Journal of Information Hiding and Multimedia Signal Processing ©2013 ISSN 2073-4212
Ubiquitous International Volume **4**, Number **1**, January **2013**

An Efficient Scheme for Detecting Copy-move Forged Images by Local Binary Patterns

Leida Li[1,2], Shushang Li[1], Hancheng Zhu[1]

[1] School of Information and Electrical Engineering,
China University of Mining and Technology, Xuzhou 221116, China
reader1104@hotmail.com

[2] Shanghai Key Laboratory of Integrate Administration Technologies
for Information Security, Shanghai 200240, China

Shu-Chuan Chu, John F. Roddick

School of Computer Science, Engineering and Mathematics,
Flinders University of South Australia, South Australia 5001, Australia

Jeng-Shyang Pan*

Department of Computer Science and Technology,
Harbin Institute of Technology Shenzhen Graduate School, Shenzhen 518055, China

Received September 2012; revised November 2012

Abstract. *Copy-move is one of the most common image tampering method. Many schemes have been proposed to detect and locate the forged regions. However, many existing schemes fail when the copied region is rotated or flipped before being pasted. To solve the problem, this paper presents a new method for detecting the copy-move forgery. The image is first filtered and divided into overlapping circular blocks. Then the features of the circular blocks are extracted using rotation invariant uniform local binary patterns* (LBP). *The feature vectors are then compared and the forged regions can be located by tracking the corresponding blocks. Experimental results demonstrate that this method is robust not only to JPEG compression, noise contamination and blurring, but also to region rotation and flipping.*
Keywords: copy-move forgery, LBP, rotation, flipping

1. **Introduction.** Most of the information we get are from visual signals. What we see influences our understanding significantly. Due to the development of information technology and the internet, the spread of the digital images becomes easy and convenient. However, duo to the powerful image processing softwares, such as Photoshop and Coreldraw, it becomes extremely easy and expedient to tamper digital images, even for the non-professionals. The traces of tampering are hard to recognize by the naked eyes. Although most people use the image processing softwares to make the image more beautiful, some may use the foraged images in news report, judicial forensics and so on, which will mislead our general comprehension of the underlying truth. Furthermore, it is necessary for us to develop automatic methods to authenticate the images and indicate potential forgeries.

The simplest method of tampering is to copy one or two region(s) and past to other regions of the same image. This kind of forgery is usually called copy-move. The idea of detecting this kind of forgery is to divide the image into small blocks, which only have

one row or one column different pixels with their neighboring blocks. In [1], Fridrich *et al.* first proposed to detect the copy-move forgery, where the quantized Discrete Cosine Transform (DCT) coefficients are used to describe the content of the square sub-blocks. A.C. Popescu proposed to extract the block features using Principle Component Analysis (PCA) [2]. This method will not be available when the signal to noise ratio (SNR) is lower than 24dB. Luo *et al.* proposed a novel method to detect this forgery in [3], where they computed seven characteristic features by the statistical analysis of the pixels in each block. This method is more effective and robust when the copied regions are subject to blurring, JPEG compression and noise. Huang *et al.* developed a method by introducing a truncating procedure to reduce the dimension of feature vectors, which can improve the detection performances based on DCT [4]. In [5], B. Mahdian took advantage of the blur invariant moments to extract the block features. Though these methods can detect the copy-move forgery in most cases, they may fail if the copied regions are rotated or flipped.

In order to detect copy-move forgery with geometric transforms, some methods have been proposed recently. Ryu *et al.* employed Zernike moments to extract the features for block matching. This method achieved an average detection precision rate of 83.59% in the case of region rotation [6]. In [8], Liu *et al.* proposed a method using Hu moments to extract the features of the blocks. This method is robust not only to noise contamination, JPEG compression and blurring, but also to moderate rotation.

In this paper, we propose a novel method to detect the copy-move forgery. To this end, a new algorithm, rotation invariant uniform local binary pattern (LBP), is employed to extract the features of the blocks. The advantage of the proposed scheme is that it can not only deal with traditional image processing operations but also geometric transforms, especially region rotation and/or flipping.

2. **Local Binary Pattern.** LBP is a kind of gray-scale texture operator which is used for describing the spatial structure of the image texture [7]. The texture T in a local neighborhood of a gray scale image can be defined as the joint distribution of the gray levels of $P(P > 1)$ image pixels using the following equation.

$$T = t(g_c, g_0, ..., g_{P-1}), \tag{1}$$

where g_c is the gray value of the central pixel corresponding to the local neighborhood, $g_p(p = 0, 1, ..., P-1)$ corresponds to the value of its neighbors. Suppose the coordinate of g_c is $(0, 0)$, and the coordinate of g_p is given by $(-R \cdot sin(2\pi p/P), R \cdot cos(2\pi p/P))$. Fig.1 shows three examples of circularly symmetric neighbor sets for different configurations of (P, R) [**?**]. The gray values of the neighbors which are not in the center of the pixels can be estimated by interpolation.

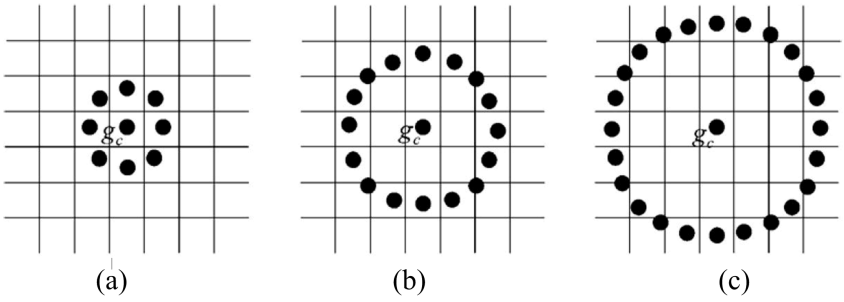

FIGURE 1. Circular symmetric neighbor sets for different (P, R) [**?**]. (a) (P, R)=(8,1), (b) (P,R)=(16,2), (c) (P,R)=(24,3).

We can subtract g_c from the gray values of the circularly symmetric neighborhood g_p.

$$T = t(g_c, g_0 - g_c, ..., g_{P-1} - g_c). \tag{2}$$

Assume that the values of $g_i - g_c$ $(i = 0, 1, ..., P-1)$ are independent of g_c, then Eq.(2) can be approximated as

$$T \approx t(g_c)t(g_0 - g_c, ..., g_{P-1} - g_c). \tag{3}$$

From [7], we know that the distribution $t(g_c)$ is unrelated to local image texture. Consequently, it does not provide useful information for texture analysis. Meantime, Eq.(1) can be replaced by the following equation to describe the information about the textural characteristic.

$$T \approx t(g_0 - g_c, ..., g_{P-1} - g_c). \tag{4}$$

The highly discriminative texture operator records various of patterns in the neighborhood of each pixel in a P-dimensional histogram. On the edge of a region with slow slope, this operator records the difference in the gradient direction and zero values along the edge, and for each spot, all directions are different.

The change of the mean luminance has no effect on the signed different $(g_p - g_c)$. Consequently, the joint difference distribution is invariant against gray-scale change. We can obtain approximate values instead of their exact values.

$$T \approx t(s(g_0 - g_c), ..., s(g_{P-1} - g_c)), \tag{5}$$

where

$$s(x) = \begin{cases} 1, & x \geq 0 \\ 0, & x < 0 \end{cases} \tag{6}$$

When each sign $s(g_p - g_c)$ gets a binomial factor 2^p, Eq.(5) can be transformed into a unique $LBP_{P,R}$ to characterize the spatial structure of the local image texture as follows.

$$LBP_{P,R} = \sum_{p=0}^{P-1} s(g_p - g_c)2^p \tag{7}$$

Local Binary Pattern, as the name of the operator, reflects of the function of the operator. The U value of an LBP pattern is defined as the number of spatial transitions(changes between 0 and 1) in that pattern [9].

$$U(LBP_{P,R}) = |s(g_{p-1} - g_c) - s(g_0 - g_c)| + \sum_{p=1}^{P-1} |s(g_p - g_c) - s(g_{p-1} - g_c)|. \tag{8}$$

For example, the LBP pattern $(11111111)_2$ has a U value of 0 and $(01000000)_2$ has a U vale of 2. From literature [7], we know that the patterns having the U value of at most 2 are defined as uniform patterns. It is demonstrated that the "uniform" patterns are the essential patterns of local image texture.

In [9], it shows an example of all uniform patterns for $P = 8$. The $LBP_{P,R}$ operator generates 2^P different output values. As a matter of fact, after the $LBP_{P,R}$ being mapped to $LBP^{u2}_{P,R}$, it will produce $P \times (P-1) + 3$ different output values. The superscript $u2$ of $LBP^{u2}_{P,R}$ means that the U value of the uniform patterns is not larger than 2.

From [9], we know that there are so many uniform patterns of a rotated version(the number of the "1" is constant for a eight-digit binary) though in the case of $P = 8$. Hence, a new pattern with rotation invariant can be defined as

$$LBP_{P,R}^{riu2} = \begin{cases} \sum_{p=0}^{P-1} s(g_p - g_c), & ifU(LBP_{P,R}) \leq 2 \\ P+1, & otherwise \end{cases} \tag{9}$$

where $LBP_{P,R}^{riu2}$ has $P + 2$ independent output values. Suppose that a texture image is $M \times N$, after operated by the $LBP_{P,R}^{riu2}$ pattern of each pixel (i, j), the whole region is represented by a histogram:

$$H^{riu2}(k) = \sum_{i=1}^{M} \sum_{J=1}^{N} f(LBP_{P,R}^{riu2}(i,j), k), k \in [1, K] \tag{10}$$

$$f(x,y) = \begin{cases} 1, & x = y \\ 0, & otherwise \end{cases} \tag{11}$$

where K is the number of $LBP_{P,R}^{riu2}$ independent output values $(P + 2)$. In this paper, we employ $H^{riu2}(k)$ as the feature of the image blocks.

3. **Proposed scheme.** The diagram of the proposed scheme is shown in Fig.2. The detection method is divided into four steps. First of all, the image is transformed into gray scale, and then the gray scale image is filtered by the low pass filter. Secondly, we divide the gray scale image into overlapping circular blocks, and then compute the LBP of each block and use lexicographical sorting to store all feature vectors. Thirdly, we compute the Euclidean distance of the feature vectors and find out corresponding blocks. At last, we reduce the false matches using a specially designed filter and morphological operations, producing the detection map.

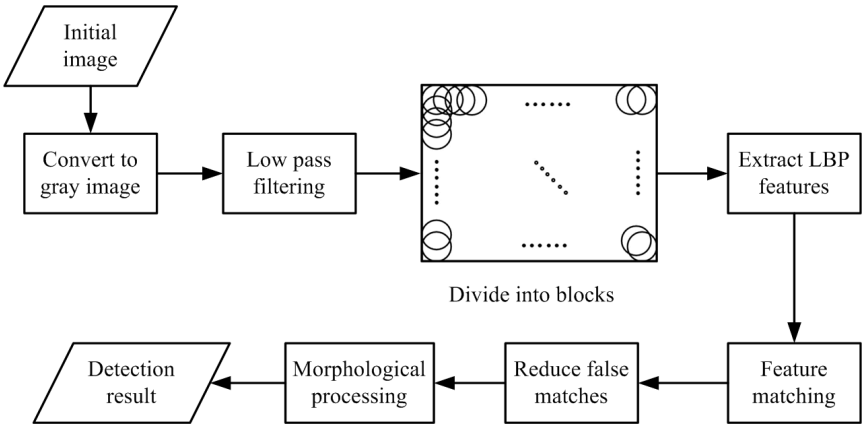

FIGURE 2. Diagram of the proposed scheme.

3.1. **Pre-processing.** The proposed scheme operates in gray scale domain. For a color image in RGB model, we first transform it into gray scale using the following equation.

$$I = 0.299R + 0.587G + 0.114B. \tag{12}$$

It is well known that the high frequency components are not stable if the image is suffered from signal processing operations, such as JPEG compression, noise contamination and so on. The low frequency features are more stable compared to the high frequency ones. Therefore, the low frequency features are used in the subsequent copy-move forgery

detection. In experiments, we find that adding more than two times of low pass filtering can improve the detection performances, especially in the case of signal processing operations. We will detail later in the experiments. In this paper, the Gaussian low pass filter is adopted. The standard deviation of the filter is 2.0 and the filter size is 5×5.

In order to find out the forged regions, the image is usually divided into overlapping blocks. Most of the existing schemes use square blocks. However, circular blocks are used in the proposed method. For an image, we divide it into overlapping circular blocks, and the diameter is $2r$. The adjacent blocks have only one different row or column. The size of the image is denoted by $W \times H$, where W and H are the size of the column and row. Consequently, the image is divided into $(W-2r+1) \times (H-2r+1)$ circular blocks in all.

3.2. **Feature extraction from the blocks.** In this paper, rotation invariant uniform local binary pattern (LBP) is used for extracting features of circular blocks. For an image, $(W-2r+1) \times (H-2r+1)$ LBP features can be extracted. We then sort the features of each block into a row array, and set all the arrays as a matrix $\mathcal{S}$, which contains $(W-2r+1) \times (H-2r+1)$ rows.

When the features of all blocks are extracted, the matches will be found from the blocks. It is obvious that similar blocks should have similar features. However, if a feature is matched with all the rest features, the computation cost will be significantly high, especially when the size of the image is large. In order to reduce the time of matching, the similar feature vectors will be stored into the neighbor rows by lexicographical sorting. In this way, similar blocks will locate at the neighboring rows and feature matching can be achieved in a small range.

3.3. **Feature matching.** Block matching is to find out the corresponding blocks, and to detect the forged regions correctly. In the proposed scheme, we search for the corresponding blocks by estimating the Euclidean distances of the feature vectors. In order to detect the forged region correctly, the distance threshold T_d and the threshold of similarity T_s should be predetermined. Since the feature vectors of the blocks are quite similar with each other which have the overlapping pixels, only the blocks with the distance larger than the diameter are compared.

The matching of the blocks starts from the first row of the matrix $\mathcal{S}$. For a feature located in the *ith* row $\mathcal{S}_i$, the distance with the following α rows will be computed, and the smallest distance, denoted by $D(i,\beta)$ here, between the *ith* row and the following α rows can be obtained.

$$D(i,\beta) = min\{D(i,i+1), D(i,i+2), ..., D(i,i+\alpha)\}. \tag{13}$$

If $D(i,\beta)$ is smaller than a threshold T_s, the corresponding blocks will be regard as correctly matched. Then the locations of the two blocks are stored. The matching will be repeated for all rows of $\mathcal{S}$. At last, all the matched block pairs are saved in a set Ω.

3.4. **Post-processing of the detection result.** When all the matched block pairs are saved in the set Ω, the forged regions can be determined, which is achieved by marking the copied region and the forged region. Generally speaking, the regions are stamped on a binary image. That is to say, all the detected blocks including the original blocks and tampered blocks are marked to generate a detection map. In this paper, we mark the innermost few pixels instead of the entire block. In implementation, we mark a circular area with the radius of one pixel. Marking the innermost five pixels has the advantage of generating fine edge in the detection map. Fig.3(b) shows an example of the proposed method of marking.

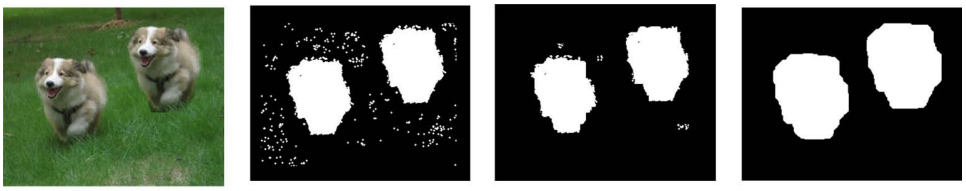

FIGURE 3. Post-processing. (a) forged image, (b) initial detection result, (c) image after filtering, (d) result after morphological operation.

In general, there are some falsely detected blocks marked on the initial detection map, and these false blocks should be removed. To this end, we design a filter to remove them. The proposed filter operates as follows. First, we generate a sliding window with the size of 8×8, and move it from left to right and up to bottom. Each time, the window moves forward by 8 pixels to make sure all the pixels of the image will be filtered and each pixel will be filtered only once. If the number of "white" pixels is less than 15 in the window, all pixels of the window are marked as black. Otherwise, keep the number of the white pixels and do nothing. After filtering, some small isolated false matches can be removed. Fig.3(c) shows the detection result after the proposed filtering operation.

It is seen from Fig.3(c) that there are still some isolated regions after filtering. In order to remove the isolate regions, the morphological processing is introduced. Morphological erosion is first conducted to remove the larger regions. Then morphological dilation is conducted to make sure that detected regions are as large as their original sizes.

4. **Experimental results and analysis.** In experiment, the test images are collected from the Internet, and the copy-move forgery is performed using Photoshop. All simulations are performed on a personal computer with 2.4GHz CPU and 2GB memory.

The P and R of the rotation invariant uniform LBP are set to 24 and 3. The diameter of the circular block is 18. The similarity threshold is set to $T_s = 6.2$, which is determined by experiments. In experiments, the search range of the block matching is 30. Fig.4 shows two groups of simulation results when no attacks are conducted, including original images, tampered images and the detection maps. Fig.4 shows that when a region is copied and pasted to another regions of the same image, the detection result is satisfactory in case of no attacks.

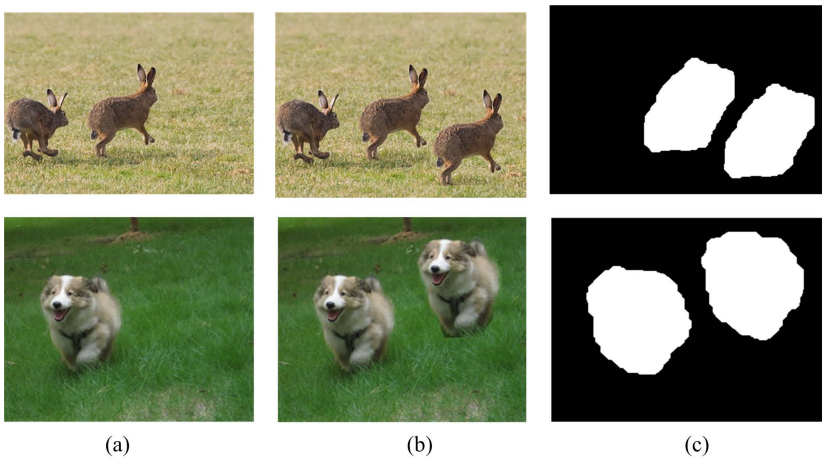

FIGURE 4. Detection results without any attack. (a) Original image, (b) Forged image, (c) Detection result.

4.1. **Robustness against rotation and flipping.** The advantage of the proposed scheme is that it can resist region rotation and flipping. The simulation results and comparisons with those of literatures [6] and [8] are shown in Fig.5 and Fig.6.

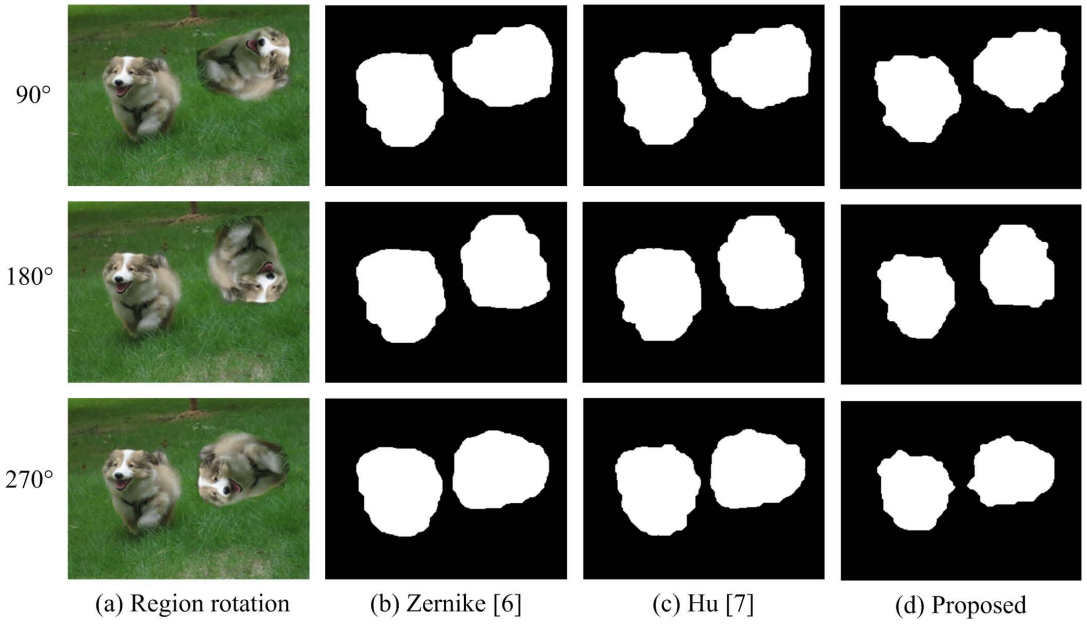

FIGURE 5. Detection results on region rotation.

Fig.5 shows the results when the copied region is rotated by 90, 180 and 270. From the test results we know that the forged regions can be detected accurately. Furthermore, as a spatial domain feature based detection method, the proposed algorithm is comparable to the invariant moment based methods. The reason is that when the image is rotated by 90, 180 or 270 degrees, there is no interpolation error. Consequently, block matching is very accurate.

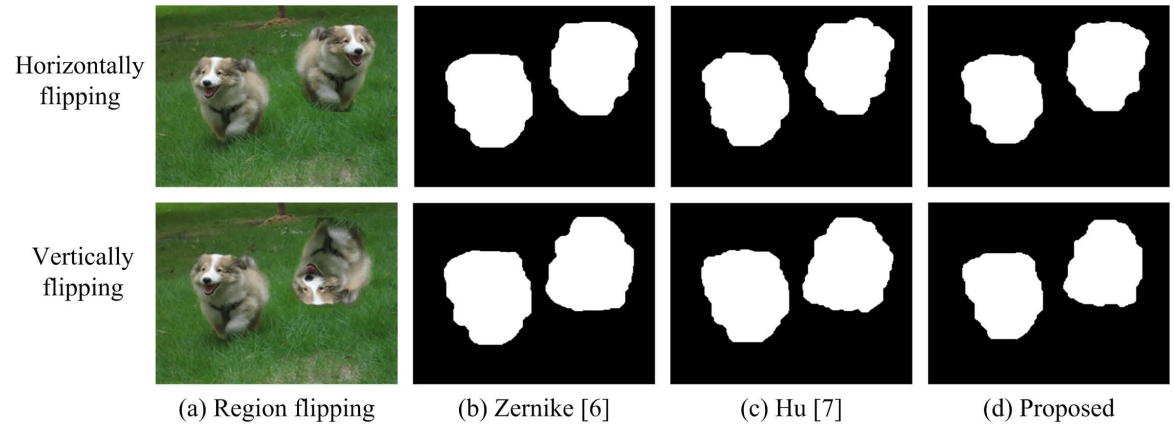

FIGURE 6. Detection results on region flipping.

Region flipping is also a needful trick for copy-move forgery, where the copied region is flipped horizontally or vertically before being pasted. From Fig.6, we know that the proposed method is robust to flipping, both horizontally and vertically. The proposed scheme and the compared two methods perform similarly.

4.2. **Robustness against common attacks.** The proposed method is also robust to the traditional signal processing attacks. Fig.7 shows the experimental results when the image is subject to JPEG compression, added white Gaussian noise (AWGN) and Gaussian blurring. For JPEG compression, five different quality factors are employed, namely 50, 60, 70, 80 and 90. For AWGN, the signal to noise ratio(SNR) of the contaminated image is 15dB, 20dB, 25dB, 30dB and 35dB, respectively. For Gaussian blurring, the size of the window is 5, and the standard deviations are 1, 2, 3, 4 and 5 as shown in the third row of Fig 7.

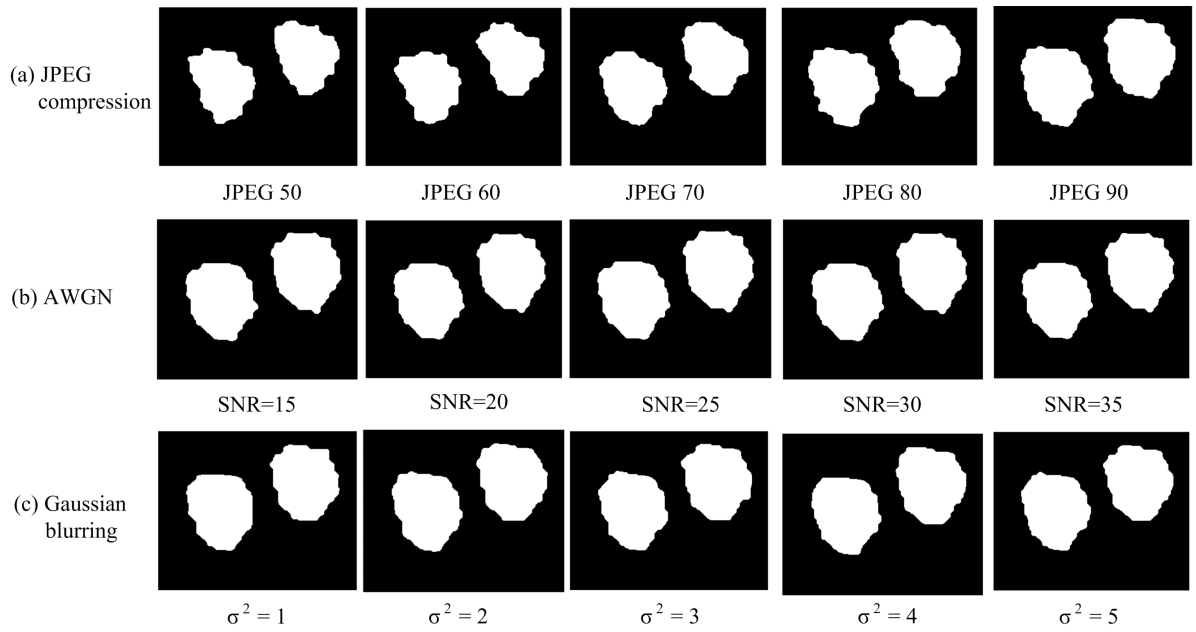

FIGURE 7. Detection results on signal processing operations.

From Fig 7, we know that the proposed scheme can detect the forged regions with high accuracy. For JPEG compression, the detection results becomes worse with the decline of the quality factors. However, by large number of experiments, we find that the proposed method can successfully detect the forged regions even when the quality factor is lower than 40. For AWGN, the SNRs have little effect on the detection results. Similar results are obtained for Gaussian blurring.

4.3. **Evaluation on the times of low pass filtering.** The good performance to the signal processing attacks is attributed to the application of the low pass pre-filtering operation. Especially in the case of JPEG compression and AWGN, the low pass filtering can remove the high frequency components, which is important for the proposed scheme. In implementation, we find that the times of low pass filtering have strong influence on the performance to signal processing attacks.

Fig.8 shows the detection results when different JPEG quality factors and different times of filtering are applied. It is known from the figure that the time of filtering is related to the overall performance directly. Generally, the detection performance improves with increasing times of low pass filtering, which is particularly true for high strength JPEG compressions. In experiments, we find that five times of filtering is an optimal option.

4.4. **Evaluation of the performance.** In this paper, the correct detection ratio F_c and the false detection ratio F_f are employed to evaluate the performance of the proposed method, which are defined as follows.

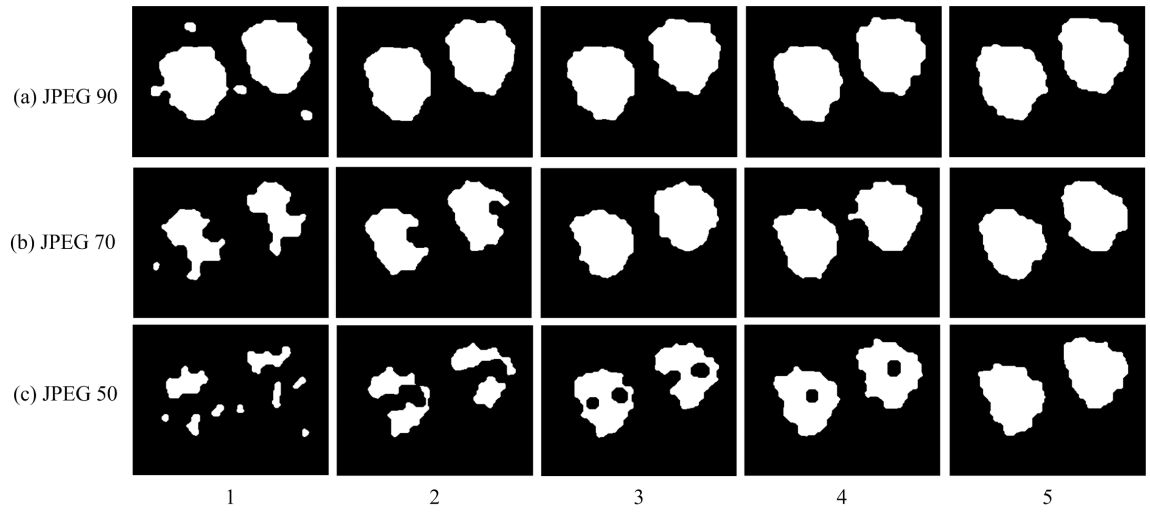

FIGURE 8. Detection results with different JPEG quality factors and different times of filtering.

$$F_c = \frac{|C_1 \bigcap C_2| + |M_1 \bigcap M_2|}{|C_1| + |M_1|}, \tag{14}$$

$$F_f = \frac{|C_1 \bigcup C_2| + |M_1 \bigcup M_2|}{|C_1| + |M_1|} - 1, \tag{15}$$

where C_1 is the original copied region and M_1 is the forged region, while C_2 and M_2 are the detected copied region and the detected tampered region respectively.

In order to evaluate of the proposed scheme, we conduct experiments on two image databases. The first database we build, Database 1, contains 100 images. All pictures are collected from the internet. Another database, Database 2, is the UCID-an Uncompressed Color Image Database [10], which contains more than 1300 images. For Database 2, we choose 100 images and use them in our experiments. In implementtaion, a 80×80 block is copied and pasted to another region of the same image. The tampered images are suffered from the signal processing attacks, including JPEG compression, AWGN and Gaussian Blurring. Fig.9 to Fig.11 show the simulation results.

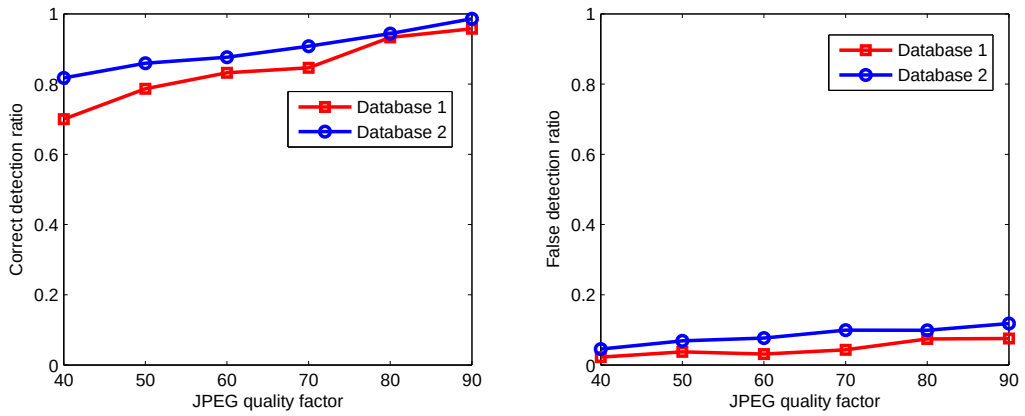

FIGURE 9. Correct detection ratio and false detection ratio on JPEG compression. Left: Correct detection ratio, Right: False detection ratio.

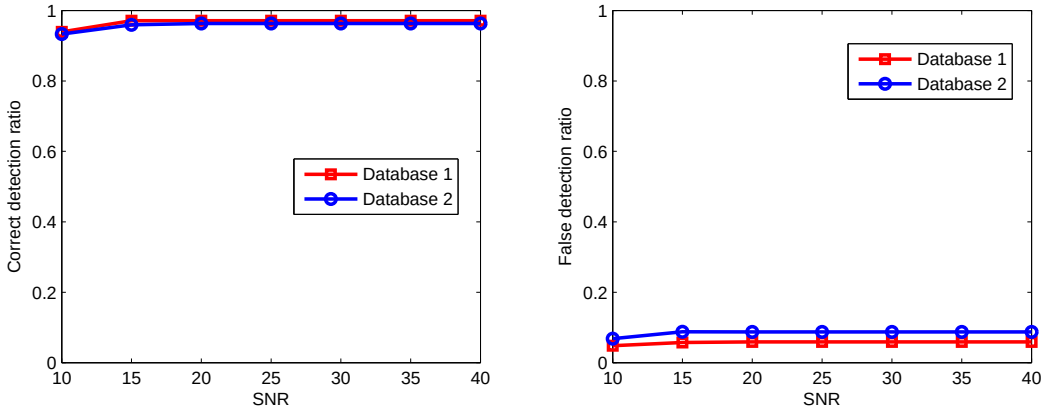

FIGURE 10. Correct detection ratio and false detection ratio on AWGN. Left: Correct detection ratio, Right: False detection ratio.

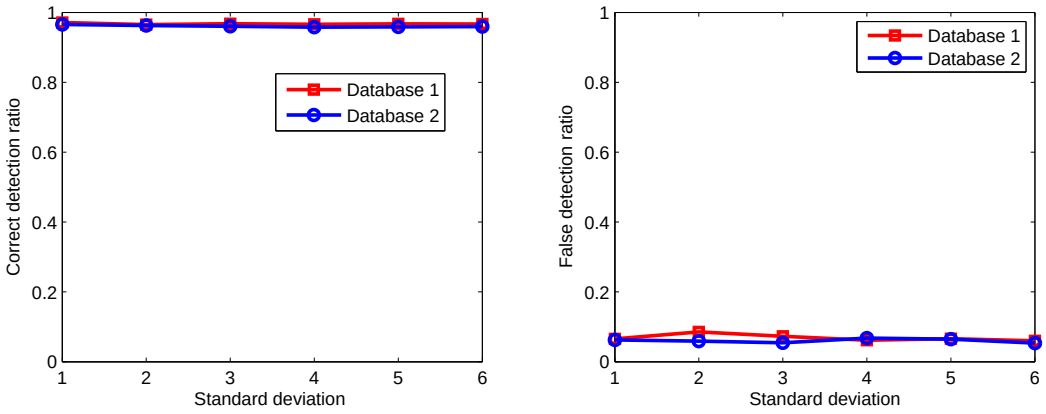

FIGURE 11. Correct detection ratio and false detection ratio on Gaussian blurring. Left: Correct detection ratio, Right: False detection ratio.

It is known form the figures that the overall performance of the proposed scheme is promising. For JPEG compression, most of the correct detection ratios are higher than 0.8 and the false detection ratios are lower than 0.1. The correct ratios are lower when the JPEG quality factors fall below 50. For AWGN and Gaussian blurring, similar results are obtained, where the correct ratios are all higher than 0.9 and the false ratios are all lower than 0.1.

5. **Conclusion.** Copy-move forgery is a very common way to tamper an image. Many researchers have proposed various schemes to detect the tampered images. However, sometimes the copied regions are rotated or flipped before being pasted. In this paper, we propose a novel method to detect this kind of images. The main contribution of this paper is that our scheme is robust not only to the traditional signal processing operations, but also to the rotation and flipping. We take advantage of low pass filtering before the image is divided into overlapping blocks, and achieve promising results. By large number of experiments, we demonstrate the advantages of the proposed scheme. A deficiency of the proposed scheme is that when the region is rotated by general angles, it is difficult to detect the forgeries. The future work is to investigate the invariant block features and appropriate selection of the dimension of the features to make the method robust to random region rotations.

Acknowledgment. This work is supported by Opening Project of Shanghai Key Laboratory of Integrate Administration Technologies for Information Security (AGK2012002), Fundamental Research Funds for the Central Universities (2012QNA59), China Postdoctoral Science Foundation (201104586, 20100471415) and National Natural Science Foundation of China (60802077).

REFERENCES

[1] J. Fridrich, D. Soukal, and J. Lukas, Detection of copy-move forgery in digital images, *Proc. of the digital forensic research workshop*, 2003.

[2] A. C. Popescu, and H. Farid, Exposing digital forgeries by detecting duplicated image regions, *Proc. of Technical report TR2004-515*, Dartmouth College, 2004.

[3] W. Q. Luo, J. W. Huang, and G. P. Qiu, Robust detection of region-duplication forgery in digital image, *Chinese Journal of Computers*, vol. 30, no. 11, pp. 1998-2007, 2007.

[4] Y. P. Huang, W. Lu, W. Sun, and D. Y. Long, Improved DCT-based detection of copy-move forgery in images, *Journal of Forensic Science International*, vol. 206, no.1-3, pp. 178-184, 2011

[5] B. Mahdian, and S. Saic, Detection of copy-move forgery using a method based on blur moment invariants, *Journal of Forensic Science International*, vol. 171, no. 2-3, pp. 180-189, 2007

[6] S. J. Ryu, M. J. Lee, and H. K. Lee, Detection of copy-rotate-move forgery using Zernike moments, *Proc. of the 12th International Conference on Information Hiding*, pp. 51-65, 2010.

[7] G. J. Liu, J. W. Wang,S. G. Lian, and Z. Q. Wang, A passive image authentication scheme for detecting region-duplication forgery with rotation, *Journal of Network and Computer Applications*, vol. 34, no. 5, pp.1557-1565, 2011.

[8] T. Ojala, M. Pietik*ä*inen, and T. M*ä*enp*ää*, Multiresolution gray-scale and rotation invariant texture classification with local binary patterns, *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 24, no. 7, pp. 971-987, 2002.

[9] Z. Li, G. Z. Liu, Y. Yang, and J. Y You, Scale- and rotation-invariant Local Binary Pattern using scale-adaptive texton subuniform-based circular shift and subuniform-based circular shift, *IEEE Trans. Image Processing*, vol. 21, no. 4, pp. 2130-2140, 2012.

[10] Z. H. Guo, L. Zhang, and D. Zhang, Rotation invariant texture classification using LBP variance(LBPV) with global matching, *Journal of Pattern Recognition*, vol. 43, no. 3, pp. 706-719, 2010.

[11] G. Schaefer, and M. Stich, UCID-An Uncompressed Colour Image Database, Technical Report, School of Computing and Mathematics, Nottingham Trent University, U.K., 2003.