ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 8, Issue, 6, pp. 17389-17393, June, 2017

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Review Article

COPY-MOVE DIGITAL IMAGE FORGERY DETECTION TECHNIQUES: A REVIEW

Sreenivasu T*[1] and Sudha Vani G[2]

[1]Department of ECE, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India
[2]Department of ECE, R.V.R& J.C College of Engg, Guntur, Andhra Pradesh, India

DOI: http://dx.doi.org/10.24327/ijrsr.2017.0806.0344

ARTICLE INFO

Article History:

Received 06th March, 2017
Received in revised form 14th April, 2017
Accepted 23rd May, 2017
Published online 28th June, 2017

Key Words:

Copy- Move, Forgery, Splicing, Resampling.

ABSTRACT

With the rapid development of multimedia technology and availability of powerful digital media editing tools such as Photoshop, PIXLR etc., it is possible to manipulate (or forge) digital images very easily. For humans, it becomes very difficult to identify visually whether the image is original or manipulated. The detection of image forgery is very important because an image carry's a lot of important information and can be used as legal evidence in medical imaging, image forensics, news media, and the court of law and in many other fields. There are many techniques to manipulate the digital images such as copy-move, image splicing, resampling and soon. Among them, the common form of image forgery is copy move forgery. In this paper reviews of the various copy-move digital image forgery detection techniques are presented.

INTRODUCTION

Now a day's Image forgery has become extremely easy due to the rapid development of multimedia technology, easy availability of many powerful image processing and digital media editing tools such as Photoshop, PIXLR etc. So images, which appear in magazines, social media, political attacks, criminal investigation, can no longer be trusted. To prevent forgery and protect copyrights, techniques for image forgery detection have become more and more important and hence it is necessary to identify the authenticity of images [1, 2].

In literature, several methods have been developed for authenticating an image. Based on whether the original image is available or not, image authentication (detection) methods are classified into two methods: Active authentication and Passive authentication methods [4]. Under each classification, the methods are further subdivided as shown in Figure 1.

Active Methods

With active image forgery detection method, a piece of information, i.e., watermarking or digital signature is inserted in order to protect the target image.

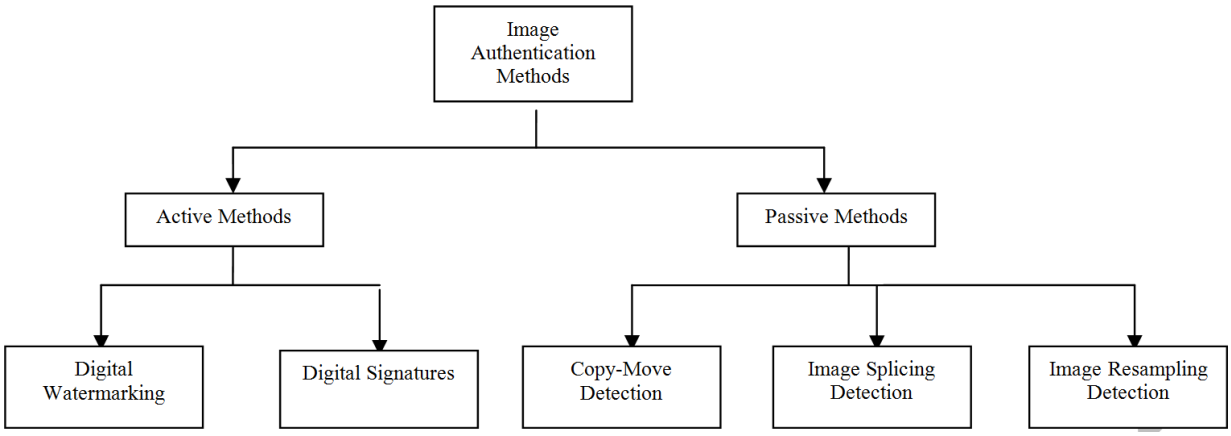


Figure 1 Classification of Image Forgery Detection Methods.

*Corresponding author: **Sreenivasu T**
Department of ECE, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India

This process is done at the time of digitizing. Hence, during the examination, the investigator will determine whether the target image is forged or not by searching for the information embedded, into the target image and looking for anomalies or inconsistencies in the embedded information [3]. These are also known as non-blind methods. However, there are millions of thousands digital images on the internet which are without any digital watermark or signature. In this context, active image forgery detection could not be used to find the authenticity of the image [4].

Passive methods

Unlike the active methods, the passive image forgery detection methods do not require any digital signature or watermark embedded in advance [5]. These methods are also known as blind methods because the presence of the original image is not required to verify the authenticity [6].

Passive methods may further subdivide into copy-move, image splicing, and image resampling methods.

Copy-move image forgery

It is a method in which an object of the same image is copied and pasted (moved) into another region of that image [7] and is shown in Figure 2. In copy-move images, copied regions in the image may be post-processed, rotated/flipped and scaled before pasting to other places to hide or remove any details [8].

Image splicing

It is a method in which a forged image is produced by copying and pasting a region from one or more images into another image [9] and is shown in Figure 3.

Image resampling

It is a method which deals with a producing forged image by using geometric transformations like rotation, scaling, stretching, skewing, flipping etc., on some portion of the image.

In Figure 4, the image on the left is the original image while the one on the right is the forged image obtained by rotation and scaling it.

Among the passive methods, the copy-move forgery is more common because of its simplicity. Now an overview of existing techniques used for detection of copy move image forgery is explained in the next section.

Copy-Move Image Forgery Detection Techniques

In the past ten years a lot of research has been going on the detection of copy -move image forgery. Copy-move forgery detection methods are categorized into either block-based methods or keypoint based methods [20].The General steps in detection of copy move image forgery as shown in Figure 5

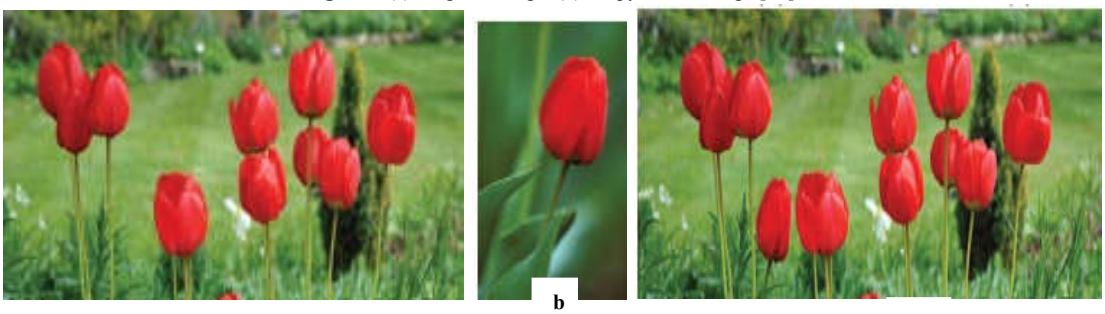
In the initial stage for both the methods, it is required to pre-process the given digital image. Most of the methods perform pre-processing on gray- scale images. The digital image is subdivided into smaller blocks in block-based methods at feature extraction block. A feature vector is calculated for every such block. Similar feature vectors of every block are subsequently matched.

In keypoint based methods without any image subdivision, compute the features only on image regions with high entropy. Now similar features of the image are matched. If the regions of such matches cluster into larger areas, then forgery are detected. In both methods, further post filtering operation is included for removing false matches [14].

J.Fridrich, D. Soukal *et al*. [11], proposed a method for detecting copy-move image forgery using Discrete Cosine Transform (DCT). In this method, the image is divided into overlapping blocks of size 16 x16, and DCT coefficients are calculated for feature extraction of these blocks. After that, the DCT coefficients of blocks are lexicographically sorted. Now after completion of lexicographical sorting, comparable squares are distinguished and forged regions are identified. In this method, it is hard to detect sophisticated manipulations.

a b

Figure 2 (a) Original Image, (b). Copy-Move Image [11]



a b c

Figure 3 (a),(b). Original Images, (c). Spliced Image [8]

a b

Figure 4 (a). Original Images, (b). Resampled (rotation) image [19]

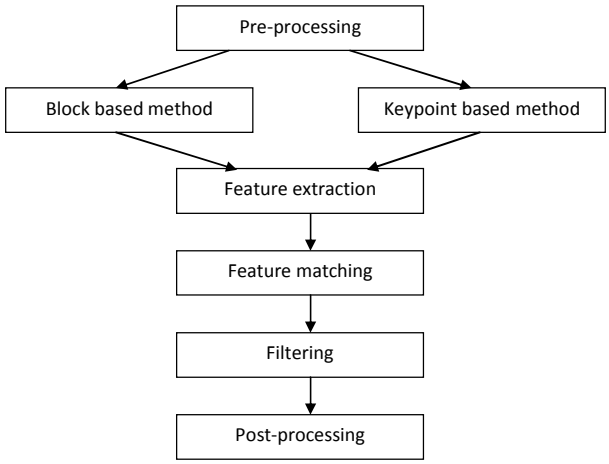


Figure 5 General framework for copy-move forgery detection

A.C Popescu and H. Farid [10], described a method for identifying duplicate image regions using principal component analysis (PCA). In this method, PCA is applied to a fixed-size image of block size (16x16, 32x32), then calculated the eigenvalues and eigenvectors of each block. The duplicate regions are automatically detected by using lexicographical sorting. This algorithm is an efficient and robust technique for image forgery detection even if the image is compressed or noisy. Also, the accuracy of this method is good except for small block size and low JPEG qualities.

Xunyu and Siwei [12], proposed a new technique for region duplication detection that is robust to distortions of the duplicated regions. This method first estimating the transform between matched scale invariant feature transform (SIFT) keypoints, which are insensitive to geometrical and illumination distortions, and then finds all pixels within the duplicated regions after discounting the estimated transforms. The algorithm results in average detection accuracy of 99.08% but the method has one limitation i.e, duplication in the smaller region is hard to detect because key points available are very few numbers.

Cheng-Shian Lin *et al*. [13], described a method for detection of region duplication forgery. In this method first the image is divided into overlapping blocks, and then the two different features, mean and variance, of each block are extracted and formed to feature clusters. Next block comparison scheme used to verify tamper block. Because of extracting the two features from each block, this method reduces comparison load efficiently and hence it becomes more efficient for detecting region duplication forgery.

Yanjun Cao *et al*. [14], proposed an efficient and robust approach for perfect detection of forged region in case of uniform background images, non-regular duplicate regions, and high resolution images using a Circle Block with DCT. Also, this method detects multiple copies–move forgery. However, the main drawback of this method is that it is not robust to geometrical operations.

Seung-Jin Ryu, Min-Jeong Lee *et al*. [15], proposed a detection method of copy-move forgery that localizes duplicated regions using Zernike moments. This method also works on intentional distortions such as additive white Gaussian noise, JPEG compression, and blurring. Also, it can detect forgery even on the rotated region since Zernike moments are algebraically invariant to rotation. However, the disadvantage of this method is that it is still weak against scaling or the other tampering based on Affine transform.

Varsha Karbhari S *et al*. [16], described a new hybrid method using 2D-Discrete Wavelet Transform (2D-DWT) and Singular Value Decomposition (SVD) for accurate detection of forged region in the input image. In this method, each layer of RGB image is extracted and then 2D-DWT is applied on the forged image. It then divides LL sub-band into overlapping blocks. After that apply SVD on each block and sort it into bucket groups to get a dominant feature.

Swapan Debbarma *et al*. [17], proposed a method to detect duplicated and distorted area in an image using keypoints based approach. In this method first input image is converted into gray scale image then keypoints as well as feature vectors are extracted using SIFT or SURF algorithm. The vector dimension is 128 in the case of SIFT and 64 for SURF. Because of using SIFT and SURF algorithms, forged regions are detected accurately and also reduce time complexities. The only drawback of this method is a lack of keypoint detection in smooth or plain areas in the image.

Chi-Man Pun, Xiao-Chen Yuan *et al*. [18], presented a novel copy-move forgery detection using both block-based and keypoint-based forgery detection methods. In this method first adaptive over segmentation algorithm segments the host image into nonoverlapping and irregular blocks adaptively. After that, the feature points are extracted from each block as block features, and the block features are matched with one another to locate the labeled feature points. This procedure could approximately indicate the suspected forgery regions. To detect the forgery regions more accurately, they used forgery region extraction algorithm, which replaces the feature points with small superpixels as feature blocks and then merges the

Table 1 Comparison of Copy-Move Digital Image Forgery Detection Techniques

Reference	Method Used	Merits	Demerits
[11]	DCT	Signal energy concentrate Only on first few coefficients others can be negligible	Will not work on noisy images, the computational cost is high.
[10]	PCA	Reduced feature vector dimension compared to DCT	Low accuracy rate for small sized blocks
[12]	SIFT	Robust to geometrical and illumination distortions.	Hard to detect smaller duplicate regions
[13]	Enhanced Cluster Expanding Block Algorithm	High detection rate and less computation time	Needs more preprocessing time.
[14]	Circle block DCT	Requires fewer features to represent each block	Not robust to geometrical operations
[15]	Zernike Moments	Robust to white Gaussian noise, JPEG compression, blurring, and rotation.	Weak against scaling or the other tampering based on Affine transform.
[16]	DWT + SVD	Accurately locates the forged region from input digital image.	Selection of different threshold values for different images becomes very difficult.
[17]	Keypoint Approach (SIFT+SURF)	Regions are detected accurately and also reduce time complexities.	Lack of keypoint detection in smooth or plain areas in the image.
[18]	Adaptive Oversegmentation and Feature Point Matching.	Robust on various challenging conditions, such as geometric transforms, JPEG compression, and down-sampling.	--------

neighboring blocks that have similar local color features into the feature blocks to generate the merged regions. Next morphological operations are applied to the merged regions to generate the detected forgery regions. This method has Robust on various challenging conditions, such as geometric transforms, JPEG compression, and down-sampling.

CONCLUSION

Copy- move forgery is one of the most commonly used forgery type by end users with different intentions. In this paper, various existing techniques for automatic detection of copy-move forgeries on digital images are discussed. Even though there are many existing algorithms, each of them still has limitations. Increasing the detections rates, reducing the false matches and complexity, researching for faster algorithms have to be done for efficient and accurate detection of image forgeries.

References

1. Yang Ta Kao, Hwei Jen Lin, Chun Wei Wang, and Yi Chun Pai, "Effective Detection for Linear Up-Sampling by a Factor of Fraction," IEEE Transactions On Image Processing, Vol. 21, No. 8, August 2012,pp.3443-3453.
2. Huayong Ge, Hafiz Malik, "Exposing Image Forgery Using Inconsistent Reflection Vanishing Point," IEEE International Conference on Audio, Language and Image Processing (*ICALIP*), 2014, pp.282-286.
3. Songpon Teerakanok and Uehara Tetsutaro, "Enhancement of Image Tampering Detection using JPEG's Quantization and Re-Interpolation Processes," IEEE 39th Annual International Computers, Software & Applications Conference, 2015, pp.35-39.
4. Mariam Saleem, M, Qasim Altaf, Qaiser Chaudry, "A Comparative Analysis on Pixel-Based Blind Cloning Techniques," IEEE International Conference on Control System, Computing and Engineering, November 2014, pp.130-135.
5. Ali Ebrahimi, Subariah Ibrahim, Eghbal Ghazizadeh and Mojtaba Alizadeh, "Paint-Doctored JPEG Image Forensics Based on Blocking Artifacts," IEEE International Conference and Workshop on Computing and Communication (IEMCON), 2015, pp.1-5.
6. Ms. Jayshri Charpe and Ms. Antara Bhattacharya, "Revealing Image Forgery through Image Manipulation Detection," IEEE Proceedings of 2015 Global Conference on Communication Technologies (GCCT 2015), 2015, pp.722-727.
7. Meenakshi Sundaram A and C. Nandini, "CBFD: Coherence Based Forgery Detection Technique in Image Forensics Analysis," IEEE International Conference on Emerging Research in Electronics, Computer Science and Technology-2015, pp.192-197.
8. Tu K.Huynh, Thuong Le-Tien, Khoa V.Huynh and Sy C.Nguyen, "A Survey on Image Forgery Detection Techniques," IEEE International Conference on Computing & Communication Technologies Research, Innovation, and Vision for Future (RIVF), 2015, pp.71-76.
9. Toqeer Mahmood and Tabassam Nawaz, "A Survey on Block Based Copy Move Image Forgery Detection Techniques," IEEE International Conference on Emerging Technologies (ICET), 2015, pp.1-6.
10. Alin C. Popescu and Hany Farid, "Exposing Digital Forgeries by Detecting Traces of Resampling," IEEE Transactions On Signal Processing, Vol. 53, NO. 2, February 2005, pp.758-767.
11. A. J. Fridrich, B. D. Soukal, And A. J. Lukas, "Detection of Copy-Move Forgery In Digital Images," Proceedings of The Digital Forensic Research Workshop, pp.5-8, Aug. 2003.
12. Xunyu Pan and Siwei Lyu, "Region duplication detection using image feature matching,"IEEE Transactions On Information Forensics And Security, Vol. 5, No. 4, December 2010, pp:857-867.
13. Cheng-Shian Lin, Chien-Chang Chen and Yi-Cheng Chang, " An Efficiency Enhanced Cluster Expanding Block Algorithm for Copy-Move Forgery Detection," International Conference on Intelligent Networking and Collaborative Systems,2015,pp.228-231.
14. Yanjun Cao, Tiegang Gao, Li Fan and Qunting Yang, "A robust detection algorithm for copy-move forgery in digital images", Forensic Science International 214 (2012), pp.33-43.
15. S Seung-Jin Ryu, Min-Jeong Lee, and Heung-Kyu Lee, "Detection of copy-rotate-move forgery using Zernike

moments," in Proc. Int. Workshop Information Hiding, Springer, 2010, pp. 51-65.
16. Varsha Karbhari S and Vanita Manikrao M, "Region Duplication Forgery Detection in Digital Images Using 2D-DWT and SVD," IEEE International Conference on Applied and Theoretical Computing and Communication Technology (ICATCCT), 2015, pp.599-604.
17. S Debbarma, A Buboo Singh and Kh.Manglem Singh, "Keypoints Based Copy-Move Forgery Detection of Digital Images," IEEE International Conference on Informatics, Electronics & Vision (ICIEV), May 2014.
18. Chi-Man Pun, Xiao-Chen Yuan and Xiu-Li Bi" Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching" IEEE Transactions on Information Forensics and Security, Vol. 10, No.8, August 2015, PP. 1705-1716
19. K. Sudhakar, Sandeep V.M and Subhash Kulkarni, " Shape Based Copy- Move Forgery Detection Using Level Set Approach," IEEE Fifth International Conference on Signals and Image Processing, 2014, pp.213-214.
20. Abdullah M. Moussa, "A Fast and Accurate Algorithm for Copy-Move Forgery Detection," IEEE Tenth International Conference on Computer Engineering & Systems, 2015, pp.281-285.

How to cite this article:

Sreenivasu T and Sudha Vani G.2017, Copy-Move Digital Image Forgery Detection Techniques: A Review. *Int J Recent Sci Res.* 8(6), pp. 17389-17393. DOI: http://dx.doi.org/10.24327/ijrsr.2017.0806.0344

****