Multimedia Tools and Applications (2019) 78:18293–18308
https://doi.org/10.1007/s11042-019-7165-8

Rotational copy-move forgery detection using SIFT and region growing strategies

Chien-Chang Chen[1] · Wei-Yu Lu[1] · Chung-Hsuan Chou[1]

Received: 1 April 2018 / Revised: 14 November 2018 / Accepted: 3 January 2019 /
Published online: 23 January 2019

Abstract
The proposed scheme detects the copy–move forgery regions using SIFT, invariant moments calculation, and the region growing strategy. First, the SIFT-based keypoints are acquired as the significant features of an image. Second, pairs of keypoints with closed scales are examined to identify all possible pair blocks of the copy–move regions. Third, the orientations for each pair of matched keypoints are adjusted to have identical orientation. Lastly, the copy–move regions are acquired using the region growing technique, and invariant moment features are applied to each pair of matched blocks. Experimental results show that the proposed scheme efficiently and effectively detects rotational copy-move duplicated regions. Moreover, the proposed computation time is proportional to the number of keypoints and the size of the copy–move forgery regions.

Keywords Forgery duplication · Invariant moment · Keypoints · Region growing

1 Introduction

With the rapid growth of image processing software, digital images have become easier than ever to modify or synthesize. Digital image forensics verifies the trustworthiness of digital images, and this field has become an important and exciting area of recent research. Digital image forensics can be categorized into active and passive approaches [1, 14]. One of the most well-known active approaches is digital image watermarking [11], which embeds watermark information into the host image. The extracted watermarks authenticate the owner of the image. However, one drawback of image watermarking strategies is that the watermark information must be embedded into the host image in advance. To overcome this pre-processing requirement problem, passive approaches like copy–move forgery detection that do not need any pre-processing have been extensively studied in recent researches.

✉ Chien-Chang Chen
ccchen34@mail.tku.edu.tw

[1] Department of Computer Science and Information Engineering, Tamkang University, No.151, Yingzhuan Rd., Tamsui Dist, New Taipei City 25137 Taiwan, Republic of China

Over the past years, many copy–move forgery detection schemes are presented, namely, DCT based [8, 15], Log-polar transform based [7, 13, 21], texture and intensity based [12], invariant key-points based [2], J-Linkage based [3], image moments based [4, 30], wavelet transform based [27, 33], SVD based [34], PCA based [29], SIFT-based [2, 6, 17, 28]. Other methods like multi-scale feature extraction [5], block matching [20], and image segmentation [22] can also detect the copy-move forgery regions. Some comparison works [10, 31] are also discussed about the copy–move forgery detection problems. Furthermore, some studies [18, 19, 23] on video forgery detection are also analyzed.

Among these approaches, the performance drawbacks currently exhibited in these works are worth improving. Fridrich's approach [15] requires $(M \times N)^2$ image comparisons with every cyclic-shifted version of itself using an exhausting search, where the image size is $M \times N$. Lynch et al. [26] proposed the expanding block algorithm (EB) to detect copy–move forgery regions. Chen et al. [9] further improved the detection performance from one cluster's EB algorithm to intersect two clusters' ECEB algorithms. Although the ECEB algorithm is much more efficient than exhaustive search, the pixel-based comparison lacks the ability to detect rotational copy–move regions.

In this paper, we propose a copy–move forgery detection scheme that is based on SIFT, invariant moments, and the region growing technique. The proposed scheme is motivated from first matched points and growing the copy-move region. The reason of using significant matched points with region growing rather than mainly by matched points is for region growing acquiring better detected results. The proposed scheme first acquires SIFT keypoints, including scale, orientation, and position, to represent significant features of an image. Initial blocks, centered by keypoints under closed scales, are compared using Hu's invariant moments [16]. For those matched initial blocks, the next step is to apply the region growing technique on the initial blocks' surrounded blocks through Hu's invariant moments for generating copy–move forgery regions. We have carried out experiments over copy–move tampering, and the results show that our approach outperforms previous EB [26] and ECEB [9] on computation time and detected regions, especially for detecting the rotation degree of duplicated regions.

The paper is organized as follows. Section 2 briefly reviews important related works, including Scale Invariant Feature Transform (SIFT) [25], Hu's invariant moment [16], the expanding block (EB) algorithm [26], and the enhanced cluster expanding block (ECEB) algorithm [9]. Section 3 presents details of the proposed algorithm, including an algorithm description and theoretical comparisons with the EB and ECEB algorithms. Section 4 presents the experimental results. Section 5 follows with concluding remarks.

2 Review of related literatures

This section briefly reviews four related works of this study. Section 2.1 introduces the SIFT process. Section 2.2 introduces the acquisition of Hu's invariant moment features. Section 2.3 reviews the EB algorithm that reduces the computation time needed for the block comparison procedure. Section 2.4 reviews the ECEB algorithm that improves the computation time required in the aforementioned EB algorithm.

2.1 Review of scale invariant feature transform (SIFT) [25]

SIFT detects the scale invariant features from a digital image [25]. The detected features are invariant to image scaling, rotation, and translation. Four important steps of the SIFT are scale-space extrema detection, keypoint localization, orientation assignment, and keypoint descriptor. Through these four major steps, we can acquire many SIFT keypoints, with each containing orientation and position. These features are partially invariant to illumination changes and are robust to local geometric distortion. Therefore, the proposed scheme adopts SIFT to acquire significant features of image regions.

2.2 Review of Hu's invariant moment features [16]

With Hu's [16] invariant moment, assuming that pixels of a $M \times N$ image are denoted by $f(x,y)$ with $1 \le x \le M$ and $1 \le y \le N$, the image moment m_{pq} of order $(p+q)$ is calculated using Eq. (1).

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

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

$$\overline{x} = \frac{m_{10}}{m_{00}}, \overline{y} = \frac{m_{01}}{m_{00}} \tag{2}$$

For a digital image $f(x,y)$, the moment equation becomes to Eq. (3).

$$\mu_{pq} = \sum_{x=1}^{M} \sum_{y=1}^{N} \left(x - \overline{x}\right)^p \left(y - \overline{y}\right)^q f(x,y) \tag{3}$$

The equations for acquiring the central moments are listed in Eqs. (4) and (5).

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

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

Hu further defined the invariant moments of order up to 3 by listing in Eq. (6).

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

Hu presented these 7 moments for representing similar properties under the processing of shifting, rotation, and mirroring.

2.3 The expanding block algorithm [26]

Exhausted comparisons between blocks are always required in conventional copy–move forgery detection methods. However, the computation complexity is very high in exhausted comparisons. The EB first clusters all blocks by block mean. Each block is only compared with dedicated blocks with closed block mean to reduce the computation load for detecting copy–move forgery regions in an image. Therefore, the EB significantly reduces the computation time that the conventional exhausted comparison algorithm requires.

2.4 The enhanced cluster expanding block algorithm [9]

The ECEB adopts block mean and block variance features to compare each block only with its neighboring blocks to reduce the computation load that the EB required. The ECEB divides the image into overlapped blocks and then calculates two different block features, mean and variance, to acquire the feature vectors. The intersection of two feature vectors reduces the block numbers that have to be compared, and the ECEB is empirically more efficient than the EB only for the adopting mean feature.

3 Proposed scheme

This section introduces the proposed algorithm and properties of the proposed scheme. Section 3.1 introduces the proposed algorithm. Section 3.2 presents the theoretical comparisons of the proposed scheme with the EB [26] and the ECEB [9].

3.1 Algorithm of the proposed scheme

The proposed algorithm acquires pairs of matched keypoints and the pair number of matched keypoints depends on the image structure. Each pair of blocks generated from matched keypoints is first compared through invariant moments and a pre-defined

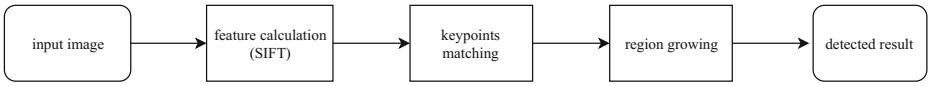

Fig. 1 Important steps of the proposed scheme

threshold to determine if the pair of blocks is matched or not. If the pair of started blocks are matched, the region growing strategy is then applied to this pair of started blocks. The started blocks and region growing blocks are measured through 7 invariant moments of the largest inner circle within the block. Figure 1 shows the important steps of the proposed scheme. In which the SIFT feature calculation, SIFT keypoints matching, and matched keypoints generated region are three major steps of the proposed scheme.

Figure 2 shows the definition of the largest inner circle within a 7×7 block. Figure 2b shows that only grey pixels are selected to calculate the invariant moment features. The determination of a $k \times k$ block with k being an odd number acquires the center pixel from a pair of matched blocks. The usage of largest inner circle exhibits the property of rotational copy–move regions detection.

The proposed scheme uses SIFT to acquire keypoints, according to scale and orientation information, for further block matching processing. By using the keypoints scale feature, the calculated keypoints are matched with similar length, and the orientation differences are therefore measured. The copy–move regions are then detected through a region growing strategy from matched blocks. Figure 3 Introduces the proposed algorithm.

In the presented algorithm, two functions and three thresholds are defined. First, *SIFT* represents the keypoints calculation and *Hu* represents the invariant moments calculation. The keypoints have the feature set of $k_i(s_i, \theta_i, x_i, y_i)$, where s_i is the strength, θ_i is the direction, and (x_i, y_i) denotes the coordinates. Moreover, *Hu_fp* represents the invariant moments calculation on a flipped block, in which horizontally and vertically flipping are both performed. Three thresholds, δ_k, δ_h, and δ_r, are determined for the keypoints scale, region invariant moments, and detected region size, respectively. The parameter δ_k is selected by $t \times \max\{|s_i|, |s_j|\}$, where $0 \leq t \leq 0.02$. The parameter δ_h is defined as Eq. (7)

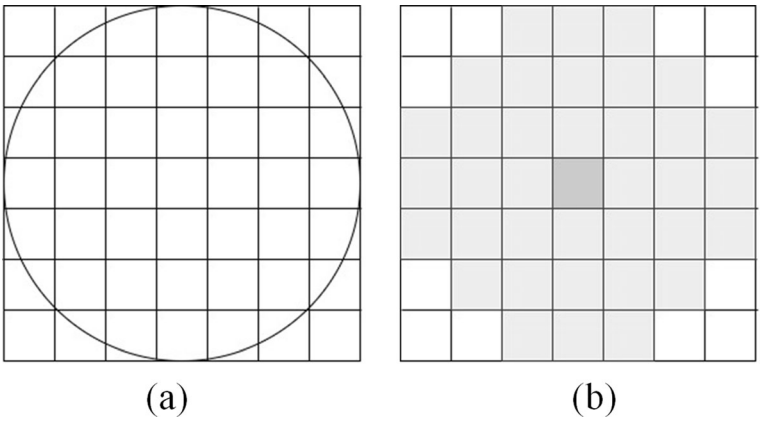

Fig. 2 Definition of (**a**) the ideal largest inner circle within a 7×7 block, (**b**) the computed largest inner circle within a 7×7 block

Input: $I(x,y)$, $1 \le x \le M$, $1 \le y \le N$, where $0 \le I(x,y) \le 255$.
Output: $R(x,y)$
Algorithm:

01 apply Gaussian smooth processing on the input image I
02 set K: $\{k_i(s_i, \theta_i, x_i, y_i)\} \leftarrow SIFT(I)$ // k_i represent keypoints
03 sort k_i by parameter s_i
04 while (not empty(K))
05 for each k_i in K
06 choose another k_j in K with $|s_i - s_j| < \delta_k$
07 diff = min($|Hu(I(r_i)) - Hu(I(r_j))|$, $|Hu(I(r_i)) - Hu\_fp(I(r_j))|$)
08 if (diff $< \delta_h$) // I(r_i) is the initial region of k_i
09 rotate surrounded region of r_j to $\theta_i - \theta_j$ degree
10 for all blocks (b_i, b_j) surrounded by (r_i, r_j) respectively
11 diff = min($|Hu(b_i) - Hu(b_j)|$, $|Hu(b_i) - Hu\_fp(b_j)|$)
12 if (diff $< \delta_h$)
13 add b_i to r_i
14 add b_j to r_j
15 endif
16 endfor
17 endif
18 if $|r_i| > \delta_r$
19 move detected copy-move regions r_i and r_j to R
20 else
21 remove the detected regions r_i and r_j
22 endif
23 if no more k_j can be searched,
24 remove k_i from K
25 endfor
26 endwhile

Fig. 3 Algorithm of the proposed scheme

$$\sum_{i=1}^{7} \log\left(\frac{\phi_{pi}}{\phi_{qi}}\right) \le \delta_h \tag{7}$$

where ϕ_{pi} and ϕ_{qi} represent Hu's 7 invariant moments of two regions p and q with $i = 1 \ldots 7$.

Figure 4 shows all region growing selections b_i of an 8 × 8 block, in which the central block is I(r_i) in Fig. 3. For each block is matched, the block is then added to the matched region. The region growing strategy stops when no further growing block is matched. Therefore, we can acquire the matched regions through the steps of lines 9–16 in Fig. 3.

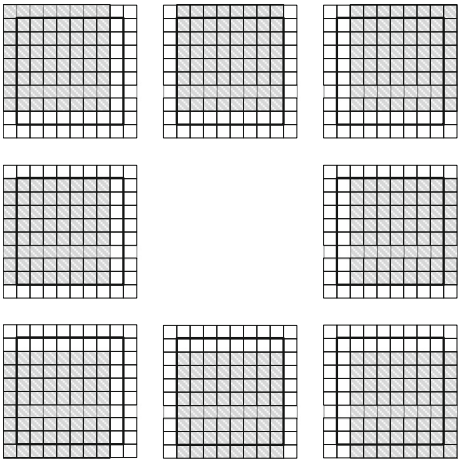

Fig. 4 Region growing blocks selection of a matched 8 × 8 block

Figure 5 shows a flowchart of the proposed algorithm to introduce the concept of the proposed algorithm. Figure 6 shows important steps of the proposed scheme. Figure 6a depicts two copy–move regions and their keypoints features, including scale and orientation. Figure 6b shows the initial matched regions and Fig. 6c depicts the growing blocks added to the matched regions.

3.2 Performance evaluation of the proposed algorithm

This section theoretically compares the properties between the proposed algorithm, the EB [26] and the ECEB [9] in Table 1. The proposed scheme adopts SIFT to acquire keypoints. The orientation of keypoints denotes the direction of the region around the keypoints. Therefore, the proposed scheme can detect rotational copy–move regions. Compared to the ECEB scheme [9] using the relationships within matched blocks, the propose scheme is further advanced in acquiring orientation information through SIFT. Moreover, the proposed scheme uses the region growing strategy to acquire the copy–move duplicated regions efficiently.

Furthermore, the proposed scheme also theoretically compares with some SIFT related works. Due to all these methods are based on SIFT features, these schemes have the property of robust on region rotation. Table 2 compares the significant technique, advantages, and disadvantages of these four methods.

4 Experimental results

This section demonstrates experimental results of our proposed scheme. All experiments were performed by MATLAB 2016a on a PC with an Intel i7–6700 CPU and 32GB RAM. Experimental results given in this section include detected results after applying some attacks on the copy–move forgery test images, and the computation times. The keypoints are detected through 5 × 5 Gaussian smoothing with $\sigma = 1.0$. Other parameters are empirically assigned as, $\delta_k = 0.015 \times \max\{|s_i|, |s_j|\}$, $\delta_h = 0.05$, $\delta_r = 0.98$.

Figure 7 shows the experimental results of applying no attacks on three test images. Figure 7a-c show three 256 × 256 original images: Birds, Coins, and Sheep. Figure 7d-f

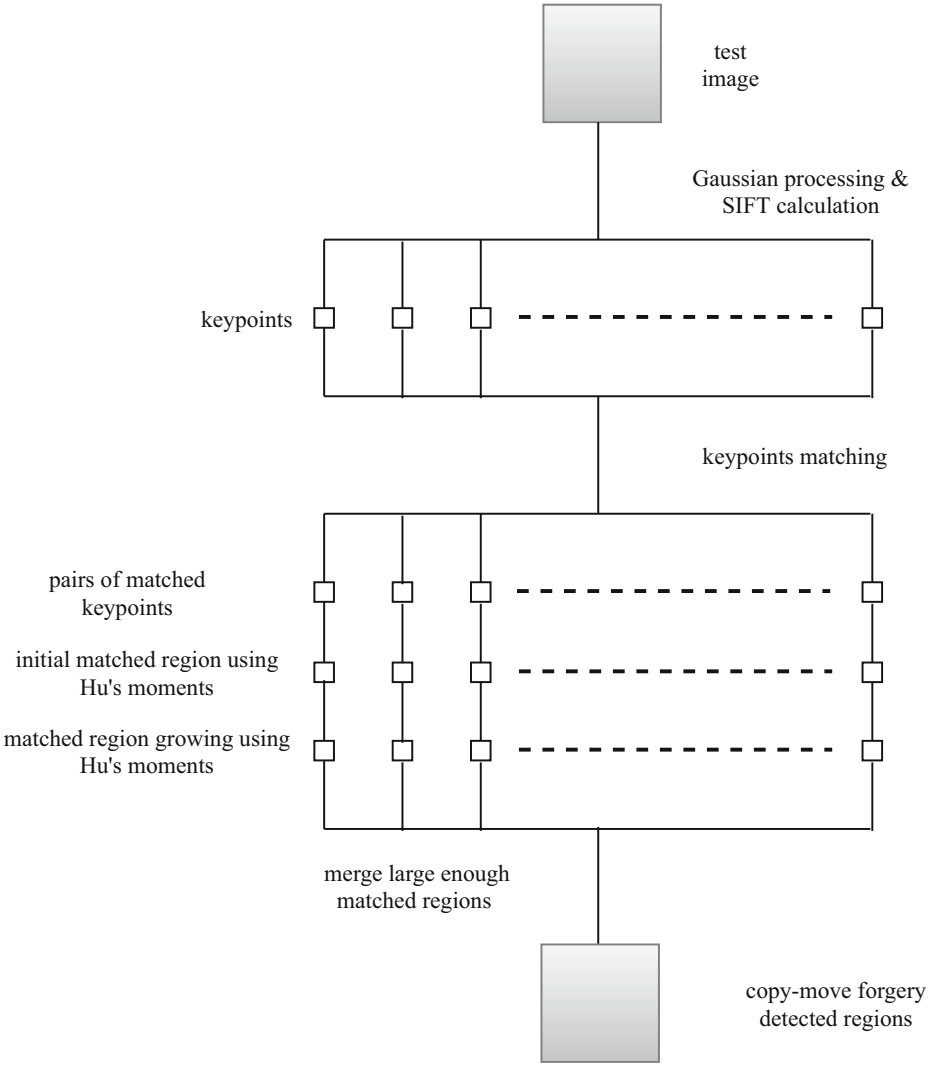

Fig. 5 Flowchart of the proposed algorithm

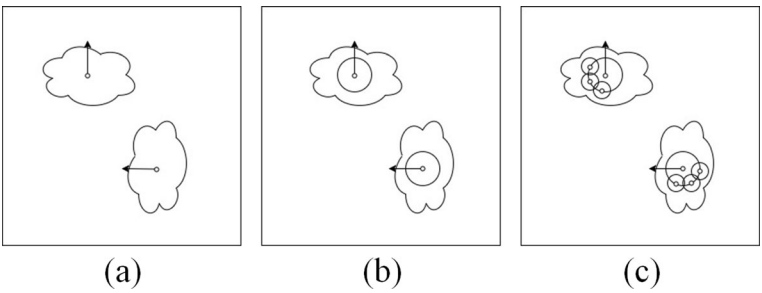

Fig. 6 Example of important steps in the proposed scheme

Table 1 Properties comparison between the proposed scheme and three important works

	the EB [26]	the ECEB [9]	the proposed scheme
Rotational detection	×	×	O
Flip detection	×	×	O

show three copy–move forgery images, respectively. Figure 7g-i show ideal detected results, Figure 7j-l show the forgery images with keypoints, and Figure 7m-o show three copy–move detected results by the proposed scheme. Figure 7g-i also shows that copy–move regions include rotating and flipped modifications. Table 3 lists important features in Fig. 7, including number of keypoints and matched keypoints, computation time, and detection rates.

Our experimental results show two important measurements, true and false positive rates, on the detected results. The true positive rate (TPR) measures the rate of correctly recognizing copy-move forgery regions. The false positive rate (FPR) measures the rate of detecting copy-move forgery regions on non-copy-move forgery regions. The true positive rate is defined by $\frac{|D\cap M|+|D\cap B|}{|M|+|B|}$, where D denotes the set of pixels in detected regions, B denotes the set of pixels in original copy-move regions, M denotes the set of pixels in copy-move forgery modified regions, and |A| denotes the pixel number of a given set A. The false positive rate is defined by $\frac{|D\cap(I-M-B)|}{|I-M-B|}$, where I denotes the set of pixels in whole test image and A–B denotes the removal of region B from region A. Table 3 lists the experimental results of Fig. 7, including TPR and FPR.

Figures 8 and 9 show the detected results of applying two kinds of smooth attacks on the forgery images. Figure 8 shows the TPR of the forgery images applying Gaussian attacks with $\sigma = 1$ from 3×3 to 9×9. Figure 9 shows the FPR of the forgery images applying Gaussian attacks also with $\sigma = 1$ from 3×3 to 9×9. Figures 8 and 9 show that serious attacks acquiring blurred images lead to poor TPR values. The FPR values are closed among these Gaussian attacks, meaning that smooth attacks generate few false detections.

Figure 10 shows the number of keypoints under different smooth processing. Among the original and four different parameter assignments, the selection principle is fewer, but not too

Table 2 Properties comparison between the proposed scheme and SIFT-based schemes

	significant technique	advantages	disadvantages
[2]	SIFT+ g2NN keypoints match + hierarchical clustering+geometric estimation	efficient matching by g2NN	need to improve on detecting highly uniform textured copy-move regions
[6]	SIFT + agglomerative hierarchical clustering	detect smooth copy-move regions	improving non-affine transformations
[17]	SIFT + nearest neighbor	robust to noise and scaling	difficult on detecting small-sized copy-move regions
[28]	SIFT + affine transform estimation	effectively detect automatically synthesized forgery images	hard to find reliable keypoints in regions with little visual structures
Proposed scheme	SIFT+ keypoints matching + region growing	region orientation detection	hard to detect small or thin copy-move regions

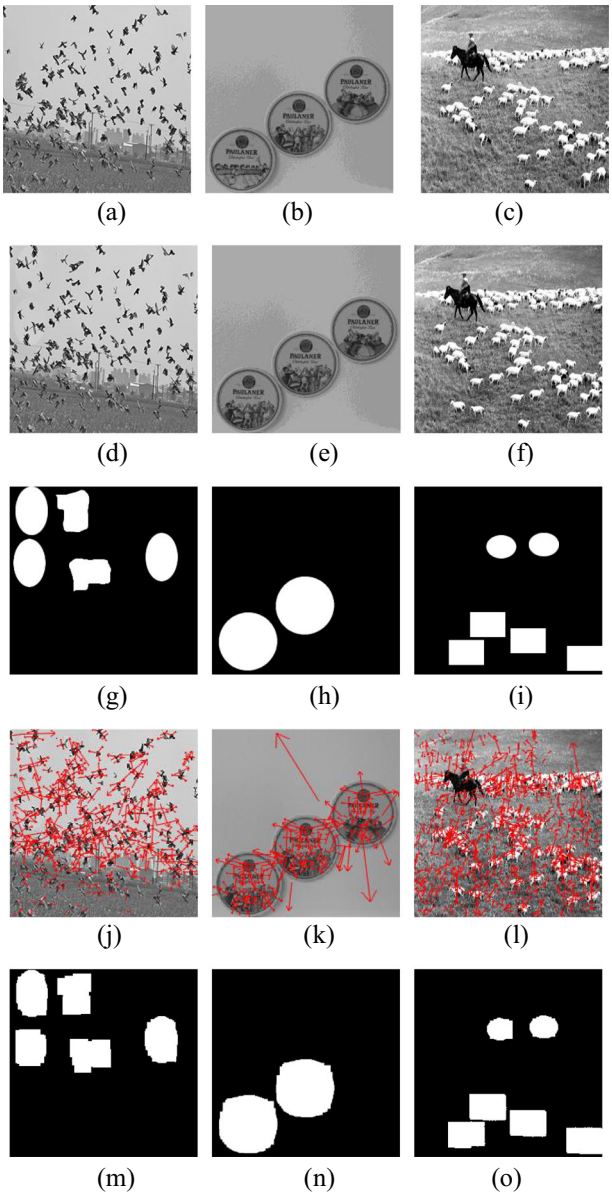

Fig. 7 Examples of three test images, (**a**)-(**c**) three test images: Birds, Coins, Sheep, (**d**)-(**f**) three copy-move forgery images, (**g**)-(**i**) ideal detected results, (**j**)-(**l**) three forgery images with keypoints, (**m**)-(**o**) three copy-move detected results by the proposed scheme

few, keypoints. Therefore, step 1 in the proposed algorithm, as shown in Fig. 3, is empirically determined by 5×5 Gaussian with $\sigma = 1.0$.

Figure 11 shows the TPRs compared with previous ECEB scheme [9] and the EB scheme [26]. Three test images include three different properties. The Coins image only includes identical copy regions, the Birds image includes identical and rotational copy regions, and the Sheep image includes identical, rotational, and flipped copy regions. Therefore, the proposed

Table 3 Experimental results of Fig. 7

Images	Birds	Coins	Sheep
number of keypoints	590	302	878
number of matched keypoints	1568	287	4692
Execution time (sec.)	44.74	18.95	130.67
True Positive rate (TPR)	97.50%	100%	98.78%
False Positive rate (FPR)	1.13%	0.21%	0.22%

scheme detects these three kinds of attacks well. The ECEB scheme detects identical and rotational copy regions well. Finally, the EB can only detect identical copy regions.

Figure 12 shows the FPRs between the proposed scheme and two conventional schemes [9] [26]. Comparing these two conventional schemes, the proposed scheme exhibits similar performance on FPR.

Table 4 shows performance comparison on detecting the CoMoFoD [32] dataset between the proposed scheme and two other works [2, 22], in which including SIFT-based and segmentation-based scheme. The proposed scheme has the property of larger detected regions because of the usage of moment-based region growing strategy. Moreover, the usage of the moment-based region growing strategy also leads to hard to detect small of thin copy-move regions.

Figure 13 compares the computation time with two previous works [9, 26] under the same hardware and software systems. Since the computation time required in the proposed scheme is through keypoints based on the image structure, the computation time on these three test images are different. Since the Coins image has the smallest keypoints among these three test images, the matched keypoints are also the smallest and the computation time is quite limited. The Birds image has the largest computation time because of the biggest quantity of matched keypoints. Experimental results in Fig. 11 show that the proposed scheme exhibits mostly less computation time than the ECEB or the EB schemes. Since the proposed scheme uses the SIFT for acquiring keypoints information, including scale and orientation, to obtain more information for detecting the copy-move regions, the proposed scheme is more robust than previous works.

Finally, the proposed algorithm shows that the computation time required is determined by SIFT, keypoints match, and region growing. Since SIFT only requires a limited amount of

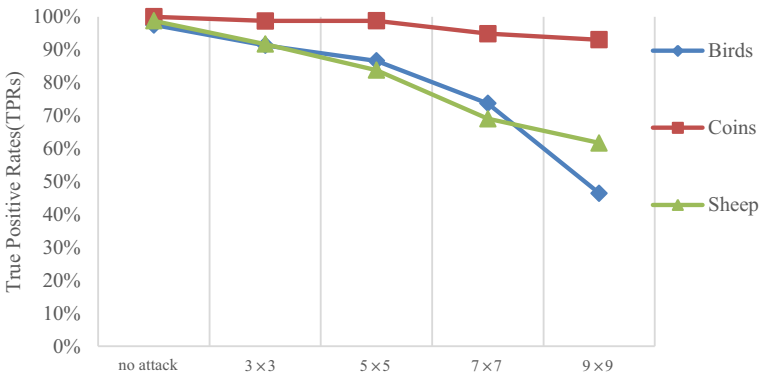

Fig. 8 True positive rates of the proposed scheme under different Gaussian attacks with $\sigma = 1$

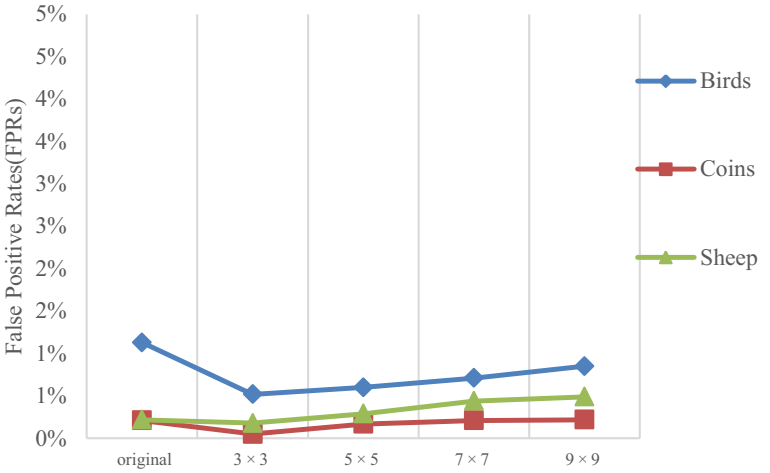

Fig. 9 FPR of the proposed scheme under different Gaussian attacks with $\sigma = 1$

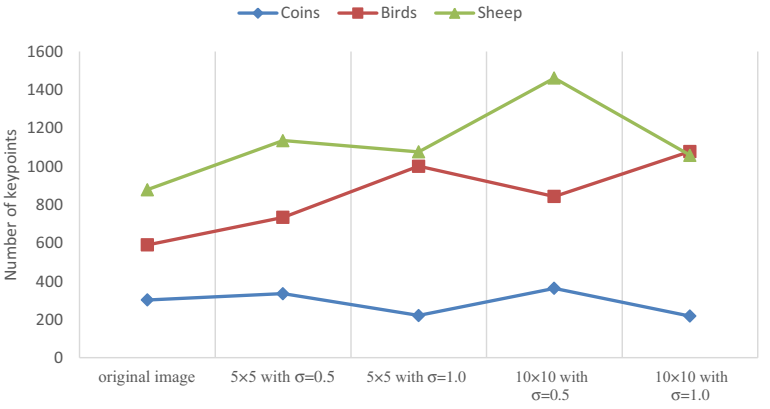

Fig. 10 Number of keypoints under different Gaussian smooth attacks

time, the two remaining parameters, number of matched keypoints and pixels of copy-move forgery regions, determine most of the computation time of the proposed algorithm. From the algorithm introduced in Fig. 3 and the experimental results in Table 3, the computation time is

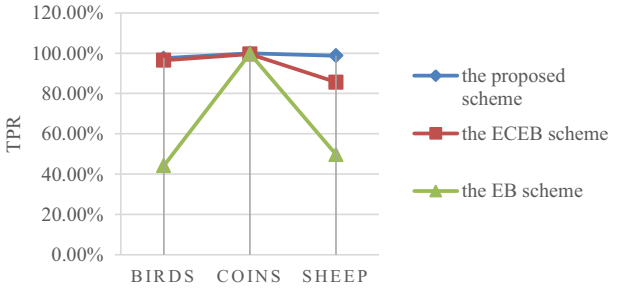

Fig. 11 TPRs of test images between the proposed scheme, the EB scheme [26], and the ECEB scheme [9]

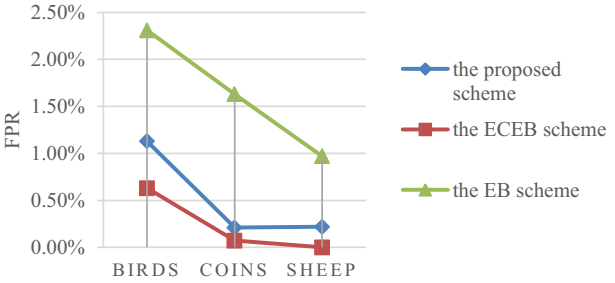

Fig. 12 FPRs of test images between the proposed scheme, the EB scheme [26], and the ECEB scheme [9]

Table 4 Comparisons with other methods [2, 22] on plain copy-move of database CoMoFoD [32]

methods	[2]	[22]	the proposed scheme
Precision	70%	54.46%	70.19%
Recall	87.5%	85.04%	84.61%

proportional to $O(M) + O(R)$ where M denotes a number of matched keypoints and R denotes the pixel number of copy-move forgery regions.

The above analysis shows that the proposed scheme exhibits good performance on computation load and detection rates, including TPR and FPR. Comparing with other works [2, 22], the Precision and Recall rate also outperforms these two works. The proposed scheme has the following properties. First, the selected SIFT acquires directional information for detected regions. The directional information used in the proposed scheme reveals the extension possibility of the proposed scheme. Second, the keypoints matching method detects similar regions. Third, the region growing method generates the copy-move regions through the region moment measurements for acquiring better detected results. The proposed scheme can be improved for detecting small or thin copy-move regions. Moreover, the proposed scheme can combine with other data like sensor data [24] or video data [18] for acquiring better detection on many kinds of copy-move manipulations.

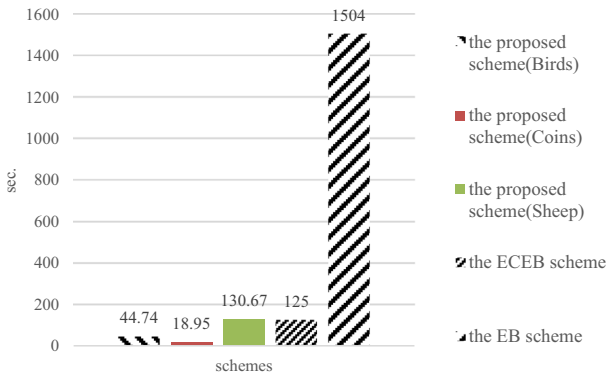

Fig. 13 Computation time comparison on the three test images between the proposed scheme, the EB scheme [26], and the ECEB scheme [9]

5 Conclusions

This proposed scheme uses SIFT keypoints features, invariant moments, and the region growing technique to detect copy–move forgery regions. The proposed scheme uses scale of SIFT keypoints to find matched initial blocks, and then uses Hu's invariant moments to check if the initial blocks are copy–move forgeries or not. For a pair of matched initial blocks, the further region growing strategy detects the exact copy–move regions through Hu's invariant moment measurements. Experimental results show that the proposed scheme is efficient for detecting copy–move regions with rotating and flipped modifications with the moments. Property discussion and performance evaluation show that the proposed scheme exhibits good detection ability among the related works. Moreover, the proposed scheme detects the orientation differences between copy-move regions. Since the computation load is mainly based on the number of matched keypoints and the size of copy-move forgery regions, reducing the matched keypoints and an efficient region growing method merits our future study.

Acknowledgements This paper was partially supported by the National Science Council of the Republic of China under contract MOST 106-2221-E-032-057.

References

1. Al-Qershi OM, Khoo BE (2013) Passive detection of copy-move forgery in digital images: state-of-the-art. Forensic Sci Int 231:284–295
2. Amerini I, Ballan L, Caldelli R, Del Bimbo A, Serra G (2011) A SIFT-based forensic method for copy–move attack detection and transformation recovery. IEEE Trans Inform Foren Sec 6:1099–1110
3. Amerini I, Ballan L, Caldelli R, Del Bimbo A, Tongo LD, Serra G (2013) Copy-move forgery detection and localization by means of robust clustering with J-linkage. Signal Process Image Commun 28:659–669
4. Bi X, Pun C, Yuan X (2016) Multi-level dense descriptor and hierarchical feature matching for copy-move forgery detection. Inf Sci 345:226–242
5. Bi X, Pun CM, Yuan XC (2018) Multi-scale feature extraction and adaptive matching for copy-move forgery detection. Multimed Tools Appl 77(1):363–385
6. Bin Y, Sun X, Guo H, Xia Z, Chen X (2017) A copy-move forgery detection method based on CMFD-SIFT. Multimed Tools Appl 2017:1–19
7. Bravo-Solorio S, Nandi AK (2011) Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics. Signal Process 91:1759–1770
8. Cao Y, Gao T, Fan L, Yang Q (2012) A robust detection algorithm for copy-move forgery in digital image. Forensic Sci Int 214:33–43
9. Chen CC, Wang H, Lin CS (2017) An efficiency enhanced cluster expanding block algorithm for copy-move forgery detection. Multimed Tools Appl 77(15):19327–19346
10. Christlein V, Riess C, Jordan J, Riess C, Angelopoulou E (2012) An evaluation of popular copy-move forgery detection approaches. IEEE Trans Inform Foren Sec 7:1841–1854
11. Cox I, Miller M, Bloom J, Fridrich J, Kalker T (2007) Digital watermarking and steganography, 2nd edition, Morgan Kaufmann
12. Davarzani R, Yaghmaie K, Mozaffari S, Tapak M (2013) Copy-move forgery detection using multiresolution local binary patterns. Forensic Sci Int 231:61–72
13. Dixit R, Naskar R (2018) Copy–move forgery detection utilizing Fourier–Mellin transform log-polar features, J. Electron Imag 27(2):023007
14. Farid H (2009) A survey of image forgery detection. IEEE Signal Process Mag 2:16–25
15. Fridrich J, Soukal D, Lukás J (2003) Detection of copy move forgery in digital images. Proc Conf Digital Forensic Res Workshop 55–61
16. Hu MK (1962) Visual pattern recognition by moment invariants. IRE Trans Inform Theory 8(2):179–187

17. Huang H, Guo W, Zhang Y (2008) Detection of copy-move forgery in digital images using SIFT algorithm. IEEE Pacific-Asia Workshop Comput Intell Industr Appl 2:272–276
18. Jia S, Xu Z, Wang H, Fang C, Wang T (2018) Coarse-to-fine copy-move forgery detection for video forensics. IEEE Access 6:25323–25335
19. Kobayashi M, Okabe T, Sato Y (2010) Detecting forgery from static-scene video based on inconsistency in noise level functions. IEEE Trans Inform Forensics Sec 5(4):883–892
20. Lai Y, Huang T, Lin J, Lu H (2018) An improved block-based matching algorithm of copy-move forgery detection. Multimed Tools Appl 77(12):15093–15110
21. Li Y (2013) Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching. Forensic Sci Int 224(1–3):59–67
22. Li J, Li XL, Yang B, Sun XM (2015) Segmentation-based image copy-move forgery detection scheme. IEEE Trans Inform Foren Sec 10:507–518
23. Lin C, Tsay J (2014) A passive approach for effective detection and localization of region-level video forgery with spatio-temporal coherence analysis. Digit Investig 11(2):120–140
24. Liu Y, Nie L, Liu L, Rosenblum DS (2016) From action to activity: sensor-based activity recognition. Neurocomputing 181(12):108–115
25. Lowe DG (2004) Distinctive image features from scale-invariant keypoints. Int J Comput Vis 60(2):91–110
26. Lynch G, Shih FY, Liao HM (2013) An efficient expanding block algorithm for image copy-move forgery detection. Inf Sci 239:253–265
27. Muhammad G, Hussain M, Bebis G (2012) Passive copy move image forgery detection using undecimated dyadic wavelet transform. Digit Investig 9:49–57
28. Pan XY, Lyu SW (2010) Region duplication detection using image feature matching. IEEE Trans Inf Forens Sec 5(4):857–867
29. Popescu AC, Huang HF (2004) Exposing Digital Forgeries by detecting duplicated image regions. Department of Computer Science TR2004–515
30. Ryu SJ, Kirchner M, Lee MJ, Lee HK (2013) Rotation invariant localization of duplicated image regions based on Zernike moments. IEEE Trans Inform Foren Sec 8:1355–1370
31. Soni B, Das PK, Thounaojam DM (2018) CMFD: a detailed review of block based and key feature based techniques in image copy-move forgery detection. IET Image Process 12(2):167–178
32. Tralic D, Zupancic I, Grgic S (2013) CoMoFoD – new database for copy- move forgery detection. Proc Int Symp ELMAR, 49–54
33. Tu HK, Thuong LT, Synh HVU, Khoa HV (2015) The efficiency of applying DWT and feature extraction into copy-move images detection. Int Conf Adv Technol Commun (ATC)
34. Zhao J, Guo J (2013) Passive forensics for copy-move image forgery using a method based on DCT and SVD. Forensic Sci Int 233:158–166

Chien-Chang Chen received the B.S. degree from Department of Computer and Information Science at Tunghai University, Taiwan, in 1991, and the Ph.D. degree from Department of Computer Science at National Tsing Hua University, Taiwan, in 1999. He is currently a Professor at the Department of Computer Science and Information Engineering, Tamkang University, Taiwan. His research interests include secret image sharing, image watermarking, and texture analysis.

Wei-Yu Lu received the Bachelor degree in computer science and information engineering from Tamkang University, New Taipei, Taiwan, in 2015. He is currently studying in Tamkang University for Master degree, and research interest is copy-move forgery detection.

Tsung-Hsuan Chou received the Bachelor degree in Mathematics from Tamkang University, Taipei, Taiwan, in 2015. He is currently studying in Tamkang University for Master degree, but he's colleage degree is in Math,now he is interesting in computer science and information engineering, and research interest is Image Copy-Move Detection.