EURASIP Journal on
Advances in Signal Processing
a SpringerOpen Journal

RESEARCH Open Access

Block-based image hashing with restricted blocking strategy for rotational robustness

Shijun Xiang[1]* and Jianquan Yang[2]

Abstract

Image hashing is a potential solution for image content authentication (a desired image hashing algorithm should be robust to common image processing operations and various geometric distortions). In the literature, researchers pay more attention to block-based image hashing algorithms due to their robustness to common image processing operations (such as lossy compression, low-pass filtering, and additive noise). However, the block-based hashing strategies are sensitive to rotation processing operations. This indicates that the robustness of the block-based hashing methods against rotation operations is an important issue. Towards this direction, in this article we propose a restricted blocking strategy by investigating effect of two rotation operations on an image and its blocks in both theoretical and experimental ways. Furthermore, we apply the proposed blocking strategy for the recently reported non-negative matrix factorization (NMF) hashing. Experimental results have demonstrated the validity of the block-based hashing algorithms with restricted blocking strategy for rotation operations.

Keywords: image hashing, non-negative matrix factorization, rotation, restricted random blocking

1. Introduction

With the development of the Internet and multimedia processing techniques, more and more digital media products become available through different online services and easy to distribute illegal copies. Recently, multimedia hashing functions [1,2] have been introduced as a potential solution for tracing the unauthorized use of digital media files since the traditional cryptography hash functions (such as MD5, SHA-1) cannot satisfy the requirements of multimedia content authentication because the cryptographic hash is sensitive to every single bit of input. In the literature, the techniques used for image authentication can be classified into two categories: (1) watermark based [3-6] and (2) media hash based [7,8]. The main difference between a watermark (robust [3], reversible [4], fragile [5] and semi-fragile [6]) and a hash is that the embedding process of the former requires the content of the media to change. Robustness of media hashing is a desired aspect. Robustness means that the hash should be resistant to content-preserving signal processing operations, e.g., image hashing should be insensitive to those common geometric deformation, lossy compression and filtering operations, which do distort the image but preserve its visual quality.

Media hashing can be broadly classified into audio hashing [9,10], video hashing [11,12] and image hashing [7,8,13-21] according to the diversity of media dimensionality space. In this article, we are focusing on image hashing. In the literature, there are a lot robust image hash functions. In [13], Fridrich and Goljan addressed a robust image hash for tamper control problem by mapping image blocks into key-based template. In [14], a robust image hash was used for indexing and database searching by using the statistic property of wavelet coefficients of image block. Perceptual image hashing was also used for content-dependent key generation in video watermarking [15]. The hash methods proposed in [13,14] were aiming to coping with common image processing operations. With another consideration of coping with geometric distortions, some researchers presented a few special image hash functions, such as in [16-21]]. In [16], the authors introduced an iterative geometric image hash method by quantizing the low-frequency components of an image into a binary image, which is further filtered by iterative filter in order to obtain a stable geometric shape to generate the hash with resistance to geometric distortion.

* Correspondence: xiangshijun@gmail.com
[1]School of Information Science and Technology, Jinan University, Guangzhou 510632, China
Full list of author information is available at the end of the article

In [17], the authors proposed two robust hashing schemes based on the invariance of Fourier-Mellin transform to affine transform, and later the schemes were improved by considering both security and robustness [18]. In [19], Lu and Hsu addressed a mesh-based image hashing method by using the mesh insensitivity to geometric distortions. Monga and Mihçak addressed a robust and secure image hashing function in [20], which provides robustness to affine transforms since the effect of geometric attacks on image blocks in the spatial domain manifests (approximately) as independent and identically distributed noise on non-negative matrix factorization vectors. By using the insensitivity of histogram in shape to geometric attacks, Xiang et al. proposed a histogram-based image hashing algorithm for various geometric distortions in [21]. In [5], a key-dependent JPEG2000-based robust hashing method was addressed for secure image authentication. Considering various attacks, Liu et al. [6] introduced Fast Johnson-Lindenstrauss Transform and content-based fingerprint, to combine different features together.

From the above introduction, we can see that the strategy to divide an image into blocks for hashing is often used (such as [13,14,20]). Usually, block-based image hashing algorithms can provide an inherent ability to tamper control problem and are robust to common image processing operations. However, image block-based hash functions are very sensitive to rotation operations since the rotation will make the content difference between an image block and its rotated versions. Towards this problem, in this article we investigate the effect of rotation operations on an image and its blocks. Our motivation is to find the effect and then propose a new blocking strategy to improve the performance of the block-based image hashing algorithm for rotation operations. There are two kinds of rotation modes: loose based and crop based. The main difference between a loose rotation and a crop rotation is that output images of the former have a bigger size than the rotated image while the later remains the size by cropping the boundaries. By analyzing the two modes of rotation operations in mathematical way, we propose a restricted randomized blocking strategy to eliminate the effect of rotation. The basic idea is to extract the central content of an image for the use of a block-based hashing. In order to measure the effectiveness of the proposed blocking strategy, we take non-negative matrix factorization (NMF) hashing algorithm proposed in [20] as an example of block-based hashing algorithms to report experimental results. Simulation results show that the hashing algorithm with the proposed blocking strategy can provide a stronger robustness to the two rotational operations.

The remainder of this article is organized as follows. In the following section, we describe the computation process of a NMF hashing algorithm. This is followed by a detailed mathematical analysis on the effect of two image rotation modes on images. By using the new blocking method, we then test the robustness performance of the NMF hashing algorithm for two image rotation operations. Finally, we draw the conclusions.

2. NMF-based image hashing

2.1. NMF

The NMF is a Matrix decomposition method [22]. It is restricted by the conditions that in the Matrix all elements are nonnegative. The mathematical description is addressed as follows:

Given a $m \times n$ nonnegative matrices $\mathbf{V}$, looking for nonnegative factor matrix $\mathbf{W}$ and $\mathbf{H}$, making

$$\mathbf{V} \approx \mathbf{WH}(\mathbf{W} \in R^{m\times r}, \mathbf{H} \in R^{r\times n}), \tag{1}$$

Here, each column in $\mathbf{W}$ can be regarded as a vector. Therefore, each column in $\mathbf{V}$ is the linear combination of the base vectors. NMF is an approximation procedure to the original matrix in a distance metric. In the NMF literature, two popular cost functions have been studied. The first is the classical Euclidean distance, given by

$$\Theta_E(\mathbf{W},\mathbf{H}) \equiv \left(\sum_{j=1}^{n} ||v_j - \mathbf{W}h_j||_2^2\right)^{\frac{1}{2}} = ||\mathbf{V} - \mathbf{WH}||, \tag{2}$$

Another measure usually used in practice is K-L divergence (Kullback-Leibler divergence)

$$\Theta_D(\mathbf{V}||\mathbf{WH}) \equiv \sum_{i=1}^{m}\sum_{j=1}^{n}\left(V_{ij}\log\frac{V_{ij}}{\sum_{l=1}^{r} W_{il}H_{lj}} - V_{ij} + [WH]_{ij}\right), \tag{3}$$

The above measure is known as the generalized Kullback-Leibler (KL) divergence. The NMF's goal is to minimize the distance between matrix $\mathbf{V}$ and $\mathbf{WH}$. In this article, we choose Euclidean distance as the objective function of the NMF. Use the following iteration formulas [16], to obtain the matrix $\mathbf{W}$ and $\mathbf{H}$ until the $\Theta_E(\mathbf{W}, \mathbf{H})$ value reaches a local minimum:

$$H_{aj} \leftarrow H_{aj}\frac{[W^TV]_{aj}}{[W^TWH]_{aj}}, W_{ia} \leftarrow W_{ia}\frac{[VH^T]_{ia}}{[WHH^T]_{ia}}, \tag{4}$$

2.2. NMF-NMF-SQ hashing algorithm

Figure 1 shows the calculation process of a NMF-NMF-SQ hashing algorithm proposed in [20], described as follows:

1) Given an image, using the private key k_1 to pseudorandomly select sub-images A_i,($A_i \in R^{m\times m}$, $1 \le i \le p$).

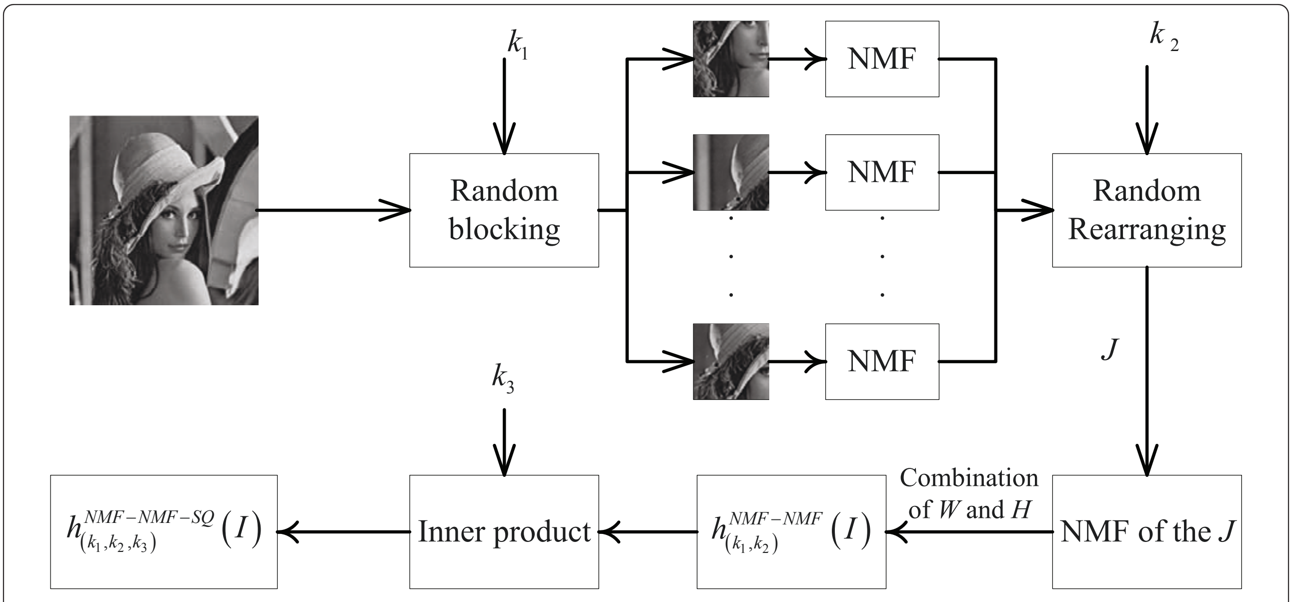

k_1
Random blocking
NMF
NMF
NMF
k_2
Random Rearranging
J
k_3
$h_{(k_1,k_2,k_3)}^{NMF-NMF-SQ}(I)$
Inner product
$h_{(k_1,k_2)}^{NMF-NMF}(I)$
Combination of W and H
NMF of the J

Figure 1 Block diagram of NMF-NMF-SQ algorithm.

2) Obtain the NMF of each sub-image:

$$A_i \approx W_i F_i^T, (W_i, F_i \in R^{m \times r_1}), \tag{5}$$

where r_1, ($r_1 \ll m$) is the rank. In this way, we get $2p$ matrix in size $m \times r_1$.

3) According to the key k_2, randomly rearrange these matrixes to get a matrix $\mathbf{J}$ in size $m \times 2pr_1$.

4) Compute the NMF of $\mathbf{J}$ on the rank r_2,($r_2 \ll$ min (m, $2pr_1$))

$$\mathbf{J} \approx \mathbf{WH}(\mathbf{W} \in R^{m \times r_2}, \mathbf{H} \in R^{r_2 \times 2pr_1}), \tag{6}$$

In such a way we obtain a $m \times r_2$ dimensional matrix $\mathbf{W}$ and a $r_2 \times 2pr_1$ dimensional matrix $\mathbf{H}$.

5) Making rows of $\mathbf{W}$ and columns of $\mathbf{H}$ in series to get a vector $h_{(k_1,k_2)}^{\text{NMF - NMF}}(I)$ in length N. Under the control of the secret key k_3, obtaining a weight vector sets $\{t_i\}_{i=1}^{M}, (M \ll N, t_i \in R^N)$, making the inner product between each weight vector $\{t_i\}$ and $h_{(k_1,k_2)}^{\text{NMFNMF}}(I)$ to obtain hash vector of the NMF-NMF-SQ algorithm: (In the following equation the expression $\langle a, b \rangle$ indicates the inner product between a and b).

$$h_{(k_1,k_2,k_3)}^{\text{NMF - NMF - SQ}}(I) = \{\langle h_{(k_1,k_2)}^{\text{NMF - NMF}}(I), t_1 \rangle, \ldots, \langle h_{(k_1,k_2)}^{\text{NMF - NMF}}(I), t_M \rangle\}, \tag{7}$$

The above hash vector $h_{(k_1,k_2,k_3)}^{\text{NMF - NMF - SQ}}(I)$ was not quantized. Therefore, each element in the vector is a real number. Similarity of the two hash vectors was measured by using Euclidean distance.

The robustness principle of the NMF hashing algorithm proposed in [20] can be summarized as follows: (1) Divide an image into blocks and then calculate the hash, in such a way that the hash is able to trace tampering and locate; (2) The hash value is a low rank decomposition by using NMF mathematical method after an image is divided into blocks,[a] therefore the algorithm has a good robustness for lossy compression, low-pass filtering and additive noise operations; (3) Since the hash is computed after an image size normalization step, the hash value is resistant to cropping and scaling operations. However, the algorithm is sensitive to a rotation manipulation since it will modify the content of a block.

3. Restricted blocking strategy for rotation

In this article, we observe the influence of two rotation operations on the NMF image hashing algorithm [20], that is, an image rotation operation will modify the content of an image block in two aspects: (1) pixel magnitude distortion due to the interpolation in the rotation [23] and (2) phase change. The NMF hashing algorithm [20] can overcome the magnitude distortion since the distortion in amplitude can be taken as an additive noise, but it is very sensitive to the phase change due to the rotation because the image block in content has been modified. The bigger rotation angle is performed, the more distortion in the block will be introduced. Towards the effect, in this section we will analyze the impact of a rotation processing operation on an image and its blocks in both theoretical and experimental ways. Furthermore, we propose a restricted random blocking strategy for the algorithm [20] so as to improve the rotational robustness while remaining its resistance to other attacks.

3.1. An image after rotation

There are two different modes of image rotation processing operations: '*loose*' based and '*crop*' based [24]. For the *loose*-based rotation mode, output images have a bigger size but the original image content in size remains unchanged; In *crop*-based rotation mode, output images have the same size as input image, but include only the central portion of the rotated image. The influence factors of the two rotation modes on an image are described as follows.

3.1.1. Rotation with the loose mode

We can see that under this mode of rotation, output images have a bigger size than the rotated image. As shown in Figure 2, two resulted images with different angles plotted in Figure 2b,c have a bigger size than the original one as shown in Figure 2a. The basic reason is that, after the rotation some redundant pixels (black regions with zero-value pixels) are padded in four homogeneous areas of the rotated image. These homogeneous regions can be processed by using line detection techniques [25]. It is worth noting that Figure 2e,f in content is more rich than the original image after a size normalization. The size normalization operation in reference [20] was applied to deal with all images from the same source to the same size so that the images can be blocked for hashing. In referring to Figure 2, we can figure out that the loose rotation operation will make a serious affection on the hashing algorithm [20] since all image blocks in content will be modified due to the phase distortion.

In order to eliminate the effect of the padded pixels (caused by the loose rotation) on image blocks, our strategy is to apply only the central content of an candidate image for block-based hashing, such as the circled region marked in Figure 2d. In such a way, we can avoid the effect of the resulted redundant pixels. For the rotated images as plotted in Figure 2e,f, only the central part in the blue circle is chosen for hashing.

For a clear description, in this article we denote the circle radius in Figure 2d as the radius of Effective Block Region (EBR), in length *R*. According to the principle of geometry mathematics, the *R* value can be derived from the following Equations (8) and (9).

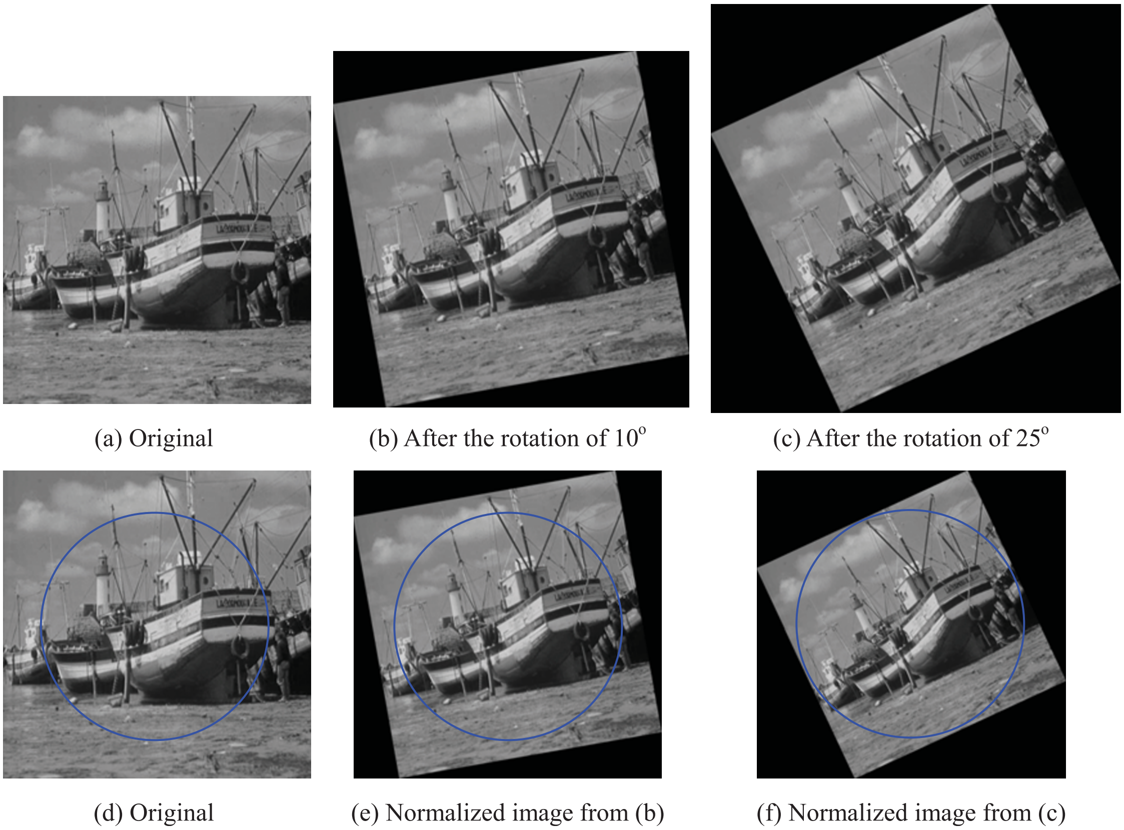

(a) Original
(b) After the rotation of 10°
(c) After the rotation of 25°
(d) Original
(e) Normalized image from (b)
(f) Normalized image from (c)

Figure 2 Effect of the "loose" mode: (a) original image, (b) and (c) rotated images with different angles. The subfigures **(d)**, **(e)** and **(f)** are the size-normalized versions of the images (a), (b) and (c) by referring to the original image in size.

Denote the original image as □*ABCD*, which is rotated by using the "loose" mode with the angle θ, and then be normalized to the same size as the original one. As shown in Figure 3, the square □*EFGH* is the rotated version of □*ABCD* with the loose mode. In this case, the difference between □*ABCD* and □*EFGH* indicates the resulted redundant pixels. In referring to Figure 3, we have the following the geometric relationships:

$$\begin{cases} \overline{EF} \cdot \cos\theta + \overline{FG} \cdot \sin\theta = \overline{AB} \\ \overline{EF} \cdot \sin\theta + \overline{FG} \cdot \cos\theta = \overline{BC}, \end{cases} \tag{8}$$

$$\begin{cases} \overline{EF} = \dfrac{\overline{AB} \cdot \cos\theta - \overline{BC} \cdot \sin\theta}{cos(2\theta)} \\ \overline{EF} = \dfrac{\overline{BC} \cdot \cos\theta - \overline{AB} \cdot \sin\theta}{cos(2\theta)}, \end{cases} \tag{9}$$

So $R = \frac{1}{2}\overline{FG}$ since the line $\overline{FG}$ in length is shorter than $\overline{EF}$.

We can see from Figure 3 and the R expression that for overcoming the impact of the redundant pixels caused by the rotation, we should select the central content of an image for block-based hashing. For the different rotation angle, the central content is different. Supposed the rotation angle θ is between zero and 45° (for other rotation angles, the analysis is similar). The bigger rotation angle is, the EBR radius (R) should be smaller so as to guarantee the block-based hash value resistant to the loose rotation operation.

3.1.2. Rotation with the crop mode

In order to better depict the effect of the crop rotation, here we adopt the well-known image '*Lena*' as another example image. From Figure 4, we can observe the effect of the crop rotation on the image, that is, output images have the same size as input image and include only the central portion of the rotated image. Under the rotation, part of the content is cropped (replaced by zero-value pixels). For different rotation angles, the cropped pixels (replaced by zero-value pixels) in number are different, corresponding to the content in the white circle of the subplots in Figure 4b,c.

Considering the effect of the rotation mode, our strategy is to extract the region as shown in the circle in Figure 5 for blocking. Suppose that the square □*ABCD* denotes the original image, then the square □*EFGH* is the one rotated. According to our analysis, the circle is the region computed for blocking in such a way that a block-based hashing can avoid the effect of those pixels (to be cut and then filled by zero-value pixels).

3.2. An block after rotation

In the Section 1, we have analyzed the effect of rotation with two different modes on an image. Furthermore, in this section we are going to investigate the effect of the two rotation processing operations on an image block.

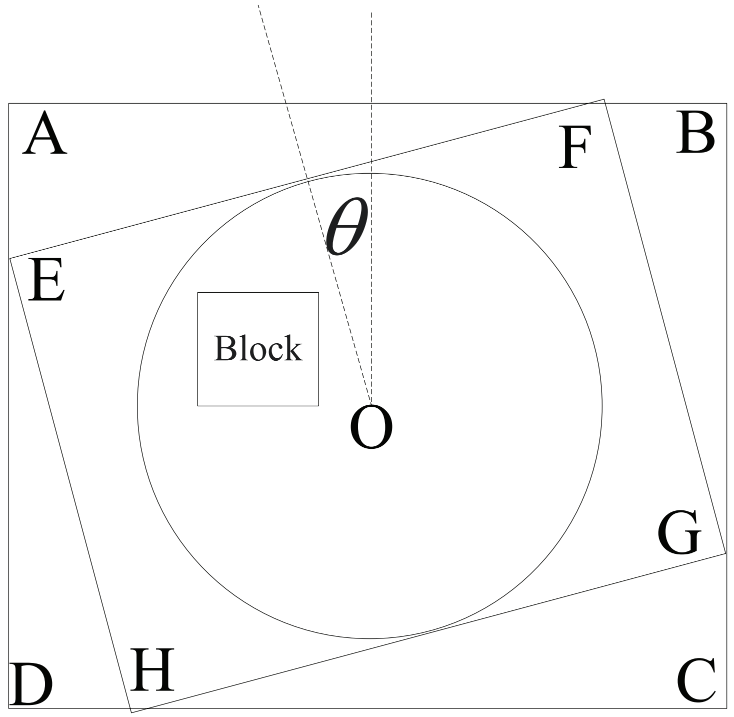


Figure 3 Effective block region under the loose rotation mode (see the circle).

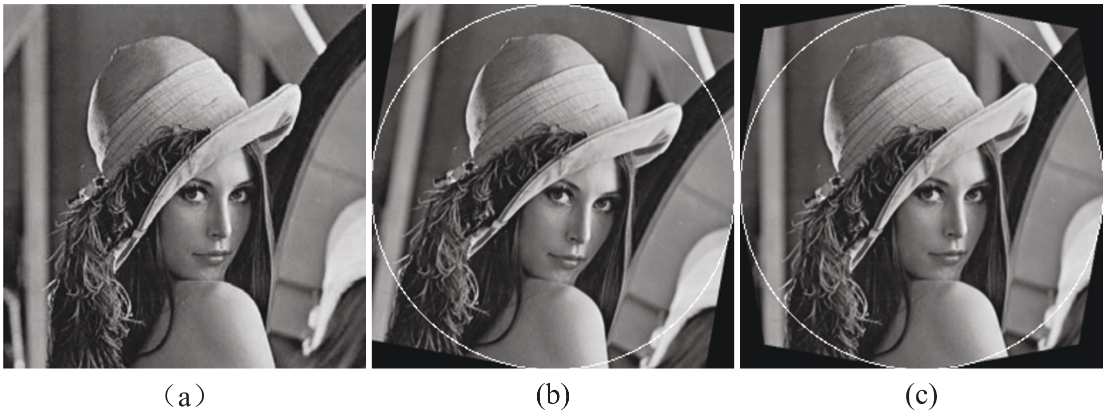


Figure 4 Effect of the 'crop' rotation mode: (a) the original image, (b) the image rotated under the crop mode, (c) an image rotated back from (b) (in this subplot, the black pixels indicate the location of the filled (or cut) pixels).

From the above analysis regarding the crop rotation mode, we have known that the rotation operation modifies the phase of pixels in the EBR (The amplitude distortion due to the interpolation is minor [23]). Therefore, there are existing public pixels before and after the rotation. A public pixel means that a pixel is still fallen into the same block under the rotation. It is worth noting that the ratio of these public pixels to the pixels in a block has an important role for the robustness of the NMF-based hashing algorithm [20]. This has been fully proven in Section 4 with extensive testing.

In order to find a better way to block an image for hashing, in theoretical way we are going to measure the ratio of public pixels in an image block after a rotation operation. The image blocks can be divided into two categories: (1) the image center in the block and 2) the center not in the block. The effect of the rotation on a block is respectively discussed as follows.

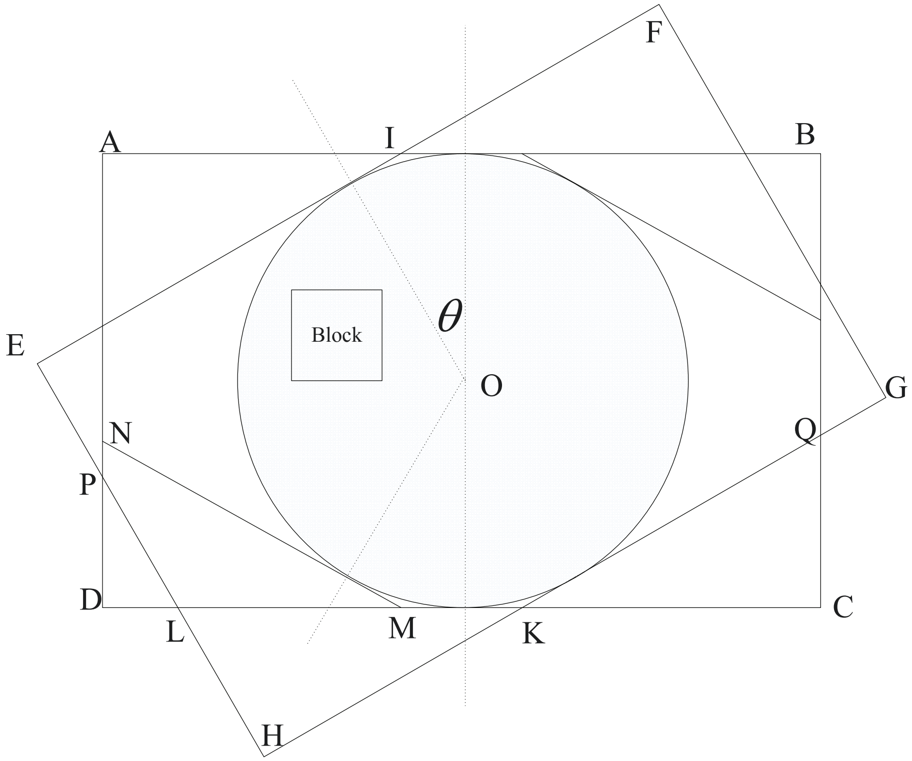


Figure 5 Effective block region under the *crop* rotation mode (see the circle).

3.2.1. Case 1: image center in the block

In Figure 6, the point O denotes the center of the EBR of an image. Suppose $\square ABCD$ is an image block, after image rotation of $\theta°$ the pixels in the $\square ABCD$ will be shifted to the $\square EFGH$. For the block $\square ABCD$, the ratio of public pixels against the block pixels after the rotation is equal to the ratio of the polygon $P'KN'GLD$ to the block in area ($\overline{AD}$ crosses $\overline{EF}$ at P', $\overline{OQ}$ crosses $\overline{EF}$ at P, $\overline{FG}$ crosses $\overline{AB}$ at N', $\overline{OT}$ crosses $\overline{AB}$ at N). From the expressions: $\overline{KP} = \overline{FP} - \overline{FK}$, $\overline{KP} = \overline{FP} - \overline{FK}$, $\overline{AK} = \overline{FK}$ and $\overline{AN} = \overline{FP}$, we have $\overline{KN} = \overline{KP}$. As a result, we conclude that the line $\overline{OK}$ is the bisector of the angle $\angle PON$. Similarly, we can prove OL is $\angle PON$'s bisector. According to the geometric relations $\overline{AK} = \overline{AN} - \overline{KN}$ and $\overline{KN} = \overline{ON} \cdot \tan\frac{\theta}{2}$, the area of the triangle $\Delta\ AKP'$ is

$$S_{AKP'} = \frac{1}{2} \cdot |\overline{AK}|^2 \cdot \tan\theta, \tag{10}$$

Similarly, we have:

$$S_{LGM} = \frac{1}{2} \cdot |\overline{LG}|^2 \cdot \tan\theta, \tag{11}$$

where $\overline{LG} = \overline{UG} - \overline{UL}$ and $\overline{UL} = \overline{UO} \cdot \tan\frac{\theta}{2}$. The area of trapezoidal $AN'MD$ is:

$$\begin{aligned} S_{AN'MD} &= \frac{1}{2}\left(\overline{AK} + \frac{\overline{KF}}{\cos\theta} + \frac{\overline{LG}}{\cos\theta}\right) \cdot \overline{AD} \\ &= \frac{1}{2}\left(\overline{AK} + \overline{LG}\right)\left(1 + \frac{1}{\cos\theta}\right) \cdot \overline{AD} \end{aligned} \tag{12}$$

Therefore, the area of hexagon $P'KN'GLD$ is:

$$S_{P'KN'GLD} = S_{AN'MD} - S_{AKP'} - S_{LGM}, \tag{13}$$

Suppose that the distance of the block center to the image center O is R_1, the block is a square in size $a \times a$, then the overlapped area (public pixels) between $\square ABCD$ and $\square EFGH$ can be computed as:

$$S_{PKNGLD} = \frac{1}{2}(\overline{AK} + \overline{LG})\left(1 + \frac{1}{\cos\theta}\right) \cdot a - \frac{1}{2} \cdot |(\overline{AK}|^2 + \overline{LG}|^2) \cdot \tan\theta, \tag{14}$$

where : $\overline{AK} = \frac{a}{2} - (R_1 + \frac{a}{2}) \cdot \tan\frac{\theta}{2}$, $\overline{LG} = \frac{a}{2} - (R_1 - \frac{a}{2}) \cdot \tan\frac{a}{2}$, when $R_1 > \frac{a}{2}$.

3.2.2. Case 2: image center not in the block

We can see from Figure 7 that in this case, the overlapped region is the octagon $VILSQNUT$, which is:

$$S_{VILSQNUT} = S_{ALMD} - S_{AiV} - S_{NGM} - 2S_{SQG}, \tag{15}$$

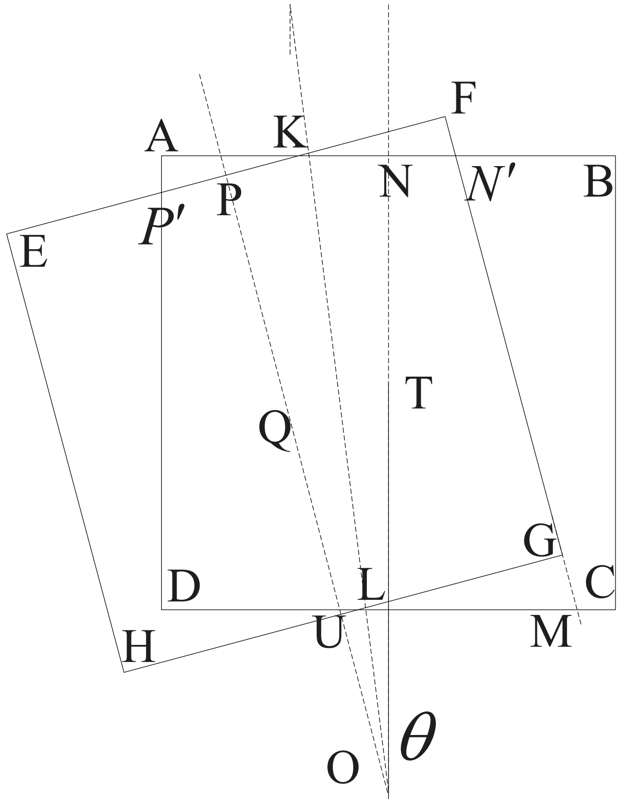


Figure 6 The case that a block does not contain the central point of the image.

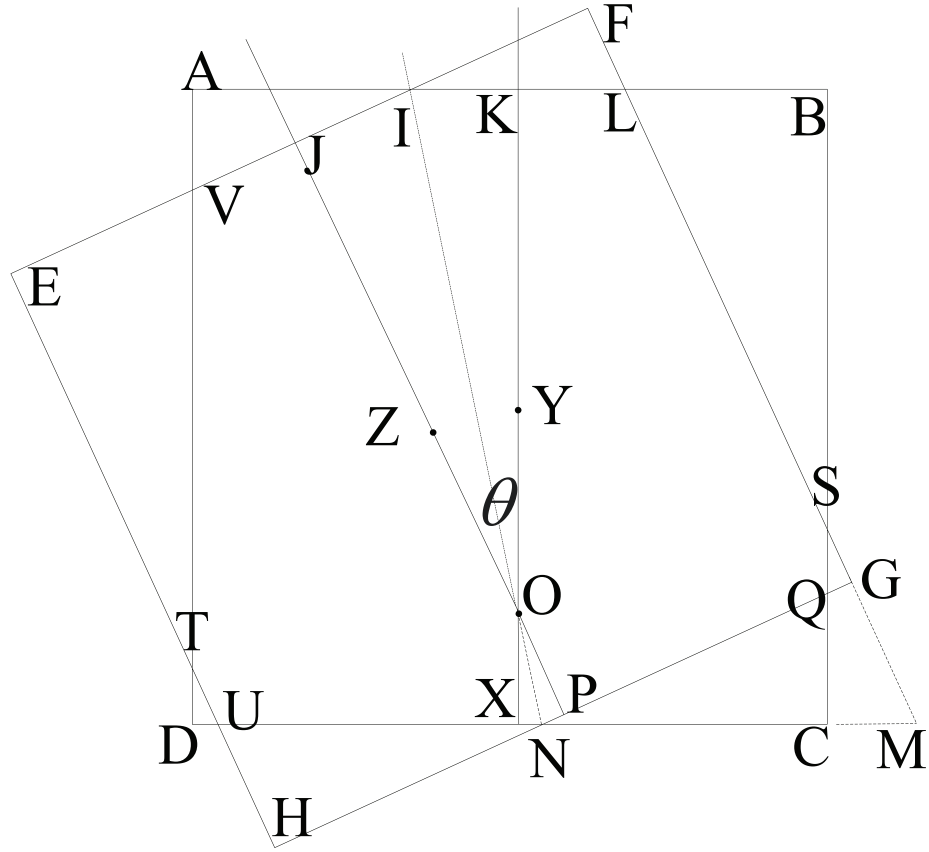


Figure 7 The case that a block contains the center of the image.

According to the geometric expressions: $\overline{AI} = \overline{IF}\overline{AI} = \overline{IF}$, we have $\overline{IK} = \overline{IJ}$. So, we conclude that the line $\overline{OI}$ is the bisector of the angle $\angle JOK$.

Similarly, we can prove that the line $\overline{ON}$ is $\angle XOP$'s bisector. So, we have

$$\begin{cases} \overline{AK} = \overline{OK} \cdot \tan \frac{\theta}{2} \\ \overline{NP} = \overline{OP} \cdot \tan \frac{\theta}{2}, \end{cases} \tag{16}$$

$$S_{AIV} = \frac{1}{2} \cdot |\overline{AI}|^2 \cdot \tan\theta, \tag{17}$$

where $\overline{AI} = \overline{AK} - \overline{IK}$. Similarly, we have

$$S_{NGM} = \frac{1}{2} \cdot |\overline{NG}|^2 \cdot \tan\theta, \tag{18}$$

where $NG = NP + PG$. And

$$S_{SQG} = \frac{1}{2} \cdot |\overline{SG}|^2 \cdot \tan\theta, \tag{19}$$

where $\overline{SG} = \overline{FG} - \overline{FL} - \overline{LS}$, $\overline{FL} = \overline{AI} \cdot \tan\theta$, and $\overline{LS} = \frac{\overline{LB}}{\sin\theta} = \frac{1}{\sin\theta}\left[\overline{AB} - \overline{AI}\left(1 + \frac{1}{\cos\theta}\right)\right]$.

At the same time, we have

$$S_{ALMD} = \frac{1}{2}(\overline{AL} + \overline{MD}) \cdot \overline{AD}, \tag{20}$$

where $\overline{AL} = \overline{AI}\left(1 + \frac{1}{\cos\theta}\right)$, $\overline{MD} = \overline{DC} + \overline{CM}$, $\overline{CM} = \frac{\overline{NG}}{\cos\theta} - \overline{XC} + \overline{NP}$.

From the above equations, we can compute the overlapped area (public pixels) as:

$$\begin{aligned} S_{VILSQNUT} &= S_{ALMD} - S_{AIV} - S_{NGM} - 2S_{SQG} \\ &= \frac{1}{2}(\overline{AL} + \overline{MD}) \cdot \overline{AD} - \frac{1}{2}\tan\theta(|\overline{AI}|^2 + |\overline{NG}|^2 + 2|\overline{SG}|^2), \end{aligned} \tag{21}$$

where the length of the lines can be calculated from Equations (17), (18), (19), and (20).

Referring to Figures 6 and 7, from the above theoretical analysis results formulated in Equations (14) and (21) we can conclude that, the ratio of public pixels after the rotation is related to the distance between the block center and the image center, the block size and the rotation angle. The smaller distance between a block and the image center is, or the smaller the rotation angle is, or the larger the block size is, so the bigger the ratio of public pixels after the rotation is, as a result the stronger rotational robustness can be achieved from a block-based hashing algorithm. The above mathematical analysis results regarding the ratio of public pixels against the rotation is beneficial to improving the rotational robustness of those block-based hashing algorithms. The strategy is to choose a desired region (the central part of an image), and then divide the region into blocks in an ideal size. The region and the block in size can be computed in advance by referring to the rotation angle that an image may suffer from. In such a way, the effect of the rotation operations will be significantly reduced. Especially, the blocking strategy is useful for those image hashing schemes based on local statistical characteristics of an image, such as the NMF-based hashing algorithm proposed in [20]. For an image block, the more public pixels are staying in this block after a rotation operation, the better the statistical characteristics will be kept. In this article, we denote the blocking strategy as *Restricted Blocking Strategy*.

4. Experimental results

In order to measure the effectiveness of the proposed blocking strategy, we apply the blocking strategy for the NMF-NMF-SQ hashing algorithm proposed in [20] to estimate its contribution for rotational robustness. The testing results are reported as below.

In this section, we tested the performance of the NMF-NMF-SQ algorithm with the proposed blocking strategy. The parameters are set as: $p = 10$, $m = 100$, $r_1 = 1$, $r_2 = 1$, $M = 64$. The test data set is composed of four hundred 256 × 256 grey images, each image rotated in both loose and crop modes at the angle of 4, 8, 12, and 16°. Rotational robustness performance of the hashing algorithm (with the restricted blocking strategy) against the algorithm [20] (without the restricted blocking strategy) is as follows.

4.1. Robustness to the *loose* rotation mode

When the block radius is fixed as 100 (pixels), we can see from the ROC curves (Receiver Operation Characteristic) as shown in Figure 8 that, the ROC curves of the NMF hashing with the new blocking strategy are always on the below of those corresponding curves calculated from the algorithm [20]. The reason is that the restricted blocking method has better avoided the effect of the rotation operations. Especially, for a bigger rotation angle, the more robustness bonus for the rotation is obtained from the new blocking strategy. This indicates that the restricted blocking strategy is effective to improve the robustness to the loose rotation.

4.2. Robustness to the *crop* rotation mode

When the block radius is fixed as 128 (pixels), the ROC curves are plotted in Figure 9. For the rotation of 4°, the two ROC curves in Figure 9a almost stay together. As for other angles of rotation operations, the ROC curves of the hashing method using the restricted blocking strategy are always below those from the algorithm [20]. These results indicate that with new blocking strategy the NMF-based hashing algorithm can provide a better robustness to the crop rotation. When the rotation angle is bigger, the more robustness is received.

4.3. Influence of the distance between block center and image center

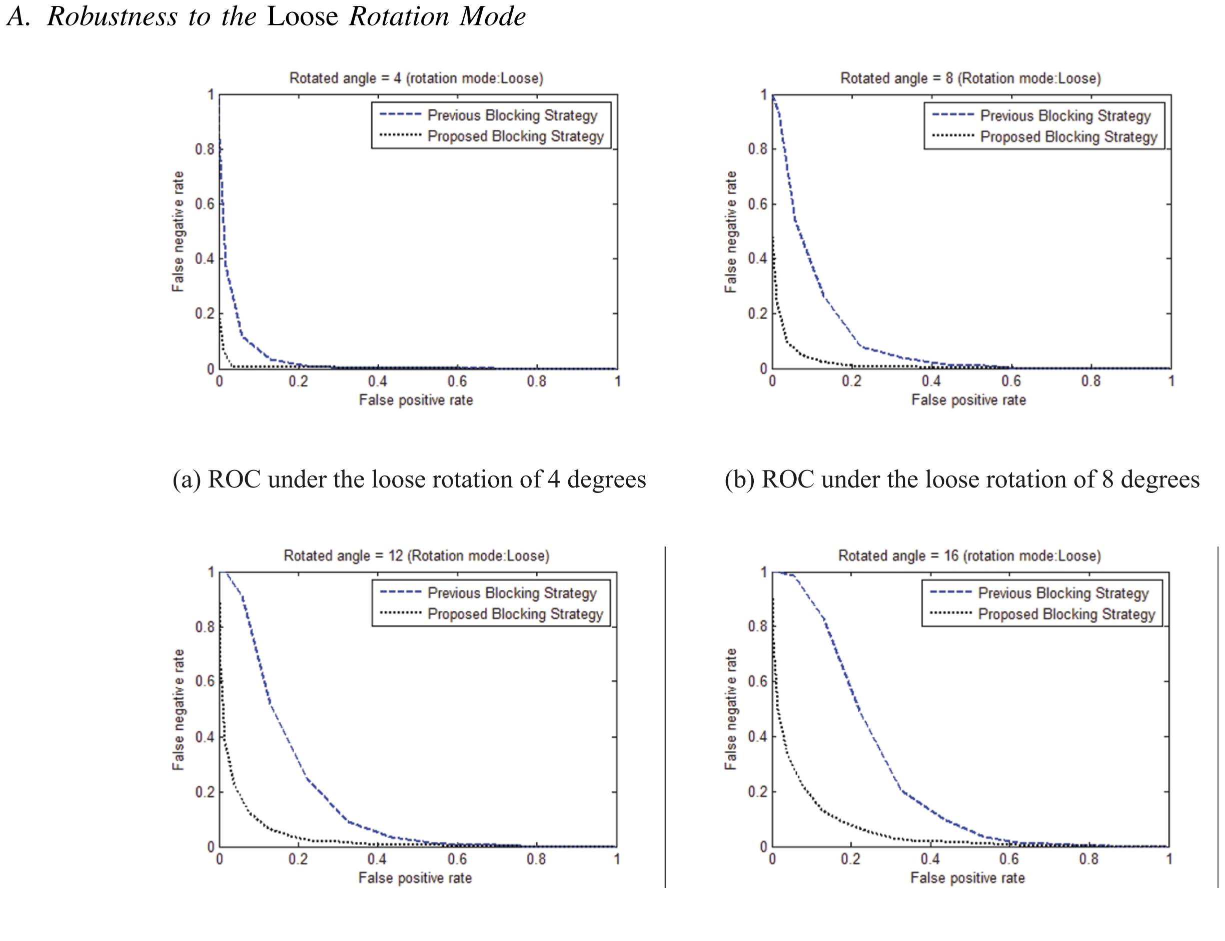
Corresponding to the analysis in Section 2, we have known that the ratio of public pixels to the pixels in a block is related to the distance between the block center and the image center, rotated angle and the block size used. Below, we modify the distance to measure its influence on the rotational robustness of the hashing algorithm with the restricted blocking strategy.

Note that the ratio of the public pixels in Figure 10 is represented as the percentage in curves. For the four hundred 256 × 256 test images, we perform a rotation operation of 8° with the crop mode. The block in size is 50 ×50. The effect of the distance on the ROC curve is plotted. From Figure 10, we can observe that the distance play an important role for the rotational robustness. When the distance is shorter, a block after the rotation can include more public pixels, so the robustness to the rotation is stronger. For example, the ratio of the public pixels is about 91.66% for the rotation of 8° while the distance is 20 (pixels). Also, we can see from this figure that a block with the shortest distance will provide stronger robustness (see the curve plotted with '□').

4.4. Influence of the block size

As analyzed in Section 2, the block size also plays a role on the ratio of public pixels in a block. Similarly, we perform a rotation operation on the four hundred 256 ×256 with the rotation angle of 8°. The distance between the block center and the image center is fixed to 60 pixels. With different block size, we have plotted their ROC curves as shown in Figure 11.

We can see from this figure that as the block size increases, the ratio of the public pixels increases. When the block size is 100×100, the algorithm with the new blocking strategy obtains the best robustness performance (the ratio of the public pixels is over 89%). It is worth noting that the robustness performance in the block size of 40 × 40 is better than that of 60 × 60, which can be explained as follows. Though the larger block size can increase the ratio of public pixels for the



(a) ROC under the loose rotation of 4 degrees

(b) ROC under the loose rotation of 8 degrees

(c) ROC under the loose rotation of 12 degrees

(d) ROC under the loose rotation of 16 degrees

Figure 8 ROC curves of the NMF hashing before and after the use of the new blocking strategy against the rotation with the loose mode.

rotational robustness improvement, in the testing we have applied the same rank for NMF decomposition in such a way that the bigger the block size is, the more feature information extracted from the NMF processing operation will be lost. As a result, the uniqueness will be reduced. Therefore, a rational block size is a trade-off between the robustness and uniqueness. For NMF-based hashing algorithm, we propose to apply the blocks of size 100×100 for hashing.

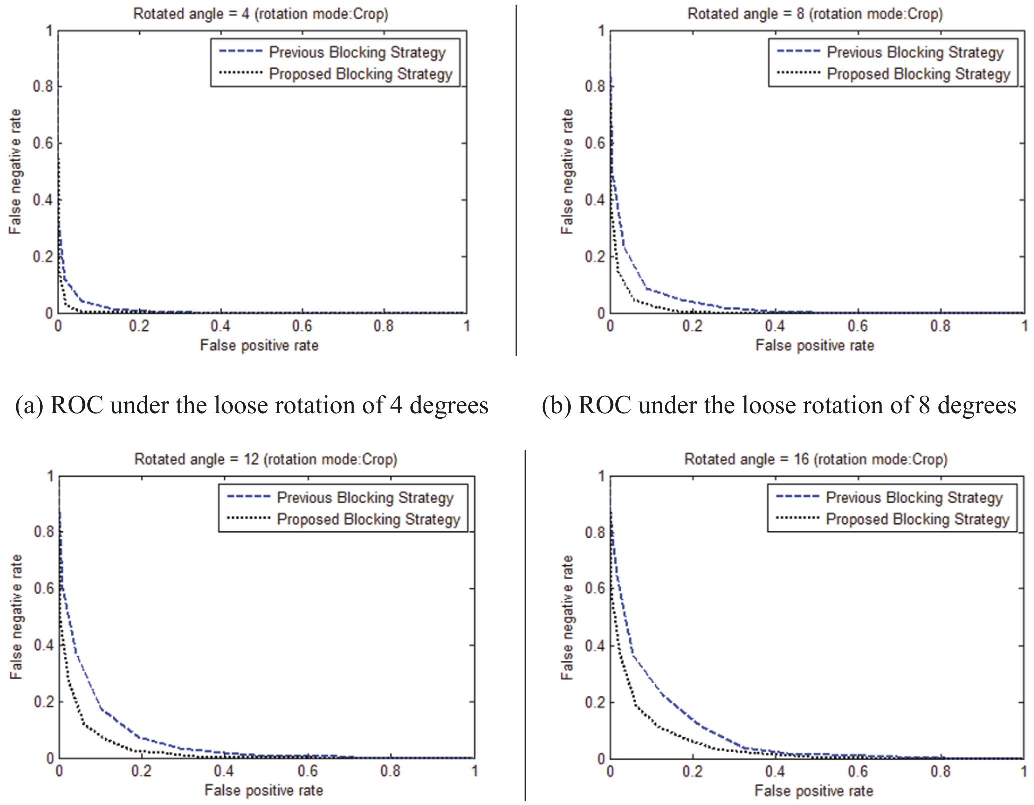
From the above experimental analysis, we can see that the NMF hashing algorithm with the restricted blocking strategy can provide stronger performance than the recently reported NMF hashing algorithm [20] in the presence of rotation with the loose and crop modes while keeping the robustness to other attacks.

5. Conclusions and remarks

In this article, we propose a restricted random blocking strategy to improve the robustness performance of block-based hashing algorithms for rotation operations. The contribution is described as follows:

1) We investigate the effect of the rotation operations with the two modes (loose and crop) on an image and its blocks in both theoretical and experimental ways. As a result, we propose a restricted blocking strategy so that the redundant pixels caused by the rotation can be excluded for blocking. Experimental testing shows that this blocking strategy can improve the stability of a block for the rotation.
2) We discuss the effect of the block size on the NMF hashing algorithm. The bigger block size is, the hashing algorithm is more resistant to rotation since a bigger block will include the more public pixels for the same rotation angle.
3) We perform a lot of testing to measure the hashing algorithm (with the restricted blocking method) against the previous NMF hashing algorithm [20].

B. Robustness to the Crop *Rotation Mode*



(a) ROC under the loose rotation of 4 degrees

(b) ROC under the loose rotation of 8 degrees

(c) ROC under the loose rotation of 12 degrees

(d) ROC under the loose rotation of 16 degrees

Figure 9 ROC curves of the NMF hashing before and after the use of the new blocking strategy against the rotation with the crop mode.

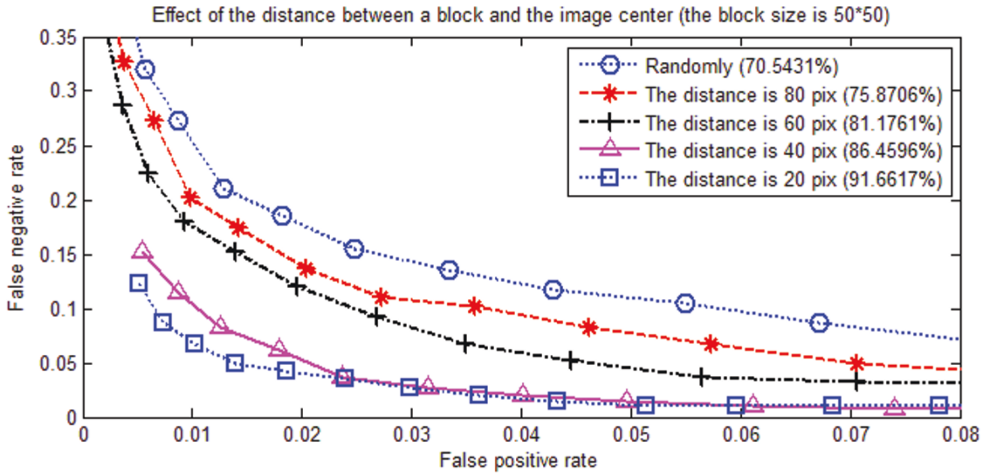


Figure 10 Effect of the distance between a block and the image center.

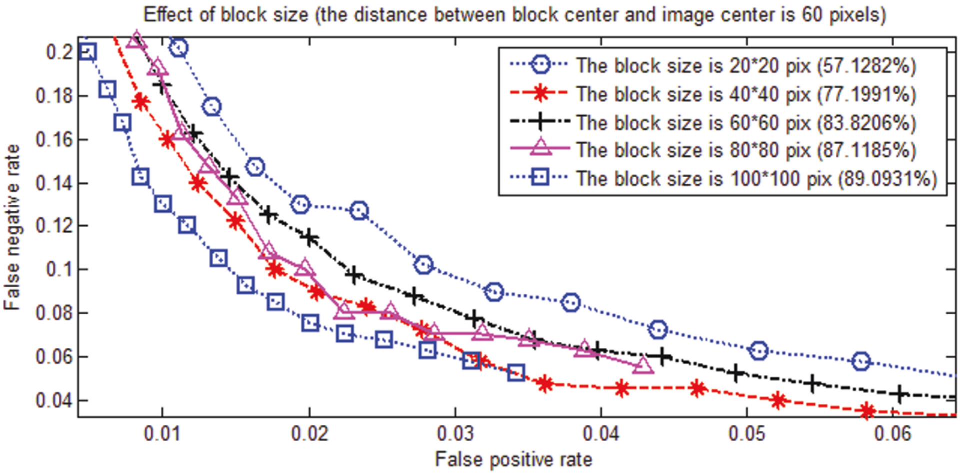


Figure 11 **Effect of the block size on rotational robustness**.

> Experimental results show that the use of the restricted blocking strategy can effectively improve the performance of the NMF hashing algorithm for the rotation operations.

In this study, our motivation is to analyze and improve the rotational performance of the block-based NMF hashing algorithm. In the future study, one of our considerations is to apply the restricted blocking strategy for other block-based hashing and watermarking algorithms (such as DCT-based image hashing [13,14], DWT-based image watermarking [26,27]) against the loose and crop rotation operations.

Acknowledgements
This work was supported in part by NSFC (No. 60903177), in part supported by the Fundamental Research Funds for the Central Universities (No. 21611408), Ph.D. Programs Foundation of Ministry of Education of China (No. 200805581048), and Guangzhou Municipal Science and Technology Program (No. 11C42070443).

Endnote

[a] Feature vectors of NMF low-rank decomposition represent the information in the low-frequency.

Author details
[1] School of Information Science and Technology, Jinan University, Guangzhou 510632, China [2] Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen 518055, China

Competing interests

The authors declare that they have no competing interests.

Received: 1 July 2011 Accepted: 4 April 2012 Published: 4 April 2012

References

1. MK Mihçak, O Koval, S Voloshynovskiy, Robust perceptual hashing of multimedia content. EURASIP, Special (2007)
2. Wacha07 Special Issue, What kind of security does perceptual hashing offer? [Online].http://wacha07.irisa.fr/Wacha07-call.pdf
3. HY Leung, LM Cheng, Robust watermarking scheme using wave atoms. EURASIP Journal on Advances in Signal Processing. **2011**, 9 (2011). Article ID 184817
4. V Sachnev, HJ Kim, S Suresh, YQ Shi, Reversible Watermarking Algorithm with Distortion Compensation. EURASIP Journal on Advances in Signal Processing. **2010**, 12 (2010). Article ID 316820
5. B Barkat, F Sattar, Time-frequency and time-scale-based fragile watermarking methods for image authentication. EURASIP Journal on Advances in Signal Processing. **2010**, 14 (2010). Article ID 408109
6. H Liu, X Yao, J Huang, Semi-Fragile Zernike Moment-Based Image Watermarking for Authentication. EURASIP Journal on Advances in Signal Processing. **2010**, 17 (2010). Article ID 341856
7. G Laimer, A Uhl, Key-dependent JPEG2000-based robust hashing for secure image authentication. EURASIP Journal on Information Security. **2008**, 18 (2008). Article ID 895174
8. X Lv, ZJ Wang, An extended image hashing concept: content-based fingerprinting using FJLT. EURASIP Journal on Information Security. **2009**, 16 (2009). Article ID 859859
9. MK Mihc¸ak, R Venkatesan, A perceptual audio hashing algorithm: a tool for robust audio identification and information hiding. IH2001, Lecture Notes in Computer Science. **2137**, 51–65 (2001)
10. H Özer, B Sankur, N Memon, E Anarim, Perceptual audio hashing functions. EURASIP J Appl Signal Process. **12**, 1780–1793 (2005)
11. J Dittmann, A Steinmetz, R Steinmetz, Content-based digital signature for motion pictures authentication and content-fragile watermarking, in *Proc IEEE Int Conf Multimedia Computing and Systems*, vol. 2. (Florence, Italy, 1999), pp. 209–213
12. B Coskun, B Sankur, N Memon, Spatio-temporal transform based video hashing. IEEE Trans Multimedia. **8**(6), 1190–1208 (2006)
13. J Fridrich, M Goljan, Robust hash functions for digital watermarking, in *Proc IEEE Int Conf Information Technology: Coding Computing*, Las Vegas, NV , USA, pp. 178–183 (2000)
14. R Venkatesan, SM Koon, MH Jakubowski, P Moulin, Robust image hashing, in *Proc IEEE Int Conf Image Processing*, Vancouver, BC, Canada, pp. 664–666 (2000)
15. MK Mihçak, R Venkatesan, Video watermarking using image hashing. *Microsoft Research Tech Rep* (2001)
16. MK Mihçak, R Venkatesan, New iterative geometric methods for robust perceptual image hashing. DRM2001, Lecture Notes in Computer Sciences. **2320**, 178–183 (2002)
17. A Swaminathan, Y Mao, M Wu, Image hashing resilient to geometric and filtering operations, in *Proc IEEE Workshop on Multimedia Signal Processing*, Siena, Italy, pp. 355–358 (2004)
18. A Swaminathan, Y Mao, M Wu, Robust and secure image hashing. IEEE Trans Inf Forensics Secur. **1**(2), 215–230 (2006)

19. S Lu, CY Hsu, Geometric distortion-resilient image hashing scheme and its applications on copy detection and authentication. Multimedia Syst. **11**(2), 159–173 (2005)
20. V Monga, MK Mihçak, Robust and secure image hashing via non-negative matrix factorizations. IEEE Trans Inf Forensics Secur. **2**(3), 376–390 (2007)
21. S Xiang, HJ Kim, J Huang, Histogram-based image hashing scheme robust against geometric deformations, in *Proc 9th ACM Multimedia and Security Workshop*, Dallas, Texas, USA, pp. 121–128 (2007)
22. DD Lee, HS Seung, Algorithms for non-negative matrix factorization, in *Neural Information Processing Systems*, vol. 13. (MIT Press, Cambridge, MA, 2000), pp. 556–562
23. S Xiang, HJ Kim, J Huang, Invariant image watermarking based on statistical features in the low-frequency domain. IEEE Trans Circ Syst Video Technol. **18**(6), 777–790 (2008)
24. Image Processing Toolbox. *imroate* function http://www.mathworks.cn/help/toolbox/images/ref/imrotate.html
25. S Lefevre, C Dixon, C Jeusse, N Vincent, A local approach for fast line detection, in *Proc IEEE Int Conf Digital Signal Process*, Santorini, Greece, pp. 1109–1112 (2002)
26. IJ Cox, J Kilian, T Leighton, T Shamoon, Secure spread spectrum watermarking for multimedia. IEEE Trans Image Proccess. **6**(6), 1673–1687 (1997)
27. IK Yeo, HJ Kim, Generalized patchwork algorithm for image watermarking. Multimedia Syst. **9**(3), 261–265 (2003)

doi:10.1186/1687-6180-2012-77
Cite this article as: Xiang and Yang: **Block-based image hashing with restricted blocking strategy for rotational robustness.** *EURASIP Journal on Advances in Signal Processing* 2012 **2012**:77.