Multimed Tools Appl (2016) 75:7681–7696
DOI 10.1007/s11042-015-2688-0

Robust image hashing with tampering recovery capability via low-rank and sparse representation

Hong Liu [1,2] · **Di Xiao** [1] · **Yunpeng Xiao** [2] · **Yushu Zhang** [3]

Received: 29 September 2014 / Revised: 22 March 2015 / Accepted: 12 May 2015 /
Published online: 29 May 2015

Abstract Multimedia hash is an effective solution to image authentication and tampering identification. We propose an image hashing scheme based on Low-Rank and Sparse Representation. Low-Rank Representation is applied to the attacked image to obtain image feature matrix and error matrix. Then the properties of dimension reduction and tampering recovery inherent in Low-Rank Representation and Compressive Sensing are exploited for hash design. We use Compressive Sensing to recover the primary feature of image. Furthermore we use Low-Rank Representation to recover the image from tampering. Thanks to the error correction and structure recover capabilities of Low-Rank Representation, experiments reveal that our proposed hashing scheme is robust to content preserving modifications and has better image recovery performance compared with existing hashing schemes.

Keywords Image hashing · Low-rank representation · Compressive sensing · Tampering recovery

1 Introduction

In the information era, multimedia data plays an important role in our daily life. To ensure trustworthiness, multimedia authentication techniques have emerged to verify content integrity and prevent forgery [4, 21].

Various image hash schemes have been proposed in literatures for image authentication. Swaminathan's hashing scheme [19] incorporates pseudo randomization into Fourier-Mellin

✉ Di Xiao
xiaodi_cqu@hotmail.com

[1] Key Laboratory of Dependable Service Computing in Cyber Physical Society (Chongqing University) of Ministry of Education, College of Computer Science, Chongqing University, Chongqing 400044, China

[2] College of Software Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

[3] School of Electronics and Information Engineering, Southwest University, Chongqing 400715, China

transform to achieve better robustness to geometric operations. However, it suffers from some classical signal processing operations such as noising. Kozat proposed to use low-rank matrix approximations obtained via the well-known singular value decomposition (SVD) for image hashing [10]. While the SVD-based hashing scheme exhibits good geometric attack robustness, it does so at the expense of significantly increasing misclassification. Monga introduced nonnegative matrix factorization (NMF) into their hashing algorithm [15]. The NMF hashing possesses excellent robustness under a large class of perceptually insignificant attacks, while it significantly reduces misclassification for perceptually distinct images. Other image hashing schemes [7–9, 14, 17] have also contributed to the development of image hashing.

In recent years, a new theory Compressive Sensing (CS) has been proposed as a more efficient sampling scheme. The theoretical framework of CS was developed by Candes et al. [1] and Donoho [5]. The CS principle claims that a sparse signal can be recovered from a small number of random linear measurements. The CS has been used to design secure digital image encryption schemes [23, 24]. In [23, 24], two new hybrid image compression–encryption algorithms based on compressive sensing are proposed. The proposed algorithms with sensitive keys and nice image compression ability can resist various attacks. From the perspective of image content integrity authentication, it is promising to use CS to generate image hash due to its properties of sensitivity, uniqueness, simple calculation, one-way and a small amount of data. In [20], an image authentication scheme based on CS and distributed source coding (DSC) was proposed, where the image hash is derived from the DSC-encoded quantized random projection coefficients of an image. This scheme has the capability of tampering recovery. In [18], an robust image hashing scheme based on CS and Fourier-Mellin transform was proposed. This scheme yields better identification performances under geometric attacks such as rotation attacks and brightness changes. This scheme does not have the capability of tampering recovery. In [22], we proposed a reversible image authentication scheme based on CS, which has a short hash for image authentication and a long hash for tamper localization and recovery.

In some areas, such as medical or military applications, we not only need to authenticate the image using the image hash, but also need to recover the original image from tampering. The state-of-the-art image hash methods do not have the capability of tampering recovery, except the image hashing scheme [20]. However, the CS hashing scheme [20] has not shown strong ability to distinguish content-preserving operations from tampering. In the situation of the tampering introduced in the image does not have a sparse representation in any basis, image hashing scheme [20] has limited tampering recovery performance. In order to solve these two problems, we proposed the LRRCS hashing method.

The state-of-the-art image hash methods do not consider the problem of robust feature extraction from manipulations. Our proposed hashing scheme is based on the robust feature extraction capability of LRR, which can recover subspace structures from corruptions and errors. We use LRR to extract the primary feature of images in the cases of manipulations. Then we use CS to recover primary feature. At last we use LRR to recover the image from tampering. Experiments reveal that our hashing scheme is robust to content preserving modifications and has better image recovery performance compared with existing hashing schemes.

The rest of this paper is organized as follows. We first introduce the theoretical background of Low-Rank Representation and Compressive Sensing in Section 2. We propose the hashing scheme for image authentication and tampering recovery in Section 3. Experimental results are exhibited in Section 4. The conclusion is given in Section 5.

2 Theoretical background

2.1 Low-rank representation

In real applications, our observations are often noisy, or even grossly corrupted, and observations may be missing. In order to recover the low-rank matrix X_0 from the given observation matrix X corrupted by errors E, it is reasonable to consider the following regularized rank minimization problem [11–13]:

$$\begin{aligned} &\min_{Z,E} \ \|Z\|_* + \lambda\|E\|_{2,1}, \\ &s.t. \ X = XZ + E, \end{aligned} \tag{1}$$

where $\|E\|_{2,1} = \sum_{j=1}^{n}\sqrt{\sum_{i=1}^{n}\left([E]_{ij}\right)^2}$ is called as the $l_{2,1}$ -norm, and the parameter $\lambda>0$ is used to balance the effects of the two parts, which could be chosen according to properties of the two norms, or tuned empirically. After obtaining an optimal solution (Z^*,E^*), we could recover the original data by using $X-E^*$ (or XZ^*). In order to solve Problem (1), we convert it to the following equivalent problem:

$$\begin{aligned} &\min_{Z,E,J} \ \|J\|_* + \lambda\|E\|_{2,1}, \\ &s.t., \ X = XZ + E, \\ &\qquad\quad Z = J, \end{aligned} \tag{2}$$

which can be solved by solving the following Augmented Lagrange Multiplier (ALM) problem:

$$\begin{aligned} &\min_{Z,E,J,Y_1,Y_2} \ \|J\|_* + \lambda\|E\|_{2,1} + \\ &tr\left[Y_1^t(X-XZ-E)\right] + tr\left[Y_2^t(Z-J)\right] + \\ &\frac{\mu}{2}\left(\|X-XZ-E\|_F^2 + \|Z-J\|_F^2\right), \end{aligned} \tag{3}$$

where Y_1 and Y_2 are Lagrange multipliers and $\mu>0$ is a penalty parameter. The above problem can by solved by inexact ALM algorithms [11]. Its convergence properties could be proved.

2.2 Compressive sensing

Compressive sensing theory asserts that it is possible to perfectly recover a signal from a limited number of incoherent nonadaptive linear measurements, provided that the signal can be represented by a small number of nonzero coefficients in some basis expansion.

Let $x\in R^n$ denote the signal of interest and $y\in R^m, m<n$, be a number of linear random projections (measurements) obtained as $y=\Phi x$. The measurement matrix must be chosen in such a way that it satisfies a restricted isometry property (RIP) of order k [2], which says that all subsets of k columns taken from Φ are in fact nearly orthogonal or, equivalently, that linear measurements taken with Φ approximately preserve the Euclidean length of k sparse signals. The entries of $\Phi\in R^{m\times n}$, the measurement matrix, can be random samples from a given statistical distribution, e.g., Gaussian or Bernoulli. At first, let us assume that x is k sparse, i.e., there are exactly $k\ll n$ nonzero components. The goal is to reconstruct x given the measurements y and the knowledge that x is sparse. The recent results of compressive sensing have shown that, if x is sufficiently sparse, an approximation of it can be recovered by solving

the following minimization problem:

$$\min\|x\|_1 \ \text{ s.t. } y = \Phi x \tag{4}$$

which can be immediately translated to a linear program. The solution of (4) is obtained provided that the number of measurements satisfies $m \geq Ck\log(n/k)$, where C is some small positive constant.

These results also hold when the signal is not sparse, but it has a sparse representation in some orthonormal basis. Let $\Psi \in R^{n\times n}$ denote an orthonormal matrix, whose columns are the basis vectors. Let us assume that we can write $x=\Psi\theta$, where θ is k sparse. Given the measurements $y=\Phi x$, the signal can be reconstructed by solving the following problem:

$$\min\|\theta\|_1 \ \text{ s.t. } y = \Phi\Psi\theta \tag{5}$$

For the case of noisy measurements, the signal model can be expressed as $y=\Phi x+z$, where the noise amplitude is assumed to be bounded, i.e., $\|z\|_2 \leq \varepsilon$. An approximation of the signal can be obtained by solving the following problem:

$$\min\|\theta\|_1 \ \text{ s.t. } \|y-\Phi\Psi\theta\|_2 \leq \varepsilon \tag{6}$$

In this work, we adopt the GPSR algorithm [6] to find a solution to (6).

3 Image hashing via low-rank and sparse representation

In this section, we propose an image hashing scheme via Low-Rank and Sparse Representation (LRRCS hashing scheme). It composes of two stages: image hash generation, image authentication and image recovery from tampering.

3.1 Generation of image hash

In the stage of image hash generation, the original image owner generates the image hash and stores it in the image authentication server as follows:

(1) Image Preprocessing. Let the original image X undergo pre-processing, including image re-sizing and color space conversion. Since the luminance plane contains most of the geometric and visually significant information, for a color image we only consider the luminance component.

(2) Apply Low-Rank Representation (LRR) to image X to obtain the low-rank feature matrix Z and error matrix E. The LRR operation to image X is defined in (1) and can be solved via ALM algorithm [11].

$$\begin{aligned} &\min_{Z,E} \|Z\|_* + \lambda\|E\|_{2,1}, \\ &s.t.\ \ X = XZ + E, \end{aligned} \tag{1}$$

where $\|\cdot\|_*$ denotes the matrix nuclear norm (sum of the singular values of a matrix) [11], which is a convex relaxation of the rank function, the parameter $\lambda>0$ is used to balance the effects of the two parts, and $\|\cdot\|_{2,1}$ is the $l_{2,1}$ norm defined as the sum of l_2 norms of the column of matrix E. Through LRR operation, the

image X is decomposed into two parts: the low-rank feature matrix Z and the error matrix E. The purpose of this step is to take the advantage of LRR operation to obtain robust feature Z to generate image hash, other than directly use the raw image X.

(3)Apply Discrete Wavelet Transform to feature matrix Z to get feature vector w. $Z=\Psi w, w\in R^n$. The feature vector w is sparse and satisfied to CS requirement.

(4) Use Compressive Sensing to encrypt and compress the feature vector w. A number of linear random projections $y\in R^m, m<n$ is produced as

$$y = \Phi w \tag{7}$$

The entries of the matrix $\Phi\in R^{m\times n}$ are sampled from a Gaussian distribution, generated using a random seed S.

(5) Post Processing. We quantize the resulting vector y and apply gray coding to obtain the binary hash sequence $H(X)$, which is stored in the authentication server for later on image authentication and tampering recovery.

3.2 Image authentication and image recovery from tampering

Image authentication and Image recovery works as follows:

(1) On the received image X', the image user follows the hash generation steps (1)-(3) in Section 3.1 to obtain the feature vector w'.

(2) Use Compressive Sensing to encrypt and compress the feature vector w'. A number of linear random projections $y'\in R^m, m<n$ are produced as

$$y^{'} = \Phi w^{'} \tag{8}$$

The entries of the matrix $\Phi\in R^{m\times n}$ are sampled from a Gaussian distribution, generated using the same random seed S as the hash generation stage. We quantize the resultant vector y' to obtain a quantized version $\overline{y'}$.

(3) The image user requests the hash $H(X)$ to the authentication server. Upon the received $H(X)$, gray decoding is applied and a quantized version $\overline{y}$ is obtained.

(4) Image authentication. An estimate of the distortion in terms of the mean square error (MSE) between the original and the received image is computed by

$$MSE\left(X, X^{'}\right)\approx\frac{1}{m}\left\|\overline{y^{'}}-\overline{y}\right\|_2^2=\frac{1}{m}\left\|\Phi\left(w^{'}-w\right)\right\|_2^2 \tag{9}$$

If the actual distortion between the original and the received image is smaller than the maximum distortion threshold expected by the original image owner, the images are declared to be the same and tampering recovery can be provided. Otherwise, the images

are declared to be different.

(5) Image recovery from tampering. We use CS to recover the primary feature vector Z, and then use LRR to recover the tampering. With the knowledge of $\overline{y'}$ and $\overline{y}$, the image user can obtain

$$\Phi\left(w'-w\right) = \overline{y'}-\overline{y} = b \tag{10}$$

Compressive Sensing has shown that if $e'=w'-w$ is sufficiently sparse, an approximation of the tampering $e'=w'-w$ can be recovered by solving the following l_1 minimization problem:

$$\begin{aligned} e' &= \min\left\|\left(w'-w\right)\right\|_1 \\ s.t.\ &\left\|b-\Phi\left(w'-w\right)\right\|_2 \le \varepsilon \end{aligned} \tag{11}$$

If a sparse solution to the problem (11) can be found, the tampering vector $e'=w'-w$ is obtained. Then through inverse wavelet transform, we obtain the primary feature vector

$$Z = \Psi w = \Psi\left(w'-e'\right) \tag{12}$$

At last, the original image and tampering signal can be recovered through LRR operation defined as

$$X = X'Z \tag{13}$$

$$e = X'-X'Z \tag{14}$$

4 Experimental results and discussion

4.1 Robustness of the proposed hashing scheme

To examine the robustness properties, we consider the performance of our proposed hashing scheme to different content preserving manipulations. The manipulations considered are: (a) rotation; (b) cropping; (c) additive noise contamination; (d) Filtering; and (e) JPEG compression. For each image of size 512×512, we generate a hash by computing random projections m=450 and quantize them with a step size Δ=10. The LRR parameter is chosen as λ=0.14. We use hamming distance as the performance metric to measure the robustness against content preserving manipulations defined as

$$HD = \sum_{i=1}^{n} |h_i(s_1)-h_i(s_2)| \tag{15}$$

where $H(s_i)=\{h_1(s_i),h_2(s_i),\ldots,h_n(s_i)\}$ means the corresponding hash vector with length n of the image s_i.

Figure 1a–e plots the hamming distance between the hash vectors of the standard image and each of the five manipulated images, respectively. We observe that the proposed hashing scheme perform very well for these distortions. We further note that the hamming distance between the hashes of the noisy image and the original image is very small. We observe that, except for some rare cases, the values of hamming distance *HD* are less than 200. This indicates that the image hashing scheme is robust against rotation, cropping, additive noise

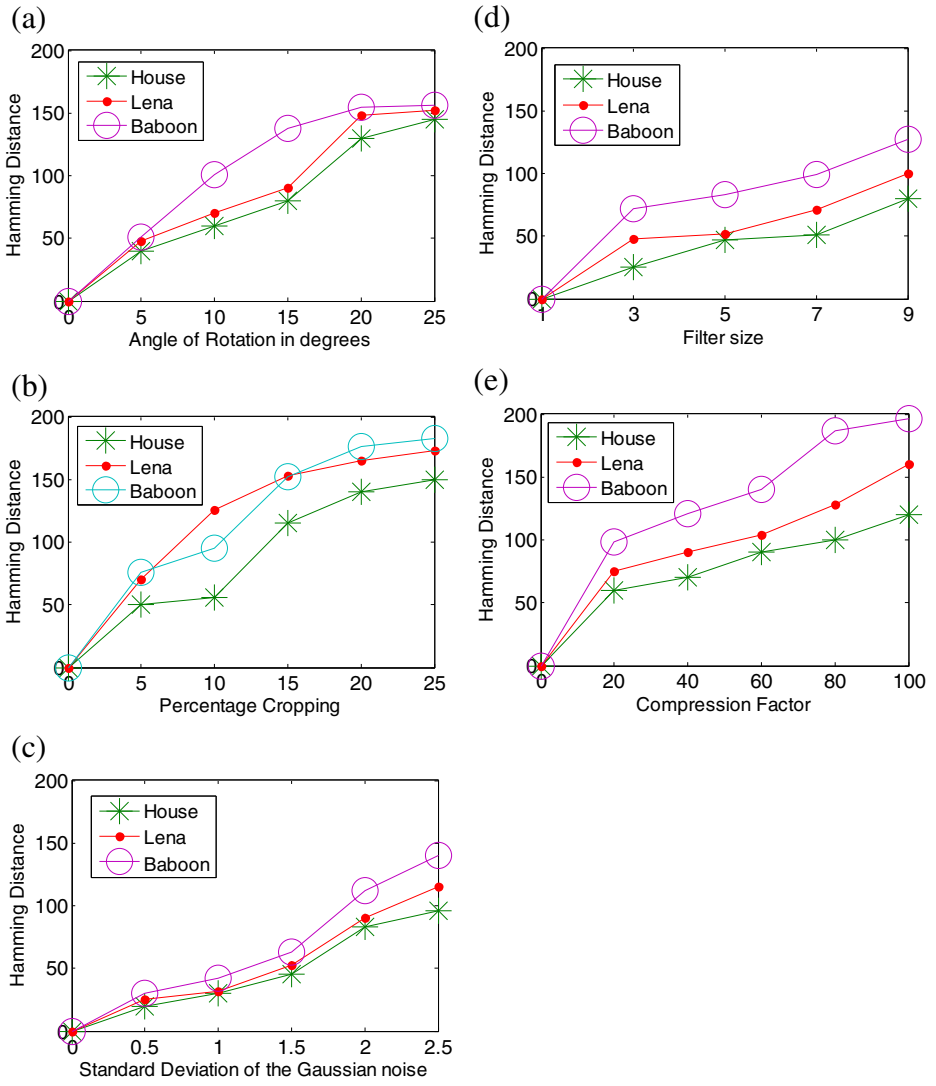

Fig. 1 **a** Hamming distance of the proposed hashing scheme under rotation. **b** Hamming distance of the proposed hashing scheme under cropping. **c** Hamming distance of the proposed hashing scheme under noise. **d** Hamming distance of the proposed hashing scheme under filter. **e** Hamming distance of the proposed hashing scheme under JPEG compression. **a**–**e** Hamming distance of proposed hashing scheme under rotation, cropping, noise, filter and JPEG compression

contamination, filtering and JPEG compression. This illustrates the advantage of taking LRR to obtain robust feature Z, other than directly use the raw image X' to generate image hash.

4.2 Comparison of hash performance

A comparison among the proposed method and [14, 15] and [20] is given in Table 1. The NMF-NMF hash method [15] is based on pseudo-randomly selected subimages, which is changed after rotation so that it is not robust against rotation. The method [15] does not have the ability to locate tampering. The SCH hash method [14] is based on feature points, which is changed after rotation so that it is not robust against rotation. The CS hash method [20] is not robust against rotation and cropping. It is remarkably mentioned that CS [20] and the proposed method have the ability to recover tampering.

We evaluate hash performance in distinguishing manipulation operations from tampering. It is based on experiments on 100 images taken from the original image database, 100 images processed with content-preserving operations, and 100 images from the CASIA tampered image detection evaluation database [3]. The receiver operating curve (ROC) is a plot of the probability of false positive P_{FP} versus the probability of false negative P_{FN} as the threshold is varied. The error probabilities are defined as

$$P_{FP} = \frac{Number \text{ of natural images detected as tampered images}}{Total \text{ number of natural images}} \tag{16}$$

$$P_{FN} = \frac{Number \text{ of tampered images detected as natural images}}{Total \text{ number of tampered images}} \tag{17}$$

Figure 2a–c show the ROC curves of tampering detection under noise, rotation and cropping manipulations. The proposed method has shown stronger ability to distinguish content-preserving operations from tampering than the other three methods [15], [14] and [20]. There is a trade-off between robustness and tamper detection capability. For example, in

Table 1 Comparison of hash performance

	NMF-NMF [15]	CS [20]	SCH [14]	Proposed method
Features used	Local	Global	Shape contexts and feature points	Primary feature
Hash length	64 floating point numbers	450 bytes	320 bits	450 bytes
Robust against noise	Yes	Yes	No	Yes
Robust against rotation	No	No	No	Yes
Robust against cropping	Yes	No	Yes	Yes
Tampering detection	Yes	Yes	Yes	Yes
Tampering location	No	Yes	Yes	Yes
Tampering recovery	No	Yes	No	Yes

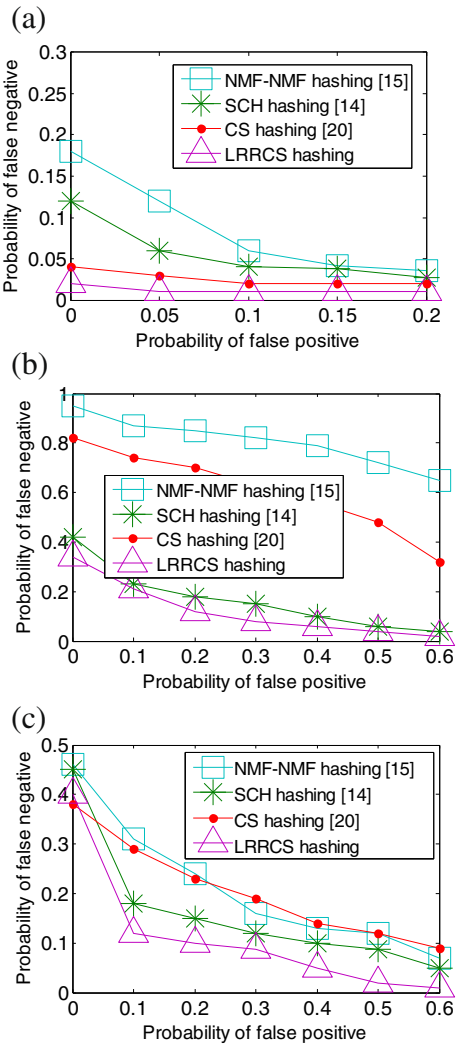

Fig. 2 **a** ROC curves of tampering detection under standard deviation of the Gaussian noise σ=0.5. **b** ROC curves of tampering detection under rotation of 10° angle. **c** ROC curves of tampering detection under cropping of 5 percentage of image. **a**–**c** ROC curves of tampering detection under noise, rotation and cropping manipulations

Fig. 2a the P_{FP} of proposed method is kept at 0.05, while the corresponding P_{FN} is 0.01, which is reasonably low.

4.3 Image recovery from tampering

We evaluate the capability of image recovery from tampering. For each image of size 512× 512, we generates a hash by computing random projections m=450 and quantizes it with a step size Δ=10. The LRR parameter is chosen as λ=0.14.

We adopt the Peak Signal to Noise Ratio (PSNR) to assess the quality of image recovery, which is calculated as

$$PSNR = 10 \times \log_{10}\left(\frac{255^2 \times h \times w}{\sum_{i=0}^{h-1}\sum_{j=0}^{w-1}\left(p_{i,j}-q_{i,j}\right)^2}\right) \tag{18}$$

where h, w are the height and width of the image signal, $p_{i,j}$ and $q_{i,j}$ are the pixel values of the original image signal and recovered image signal.

Figure 3a shows the image recovery performance under the attack of one logo added to the original Lena image (PSNR=27.82 dB). Figure 3b shows the image recovered using the

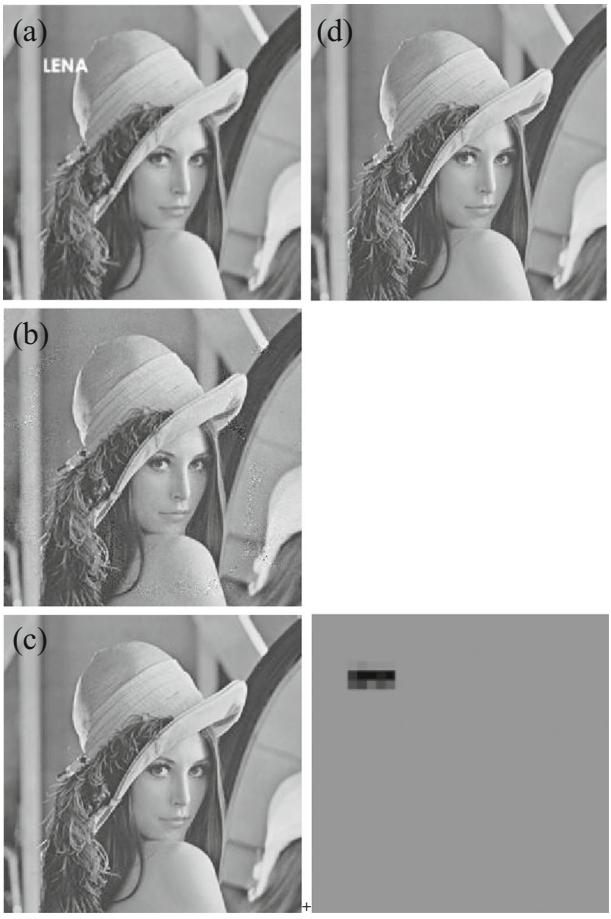

Fig. 3 Image recovery performance under the attack of one logo insertion. **a** Tampered image (27.8 dB). **b** Image recovered using CS hashing [20] (PSNR=32.85 dB). **c** The corrected data ($X'Z'$) and the error (E') after applying LRR to attacked X'. **d** Image recovered using proposed hashing scheme (PSNR=59.47 dB)

scheme of CS hashing [20] (PSNR=32.85 dB). Figure 3c shows the $X'Z'$ and E' through Low-Rank Representation operation to the attacked image X'. Figure 3d shows the image recovered using our proposed LRRCS hashing scheme (PSNR=59.47 dB).

Figure 4 shows the image recovery performances under the attacks of several logos are added to the original Lena image. When more than four logos are added to Lena image, the PSNR becomes much smaller for the scheme of CS hashing [20] (PSNR=22.93 dB). This is because when more logos are added to the image, the sparse of $(X'-X)$ becomes small which influences the recovery performance of Compressive Sensing. However, our proposed scheme adopts Low-Rank Representation operation which separates the errors caused by tampering to E and makes the sparse of feature vector $(Z'-Z)$ little changed during attack, which results in better recovery performance. When more than six logos are added to the image, the recovery performance of LRR decreases, so the PSNR of our proposed scheme becomes small (PSNR=47.35 dB).

Figure 5a shows the image recovery performance under the attack of brightness adjustment to the original Pepper image (PSNR=23.57 dB). Figure 5b shows the image recovered in the Haar domain using the scheme of CS hashing [20] (PSNR=28.94 dB). Figure 5c shows the $X'Z'$ and E' through LRR operation to attacked image X'. Figure 5d shows the image recovered using our proposed scheme (PSNR=48.63 dB).

Figure 6 shows the image recovery performance under the attacks of cropping the original Lena image. The image recovery performance of our proposed hashing scheme is better than the CS hashing scheme [20]. When the percentage of cropping is less than 10 %, the recover performance in CS hashing scheme [20] is good (PSNR=30.76 dB). However, when the percentage of cropping is more than 30 %, the attack becomes not sparse enough, which influences the recover performance of CS hashing scheme [20] (PSNR=20.18 dB). When the percentage of cropping is more than 40 %, the capability of LRR's error correction decreases, which results in PSNR=28.51 dB.

Figure 7 shows the image recovery performance under the attacks of noise contamination to the original Lena image. The CS hashing scheme [20] has very good performance under noise attacks due to CS's capability of recovery from noise

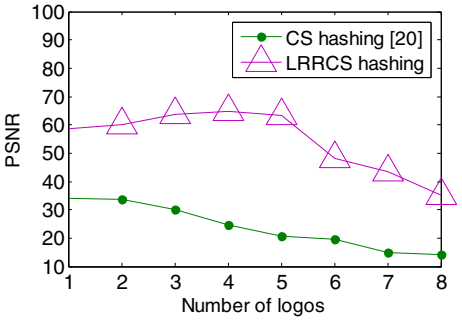

Fig. 4 Image recovery performance under the attacks of logos insertion.

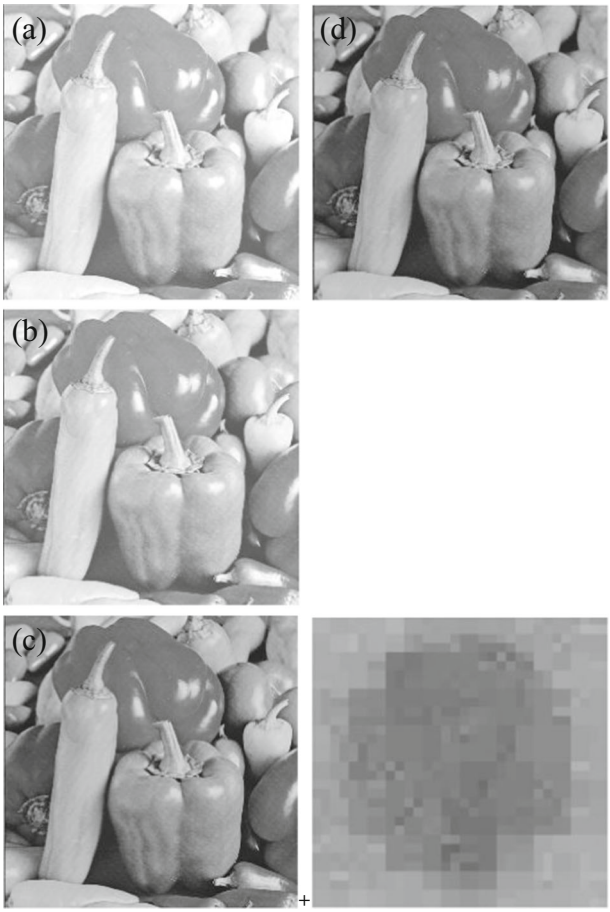

Fig. 5 Image recovery performance under the attack of brightness adjustment. **a** Tampered image (23.5 dB). **b** Image recovered using the CS hashing [20] (PSNR=28.94 dB). **c** The corrected data ($X'Z'$) and the error (E') after applying LRR to attacked X'. **d** Image recovered using proposed hashing scheme (PSNR=48.63 dB)

(PSNR=30.75 dB when the standard deviation of the Gaussian noise is 2). Our proposed hashing scheme has a little better recover performance due to the error

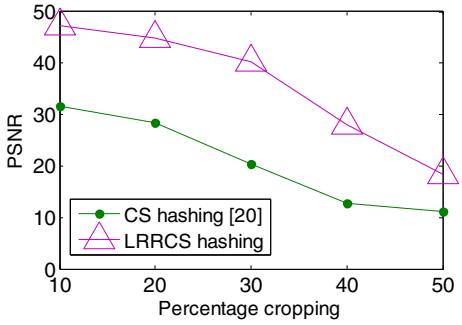

Fig. 6 The image recovery performance under the attacks of cropping to the Lena image

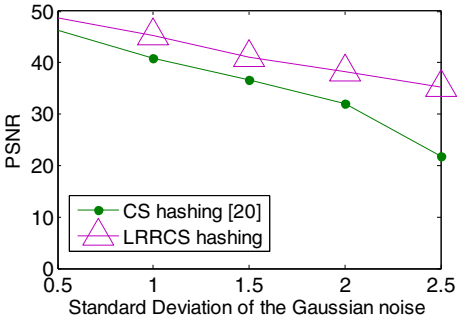

Fig. 7 The image recovery performance under the attacks of noise contamination to the Lena image

correction capability of LRR (PSNR=36.58 dB when the standard deviation of the Gaussian noise is 2).

Figure 8 shows the image recovery performance of our proposed hashing scheme under different JPEG compression factor. It is worth noting that we don not present the CS hashing scheme [20] here, because the JPEG compression introduced in the image does not have a sparse representation in any basis, it can not be recovered by the CS hashing scheme [20].

4.4 Computation complexity and security analysis

4.4.1 Computation complexity

We consider average time consumed in calculating image hashes on a desktop computer with Dual Core 2.6-GHz CPU and 2GB RAM, running Matlab10a. The average time of the proposed method is 5.83 s. The major computation load of our proposed method is in LRR operations to extract the primary feature. When considering the cost time of image recovery, the average time of the proposed method is 10.74 s. The average time of the method of [20] is 1.58 s. The average time of the

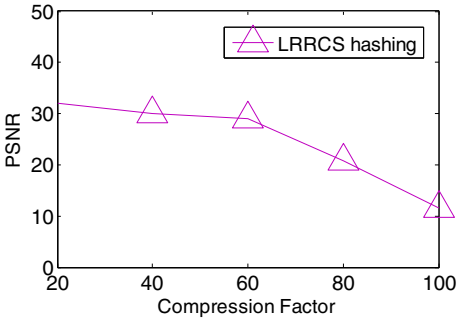

Fig. 8 The image recovery performance under the attacks of JPEG compression

method of [15] and [14] are 1.42 s and 3.96 respectively. Compared with the other three methods, the proposed method needs more time.

4.4.2 Security analysis

Most of the image hashing methods proposed in the literatures, for example [14, 15], use the secret key to randomly select the features. In this paper, we adopt a different approach. Instead of using the secret key to randomly select features, we use the secret key (measurement matrix) to transform the feature space into the Compressive Sensing domain, which increases the entropy of the feature space and increases the security of the hash.

The CS has proven to be computational secure [16]. Without the knowledge of the key, the attacker can not obtain the content of original image. Furthermore, the sensitivity of the secret key on the randomness of the features makes the proposed method have strong security. The little change in the secret key significantly changes the hash. Experiment shows that the hash of Lena image is generated and compared with 100 hashes of the same image generated with 100 randomly generated keys, 98 % of images for different keys are detected as tampered.

We do the anti-collision tests to evaluate the security of the proposed method. If two different images have a hash distance less than a given threshold T, collision occurs. We generate hashes of 100 different images. The threshold T is set to 50. The probability density functions (PDF) of these hash distances are identified as the normal distribution with its mean and standard deviation being μ=120.9 and σ=11.7. Then the collision probability is computed as 6.81×10^{-10}.

5 Conclusion

We propose an image hashing scheme based on Low-Rank and Sparse Representation for image authentication and tampering recovery. Low-Rank Representation is applied to the attacked image to obtain image feature matrix and error matrix. Then we use CS to recover the primary feature and furthermore use LRR to recover the image from tampering. Experiments reveal that our proposed hashing scheme is robust to content preserving manipulations and has better image recovery performance compared with existing hashing schemes.

Acknowledgments The work was supported by Chongqing Youth Innovative Talent Project (Grant No. cstc2013kjrc-qnrc40004), the open research fund of Chongqing Key Laboratory of Emergency Communications (Grant No. CQKLEC, 20140504), Project Nos. 106112013CDJZR180005, 106112014CDJZR185501, XDJK2015C077 supported by the Fundamental Research Funds for the Central Universities, the Natural Science Foundation of Chongqing Science and Technology Commission (Grant Nos. cstc2013jcyjA40017, cstc2013jjB40009) and the National Natural Science Foundation of China (Grant Nos. 61173178, 61272043, 61302161, 61472464).

References

1. Candès E, Romberg J, Tao T (2006) Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information. IEEE Trans Inf Theory 52(2):489–509
2. Candés EJ, Wakin MB (2008) An introduction to compressive sampling: a sensing/sampling paradigm that goes against the common knowledge in data acquisition. IEEE Signal Process 25(2):21–30

3. CASIA-Tampered Image Detection Database, Available online: http://forensics.idealtest.org/
4. Cox IJ, Miller ML, Bloom JA (2001) Digital watermarking. Morgan Kaufmann Publishers Inc., San Francisco
5. Donoho DL (2006) Compressive sensing. IEEE Trans Inf Theory 52:1289–1306
6. Figueiredo MAT, Nowak RD, Wright SJ (2007) Gradient projection for sparse reconstruction: application to compressed sensing and other inverse problems. IEEE J Sel Top Sign Process 1(4):586–597
7. Gerold L, Andreas U (2008) Key-dependent JPEG2000-based robust hashing for secure image authentication. EURASIP J Inf Secur 8(1):1–19
8. Kailasanathan C, Naini RS (2001) Image authentication surviving acceptable modifications using statistical measures and k-mean segmentation. In: Proc IEEE-EURASIP Work. Nonlinear Sig. Image
9. Kailasanathan C, Naini RS, Ogunbona P (2003) Compression tolerant DCT based image hash. In: Proceedings of International Conference on Distributed Computing Systems, pp 562–567
10. Kozat SS, Venkatesan R, Mihcak MK (2004) Robust perceptual image hashing via matrix invariants. In: Proc IEEE Intl Conf Image Process pp 3443–3446
11. Liu G, Lin Z, Yan S, Sun J, Yu Y, Ma Y (2013) Robust recovery of subspace structures by low-rank representation. IEEE Trans Pattern Anal Mach Intell 35:171–184
12. Liu G, Lin Z, Yu Y (2010) Robust subspace segmentation by low-rank representation. International Conference Machine Learning, In, pp 663–670
13. Liu G, Yan S (2012) Active subspace: towards scalable low-rank learning. Neural Comput 24(12):3371–3394
14. Lv XD, Wang ZJ (2012) Perceptual image hashing based on shape contexts and local feature points. IEEE Trans Inf Forensics Secur 7(3):1081–1093
15. Monga V, Mihcak MK (2007) Robust and secure image hashing via non-negative matrix factorizations. IEEE Trans Inf Forensics Secur 2(3):376–390
16. Rachlin Y, Baron D (2008) The secrecy of compressed sensing measurements, In: Proc. 46th Annual Allerton Conf. Comm. Control Comput, pp 813–817
17. Seo JS, Haitsma J, Kalker T, Yoo CD (2004) A robust image fingerprinting system using the radon transform. Signal Process Image Commun 19(4):325–339
18. Sun R, Zeng WJ (2014) Secure and robust image hashing via compressive sensing. Multimed Tools Appl 70: 1651–1665
19. Swaminathan A, Mao YN, Wu M (2006) Robust and secure image hashing. IEEE Trans Inf Forensics Secur 1(2):215–230
20. Tagliasacchi M, Valenzise G, Tubaro S (2009) Hash-based identification of sparse image tampering. IEEE Trans Image Process 18(11):2491–2504
21. Venkatesan R, Koon S-M, Jakubowski MH, Moulin P (2000) Robust image hashing. In: Proceedings IEEE International Conference on Image Processing (ICIP), Vol. 3, pp 664–666
22. Xiao D, Deng MM, Zhu XY (2014) A reversible image authentication scheme based on compressive sensing. Multimed Tools Appl. doi:10.1007/s11042-014-2017-z
23. Zhou NR, Zhang AD, Wu JH, Pei DJ, Yang YX (2014) Novel hybrid image compression-encryption algorithm based on compressive sensing. Optik 125(18):5075–5080
24. Zhou NR, Zhang AD, Zheng F, Gong LH (2014) Image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing. Opt Laser Technol 62:152–160

Hong Liu received the Master's degree in Communication Engineering from University of Electronic Science and technology of China, Chengdu, China in 2006. From 2006 to 2014, she is a lecturer at College of Software

Engineering, Chongqing University of Posts and Telecommunications, China. Currently, she is pursuing her Ph. D. degree from College of Computer Science, Chongqing University, China. Her research interests include image security, compressive sensing, etc.

Di Xiao received the Ph. D. degree in Computer Software and Theory from Chongqing University, Chongqing, China in 2005. Form 2006 to 2008, he has done postdoctoral research at Chongqing University. From 2008 to 2009, he has been a visiting scholar funded by the Chinese government at the Department of Computer Science, New Jersey Institute of Technology, USA. At present, he is a professor at College of Computer Science, Chongqing University, China. His research interests include image processing, compressive sensing, chaos based cryptography, image and graphics watermarking, etc. He is a member of IEEE and ACM.

Yunpeng Xiao received the Ph. D. degree and Master degree in Computer Science and Engineering from Beijing University of Posts and Telecommunications, China. Currently, he is an Assistant Professor in the College of Software Engineering, Chongqing University of Posts and Telecommunications, China. His research interests include image security, social network analysis and big data analysis.