An Efficiency Enhanced Cluster Expanding Block Algorithm for Copy-Move Forgery Detection

Cheng-Shian Lin
Department of Banking and Finance
Chinese Culture University
Taipei, Taiwan
e-mail: charleslin2015313@gmail.com

Chien-Chang Chen, Yi-Cheng Chang
Department of Computer Science and Information Engineering
Tamkang University
Taipei, Taiwan
e-mail: ccchen34@mail.tku.edu.tw
tim3553431992@hotmail.com.tw

***Abstract*— This paper presents an efficient scheme for detecting copy-move forgery tampering attacks. The copy-move forgery attack is defined as a region of an image is replaced by a copy of other region in the same image. This detection is useful for malicious modifying an image. The proposed scheme improves previous cluster expanding block scheme to clustering by mean and variance for reducing the computation time. Experimental results show that the proposed scheme requires fewer computation time. Although the overhead of preprocessing is an extra load that takes more time than previous cluster expanding block scheme, but the total computation time is still improved at least 10% comparing with previous study. Moreover, the using of block variance reduces the false positive rate.**

Keywords—copy-move forgery detection; mean; variance;

I. INTRODUCTION

With the rapid growth of digital devices and image/video editing software, the digital media file has become easier than ever to modify, synthesis, and produce with increasing sophistication. The purpose of digital image forensics is to verify the trustworthiness of digital image/video, and it has become an important and exciting field of recent research [1-15].

Digital image forensics can be categorized as active and passive approaches [2, 3]. Active approaches, such as digital watermark or signature, proposed in the past as a way to verify the integrity and authenticity of digital images. The watermark or signature is inserted into image while it is acquired, and any malicious tampering of the image can be detected through analysis of the value of a digital watermark or signature. However, a major drawback of active approaches is that the digital capture devices do not contain the module to insert watermarks and signatures. To overcome this problem, passive approaches which do not need any prior information about image to detect traces of tampering are extensively studied in recent research.

Over the past years, a large number of passive approaches for image copy-move forgery detection have been proposed, which can be classified into eight categories based on the extracted feature [3], namely, DCT-based [1, 4], Log-polar transform-based [5], texture and intensity-based [6], invariant key-points based [7], invariant image moments based [8], PCA-based, SVD-based, and other algorithms [9-12]. In DCT-based approach, Fridrich et al. [1] presented a method for detecting copy-move regions in digital image. The DCT coefficients were extracted and then sorted with lexicographically scheme to reduce complexity of the comparisons. Finally, the tampered regions can be detected based on approximate block matching. Cao et al. [4] proposed a DCT-based approach, the aim of this approach is to reduce the size of the feature vector and add robustness against attacks, such as blurring and noise adding. For texture and intensity-based approach, Davarzani et al. [6] extracted feature vectors for each overlapping image block using multi-resolution local binary patterns operators (MLBP) and then sorted by lexicographical order. They also utilized the k-d tree and random sample consensus (RANSAC) algorithms to reduce the block matching time and eliminate false detections, respectively. In [7], invariant key-points based approach, Amerini et al. used scale invariant features transform (SIFT) to detect the duplicated region which altered the size or angle using the geometric transformations before it is pasted. Invariant image moments based approach, Ryu et al. [8] presented a forensic approach to detect and localize the copy-rotate-move duplicated regions based on Zernike moments. Based on their experimental results, the Zernike moments based algorithm have high detection accuracy rate with various rotation degrees compared to the polar-based approach [5] and the SIFT-based approach [7].

For other detection algorithms, Muhammad et al. [9] decomposed image using undecimated dyadic wavelet transform. They take the wavelet coefficients from each block as the feature vector. If a pair of vectors have similar Euclidean distance values, the corresponding pairs of blocks is detected as duplicated. Lynch et al. [10] proposed an efficient expanding block algorithm, which primarily use direct block comparison based on block features for detecting the duplicated region. Zhao et al. [11] further integrated DCT and SVD techniques to extract image feature and localize tampered regions. Li et al. [12] segments the image into semantically independent patches prior to keypoint extraction. And then the copy-move regions can be detected by matching between these patches. Besides the aforementioned methods, a few other methods have been proposed for video copy-move forgery detection [13-15].

Although the previous approaches can detect copy-move forgery, there are some drawbacks to be improved. Fridrich's approach [1] requires $(MN)^2$ comparisons to compare the image with every cyclic-shifted version of itself by exhausting search, where image size is $M \times N$. Lynch et al. [10] proposed

978-1-4673-7695-2/15 $31.00 © 2015 IEEE
DOI 10.1109/INCoS.2015.90

the expanding block (EB) approach to detect forged region. Although this method is more efficient as compared to exhaustive search, it still requires much time for block comparing.

In this paper, we propose an enhanced cluster expanding block algorithm for detecting region duplication forgery. We first divided image into overlapping blocks, and then the two different features, mean and variance, of each block are extracted and formed to feature clusters. We use the block comparison scheme to verify tamper block. Since two features can reduce comparison load efficiently, the proposed approach is assumed to be efficient for detecting region duplication forgery. Finally, the refinement process eliminates the false detection.

We have carried out experiments over copy-move tampering, and the results show that our approach outperforms previous approaches [10], and can effectively detect and localize duplicated regions.

The paper is organized as follows. Section II gives a brief review of previous expanding block (EB) algorithm [10]. Section III presents the details of the proposed enhanced cluster expanding block (EB) algorithm. Section IV presents the experimental results. Section V followed by concluding remarks.

II. REVIEW OF RELATED WORKS

In this section, we briefly review the expanding block algorithm [10], which is described as follows.

The expanding block (EB) algorithm primarily uses direct block comparison rather than indirect comparisons based on block features. The EB approach first partition an image into a number of overlapping blocks. For computation efficiency, the feature of each block is extracted by calculating the average intensity of all pixels within block. According to the block feature, blocks are sorted and grouped evenly into K groups. Each group contains the blocks with a similar feature. For reducing the gap of block feature between each group, the blocks from the ith, (i-1)th, (i+1)-th groups are placed into the ith bucket. Fig. 1 illustrates an example of sorting 10 blocks and grouping them into buckets. For reducing the block comparisons, blocks are compared only against other blocks in the same bucket. A block can be removed from the bucket if it does not match any other block in the bucket; otherwise, the block comparisons are continued. Finally, the remaining blocks in buckets are detected as the duplicated region.

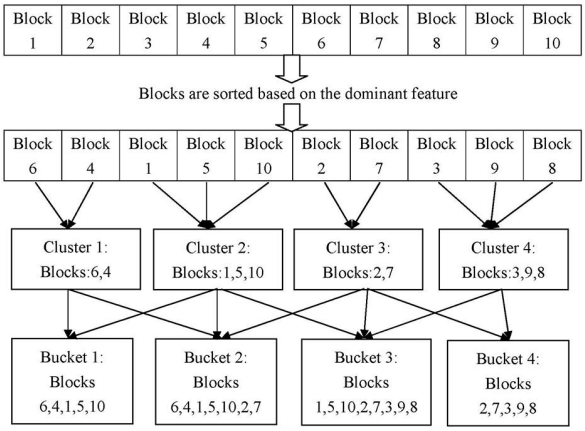

Fig. 1. Example of grouping 10 blocks to 4 buckets.

III. THE PROPOSED ALGORITHM

This section introduces our proposed cluster enhanced copy-move forgery detection method. The proposed scheme improves searching performance of previous expanding block algorithm [10] from one cluster mean to two clusters mean and variance. The image is first partitioned into overlapped blocks with size $k \times k$. Mean and variance of each block is then calculated as features. The blocks are then sorted in order and uniformly partitioned to c clusters. Since we have two clusters, mean and variance, any block within the same bucket is applied full comparison with all other blocks in the same bucket. The proposed algorithm is introduced as follows,

1. Partition the image of size $M \times N$ into overlapped blocks with size $k \times k$ to generate $(M-k+1) \times (N-k+1)$ blocks.
2. Calculate mean and variance of each block to acquire two feature vectors.
3. Sort each feature vector independently.
4. Uniformly partition each feature vector to c clusters.
5. Combine neighboring s clusters to acquire buckets.
6. For each block a in a mean bucket and all other blocks b in the same mean bucket, apply the following steps to search similar blocks

6.1 If a and b in the same variance bucket, calculate Euclidean distance d between blocks a and b

$$d = \sum_{i=0}^{n-1} (b_i - a_i)^2$$

6.2 If d is smaller than a pre-defined threshold t, then block a and block b is taken as match block.

7. Summarize distances of all match block pairs and filter out those block pairs with appearance smaller than a pre-defined occurrence p.
8. Merge those blocks with the same distance to acquire the copy-forgery area detecting result.

In the proposed algorithm, many parameters should be pre-determined. In step 4, the cluster number c determines the number of mean and variance should be separated. A larger number c creates small blocks in each cluster and more buckets we have to process. In Step 5, the neighboring blocks selection parameter s determines the number of blocks that have to be compared. A larger number s increases the comparison load. In Step 6.2, the threshold t determines the robustness that the proposed scheme can have. When the image is suffering from modifications like jpeg compression, a large number t can detect the similarity after larger jpeg compression. Therefore, there are three parameters c, s, and t to determine the detection result.

IV. Experimental Results

This section demonstrates some experimental results of our proposed scheme. All experiments were performed by MATLAB 7.11 on a PC with an Intel i7-3770 CPU and 4GB RAM. Experimental results given in this section include detection result of a copy-move forgery attacks and computation time. Fig. 2 shows the detection results under difference parameters. Fig. 2.(a) shows the copy-move forgery image, in which a vertical area in left is copied to right of the image. The parameters are assigned as k=16, c=256, s=1, and t=0.15. Figs. 2.(c), 2.(e), and 2.(g) depict the JPEG compressed image by QF=95, 75, and 50, respectively. Figs. 2.(b), 2.(d), 2.(f), and 2.(h) are detection result of Figs. 2.(a), 2.(c), 2.(e), and 2.(g), respectively.

(a) (b) (c) (d) (e) (f) (g) (h)

Fig. 2. (a) one copy-move forgery image, (b) the proposed forgery detected result of (a), (c) the JPEG QF=95 of (a), (d) the proposed forgery detected result of (c), (e) the JPEG QF=75 of (a), (f) the proposed forgery detected result of (e), (g) the JPEG QF=50 of (a), (h) the proposed forgery detected result of (g).

Table 1 lists the true positive rate and false positive rate between the proposed scheme and EB algorithm [10]. The true positive rate is defined by the rate of an algorithm identifies the forgery pixels in a forgery region. The false positive rate defines the ratio of an algorithm recognize not forgery pixels as a forgery region. Table 1 shows that the proposed scheme has better detection results than EB algorithm. Moreover, Table 1 also shows that the detection rate is decayed according to the image quality reduction by higher JPEG compressions.

Table 1. True positive rate and false positive rate of Fig. 2.

	true positive rate	false positive rate
No JPEG compression	1	0
No JPEG compression of EB algorithm	1	0
JPEG QF=95	0.9329	0
No JPEG compression of EB algorithm	0.9329	0
JPEG QF=75	0.9491	0
No JPEG compression of EB algorithm	0.9491	0
JPEG QF=50	0.5363	0
JPEG QF=50 of EB algorithm	0.5363	0.0747

Table 2 lists the computation time between the proposed scheme and previous expanding block (EB) algorithm [10]. The experiments are executed by parameters under the parameters k=16, s=1, c=256, and t=0.15. The computation time includes preprocessing and block matching time. The

preprocessing time includes the time to segment an image to blocks, to categorize all blocks into clusters, to eliminate overlapped blocks for matching calculation. Table 2 shows the proposed scheme needs more preprocessing time than previous EB algorithm [10]. Moreover, the block matching time is quite less than previous EB algorithm. Therefore, the total computation time in the proposed scheme is around 5% less than previous studies.

Table 2. Computation time comparison between the proposed scheme and Lynch et al.' work [10].

		EB algorithm [10]	proposed algorithm	performance improved
pre-processing	image segmentation time	16.9255	20.1043	118.78%
	clustering	93.4247	89.4476	95.74%
	overlapped blocks elimination	68.0844	167.4650	245.97%
block matching		425.2584	248.9053	58.53%
total time		603.693	527.9222	87.12%

Above experimental results show that the proposed scheme improves previous scheme both in detection rate and computation time. Thus, these experimental results reveal the significance of the proposed scheme.

V. CONCLUSIONS

This paper detects the copy-move forgery areas in an image from two perspectives of block mean and block variance. The proposed scheme improves previous cluster-based scheme both in detection rate and computation time. Experimental results show that the proposed scheme retains better performance than previous scheme. More techniques can be applied to reduce total computation time.

REFERENCES

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

[2] H. Farid, "A survey of image forgery detection," IEEE Signal Processing Magazine, vol. 2, no. 6, pp. 16-25, 2009.

[3] 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.

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

[5] S. Bravo-Solorio and A. K. Nandi, "Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics," *Signal Process.*, vol. 91, no. 8, pp. 1759-1770, 2011.

[6] 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.

[7] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy–move attack detection and transformation recovery," *IEEE Trans. on Information Forensics and Security*, vol. 6, no. 3, pp. 1099- 1110, 2011.

[8] 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, no. 8, pp. 1355-1370, 2013.

[9] G. Muhammad, M. Hussain, and G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform," *Digital Investigation*, vol. 9, no. 1, pp. 49-57, 2012.

[10] 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. 2539-265, 2013.

[11] J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD," *Forensic Science International*, vol. 233, pp. 158-166, 2013.

[12] J. Li, X.L. Li, B. Yang, and X.M. Sun, "Segmentation-Based Image Copy-Move Forgery Detection Scheme," *IEEE Trans. on Information Forensics and Security*, vol. 10, no. 3, pp. 507-518, 2015.

[13] C.C. Hsu, T.Y. Hung, C.W. Lin, and C.T. Hsu, "Video forgery detection using correlation of noise residue," *in Proc.of IEEE Int.Conf. on multimedia signal processing*, 2007, pp. 170-174.

[14] A. V. Subramanyam and Sabu Emmanuel, "Pixel estimation based video forgery detection," *in Proc.of IEEE Int.Conf.on Acoustics, Speech and Signal Processing*, 2007, pp. 3038- 3042.

[15] S.Y. Liao and T.Q. Huang, "Video copy-move forgery detection and localization based on tamura texture features," *in Proc. of IEEE Int. Conf. on Image and Signal Processing*, 2013, pp. 864-868.