Journal of Information Hiding and Multimedia Signal Processing ©2017 ISSN 2073-4212
Ubiquitous International Volume **8**, Number **3**, May **2017**

Perceptual Hashing of Color Images Using Interpolation Mapping and Non-negative Matrix Factorization

Qiu-Yu Zhang, Qi-Yan Dou, Zi Yang, Yan Yan

School of Computer and Communication
Lanzhou University of Technology
Gansu, Lanzhou, 730050, P. R. China

zhangqylz@163.com; 1147025638@qq.com; 15709440859@163.com; yanyan@lut.cn

Received July, 2016; revised January, 2017

Abstract. *In order to improved tampering detection ability and resistance of arbitrary rotation attack in color image authentication, a color image perceptual hashing algorithm combining interpolation mapping with non-negative matrix factorization (NMF) was proposed in this paper. Firstly, this algorithm employs interpolation mapping, which maps the content of the four corners of a square image into its inscribed circle, to retain image information as much as possible. Secondly, the circular image is divided into rings to make it resistible to rotation attack. Finally, NMF and quantification are conducted on the secondary image mapped from the rings to generate final hash values. The experiment results illustrate that the proposed algorithm was robust to most image content preserving operations and had a good discrimination performance. In addition, it had good tamper detection ability which can detect the content tampering of an image edges effectively and resist arbitrary angle rotation attack.*
Keywords: Image authentication, Image hashing, Interpolation mapping, Non-negative matrix factorization, Tamper detection

1. **Introduction.** Most existing image hashing algorithms cannot meet the requirements of authenticity and integrity from different applications such as anti-malicious tamper and anti-rotation. As for the image hashing research, especially the real color image hashing study, is of great practical and theoretical significance [1-2].

Traditional cryptographic hash functions, such as MD5 and SHA-1 algorithms can also produce hash values. But multimedia data in the transmission process will inevitably experience compression, filtering, distortion, noise pollution, format conversion and other changes. What's more, these changes will modify original multimedia contents. Thus, traditional cryptographic hash function is inapplicable for multimedia information. In addition, from the perspective of multimedia security, image perceptual hashing function should also have the robustness of content-preserving operations and the sensitivity of malicious tampering [3].

At present, there have been a lot of research achievements in the field of image perceptual hashing technology, and its feature extraction can be carried out in spatial and transform domain. Image perceptual hashing technologies which based on spatial domain include statistical properties [4-6], structure information [7], matrix decomposition

[8-10] and scale invariant feature transform (SIFT) [11]. Technologies based on transform domain are DCT [12], DWT [13], Radon [14] and DFT [15]. In [4], the pseudo random blocks of an image are normalized to same size squares. These squares will be conformably mapped to unit circles. Then this method calculates magnitude and phase of Zernike moments which come from unit circles. Finally, it scrambles magnitude and phase of these moments to get image hashes. In this method, the four corners of each image block are incorporated into hashes, so tamper detection performance is improved. The luminance component of color image is divided into rings, and these rings will be mapped to be a secondary image in [16]. Next, the secondary image will be decomposed by NMF to get coefficient matrix as final perceptual hash values. This method is robust to image rotation, JPEG compression, watermarking embedding and filtering. But this algorithm can only detect the tampering of inscribed circle of an image. The algorithm in [17] improves disadvantage of missing image content when using inscribed circle to ring in [16]. It uses the circumcircle instead of the inscribed one to extract image hash values, but the hash values significantly become longer in this method. In [18], rectangular image is directly mapped by interpolation to be a circle one. After calculating Zernike moments of circle image, scrambling is conducted on these moments to form final hash values. The method can preserve the four corners information and could be better than conformal mapping in tamper detection.

To sum up, in view of the problems in [16-17] and the original interpolation mapping algorithm in [18], a novel color image perceptual hashing algorithm combined the interpolation mapping method and NMF was proposed in this paper. The experiment results show that the proposed algorithm shortens the length of the hash value, which retains the integrity of the information of four corners. Meanwhile, the advantages of ring and NMF can be fully used. Furthermore, it greatly improves tampering detection performance and has good resistance of anti-rotation attack.

The rest of this paper is organized as follows. Section 2 describes theories of original interpolation mapping, ring partition and second mapping, and NMF. A detailed color image perceptual hashing algorithm is described in Section 3. Subsequently, Section 4 gives the experimental results and performance analysis as compared with other related methods. Finally, we conclude our paper in Section 5.

2. **Problem Statement and Preliminaries.**

2.1. **Original Interpolation Mapping.**

The original interpolation mapping aims at transforming an image of size $M \times N$ to a circular of $R = L$. Firstly, this method constructs polar coordinates transform for an image with phase as horizontal axis and amplitude as vertical axis. Then it obtains L rays emitted from the center of the image by anticlockwise equal-interval sampling. Thus, the phase of these rays can be represented as $\left[0, \frac{2\pi}{L}, \frac{2\pi}{L}2, \cdots, \frac{2\pi}{L}(L-1)\right]$, and the phase of diagonal is $\varphi = arctan(\frac{N}{M})$. Moreover, the length of line corresponding to i-th phase can be calculated by

$$R_i = \begin{cases} \frac{M/2}{cos(\theta_i)} & 0 < \theta_i < \varphi, 2\pi - \varphi < \theta_i < 2\pi \\ \frac{N/2}{sin(\theta_i)} & \varphi < \theta_i < \pi - \varphi \\ \frac{-M/2}{cos(\theta_i)} & \pi - \varphi < \theta_i < \pi + \varphi \\ \frac{-N/2}{sin(\theta_i)} & \pi + \varphi < \theta_i < 2\pi - \varphi \end{cases} \tag{1}$$

Then this method uniformly take samples L points on every line and the amplitude R of these points comes to be $\left[\frac{R_i}{L}, \frac{R_i}{L}2, \cdots, R_i\right]$. The value of each sampled pixel point

comes from the mean of four points around it. Finally, after converting the polar diagram into rectangular coordinates, a rectangular image is mapped to a circular one.

2.2. **Ring Partition and Second Mapping.** The image ring partition can resist rotation attack, so this paper employs the method used in [16] to conduct ring partition on a square image. The specific steps of ring partition and second mapping could refer to Ref. [16]. The rotate invariance of ring partition has been proved in Section 2.3 of Ref. [19].

2.3. **Non-negative Matrix Factorization.** Most of the existing literatures using the method of matrix decomposition for image processing, but these methods cannot guarantee the matrix is non-negative after dimension reduction. NMF is a matrix decomposition method which makes all elements in matrix to be non-negative [20]. NMF is also an orthogonal transformation, which can achieve linear dimensionality reduction. In addition, non-negative conditional limit of NMF can resist rotation and illumination change in a certain degree.

The basic idea of NMF is: for any arbitrary non-negative matrix $\boldsymbol{V}_{M\times N}$ given, the matrix can be decomposed to two parts: a basic matrix $\boldsymbol{W}_{M\times R}$ and a coefficient matrix $\boldsymbol{H}_{R\times N}$. They can be used to approximately represent $\boldsymbol{V}$ such that:

$$\boldsymbol{V}_{M\times N} \approx \boldsymbol{W}_{M\times R} \times \boldsymbol{H}_{R\times N} \tag{2}$$

where R is the rank, it should satisfy the condition: $(M+N)R < MN$ or $R < min(M, N)$, for the realizing of the data dimension reduction.

By this form of decomposition, the product of $\boldsymbol{W}$ and $\boldsymbol{H}$ can be represented as $\boldsymbol{V}$. Using coefficient matrix $\boldsymbol{H}$ to replace the original non-negative matrix $\boldsymbol{V}$, the reduction of original data $\boldsymbol{V}$ can be achieved. In order to realize non-negative matrix $\boldsymbol{V}$, objective function is defined in non-negative constraint, and the convergence of NMF is determined to guarantee approximation effect of NMF. The objective functions of judging convergence are: Euclidean distance and Kullback-Leibler (KL) divergence. In this paper, KL divergence is used to measure convergence of NMF. The target function based on KL divergence is Eq. (3):

$$\Theta_D(\boldsymbol{V}\|\boldsymbol{W}\boldsymbol{H}) = \sum_{i=1}^{M}\sum_{j=1}^{N}\left(\boldsymbol{V}_{ij}log(\frac{\boldsymbol{V}_{ij}}{\sum_{j=1}^{R}\boldsymbol{W}_{il}\boldsymbol{H}_{lj}}) - \boldsymbol{V}_{ij} + \left[\boldsymbol{W}\boldsymbol{H}\right]_{ij}\right) \tag{3}$$

Now, the problem of NMF is transformed to minimize the objective function. This paper chooses the iterative rule which converges fast and computes the low complexity. After the NMF, the matrix $\boldsymbol{W}$ and the matrix $\boldsymbol{H}$ can be obtained.

The multiplicative iteration formula of the KL divergence is like the Eq. (4):

$$\boldsymbol{W}_{ir} \leftarrow \boldsymbol{W}_{ir}\frac{\sum_{j=1}^{N}\frac{\boldsymbol{H}_{rj}\boldsymbol{V}_{ij}}{(\boldsymbol{W}\boldsymbol{H})_{rj}}}{\sum_{j=1}^{N}\boldsymbol{H}_{rj}} \qquad \boldsymbol{H}_{rj} \leftarrow \boldsymbol{H}_{rj}\frac{\sum_{i=1}^{M}\frac{\boldsymbol{W}_{ir}\boldsymbol{V}_{ij}}{(\boldsymbol{W}\boldsymbol{H})_{ij}}}{\sum_{i=1}^{M}\boldsymbol{W}_{ir}} \tag{4}$$

where $i = 1, 2, \cdots, M, j = 1, 2, \cdots, N, r = 1, 2, \cdots, R$.

The target dimension of the non-negative $\boldsymbol{H}$ and $\boldsymbol{W}$ is selected randomly, and the results of the NMF are obtained by the number of iterative operations.

3. **Proposed Image Hashing.** Fig. 1 shows this color image perceptual hashing algorithm framework combined interpolation mapping with NMF. Its process includes image preprocessing, square image interpolation mapping into circle, circle split into rings and NMF on secondary image mapped from the rings. Compared with Ref. [16], this paper performs interpolation mapping before ring partition, rather than directly interception of inscribed circle on images. After this operation, the information outside inscribed circle can be retained effectively.

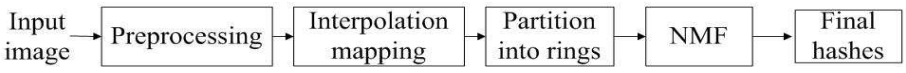


FIGURE 1. Block diagram of our image hashing.

3.1. **Improved Interpolation Mapping.** The thought of interpolation mapping used in this algorithm which transfers rectangular image to a circular one is: after calculating the radian in transform from rectangle to circle, exploiting symmetry to simplify procedures of calculating the distance from boundary to the center of an image, forward interpolation method is adopted to reduce pixel values of original image to form a new one by proportion, then circular image comes to be the result of interpolation mapping. As shown in Fig. 2.

(a) Original image.

(b) Image after interpolation mapping.

FIGURE 2. The diagram of interpolation mapping.

Mapping a color image of size $M \times N$ to a circular of $R_N = \lfloor M/2 \rfloor$, which needs the following steps:

Step 1.: The center coordinates of the original image can be calculated as (cx, cy), and the distance of the current pixel to the image center is measured by Euclidean distance as shown in Eq. (5)

$$r(x_i, y_j) = \sqrt{(x_i - cx)^2 - (y_j - cy)^2} \tag{5}$$

Step 2.: Figure out the θ corresponding to the difference point $(x_i - cx, y_j - cy)$ which comes from every pixel (x_i, y_j) and the image center (cx, cy), on the basis of the range of θ, work out the distance from the edge pixel to the image center on the line which go through (x_i, y_j) and (cx, cy).

$$R_i = \begin{cases} \sqrt{cy^2 + (x_i - cx)^2} & \frac{\pi}{4} < \theta_i < \frac{3\pi}{4}, -\frac{\pi}{4} < \theta_i < -\frac{3\pi}{4} \\ \sqrt{cx^2 + (y_j - cy)^2} & \text{other} \end{cases} \tag{6}$$

Step 3.: The proportion coefficient of image transform can be calculated by

$$t_i = r_i / R_i \tag{7}$$

Step 4.: Apply Eq. (8) and (9) to obtain the pixels (xx_i, yy_j) after transform.

$$xx_i = round(R_N \times t_i \times cos(\theta_i) + cx) \tag{8}$$

$$yy_j = round(R_N \times t_i \times sin(\theta_i) + cy) \tag{9}$$

Thus, the image I_N after interpolation mapping can be calculated by

$$I_N(yy_j, xx_i) = I(y_j, x_i) \qquad 1 \le xx_i \le M \quad and \quad 1 \le yy_j \le N \tag{10}$$

3.2. **Proposed Scheme.** According to Fig. 1, the algorithm is described as follows:

Step 1.: Image preprocessing. The input image is resized to 512×512 by bilinear interpolation. Then the image is converted from RGB color space to YCbCr color space according to the following Eq. (11), and then the luminance component Y is selected for subsequent processing.

$$\begin{aligned} Y &= 0.257 * R + 0.564 * G + 0.098 * B + 16 \\ Cb &= -0.148 * R - 0.291 * G + 0.439 * B + 128 \\ Cr &= 0.439 * R - 0.368 * G - 0.071 * B + 128 \end{aligned} \tag{11}$$

Step 2.: Interpolation mapping. After preprocessing Y according to the method of proposed interpolation mapping in Section 3.1, a normalized 512×512 square image is interpolation mapped a circle of R=256.

Step 3.: Ring partition and second mapping. According to the description of ring partition operation in Section 2.2, the image is divided into 32 equal area rings to be resilient to rotation, and then construct the secondary image $\boldsymbol{V}$ with the rings for sequential NMF operation.

Step 4.: NMF. The NMF of rank R of the secondary images $\boldsymbol{V}$ is used to reduce the dimension and compress image data.

Step 5.: Hash generation. The coefficient matrix after NMF is used as final perceptual hash values: $\boldsymbol{H} = \left[H_{11}, H_{12}, \cdots, H_{1N}, \cdots, H_{R1}, H_{R2}, \cdots, H_{RN}\right]$.

To measure similarity between two image hashes, we take correlation coefficient as the metric, and also used as hash distance. The correlation coefficient S is defined as follows:

$$S = \frac{\sum_{i=1}^{L}(H_i^{(1)} - \overline{H^{(1)}})(H_i^{(2)} - \overline{H^{(2)}})}{\sqrt{\sum_{i=1}^{L}(H_i^{(1)} - \overline{H^{(1)}})^2}\sqrt{\sum_{i=1}^{L}(H_i^{(2)} - \overline{H^{(2)}})^2}} \tag{12}$$

where $H^{(1)}$ represents final hashes of the first image, and $H^{(2)}$ represents final hash values of the secondary image, while $\overline{H^{(1)}}$ is the mean of $H^{(1)}$, $\overline{H^{(2)}}$ is the mean of $H^{(2)}$.

The correlation coefficient S ranges from -1 to +1. Two variable are positively correlated when $r > 0$, while $r < 0$ means they are negative correlation. Moreover, they are full positive correlation when $r = 1$, while $r = -1$ means they are totally negative correlation. In addition, $r = 0$ indicates there is no linear correlation between two variables.

4. **Experimental Results and Performance Analysis.** In order to make a comprehensive assessment, we randomly captured 200 images from three well-known public databases, i.e., the USC-SIPI Image Database [21], the Ground Truth Database [22] and James Z. Wang Research Group Database [23], including people, animals, food, flowers, and cars. Some example images are presented in Fig. 3.

We adopted MATLAB 2009a as the experiment platform and the images in our experiment were 24 bit true-color while their size ranged from 256×384 to 1024×1024. In the experiments, every image was preprocessed to standard size of 512×512, the radius of circle was 256 by interpolation mapping. The number of equal area's rings in the ring partition was 32, and the rank for NMF was 2, i.e., R_N=256, R=2.

FIGURE 3. Examples of test image.

4.1. **Perceptual Robustness.** Five 24 bit true-color standard test images were used in this experiment: Airplane, Baboon, House, Lena and Peppers, as shown in Fig. 4.

(a) Airplane (b) Baboon (c) House (d) Lena (e) Peppers

FIGURE 4. Standard color images for robustness validation.

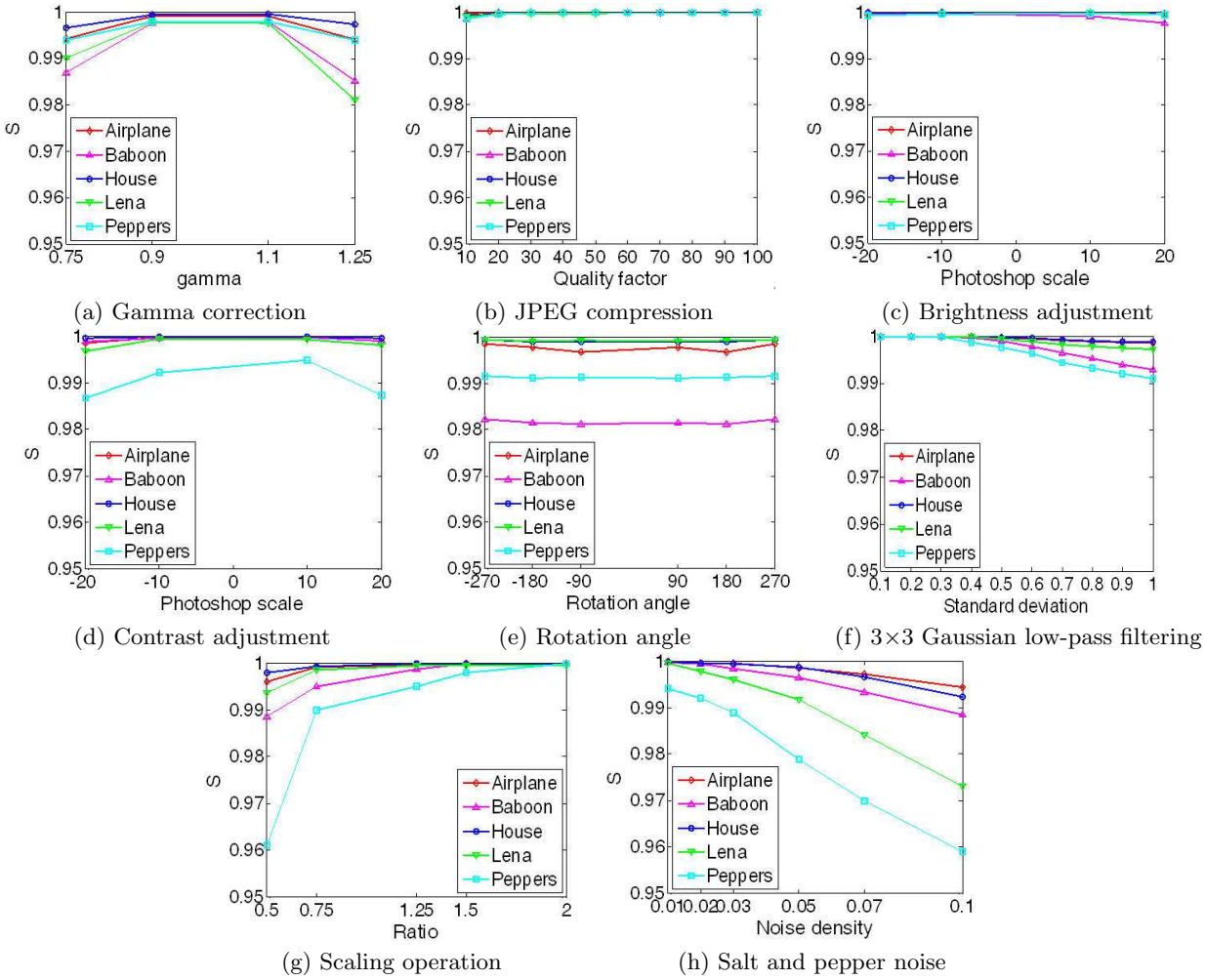
We conducted some normal image processing operations on them, including JPEG compression, scaling, adding Gaussian noise, adding Salt and pepper noise, 3×3 Gaussian low-pass filtering, gamma correction, rotation, brightness adjustment and contrasting adjustment with Photoshop. Considering the authentication of images, the similarity of hash sequences can be calculated by the using of Eq. (12) which was regarded as the similarity measure function. The parameters values of our experiments were listed in Table 1.

TABLE 1. The used content-preserving operations and their parameter values

Image content-preserving operations	Parameter	Parameter values
Gamma correction	γ	0.75, 0.9, 1.1, 1.25
JPEG compression	Quality factor	10, 20, 30, $\cdots$, 100
Brightness adjustment	Photoshop's scale	$\pm$20, $\pm$10
Contrast adjustment	Photoshop's scale	$\pm$20, $\pm$10
Rotation	Angle	$\pm$270,$\pm$180,$\pm$90
3×3 Gaussian low-pass filtering	Standard deviation	0.1,0.2,0.3, $\cdots$, 1.0
Scaling	Ratio	0.5, 0.75, 1.25, 1.5, 2
Salt and pepper noise	Noise density	0.01, 0.02, 0.03, 0.05, 0.07, 0.1

The experiment results are presented in Fig. 5, where the ordinate shows correlation coefficients and the abscissa shows corresponding parameter values for content-preserving operations. Fig. 5 shows that this algorithm has good robustness to JPEG compression, scaling, adding Gaussian noise, adding salt and pepper noise, 3×3 Gaussian low-pass filtering, gamma correction, rotation, brightness adjustment and contrast adjustment. When the correlation coefficient threshold T is assigned to 0.98, almost all images possess good robustness except for individual image after a few content-preserving operations. When the threshold T is assigned to 0.955, this algorithm is robust to all image content-preserving operations.

This paper compares the robustness of the algorithm in [16] with ours after obtaining the mean of five standard images. As shown in Fig. 6, the ordinate is correlation coefficient S.



(a) Gamma correction (b) JPEG compression (c) Brightness adjustment

(d) Contrast adjustment (e) Rotation angle (f) 3×3 Gaussian low-pass filtering

(g) Scaling operation (h) Salt and pepper noise

FIGURE 5. Robustness test based on five standard test images.

Aim at these image content-preserving operations, for instance, brightness adjustment, contrast adjustment and JPEG compression. The correlation coefficient S of the proposed algorithm is closer to 1. This means that, for these three operations, the proposed algorithm has better robustness than Ref. [16]. For gamma correction operation, S in Ref. [16] is higher than ours when the gamma value is 0.75, which indicates the robustness is slightly stronger. However, in the other three points, the correlation coefficient are all higher than those in Ref. [16], which means that the proposed algorithm has stronger robustness. For scaling operation, the robustness of Ref. [16] is better when scaling factor is 0.5 and 0.75, while the robustness of the proposed algorithm is better in the rest 3 scaling factors as shown in Fig. 6(e).

4.2. **Discriminative Capability.** To validate the discrimination, we calculated image hashes of these 200 images from image database [21-23], computed correlation coefficient S between each pair of different images, and then obtained $C_{200}^2 = 19900$ values after applying the proposed algorithm. Distribution of these results is presented in Fig. 7.

In Fig. 7, the mean μ and the standard deviation σ of all S values are 0.3647 and 0.3321, and the minimum and maximum S values are -0.7934 and 0.9789. If T=0.95 is selected as a threshold, more than 22 pairs of different images will be wrong regarded as similar images, and the conflict probability is 1.1055 $\times 10^{-3}$. If T=0.97 is selected as a threshold, 3 pairs of different images will be wrongly judged, and the collision probability

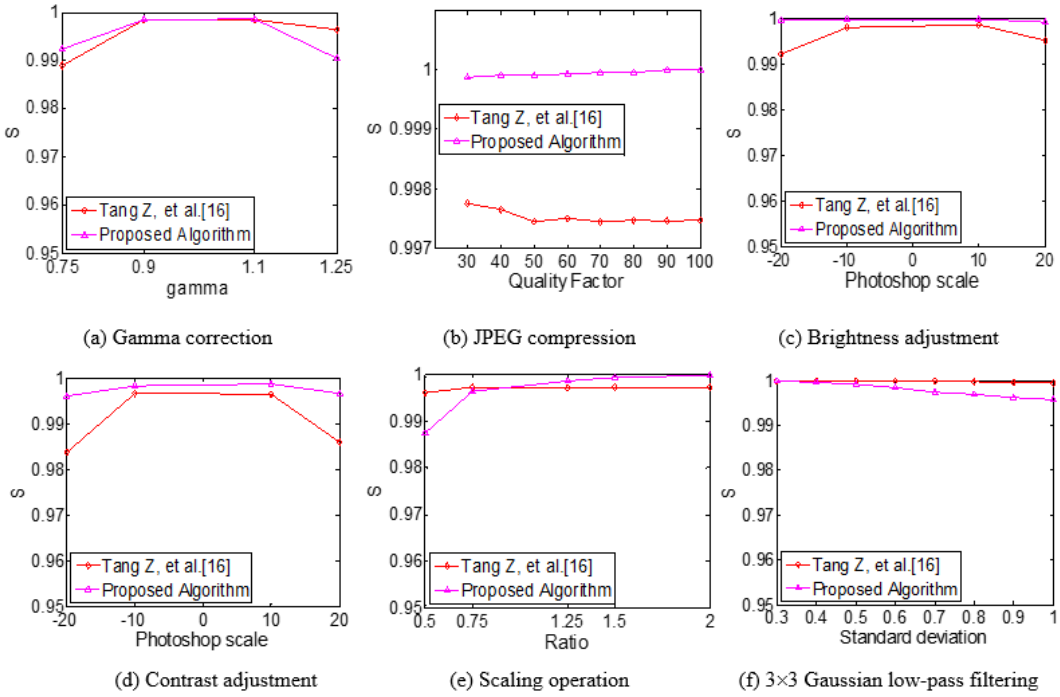


FIGURE 6. Performance comparisons.

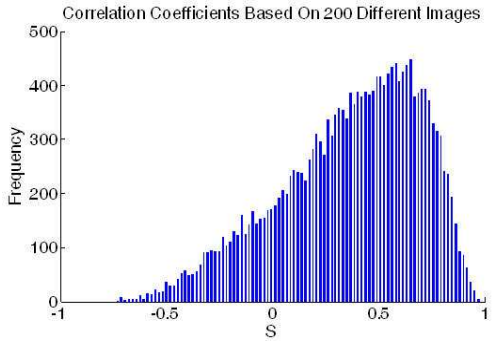


FIGURE 7. Distribution of correlation coefficients based on 200 different images.

is 1.5075 $\times 10^{-4}$. If T=0.98 is selected as a threshold, only 1 pair of different images will be incorrectly identified, the collision probability is 5.0251 $\times 10^{-5}$. Therefore, the probability of collision is very small, which meet the uniqueness. By comprehensive considering above robustness and discrimination experiments, in this paper, the threshold was set to 0.98.

In Ref. [16], the minimum and maximum S values are -0.6836 and 0.9717, and the mean and the standard deviation of all S values are 0.3910 and 0.3014, respectively. If T=0.95 is selected as a threshold, 0.12% of different images pairs are falsely considered as visually similar images. Compared with 0.11055% of the error rate of the proposed algorithm, the former one is slightly higher. When threshold is set at 0.98, false judgment will not occur in Ref. [16].

4.3. **Tamper Detection Ability Test and Analysis.** Ref. [16] conducts ring partition on the inscribed circle of the image, and only 79% of the image pixels can be used for feature extraction. However, when the pixels outside the inscribed circle of the image have been tampered, Ref. [16] will lose effectiveness.

In Fig. 8, Fig. 8(a), (e) and (i) are original images; Fig. 8(b), (f) and (j) are the ones after tampering on original images; Fig. 8(c), (g) and (k) are the original images experienced the interpolation mapping; Fig. 8(d), (h) and (l) are the tampered images conducted the interpolation mapping. That tampered image in Fig. 8(b), (f) and (j) are modified by Photoshop software from the original image in Fig. 8(a), (e) and (i). The differences are three birds on upper left corner, upper right corner and lower left corner in Fig. 8(b), add a pillar on the right in Fig. 8(f), and remove the building on the lower left corner in Fig. 8(j).

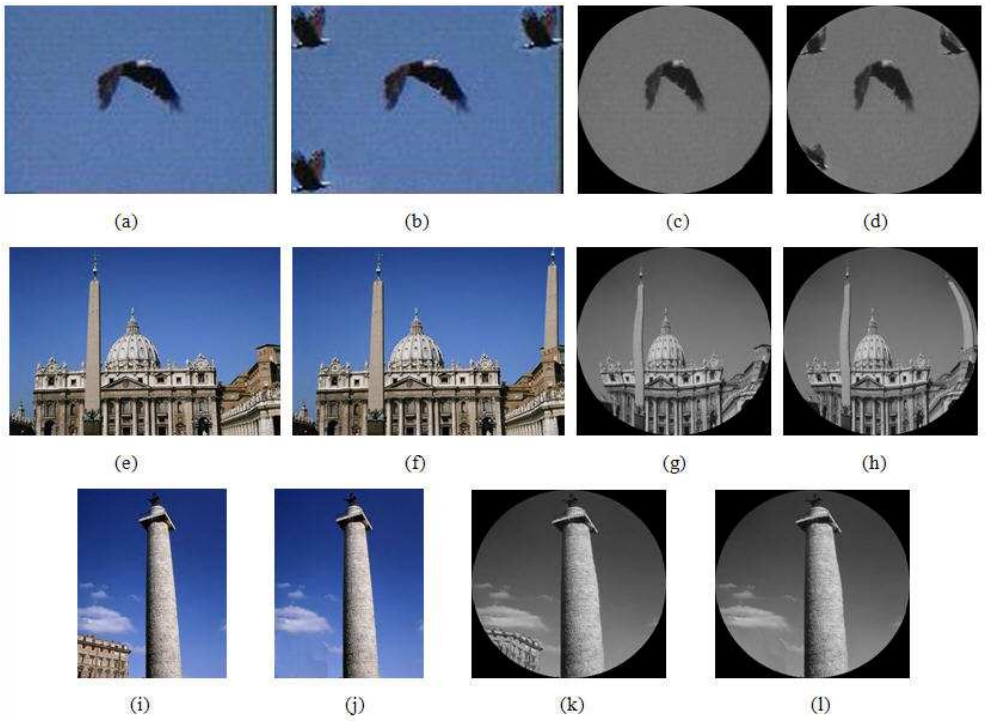


FIGURE 8. Original, tampered and interpolation mapping images.

Table 2 compares the correlation coefficients of the method in Ref. [16] with our interpolation mapping algorithm, (a)-(l) in Table 2 corresponding to Fig. 8 shows the 12 images. In Table 2, we call original images undergo interpolation mapping Orig-Map and tampering images undergo interpolation mapping Tamp-Map for the sake of simplicity.

TABLE 2. Correlation coefficients (S) of Ref. [16] and the proposed algorithm

Original image	Tampering image	Image size	Orig-Map	Tamp-Map	Image size	S in Ref. [16]	S in our hashing
(a)	(b)	128 × 96	(c)	(d)	512 × 512	0.99549	0.7805
(e)	(f)	384 × 256	(g)	(h)	512 × 512	0.99212	0.9642
(i)	(j)	256 × 384	(k)	(l)	512 × 512	0.98678	0.9136

As shown in Fig. 8 and Table 2: Fig. 8(b) is a tampered image which adds three birds on three corners of original image Fig. 8(a). After adopting the method in Ref. [16], the correlation coefficient obtained between original images Fig. 8(a) and tampered image Fig. 8(b) is 0.99549, while the three birds out of the inscribed circle are not detected, which causes the correlation coefficient being much larger than threshold 0.98 that set in the reference. Furthermore, the two pieces of images would be wrongly regarded as similar

images. However, the original image Fig. 8(a) comes to be Fig. 8(c) after interpolation mapping, whiles the tampered image Fig. 8(b) comes to be Fig. 8(d) after the same operation. As shown in Fig. 8(d), where three birds outside the inscribed circle are well mapped into the circle, so the correlation coefficient between Fig. 8(a) and Fig. 8(b) is 0.7805 which is far below threshold $T = 0.98$. Moreover, the malicious tampering with the edge information of Fig. 8(a) has been exactly detected. Experiment results show that the method in Ref. [16] will lose its effectiveness when the edge information outside the inscribed circles changes.

In allusion to the original image Fig. 8(e) and tampered image Fig. 8(f), the correlation coefficient obtained by the method in Ref. [16] is 0.99212 which also comes to be larger than threshold 0.98, while the tampering–an excrescent pillar still cannot be detected. Meanwhile, the tampered image and the original image are mistaken for similar images. After exploiting proposed algorithm, the original image Fig. 8(e) is interpolation mapped for Fig. 8(g) and tampered image Fig. 8(f) is mapped for Fig. 8(h), while the excrescent pillar is well mapped into the circle. The correlation coefficient we obtained between Fig. 8(e) and Fig. 8(f) is 0.9642 which is less the given threshold 0.98. Compared with Ref. [16] and proposed algorithm is still capable of detecting tampering with the image content, especially for the four corners outside the incircle. For the original image Fig. 8(i) and tampered image Fig. 8(j) which removes the building on lower left corner of the image, the correlation coefficient of the two images obtained by the method in Ref. [16] is 0.98678, which is greater than the threshold 0.98 in that Ref. [16]. The original image Fig. 8(i) and tampered image Fig. 8(j) is wrongly identified as similar images and the tampering with original image Fig. 8(i) has not been detected. While the correlation coefficient between Fig. 8(k) and Fig. 8(l) which is interpolation mapped from Fig. 8(l), is 0.9136, which is much lower than the threshold 0.98. And these two images with different content are correctly judged as different image/tampered image, so proposed algorithm could be able to detect malicious tampering with Fig. 8(i).

Based on the above tampering detection experiments, the proposed algorithm can be good to retain the information of the image as much as possible, including the tampering with all areas of the image. And adding or deleting objects could be well detected. It is much better than Ref. [16] which only considers the pixels in inscribed image, while totally ignoring the information outside the inscribed circle. So Ref. [16] will lose the ability of tampering detection when the four corners outside the incircle under malicious tampering, which means missed and false detection. In addition, compared with Ref. [17] which adopts circumcircle for ring partition to generate hash, the length of the hash values in this paper is shorter, which is only 64 bits. Thus, on the one hand, there is no increase in the length of the hash and ensure the distinction of algorithms. On the other hand, it can also be a certain save on the time cost of the algorithm, which means more efficient.

5. **Conclusions.** This paper proposed a robust color image perceptual hashing algorithm using interpolation mapping and NMF. The conclusions are as follows:

(1) The proposed interpolation mapping can map a rectangle image into a circular one and it retains the side information as much as possible;

(2) Dividing circular image into rings can resist arbitrary rotation;

(3) Conducting NMF on secondary image can reduce dimension, decrease complexity of hashing algorithm and improve detecting tamper capability;

(4) The proposed algorithm provides more comprehensive expressions of image content compared to Ref. [16]. When image side information under malicious tampering, this algorithm possesses better ability of tampering detection and reducing error detection

rate. Compared to Ref. [17], the proposed algorithm can retain image edge information and shorten hashing length.

Acknowledgment. This work is supported by the National Natural Science Foundation of China (No. 61363078), the Natural Science Foundation of Gansu Province of China (No. 1310RJYA004). The authors would like to thank the anonymous reviewers for their helpful comments and suggestions.

REFERENCES

[1] Z. Tang, X. Zhang, X. Li, et al, Robust image hashing with ring partition and invariant vector distance, *IEEE Trans. on Information Forensics and Security*, vol. 11, no. 1, pp. 200-214, 2016.

[2] X. Xing, Y. Zhu, Z. Mo, et al, A novel perceptual hashing for color images using a full quaternion representation, *KSII Transactions on Internet and Information Systems*, vol. 9, no. 12, pp. 5058-5072, 2015.

[3] R. Davarzani, S. Mozaffari and K. Yaghmaie, Perceptual image hashing using center-symmetric local binary patterns, *Multimedia Tools and Applications*, vol. 75, no. 8, pp. 4639-4667, 2016.

[4] Y. Zhao, S. Z. Wang, H. Yao, et al, Perceptual image hashing based on conformal mapping and Zernike moments, *Journal of Applied Sciences*, vol. 30, no. 1, pp. 75-81, 2012.

[5] H.X. Wang and B.X. Yin, Perceptual hashing-based robust image authentication scheme for wireless multimedia sensor networks, *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID. 791814, 9 pages, 2013.

[6] Y. Chen, W. Yu and J. Feng, Robust image hashing using invariants of Tchebichef moments, *Optik-International Journal for Light and Electron Optics*, vol. 125, no. 19, pp. 5582-5587, 2014.

[7] H. Zhang, *Research on benchmark and algorithm of image perceptual hashing*, PH.D. Thesis, Harbin: Harbin Institute of Technology, China, 2009.

[8] Z. Tang, X. Zhang and S. Zhang, Robust perceptual image hashing based on ring partition and NMF, *IEEE Transactions on Knowledge and Data Engineering*, vol. 1, no. 1, pp. 376-390, 2013.

[9] Y. Lu, Z. Lai, Y. Xu, et al, Projective robust nonnegative factorization, *Information Sciences*, vol. 364, pp. 16-32, 2016.

[10] L. Ghouti, Robust perceptual color image hashing using quaternion singular value decomposition, *Proc. of the 2014 IEEE International Conference on Acoustics, Speech & Signal Processing*, pp. 3794-3798, 2014.

[11] R. Sun, X.X. Yan and J. Gao, A perceptual image hashing method via SIFT and PCA, *Journal of Circuits and Systems*, vol. 18, no. 1, pp. 274-278, 2013.

[12] Z. Tang, F. Yang, L. Huang, et al, Robust image hashing with dominant DCT coefficients, *Optik-International Journal for Light and Electron Optics*, vol. 125, no. 18, pp. 5102-5107, 2014.

[13] Z.J. Tang, X.Q. Zhang, Y.M. Dai, et al, Perceptual image hashing using local entropies and DWT, *The Imaging Science Journal*, vol. 61, no. 2, pp. 241-251, 2013.

[14] Y. Lei, Y. Wang and J. Huang, Robust image hash in Radon transform domain for authentication, *Signal Processing: Image Communication*, vol. 26, no. 6, pp. 280-288, 2011.

[15] J. Ouyang, G. Coatrieux and H. Shu, Robust hashing for image authentication using quaternion DFT and log-polar transform, *Digital Signal Processing*, vol. 41, pp. 98-109, 2015.

[16] Z. Tang, X. Zhang, S. Zhang, Robust perceptual image hashing based on ring partition and NMF, *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 3, pp. 711-724, 2014.

[17] S. Tabatabaei and C. Ruland, The analysis of an NMF-based perceptual image hashing scheme, *Proc. of the 2013 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, pp. 108-112, 2013.

[18] Y. Zhao, *Image hashing and content authentication based on Zernike moments*, PH.D. Thesis, Shanghai: Shanghai University, China, 2013.

[19] L.Y. Huang, *Image hashing algorithms resistant to rotation*, MS.D. Thesis, Guilin: Guangxi Normal University, China, 2014.

[20] D.D. Lee and H.S. Seung, Algorithms for non-negative matrix factorization, *Proc. of the 2000 Advances in Neural Information Processing Systems (NIPS 2000)*, pp. 556-562, 2000.

[21] *USC-SIPI Image Database*, http://sipi.usc.edu/database/, Feb. 2007.

[22] *Ground Truth Database*, http://www.cs.washington.edu/groundtruth/, May. 2008.

[23] *James Z. Wang Research Group Database*, http://wang.ist.psu.edu/docs/ related.shtml, 2001.