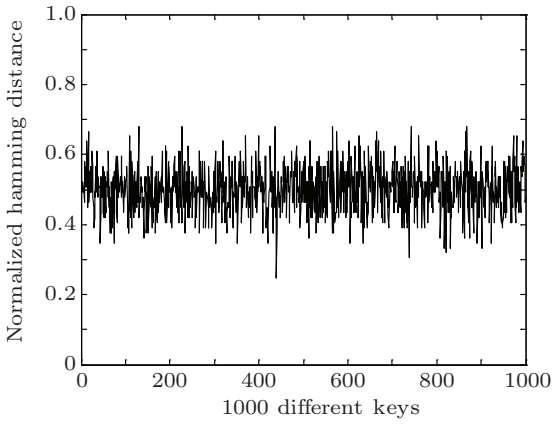


Fig. 9. Effect of the change in secret keys.

5.4. Resistance to chosen-plaintext attack

Note that in a chosen-plaintext attack, the adversary can choose arbitrary images to be encrypted and obtain the corresponding hash code when the proposed scheme is treated as a black box. It is known that the linear permutation-only encryption is not secure enough to prevent the chosen-plaintext attack. Due to the nonlinear effect of the Rényi map-based RPM and wave atom transform, this three-layer system can be referred to a non-deterministic polynomial (NP)-problem. Furthermore, the three-layer system contributes to a space compression after the expansion and lets the scheme own the one-way property. The hash code does not give any clue to the respective image and it is also impossible for the adversary to recover the image. Without knowing the actual parameters employed by the system, the adversary is not able to extract the hash code correctly, or to create a forged image such that the hash of the forged image matches with the hash of the original one.

6. Conclusion

In this paper, a novel image hashing scheme is proposed based on wave atom transform for various applications, including image authentication, watermarking, and database retrieval. Instead of using a traditional transform, wave atom transform is employed due to its sparser expansion and better characteristics of texture feature extraction, which enables the scheme to outperform others both in robustness and in fragility. Furthermore, multi-frequency detection is proposed to make an application-defined tradeoff by increasing the capability of fragility and further preventing hash collisions. The experimental results show that the proposed algorithm is robust against common signal processing such as JPEG compression, low-pass filtering, Gaussian noise, and contrast enhancement. In addition it has a good capability to discriminate malicious tampering. A comparison of results also shows that our proposed algorithm achieves better performance in robustness than the schemes proposed by Guo *et al.*, Seo *et al.* and Venkatean *et al.* In addition, the system security is also guaranteed by combining the Rényi chaotic map-based randomized pixel modulation and the nonlinear wave atom transform. The scheme possesses a high security level and is resistant to chosen-plaintext attack.

References

[1] Schneier B 1996 *Applied Cryptography* (New York: John Wiley & Sons, Inc.)

[2] Monga V, Banerjee A and Evans B L 2006 *IEEE Transaction on Information Forensics and Security* **1** 68

[3] Lamberger M, Pramstaller N, Rechberger C and Rijmen V 2008 *IEEE Transaction on Information Theory* **54** 3647

[4] Schneider M and Chang S F 1996 *Proceeding of IEEE International Conference on Image Processing*, September 16–19, 1996, Lausanne, Switzerland, Vol. 3, p. 227

[5] Venkatesan R, Koon S M, Jakubowski M H and Moulin P 2000 *Proceeding of IEEE International Conference Image Processing*, September 10–13, 2000, Vancouver, BC, Canada, Vol. 3, p. 664

[6] Kailasanathan C, Naini R S and Ogunbona P 2001 *Proceeding of IEEE-EURASIP Workshop on Nonlinear Signal Image Processing*, June 3–6, 2001, Baltimore, MD, USA, doi=10.1.1.15.2556

[7] Lin C Y and Chang S F 2001 *IEEE Transaction on Circuits and Systems for Video Technology* **11** 153

[8] Lu C S and Liao H Y M 2003 *IEEE Transaction on Multimedia* **5** 161

[9] Bhattacharjee S and Kutter M 1998 *Proceeding of IEEE International Conference on Image Processing*, October 4–7, 1998, Chicago, USA, Vol. 1, p. 435

[10] Monga V, Vats D and Evans B L 2005 *Proceeding of IEEE international Conference on Multimedia and Expo*, July 6–8, 2005, Amsterdam, The Netherlands, p. 229

[11] Monga V and Evans B L 2006 *IEEE Transaction on Image Processing* **15** 3452

[12] Khelifi F and Jiang J M 2009 *IEEE Transaction on Image Processing* **19** 981

[13] Fridrich J and Goljan M 2000 *Proceeding of IEEE International Conference on Information Technology: Coding and Computing*, March 27–29, Las Vegas, USA, p. 178

[14] Swaminathan A, Mao Y and Wu M 2006 *IEEE Transaction on Information Forensics and Security* **1** 215

[15] Monga V and Mihcak M K 2007 *IEEE Transaction on Information Forensics and Security* **2** 376

[16] Demanet L and Ying L 2007 *Applied and Computational Harmonic Analysis* **23** 368

[17] Wang F L 2010 *Chin. Phys.* B **19** 090505

[18] Liu S B, Sun J, Xu Z Q and Liu J S 2009 *Chin. Phys.* B **18** 5219

[19] Mallat S 1999 *A Wavelet Tour of Signal Processing* 2nd edn. (Orlando/San Diego: Academic Press)

[20] Antoine J P and Murenzi R 1996 *Signal Processing* **52** 259

[21] Ahmed F, Siyal M Y and Vali U A 2010 *Signal Processing* **90** 1456

[22] Addabbo T, Alioto M, Fort A, Pasini A, Rocchi S and Vignoli V 2007 *IEEE Transactions on Circuit and Systems* I: *Regular Papers* **54** 816

[23] Guo X C and Hatzinakos D 2007 *PCM* **4810** 755

[24] Seo J S, Haitsma J, Kalker T and Yoo C D 2004 *Signal Processing: Image Communication* **19** 325