ISSN 2278-3091

Volume 8, No.1.6, 2019

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse1081.62019.pdf

https://doi.org/10.30534/ijatcse/2019/1081.62019

Block-based Approaches for Copy-move Image Forgery Detection :A Review

Rafidah Muhamad[1], Azurah A. Samah[2], Hairudin Abdul Majid[3], Zuraini Ali Shah[4], Haslina Hashim[5], Nik Azmi Nik Mahmood[6], Dewi Nasien[7], M. Hasmil Adiya[8]

[1,2,3,4,5]School of Computing, Faculty of Engineering. Universiti Teknologi Malaysia (UTM), Malaysia

[6]School of Chemical and Energy Engineering, Faculty of Engineering Universiti Teknologi Malaysia (UTM), Malaysia

[7,8]Sekolah Tinggi Ilmu Komputer (STIKOM) Pelita Indonesia, Pekanbaru, Riau, Indonesia

ABSTRACT

Detecting tampered region caused by copy-move forgery has become one of the most prominent and interesting research areas. It is easy to perform with simple copying and pasting desire object and use it to add or delete existing object in an image. This paper discussed a few algorithms for copy-move forgery detection in terms of their advantage, disadvantage, and type of attacks that can be handled. Generally, there are two groups of approaches; active and passive where passive approach does not need prior information of the image, thus making it more popular. These attacks aim to increase the level of difficulty on detecting tampered region. The focus of the review is to evaluate the performance of existing block-based methods under passive approach that able to handle various post-processing attacks.

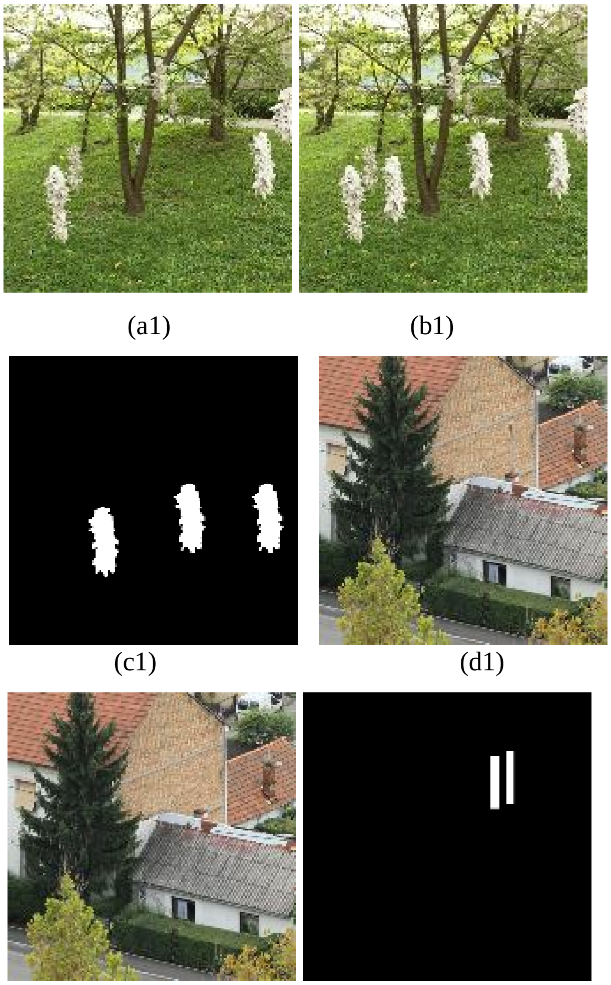
Key words : Passive approach, Block-based, Copy-move, Forgery detection.

1. INTRODUCTION

Primarily, information has been passed using word, but it has been replaced by image where it can convey better information especially in the field of crime, journalism, etc [1-2]. However, the concern is that there is a high potential of vicious tampering where digital images can be changed to hide the truth by using various image editing tools such as Photoshop. In the early-to-mid 20th century, photographers had realized that image forgeries could be powerful tools for changing public perception and even history [3]. In the field of image forgery, copy-move is known as the most actively investigated subtopic of digital image tampering because of the simplicity as it only involves copying and pasting of some objects in the same image [4]. Besides, to make it worse, most of the tampered images does not tamper by solely copy-move, but also being tampered by post-processing attacks and geometric transformation before pasted which make it more challenging [5].

Some early works of image tampering detection did not consider image post-processing after the tampering operations (copy-move forgery, splicing, etc). However, practical tampering often involves post-processing operations to smooth the boundaries of tampered regions, in order to make the final artifact less visually suspectable [6]. There are two kinds of post-processing operations. One is active post-processing for improving the tampering effect, e.g., image blurring, brightness change and contrast adjustments. The other one is passive post-processing that may be unintentionally introduced to tampered images during data transmission, e.g., JPEG compression, noise adding, and colour reduction [7]. Nowadays, the term image tampering implies all the tampering processes with or without post-processing. These post-processing operations increase the difficulty of exposing such forgery.

Figure 1 shows two examples of copy-move image forgery without any post-processing attacks. Shown in the left column are two original images and in the middle are their counterpart tampered images while the right column shows the ground truth of the images. The top middle panel shows an undesirable background is concealed by a region belonging to foreground while the bottom middle panel shows a duplicated region belonging to the foreground is used to create another foreground that contains large identical textured regions. These duplicated regions are well-blended into the surroundings at the target locations and become very difficult to detect visually. Figure 2 shows the images in Figure 1 that have been tampered with post-processing attacks; blurring. According to [8], many times, an intelligent adversary intentionally blurs a region of an image or the whole image while duplicating it, specifically its edges, so as to ensure that it does not stand out or seem out of place due to the abrupt variations along the edges. This makes the image imperceptible to human eyes, as well as helps to avoid detection of the forgery by conventional copy-move forgery detection algorithms such as [9]. Therefore, to detect such forgeries reliably and be robust to some of the post-processing operations, a number of approaches have been carried out.



(a1) (b1)

(c1) (d1)

(e1) (f1)

Figure 1: Original images (a1&d1), forged images (b1&e1) and their ground truth (c1&f1) without post-processing attack [7]

2. DIGITAL IMAGE FORGERY DETECTION APPROACHES

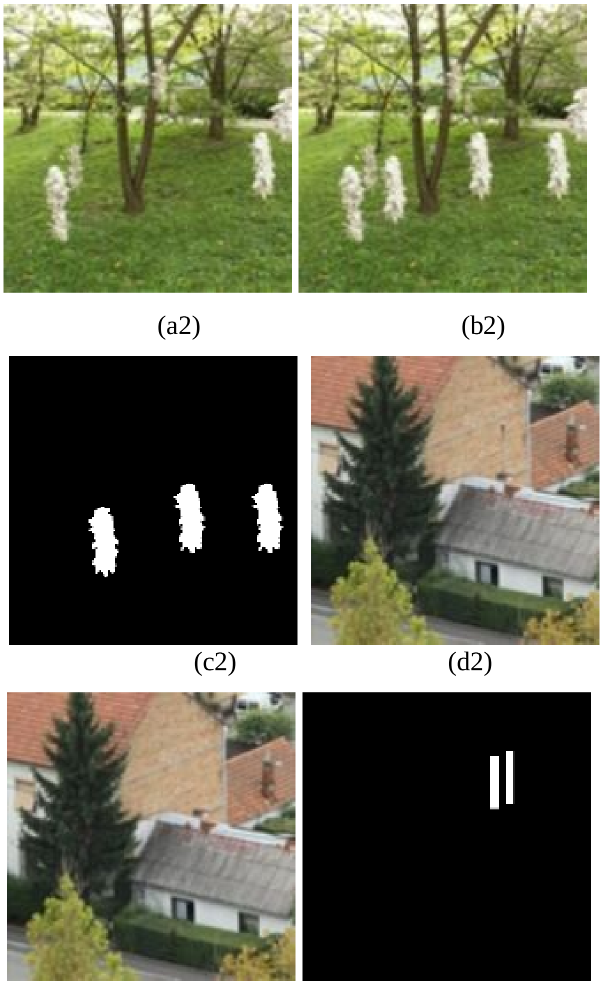
Two categories of image forgery detection techniques are active and passive approaches. Active approaches are also known as intrusive approaches [10]. Active detection approaches require post-processing manipulations of the image after being captured. The examples of this approach are digital signature and digital watermark [11].

The advantage of this method is less computational complexity and simple to apply [12]. Unfortunately, the drawbacks are more than benefits which need the signature or watermark to be inserted using special equipment which known to be expensive [13]. Besides, millions of images which are already on the internet cannot benefit from these approaches [14].

On the other hand, passive approaches or non-intrusive approaches does not require prior presence of digital signature or watermark to attest the image [14]. Passive approaches are also called blind image forgery technique [13]. These approaches take into account, the correlation of the image for forgery detection. Hence, they come out to be the most useful approach for those images that are already on the web.

3. BLOCK-BASED METHOD

In block-based methods, image is divided in blocks of fixed dimensions and further features are extracted corresponding to each block of image. Features are extracted from each block using several methods such as moment-based, dimensionality reduction-based, frequency transform-based, intensity-based, and texture-based.



(a2) (b2)

(c2) (d2)

(e2) (f2)

Figure 2: Original images (a2&d2), forged images (b2&e2) and their ground truth (c2&f2) with post-processing attack (blurring) [7]

3.1. Moment-based Method

The moment-based was initially employed in copy-move by [15] using blur invariant moment. This method is resilient to blur degradation, additive noise and arbitrary contrast changes as the method is represented using the function of central moments. However, the issue arises when large image is used. This is because large image means high computational complexity since the there is a high number of features to be extracted. Fortunately, a combination of blur moment and DWT [16] able to reduce it. Alternatively, according to [17], the implementation of mixed moments, which is a combination of exponential moments and histogram-invariant moment can help in not only detecting forgery when there is post-processing attack such as brightness adjustment and contrast change but also giving a good result when facing geometric transformations; scaling and rotation. Besides, it shows that aside from a good detection result, the method also happens to have low processing time. The advantages of exponent moments encourage Wang et al. [18] to propose a new method that used invariant quaternion exponent moments (QEMs). This method used the original tampered color image for feature extraction and shows that it is invariance under various conditions such as noise, JPEG compression and geometric transformations. However, it hardly can be used for real-time application cause the method had high computational complexity. Table 1 shows the summary of moment-based methods for CMFD.

3.2. Dimensionality Reduction-based Method

Dimension reduction techniques are commonly used with domain features to reduce the dimensionality of the image and lowering the complexity. Among these techniques are Principal Component Analysis (PCA), and Singular Value Decomposition (SVD). As the problem in detecting copy-move forgery becomes more complex and advanced, researchers had improved the original PCA [9] by hybridizing it with other method such as DCT and SIFT. Sunil et al. [19] proposed DCT-PCA to overcome the problem of brightness changes in copy-move region. The generated feature vector is invariant to the changes of intensity by down sampling the low frequency of DCT coefficients. Alternatively, the algorithm proposed by [20] has lower computational complexity as well as invariance to geometric transformations. This is the result of combining PCA with SIFT. However, these methods are limited to certain attacks and the usage of key points method decrease the performance when homogeneous regions are present.

Table 1: Summary of Moment-based Methods for CMFD

Reference	**Moment-based methods**	**Performance**	**Limitation**
[13]	Blur Moment	Invariance to blur degradation, additive noise and arbitrary contrast changes	High calculation time of the procedure.
[14]	BLUR Moment and DWT	High ability of detecting copy move forgery in the presence of noise, blur or contrast changes	Limited to images with post-processing attacks only
[15]	Mixed Moment	Insensitive to translation, scaling, rotation, brightness and contrast change	Limited to big tamper region.
[16]	QEMs	Able to detect duplicated object in scaling, rotation, noise and compression conditions	High computational complexity

3.3. Frequency Transform-based Method

To overcome the limitation of dimensionality reduction-based methods, [21], [22] as well as [23] had use the advantage of SVD and combined it with methods based on frequency-transform such as DCT, DWT and 2D-DWT respectively, for better detection and localization of duplicated region. SVD is generally stable and robust to various operations particularly Gaussian blurring, noise, JPEG compression and their mixed operations [24] as well as achieves rotation invariance for both algebraic and geometric properties. Contrary, [8] replace DWT with Stationary Wavelet Transform (SWT) as it is shift invariant and able to find the edges of forged region even in blurring condition. Table 2 shows the summary of dimensionality reduction and frequency transform-based methods for CMFD.

Table 2: Summary of Dimensionality Reduction and Frequency Transform-based Methods for CMFD

Reference	**Dimensionality reduction and frequency transform-based methods**	**Performance**	**Limitation**
[19]	DCT-PCA	Insensitive to image with changes in intensity	Limited to large size of duplicated region
[20]	Improved PCA-SIFT	Capable to detect copy-move with geometric transformations	Low accuracy for noise and blurring conditions
[21]	DCT and SVD	Capable of detecting and localizing multiple copy-move for image under Gaussian blurring, AWGN, JPEG compression and their mixed operations	Limited to image distorted by post-processing attacks
[22]	DWT and SVD	Can effectively detect multiple copy-move forgery and precisely locate the duplicated regions, even when an image was distorted by Gaussian blurring, JPEG compression and their mixed operations	Limited to non-overlapping duplicated region
[23]	2D-DWT and SVD	Fast, efficient and accurate identification and localization of duplicated object with gaussian blurring, noise, JPEG compression, rotation invariance	Use varies threshold for different types of image
[24]	SVD	Can detect copy-move forgery when the post-processing operations like rotation, scaling, JPEG compression are applied.	Longer time for detection of images with larger size of block
[8]	SWT-SVD	Shift invariant and robust to noise and blurring.	Low accuracy for small size of duplicated region

3.4 Intensity and Texture-based Method

For intensity and texture-based approaches, since being introduced by [25], feature extraction using image intensity has been widely used. Their method searched for blocks with similar intensity patterns based on a kd-tree and this method results in invariancies against JPEG compression.

Zimba and Xingming [26] proposed a method that calculate the average intensity of sub-blocks, enable it to detect duplicated object in an image concealed with JPEG compression and noise. Davarzani et al. [26] 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. Zheng et al. [28] proposed an algorithm based on Local Binary Pattern (LBP) to extract image features using the statistical analysis of pixels of small overlapped blocks of an image, then they compared the similarity of these blocks where the features are directly extracted from each overlapping block. This method is robust to noise, blurring and rotation attacks. In 2016, [29] introduced a method where the features were extracted by calculating the average value of the intensity of each block. This method is not only resilient against image compression but also rotation. Table 3 shows the summary of intensity and texture-based methods for CMFD.

Table 3: Summary of Intensity and Texture-based Methods for CMFD

Reference	Intensity and texture-based methods	Performance	Limitation
[23]	Intensity calculation based on k-d tree	Robust to JPEG compression	By using smaller block sizes allows more details in the duplicated regions to appear, but the algorithm is sensitive to mismatches due to the smaller area of comparison.
[24]	Calculation of the average intensity of sub-blocks	Capable to detect duplicated object in JPEG compression and noise condition	Limited to certain post-processing attacks
[25]	MLBP	Robust to noise, blurring and rotation attacks	Time consuming for forgery detection in high resolution images and cannot detect duplicated regions with arbitrary rotation angles.
[26]	LBP	Robust to noise, blurring and rotation attacks	Limited to non-regular regions of duplication
[27]	Calculation of the average value of the intensity of each block	Invariance to image compression and rotation	Limited to image with small area of homogeneous region

4. CONCLUSION

As the development of technologies have been advance over the years, many approaches have been developed for copy-move image forgery detection and reveals the tampered region whether the image had been attacked by post-processing operations or not. Although there are some differences between all the approaches being developed but mainly all of them share the same principal which is to develop better method that can cope with the post-processing attacks and at the same time providing better algorithm with low complexity.

Other issue is that, beside post-processing attacks, there are also geometric transformations such as rotation and scaling that had been employed by forgers nowadays to increase the challenge of forgery detection. Even though there were studies that address these problems however, there are cases that the parameters of rotation and scaling had been altered severely causing the methods to not able to detect the region of tampering accurately [30]. The suggestion to address this problem might be to use feature extraction method with circular block instead of using square block.

ACKNOWLEDGEMENTS

The authors would like to express gratitude to the reviewers and editors for helpful suggestions, School of Computing, Faculty of Engineering and Universiti Teknologi Malaysia for sponsoring this research by the GUP Research Grant (Grant Number: Q.J130000.2528.19H17).

REFERENCES

1. Kuchuk, Heorhii, et al. “Adaptive Compression Method for Video Information.” International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, no. 1, 2019.
2. Saravana Balaji, B., et al. “Semantically Enriched Tag Clustering and Image Feature Based Image Retrieval System.” International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, no. 1, 2019, pp. 138–41.
3. S. A. Thajeel, “Copy-move Image Forgery Detection Scheme Based on New Texture Descriptor Utilising Graphical Processing Unit,” 2016.
4. C. S. Prakash, S. Maheshkar, V. Maheshkar, “Detection of copy-move image forgery with efficient block representation and discrete cosine transform,” Journal of Intelligent & Fuzzy Systems (Preprint), pp. 1–13, 2018. https://doi.org/10.3233/JIFS-169808
5. S. Sharma, U. Ghanekar, “Dominating direction based an efficient copy–move image tampering detection technique,” The Imaging Science Journal, vol. 66 (4), pp. 254–262, 2018.
6. L. Zheng, Y. Zhang, V. L. Thing, “A survey on image tampering and its detection in real-world photos” Journal of Visual Communication and Image Representation, 58, 380-399, 2019.
7. D. Tralic, I. Zupancic, S. Grgic, M. Grgic, “CoMoFoD - New Database for Copy-Move Forgery Detection,” Proc 55th Int Symp ELMAR-2013, pp. 25–7, 2013.
8. R. Dixit, R. Naskar, S. Mishra, “Blur-invariant copy-move forgery detection technique with improved detection accuracy utilising SWT-SVD,” IET Image Processing, vol. 11(5), pp. 301–9, 2017.
9. A. C. Popescu & H. Farid, “Exposing digital forgeries by detecting duplicated image regions,” Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, pp. 1-11, 2004.

10. G. K. Saini, M. Mahajan, “Study of Copy Move Image Forgery Detection Based On Surf Algorithm,”vol. 4, pp. 46–9, 2016.
11. R. C. Pandey, S. K. Singh, K. K. Shukla, “Passive forensics in image and video using noise features: A review,” Digit Investig, vol. 19 (2016), pp. 1–28, 2016.
12. R. Singh, M. Kaur, “Copy move tampering detection techniques: A review,” Int J Appl Eng Res., vol. 11(5), pp. 3610–5, 2016.
13. A. Dixit, R. K. Gupta, “Copy-Move Image Forgery Detection a Review,” Int J Image, Graph Signal Process, vol. 8(6), pp. 29–40, 2016.
14. S. Kaur, N. Julka, “International Journal of Advance Engineering and Research A 2D-DWT Based Enhanced Technique of Copy Move Forgery Detection,” pp. 119–23, 2016.
15. B. Mahdian, S. Saic, “Detection of copy-move forgery using a method based on blur moment invariants,” Forensic Sci Int., vol. 171(2–3), pp. 180–9, 2007.
16. A. Kashyap, S. D. Joshi, “Detection of copy-move forgery using wavelet decomposition,” 2013 Int Conf Signal Process Commun ICSC, pp. 396–400, 2013. https://doi.org/10.1109/ICSPCom.2013.6719820
17. Z. Le, W. Xu, “A robust image copy-move forgery detection based on mixed moments,” Proc IEEE Int Conf Softw Eng Serv Sci ICSESS, pp. 381–4, 2013.
18. X. Y. Wang, Y. N. Liu, H. Xu, P. Wang, H. Y. Yang, “Robust copy–move forgery detection using quaternion exponent moments,” Pattern Analysis and Applications, vol. 21(2), pp. 451-467, 2018.
19. K. Sunil, D. Jagan, M. Shaktidev, “DCT-PCA Based Method for Copy-Move Forgery Detection,” In: ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of CSI, vol. 2, pp. 577–83, 2014.
20. K. Li, H. Li, B. Yang, Q. Meng, S. Luo, “Detection of Image Forgery Based on Improved PCA-SIFT,” In: Computer Engineering and Networking, Lecture Notes in Electrical Engineering vol. 277, pp. 679–86, 2014.
21. J. Zhao, J. Guo, “Passive forensics for copy-move image forgery using a method based on DCT and SVD,” Forensic Sci Int., vol. 233(1), pp. 158–66, 2013.
22. F. Liu & H. Feng, “An efficient algorithm for image copy-move forgery detection based on DWT and SVD,” Int J Secur its Appl., vol. 8(5), pp. 377–90, 2014.
23. V. K. Sanap & V.M Mane, “Region duplication forgery detection in digital images using 2D-DWT and SVD,” In 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), pp. 599–604, 2015.
24. S. K. Patra & A. D. Bijwe, “Copy-Move Image Forgery Detection using SVD,” pp. 2220–4, 2016.
25. A. Langille & G. Minglun, “An Efficient Match-based Duplication Detection Algorithm,” In The 3rd Canadian Conference on Computer and Robot Vision (CRV’06), 2006.
26. M. Zimba & S. Xingming, “Fast and Robust Image Cloning Detection using Block Characteristics of DWT Coefficients,” JDCTA: International Journal of Digital Content Technology and its Applications, vol. 5(7), pp. 359–67, 2011. https://doi.org/10.4156/jdcta.vol5.issue7.44
27. R. Davarzani, K. Yaghmaie, S. Mozaffari, M. Tapak, “Copy-move forgery detection using multiresolution local binary patterns,” Forensic Sci Int., vol. 231(1–3), pp. 61–72, 2013.
28. N. Zheng, Y. Wang, M. A. Xu, “A LBP-Based Method for Detecting Copy-Move Forgery with Rotation,” In: Lecture Notes in Electrical Engineering (LNEE), pp 261-267, 2013.
29. M. Brajic, T. Eva, J. Raka, “Overlapping Block Based Algorithm for Copy-Move Forgery Detection in Digital Images,” 2016.
30. D. Cozzolino, G. Poggi, L. Verdoliva, “Copy-move forgery detection based on patchmatch,” In 2014 IEEE International Conference on Image Processing (ICIP), pp. 5312-5316, 2014. https://doi.org/10.1109/ICIP.2014.7026075