PAPER

Effective and Efficient Image Copy Detection with Resistance to Arbitrary Rotation

Zhili ZHOU[†a)], **Ching-Nung YANG**[††b)], **Beijing CHEN**[†c)], **Xingming SUN**[†d)], ***Nonmembers***, **Qi LIU**[†e)], ***Member***, ***and*** **Q.M. Jonathan WU**[†††f)], ***Nonmember***

SUMMARY For detecting the image copies of a given original image generated by arbitrary rotation, the existing image copy detection methods can not simultaneously achieve desirable performances in the aspects of both accuracy and efficiency. To address this challenge, a novel effective and efficient image copy detection method is proposed based on two global features extracted from rotation invariant partitions. Firstly, candidate images are preprocessed by an averaging operation to suppress noise. Secondly, the rotation invariant partitions of the preprocessed images are constructed based on pixel intensity orders. Thirdly, two global features are extracted from these partitions by utilizing image gradient magnitudes and orientations, respectively. Finally, the extracted features of images are compared to implement copy detection. Promising experimental results demonstrate our proposed method can effectively and efficiently resist rotations with arbitrary degrees. Furthermore, the performances of the proposed method are also desirable for resisting other typical copy attacks, such as flipping, rescaling, illumination and contrast change, as well as Gaussian noising.

key words: *image copy detection, copy attacks, arbitrary rotation, rotation invariant, intensity orders*

1. Introduction

With the rapid development of Internet communication technologies and the emergence of various image processing tools such as Photoshop and ACDSee, digital images can be easily replicated, modified and transmitted on the internet [1], [2]. Therefore, the copyright protection of legal digital images has become a crucial issue. Detecting illegal image copies is the key step of image copyright protection.

Generally, there are two technologies for detecting image copies: digital watermarking and content-based copy detection [3]–[5]. The digital watermarking technology [6], [7] can be regarded as an active approach. It embeds the imperceptible copyright information, namely watermark, into the protected images. Thus all copies of the marked image will contain the same watermark, which can be extracted later to verify the ownership. However, since the information should be embedded prior to distribution, the technology has a limitation in practical applications. Moreover, the embedded watermark can be easily destroyed or removed by illegal users using various malicious attacks, and thus it also suffers from the problem of robustness [8]. Recently, content-based copy detection has been studied as a passive approach to detect illegal copies. Different from watermarking which embeds additional information into images, the content-based copy detection technology only utilizes the image itself to implement copy detection. A content-based copy detection system usually works as follows. It first extracts content-based feature of a given original (query) image and those of the images distributed on the networks, and then compares them to determine whether illegal copies of the original are available on the networks. Compared with watermarking, the main advantages of content-based copy detection are that it does not need any additional information but only image itself, and the copy detection can be implemented after the image distribution. Due to the above advantages, the technique of content-based copy detection is studied in this paper.

The copies of an original image are not only the exact duplicates, but also the modified versions of the original generated by various copy attacks in most cases [3], [9]. These copy attacks usually include various geometric transformations such as rotation, rescaling and flipping, signal manipulations such as illumination and contrast changes, and image noising attacks such as Gaussian noising, watercoloring and mosaic tiling. In these copy attacks, rotation is a normal image processing in our daily life [10]. Through various image processing tools such as Photoshop and ACDSee, a large number of image copies can be generated by rotating the original images by arbitrary degrees. In this study, we mainly deal with arbitrary rotation, which has an important significance for image copyright protection.

In the literatures, many content-based image copy detection methods have been proposed. To detect illegal image copies of a given original image, they usually extract proper features from the original image and all the candidate images, and then match these features for evaluation

Manuscript received August 25, 2015.
Manuscript revised January 30, 2016.
Manuscript publicized March 18, 2016.

[†]The authors are with the School of Computer and Software & Jiangsu Engineering Centre of Network Monitoring, Nanjing University of Information Science and Technology, Nanjing, 210044, China.
[††]The author is with Department of Computer Science and Information Engineering, National Dong Hwa University, Shoufeng, Hualien 974, Taiwan.
[†††]The author is with the Department of Electrical and Computer Engineering, University of Windsor, Windsor, Ontario, N9B 3P4, Canada.
a) E-mail: zhou_zhili@163.com (Corresponding author)
b) E-mail: cnyang@mail.ndhu.edu.tw
c) E-mail: nbutimage@126.com
d) E-mail: sunnudt@163.com
e) E-mail: qrankl@163.com
f) E-mail: jwu@uwindsor.ca

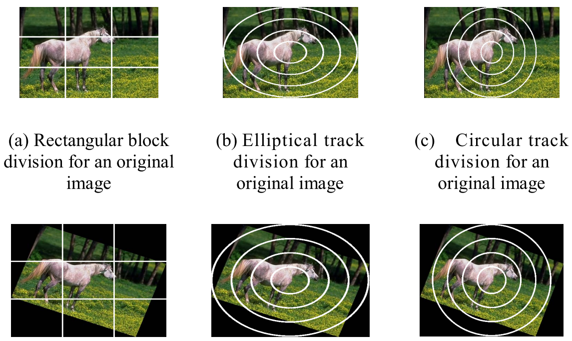
DOI: 10.1587/transinf.2015EDP7341

of the similarity between them. According to the natures of their extracted features, these methods can be roughly classified into two groups: global feature-based and local feature-based methods.

The global feature-based methods [3], [4], [11]–[14] extract global features from the whole image region for copy detection. To the best of our knowledge, the work of Change et al. [11] was the first study in the field of content-based image copy detection. It proposed a near-replica search engine called RIME (Replicated Image Detector), in which the global image features based on wavelets and $C_1C_2C_3$ color space are extracted to detect unauthorized copies of images on the Internet. Although the method is effective to detect slightly modified images, it fails to identify seriously distorted images. Image histogram-based methods [15], [16] have been widely used in image retrieval. However, since the color histograms are the global features which do not encode the spatial information, many irrelevant images may be falsely detected as copies. In addition, the histograms are sensitive to the noising attacks. Therefore, these methods are not suitable for coy detection. To address the above issues, some global feature-based copy detection methods [3], [4], [14] applied image division strategies to extract the features. Kim [3] proposed the ordinal measure of AC coefficients of discrete cosine transform (DCT) by using rectangular block division for image copy detection. More specially, images were firstly divided into 64 (8×8) equal-sized rectangular blocks and their average intensities were derived, and then some important AC coefficients of these blocks were ranked by the ordinal measure to generate the image features. However, when an image suffers rotation transformations, some pixels of one block may shift to another block. It will cause the average intensities of the blocks to be different before and after rotations. Consequently, Kim's method can only resist the 180 degree rotation, but it fails to detect those copies transformed by minor rotations such as 2 and 5 degrees. To improve the robustness to rotation, Wu et al. [12] and Zou et al. [14] extracted image features based on the division of elliptical or circular tracks. In these methods, images were divided into N elliptical or circular tracks, and then the features were generated by computing the average intensities of these tracks. Although the two methods can deal with minor rotations at a certain extent, they are also sensitive to large rotations. That is because the image content in those tracks will be quite different before and after rotation with larger degrees.

Figure 1(a)–(c) show the different image division strategies used in these methods. From the Fig. 1(d)–(f), the content in those blocks or tracks of a given original image is quite different before and after rotation with 20 degree, so that the features extracted from these blocks are sensitive to large rotation. As a result, these methods fail to detect the copies transformed by the rotation.

To address the problem of the robustness to rotation and some other geometric transformations, recently, some local feature-based image copy detection methods have been proposed [17]–[22]. They have achieved desirable performances for image copy detection because of the good robustness of local features. However, the robustness comes with the expense of extensive computation. These methods are usually based on Scale Invariant Feature Transform (SIFT) [23] or its variants such as principle components analysis on SIFT (PCA-SIFT) [24] and speeded up robust feature (SURF) [25]. All of these features are generated by detecting hundreds of interest points for each image in scale-space and then capturing the high dimensional descriptors of the surrounding region of each interest point. Thus, these methods usually require a huge amount of computation in the step of feature extraction for large databases. Moreover, for judging the image copy relationship, the matching of these features is also a time-consuming process. As a result, the computational problem makes them less appealing in copy detection [26].



(a) Rectangular block division for an original image
(b) Elliptical track division for an original image
(c) Circular track division for an original image
(d) Rectangular block division after rotation with 20 degree
(e) Elliptical track division after rotation with 20 degree
(f) Circular track division after rotation with 20 degree

Fig. 1 The image division strategies used in different methods.

From the above analysis, the existing image copy detection methods can not simultaneously achieve desirable performances in the aspects of both accuracy and efficiency for resisting rotations with arbitrary degrees. The local feature-based methods usually have computational problem. To avoid the extensive computation, we investigate the global features in this study. However, the existing global feature-based methods are not robust enough against arbitrary rotation. The main reason is that the image division strategies used in these methods are not invariant to rotation. Therefore, to address this problem, we are motivated to construct rotation invariant image partitions and then extract features from these partitions for copy detection. In this paper, a novel effective and efficient image copy detection method is proposed to resist arbitrary rotation. Our main contributions are: (1) An averaging operation is used to effectively suppress image noise in preprocessing; (2) To resolve the defects of the division strategies used in the existing global feature-based methods, by using pixel intensity orders, each preprocessed image is divided into several rotation invariant partitions, which are the basis and guarantee of resisting arbitrary rotation; (3) By utilizing image gradient magnitudes and orientations, two robust global features, gradient magnitude-based and gradient orientation-based features, are extracted from these partitions; (4) The effectiveness and efficiency of our method for resisting arbitrary rotation are proved by theoretical analysis and experimental results. Meanwhile, the performances of our method for resisting other typical copy attacks are also proved to be desirable.

The rest of the paper is organized as follows. Section 2 introduces the proposed image copy detection method in details. The robustness and time complexity of the proposed method are analyzed in Sect. 3. The experimental results are presented in Sect. 4. Conclusions are drawn in Sect. 5.

2. Proposed Method

2.1 Design Concept

According to the above section, the local feature-based copy detection methods usually have computational problem. Since both the extraction and matching of global features are more efficient to compute, the global feature-based methods can avoid the computational problem and thus they are more suitable for efficient copy detection. Unfortunately, the traditional global feature-based methods are not robust enough to arbitrary rotation. The main reason is that their image division strategies used for global feature extraction are not rotation invariant.

To achieve robustness to arbitrary rotation while maintaining high efficiency for copy detection, the key idea of our method is to extract robust global features by using a rotation invariant image division strategy based on pixel intensity orders. Instead of geometrically dividing images into regular regions, we construct several irregular partitions based on pixel intensity orders, and then extract the robust global features from these partitions. Since the intensity orders of pixel points are rotation invariant, these partitions are also rotation invariant and thus the global features extracted from these partitions can be invariant to arbitrary rotation.

The details of our proposed method will be described in the following sections.

2.2 Preprocessing

The image copies distributed on the internet may be derived from the original images by some noising attacks, such as Gaussian noising. To decrease the effects of nosing attacks, we employ an averaging operation in the preprocessing.

For a given image of size $w \times h$, we first transform the image into the gray-level image, since our image features are extracted by utilizing the gradient magnitudes and orientations in gray-levels. Then, we divide the gray-level image into some nonoverlapping blocks of size $b \times b$. Next, for each block, we compute the average intensity of its $b \times b$ pixels. Finally, a lower resolution image of size $m \times n$ can be obtained, where $m = [w/b]$, $n = [h/b]$, and $[x]$ is the nearest integer to x.

Note that the image and its copies generated by certain transformations such as rescaling will have different scales. If the block size b is set to a certain value, it will cause the content of the corresponding blocks between the image and these copies is quite different so that the robustness of our method will be significantly affected. To conquer this weakness, we use an adaptive block size

$$b = \left[\sqrt{(w \times h - n_0)/C} \right] \tag{1}$$

where C is a constant and n_0 is the number of redundant pixels. The definition of redundant pixels is given as follows. As we know, when the image suffers rotation transformations, it will be padded with some black pixels. As shown in Fig. 1(d)–(f), the black pixels are called as redundant pixels.

If the image does not suffer rotation transformations, the number of redundant pixels n_0 equals to 0 and the block size b is relative to the image size $w \times h$. Thus, by using the adaptive block size, the image and its copies generated by rescaling can be preprocessed to the same scale. When the image is transformed by rotation, its scale remains the same, but its size will be larger since the redundant pixels are padded and n_0 is greater than 0. By using Eq. (1), the number of redundant pixels is subtracted to compute the block size, which can ensure the block size of the image and its rotated versions will be consistent. As a result, after the preprocessing, the image and its rotated versions are also at the same scale.

Small b leads to lower robustness to noising attacks, while large b results in loss of fine details. In this paper, for the images of size 384×256 or 256×384 used in our experiment part, we choose the block size $b = 4$ as an appropriate trade-off by setting $C = 6144$. It's worth noting that, the averaging operation can not only decrease the effects of nosing attacks, but also cause less image pixels to be processed in the following steps, which can apparently enhance the efficiency of our method.

2.3 The Construction of Rotation Invariant Partitions

In this subsection, we will introduce the construction of rotation invariant image partitions. For a given image, one can divide it into several regular regions such as rectangular blocks, elliptical tracks and circular tracks. However, these regions are not rotation invariant so that the features extracted from them will be sensitive to arbitrary rotation. Therefore, a rotation invariant division strategy is the basis and guarantee of resisting arbitrary rotation. In [27], the local patch partition method based on intensity orders of sample points was proposed to divide each local patch into several rotation invariant partitions for generating robust local descriptors. In this paper, instead of geometrically dividing images into regular regions, similar with [27], we employ the intensity order-based image division strategy to divide images into several rotation invariant partitions. The details are given as follows.

Let function $F = \{p_1, p_2, \ldots, p_n\}$ denotes a preprocessed image with n pixels, and $I(p_x)$ the intensity of the pixel p_x. As mentioned in the above subsection, if the image is a copy of an original image generated by rotation with a certain degree, it will be padded with some redundant pixels. That will significantly affect the result of the following intensity order-based image division. Thus, if the preprocessed image is the rotated one, we first remove those redundant pixels of the preprocessed image, which with same intensities are located at the boundary region. The number of remaining pixels is denoted by n', and the preprocessed image with n' remaining pixels by $F' = \{p_1, p_2, \ldots, p_{n'}\}$. If it is not the rotated one, there are no redundant pixels and thus the number $n' = n$.

Then, the remaining pixels of the preprocessed image are divided into k groups according to their intensity orders. More specially, the intensities of all the pixels are sorted in nondescending order and then a set of sorted pixels is derived as

$$\{p_{f(1)}, p_{f(2)}, \ldots, p_{f(n')} : I(p_{f(1)}) \leq I(p_{f(2)}) \leq \cdots \leq I(p_{f(n')})\} \tag{2}$$

Where $p_{f(1)}, p_{f(2)}, \ldots, p_{f(n')}$ is a permutation of $1, 2, \ldots, n'$. Next, $k+1$ intensities can be generated from them as follows:

$$t_i = I(p_{f(s_i)}) : t_0 \leq t_1 \leq \cdots \leq t_k \tag{3}$$

where

$$s_i = \begin{cases} \left\lceil \dfrac{n'}{k} i \right\rceil, & i = 1, 2, \ldots, k \\ 1, & i = 0 \end{cases} \tag{4}$$

Finally, the n' pixels are divided into k groups represented as follows

$$P_i = \{p_j \in F' : t_{i-1} \leq I(p_j) \leq t_i\}, \quad i = 1, 2, \ldots, k \tag{5}$$

Where, P_i is the i-th partition of the preprocessed image. Each group corresponds to a partition and thus k partitions of an image are generated. Figure 2 shows the intensity order-based division for a preprocessed image when the number of partitions k equals to 4. It is worth noting that, since the intensity orders of image pixels cannot be changed by various rotations, these partitions are rotation invariant. In this paper, the number of partitions k is set as 10.

2.4 Feature Extraction

After constructing the image partitions, we propose two global features, which are called the gradient magnitude-based and gradient orientation-based features, respectively. The gradient magnitudes and orientations of the preprocessed image are precomputed in a rotation invariant coordinate system. Then, the two global features are extracted from those image partitions. The procedure of our feature extraction can be divided into three steps as follows.

Step 1): The precomputation of the gradient magnitudes and orientations in a rotation invariant coordinate system. For each pixel p_x, we first construct a rectangular coordinate system. As shown in Fig. 3, suppose o is the central point of the preprocessed image and p_x is a pixel point. The rectangular coordinate system can be established by setting $\overrightarrow{op_x}$ as the positive y-axis for the point p_x. Then, the gradient magnitude $m(p_x)$ and orientation $o(p_x)$ of p_x are precomputed in the coordinate system by:

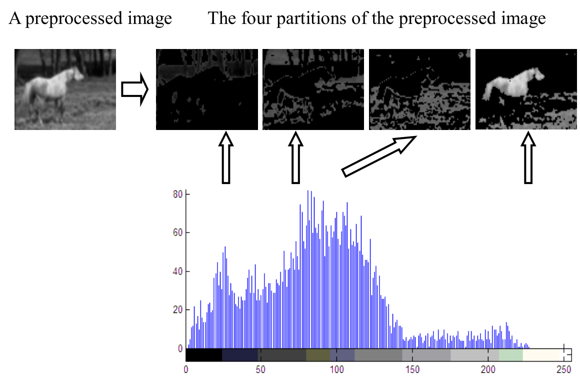


Fig. 2 The intensity order-based division for a preprocessed image (k = 4).

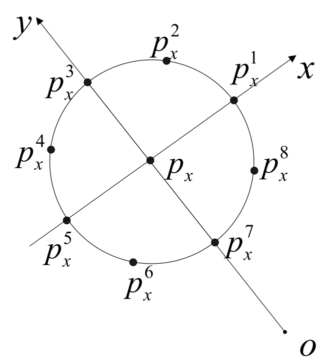


Fig. 3 The rotation invariant coordinate system used for computing the gradient of pixel p_x.

$$m(p_x) = \sqrt{(I(p_x^1) - I(p_x^5))^2 + (I(p_x^3) - I(p_x^7))^2} \tag{6}$$

$$o(p_x) = \tan^{-1}((I(p_x^1) - I(p_x^5))/(I(p_x^3) - I(p_x^7))) \tag{7}$$

where p_x^j, $j = 1, 2, \ldots, 8$, are the neighboring pixels of p_i, as shown in Fig. 3, and $I(p_x^j)$ is the intensity of p_x^j. Since the coordinates of p_x and other pixels will be invariant when the image is rotated, the rectangular coordinate system is rotation invariant and thus the precomputed gradient magnitudes and orientations are also rotation invariant.

Step 2): The extraction of gradient magnitude-based feature. From the above, the precomputed gradient magnitudes are rotation invariant. In this step, we utilize the average magnitudes to form the gradient magnitude-based feature of the preprocessed image in the rotation invariant coordinate system. For each partition P_i, we first compute the average magnitude of all of the pixels in the partition by

$$M(P_i) = \frac{\sum\limits_{p_x \in P_i} m(p_x)}{n_i} \tag{8}$$

where n_i is the number of pixels of partition P_i. Then, all the average magnitudes are concatenated to generate a k dimensional vector $(M(P_1), M(P_2), \ldots, M(P_k))$. Finally, all elements of the feature vector are normalized by

$$MF(P_i) = \frac{M(P_i)}{\sum_{i=1}^{k} M(P_i)} \tag{9}$$

As a result, the gradient magnitude-based feature, denoted as $MF = (MF(P_1), MF(P_2), \ldots, MF(P_k))$, are generated, where all of its element values are in the range of [0, 1].

Step 3): The extraction of gradient orientation-based feature. As we know, if the precomputed gradient orientations are rotation invariant, the average deviation of orientations of all pixels in a partition is also rotation invariant. In this step, the average deviations of orientations are utilized to extract the gradient orientation-based feature. Similar with Step (2), for each partition P_i, we first compute the average orientation of the pixels in the partition by

$$O(P_i) = \frac{\sum_{p_x \in P_i} o(p_x)}{n_i} \tag{10}$$

Then, instead of computing the normalized value of the average orientation, we compute the average deviation of orientations of P_i by

$$OF(P_i) = \frac{\sum_{p_x \in P_i} |o(p_x) - O(P_i)|}{n_i} \tag{11}$$

where $O(P_i)$ is the average orientation of all pixels in P_i. Finally, all average deviations of orientations are concatenated to form the gradient orientation-based feature, denoted as $OF = (OF(P_1), OF(P_2), \ldots, OF(P_k))$.

From the above procedure, the image partitions and rectangular coordinate system are rotation invariant, and thus the gradient magnitude-based and gradient orientation-based features are robust to arbitrary rotation.

2.5 Copy Detection

In this subsection, we will discuss how to detect copies of a query image from an image database. Figure 4 shows the flowchart of our copy detection method. From Fig. 4, the procedure of the method can be broken down into two phases: offline processing and online processing. In the offline processing, the gradient magnitude-based and gradient orientation-based features of each test image from the database are extracted by using the above feature extraction algorithm. Then, these features are stored in the feature database for future use. In the online processing, for each query image, its two features are also extracted by using the same feature extraction algorithm. Then, the two features of the query image are compared with those features stored in the feature database by the following comparison method.

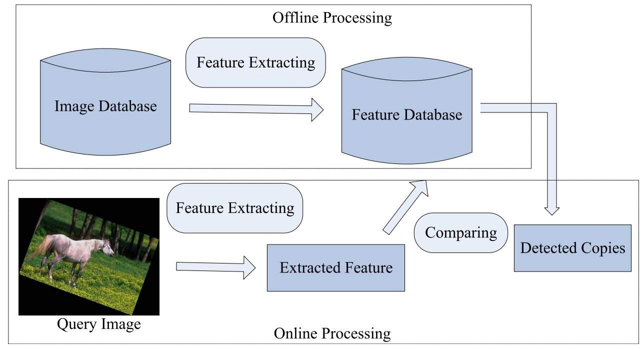


Fig. 4 The flowchart of our copy detection method.

Let the gradient magnitude-based and gradient orientation-based features of a query (original) image Q, be $MF^Q = [MF^Q(P_1),\ MF^Q(P_2),\ \ldots, MF^Q(P_k)]$ and $OF^Q = [OF^Q(P_1),\ OF^Q(P_2),\ \ldots, OF^Q(P_k)]$ respectively, and those of a test image T, $MF^T = [MF^T(P_1),\ MF^T(P_2), \ldots, MF^T(P_k)]$ and $OF^T = [OF^T(P_1),\ OF^T(P_2),\ \ldots, OF^T(P_k)]$. Then the distance between the two images $D(Q,T)$ can be computed by

$$D(Q,T) = \alpha \times d_M + (1-\alpha) \times d_O \tag{12}$$

Where d_M and d_O can be computed by the Jaccard coefficient:

$$d_M = \frac{\sum_{i=1}^{k} \min(MF^Q(P_i), MF^T(P_i))}{\sum_{i=1}^{k} \max(MF^Q(P_i), MF^T(P_i))} \tag{13}$$

$$d_O = \frac{\sum_{i=1}^{k} \min(OF^Q(P_i), OF^T(P_i))}{\sum_{i=1}^{k} \max(OF^Q(P_i), OF^T(P_i))} \tag{14}$$

In Eq. (13) and (14), d_M and d_O mean the gradient magnitude-based feature distance and gradient orientation-based feature distance between the two images, respectively, and α is a weighting factor ranging from 0 to 1. The computed distance between the query image and the test image is denoted as $D(Q,T)$, whose range is from 0 to 1, can be compared with a preset threshold to determine whether the test image is a copy of the query image. The smaller value of $D(Q,T)$ implies greater similarity between the two images. Given a preset threshold τ, if the condition $D(Q,T) \leq \tau$ is true, we can determine that the test image from the database is the copy version of the original, or else it is not.

3. Robustness and Time Complexity Analysis

In this section, the robustness and time complexity of the proposed method will be analyzed to illustrate the effectiveness and efficiency.

3.1 Robustness Analysis

In this subsection, we will analyze the robustness of the proposed method to the arbitrary rotation, and other typical copy attacks such as rescaling, flipping and Gaussian noising.

Arbitrary Rotation: From Sect. 2.2 and Sect. 2.3, since the image partitions and the coordinate system are constructed in a rotation invariant way, the extracted gradient magnitude-based and gradient orientation-based features are rotation invariant. Therefore, our method is robust to rotations with arbitrary degrees, which is also demonstrated by our experimental results.

Flipping and Rescaling: Our method is robust to flipping transformation, because the image partitions, average magnitudes and average deviations of orientations will not be changed by flipping transformation and thus our features are invariant to this type of attack. Rescaling transformations will change the original image resolution, but will not significantly change that of the preprocessed image since the preprocessed one is generated by using the adaptive block size in the averaging operation. For this reason, our method is insensitive to rescaling.

Rotation with central cropping, shifting and cropping: These attacks, which can be regarded as partial region-discarded attacks, will cause some image content to be lost. Thus our features will be changed. However, the experimental results in Sect. 4 show that our method can successfully detect the copies slightly modified by these attacks. However, for dealing with the copies seriously modified by these attacks, the robustness of our method will be limited.

Illumination and contrast changes: An illumination change will cause a constant to be added to each image pixel, but it will not affect the gradient magnitudes and orientations since they are computed by utilizing pixel differences. A contrast change will cause each pixel value to be multiplied by a constant, and thus the gradient magnitudes will be multiplied by the same constant, but the effects of contrast will be removed by using the normalizing operation in Eq. (9). Meanwhile, the gradient orientations will not be changed by contrast change due to the division operation during their computation. Therefore, the extracted gradient magnitude-based and gradient orientation-based features are invariant to these attacks, and our method is robust to illumination and contrast changes.

Noising attacks: The typical noising attacks include Gaussian noising, watercoloring, mosaic tiling and so on. These noising attacks can significantly change the individual pixels. However, in the preprocessing, the averaging operation also can effectively decrease such effects [28]. Thus, our method is robust to these attacks to some extent.

All of the above analysis illustrates that, our method can effectively resist arbitrary rotation, and it also has the effectiveness to other typical attacks. These will be further demonstrated by experimental results.

3.2 Time Complexity Analysis

The computation time of copy detection usually consists of offline processing time and online processing time [29]. Therefore, we analyze the time complexities of offline processing for test images from an image database and online processing for query images. For these images, suppose that all of them have n pixels. Note that the time complexity of our feature extraction (including the preprocessing and construction of image partition) for a given image is proportional to the number of image pixels n. Therefore, in offline processing, the time complexity of the feature extraction for a test image is $O(n)$. If there are l images in the database, the time complexity is $O(n \times l)$. In online processing, the time complexity of feature extraction for a query image is also $O(n)$. Due to the two extracted features of each image are k dimensional, the time complexity of feature comparison between the query image and the test images is $O(2 \times k \times l)$, where $k = 10$ in this paper. Thus, the average time complexity of online processing for searching for per query image in the database can be represented as $O(n) + O(20 \times l)$. It's worth noting that the offline processing can be realized beforehand. Therefore, for searching for per query image in a database with l images, the average time complexity of our method only includes that of the online processing, which is only $O(n) + O(20 \times l)$. The above time complexity analysis illustrates that our method is simple and efficient, which is also demonstrated in the following experimental part.

4. Experimental Results

In this section, first, we describe the data set and evaluation criteria applied in our experiments. Second, according to the accuracy performances with different values of weighting factor α, we determine the value of α for our method. Third, we test accuracy performances of our method for resisting arbitrary rotation and other copy attacks, and compare them with those of Kim's [3], Wu's [4], Ling's [22] and Fan's [27] methods. Where, Ling's method is based on the sparse representation of SIFT features for copy detection. We also use the improved SIFT features proposed by Fan's method [27], called as multisupport region order-based gradient histogram (MROGH) features, for copy detection. Finally, the computation time of these methods are test and compared. All experiments are run on a standard PC (Core2 Duo E7500 CPU, 2G RAM) with Matlab7.0 program.

4.1 Data Set and Evaluation Criteria

In the experiments, we use the image database downloaded from [30]. The image database includes 1,000 images of size of 384×256 or 256×384, which are saved in JPEG format. Firstly, 30 images are randomly chosen from the image database. Then, each chosen image has modified by 35 image attacks by Adobe Photoshop 7.0. Thus, 1050 image copies are generated for our experiments. The 35 copy attacks are listed as follows:

1) Rotation: The rotation angles are 2, 5, 10, 20, 40, 90 and 180 degrees.
2) Flipping: Horizontal and vertical flipping.
3) Rescaling: The rescaling factor are 0.5, 2, and 4.

4) Rotation with central cropping: The rotation angles are 2, 5, 10, and 20 degrees, and the rotated image are then cropped to the original size.
5) Shifting: Horizontal and vertical shifting with the loss of 2%, 5%, 10%, and 20% image content.
6) Cropping: The cropping percentages are 2%, 5%, 10%, and 20%.
7) Illumination change: The constants added to the illumination of each pixel are −10 and 10.
8) Contrast change: The change ratios are 0.8 and 1.2.
9) Nosing: The nosing attacks include Gaussian noising, watercoloring, mosaic tiling, mosaic, sponge, ocean ripple and crayon. The default setting of Adobe Photoshop 7.0 is used for these attacks.

To evaluate the accuracy performances of those methods, in our experiments, we adopt the precision and recall curve (P-R curve), which is a plot of the precision rate versus the recall rate. When the distance threshold τ equals to a certain value, the precision rate and the recall rate can be defined as follow. Let N_T be the number of total detected images which are below the threshold, where the detected images may include non-copies, and N_c the number of total copies. The number of correct positives (number of copy images that are successfully detected) is denoted by CP. The precision rate and the recall rate are denoted by

$$precision(\tau) = CP/N_T \qquad (15)$$

$$recall(\tau) = CP/N_c \qquad (16)$$

Where τ can range from 0 to 1. We can plot points representing these rates on a two dimensional graph with varying the threshold value τ from 0 to 1 to generate P-R curves. Where, the X-axis and Y-axis of the graph denote the recall and precision, respectively. The ideal P-R curve should pass through (1, 1), namely 100% recall rate and 100% precision rate.

4.2 Parameter Determination

The parameter α plays an important role in our proposed method. A low value of α means the distance of gradient orientation-based features d_O plays a lager role on copy detection, whereas a large value of α indicates the distance of gradient magnitude-based features d_M has more impact on copy detection. We test the proposed method with five different α values: 0.0, 0.25, 0.5, 0.75, and 1.0. For the test, the 1050 generated copies are inserted to the database, and thus there are 2050 test images in the database. The 30 chosen images sever as the query images. Then, we search for the query images in the image database one by one. Figure 5 presents the P-R curves of our method with different α values. As shown in Fig. 5, when $\alpha = 0.5$, our method achieves best precision for all recall rates. This implies that the detection performance is the peak when gradient magnitude-based feature and gradient orientation-based feature play a balanceable effect for copy detection. In the following experiments, we set $\alpha = 0.5$ for our method.

4.3 Accuracy Performances

This subsection reports the accuracy performances of our method for arbitrary rotation and other typical copy attacks, and compares them with those of Kim's, Wu's, Ling's and Fan's methods. Two experiments are conducted to measure 1) P-R curves of these methods for all the 35 copy attacks and 2) the number of successfully detected copies generated by arbitrary rotation and other typical copy attacks. In the experiments, the 30 randomly chosen images are treated as query images. The 1050 image copies generated from the chosen images are inserted into the database and there are 2050 test images in the database.

The first experiment is conducted to observe the accuracy performances of those methods for all the 35 copy attacks. Figure 6 presents the P-R curves of those methods for all the 35 copy attacks. From Fig. 6, we can see that the precision and recall rates of our method are up to about 92%, while the four other methods can achieve about 66%, 68%, 89% and 90%, respectively. The accuracy performance of our method is significantly higher than those of Kim's and Wu's methods, and slightly higher than those of Ling's and Fan's methods.

In the second experiment, we will observe the effec-

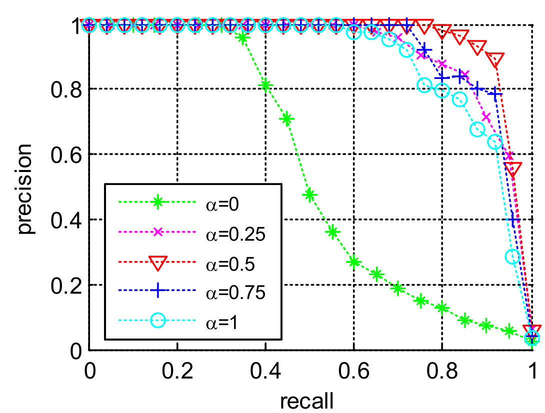


Fig. 5 The performances of our method with the different α values.

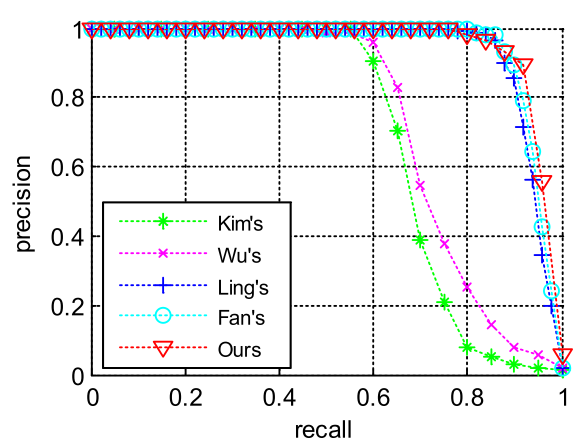


Fig. 6 P-R curves of different methods for all of the 35 copy attacks.

tiveness of our method and the four other methods for each attack in details. To facilitate the observation, for each copy attack, we count the numbers of successfully detected copies by using these methods. As we know, to detect image copies, we need a certain distance threshold to judge whether an image is a copy of another. Here, the threshold of each method is set according to its P-R curve obtained in the first experiment. In particular, when the detection precision is 90%, the according threshold of each method is used as its own threshold. Table 1 lists all of the 35 copy attacks, and the number of detected copies for each attack. Because we chose 30 original images to undergo 35 copy attacks, there are 30 copies for each attack and 1050 copies in total. The row values of Table 1 are the numbers of copies which are successfully detected by using their original images as queries for each copy attack.

As Table 1 shows, Ling's, Fan's and our methods can successfully detect all of the 210 copies transformed by arbitrary rotation, while Kim's and Wu's methods can only detect 60 and 73 respectively. Our method performs excellently for dealing with arbitrary rotation, and outperforms Kim's and Wu's methods.

For the partial region-discarded attacks such as rotation with central cropping, copping and shifting, the number of successfully detected copies of our method is higher that those of Kim's and Wu' methods, but lower than Ling's and Fan's methods. It is clear that our method is more robust than Kim's and Wu's methods for resisting these attacks. However, our method is limited for detecting the copies seriously modified by these attacks. That is because our features are extracted from the whole image region and the loss of image content caused by the partial region-discarded attacks will significantly affect the performance of our method for dealing with these attacks. From Table 1, we can see that when the images are suffered more serious versions of these attacks, the performance of our method will significantly decrease.

Once the query images are modified by nosing attacks such as Gaussian nosing, water coloring and sponge, the numbers of successfully detected copies of Wu's, Ling's and Fan's methods are significantly decreased, while our method can detect most of the copies generated by these nosing attacks.

The total number (percentage) of successfully detected copies of our method is 977 (93%), While those of Kim's, Wu's, Ling's and Fan's methods are 655 (62%), 672 (64%), 924 (88%) and 940 (90%), respectively. The result shows that our method is much better than Kim's and Wu's methods for dealing with various copy attacks, and slightly superior to Ling's and Fan's methods. The experimental results show that our method can achieve desirable performances for resisting arbitrary rotation and other typical copy attacks.

Table 1 The number of successfully detected copies for 35 different copy attacks.

	Copy attacks	Kim's	Wu's	Ling's	Fan's	Ours
1	rotation (2°)	24	13	30	30	30
2	rotation (5°)	6	0	30	30	30
3	rotation (10°)	0	0	30	30	30
4	rotation (20°)	0	0	30	30	30
5	rotation (40°)	0	0	30	30	30
6	rotation (90°)	0	30	30	30	30
7	rotation (180°)	30	30	30	30	30
8	Horizontal flipping	30	30	3	3	30
9	Vertical flipping	30	30	4	3	30
10	Rescaling (×0.5)	30	30	30	30	30
11	Rescaling (×2)	30	30	30	30	30
12	Rescaling (×4)	30	30	30	30	30
13	Rotation with central cropping (2°)	29	30	30	30	30
14	Rotation with central cropping (5°)	3	27	30	30	30
15	Rotation with central cropping (10°)	0	12	30	30	28
16	Rotation with central cropping (20°)	0	1	30	30	22
17	Shifting (loss of 2% content)	29	30	30	30	30
18	Shifting (loss of 5% content)	24	19	30	30	29
19	Shifting (loss of 10% content)	13	8	30	30	28
20	Shifting (loss of 20% content)	2	0	30	30	23
21	Cropping (2%)	2	29	30	30	30
22	Cropping (5%)	2	17	30	30	22
23	Cropping (10%)	0	8	30	30	20
24	Cropping (20%)	0	0	30	30	13
25	Illumination change (-10)	30	30	30	30	30
26	Illumination change (+10)	30	30	30	30	30
27	Contrast change (× 0.8)	30	30	30	30	30
28	Contrast change (× 1.2)	30	30	30	30	30
29	Gaussian noising	30	30	30	30	30
30	Water coloring	26	18	10	15	27
31	Mosaic tiling	28	14	18	21	25
32	Mosaic	30	30	12	14	28
33	Sponge	28	21	25	26	27
34	Ocean ripple	27	18	19	21	26
35	Crayon	29	17	23	25	29
	Total number (Percentage)	655 (62%)	672 (64%)	924 (88%)	940 (90%)	977 (93%)

4.4 Computation Time

As copy detection usually consists of offline processing and online processing, we test and compare the computation time of our method and the four other methods in an analytic way. Table 2 lists the computation time of offline processing for the image database and average computation time of online processing for searching for per query image in the database by using different methods. As shown in Table 2, the computation time of offline and online processing of Kim's, Wu's and our methods is much less than that of Ling's and Fan's methods. In other words, Kim's, Wu's and our methods are much more efficient than Ling's and Fan's methods, which are time-consuming. The computation time of offline and online processing of our method is only 116.24 seconds and 0.06 seconds, respectively.

From all of the above experiments, we can see that the performances of our method for resisting arbitrary rotation and other typical attacks are desirable in the aspects of both

Table 2 Computation time of different methods.

Methods	Offline processing (s)	Online processing (s)
Kim's	58.56	0.04
Wu's	69.63	0.03
Ling's	3.07×10^3	1.60
Fan's	5.54×10^3	2.89
Our	116.24	0.06

accuracy and efficiency.

5. Conclusion and Future Work

In this study, a novel image copy detection method has been presented. Experimental results show that our method can achieve desirable performances for resisting arbitrary rotation and other typical copy attacks in the aspects of both accuracy and efficiency. There are two reasons, which can be summarized as follows. The first one is that because of the rotation invariance of the constructed image partitions and coordinate system, the extracted gradient magnitude-based and gradient orientation-based features are robust to the rotations with arbitrary degrees. Meanwhile, they are also robust to other typical attacks. The second is that the two features, which are only 10 dimensional, can be extracted and compared efficiently for copy detection. In future, by using the indexing method, we will further improve the efficiency of our method to implement efficient copy detection in a very large image database without decreasing the effectiveness.

Acknowledgments

Acknowledgments: This work is supported by the Jiangsu Basic Research Programs-Natural Science Foundation (BK20150925), Startup Foundation for Introducing Talent of Nanjing University of Information Science and Technology (2014r024), National Natural Science Foundation of China (NSFC) (U1536206, 61232016, U1405254, 61373133, 61502242, 61572258), Open Fund of Demostration Base of Internet Application Innovative Open Platform of Department of Education (KJRP1406, KJRP1407), Priority Academic Program Development of Jiangsu Higher Education Institutions (PADA) Fund, Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET) Fund, National Ministry of Science and Technology Special Project Research GYHY201301030, 2013DFG12860, BC2013012, and College Students Practice Innovation Training Program (201510300155).

References

[1] Z.H. Xia, X.H. Wang, X.M. Sun, and B.W. Wang, "Steganalysis of least significant bit matching using multi-order differences," Security and Communication Networks, vol.7, no.8, pp.1283–1291, Aug. 2014.
[2] J. Li, X.L. Li, B. Yang, and X.M. Sun, "Segmentation-based image copy-move forgery detection scheme," IEEE Trans. Information Forensics and Security, vol.10, no.3, pp.507–518, March 2015.
[3] C. Kim, "Content-based image copy detection," Signal Processing: Image Communication, vol.18, no.3, pp.169–184, 2003.
[4] M.-N. Wu, C.-C. Lin, and C.-C. Chang, "Novel image copy detection with rotating tolerance," J. Systems and Software, vol.80, no.7, pp.1057–1069, 2007.
[5] Y.H. Wan, Q.L. Yuan, S.M. Ji, L.M. He, and Y.L. Wang, "A survey of the image copy detection," Proc. IEEE International Conference on Cybernetics and Intelligent Systems, pp.738–743, Chengdu, China, 2008.
[6] Z.C. Ni, Y.Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol.16, no.3, pp.354–362, March 2006.
[7] M. Qi, B.-Z. Li, and H. Sun, "Image watermarking via fractional polar harmonic transforms," J. Electronic Imaging, vol.24, no.1, Jan. 2015.
[8] J.-H. Hsiao, C.-S. Chen, L.-F. Chien, and M.-S. Chen, "A new approach to image copy detection based on extended feature sets," IEEE Trans. Image Process., vol.16, no.8, pp.2069–2079, 2007.
[9] A. Joly, O. Buisson, and C. Frelicot, "Content-based copy retrieval using distortion-based probabilistic similarity search," IEEE Trans. Multimedia, vol.9, no.2, pp.293–305, 2007.
[10] L. Li, H. Xu, and C.-C. Chang, "Rotation invariant image copy detection using DCT domain," Int. J. Innovative Computing, Information and Control, vol.7, no.7, pp.3633–3644, 2011.
[11] E.Y. Chang, J.Z. Wang, C. Li, and G. Wiederhold, "RIME: A replicated image detector for the world-wide web," Proc. SPIE Multimedia Storage and Archiving Systems, pp.58–67, Boston, MA, United states, 1998.
[12] M.-N. Wu, C.-C. Lin, and C.-C. Chang, "A robust content-based copy detection scheme," Fundamenta Informaticae, vol.71, no.2-3, pp.351–366, 2006.
[13] C.-C. Lin and S.-S. Wang, "An edge-based image copy detection scheme," Fundamenta Informaticae, vol.83, no.3, pp.299–318, 2008.
[14] F. Zou, X. Li, Z. Xu, H. Ling, and P. Li, "Image copy detection with rotation and scaling tolerance," Jisuanji Yanjiu yu Fazhan/Computer Research and Development, vol.46, no.8, pp.1349–1356, 2009.
[15] Y. Kumagai and G. Ohashi, "Query-by-Sketch image retrieval using edge relation histogram," IEICE Trans. Inf. & Syst., vol.E96-D, no.2, pp.340–348, Feb. 2013.
[16] K. Konstantinidis, A. Gasteratos, and I. Andreadis, "Image retrieval based on fuzzy color histogram processing," Optics Communications, vol.248, no.4-6, pp.375–386, April 2005.
[17] C.-S. Lu and C.-Y. Hsu, "Geometric distortion-resilient image hashing scheme and its applications on copy detection and authentication," Multimedia Systems, vol.11, no.2, pp.159–173, 2005.
[18] L.-W. Kang, C.-Y. Hsu, H.-W. Chen, and C.-S. Lu, "Secure sift-based sparse representation for image copy detection and recognition," Proc. 2010 IEEE International Conference on Multimedia and Expo, Singapore, Singapore, pp.1248–1253, 2010.
[19] H.-F. Ling, L.-Y. Wang, L.-Y. Yan, F.-H. Zou, and Z.-D. Lu, "PM-DFT: A new local invariant descriptor towards image copy detection," J. Computer Science and Technology, vol.26, no.3, pp.558–567, 2011.
[20] Z. Xu, H. Ling, F. Zou, Z. Lu, and P. Li, "A novel image copy detection scheme based on the local multi-resolution histogram descriptor," Multimedia Tools and Applications, vol.52, no.2-3, pp.445–463, 2011.
[21] H.-F. Ling, H. Cheng, Q. Ma, F. Zou, and W. Yan, "Efficient image copy detection using multiscale fingerprints," IEEE Multimedia Mag., vol.19, no.1, pp.60–69, 2012.
[22] H. Ling, L. Yan, F. Zou, C. Liu, and H. Feng, "Fast image copy detection approach based on local fingerprint defined visual words," Signal Process., vol.93, no.8, pp.2328–2338, 2013.

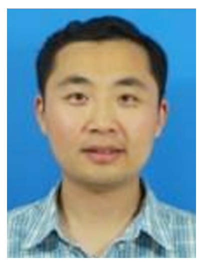
[23] D.G. Lowe, "Distinctive image features from scale-invariant keypoints," Int. J. Comput. Vis., vol.60, no.2, pp.91–110, 2004.
[24] K. Yan and R. Sukthankar, "PCA-sift: A more distinctive representation for local image descriptors," Proc. 2004 IEEE Computer Society Conference on Comput. Vis. Pattern Recognit., pp.506–513, Los Alamitos, CA, USA, 2004.
[25] H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool, "Speeded-up robust features (SURF)," Computer Vision and Image Understanding, vol.110, no.3, pp.346–359, 2008.
[26] M.M. Esmaeili, M. Fatourechi, and R.K. Ward, "A robust and fast video copy detection system using content-based fingerprinting," IEEE Trans. Information Forensics and Security, vol.6, no.1, pp.213–226, 2011.
[27] B. Fan, F. Wu, and Z. Hu, "Rotationally invariant descriptors using intensity order pooling," IEEE Trans. Pattern Anal. Mach. Intell., vol.34, no.10, pp.2031–2045, 2012.
[28] Y. Lei, W. Luo, Y. Wang, and J. Huang, "Video sequence matching based on the invariance of color correlation," IEEE Trans. Circuits Syst. Video Technol., vol.22, no.9, pp.1332–1343, 2012.
[29] A. Sarkar, V. Singh, P. Ghosh, B.S. Manjunath, and A. Singh, "Efficient and robust detection of duplicate videos in a large database," IEEE Trans. Circuits Syst. Video Technol., vol.20, no.6, pp.870–885, 2010.
[30] "Content based image retrieval," http://wang.ist.psu.edu/docs/related/ 2003.

Zhili Zhou received his B.S. degree in communication engineering from Hubei University in 2007, and his M.S. and Ph.D. degrees in computer application at School of Information Science and Engineering from Hunan University in 2010 and 2014, respectively. He is an assistant professor at Nanjing University of Information Science and Technology. His current research interests include digital forensics, image/video copy detection, pattern Recognition, and image processing.

Ching-Nung Yang received the B.S. and M.S. degrees in telecommunication engineering from National Chiao Tung University, Hsinchu, Taiwan, in 1983 and 1985, respectively, and the Ph.D. degree in electrical engineering from National Cheng Kung University, Tainan City, Taiwan, in 1997. He is currently a Full Professor with the Department of Computer Science and Information Engineering, National Dong Hwa University, Hualien, Taiwan. His research interests include coding theory, information security, and cryptography.

Beijing Chen received his M.S. in applied mathematics from Zhengjiang University in 2006, and the Ph.D. degrees in Computer Application from Southeast University in 2011. He is an associate professor at Nanjing University of Information Science and Technology. His current research interests include image processing and digital forensics.

Xingming Sun received his B.S. in mathematics from Hunan Normal University, China, in 1984; his M.S. in computing science from Dalian University of Science and Technology, China, in 1988; and his Ph.D. in computing science from Fudan University, China, in 2001. He is currently a professor at the College of Computer and Software, Nanjing University of Information Science and Technology, China. In 2006, he visited the University College London, UK; he was a visiting professor in University of Warwick, UK, between 2008 and 2010. His research interests include network and information security, database security, and natural language processing.



Qi Liu received his M.S. degree in 2006 and his Ph.D. in Data Communication and Networks from the University of Salford, UK in 2010. He was promoted to Professor of Computer at the Nanjing University of Information Science and Technology in 2011. His research interests include wireless ad hoc network, wireless sensor networks, Internet of things and its application, meteorological sensor networks.

Q.M. Jonathan Wu received the Ph.D. degree in electrical engineering from the University of Wales, Swansea, U.K., in 1990. He is currently a Professor with the Department of Electrical and Computer Engineering, University of Windsor, Windsor, ON, Canada. His current research interests include 3-D computer vision, active video object tracking and extraction, interactive multimedia, sensor analysis and fusion, and visual sensor networks.