

Detection of Copy-Rotate-Move Forgery Using Zernike Moments

Seung-Jin Ryu, Min-Jeong Lee, and Heung-Kyu Lee

Department of Computer Science,
Korea Advanced Institute of Science and Technology,
Daejeon, Republic of Korea
{sjryu,mjlee,hklee}@mmc.kaist.ac.kr

Abstract. As forgeries have become popular, the importance of forgery detection is much increased. Copy-move forgery, one of the most commonly used methods, copies a part of the image and pastes it into another part of the the image. In this paper, we propose a detection method of copy-move forgery that localizes duplicated regions using Zernike moments. Since the magnitude of Zernike moments is algebraically invariant against rotation, the proposed method can detect a forged region even though it is rotated. Our scheme is also resilient to the intentional distortions such as additive white Gaussian noise, JPEG compression, and blurring. Experimental results demonstrate that the proposed scheme is appropriate to identify the forged region by copy-rotate-move forgery.

Key words: Digital Forensics, Copy-Move Forgery, Copy-Rotate-Move Forgery, Zernike Moments

1 Introduction

As the image processing softwares have been developed, even people who are not experts in image processing can easily alter digital images. It brings about great benefits, but also side effects: a number of tampered images have recently been distributed or have even been published by major newspapers. Therefore, it is important to verify the authenticity of digital images. Among forgery techniques using typical image processing tools, copy-move forgery is one of the most commonly used methods. The copy-move forgery copies a part of the image and pastes it into another part of the image to conceal an evidence or deceive people. Figure 1 shows an example of the altered photograph released by Iran and published by western media including The New York Times, The Los Angeles Times, BBC News, and *etc.* on July 9, 2008 [1]. In Fig. 1(a), two major sections (encircled in black) appear to be replicated from other sections (encircled in white). Actually Fig. 1(a) was released on the front pages of those of newspapers and lately corrected to the original image as Fig. 1(b).

The first method for detecting copy-move forgery was suggested by Fridrich *et al.* [2]. They lexicographically sorted quantized discrete cosine transform (DCT) coefficients of small blocks and then checked whether the adjusted blocks are

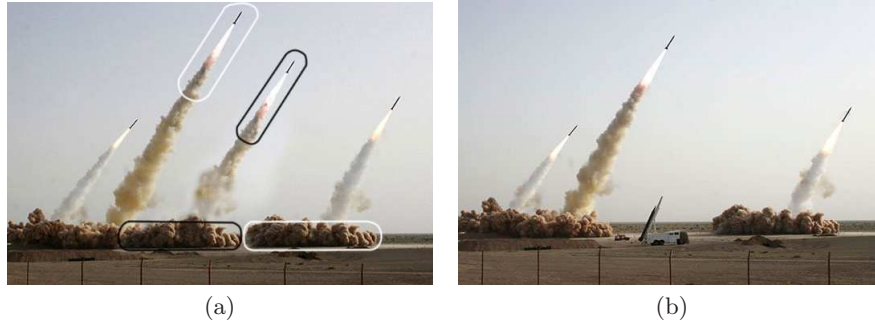


Fig. 1. An example of copy-move forgery [1]: (a) the forged image with four missiles and (b) the original image with three missiles.

similar or not. On the other hand, Popescu *et al.* employed principal component analysis (PCA) to extract important feature vectors and checked the similarity of blocks [3]. Similarly, Li *et al.* calculated the similarity of blocks based on discrete wavelet transform and singular vector decomposition (DWT-SVD) and Luo *et al.* measured block characteristics vector from each block [4, 5]. Mahdian *et al.* exploited blur invariant moments to detect duplicated regions [6]. Since they used the property invariant to blur, their scheme has robustness against post-processing such as blur degradation, additional noise, and arbitrary contrast changes.

Copy-move forgery as depicted in Fig. 1 usually means that the copied part of the image is pasted into another part of the image without any geometric change. However, people easily modify the geometry of the copied part so that the forged image seems to be original. Among the geometric modifications, rotation is commonly used to provide spatial synchronization between the copied region and its neighbors. In this paper, therefore, the forgery technique which copies a region and rotates it before pasting is named as copy-rotate-move (CRM) forgery. Figure 2 shows an example of CRM forgery. Fig. 2(a) is an original image and Fig. 2(b) and Fig. 2(c) are the forged images. In Fig. 2(b), the left aircraft (encircled in white) is copied and pasted into the image with no change. In Fig. 2(c), by contrast, the copied aircraft (encircled in black) is slightly rotated before pasting into the middle region. As seen with the naked eye, the rotated aircraft in Fig. 2(c) looks more natural than the duplicated aircraft in Fig. 2(b).

There are several papers for figuring out CRM forgery. Bayram *et al.* applied Fourier-Mellin transform to the block [7]. However, according to their experimental results, the scheme performed well when the degree of rotation is small. Bravo-Solorio *et al.* suggested to represent each block in log-polar coordinates [8]. Then they defined 1-D descriptor as summation of angle values to achieve rotational invariance. Since the method depends on the pixel values, it is sensitive to the change of the pixel values. There are some approaches that extracted interest points on the whole image by scale-invariant feature transform (SIFT)

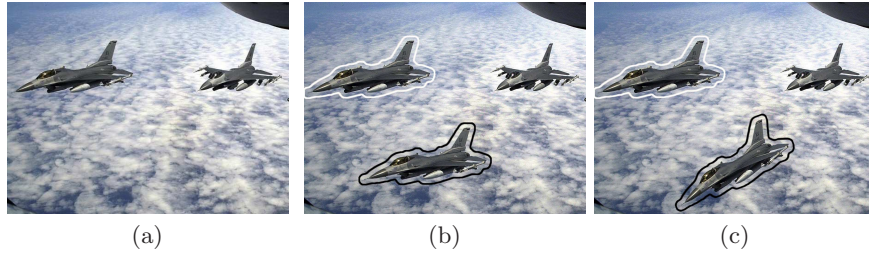


Fig. 2. An example of copy-rotate-move forgery: (a) the original image with two aircrafts, (b) the forged image with three aircrafts by copy-move forgery, and (c) the forged image with three aircrafts by copy-rotate-move (CRM) forgery.

[9–11]. Due to the fact that SIFT keypoints guarantee geometric invariance, their method enables to detect rotated duplication. However, these schemes still have a limitation on detection performance since it is only possible to extract the keypoints from peculiar points of the image.

In this paper, we propose detection scheme for copy-rotate-move (CRM) forgery using Zernike moments. Since the magnitude of Zernike moments are algebraically invariant against rotation, the proposed method can detect the forged region even though it is rotated before pasting. The proposed scheme also performs well when white Gaussian noise is added to the image, the image is compressed in JPEG format, and even blurred.

The rest of the paper is structured as follows. We first overview the Zernike moments in Sec. 2. The details of proposed method are explained in Sec. 3. Experimental results are then exhibited in Sec. 4 and Sec. 5 concludes.

2 Zernike moments

Moments and invariant functions of moments have been extensively used for invariant feature extraction in a wide range of pattern recognition, digital watermark applications and *etc.* [12, 13]. Of various types of moments defined in the literature, Zernike moments have been shown to be superior to the others in terms of their insensitivity to image noise, information content, and ability to provide faithful image representation [13–15]. In this section, we describe Zernike moments mathematically. Some of the materials in the following are based on [13, 15].

2.1 Definition

The Zernike moments [16] of order n with repetition m for a continuous image function $f(x, y)$ that vanishes outside the unit circle are

$$A_{nm} = \frac{n+1}{\pi} \int \int_{x^2+y^2 \leq 1} f(x, y) V_{nm}^*(\rho, \theta) dx dy, \quad (1)$$

where n a nonnegative integer and m an integer such that $n - |m|$ is nonnegative and even. The complex-valued functions $V_{nm}(x, y)$ are defined by

$$V_{nm}(x, y) = V_{nm}(\rho, \theta) = R_{nm}(\rho) \exp(jm\theta), \quad (2)$$

where ρ and θ represent polar coordinates over the unit disk and R_{nm} are polynomials of ρ (Zernike polynomials) given by

$$R_{nm}(\rho) = \sum_{s=0}^{(n-|m|)/2} \frac{(-1)^s [(n-s)!] \rho^{n-2s}}{s! (\frac{n+|m|}{2}-s)! (\frac{n-|m|}{2}-s)!}. \quad (3)$$

Note that $R_{n,-m}(\rho) = R_{nm}(\rho)$. These polynomials are orthogonal and satisfy

$$\int_{x^2+y^2 \leq 1} [V_{nm}^*(x, y)] \times V_{pq}(x, y) dx dy = \frac{\pi}{n+1} \delta_{np} \delta_{mq}, \quad (4)$$

where $\delta_{ab} = \begin{cases} 1, & a = b \\ 0, & \text{otherwise} \end{cases}$

For a digital image, the integrals are replaced by summations. To compute the Zernike moments of a given block, the center of the block is taken as the origin and pixel coordinates are mapped to the range of the unit circle. Those pixels falling outside the unit circle are not used in the computation. Note that $A_{nm}^* = A_{n,-m}$.

Suppose that one knows all moments A_{nm} of $f(x, y)$ up to a given order n_{max} . A discretized original image function $\hat{f}(x, y)$ whose moments are those of $f(x, y)$ up to the given order n_{max} can be computed. By orthogonality of the Zernike basis, we can reconstruct $\hat{f}(x, y)$ as

$$\hat{f}(x, y) = \sum_{n=0}^{n_{max}} \sum_m A_{nm} V_{nm}(\rho, \theta). \quad (5)$$

Note that as n_{max} approaches infinity, $\hat{f}(x, y)$ will approach $f(x, y)$.

2.2 Rotational Invariance of Zernike Moments

This section proves algebraic invariance of Zernike moments against rotation. Consider a rotation of the image through angle α . If the rotated image is denoted by f' , the relationship between the original and rotated image in the same polar coordinate is

$$f'(\rho, \theta) = f(\rho, \theta - \alpha). \quad (6)$$

From Eq. (1) and (2), we can construct

$$\begin{aligned} A_{nm} &= \frac{n+1}{\pi} \int_0^{2\pi} \int_0^1 f(\rho, \theta) V_{nm}^*(\rho, \theta) \rho d\rho d\theta \\ &= \frac{n+1}{\pi} \int_0^{2\pi} \int_0^1 f(\rho, \theta) R_{nm}(\rho) \exp(-jm\theta) \rho d\rho d\theta. \end{aligned} \quad (7)$$

Therefore, the Zernike moment of the rotated image in the same coordinate is

$$A'_{nm} = \frac{n+1}{\pi} \int_0^{2\pi} \int_0^1 f(\rho, \theta - \alpha) R_{nm}(\rho) \exp(-jm\theta) \rho \, d\rho \, d\theta. \quad (8)$$

By a change of variable $\theta_1 = \theta - \alpha$,

$$\begin{aligned} A'_{nm} &= \frac{n+1}{\pi} \int_0^{2\pi} \int_0^1 f(\rho, \theta_1) R_{nm}(\rho) \exp(-jm(\theta_1 + \alpha)) \rho \, d\rho \, d\theta_1 \\ &= \left[\frac{n+1}{\pi} \int_0^{2\pi} \int_0^1 f(\rho, \theta_1) R_{nm}(\rho) \exp(-jm\theta_1) \rho \, d\rho \, d\theta_1 \right] \exp(-jm\alpha) \\ &= A_{nm} \exp(-jm\alpha). \end{aligned} \quad (9)$$

Equation (9) shows that each Zernike moment acquires a phase shift on rotation. Thus $|A_{nm}|$, the magnitude of the Zernike moment, can be used as a rotation invariant feature of the image. Therefore we calculate the magnitude of the Zernike moments to uniquely describe each block regardless of the rotation.

3 Copy-rotate-move (CRM) Forgery Detection

In order to detect CRM forgery, it is reminded that the proposed scheme should satisfy the property of Eq. (6) from the algebraic point of view. Moreover, it should be insensitive to additive noise or blurring since a forger might slightly manipulate the tampered region to conceal clues of forgery. In this perspective, we adopt Zernike moments which have desirable properties such as rotation invariance, robustness to noise, and multi-level representation [14].

We first divide the suspicious image f of $M \times N$ into overlapped sub-blocks of $L \times L$ to calculate Zernike moments. Each block is denoted as B_{ij} , where i and j indicates the starting point of the block's row and column, respectively.

$$\begin{aligned} B_{ij}(x, y) &= f(x + i, y + j), \\ \text{where } x, y &\in \{0, \dots, L - 1\}, \quad i \in \{0, \dots, M - L\}, \text{ and } j \in \{0, \dots, N - L\} \end{aligned} \quad (10)$$

Hence, we are able to obtain N_{blocks} of overlapped sub-blocks from the suspicious image.

$$N_{blocks} = (M - L + 1) \times (N - L + 1) \quad (11)$$

We assume that the pre-defined size of block is smaller than the tampered region. After that, the Zernike moments of particular degree n are calculated from each block and vectorized by *getZernikeMoments* function as follows:

$$\mathbf{V}_{ij} = \text{getZernikeMoments}(B_{ij}, n), \quad (12)$$

where **function** $\mathbf{V} = \text{getZernikeMoments}(\text{Block}, nMax)$

```

1: Vector  $\mathbf{V}$ 
2: for  $n = 0$  to  $nMax$  do
3:   for  $m = 0$  to  $n$  do
4:     if  $(n - m) \% 2 = 0$  then
5:        $\mathbf{V}.\text{pushBack}(\frac{n+1}{\pi} \sum \sum (\text{Block} \times V_{nm}^*))$ 
6:     end if
7:   end for
8: end for
9: return  $\mathbf{V}$ 

```

By analyzing *getZernikeMoments* **function** of given order $nMax$, the entire number of moment is

$$N_{moments} = \sum_{i=0}^{nMax} \left(\left\lfloor \frac{i}{2} \right\rfloor + 1 \right). \quad (13)$$

After that, we can construct \mathbf{Z} , a set of vectorized moments \mathbf{V}_{ij} .

$$\mathbf{Z} = \begin{bmatrix} \mathbf{V}_{00} \\ \dots \\ \mathbf{V}_{(M-L)(N-L)} \end{bmatrix} \quad (14)$$

The set \mathbf{Z} is then lexicographically sorted since each element of \mathbf{Z} is a vector. The sorted set is denoted as $\hat{\mathbf{Z}}$. From the set $\hat{\mathbf{Z}}$, the Euclidean distance between two adjacent pairs of $\hat{\mathbf{Z}}$ is calculated. If the distance is smaller than the pre-defined threshold D_1 , we consider the inquired blocks as a pair of candidates for the forgery.

$$\begin{aligned} \hat{\mathbf{Z}}_p &= (\hat{z}_1^p, \hat{z}_2^p, \dots, \hat{z}_{N_{moments}-1}^p, \hat{z}_{N_{moments}}^p), \\ \hat{\mathbf{Z}}_{p+1} &= (\hat{z}_1^{p+1}, \hat{z}_2^{p+1}, \dots, \hat{z}_{N_{moments}-1}^{p+1}, \hat{z}_{N_{moments}}^{p+1}), \end{aligned} \quad (15)$$

$$\sqrt{\sum_{q=1}^{N_{moments}} (z_q^p - z_q^{p+1})^2} < D_1$$

Due to the fact that the neighboring blocks might result in relatively similar Zernike moments, we calculate the distance between the actual blocks of the image as follows:

$$\sqrt{(i-k)^2 + (j-l)^2} > D_2, \quad (16)$$

where $\hat{\mathbf{Z}}_p = \mathbf{V}_{ij}$ and $\hat{\mathbf{Z}}_{p+1} = \mathbf{V}_{kl}$

We determine whether the investigated blocks are duplicated or not according to the Eq. (15) and Eq. (16).

3.1 Complexity Analysis

This section analyzes time complexity of the proposed method. We first calculate $N_{moments}$ of Zernike polynomials from Eq. (2). It roughly takes

$$O(N_{moments}).$$

After that, we should compute Zernike moments from each overlapped block using the polynomials. Since a moment is calculated by the pointwise multiplication of the polynomial and the overlapped block, we need $O(L^2)$ time to attain the moment value. Therefore, we entirely need about

$$O(N_{blocks} \times N_{moments} \times L^2)$$

time to quantify all the moments. The following component to consider is time complexity of the lexicographical sorting of N_{blocks} data with the length of $N_{moments}$. It approximately takes

$$O(N_{moments} \times N_{blocks} \times \log N_{blocks}).$$

Since L is relatively small, $O(N_{blocks} \times N_{moments} \times L^2)$ takes similar time to $O(N_{moments} \times N_{blocks} \times \log N_{blocks})$. To sum up, total time complexity is around

$$O(N_{moments}) + O(N_{blocks} \times N_{moments} \times L^2) + O(N_{moments} \times N_{blocks} \times \log N_{blocks}).$$

In the actual experiment with the machine of 2.4 GHz quadcore processor, 4 GB RAM, coded by C++, and the condition of Sec. 4, it takes about 50 seconds to process one image.

4 Experimental Results

4.1 Measuring the Forgery

For a detection of copy-rotate-move or copy-move forgery, we need appropriate measures to evaluate the performance of the method. In this paper, we adopt *Precision*, *Recall*, and F_1 – *measure* which are often-used measures in the field of information retrieval [17].

Precision and *Recall*, corresponding to exactness and completeness of the method, respectively, are defined as

$$Precision = \frac{True\ Positive}{True\ Positive + False\ Positive} \quad (17)$$

$$Recall = \frac{True\ Positive}{True\ Positive + False\ Negative} \quad (18)$$

From Equations (17) and (18), we see that high *Precision* values indicate low a *FalsePositive* rate, whereas high *Recall* values correspond to a low *FalseNegative* rate. More specifically, the *Precision* denotes the ratio of *True*



Fig. 3. Examples of CRM forgery and its detection result: (a) the forged image by CRM forgery of 10° , (b) *forged region*, (c) *detected region*, and (d) (*forged region* \cap *detected region*)

Positive components to elements categorized into the positive class after investigating. In summary, the *Precision* is a measure for the probability that a detected region is correct. In our perspective, the *Precision* in percentage terms is represented as below.

$$Precision = \frac{(Forged\ Region \cap Detected\ Region)}{Detected\ Region} \times 100 [\%] \quad (19)$$

On the other hand, the *Recall* is the ratio of *True Positive* components to elements inherently ranked as the positive class. It means that the *Recall* is a measure for the probability that a correct region is detected. In this context, the *Recall* in percentage terms is

$$Recall = \frac{(Forged\ Region \cap Detected\ Region)}{Forged\ Region} \times 100 [\%] \quad (20)$$

However, there is a trade-off between *Precision* and *Recall*. Greater *Precision* might decrease *Recall* and *vice versa*. To consider both *Precision* and *Recall* together, we compute the F_1 - *measure*, the harmonic-mean of *Precision*(P) and *Recall*(R).

$$F_1 - measure = \frac{2}{\frac{1}{P} + \frac{1}{R}} = \frac{2PR}{P + R} \quad (21)$$

Figure 3 shows examples of CRM forgery and its detection result. We can calculate *Precision*, *Recall*, and F_1 - *measure* from the forged and detected region.

4.2 Experimental Setup

We conducted our experiments with 12 images comming from a personal collection and [3, 6]. Using these images, copy-move forgery with various manipulations such as rotation, JPEG compression, AWGN, blurring and combined attacks was performed. Figure 4 shows the images used in the experiments. We carried out the proposed method for every test image and consequently *Precision*, *Recall*, and F_1 - *measure* were evaluated.

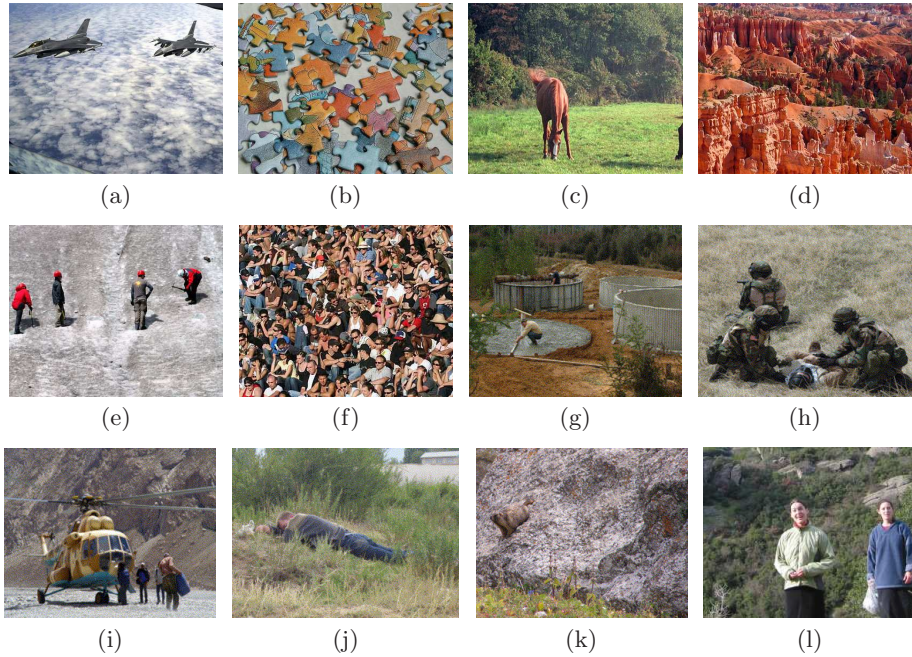


Fig. 4. Images used in the experiments

Since the targets to be investigated are normally color images, there exist two options for operating the method: 1) calculate Zernike moments from each color channel and subsequently concatenate the moment values, 2) simply convert the RGB image into a gray image. Since each individual color channel undergoes the same copy-move forgery, we choose the latter method.

In addition, the parameters in Eq. (11), D_1 , and D_2 are selected for the experiments. As mentioned in Eq. (11), the number of blocks in a suspicious image is $N_{blocks} = (M - L + 1) \times (N - L + 1)$. Since L is relatively smaller than M or N , the complexity of the method is dominated by the image size. We define L , M , and N as 24, 400, and 320, respectively. Therefore, total number of blocks to be dealt with is $(400 - 24 + 1) \times (320 - 24 + 1) = 111969$. Each block is represented by the Zernike moments of 5 indicating $N_{moments} = 12$ by Eq. (13). Finally, we need to define decision threshold D_1 and D_2 , which represent the similarity between two blocks and the distance of them, respectively. D_1 for the order of 5 is determined as 300 by experiments. Since the adjacent blocks might have similar moment values, the distance threshold D_2 is defined as 50.

Under these conditions, the following sub-sections analyze the performance of the proposed scheme in three perspectives. First of all, we take account of CRM forgery. After that, we present the robustness against intended distortions such as JPEG compression, AWGN, and blurring. Finally, combined attacks are considered.

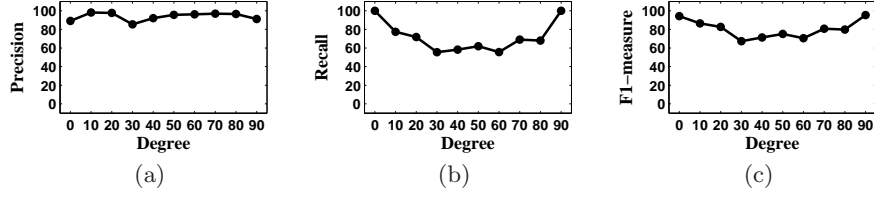


Fig. 5. CRM forgery detection results for Fig. 4(a) : (a) *Precision*, (b) *Recall*, and (c) F_1 - *measure*

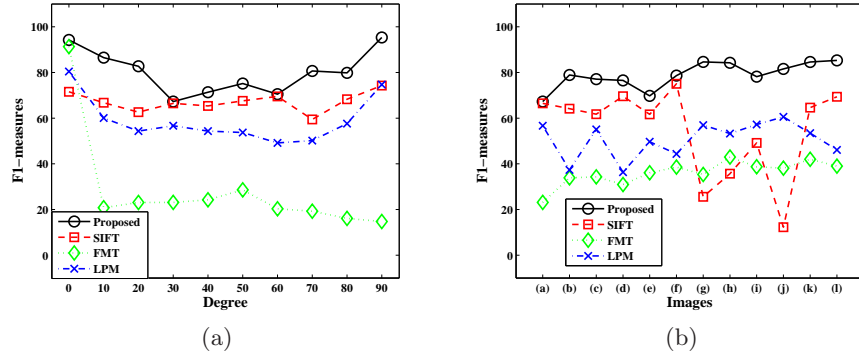


Fig. 6. Detection results for CRM forgery among proposed, SIFT, FMT, and LPM detector: (a) F_1 - *measure* of various degrees for Fig. 4(a), (b) F_1 - *measure* for 12 images undergoing CRM of 30°

4.3 Test for CRM Forgery

In this experiment, we conducted CRM with rotations in the range of 0° to 90° , applied in steps of 10° . Figure 5 depicts *Precision*, *Recall*, and F_1 - *measure* of various degrees for Fig. 4(a). Even though the proposed scheme is theoretically invariant against rotation, the actual results have lower performance than expected as shown in Fig. 5. There might be two reasons for the degradation. At first, Zernike moments calculated on the discrete domain have inherent quantization error since the moments are originally defined on the continuous domain. Secondly, the interpolation caused by the rotation step can also increase the error rate. In this experiment, we used cubic kernel for the interpolation. Nevertheless, the experiments confirm that the precision is relatively high, which means most part of detected region is correct. Table 1 shows experimental results for 12 images undergoing CRM of 30° . All duplications were performed with the region which size is 100×70 and the translation of (100, 50). The average rate of *Precision*, *Recall*, and F_1 - *measure* were 83.59%, 76.63%, and 78.89%, respectively.

We also compared our method with several CRM detectors: SIFT [10], FMT [7], and LPM [8]. Except for the SIFT based detector, we lexicographically sorted

the extracted features from overlapping blocks to find adequate pairs of similar blocks. Since the SIFT is a kind of region descriptor, constructed with a set of matched points, it is hard to define where detected area is. Therefore we constructed a maximum polygonal convex inside the detected cluster. Then we calculated $F_1 - measure$ of each detector to measure quantitative performance. Figure 6(a) shows $F_1 - measure$ of various degrees for Fig. 4(a) by 4 detectors. Similarly, Fig. 6(b) represents the experimental results for 12 images undergoing CRM of 30° by the detectors. It is noticeable that the SIFT based method shows low detectability for the image (g) and (j) in Fig. 6(b) since the number of matched points are reduced for the image with less prominent structures. As a consequence, we observe that the proposed detector provides higher $F_1 - measure$ than the others regardless of the amount of rotation or the concrete image. The experimental results suggest that the proposed method is indeed capable of detecting CRM forgeries.

4.4 Test for Intended Distortions

Through this section, we present the detectability of copy-move forgery against intended distortions such as JPEG compression, AWGN, and blurring. We added Gaussian noise to the copied region or performed blurring before pasting into another part of the image. In case of JPEG compression, we compressed the whole image and not only the copied part. Figure 7 shows detection results of forgeries under several circumstances. We regularly changed the strength of each attack and analyzed the result.

By concentrating on the graphs for *Recall* in Fig. 7, we notice that the *Recall* values decrease considerably as a function of image quality. From these results, we conclude that severe attacks cause low detectability. Therefore we restrict our analysis in the following to attacks where the PSNR of the distorted region is above 30 dB. For example, we concentrate on noisy images with a variance of the Gaussian noise less than or equal to 0.003, since a distortion with $N(0, 0.003)$ amounts to about 31 dB. Similarly, the blurring with the radius larger than 2 or the quality factor for JPEG compression smaller than 60% is not considered in this test. Table 2 shows experimental results with intended distortions for 12

Table 1. Detection rates for CRM of 30° for 12 images

Image	Measures (%)			Image	Measures (%)		
	P	R	F_1		P	R	F_1
(a)	85.41	55.50	67.28	(g)	83.76	85.49	84.62
(b)	92.76	68.67	78.91	(h)	86.60	82.01	84.24
(c)	66.78	91.10	77.06	(i)	73.43	83.54	78.16
(d)	97.84	62.87	76.55	(j)	79.31	83.97	81.57
(e)	67.96	71.66	69.76	(k)	83.57	85.68	84.51
(f)	98.80	65.33	74.71	(l)	86.88	83.76	85.29
Average					83.59	76.63	78.89

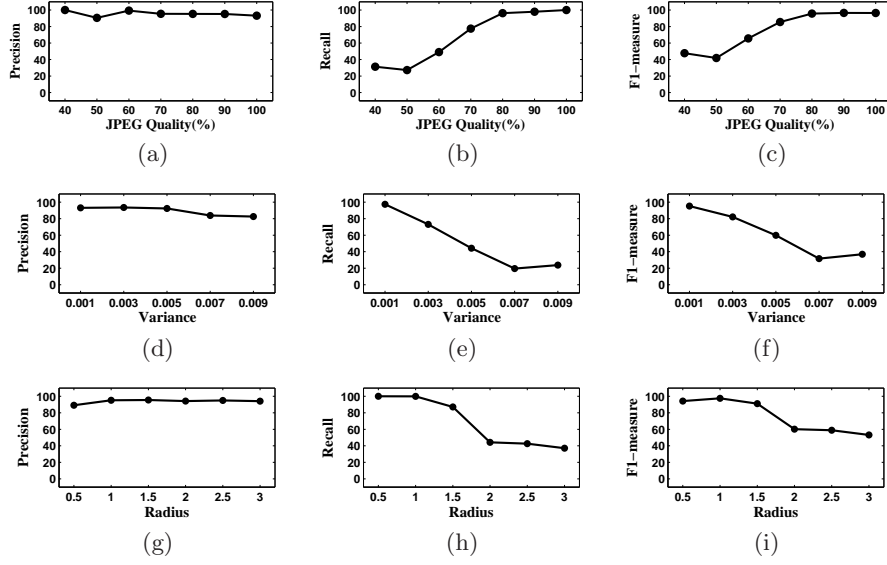


Fig. 7. Detection rates for intended distortions: (a)~(c): detection rate against JPEG quality factor, (d)~(f): detection rate against AWGN with different variances, and (g)~(i): detection rate against blurring with different radius

images. The average rate of $F_1 - measure$ for each case was 81.20%, 72.50%, and 93.67%, respectively. The experiments demonstrate that the proposed method is reasonably robust against intended distortions.

4.5 Test for Combined Manipulation

Finally, we present the robustness of proposed CRM detection scheme against combined manipulation. There might be two scenarios of CRM when a forger tampers an image. The forger would spread additional noise to eliminate the

Table 2. Detection rates for intended distortions for 12 images

Image	$F_1 - Measures(\%)$			Image	$F_1 - Measures(\%)$		
	JPEG (QF=70%)	AWGN (var=0.003)	Blurring (radius=1)		JPEG (QF=70%)	AWGN (var=0.003)	Blurring (radius=1)
(a)	85.50	71.46	97.47	(g)	74.34	60.06	92.01
(b)	88.74	82.07	94.83	(h)	72.55	60.59	89.85
(c)	82.82	69.05	96.19	(i)	72.75	75.55	94.67
(d)	78.58	70.75	92.50	(j)	68.14	61.16	92.89
(e)	91.05	55.50	95.70	(k)	85.53	88.95	94.45
(f)	88.38	93.95	85.62	(l)	86.06	80.94	97.85
Average					81.20	72.50	93.67



Fig. 8. Two scenarios of combined manipulation: (a) CRM of 10° , AWGN with $var = 0.003$, and JPEG re-compression (QF=80%), (b) CRM of 10° , blurring with $radius = 1$, and JPEG re-compression (QF=80%)

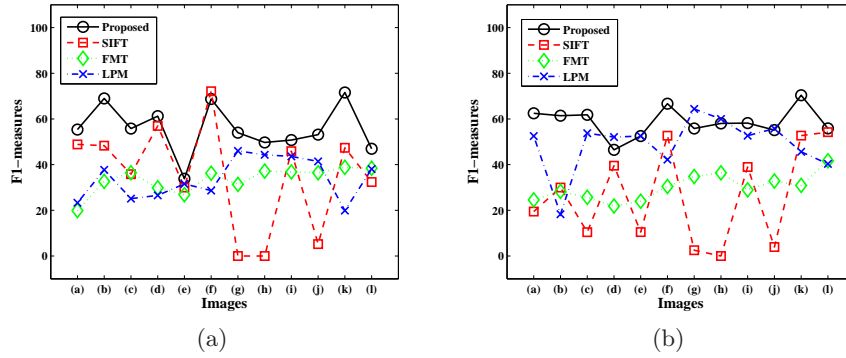


Fig. 9. Detectability for combined attacks among proposed, SIFT, FMT, and LPM detector: (a) F_1 - measure for 12 images undergoing the scenario of Fig. 8(a), (b) F_1 - measure for 12 images undergoing the scenario of Fig. 8(b)

clues for manipulation after CRM. And then he or she will recompress the forged image. Similarly, the falsifier would blur the altered region instead of adding noise in the second scenario. Figure 8 depicts the detailed scenarios. Furthermore, Figure 9 represents detectability of various detectors of the scenario. We observe that the detectability of the SIFT based method in Fig. 9 has become worse compared with Fig. 6(b). This is so because the number of matched points by the SIFT method is reduced as we manipulate the image. On the other hand, the results confirm the reliability of the proposed scheme even after combined manipulation. Through the experiments, it proves that the proposed detector performs better than others as well.

5 Conclusion

With the rapid progress of image processing technology, an appropriate forensic application has become more important. In this paper, we proposed copy-rotate-move (CRM) detection scheme for a suspicious image. To extract feature vectors of a given block, we calculated the magnitude of Zernike moments. The vectors were then sorted in lexicographical order. We investigated the similarity of adjacent vectors after that. Finally, the suspected regions were measured by *Precision*, *Recall*, and F_1 - *measure*. Experimental results supported that the proposed method was appropriate to identify and localize the CRM region even though the region had been manipulated intentionally. However, in spite of an algebraic invariant of rotation, detection errors occurred due to the quantization and interpolation error. Though we concerned several attacks, our method is still weak against scaling or the other tempering based on Affine transform. Thus, we need to improve the proposed method so that it is robust against those of attacks. Additionally, there exist many efficient data structures to represent nearest neighbors. Therefore, our future work concentrates on establishing an appropriate data structure as well.

Acknowledgments. We are grateful to Matthias Kirchner for many helpful advices and suggestions. This work was partially supported by Defense Acquisition Program Administration and Agency for Defense Development under the contract. (UD060048AD)

References

1. Nizza, M., Lyons, P.J.: In an iranian image, a missile too many. In: The Lede, The New York Times News Blog (2008) <http://thelede.blogs.nytimes.com/2008/07/10/in-an-iranian-image-a-missile-too-many/>.
2. Fridrich, J., Soukal, D., Lukáš, J.: Detection of copy-move forgery in digital images. In: Proc. of Digital Forensic Research Workshop. (2003)
3. Popescu, A.C., Farid, H.: Exposing digital forgeries by detecting duplicated image regions. In: Technical Report, TR2004-515, Dartmouth College, Computer Science (2004)
4. Li, G., Wu, Q., Tu, D., Sun, S.: A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. In: Proc. of ICME. (2007)
5. Luo, W., Huang, J., Qiu, G.: Robust detection of region-duplication forgery in digital image. In: Proc. of ICPR. (2006)
6. Mahdian, B., Saic, S.: Detection of copy-move forgery using a method based on blur moment invariants. *Forensic Science International* **171** (2007) 180–189
7. Bayram, S., Sencar, H.T., Memon, N.: An efficient and robust method for detecting copy-move forgery. In: Proc. of ICASSP. (2009)
8. Bravo-Solorio, S., nandi, A.K.: Passive method for detecting duplicated regions affected by reflection, rotation and scaling. In: EUSIPCO. (2009)
9. Huang, H., Guo, W., Zhang, Y.: Detection of copy-move forgery in digital images using SIFT algorithm. In: Proc. of PACIA. (2008)

10. Amerini, I., Ballan, L., Caldelli, R., Bimbo, A.D., Serra, G.: Geometric tampering estimation by means of a SIFT-based forensic analysis. In: Proc. of ICASSP. (2010)
11. Pan, X., Lyu, S.: Detecting image region duplication using SIFT features. In: Proc. of ICASSP. (2010)
12. Hu, M.K.: Visual pattern recognition by moment invariants. *IEEE Trans. Information Theory* **8** (1962) 179–187
13. Kim, H.S., Lee, H.K.: Invariant image watermark using Zernike moments. *IEEE Trans. Circuits and Systems for Video Technology* **13**(8) (2003) 766–775
14. Teh, C.H., Chin, R.T.: On image analysis by the methods of moments. *IEEE Trans. Pattern Analysis and Machine Intelligence* **10**(4) (1988) 496–513
15. Khotanzad, A., Hong, Y.H.: Invariant image recognition by Zernike moments. *IEEE Trans. Pattern Analysis and Machine Intelligence* **12**(5) (1990) 489–497
16. Zernike, F.: Beugungstheorie des schneidenverfahrens und seiner verbesserten form, der phasenkontrastmethode. *Physica* **1** (1934) 689–704
17. Manning, C.D., Raghavan, P., Schütze, H.: *An Introduction to Information Retrieval*. Cambridge University Press (2009)