Robust Copy-Move Forgery Detection Based on Dual-Transform

Munkhbaatar Doyoddorj[1] and Kyung-Hyune Rhee[2](✉)

[1] Department of Information Security, Pukyong National University,
Busan, Republic of Korea
d_mbtr@pknu.ac.kr

[2] Department of IT Convergence and Application Engineering,
Pukyong National University, 599-1, Daeyeon3-Dong, Nam-gu,
Busan 608-737, Republic of Korea
khrhee@pknu.ac.kr

Abstract. With the increasing popularity of digital media and the ubiquitous availability of media editing software, innocuous multimedia are easily tampered for malicious purposes. Copy-move forgery is one important category of image forgery, in which a part of an image is duplicated, and substitutes another part of the same image at a different location. Many schemes have been proposed to detect and locate the forged regions. However, these schemes fail when the copied region is affected by post-processing operations before being pasted. To rectify the problem and further improve the detection accuracy, we propose a robust copy-move forgery detection method based on dual-transform to detect such specific artifacts, in which a cascade of Radon transform (RT) and Discrete Cosine Transform (DCT) is used. It will be shown that the dual-transform coefficients well conform the efficient assumption and therefore leads to more robust feature extraction results. Experimental results demonstrate that our method is robust not only to noise contamination, blurring, and JPEG compression, but also to region scaling, rotation and flipping, respectively.

Keywords: Passive image forensics · Copy-move forgery · Dual-transform · Duplicated region detection · Mixture Post-processing

1 Introduction

With the ever increasing diffusion of simple and powerful software tools for digital source editing, image tampering is becoming more common, stimulating an intense quest for algorithms, to be used in the forensics field, which help deciding about the integrity of digital images. Furthermore, it is necessary for us

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2013R1A1A4A01009848) and a Research Grant of Pukyong National University (2013-0472).

P. Gladyshev et al. (Eds.): ICDF2C 2013, LNICST 132, pp. 3–16, 2014.
DOI: 10.1007/978-3-319-14289-0_1

to develop automatic methods to authenticate the images and indicate potential forgeries.

In order to protect the integrity and reveal the manipulation of digital media, two types of countermeasures, active and passive approaches, are extensively investigated in previous studies. Active approach, including digital signature, watermarking, and *etc.*, relies on pre-processing before distribution, which requires additional and shared information. However, there is no universally recognized standard, and the complexity greatly restricts its application. On the other hand, the passive approach only requires digital media without any supplemental information.

Due to the variety of manipulations and the diversity of individual characteristics of media, passive approach usually faces difficulties at a larger scope, and suffers from complicated and time consuming problems [11].

One of the most common types of image forgeries is the copy-move forgery [12], where a region from one part of an image is copied and pasted onto another part in same image, thereby concealing the image content in the latter region. Such concealment can be used to hide an undesired object or increase the number of objects apparently present in the image. Although a simple translation may be sufficient in many cases, additional operations are often performed in order to better hide the tampering. These include rotation, scaling, lossy compression, noise contamination, blurring, and among others. Also, the copied part comes from the same image, all of its properties and statistic information are the same as the rest of the image. Thus, it is difficult to detect forgeries by techniques that compare statistics of different part of an image to each other. Hence, in order to be able to reliably detect such forgeries, a several techniques have been recently proposed which try to be robust to some of these transformations.

In the literature, researchers have developed various techniques. Huang *et al.* [1] proposed improved robustness using a discrete cosine transform (DCT) to noise addition, global blurring and lossy compression, but does not deal with geometrical transformations of the tampered region. The method of Khan *et al.* [2] reduces the time complexity of the PCA-based approach by using a discrete wavelet transform (DWT), but also does not address geometrical transformations. In [3], Mahdian *et al.* 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. Ryu *et al.* [4] 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. In [5], 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.

Our contributions. The aim of this paper is to demonstrate a robust copy-move forgery detection method for passive image forensics through a construction of the invariant features from dual-transform, such as Radon and discrete cosine transforms. The key insight of our work is that the copied region concealed with post-processing operations before being pasted in same image, the invariant image features are detectable by using the ability of such transform even if the feature strength is weakened. When the position of the copied part is unknown, we able to detect the exact pasted position that using the extracted invariant features, under the assumption that the pasted regions will yield similar features with the copied regions.

In the proposed method, Radon transform is utilized to project the image onto directional projection space, and then 1-D DCT is used to extract significant frequency features from the Radon space. Dual-transform largely reduces the influence of geometrical and image processing operations, and the invariant feature of the dual-transform coefficients is found to be stable. Extensive comparative studies show the superiority and robustness of the proposed method.

The remainder of the paper is organized as follows. Section 2 introduces the concept of the dual-transform, which includes Radon and DCT transforms. The proposed method is presented in Sect. 3. The experimental results are provided in Sect. 4. Conclusion is drawn in Sect. 5.

2 The Concept of the Dual-Transform

2.1 Radon Transform (RT)

Applying Radon transform on an image $f(x, y)$ for a given set of angles can be thought of as computing the projection of the image along the given angles [6]. The resulting projection is the sum of the intensities of the pixels in each direction, *i.e.* a line integral. For an image $f : \mathbb{R} \times \mathbb{R} \rightarrow [0, 255]$ containing an object, the result g of Radon transform is a function $\mathcal{R} : \mathbb{R} \times [0, 2\pi] \rightarrow \mathbb{R}_+$ defined as:

$$g(s, \vartheta) = \mathcal{R}(f(x, y)) = \int_{-\infty}^{\infty} f(s\cos\vartheta - t\sin\vartheta, s\sin\vartheta + t\cos\vartheta)dt \qquad (1)$$

$$\begin{bmatrix} s \\ t \end{bmatrix} = \begin{bmatrix} \cos\vartheta & \sin\vartheta \\ -\sin\vartheta & \cos\vartheta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \qquad (2)$$

Radon transform of the translated, rotated and scaled images exhibits interesting properties, which can be employed to construct a method for invariant object recognition. Therefore, the behavior of the transform for these three variations in the input image should be defined. Any translation in spatial domain leads in the Radon domain to translation in the s direction. The amount of the translation varies with the ϑ dimension. The scaling of the original image along both axes results in the scaling along the s axis in the Radon domain. The value of the transform is also scaled. The rotation in spatial domain leads to circular translation along the ϑ axis in the Radon domain. The behaviour of Radon transform is summarized in Table 1, and depicted in Fig. 1.

2.2 Discrete Cosine Transform (DCT)

Discrete cosine transform is used to know frequency components present in a image [7]. DCT mainly reduces the redundant information present in the image

Table 1. Behavior of Radon transform for rotated, scaled and translated images.

Behavior	Image function, f	Radon transform, $g = \mathcal{R}(f)$.
Original	$f(x, y)$	$g(s, \vartheta)$
Rotated	$f_{polar}(r, \vartheta_0 + \varphi)$	$g(s, (\vartheta + \vartheta_0) mod 2\pi)$
Scaled	$f(\alpha x, \alpha y)$	$\frac{1}{\lvert\alpha\rvert} g(\alpha s, \vartheta)$
Translated	$f(x - x_0, y - y_0)$	$g(s - x_0 \cos\vartheta - y_0 \sin\vartheta, \vartheta)$

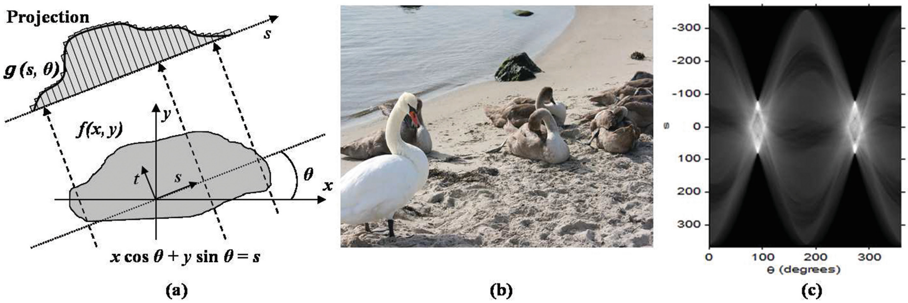


Fig. 1. Radon transform. (a) Image projection, (b) Test image, and (c) Its projection on Radon space.

by omitting the undesired parts of the image. Orthogonality, symmetry, separability, and decorrelation are important properties of DCT. The most common DCT definition of a 1D sequence of length N is

$$C(u) = \alpha(u) \sum_{x=0}^{N-1} f(x) \cos\left[\frac{\pi(2x+1)u}{2N}\right], \tag{3}$$

for $u = 0, 1, ..., N - 1$. In Eq. (3), $\alpha(u)$ is defined as

$$\alpha(u) = \begin{cases} \sqrt{\frac{1}{N}} & \text{for} \quad u = 0 \\ \sqrt{\frac{2}{N}} & \text{for} \quad u \neq 0. \end{cases} \tag{4}$$

The DCT coefficients for the transformed output image $C(u)$ with an input image $f(x)$ can be calculated by using the Eq. (3). N is the pixel dimensions of the input image $f(x)$. The intensity value of the pixel N of the image is given by $f(x)$ and $C(u)$ is the DCT coefficients in u of the DCT matrix.

3 Robust Copy-Move Forgery Detection

In this section, we present the proposed robust copy-move forgery detection method based on dual transform. At first, we describe a model for copy-move forgery in digital images, and then introduce our proposed method to detect such specific artifact.

3.1 Model for Copy-Move Forgery

The task of finding the copy-move forgery is that of finding at least two large similar regions. Given an image $f(x, y)$, the tampered image $f'(x, y)$, must subject to: $\exists$ regions D_1 and D_2 are subsets of D and a shift vector $d = (dx, dy)$, (we assume that $|D_1| = |D_2| > |D| * 0.85\,\%$ and $|d| > L$), $f'(x, y) = f(x, y)$ if $(x, y) \notin D_2$ and $f'(x, y) = f(x-dx, y-dy)$ if $(x, y) \in D_2$, where D_1 is the source and D_2 is the target region, $D_2 = D_1 + d$. We consider that the similarity of the target region is larger than $0.85\,\%$ of the image size. It would be easy to detect above forgery via exact match. However, to make the tampered image harder to detect, the attacker may perform various processing on $f'(x, y)$. Then the tampered image becomes $f''(x, y) = \xi(f'(x, y))$, where ξ is the post-processing operator, which includes geometrical and image processing operations. The post-processing attack makes the task of detecting forgery significantly harder. In the next section, we present an efficient method for detecting copy-move forgery which is also robust against various forms of post-processing operations.

3.2 The Proposed Method

Our proposed method is based on dual-transform, which includes Radon and discrete cosine transformations. This set of transformations were designed for an efficient and robust approach. The main issue in directly applying these tools to image forgery detection is that these tools were designed to find duplicate but separate, images, whereas we are trying to find identical regions in same image. We perform modifications in the feature extraction and matching processes to efficiently detect such forgery. Firstly, we apply Radon transform on each divided blocks to project the image into a directional projection space, then perform 1-D DCT to derive the frequency features from the Radon space. Following we select the DCT coefficients with low frequency by using a dimension reduction. Finally, an invariant robust features are extracted. The details of the proposed method is given as the following:

1. **Pre-processing.** Image is tiled by overlapping blocks of $b \times b$ pixels. Blocks are horizontally slid by one pixel rightwards starting with upper left corner and ending with the bottom right corner. The total number of overlapping blocks for an image of $M \times N$ pixels is $S_{blocks} = (M - b + 1) \times (N - b + 1)$, for each block $B_l (l = 1, ..., S_{block})$. For instance, an image with the size of 640×480 with blocks of size 8×8 yields $299,409$ overlapping blocks.
2. **Feature extraction.** Each block is applied Radon transform, the space is projected on the Radon space. The results of Radon transform are contained in the columns of a matrix with the number of projections generated being equal to the number of the defined angles, $(\vartheta_1, \vartheta_2, ..., \vartheta_n)$. Then, delete the rows in projection matrix, which are composed of 0. This will remove the redundancy data generated by Radon transform.

   On each projection (represented by column of the projection matrix) according to projection angles, we apply 1-D DCT to derive the frequency features from the Radon space. We quantize the coefficients according to the JPEG quantization table using a predetermined quality factor Q. The quantized coefficients can be denoted as $\mathrm{c}_k = \{c_1, c_2, ..., c_k\}$. The dimension reduction can make the sorting and matching faster. The frequency features are the nature of 1-D DCT that the energy of transformed DCT coefficients will be focused on the first several values (lower frequency values). Thus, those higher frequency coefficients can be truncated. The truncation can be done by saving only a part of vector components. Here, we define a factor $p, (0 < p \leq 1)$, that only first $\lceil p \times k \rceil$ DCT coefficients are saved for further processing. $\mathrm{c}_r = \{c_1, c_2, ..., c_r\}$, $(r = \lceil p \times k \rceil,\ r < k)$, where p denotes a saved the percentage of DCT coefficients and k denotes the number of coefficients on the projections according to angles ϑ_n. For example, we select the projection angle $\vartheta = 8$, and derived the 1-D DCT coefficients (column matrix 15 × 1) from the projection space. Five coefficients are deleted, which are composed of 0. The concentration of energy in 80 % is calculated as, $\lceil p * k \rceil = \lceil 0.8 * 10 \rceil = 8$ coefficients.

The truncated DCT coefficients in projection matrix are sorted by a lexicographically order. Let the matrix C denote the sorted vectors, the size of the matrix will be C_r^m.

$$C = \begin{bmatrix} \mathrm{C}_1^1 & \mathrm{C}_2^1 & ... & \mathrm{C}_r^1 \\ \mathrm{C}_1^2 & \mathrm{C}_2^2 & ... & \mathrm{C}_r^2 \\ . & . & ... & . \\ \mathrm{C}_1^m & \mathrm{C}_2^m & ... & \mathrm{C}_r^m \end{bmatrix}_{(M-b+1)(N-b+1)} \tag{5}$$

By using a lexicographic sorting, similar features will locate at the neighboring rows and the feature matching can be achieved in a small range.

3. **Similarity matching.** The feature matching is to find out the corresponding similar rows from between m rows of the C matrix. In order to detect the forged region correctly, the similarity threshold τ_s and the distance threshold τ_d should be predetermined, respectively. In our method, we search for the corresponding rows by estimating the Euclidean distance of feature vectors, as follows:

$$D(\mathrm{C}_r^m, \mathrm{C}_r^{m+v}) = \sqrt{\sum_{r=1}^{u} \mathrm{C}_r^m - \mathrm{C}_r^{m+v})^2} < \tau_s \tag{6}$$

If $D(\mathrm{C}_r^m, \mathrm{C}_r^{m+v})$ is smaller than a threshold τ_s, the corresponding features will be regard as correctly matched. Then the locations of two features are stored. The matching will be repeated for all rows of C. Since the feature vectors of the rows are quite similar with each other which have the overlapping pixels, only the rows with the actual distance between two similar features are compared as follows:

$$L(\mathrm{C}_r^m, \mathrm{C}_r^{m+v}) = \sqrt{(x_i - x_{i+j})^2 + (y_i - y_{i+j})^2} > \tau_d \tag{7}$$

where x and y are the coordinates of the corresponding features.

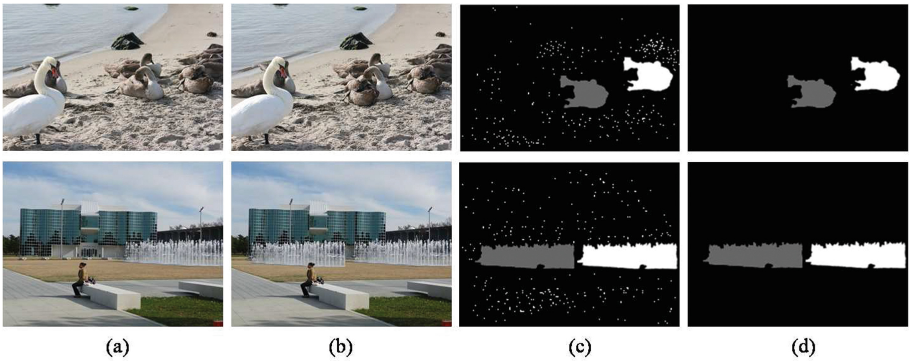


Fig. 2. Image forgery detection. (a) Original image, (b) Forged image, (c) Detected forgery with similar features, and (d) Results after filtering.

4. **Detection.** When all the matched feature pairs are saved, which is achieved by marking the copied and forged regions, respectively. Generally speaking, the regions are stamped on a binary image. That is to say, all the detected features including the forged and un-forged features are marked to generate a detection map. Fig. 2 shows an example of the proposed method for marking. In general, there are some falsely detected features marked on the initial detection map in Fig. 2(c), and these falsely detected features should be removed by filtering in Fig. 2(d). For the filtering, we generate a sliding window with the size of 8×8 pixels, 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 are less than 60 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. Figure 2(d) shows the detection result after the filtering operation.

4 Experimental Results

In this section, we present the experimental results of our proposed method. We simulated our method under a PC with 3.2G Hz Core i5 CPU, 8G RAM, and Windows 8 platform. The simulation was carried out using Matlab version R2008a. We test our method on Benchmark data for image copy-move detection dataset including 120 authentic and 124 forged color images of size 3888×2592 pixels with different outdoor scenes, as shown in Fig. 3. The authentic images were taken by different digital cameras. All tampered images in this dataset are generated from the authentic images by crop-and-paste operation using Adobe Photoshop CS3 version 10.0.1 on Windows XP. The tampered regions are from the same authentic image.

Fig. 3. Examples of test images.

4.1 Robustness Test for Feature Vectors

We extracted the features, which expressed by DCT coefficients of 1-D DCT based on the Radon space. These features will not change a lot after some post-processing operations. We have defined the model for copy-move forgery in Sect. 3.1. If an image is contaminated by additive Gaussian noise operation (AWGN), then the pixel value will be changed, for each pixel, we define $f(x,y) = \lfloor f(x,y) \rfloor + \xi_{noise}, (0 < \xi < 1)$, where $f(x,y)$ is the corresponding pixel value that contaminated by signal noise, $\lfloor f(x,y) \rfloor$ is the nearest value less than or equal to the original pixel value, ξ_{noise} is the random noise which is independent identically distributed. For instance, each noisy block $B'_i = B_i + \xi_{noise}$, and the extracted features $c'_r = c_r + \xi'_{noise}$, since $E(\xi'_{noise}) = 0$, $D(\xi'_{noise}) = \sum_{i=1}^{b^2} \xi'_{noise}/b^2$, generally $\sum_{i=1}^{b^2} (\xi')^2_{noise} \ll b^2$. Since we get $c'_r \approx c_r$. For the Gaussian blurring only affects in some high frequency components of each blocks, but changes in the low frequency components are a little. The robustness against

Table 2. The correlation coefficients for the feature vectors, $\vartheta = 8$, (8×8).

Vectors	Extracted, c_r	Post-processed, c_ξ					
		AWGN	AWGN	Blurring	Blurring	JPEG	JPEG
		SNR	SNR	w, σ	w, σ	Q	Q
		25dB	50dB	3, 1	5, 0.5	5	10
c_1	958.75	959.26	962.31	957.45	959.07	958.26	962.12
c_2	886.37	893.63	896.25	884.16	886.36	884.69	887.02
c_3	875.12	885.02	894.89	873.52	874.85	873.81	878.29
c_4	801.50	820.75	828.20	799.21	802.80	798.68	796.93
c_5	745.25	753.39	761.62	744.03	746.68	748.52	736.84
Correlation coefficients		0.9980	0.9804	1.0000	1.0000	1.0000	1.0000

the geometrical operations are provided by the property of Radon transform. In order to show the robustness of the feature vectors, we chose a size of block 8 × 8, 16 × 16, and 32 × 32, respectively, from the natural images. Then we applied some post-processing operations with different parameters. The results of robustness test are presented in Table 2. c_r and c_ξ are feature vectors that the extracted and post-processed vectors, respectively. After some post-processing, we calculate the correlation coefficients between them, if the result is close to 1, which implies the feature vector is robust and the invariance is more stable. The correlation coefficient is used as a measure of correlation, as it is invariant to intensity change. (Here we note that the extracted feature vectors are reduced by dimension reduction.)

4.2 The Evaluation of the Detection Performance

In order to quantify the accuracy of detection, the true positive ratio (TPR) and the false positive ratio (FPR) are employed, as follows:

$$TPR = \frac{|\varOmega_1 \bigcap \varOmega_2| + |\overline{\varOmega_1} \bigcap \overline{\varOmega_2}|}{|\varOmega_1| + |\overline{\varOmega_2}|}, \qquad FPR = \frac{|\varOmega_1 \bigcup \varOmega_2| + |\overline{\varOmega_1} \bigcup \overline{\varOmega_2}|}{|\varOmega_1| + |\overline{\varOmega_1}|} - 1 \qquad (8)$$

where $\varOmega_1$ and $\varOmega_2$ are the original copied region and the detected copied region, while $\overline{\varOmega_1}$ and $\overline{\varOmega_2}$ are the forged region and the detected forged region, respectively. In order to set the threshold parameters, we randomly chose 50 images from the dataset and then make a series of forgeries. After that, we use different the projection angles ranging from 8 to 64 degree with 8 increment, then a set of values for $\tau_s = 0.005$ and $\tau_d = 4$, respectively, from the number of testing results. The threshold parameters are chosen by highest true positive ratio with corresponding lowest false positive ratio. In order to decide the block size, we tested

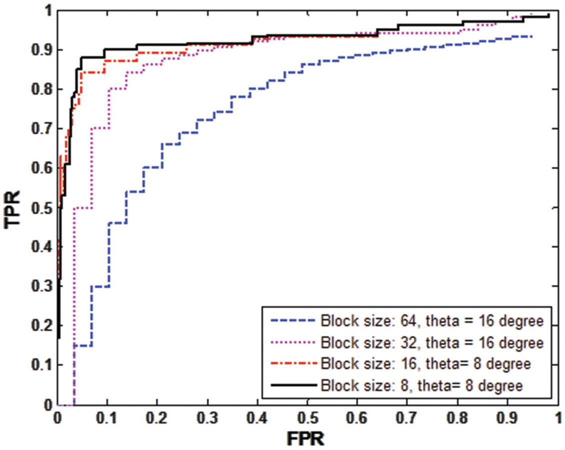


Fig. 4. Detection results for varying block sizes.

the TPR and FPR curves for various block sizes with a selection of different directional projection angles.

As shown in Fig. 4, we notice that smaller block size is resulted higher detectability property. But, large block size is indicated lowest detection performance. Therefore, we set the block size of 8 × 8 pixels in all our following experiments.

Table 3. The feature matching accuracies with various post-processing operations.

Operations		*Compression*			*Additive Gaussian noise*		
		JPEG 30	JPEG 60	JPEG 90	SNR 10	SNR 20	SNR 30
Rotation	10^o	0.979	0.982	0.987	0.969	0.971	0.975
	30^o	0.971	0.974	0.985	0.950	0.956	0.969
	45^o	0.963	0.966	0.976	0.936	0.938	0.948
Scaling	5	0.984	0.984	0.987	0.974	0.975	0.978
	10	0.982	0.983	0.988	0.968	0.971	0.979
	15	0.965	0.976	0.978	0.956	0.964	0.966
Blurring	3 × 3	0.970	0.972	0.976	0.931	0.948	0.951
	5 × 5	0.962	0.968	0.971	0.920	0.927	0.939
	7 × 7	0.927	0.931	0.935	0.901	0.917	0.919
Contrast changing	10	0.975	0.976	0.976	0.970	0.973	0.976
	30	0.973	0.970	0.974	0.960	0.966	0.968
	45	0.967	0.966	0.966	0.947	0.956	0.957
Rot. + Flip	10^o, Hor.	0.889	0.898	0.897	0.836	0.847	0.848
Sc. + Flip	10, Ver.	0.885	0.890	0.893	0.825	0.826	0.825
Rot. + Sc.	10^o, 10	0.738	0.768	0.787	0.704	0.731	0.747

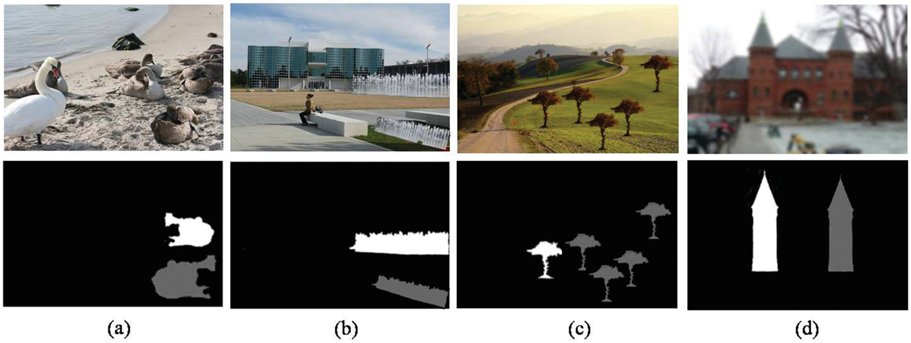
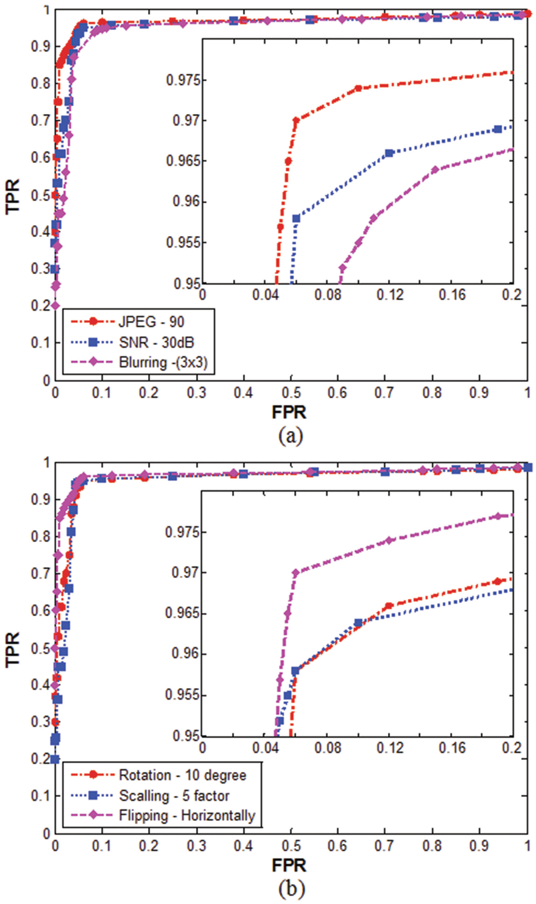


Fig. 5. Detection results with various mixture operations. (a) Object scaling with horizontally flipping, (b) Object scaling with rotation, (c) Multi-copy with JPEG, and (d) Blurring with scaling.



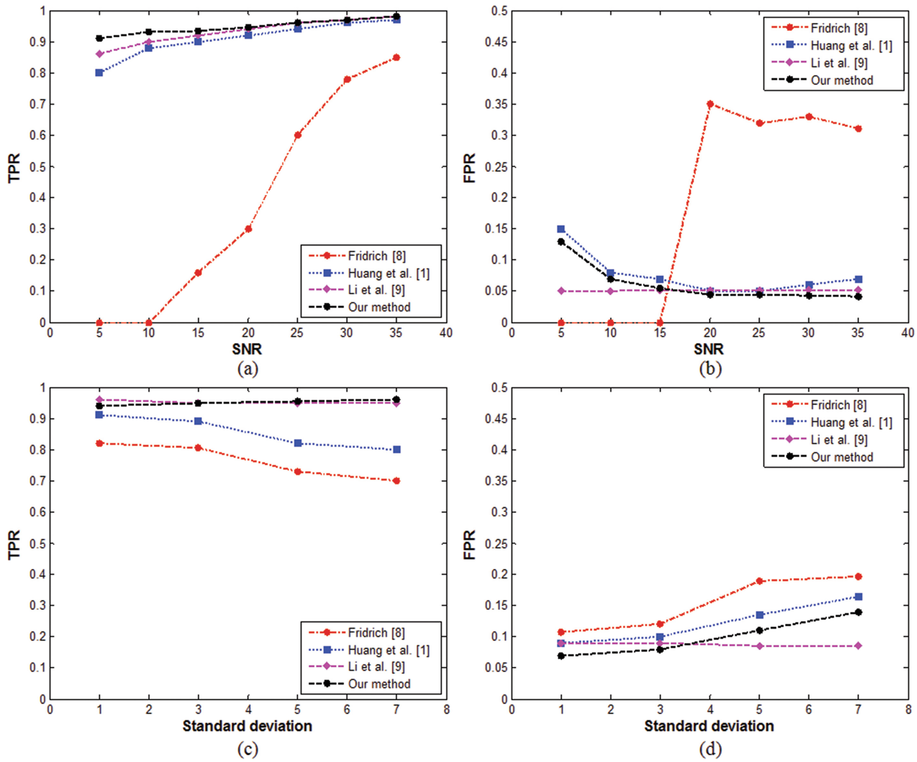
(a)

(b)

Fig. 6. Detection results with various attacks. (a) Image processing operations, and (b) Geometrical operations.

(a) The performance of the feature matching. We evaluated the feature matching process that the copied regions have been subjected to various geometrical operations (rotation, scaling and flipping) and image processing operations (blurring and contrast changing). Additionally varying the levels of lossy compression (JPEG) and the additive Gaussian noise (AWGN) were performed with mixture operations. The purpose of this testing is to highlight the performance of features that we have employed. The accuracies of the feature matching are determined by proportion of true positives in the matching feature pairs. The obtained results are reported in Table 3.

In Table 3, the mixture operations tend to have somewhat lower accuracy than other operations, which is shown at low quality factors and signal noise ratio (SNR). Especially, the accuracies for blurring and contrast changing indicate lower layer among of individual operations, respectively. Nevertheless, TPR and



(a) (b) (c) (d)

Fig. 7. Detection results with TPR/FPR curves. The performance comparisons (a–b) with different the SNR levels ($5dB \leq SNR \leq 35dB$), and (c–d) with Gaussian blurring (w $=$ 5, $\sigma = 1$ to 7).

FPR are quite acceptible even with low quality factors and signal noise ratio (SNR).

(b) The robustness against post-processing operations. The advantage of the proposed method is that it can resist against geometrical and image processing operations. In order to test the efficiency and robustness of our method further, we test all images from Benchmark dataset. For each image, a random sized region was copied then pasted onto a non-overlapping position, while the copied regions are distorted by different mixture post-processing operations. For instance, as shown in Fig. 5, the copied region is distorted by scaling with horizontal flipping, rotation with scaling, multi-copy with JPEG, and blurring with scaling, respectively. From the results we show that the forged regions can be detected accurately. Figure 6 presents the detection results of our method on various kind of individual post-processing operations. As can be seen, we are able to attain quite high accuracies at low false positive rates in selection of higher rate values. In the case of blurring, it can be seen that the resistance of such operation is lower than other post-processing operations.

(c) The performance comparisons. The overall average performance comparisons of our method with other related work are performed more precisely in this section. Some invariant feature extraction methods for copy-move forgery are presented in Fridrich [8], Huang *et al.* [1], and Li *et al.* [9]. As shown in Fig. 7(a–b), the forged images are contaminated with additive Gaussian noise ($5dB \leq SNR \leq 35dB$). Fridrich's method has the lowest TPR than other methods, when less than $10dB$, the TPR is approximate to zero. Observation of TPR in our method achieves higher TPR among other methods. For FPR, Fridrich's method has lower FPR value, that cannot detect any forged region, when the FPR is less than $15dB$. However, such method quickly leads to higher FPR when the SNR level is higher, which indicates it is sensitive to noise adding. Our method have a better performance with Li *et al.*'s method, however with lower FPR.

In case of blurring, the forged regions are blurred by a Gaussian blurring filter ($w = 5$, $\sigma = 1$ to 7). Figure 7(c–d) shows the TPR curve of our method has better performance followed by Li *et al.*'s method, however, the TPR curves of Fridrich and Huang *et al.* are drop significantly, when the blurring radius increased. In FPR, our method has the lowest value, even increased the larger blurring radius.

5 Conclusion

In this paper, we proposed a robust copy-move forgery detection method for a suspicious image. To extract an invariant robust features of a given image, we applied dual-transform. The extracted features are represented by lexicographically ordered DCT coefficients on the frequency domain from the Radon space, that each overlapped image blocks are projected by the columns of a matrix with the number of the defined angles ϑ_n on the Radon domain. Experimental results supported that the proposed method was appropriated to identify and localize the copy-move forgery even when though the forged region had been manipulated intentionally. The main contribution of our work is a method capable of easily detecting traces of various attacks. We concerned the geometrical and image processing operations, and any of their arbitrary combinations. The detection performance of our method is satisfactory enough and meets the robustness criteria.

References

1. Huang, Y., Lu, W., Sun, W., Long, D.: Improved DCT-based detection of copy-move forgery in images. J. Forensic Sci. Int. **206**(13), 178–184 (2011)
2. Khan, S., Kulkarni, A.: Reduced time complexity for detection of copy-move forgery using discrete wavelet transform. Int. J. Comput. Appl. **6**(7), 31–36 (2010)
3. Mahdian, B., Saic, S.: Detection of copy-move forgery using a method based on blur moment invariants. J. Forensic Sci. Int. **171**(27), 180–189 (2007)

4. Ryu, S.-J., Lee, M.-J., Lee, H.-K.: Detection of copy-rotate-move forgery using zernike moments. In: Böhme, R., Fong, P.W.L., Safavi-Naini, R. (eds.) IH 2010. LNCS, vol. 6387, pp. 51–65. Springer, Heidelberg (2010)
5. Liu, G.J., Wang, J.W., Lian, S.G., Wang, Z.Q.: A passive image authentication scheme for detecting region duplication forgery with rotation. J. Netw. Comput. Appl. **34**(5), 1557–1565 (2011)
6. Fiffy, M.A.: The radon transform and some of its applications. J. Mod. Optics. **32**(1), 3–4 (1985)
7. Khayam, S.A.: The Discrete Cosine Transform (DCT): Theory and Application. J. Inf. Theor. Coding, 1–31 (2003)
8. Fridrich, A.: Detection of copy-move forgery in digital images. In: Proceedings of the Digital Forensic Research Workshop, Cleveland OH, USA (2003)
9. Li, L., Li, S., Zhu, H.: An efficient scheme for detecting copy-move forged images by local binary patterns. J. Inf. Hiding Multimedia Signal Process. **4**(1), 46–56 (2013)
10. Christlein, V., Riess, R., Angelopoulou, E.: On rotation invariance on copy-move forgery detection. In: IEEE International Workshop on Information Forensics and Security, pp. 1–6 (2010)
11. Farid, H.: A survey of image forgery detection. IEEE Signal Process. Mag. **26**(2), 16–25 (2009)
12. Chrislein, V., Riess, R., Jordan, J., Angelopoulou, E.: An evaluation of popular copy-move forgery detection approaches. IEEE Trans. Inf. Forensics Secur. **7**(6), 1841–1854 (2012)