Robust Copy-move Forgery Detection through Invariant Moment Features

Chien-Chang Chen and *Han Wang*

Department of Computer Science and Information Engineering
Tamkang University
No.151, Yingzhuan Rd., Tamsui Dist., New Taipei City 25137, Taiwan (R.O.C.)
e-mail: ccchen34@mail.tku.edu.tw

ABSTRACT

The proposed scheme uses the invariant features extracted from each block to detect the copy-move forgery regions in a digital image. In the proposed scheme, an image is first divided into overlapping blocks. Then, seven invariant moments of the maximum circle area in each block are calculated as moment features. Mean and variance of these seven moment features, as second feature set, are acquired for block comparison to reduce computation time. Thus, the proposed scheme outperforms previous schemes. The copy-move forgery regions can be found by matching the detected blocks with relative distance calculation. Experimental results show that the adopted moment features are efficient for detecting rotational or flipped duplicated regions.

KEYWORDS

forgery duplication; invariant moment; mean; variance; clustering

1 Introduction

With the rapid growth of image editing software, the digital image has become easier than ever to modify or synthesize. The purpose of digital image forensics is to verify the trustworthiness of a digital image, and it has become an important and exciting field for recent research. Schemes for digital image forensics can be categorized into active and passive approaches [1, 5]. One of the most important active approaches is digital watermarking [3], which embeds watermark information into the host image and malicious tampering of the image can be detected through analyzing the extracted watermarks. The integrity and authenticity of digital images can be therefore acquired. Although the image watermarking technique efficiently detects malicious tampering, one drawback of image watermarking strategies is that the watermark information should be embedded into the host image in advance. To overcome this problem, passive approaches like copy-move forgery detection that do not need any prior processing are extensively studied in recent researches.

Over the past few years, many copy-move forgery detection schemes have been presented through the following features, namely, DCT-based [2, 6], texture and intensity-based [4], dyadic wavelet transform [10], and Zernike moments [11].

Although the previous approaches can detect copy-move forgery regions, performance drawbacks exhibited in these works are worth improving. Fridrich's approach [6] requires $(MN)^2$ comparisons to compare the image with every cyclic-shifted version of itself by exhausting the search, where image size is M×N. Lynch et al. [9] proposed the EB to detect copy-move forgery regions. Lin et al. [8] further improved the detection performance from one cluster's EB algorithm to the intersection of two clusters' ECEB algorithm. Although the ECEB algorithm is much more efficient than an exhaustive search, the pixel-based comparison lacks robust detection on rotational or flipped copy-move regions.

In this paper, we propose a copy-move forgery detection scheme that is based on invariant moments for detecting rotational or flipped regions. The proposed scheme first acquired overlapped blocks from the image. Seven invariant moments, calculated from each block, are the first block feature set. Moreover, the second block feature set constructed from the mean and variance of these seven invariant moments is calculated to improve performance of the proposed scheme. At last, the refinement process combines the matched blocks and eliminates false detection. We have carried out experiments over copy-move tampering, and the results show that our approach outperforms the previous methods EB [9] and ECEB [8] on computation time, and can effectively localize rotationally duplicated regions.

The paper is organized as follows. Section II gives a brief review of related works, including invariant moment, the expanding block (EB) algorithm [9] and the enhanced cluster expanding block (ECEB) algorithm [8]. Section III presents details of the proposed algorithm, including algorithm description and theoretical comparisons with EB and ECEB algorithms. Section IV presents the experimental results. Section V follows with concluding remarks.

2 Review of Invariant Moment features

This section introduces the definition of invariant moment features [7]. Assume that pixels of a $M \times N$ image are denoted by $f(x,y)$ with $1 \le x \le M$ and $1 \le y \le N$, and the image moment m_{pq} of order $(p+q)$ in the digital image $f(x,y)$ are calculated using Eq. (1),

$$m_{pq} = \sum_{x=1}^{M} \sum_{y=1}^{N} x^p y^q f(x,y) \qquad (1)$$

The components of the centroid are calculated using Eq. (2),

$$\bar{x} = \frac{m_{10}}{m_{00}}, \ \bar{y} = \frac{m_{01}}{m_{00}}, \qquad (2)$$

The moment equation is then defined by Eq. (3),

$$\mu_{pq} = \sum_{x=1}^{M} \sum_{y=1}^{N} (x-\bar{x})^p (y-\bar{y})^q f(x,y) \qquad (3)$$

The equations for acquiring the central moments are listed in Eq. (4). Eq. (5) shows the calculation of the central moments from Eqs. (3) and (4),

$$\eta_{pq} = \frac{\mu_{pq}}{\mu_{00}^{\left(1+\frac{p+q}{2}\right)}} \tag{4}$$

$$\eta_{pq} = \frac{\sum_{x=0}^{M}\sum_{y=0}^{N}(x-\bar{x})^p (y-\bar{y})^q f(x,y)}{\left[\sum_{x=0}^{M}\sum_{y=0}^{N} f(x,y)\right]^{\left(1+\frac{p+q}{2}\right)}} \tag{5}$$

In 1962, Hu [7] defined the invariant moments of orders up to 3, and these seven moments are listed in Eq. (6),

$$\begin{aligned}
\phi_1 &= \eta_{20} + \eta_{02} \\
\phi_2 &= (\eta_{20} - \eta_{02})^2 + 4\eta_{11}^2 \\
\phi_3 &= (\eta_{30} - 3\eta_{12})^2 + (3\eta_{21} - \eta_{03})^2 \\
\phi_4 &= (\eta_{30} + \eta_{12})^2 + (\eta_{21} + \eta_{03})^2 \\
\phi_5 &= (\eta_{30} - 3\eta_{12})(\eta_{30} + \eta_{12})\left[(\eta_{30} + \eta_{12})^2 - 3(\eta_{21} + \eta_{03})^2\right] \\
&\quad + (3\eta_{21} - \eta_{03})(\eta_{21} + \eta_{03})\left[3(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2\right] \\
\phi_6 &= (\eta_{20} - \eta_{02})\left[(\eta_{30} + \eta_{12})^2 - (\eta_{21} - \eta_{03})^2\right] + 4\eta_{11}(\eta_{30} + \eta_{12})(\eta_{21} + \eta_{03}) \\
\phi_7 &= (3\eta_{21} - \eta_{30})(\eta_{30} + \eta_{12})\left[(\eta_{30} + \eta_{12})^2 - 3(\eta_{21} + \eta_{03})^2\right] \\
&\quad + (\eta_{03} - 3\eta_{12})(\eta_{21} + \eta_{03})\left[3(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2\right]
\end{aligned} \tag{6}$$

Seven invariant moments $\phi_1 \sim \phi_7$ are efficient for acquiring the properties of image shifting, rotation and mirroring. The proposed scheme adopts the seven invariant moments as the first block feature set.

3 Algorithm of the proposed scheme

The proposed scheme compares image blocks through invariant moments of the largest inner circle within each block. Moreover, the intersection strategy in ECEB is also adopted to improve the performance of the proposed scheme. The test image is first partitioned to overlap blocks with size $k \times k$. In each block, seven invariant moments are calculated as the first block feature set. The second feature set is calculated from mean and variance of the seven invariant moments acquired from the first block feature set. Blocks are first compared by the second feature set and then by the first feature set to improve performance. The algorithm of the proposed scheme is introduced as follows:

1. Partition the $M \times N$ test image into overlapped blocks with size $k \times k$ to acquire $(M-k+1) \times (N-k+1)$ blocks.
2. Apply Eq. (6) to each block to acquire the seven invariant moments of the largest inner circle in a block.
3. Normalize each invariant moment.
4. Calculate mean and variance of the seven invariant moments in each block, and then store mean and variance to vectors M and V, respectively.
5. Sort M and V independently.
6. For a block b_e, assume that the set M_e includes some blocks in sorted M of indexes within the range of the pre-defined d to b_e. The set V_e is similarly defined in V and d.

6.1 If a block b_o belongs to $M_e \cap V_e$, which is the second feature set, use Eq. (7) to calculate Euclidean distance *mdis* between moments of blocks b_e and b_o,

$$mdis = \sqrt{\sum_{i=0}^{6} (b_e(i) - b_o(i))^2} \tag{7}$$

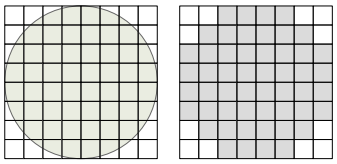
where $b_e(i)$ and $b_o(i)$ with $0 \le i \le 6$ denote the seven invariant moments acquired from blocks b_e and b_o, respectively.

6.2 If *mdis* is smaller than a pre-defined Euclidean threshold *ETHD*, then blocks b_e and b_o are denoted as a pair of matched blocks.

7. The copy-move forgery regions are detected by the following two steps.

7.1 The matched blocks of the same index distance, where the matched number is larger than a pre-defined occurrence threshold *OTHD*, denotes identical copy-move detected regions.

7.2 The matched blocks of relative index distance, where two pair of blocks have the same index distance and the number of these match pairs is larger than a pre-defined parameter *T_d*, denote rotational copy-move detected regions.



(a) (b)

Fig. 1. Definition of (a) the ideal largest inner circle within an 8×8 block and (b) the digitized largest inner circle within an 8×8 block.

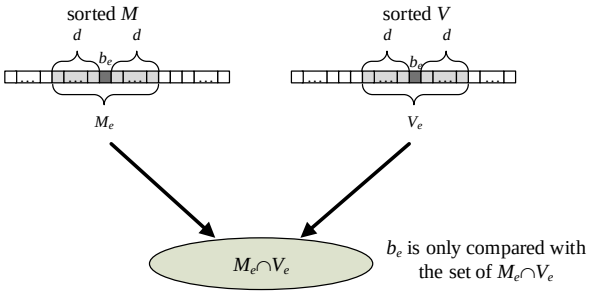


Fig. 2. Comparison set defined in the intersection of M_e and V_e.

The proposed algorithm calculates seven invariant moments of the largest inner circle within the block. Fig. 1 shows the definition of the largest inner circle within an 8×8 block. Fig. 1(b) shows that only grey pixels are applied to the invariant moment calculation. The usage of the largest inner circle exhibits the property of rotational or flipped copy-move regions detection.

The intersection of the mean and variance vectors in the comparison step is depicted in Fig. 2 and defined in Step 6. Fig. 2 shows that seven moments in one block are only compared to b_e, such that b_e denotes one block's seven moments in the intersection of two sets M_e and V_e. The computation time is greatly reduced when the intersection probability is small.

Moreover, many parameters should be determined in the proposed scheme. In Step 6, the pre-defined *d* value determines the range of blocks that a block b_e will be compared to. A large *d* value increases the number of blocks that should be compared but with a higher possibility to detect copy-move regions. However, a large *d* value also increases the computation time. On the contrary, a small *d* value leads to limited computation time, but some copy-move regions may not be detected. Therefore, the selection of the *d* value is a trade-off between the computation time and detection accuracy.

In Step 6.2, the threshold *ETHD* determines the robustness of the proposed scheme. When the test image suffers from a smooth attack, like a Gaussian low-pass filter, a large *ETHD* assignment robustly detects pairs of similar blocks. However, more detection errors may also be included. Therefore, the parameter *ETHD* is a trade-off between robustness and exactness. The occurrence threshold *OTHD* in Step 7.1 is adopted to filter out those regions with small numbers of matched blocks. The

ISBN: 978-1-941968-41-3

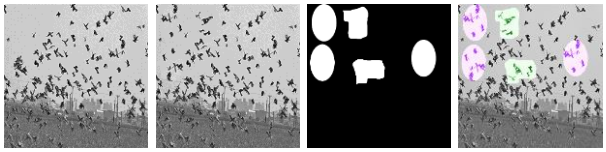
parameter *T_d*, used in Step 7.2, denotes the threshold of relative pairs of blocks to find rotational copy-move regions.

Therefore, five parameters including a block size *k*, a category distance *d*, a threshold *ETHD*, a threshold *OTHD*, and *T_d* determine the accuracy of the proposed scheme.

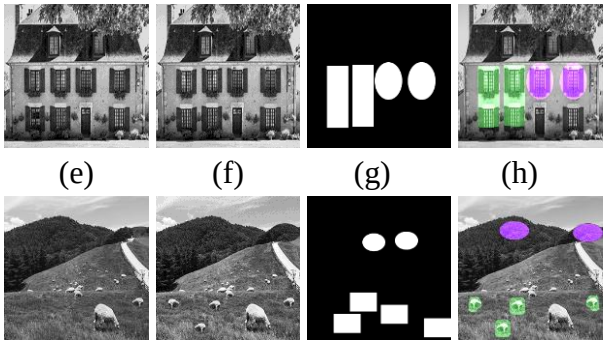
4 Experimental Results

This section demonstrates the experimental results of our proposed scheme. All experiments were performed using MATLAB 2016a on a PC with an Intel i7-6700 CPU and 32GB RAM. Experimental results include detected results after applying some attacks on the copy-move forgery test image and computation times under different parameters assignment. The parameters are assigned to be $d = 200$, $ETHD = 10^{-8}$, $T\_d = 0$, $OTHD = 20$, and $k = 16$.

Fig. 3 shows applying no attacks on three test images. Figs. 3(a)(e)(i) show three 256×256 original images Birds, House, and Sheep, and Figs. 3(b)(f)(j) show three copy-move forgery images, respectively. The copy-move regions are shown in Figs. 3(c)(g)(k). Figs. 3(d)(h)(l) show three copy-move results detected by the proposed scheme, where the green or purple areas represent the detected copy-move forgery regions.



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



(e) (f) (g) (h)

(i) (j) (k) (l)

Fig. 3. Examples of three test images, (a)(e)(i), of three test images: Birds, House, Sheep; (b)(f)(j) three copy-move forgery images; (c)(g)(k) ideal copy-move regions; and (d)(h)(l) three copy-move results detected by the proposed scheme.

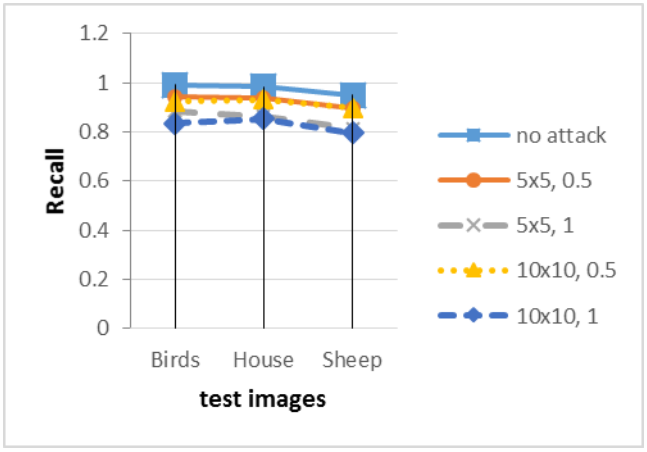
Two measurements, Precision (*P*) and Recall (*R*), are calculated to demonstrate the detected rate on copy-move forgery regions. Assuming that we use the following definitions of *D* being the set of pixels in detected regions, *B* being the set of pixels in original copy-move regions, *M* being the set of pixels in copy-move forgery modified regions and |A| being the pixel number of a given set A. *P* is the probability that a detected forgery is truly a forgery and *P* is denoted by $\frac{|M \cap D| + |B \cap D|}{|D|}$. *R* shows the probability that a forged image is detected and *R* is denoted by $\frac{|M \cap D| + |B \cap D|}{|M| + |B|}$.

Fig. 4 depicts the detected results of applying a Gaussian low-pass filter to the three copy-move forgery images. Fig. 4(a) shows that the three test images acquire an almost perfect Precision measurement. Fig. 4(b) depicts the Recall measurements of these three test images

ISBN: 978-1-941968-41-3

applying the same Gaussian low-pass attacks. The test image House exhibits the best Recall measurements among these three test images. Moreover, Fig. 4(b) also shows that the Gaussian attacks with large σ assignments (σ=1) acquire worse recall measurements than other σ assignments (σ=0.5).

(a)



(b)

Fig. 4. (a) Precision and (b) Recall measurements of the three forgery images under different Gaussian attacks.

Fig. 5 compares the Precision and Recall measurements of House image under Gaussian attacks between the proposed scheme and the EB scheme [9]. Since the left pair of vertical regions are flipped, it is hard to detect this pair of vertical regions in the EB scheme, and the Precision or Recall measurements of the EB are around 0.4. Fig. 5 only depicts experimental results of EB because both EB and ECEB have the same experimental results.

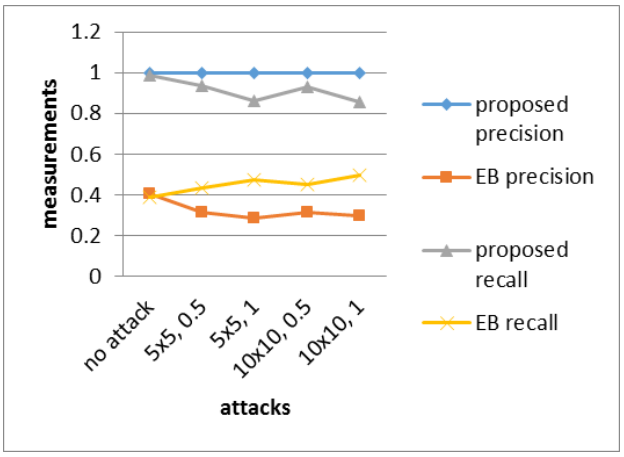


Fig. 5. Measurement comparison on the House image between the proposed scheme and EB [9] under Gaussian attacks.

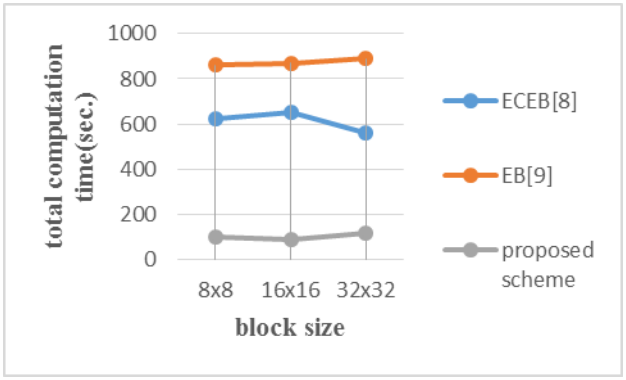


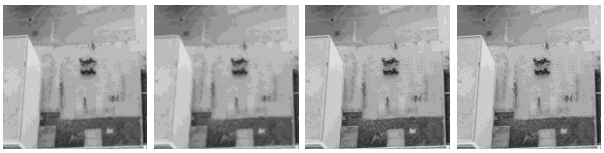
Fig. 6. Total computation time compared between the proposed ECEB [8] and the conventional EB [9] under different *ETHD* thresholds.

Fig. 6 compares the computation time between the proposed scheme and two previous works [8, 9]. The proposed scheme, using seven

invariant moment features, and the second group exhibit the best computation time among these works.

(a) Forgery (b) BC1 (c) BC2 (d) BC3

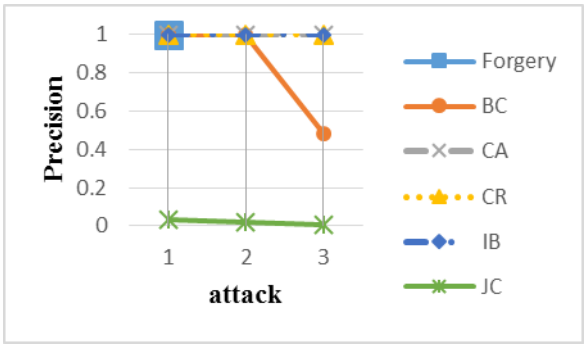
(e) CA1 (f) CA2 (g) CA3 (h) IB1



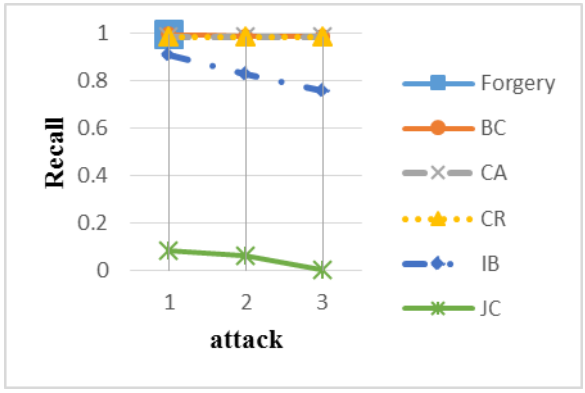
(i) IB2 (j) IB3 (k) CR1 (l) CR2

(m) CR3 (n) JC1 (o) JC2 (p) JC3

Fig. 7. Test images in CoMoFoD copy-move database [12], (a) forgery image, (b)-(d) brightness attacks, (e)-(g) darkness attacks, (h)-(j) blur attacks, (k)-(m) color reduction attacks, and (n)-(p) jpeg compression attacks.



(a)



(b)

Fig. 8. Precision and Recall measurements of Fig. 7.

Fig. 7 shows a set of test images in the CoMoFoD copy-move database [12]. Fig. 7 shows many different attacks applying to the copy-move forgery images. The Precision and Recall measurements of the test images are depicted in Fig. 8. Fig. 8 shows that the proposed scheme detects the brightness, darkness and color reduction in the attacked forgery images well. However, the detected results on blur attacks are not so ideal because the blur attacks modify the copy-move forgery regions quite a lot, especially in the boundary regions. Moreover, the jpeg compression attacks are very difficult to detect because the jpeg compression attacks break the similarity between each pair of copy-move regions. Moreover, the jpeg compression attacked forgery images also have poorly detected results.

5 Conclusions

This proposed scheme adopts invariant moments to detect copy-move forgery regions.

ISBN: 978-1-941968-41-3 ©2016 SDIWC

The moment features detect regions with rotating or flipping modifications. The usage of intersections under the mean and variance of moment features improves the performance. The performance evaluation and experimental results show that the proposed scheme exhibits low intersection probability that diminishes the computation time the most among all other related works. Use of a more robust strategy to detect the copy-move regions for scaling forgery regions also merits future study.

REFERENCES

[1] O.M. Al-Qershi, and B.E. Khoo, "Passive detection of copy-move forgery in digital images: State-of-the-art," Forensic Science International, vol. 231, pp.284-295, 2013.

[2] Y. Cao, T. Gao, L. Fan, and Q. Yang, "A robust detection algorithm for copy-move forgery in digital image," Forensic Science International, vol. 214, pp.33-43, 2012.

[3] C.C. Chen, Y.H. Tsai, and H.C. Yeh, "Difference-Expansion Based Reversible and Visible Image Watermarking Scheme," Multimedia Tools and Applications, 2016. (accepted)

[4] R. Davarzani, K. Yaghmaie, S. Mozaffari, and M. Tapak, "Copy-move forgery detection using multiresolution local binary patterns," Forensic Science International, vol. 231, pp.61-72, 2013.

[5] H. Farid, "A survey of image forgery detection," IEEE Signal Processing Magazine, vol. 2, pp.16-25, 2009.

[6] J. Fridrich, D. Soukal, and J. Lukás, "Detection of copy move forgery in digital images," in Proc.of Conf. on Digital Forensic Research Workshop, pp.55-61, 2003.

[7] M.K. Hu, "Visual pattern recognition by moment invariants," IRE Transactions on Information Theory, vol. 8, pp. 179-187, 1962.

[8] C.S. Lin, C.C. Chen, and Y.C. Chang, "An efficiency enhanced cluster expanding block algorithm for copy-move forgery detection," IEEE International Conference on Intelligent Networking and Collaborative Systems (INCOS), pp. 228-231, 2015.

[9] G. Lynch, F.Y. Shih, and H.M. Liao, "An efficient expanding block algorithm for image copy-move forgery detection," Information Sciences, vol. 239, pp.253-265, 2013.

[10] G. Muhammad, M. Hussain, and G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform" Digital Investigation, vol. 9, pp.49-57, 2012.

[11] S.J. Ryu, M. Kirchner, M.J. Lee, and H.K. Lee, "Rotation invariant localization of duplicated image regions based on Zernike moments," IEEE Trans. on Information Forensics and Security, vol. 8, pp.1355-1370, 2013.

[12] D. Tralic, I. Zupansis, S. Grgic, and M. Grgic M, "CoMoFoD-New Database for copy-move forgery detection," The 55th Internationsl Symposium on ELMAR, pp. 49-54, 2013.