Robust Image Hashing for Tamper Detection Using Non-Negative Matrix Factorization

Zhenjun Tang, Shuozhong Wang, Xinpeng Zhang, Weimin Wei, and Shengjun Su

Abstract—The invariance relation existing in the non-negative matrix factorization (NMF) is used for constructing robust image hashes in this work. The image is first re-scaled to a fixed size. Low-pass filtering is performed on the luminance component of the re-sized image to produce a normalized matrix. Entries in the normalized matrix are pseudo-randomly re-arranged under the control of a secret key to generate a secondary image. Non-negative matrix factorization is then performed on the secondary image. As the relation between most pairs of adjacent entries in the NMF's coefficient matrix is basically invariant to ordinary image processing, a coarse quantization scheme is devised to compress the extracted features contained in the coefficient matrix. The obtained binary elements are used to form the image hash after being scrambled based on another key. Similarity between hashes is measured by the Hamming distance. Experimental results show that the proposed scheme is robust against perceptually acceptable modifications to the image such as Gaussian filtering, moderate noise contamination, JPEG compression, re-scaling, and watermark embedding. Hashes of different images have very low collision probability. Tampering to local image areas can be detected by comparing the Hamming distance with a predetermined threshold, indicating the usefulness of the technique in digital forensics.

Index Terms—image hashing, non-negative matrix factorization, robustness, tamper detection.

1 Introduction

IMAGE hashing derives a content-based compact representation of an image called the hash. It finds applications in image authentication, digital watermarking, and content-based image retrieval (CBIR). The traditional cryptographic hash functions such as MD5 and SHA-1 map input data to a short string with a fixed size. But they are unsuitable for images. For cryptographic hashes, any small changes in the input, even a single bit, will significantly change the hash value. An image may undergo various digital manipulations, e.g., de-noising, contrast enhancement, geometric transformation, and JPEG compression. Since these normal operations do not change the main contents in the image, they should not significantly change the hash value. On the other hand, image may be tampered by malicious attackers. Unacceptable changes should produce a completely different hash. In general, an ideal image hash should have the following desirable properties:

- Perceptual robustness: The hash function should map visually identical images to the same hash even if their digital representations are not exactly the same. Visually similar images without significant differences may have hashes with a small distance.
- Uniqueness, or anti-collision capability: Probability of two different images having an identical hash value, or very close hash values, should tend to zero.
- Sensitivity to visual distinction: Perceptually important changes to an image should lead to a completely different hash. This feature is essential for the image hash to be useful in image authentication and digital forensics.
- Key-dependence: The hash must be generated under the control of a secret key or several keys. It should be extremely

• *Z. Tang, S. Wang, X.Zhang, W. Wei, and S.Su are with the School of Communication and Information Engineering, Shanghai University, Shanghai 200072, P.R.China*

Contact author: S. Wang, e-mail: shuowang@shu.edu.cn
Work supported by the Natural Science Foundation of China (60502039, 60773039) and the High-Tech Research and Development Program of China (2007AA01Z477)
Manuscript received February 15, 2008; revised March 20, 2008.

difficult to estimate the hash without a correct key. The last two requirements may collectively be considered as security of image hashing.

Earlier methods of image hashing include the wavelet coefficient statistics-based scheme, DCT-based approach, relation based technique, Radon transform method, etc. In [13] , Venkatesan et al. introduce an algorithm using randomized signal processing strategies for a non-reversible compression of images into random binary strings. It is robust against compression and geometric distortions. Their method is analogous to message authentication codes (MAC) in cryptography to minimize collision probability. Fridrich and Goljan [1] describe an algorithm using a DCT-based approach and evaluate its performance. The perceptual robustness and sensitivity to secret keys are satisfied by using special image digest functions that return the same bit-string for a class of images derived from an original image using common processing operations. Different images produce completely different bit-strings. Lin and Chang [8] present a technique for image authentication, which can distinguish JPEG lossy compression from malicious attacks. They found that relationships between DCT coefficients at the same position in separate blocks are preserved before and after JPEG compression. The method can also handle distortions introduced by various acceptable manipulations such as integer rounding, image filtering, image enhancement, and scaling-rescaling. In [5], Lefebvre et al. use Radon transform to obtain image characteristics invariant against rotation and scaling. It is also robust against basic image processing operations and Stirmark attacks. Another method [6] is a one-way function for images, which also uses the Radon transform together with the principal component analysis (PCA) to extract characteristics robust against geometrical transformation including rotation and scaling, and normal image manipulations such as compression, filtering, and blurring.

In recent years, more works on image hashing have been reported. In [3], Kozat et al. view images and attacks as a sequence of linear operators, and propose to calculate hashes using transforms based on matrix invariants. The algorithms first construct a secondary image from the input image by pseudo-randomly extracting features that capture semi-global geometric characteristics. From the secondary image, they extract the final features to be used as a hash value. In this process, they use spectral matrix invariants as embodied by singular value decomposition (SVD). In another work [11], a hashing scheme for still images is introduced. The RAdial Variance (RAV) vector is first extracted by using the radial projections of image pixels. The low-frequency DCT coefficients of the RAV vector are then quantized to form the image hash. This scheme is resilient to image rotation and re-scaling, but its collision risk is not low enough. Swaminathan et al. [12] propose to generate an image hash based on Fourier transform features and controlled randomization. They formulate robustness of image hashing as a hypothesis testing problem and evaluate the performance under various image processing operations. The hash function is resilient to several content-preserving modifications such as moderate geometric and filtering. A general framework is introduced to model the hash values as random variables and quantify its uncertainty in terms of differential entropy.

Monga and Mihcak [9] first proposed to derive the image hash using non-negative matrix factorization (NMF). They apply NMF to some sub-images, use the factorization factors to construct a secondary image, and obtain the low-rank matrix approximation of the secondary image with NMF again. The matrix entries are concatenated to form an NMF-NMF vector. To get a short vector, they calculate the inner product between the NMF-NMF vector and a set of weight vectors which have i.i.d. Gaussian components of zero mean and unit variance. The NMF-NMF-SQ hashing has been shown to have good performances.

In this paper, we develop an image hashing scheme using the property of non-negative matrix factorization in a different way. The image is first converted into a normalized monochrome pixel array. By re-arranging its entries, a secondary image is obtained. NMF is

applied to produce a feature-bearing coefficient matrix, which is then coarsely quantized to achieve high-rate compression. The obtained binary string is scrambled to generate the image hash.

The rest of the paper is organized as follows. In Section 2, the proposed NMF hashing approach is introduced. Section 3 describes the experiments and presents the results. In Section 4, comparisons are made with other image hashing schemes. Section 5 concludes the paper.

2 IMAGE HASHING BASED ON NMF

A non-negative matrix $\mathbf{V}$ of size $M \times N$ can be viewed as N column vectors, each sized $M \times 1$. The aim of NMF is to find two non-negative matrix factors, $\mathbf{B}$ of size $M \times R$ and $\mathbf{C}$ of size $R \times N$, to approximately represent the original matrix $\mathbf{V}$ such that $\mathbf{V} \approx \mathbf{BC}$, where $\mathbf{B}$ and $\mathbf{C}$ are called the base matrix and the coefficient matrix (or encoding matrix), respectively. Equivalently, the columns of $\mathbf{V}$, $\mathbf{v}_n$, can be approximated as $\mathbf{v}_n = \mathbf{B}\mathbf{c}_n$, where $\mathbf{c}_n$ are columns of $\mathbf{C}$. When $R < \min(M, N)$, NMF may be used as a technique of dimensionality reduction. In the present work, we employ the following updating rules described in [4] to find the non-negative matrix factors $\mathbf{B}$ and $\mathbf{C}$:

$$B_{m,r} \leftarrow B_{m,r} \frac{\sum_{n=1}^{N} C_{r,n} V_{m,n} / (\mathbf{BC})_{m,n}}{\sum_{n=1}^{N} C_{r,n}} \quad (1)$$

$$C_{r,n} \leftarrow B_{r,n} \frac{\sum_{m=1}^{M} B_{m,r} V_{m,n} / (\mathbf{BC})_{m,n}}{\sum_{m=1}^{M} B_{m,r}} \quad (2)$$

where $m = 1, 2, \ldots, M; n = 1, 2, \ldots, N; r = 1, 2, \ldots, R$. It can be shown that the above rules correspond to the following cost function:

$$F = \sum_{m=1}^{M} \sum_{n=1}^{N} \left[V_{m,n} \log \frac{V_{m,n}}{(\mathbf{BC})_{m,n}} - V_{m,n} + (\mathbf{BC})_{m,n} \right] \quad (3)$$

which is known as the generalized Kullback-Leibler (KL) divergence. Since the updating rules allow only additive combinations, but not subtractive combinations, the NMF can obtain a representation based on local image features. This is advantageous in feature extraction for the image hashing.

The proposed image hashing scheme is composed of the following four steps: 1) image pre-processing, 2) construction of a secondary image subject to NMF, 3) data reduction with NMF to obtain a low-rank approximation of the secondary image, and coarse quantization of the obtained coefficient matrix, and 4) encryption of the binary string based on a secret key to produce the hash string.

First, we let the original image undergo a sequence of pre-processing, or normalization, including image re-sizing, color space conversion, and low-pass filtering. This is shown in Fig. 1 Image re-sizing changes the image into a standard size $Q \times Q$ using bi-linear interpolation. This is done to ensure that the generated image hash has a fixed-length. It can also make the final hash scaling-resistant. Since the luminance plane contains most of the geometric and visually significant information, for a color image we only consider the luminance component $\mathbf{Y}$ of the YCrCb representation in the present work. Color features will be considered in the future to take into account color-related tampering. The resized $\mathbf{Y}$ plane is passed through a low-pass filter to produce the pre-processed image denoted $\mathbf{U}$. The purpose of low-pass filtering is to alleviate influences of minor image modification on the final hash value. The modifications include noise contamination and filtering.

In the second step, a secondary image is formed by reorganizing the original image pixels. The pre-processed image $\mathbf{U}$ is randomly partitioned into t strips, and each strip is again divided into t non-overlapping blocks with varied sizes, resulting in $t^2 = N$ blocks in total. This is shown in the left part of Fig. 2. All blocks are re-scaled to a pre-determined size $k \times k$ with bi-linear interpolation. Stack the columns of each normalized $k \times k$ block to form a $k^2 \times 1$ vector $\mathbf{v}_n = [\mathbf{v}_{n,1}, \mathbf{v}_{n,2}, \ldots, \mathbf{v}_{n,M}]^{\mathrm{T}}$ where $M = k^2$, and $n = 1, 2, \ldots, N$. These vectors are used as columns in a pseudo-random order to form an $M \times N$ matrix $\mathbf{V}$. We call the matrix $\mathbf{V} = [\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_N]$ the secondary image that will undergo non-negative matrix factorization

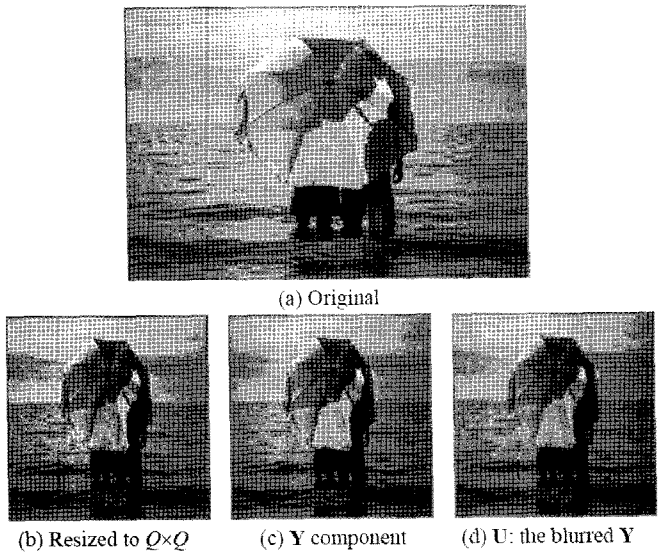


Fig. 1. Image pre-processing

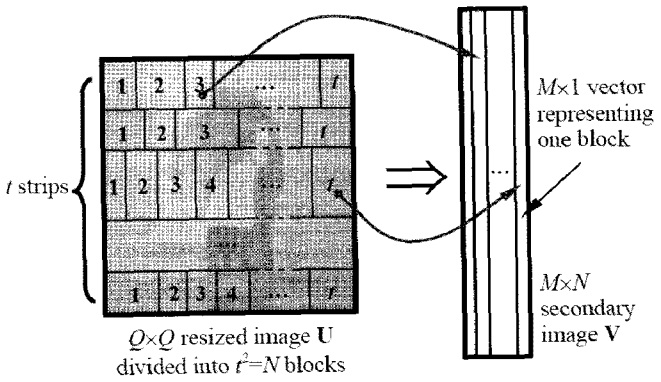


Fig. 2. Conversion of the re-scaled image U into a secondary image V

in the next step. This operation achieves the initial data reduction and lets us use fewer vectors to represent the original image when the block size is sufficiently large so that N is considerably smaller than the column number Q of the image U.

Next, we apply NMF to the secondary image V using the iteration method as defined in (1) and (2) to obtain the corresponding coefficient matrix C. In order to compress the feature-bearing coefficient matrix, its entries are coarsely quantized to produce a binary matrix $\mathbf{C}^{(b)}$ according to the following rule:

$$c_{r,n}^{(b)} = \begin{cases} 0 & c_{r,n} \leq c_{r,n+1} \\ 1 & c_{r,n} > c_{r,n+1} \end{cases} \quad \begin{matrix} n = 1, 2, \ldots, N \\ r = 1, 2, \ldots, R \end{matrix} \tag{4}$$

where $c_{r,n}$ denotes the entry of C in the r-th row and the n-th column , and $c_{r,N+1} = c_{r,1}$. The quantization rule of (4) can be understood in the following reasoning: Content-preserving manipulations generally make small changes of the entries in the coefficient matrix, while the relations as to which one is larger between two neighboring entries are most likely invariant. This will be justified in the experiments.

Finally, concatenating the quantized binary values to form a binary string, a key-dependent image hash h is obtained by randomly scrambling the binary string. The hash generation process is illustrated in Fig. 3.

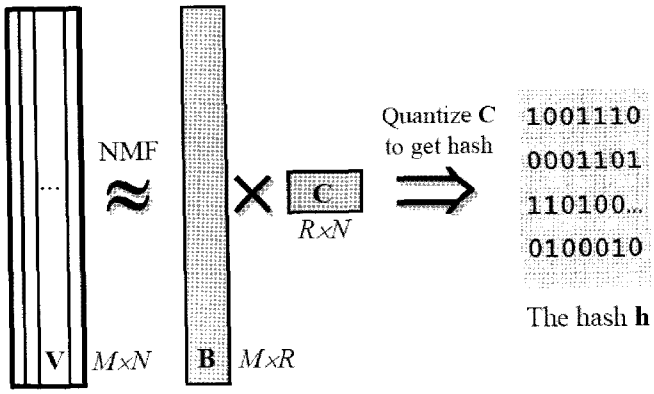


Fig. 3. Generation of the hash

3 Experimental Results

In the experiment, the image size is normalized to 512×512. The resized image is low-pass filtered with a 5×5 Gaussian low-pass mask with a unit standard deviation. The parameters used for the NMF are $t = 8$, $k = 64$, and $R = 5$. Therefore, the hash length is $64 \times 5 = 320$ bits. We use Hamming distance to measure the similarity of hashes, which is defined as follows.

$$d(\mathbf{h}^{(1)}, \mathbf{h}^{(2)}) = \sum_{l=1}^{L} \left| h_l^{(1)} - h_l^{(2)} \right| \tag{5}$$

where L is the length of the hash string. If the distance between two hashes is greater than a predetermined threshold T, their corresponding images are considered significantly different. Based on the experiments as described in the following, we observe that a good trade-off between robustness and tampering detection capability can be obtained when $T = 25$.

3.1 Perceptual Robustness

To examine robustness of the hash, we use Stirmark 4.0 [10] to perform attacks on some standard color images sized 512×512, including Airplane, Baboon, House, Lena, and Peppers. The content-preserving manipulations used in the experiment include linear filtering, additive noise contamination, JPEG compression coding, re-scaling, and watermark embedding. By calculating Hamming distance between the original image and the attacked version, we have obtained the results illustrated in Fig. 4. In the figure, the indices of the abscissa represent various Stirmark attacks on the image, which are listed in Table 1. The Gaussian low-pass filtering uses a 3×3 mask; the additive noise levels used include 1, 2, 3, 4, and 5; the JPEG compression quality factors are $5, 10, 20, \ldots, 100$; the scaling ratios are 0.5, 0.75, 0.9, 1.1, 1.5, 2.0, respectively; and the watermark embedding strengths include $10, 20, \ldots, 100$. The ordinate is the Hamming distance d between the original and attacked images. We observe that, except for some rare cases, the values of d are less than 20. The only exception in the experiment occurs for very low quality JPEG compression of Lena. This indicates that the image hash is robust against linear filtering, additive noise contamination, JPEG compression, scaling, and watermark embedding. Therefore, to resist these attacks, we can safely set the threshold $T = 25$.

3.2 Discriminative Capabilities

Collision occurs if the Hamming distance between two hash values of visually distinct images is sufficiently small, say, less than a given threshold T. In order to find the collision probability, we generated hashes of $1,700$ different color images. The images used in this experiment included 12 standard test images

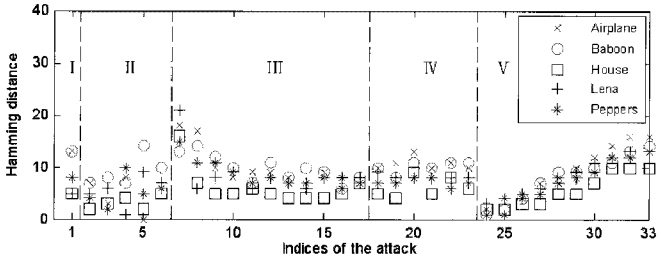


Fig. 4. Robustness validation based on 5 test images. Indices of the abscissa indicate different attacks as listed in Table 1

sized 512×512 such as Airplane, Baboon, House, Lena, and Peppers, and 1,688 images from the image database of Washington University [2], with sizes ranging from 256×256 to 883×589. We used a desktop computer with a 2.8 GHz Pentium CPU and 512 MB RAM, running MATLAB, in the experiment. Generating 1,700 hashes took about 210 minutes, and calculating 1,444,150 Hamming distances between hashes of different images took about 40 seconds. Assume the Hamming distances d follow one of the common distributions, i.e., Poisson, lognormal, and normal distributions. We apply chi-square test [7] to determine which is the closest. Parameters of these distributions are obtained based on the maximal likelihood estimation, and the probability density functions (PDF) are computed at the values ranging from 0 to the hash length L. The statistics χ^2 is then calculated:

$$\chi^2 = \sum_{i=0}^{L} \frac{(n_i - np_i)^2}{np_i} \tag{6}$$

where n is the number of trials, n_i occurring frequency of the Hamming distance being i, and p_i the probability at i obtained by using PDF. The results of chi-square test are shown in Table 2. Since χ^2 of normal distribution is the smallest, we can identify the distribution of Hamming distances as the normal distribution with its mean and standard deviation being $\mu = 147.4$ and $\sigma = 14.2$, respectively. Fig. 5 gives comparison between the actual distribution and the ideal normal distribution. Given a threshold T, the collision probability can be

TABLE 1
Attacks corresponding to indices in Figures 4, 7 and 8

Indices	Codes	Stirmark attacks	Description
1	I	Gaussian low-pass	mask
2-6	II	additive noise	level
7-17	III	JPEG compression	Q factor
18-23	IV	scaling	ratio
24-33	V	watermark embedding	strength

obtained as

$$P(d \le T) = \frac{1}{\sqrt{2\pi}\sigma}\int_0^T e^{-\frac{(x-\mu)^2}{2\sigma^2}}\,\mathrm{d}x = \\ = \frac{1}{2}\mathrm{erfc}\Big(-\frac{T-\mu}{\sqrt{2}\sigma}\Big) \tag{7}$$

Then, a very low collision probability of $\mathrm{erfc}(6.10)/2 = 3.16 \times 10^{18}$ is achieved when $T = 25$.

In addition to low collision probability, the proposed method can distinguish tampered images from the original version. Fig. 6 shows the original and tampered versions of Baboon sized 512×512 and a digital photograph sized 540×319. The right eye of Baboon in Fig. 6(b) is covered, leading to a Hamming distance from the original equal to 46. In Fig. 6(d), a vehicle is erased from the road. The Hamming distance between (c) and (d) is 63. In both cases the Hamming distances are significantly greater than the above threshold value, indicating the ability of the proposed method to detect malicious tampering.

4 Performance Comparison

In this section, comparisons are made between the proposed method and two other image hashing techniques: the RASH [11] and NMF-NMF-SQ [9] schemes. For these two schemes, we use the same images and the Stirmarked versions in Subsection 3.1 and the same examples of malicious attacking in Subsection 3.2 to check perceptual robustness and sensitivity to tampering, respectively. For a color image, only the luminance component Y in the YCrCb space is considered. The distance metrics used in the respective papers are adopted here for the methods being compared.

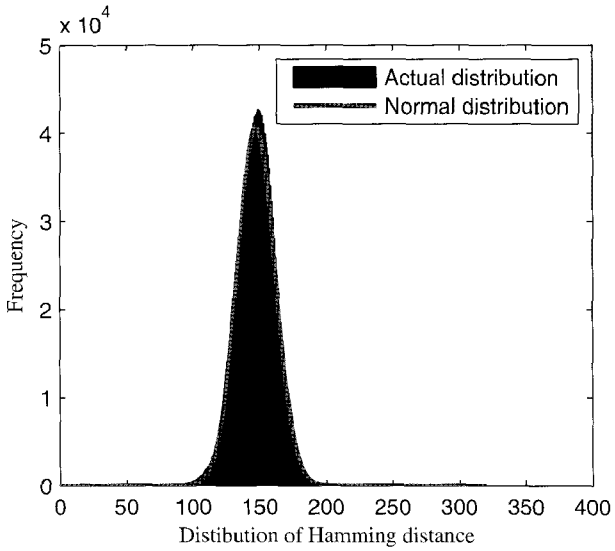


Fig. 5. Distribution of Hamming distances between different image hashes

4.1 RASH method

In the RASH method [11], peak of cross correlation (PCC) is used to measure visual similarity between images. The authors take 0.87 as the threshold. If PCC > 0.87, the two images are considered perceptually similar. Fig. 7 shows PCC values between hashes of the original and the 33 Stirmark-attacked images. It is observed that the method is robust against the tested attacks with a few exceptions, that is, for additive noise levels 3, 4 and 5, and JPEG $Q = 5$. Collision probability reported in [11] is 5.86×10^{-6} that is significantly greater than that of the proposed method as given in Subsection 3.2. PCC between the hashes of Figs. 6(a) and 6(b) is 0.965, and that between 6(c) and 6(d) is 0.914, both above the threshold value 0.87. This means that the RASH method is not sensitive enough to detect the small-area tampering

TABLE 2
Results of chi-square test for Hamming distance d

Distribution type	Estimated parameters	χ^2
Gamma	$\alpha = 104.4, \beta = 1.4$	2.6×10^{15}
Poisson	$\lambda = 147.4$	6.4×10^{14}
Rayleigh	$\beta = 104.7$	4.5×10^{6}
Weibull	$\beta = 11.7, \eta = 153.7$	2.6×10^{6}
lognormal	$\mu = 5.0, \sigma = 0.1$	4.6×10^{15}
normal	$\mu = 147.4, \sigma = 14.2$	1.4×10^{6}

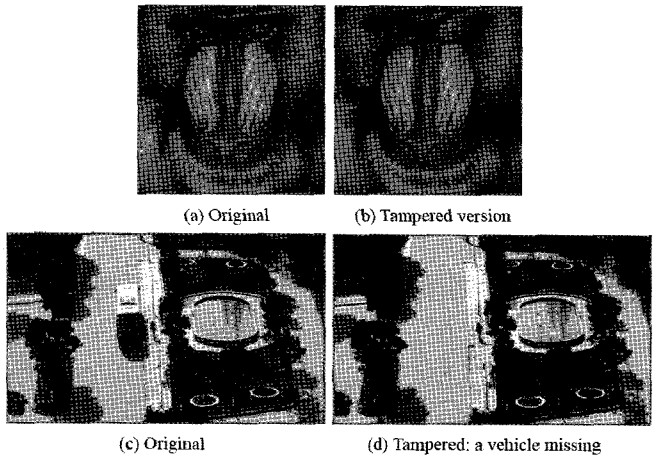


Fig. 6. Original and tampered images

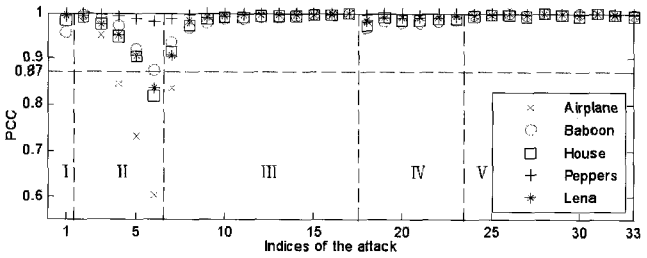


Fig. 7. Robustness of RASH based on 5 test images. Indices of the abscissa indicate different attacks as listed in Table 1.

of Fig. 6. This is because the radial variance (RAV) extracted from the image is a global-based feature, which is unable to capture small changes in the image. Since the RAV vector is obtained by calculating variances of pixel luminance over many radial projections crossing the image center, the more the tampered region are located away from the image center, the less sensitive the hash will be to the tampering.

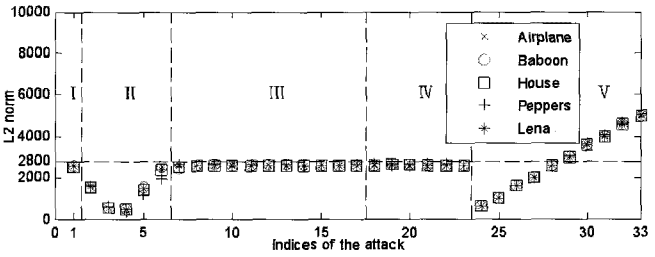


Fig. 8. Robustness of NMF-NMF-SQ hash. Indices of the abscissa indicate different attacks listed in Table 1.

4.2 NMF-NMF-SQ hash scheme

To compare with the scheme introduced in [9], the images are also resized to 512×512 as in our experiments before calculating the NMF-NMF-SQ hash. The parameters used are: the number of sub-images $p = 80$, length and width of sub-images $m = 64$, rank of the first NMF $r_1 = 2$, rank of the second NMF $r_2 = 1$, and the hash length $M = 64$.

Calculate the L2 norm between hashes of the original and attacked versions. The obtained results are shown in Fig. 8. The ordinate represents the L2 norm τ between the original and attacked images. All values of τ are below 2800 except some strong watermarking attacks. The τ value increases approximately linearly with the increasing watermark strength.

To check its collision property, extract NMF-NMF-SQ hashes of the same 1,700 images as used in Section 3, and compute the L2 norm between each pair of two hashes. The chi-square test is applied to determine the distribution of L2 norm again. We observe that the L2 norm between the NMF-NMF-SQ hashes follow a Gamma distribution with $\alpha = 9.5$, $\beta = 1564$. The χ^2 results are shown in Table 3. Given a

TABLE 3
Results of chi-square test for the L2 norm τ

Distribution type	Estimated parameters	χ^2
Gamma	$\alpha = 9.5, \beta = 1564$	7.4×10^3
Poisson	$\lambda = 14876$	4.3×10^{24}
Rayleigh	$\beta = 11048$	4.1×10^5
Weibull	$\beta = 3.32, \eta = 16570$	1.5×10^5
lognormal	$\mu = 9.6, \sigma = 0.33$	1.2×10^7
normal	$\mu = 14876, \sigma = 4778$	9.4×10^4

threshold T, the collision probability can be obtained as

$$P(\tau \leq T) = \int_0^T \frac{1}{\beta^\alpha \Gamma(\alpha)} x^{(\alpha-1)} e^{(\frac{-x}{\beta})} \, \mathrm{d}x \quad (8)$$

where $\Gamma(\alpha)$ is the well-known Gamma function given by

$$\Gamma(\alpha) = \int_0^{+\infty} t^{\alpha-1} e^{-t} \, \mathrm{d}t \quad (9)$$

Without taking into account the watermark embedding attacks which is not considered in [9], we can choose a threshold $T = 2800$. In this case the collision probability is 4.3×10^{-5}, even greater than that of RASH.

In addition, the L2 norm between the hashes of Figs. 6(a) and 6(b) is 574, much lower than that produced by JPEG compression. Similar result can be obtained for Figs. 6(c) and 6(d). Therefore the NMF-NMF-SQ hash is not applicable to detect such small area tampering.

An advantage of RASH and NMF-NMF-SQ over the proposed method is their capability in resisting rotation attacks, which has not been treated in the present work.

In summary, the proposed method is generally equivalent to RASH and NMF-NMF-SQ in terms of perceptual robustness except for rotation, while it is superior to the other two methods both in anti-collision properties and the detection capability of local area tampering. As to the length of image hashes, the RASH hash is 320 bits long, equal to our hash. The NMF-NMF-SQ hash contains M decimal digits. Taking Baboon as an example, $M = 64$ with the decimal entries ranging from -10369 to 7391, thus each entry needs 15 bits for storage. Therefore in a binary form, the hash has 960 bits, considerably longer than ours.

5 Conclusions

By using a non-negative matrix factorization to extract image features, we have developed a perceptual image hashing scheme. Because relations between adjacent entries of the coefficient matrix are largely invariant after the image undergoes common digital processing, a quantization rule can be defined to produce a binary string. This forms the basis of the image hash. The obtained hash is robust against perceptually acceptable image modifications such as linear filtering, additive noise contamination, JPEG compression coding, image re-sizing and watermark embedding. Probability of collision between hashes of different images is very low, while a significant change in the hash value occurs when the image is maliciously tampered.

To avoid the security loopholes existing in some early techniques such as those discussed in [14], secret keys are introduced in several steps including the pseudo-random partitioning and normalization of the original image, the way in which the secondary image is constructed, and the final scrambling of the binary hash string. Attempts to coin a fake hash are therefore very unlikely to succeed.

Further research on the NMF-based image hash is in order. This includes in-depth investigation into the relation between various parameters and the hash performance, provision of anti-rotation capabilities, improvement of detection sensitivity against less obvious tampering, consideration of color components for detecting color-related modifications, analytical or semi-analytical determination of the threshold value, and so forth.

REFERENCES

[1] J. Fridrich and M. Goljan, *Robust hash functions for digital watermarking*, IEEE Proceedings International Conference on Information Technology: Coding and Computing, pp. 178-183, 2000.

[2] Ground Truth Database, [online]. Available: http://www.cs.washington.edu/research/imagedatabase/groundtruth/

[3] S. S. Kozat, K. Mihcak, and R. Venkatesan, *Robust perceptual image hashing via matrix invariants*, Proceedings of IEEE Conference on Image Processing, pp. 3443-3446, 2004.

[4] D. D. Lee and H. S. Seung, *Algorithms for non-negative matrix factorization*, Advances in Neural Information Processing Systems, vol. 13, pp. 556-562, 2000.

[5] F. Lefebvre, B. Macq, and J.-D. Legat, *RASH: Radon soft hash algorithm*, Proceedings of European Signal Processing Conference, pp. 299-302, 2002.

[6] F. Lefebvre, J. Czyz, and B. Macq, *A robust soft hash algorithm for digital image signature*, Proceedings of International Conference on Image Processing, vol. 2, pp. 14-17, September 2003: II - 495-8.

[7] E. L. Lehmann and J. P. Romano, *Testing Statistical Hypotheses*, 3rd ed., New York, USA, Springer, pp. 590-599, 2005.

[8] C. Y. Lin and S. F. Chang, *A robust image authentication system distinguishing JPEG compression from malicious manipulation*, IEEE Transactions on Circuits System and Video Technology, vol. 11, no. 2, pp. 153-168, 2001.

[9] V. Monga and M. K. Mihcak, *Robust and secure image hashing via non-negative matrix factorizations*, IEEE Transactions on Information Forensics and Security, vol. 2, no. 3, pp. 376-390, 2007.

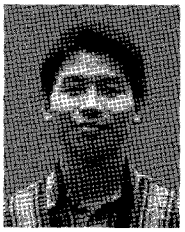
[10] F. A. P. Petitcolas, *Watermarking schemes evaluation*, IEEE Signal Processing Magazine, vol. 17, no. 5 pp. 58-64, 2000.

[11] C. De Roover, C. De Vleeschouwer, F. Lefebvre, and B. Macq, *Robust video hashing based on radial projections of key frames*, IEEE Transactions on Signal Processing, vol.53, no.10, pp.4020-4036, 2005.

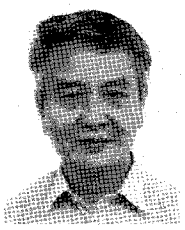
[12] A. Swaminathan, Y. Mao, and M. Wu, *Robust and secure image hashing*, IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 215-230, 2006.

[13] R. Venkatesan, S.-M. Koon, M. H. Jakubowski, and P. Moulin, *Robust image hashing*, Proceedings of IEEE International Conference on Image Processing, vol. 3, pp. 664-666, 2000.

[14] S. Wang and X. Zhang, *Attacks on perceptual image hashing*, Proceedings of the 2nd International Conference on Ubiquitous Information Technologies and Applications, pp. 199-203, 2007.



Zhenjun Tang received B.S. and M.S. degrees from Guangxi Normal University, Guilin, P.R. China, in 2003 and 2006, respectively. He is currently a Ph.D. student at Shanghai University, P.R. China. His research interests include image processing and information security of digital media.



Shuozhong Wang received B.S. degree from Peking University, P.R. China, in 1966 and Ph.D. degree from University of Birmingham, England, in 1982. Currently, he is a professor of Shanghai University. His research interests include image processing, audio processing, and information hiding.

Xinpeng Zhang received Ph.D. degree from Shanghai University, P.R. China, in 2004. Currently, he is an associate professor of Shanghai University. His research interests include image processing, information security of digital media, digital watermarking, steganography and steganalysis.

Weimin Wei received M.S. degree from Wuhan University, P.R. China, in 2004. He is currently a Ph.D. student at Shanghai University. His research interests include image processing, digital forensics and data mining.

Shengjun Su received M.S. degree from Huazhong University of Science and Technology, Wuhan, P.R. China, in 1999. She is currently a Ph.D. student at Shanghai University. Her research interests include image processing and information security.