RESEARCHERID
THOMSON REUTERS

[Uma, 6(1): January 2019] ISSN 2348 – 8034
DOI- 10.5281/zenodo.2537823 Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

A DETAILED REVIEW OF COPY-MOVE FORGERY DETECTION IN DIGITAL IMAGE

S. Uma[*1] & Dr. P. D. Sathya[2]

[*1]Research Scholar, Department of Electronics and Communication Engineering, Annamalai University
[2]Assistant Professor, Department of Electronics and Communication Engineering, Annamalai University

ABSTRACT

Today it became very hard to trust the digital photographs; these have to be verified for their originality. Recently a BBC News article says **that *"Eduardo Martins fooled journalists and picture editors by making slight alterations to the images, such as inverting them, just enough to elude software that scans pictures for plagiarism "***. To address these issues, in this article we are going to discuss the image forensic concepts. Two Different techniques are used to create forgery in the digital image: Active and Passive approaches we have focussed image forensics technologies for copy-move forgery which comes under passive approach. Copy-move forgery is formed by copying the area from a particular image and hitting that area on same image to deceive the user. Copy Move forgery detection technique is grouped into two methods: Block based and Key Point based. In this paper, we have discussed the various block based and key point based copy move forgery detection techniques (CMFD).

Keywords: *Digital image, Digital Image Forgery, Copy-move forgery, y, Block-based methods. Key point based.*

I. INTRODUCTION

Digital image forensics is a division of digital forensics which deals with probing the digital photographs for their truth and realism. Images are very vulnerable to modifications. Modifications in the images are carried out by attackers to change or conceal its meaning by using sophisticated image editing software.. Hence, these images need to be authenticated. This can be very important task when images are used as evidence which cause change in judgment like, for example in a court of law and poses threats to the public, government, and businesses.

The fundamental problems digital image forensics techniques attempt to solve is the identification of the source and detecting the integrity of digital images. Identification of source involves determining the means by which the images are created like camera, scanner, and regenerative algorithm. Integrity can be confirmed by analyzing the images for its modification. The detection algorithms for the digital image forensics are classified as **active detection approaches and passive detection approaches** shown in figure (1).

ISSN 2348 – 8034
Impact Factor- 5.070

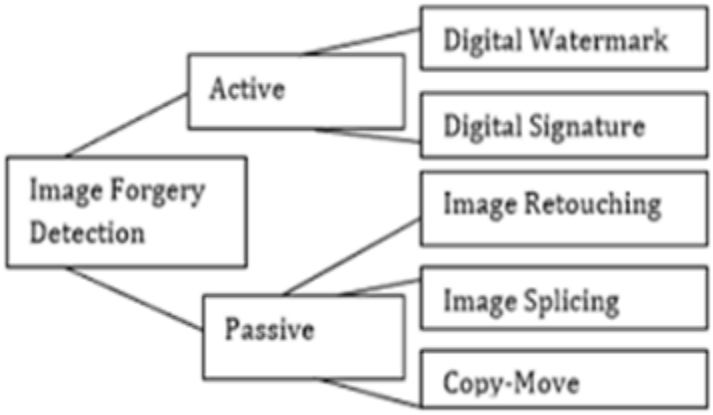

Figure (1) Types of digital image forgery

In active forgery detection, the traces of tampering are directly visible in most cases. In this approach some type of pre-processing such as watermarking, digital signature is done at the time of image creation. Digital watermarking and digital signature are the major protection techniques, Something is embedded into images when they are obtained from the authenticated sources. The active approach involves authenticating images by extracting the watermark and digital signature embedded in it. Special digital cameras are required to embed a digital watermark into an image at the time of their capture. So, any tampering operation done on images can deteriorate the embedded watermark and signature. This detected deterioration in the extracted watermark can help us confirming the authenticity of the images.

In passive blind approach, there will not be any evidence of tampering. In contrast to active approaches, passive methods do not require any prior information about the picture. Passive image forgery detection is a challenging task in image processing. There are many passive image forgery detection techniques which can detect specialized forgery in different manner. Passive detection deals with the raw image analysis based on different statistics of image content to localise tampering of image. The methods and algorithms of detection are highly dependent upon the type of security constraints used. The core assumption for this class of techniques is the assumption that original non-forged content owns some inherent patterns that are always consistent in the un-forged content, but they are very likely to be altered by some tampering processes. Although visually imperceptible, such changes can be detecting by statistical analysis of the content itself, without the need of any appropriate information.

The rest of this paper is organised as follows. In Section 2, we analyse the types of Passive blind approaches. Section 3 describes general workflow of CMFD techniques. Section 4 demonstrated Methods of CMFD techniques and survey

II. TYPES OF PASSIVE BLIND APPROACHES

Passive blind approaches are classified as

2.1. Copy-move: Copy-move is the popular and most common kind of image tampering technique [5]. One part of the image is used to add or remove information. Copying from one part and pasting the same in some other part in the same image with an intention to hide certain content in the original image or duplicating some content that is not actually present in the image. Textured areas in an image like grass, foliage, or fabric with non-regular patterns, are ideal for this purpose due to the blend of the copied areas with the background and it is difficult for the human eye to recognize the forgery. Duplicate image regions can be created using this technique. These regions may or may not

be the forged region or exact duplicate region. Since the copy-paste is within an image, properties of the tampered portion will be same as that of other regions and it is difficult for human eye to detect forgery.

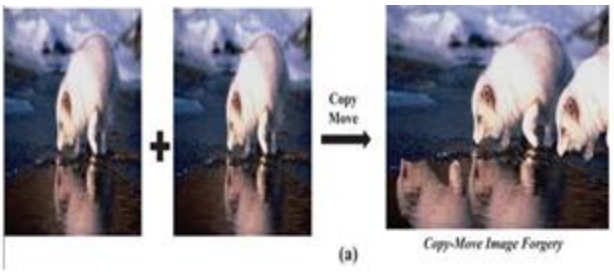

Figure (2.a) an example of copy-move operation

2.2 Image splicing: Image splicing is a commonly used forgery technique in image tampering Replacing one or more portions of a picture with fragments other picture causes the splicing operation. There are many tools available for image tampering like morphing, enhancement, rebroadcast, computer generation etc. Splicing is a form of photographic manipulation in which there is digital splicing of two or more images into a single composite image may not have further post processing such as smoothening of boundaries among different fragments. Splicing can cause inconsistencies in many features like the abnormally sharp transient at the splicing edges and these inconsistencies are used to detect the forgery. Figure (2.b) describes how two images are spliced to form a third one

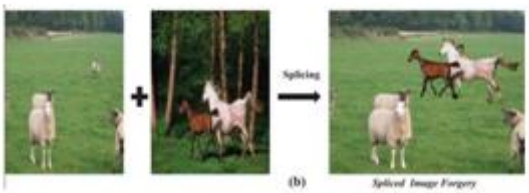

Figure (2.b) an example of Slicing operation.

2.3 Retouching: Modification of the image using any image editing tool to achieve some specific result such asto make fun of others, comes under this category. It is a balancing act and an art. Retouching make the images look as real as possible. No matter which camera is used to take pictures, it is possible to retouch each photo to get rid of any flaws later on. Retouching involves a lot of treatments like basic colour correction, glamor retouching, skin retouching, photo restoration, photo cartooning etc. Image retouching detection is carried out by trying fine enhancement, colour changes and illumination changes in the forged image. The detection is not so difficult if the original image is available however passive detection is a challenging task. This can be treated to be the less harmful/fatal kind of digital image forgery. This method does not alter an image, but instead, enhances (or reduces) feature of an image. (Figure 2.c) shows image retouching, and the difference between left image and right images (enhanced) clearly

Figure (2.c) an example of Retouching-move operation.

III. GENERAL WORKFLOW FOR COPY-MOVE FORGERY DETECTION (CMFD) TECHNIQUES

The general process for detection of copy move forgery based on the feature extraction and matching technique is illustrated in Figure (3).

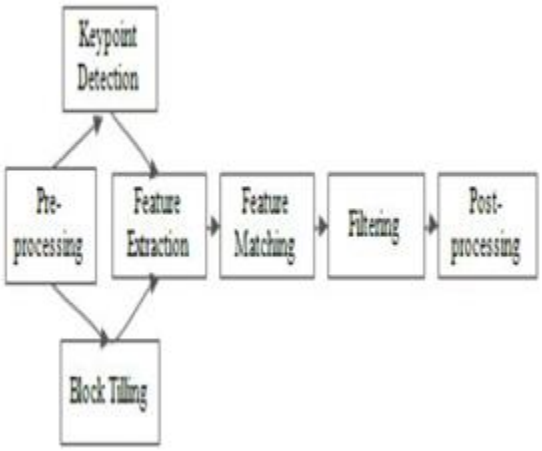

Figure (3) General process for CMFD techniques

Passive copy move forgery detection technique which uses feature matching technique to locate similar regions in the image can be classified into two main categories: block-based and key point-based methods. In both approaches the pre-processing of the images is done such as conversion of image into grey scale, etc. In next step features are extracted by either using block based approach or key point based method. Then the different approaches like clustering and Euclidean distance etc is used for feature matching and a forgery shall be reported if matching features are found. In order to remove spurious matches, filtering is applied. Finally the post-processing is used to analyse filtered result for forgery detection.

IV. METHODS OF CMFD TECHNIQUES

CMFD can be broadly classified into two main categories: block based and key point based approaches.
Figure (4) shows the methods for copy move forgery detection techniques in detail

ISSN 2348 – 8034
Impact Factor- 5.070

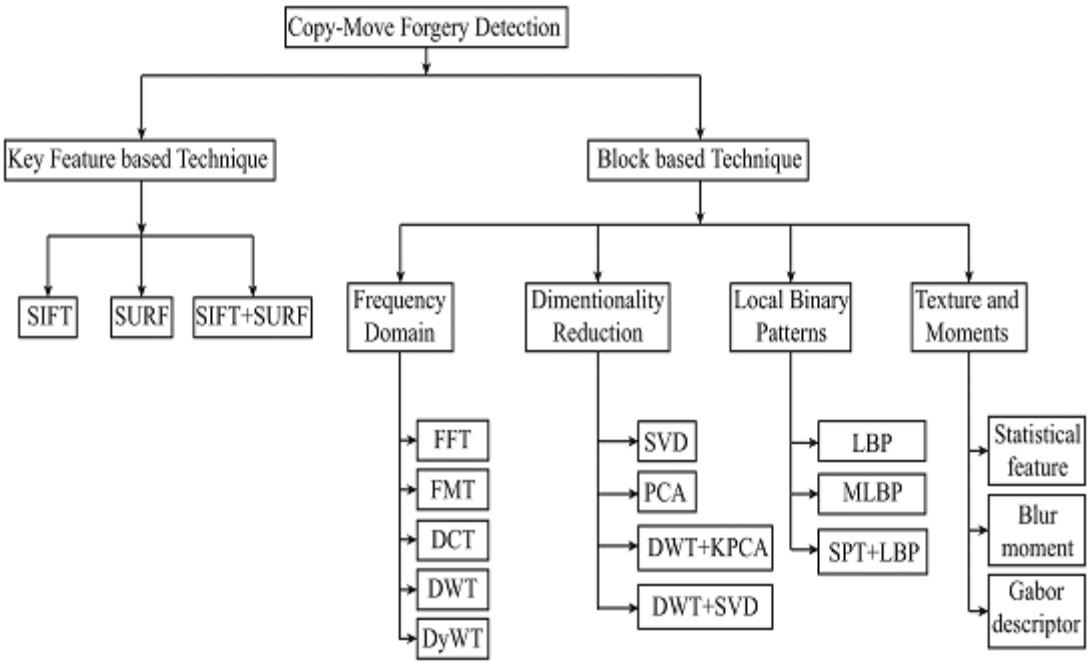

Figure (4) methods for copy move forgery detection techniques

4.1 Block based Methods

The block based methods subdivide the image into overlapping or non-overlapping blocks such as rectangular, circular *etc*. for feature extraction. The block based methods work as following steps [4]:
Step 1: Convert the image into grey scale image
Step 2: For overlapping blocks division, consider an image of size $M \times N$ pixels and size of the block $b \times b$, the block slide over the whole image by one pixel each time from left to right and top to bottom. The total number of overlapping blocks for the image is $\{(M - b + 1) \times (N - b + 1)\}$.
Step 3: Robust feature(s) extraction from each block is done.
Step 4: Finally, the extracted feature(s) are sorted or arranged using appropriate data structures to make a forgery decision based on the similarity of adjacent feature pairs.
In block-based CMFD, different matching techniques are explored by researchers such as lexicographical sorting, k-d tree, radix sort, hash value, Euclidean distance etc.

Some existing block based image forgery detection techniques:
Alaa Hilal, Taghreed Hamzeh, **[7] p**roposed the combination of principal component analysis and discrete cosine transform in order to identify copy-move image forgeries. The first principal component of the image is considered and divided into non-overlapping blocks. 2D DCT is then applied over each block and autocorrelation is used to detect similar blocks. The system is implemented and compared to a reference method over a database of forged images. System's parameters are optimized to the database. The false accept rate has been decreased

Anil Dada Warbhe, R. V. Dharaskar, , V. M. Thakare [6] presented the NCC alone can perform well in detecting the tampering in images, even after transformation such as scaling. The image is first divided into the *NOB*. Step size *Sh (Horizontal step size)* and *Sv (vertical step size)*decides the degree of block overlapping. To achieve efficiency and precision in the tampering detection, we have developed a 3-stage algorithm. The first stage is to detect the percentage of scaling. Once the scaling feature is noticed successfully, the Coarse Scale Tampering detection (CSTD) is done and the output of the second phase is i.e. CSTD is used to Fine-tune Scale Tampering detection (FSTD). This method does not need dimensionality reduction and any sorting scheme to sort feature

vectors and hence becomes computationally efficient as compared to some of the other block-based approaches in the literature.

Sunil Kumar et.al [33] suggests a way using PCA on DCT. Firstly DCT is practiced to compute DCT coefficient for feature removal and PCA to capitulate a abridged dimension representation respectively. Features, invariant to limited change of intensity are formed by means of down sampling of low frequency DCT coefficients. The way is strong against manipulation techniques like additional noise and JPEG compression and also concentrate invariance to illumination, but it is fails in case of contrast variations. To overcome this limitation (contrast variations), same author [33] proposed a method based on binary DCT coefficients. In this method, input image is divided overlapping blocks and DCT is applied to blocks to calculate DCT coefficients. Later than those binary DCT characteristics are extracted by sign of the DCT coefficients. Coefficient of correlation is used to match resulting binary vectors. This approach is strong in opposition to various manipulation techniques such as Gaussian noise addition, compression and minor rotation and scaling.

Zhong and Xu [24] presented a method that was based on mixed moments. First, to extraction of the information that has low-frequency from the image Gaussian pyramid transform used then the artefact is divided into overlapping blocks; Secondly it is lexicographically sorted the block eigenvector using by the moments such as exponential Fourier and histogram. Thirdly, tampered region was positioned precisely and quickly based to their Euclidean distance and space distance. In shortly Experimental results depicts successfully can detect the forged part of image that is translated, rotated, scaled and mixed operation tamper when the image is changed by brightness variation and contrast adjustment. But the qualitative evaluation, rotation angle and scaling factor are not specified.

Junliu zhond, Yenfen gan, [36].
Presented an improved block-based efficient method for CMFD. First, after pre-processing, an secondary overlapped circular block is offered to divide the forged image into overlapped circular blocks. The local plus inner image trait is removed by the DRHFMs with the overlapped circular block from the doubtful image. Then, the similar feature vectors of blocks are searched by 2 Nearest Neighbours (2NN) test. Euclidean distance and correlation coefficient is employed to filter these features and then remove the false matches. Morphologic operation is employed to delete the isolated pixels. Sequences of experiments are made to examine the performance for CMFD. Experimental results show that the new DRHFMs can obtain outstanding performance even under image geometrical distortions

Table 1 .Comparative study on Block Based Copy Move Forgery Detection techniques.

S.No	Paper	Year	Techniques	Matching Procedure	Performance
1	20	2016	LBP	Euclidean distance measure and similarity threshold	this method is robust against rotation and flipping but unable to detect forgery if regions are rotated at random angles
2	21	2016	log-polar Fourier	Euclidean distance	robust against rotation, scaling and processing time is more than the key point-based method
3	22	2017	Fast Fourier Transform + SVD + PCA	cascade filtering with city block, horizontal, vertical and frequency filters	the method is threshold free and robust against noise, blurring and JPEG compression
4	23	2016	PCT; Spectral hashing; PCA	Sorting; Hamming distance; Euclidean Distance	the method is threshold free and robust against noise, blurring and JPEG compression

ISSN 2348 – 8034
Impact Factor- 5.070

5	24	2017	DRPCET	Sorting; Person correlation coefficient	robust against rotation, flipping ,scaling resizing and compression
6	14	2016	DCT and LBP	Euclidean distance and used SVM Classifiers	. robust against rotation and scaling and also result is consistent
7	13	2016	Auto Color Correlogram (ACC) DCT and PCA	Manhattan distance measure	robust to transformations, such as scaling, translation and rotation. it is effective in detecting multiple copy-move forgeries in same image.
8	11		DCT	Patch level matching	Detection, especially for difficult cases, such as small objects, objects covered by textureless areas and repeated patterns.
9	9	2017	LBP and SVD	Generate shift vectors from similar vectors and sorted lexicographically	has good performance on regular or non-regular copy move forgery operation, good performance on multiple-region copy move forgery and has a higher accuracy even if the image has undergone some post processing operations.
10	41	2016	multi-radius polar complex exponential transform (PCET)	Lexicographic order matching algorithm	large-scale rotation or scaling and is robust against Joint Photographic Experts Group (JPEG) compression, smoothing and noise degrading. performs well in computing time based on the multi-thread and GPU acceleration technology

4.2 Key-point based Methods

Key-point based methods compute the feature vectors for regions with high entropy in an image. The working of key point based methods is given below [4].

Step 1: Convert the image into grey scale image,

Step 2:Local features are extracted such as corners, blobs and edges from the tampered image and each feature is represented by a set of descriptors. The descriptor increases the reliability of the features.

Step 3: Each descriptor is matched with others to find the forged regions in the image.

In key-point-based forgery detection, matching techniques explored by researchers are best bin first, 2-nearest neighbours (2NN), generalised 2NN (g2NN), Broad First Search Neighbors (BFSN), clustering etc

Some existing key point based image forgery detection techniques:

Prinkle Rani and Jyoti Rani[30], implemented the Enhanced SIFT (E-SIFT) algorithm to detect the copy move forgery in the digital images. They used clusters and their mean values to find the forged area within the image to reduce the overall processing time. Proposed system also shows good accuracy in the images that can contain scaled forgery or forgery with geometric transformations. The processing time to detect the forgery in the images is comparatively high.

Navneet Kaur and Nitish Mahajan, [31] proposed an improvement in Principal Component Analysis (PCA)algorithm for forgery detection. In the proposed method the key point features obtained by using SIFT algorithm is given as input to PCA algorithm for classification. The simulation is performed in MATLAB and it is been analysed that accuracy is improved, fault detection rate is reduced

Prajwal Pralhad Panzade [10] analyzed a reliable way to detect copy move attacks on images based on HSV pre-processing, SIFT features and clustering has been proposed. The use of HSV pre-processing in order to reduce the false positives found up to the mark. Clustering increases the accuracy of matching the duplicated patches over simple key point matching. From the given forged image, this method can legitimately detect the cloned regions even if they are processed by geometrical transformations like rotation, translation and scaling or combination of them. Also this method reliably detects forgery caused by multiple cloning of regions. And method is robust and efficient to detect copy-move forgeries in the digital images.

M Reshmi mi et al. [34] proposed combining SURF and Wavelet Transform. The image is first transformed into wavelet domain. SURF is applied on this transformed image for key points detection and feature extraction. The SURF feature descriptor vector is obtained. Because of the multispectral components produced by the wavelet, the features are more predominant. The algorithm finds a match between the descriptor vectors and marks forged regions.

Gargi rathod, Shruti Chodankar [19] : proposea an image forensics algorithm for detecting copy-move forgery based on improved PCA-SIFT. The present method works first by extracting features of an image and then reducing its dimensionality, and the method uses k-nearest neighbour to operate forgery detection. Owing to the similarity between pasted region and copied region, the descriptors are then matched between each other to seek for any possible forgery in images. Extensive experimental results are presented to confirm that the algorithm is able to precisely individuate the tampered image and quantify its robustness and sensitivity to image post-processing and offer a considerable improvement in time efficiency.

Reshma Raja, Niya Joseph [42]:presented a new framework for CMFD. The test image is first segmented into non overlapped patches. The matching between the patches is carried out in two stages of matching. The aim of the first stage is to find the suspicious matches, and a transform matrix between them is roughly estimated. Then in the second stage we confirm the existence of CMF by means of refining the transform matrix

Table 2. Comparative study on Key point Based Copy Move Forgery Detection techniques

S.No	Paper	Year	Techniques	Matching Procedure	Performance
1.	28	2013	MIFT	RANSAC and hysteresis thresholding	Detect forged region with high accuracy and robustness
2	29	2014	SIFT and SURF	Euclidian distance	SIFT and SURF give fast and robust performance with respect to geometrical transformation
3	27	2017	SIFT	agglomerative hierarchical clustering	invariant to mirror transformation and

ISSN 2348 – 8034
Impact Factor- 5.070

					rotation able to detect forgery in the smooth area
4	39	2015	SIFT and SURF	Harris corner points	Robust to Mixture operations (Rotation+ Gaussian blurring, Flipping+ Gaussian blurring, etc.)
5	34	2014	SURF	Use descriptor vector	Detect scaling and rotated object , reduce computational complexity
6	17		SIFT	Local feature matching using Euclidean matching	Has good performance in both authenticity detection and patch localization tasks
7	16	2016	SIFT	Agglomerative hierarchical clustering (AHC)	improves the invariance to mirror transformation and rotation by using an improved descriptor give good performance on, scaling, rotation, flipping, blurring, illumination changes and multiple cloning).
8	15	2017	SIFT and PCA	Matching with Euclidian distance	Superior even if the tampered images are exposed to different post-processing operations.
9	40	2016	Based on angular radial partitioning	Harris key point matching	can detect duplicated and multiple regions effectively, and with high accuracy, in the presence of several geometric transformation operations including (rotation and scaling), image degradations including JPEG compression and Additive White Gaussian Noise
10	5	2017	SIFT	Matching with Euclidian distance	Better detection than other existing methods.

V. CONCLUSION

Passive forensics technology of digital image is one of the rapidly growing fields of research. Our brief review of image forgery technologies indicates that the research is still in the phase of vigorous development and has a huge potential for the future research and development applications. Three types of copy move passive blind approach are presented at first. Then, block-based and key point-based CMFD methods are reviewed from different aspects, While going through the various papers on digital image forgery, which describes method for detection of copy move image forgery in digital image, it has been seen that a lot of work has been completed for copy move forgery detection. Thus additional research attempt is still needed to develop an suitable algorithm that can notice the copy move.. Some CMFD schemes with high performance are expected to become standard tools in the future. We also hope that this survey will provide related information to scientists, researchers, and relevant research communities in

this field. The investigation on image forensics is still a continual, sustainable process and it will continue to explore forensics technologies with high accuracy and robustness.

REFERENCES

1. *Devanshi Chauhan, Dipali Kasat, Sanjeev Jain, Vilas Thakare, "Survey On Key point Based Copy-move Forgery Detection Methods On Image" International Conference on Computational Modeling and Security (CMS 2016), Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license*
2. *Zhi Zhang*, Chengyou Wang*, and Xiao Zhou*, "A Survey on Passive Image Copy-Move Forgery Detection", J Inf Process Syst, Vol.14, No.1, pp.6~31, February 2018*
3. *Badal Soni. , Pradip K. Das, Dalton Meitei Thounaojam "CMFD: a detailed review of block based and key feature based techniques in image copy move forgery detection", IET Image Process., 2018, Vol. 12 Iss. 2, pp. 167-178*
4. *Remya Revi K, Dr. M Wilscy "Scale Invariant Feature Transform based Copy-Move Forgery Detection Techniques on Electronic Images-A Survey" IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI-2017), 978-1-5386-0814-2/17/$31.00 ©2017 IEEE*
5. *Resmi M.R. Vishnukumar S." A Novel Segmentation Based Copy-Move Forgery Detection in Digital Images", 2017 International Conference on Networks & Advances in Computational Technologies (NetACT) |20-22 July 2017| Trivandrum*
6. *Anil Dada Warbhe, R. V. Dharaskar, , V. M. Thakare, "A Scaling Robust Copy-Paste Tampering Detection for Digital Image Forensics" 7th International Conference on Communication, Computing and Virtualization 2016, Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license, ScienceDirect Procedia Computer Science 79 (2016) 458 – 465*
7. *Alaa Hilal, Taghreed Hamzeh, Samer Chantaf, "Copy-Move Forgery Detection using Principal Component Analysis and Discrete Cosine Transform", 978-1-5090-6011-5/17/$31.00 ©2017 IEEE*
8. *Khaled W. Mahmoud, Arwa Husien Abu Al-Rukab , "Moment Based Copy Move Forgery Detection Methods", International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 7, July 2016*
9. *Yuan Wang, Lihua Tian, Chen Li, "LBP-SVD Based Copy Move Forgery Detection Algorithm", 2017 IEEE International Symposium on Multimedia*
10. *Prajwal Pralhad Panzade, Choudhary Shyam Prakash, Sushila Maheshkar "Copy-Move Forgery Detection by Using HSV Preprocessing and Keypoint Extraction", 2016 Fourth international conference on parallel, Distributed and Grid computing.*
11. *Adam Novozamsky and Michal Sorel, "JPEG Compression Model in Copy-move Forgery Detection" The Czech Academy of Sciences, Institute of Information Theory and Automation*
12. *Er. Harish kundra, Er. Nancy Mahajan, "A REVIEW ON THE DIGITAL IMAGE RESAMPLING FORGERY DETECTION TECHNIQUES", International Journal of Computer Science and Communication Engineering Volume 4 issue 1(Jully 20015 issue)*
13. *Ashwini V Malviya, Siddharth A Ladhake, "Pixel based Image Forensic Technique for copy-move forgery detection using Auto Color Correlogram", 7th International Conference on Communication, Computing and Virtualization 2016, Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license*
14. *Amani Alahmadi, Muhammad Hussain, Hatim Aboalsamh, Ghulam Muhammad, George Bebis, Hassan Mathkour," Passive detection of image forgery using DCT and local binary pattern", Accepted: 15 April 2016 © Springer-Verlag London 2016*
15. *Mona F. Mohamed Mursi, May M. Salama, Mohamed H. Habeb, "An Improved SIFT-PCA-Based Copy-Move Image Forgery Detection Method", International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE) Volume 6, Issue 3, March 2017*
16. *Bin Yang, Zhihua Xia, Xingming Sun, Xianyi Chen & Honglei Guo, "A copy-move forgery detection method based on CMFD-SIFT", Accepted: 20 December 2016 Springer Science+Business Media New York 2017*
17. *Yi Fan, Yue-Sheng Zhu and Zhen Liu, "An Improved SIFT-Based Copy-Move Forgery Detection Method Using T-Linkage and Multi-Scale Analysis", Journal of Information Hiding and Multimedia Signal Processing, 2016 ISSN 2073-4212, International Volume 7, Number 2, March 2016*

18. *Leida Li, Shushang Li, Hancheng Zhu, "An Efficient Scheme for Detecting Copy-move Forged Images by Local Binary Patterns", Journal of Information Hiding and Multimedia Signal Processi ng International Volume 4, Number 1, January 2013*
19. *Gargi rathod, Shruti Chodankar, Rupali Deshmukh,s. P. Pattanaik, Priyanka shinde, "Image forgery detection on cut-paste and copy-move forgeries", International Journal of Advances in Electronics and Computer Science, ISSN: 2393-2835 Volume-3, Issue-6, Jun.-2016*
20. *Li, L., Li, S., Zhu, H., et al.: 'An efficient scheme for detecting copy-move forged images by local binary patterns', IEEE Trans. Image Process., 2016, 4,(1), pp. 46–5*
21. *Chun-Su, P., Changjae, K., Jihoon, L., et al.: 'Rotation and scale invariant upsampled log-polar Fourier descriptor for copy-move forgery detection', Multimedia Tools Appl., 2016, 75, (23), pp. 16577–16595*
22. *Deng-Yuan, H., Ching-Ning, H., Wu-Chih, H., et al.: 'Robustness of copy move forgery detection under high JPEG compression artifacts', Multimedia Tools Appl., 2017, 76, (1), pp. 1509–1530*
23. *R. E. J. Granty and G. Kousalya, "Spectral-hashing-based image retrieval and copy-move forgery detection," Australian Journal of Forensic Sciences, vol. 48, no. 6, pp. 643-658, 2016.*
24. *J. Zhong, Y. Gan, J. Young, and P. Lin, "Copy move forgery image detection via discrete Radon and polar complex exponential transform-based moment invariant features," International Journal of Pattern Recognition and Artificial Intelligence, vol. 31, no. 2, article no. 1754005, 2017.*
25. *L. Yu, Q. Han, and X. Niu, "Feature point-based copy-move forgery detection: covering the non-textured areas," Multimedia Tools and Applications, vol. 75, no. 2, pp. 1159-1176, 2016.*
26. *R. K. Karsh, A. Das, G. L. Swetha, A. Medhi, R. H. Laskar, U. Arya, and R. K. Agarwal, "Copy-move forgery detection using ASIFT," in Proceedings of the 1st India International Conference on Information Processing Delhi, India, 2016, pp. 1-5*
27. *Bin, Y., Xingming, S., Honglei, G., et al.: 'A copy-move forgery detection method based on CMFD-SIFT', Multimed. Tools Appl., 2017, pp. 1–19*
28. *Jaberi, Maryam, et al. "Improving the detection and localization of duplicated regions in copy-move image forgery." IEEE, 2013.*
29. *Pandey, Ramesh Chand, et al. "Fast and robust passive copy-move forgery detection using SURF and SIFT image features." IEEE, 2014 keys*
30. *Prinkle Rani and Jyoti Rani, "Copy-Move Forgery Attack Detection using Enhanced SIFT", International Journal of Engineering Research & Technology (IJERT), Oct. 2015.*
31. *Navneet Kaur and Nitish Mahajan "Image Forgery Detection using SIFT and PCA Classifiers for Panchromatic Images", Indian journal of Science and Technology, Sep. 2016.*
32. *Kumar, Sunil, J. V. Desai, and Shaktidev Mukherjee .2015. "Copy Move Forgery Detection in Contrast Variant Environment using Binary DCT Vectors". International Journal of Image, Graphics and Signal Processing (IJIGSP) 7.6 (2015): 38.b*
33. *Sunil Kumar, Desai Jagan, and Mukherjee Shaktidev .2014. "DCT-PCA based method for copy-move forgery detection". ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 03 Issue: 06 | June-2016 | Page 1252 Vol II. Springer International Publishing.*
34. *Hashmi MF, Anand V, Keskar AG. A copy-move image forgery detection based on speeded up robust feature transform and Wavelet Transforms. In: Computer and Communication Technology (ICCCT), 2014 International Conference on. IEEE; 2014. p. 147–52.*
35. *Y. Wo, K. Yang, G. Han, H. Chen, and W. Wu,(Feb. 2017) "Copy–move forgery detection basedon multi-radius PCET," IET Image Processing, Vol. 11, No. 2, PP. 99–108*
36. *Junliu zhond, Yenfen gan, Y. Wo, K. Yang, G. Han, H. Chen, and W. Wu,(Feb. 2017) "Copy–move forgery detection basedon multi-radius PCET," IET Image Processing, Vol. 11, No. 2, PP. 99–108*
37. *Junliu zhond, Yenfen gan, "A new block based method for copy move forgery detection under image geometric transforms", Journal of Multimedia Tools and Applications, Vol 76, issue 13, July 2107*
38. *Sreelakshmy I J, Jesna Anver, "An Improved Method For Copy-move Forgery Detection In Digital Forensic", 2016 Online International Conference on Green Engineering and Technologies (IC-GET)*

39. *Rachana, Ashok Kumar, H.L.Mandoria, Binay Pandey, "Study and Analysis of Copy-Move Forgery Detection in Digital Image: A Review", International Research Journal of Engineering and Technology (IRJET) vome 03, issue 06, June 2016.*
40. *Diaa M. Uliyan, Hamid A. Jalab *, Ainuddin W. Abdul Wahab and Somayeh Sadeghi, "Image Region Duplication Forgery Detection Based on Angular Radial Partitioning and Harris Key-Points", Symmetry 2016, 8, 62; doi:10.3390/sym8070062*
41. *Yan Wo, Kemin Yang,Guoqiang Han, Haichao Chen, Wenbo Wu," Copy–move forgery detection based on multi radius PCET", IET Image Process., 2017, Vol. 11 Iss. 2, pp. 99-108*
42. *Reshma Raja, Niya Joseph, "Keypoint Extraction Using SURF Algorithm For CMFD", Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license.*