A LITERATURE REVIEW ON COPY-MOVE IMAGE FORGERY DETECTION

[1]Aparna Dhendwal, [2]Praveen K Sharma, [3]Rakesh Saini,
[1]B.Tech Scholar, [2]Assistant Professor, [3]Assistant Professor
[1,2]Department of ECE, [3]Department of IT
[1,2,3]BK Birla Institute Of Engineering And Technology, Pilani, India

Abstract: In today's digital world very advanced photo editing tools or software are available so that sometimes the wrong advantages are also raised that could never have imagined before. Through Digital photography, Photoshop and computer graphics image forgery is much easier to make and as well as it is harder to detect. To add, modify or remove important features from an image is now possible without leaving any perceptual traces of tempering. Image forgery is generally used to copy and paste the image on one to another. This paper presents a detailed review on Image Forgery and its detection techniques.

Key Terms: **Scale-Invariant Feature Transform (SIFT), Copy-Move Forgery (CMF), Discrete Wavelet Transform (DWT)**

I. INTRODUCTION

Now a days sharing information is very easy because world is living in the remarkable era of visual imagery. But, in today's digital age, it is now possible to change the information very easily signified by an image. On the internet and the main stream media, forgeries are rapidly increased. This indicates the trend of serious vulnerabilities and decreases the credibility of digital image. Therefore, to verify the trustworthiness and genuineness of the digital images is very important for the developing techniques. In this sense, image forgery detection is one of the primary goal of image forensics [20].

Figure-1: Example of image forgery [20]

Digital image processing is used to process images to improve pictorial information for human perception, image processing for autonomous machine application and efficient storage application. Digital image processing is used to process images which are digital in nature by digital computers. There are many typical applications like noise filtering, content enhancement, weather forecasting, atmospheric study, astronomy, machine vision application, video sequence processing, image audio or video forgery detection [22].

II. TYPES OF IMAGE FORGERY DETECTION

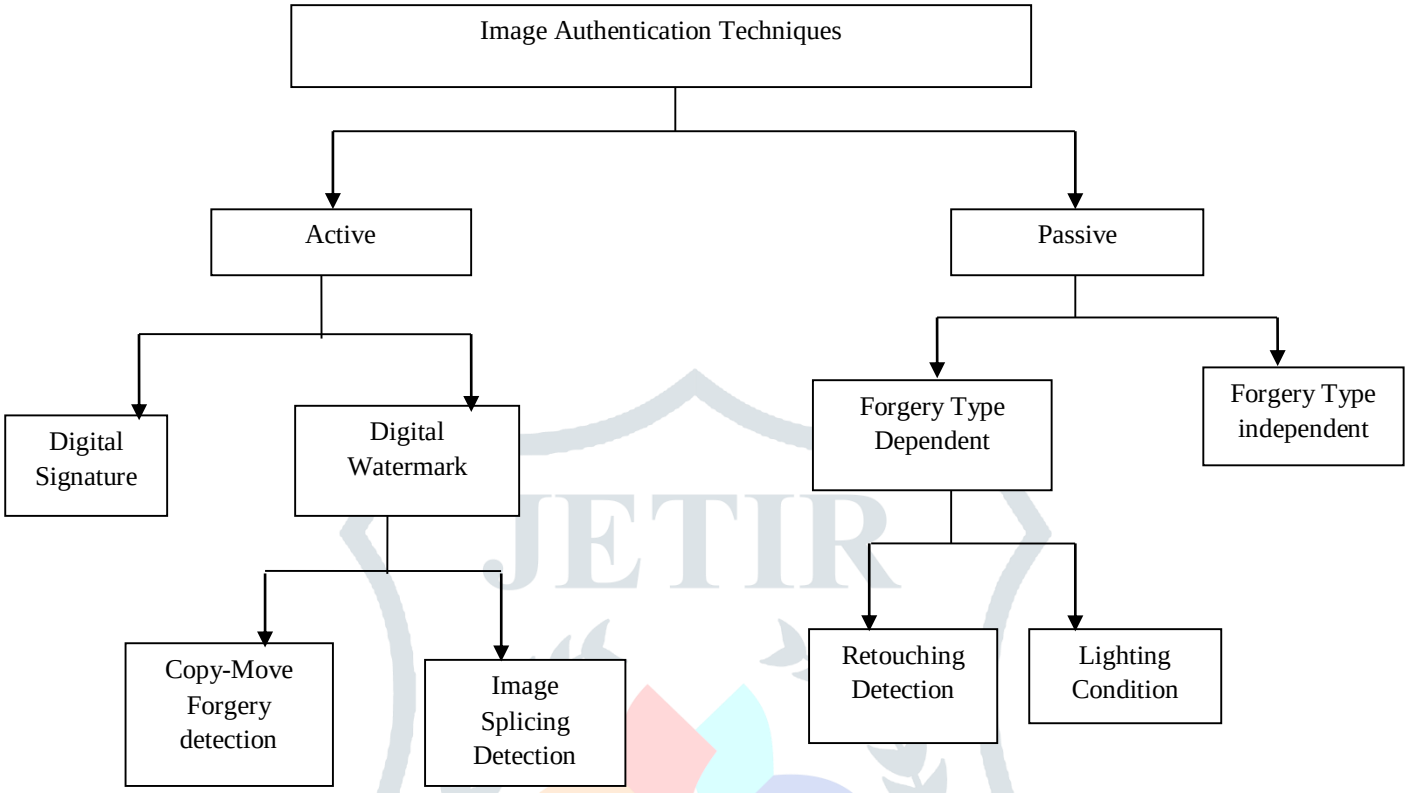


Figure-2: Image authentication technique

Digital image forgery detection techniques are broadly classified into two approaches: Active approach and Passive approach .The digital image desires preprocessing of image in the active approach such as Watermark embedding or the signature generation, which limit their application in practice. The two main active protection techniques are Digital watermarking and signature, as something are embedded into images when they are obtained. We can detect the image is tempered, if special information cannot be extracted from that obtained image. In recent times number of proposed schemes are available to provide security to the image. In the passive approach, during the creation there is no pre-embedded information inside an image. Analysis of the binary information of an image works purely by this method. Passive image forgery detection can be classified into five categories: Pixel Based Techniques, Format based techniques, Camera Based Techniques, Physical environment Based Techniques and Geometry Based Techniques [22].

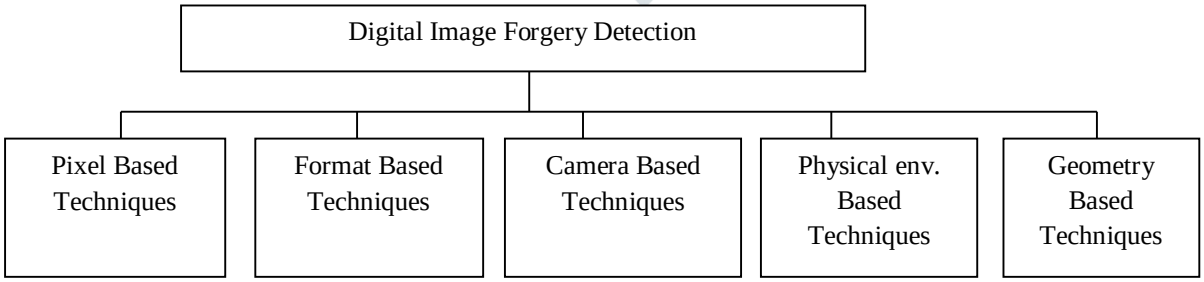
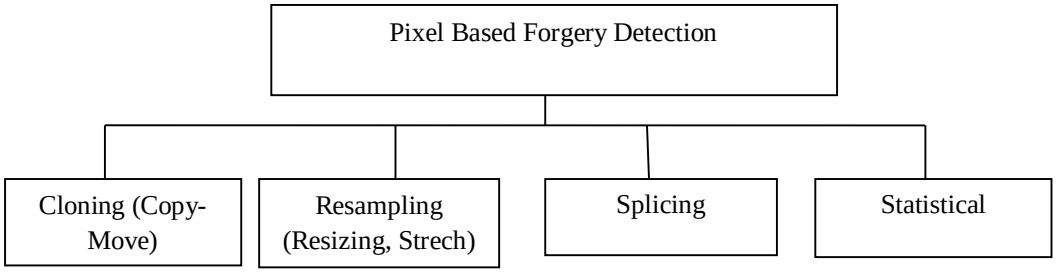


Figure-3: Forgery detection techniques

Statistical anomalies introduced at the pixel level by Pixel-based techniques detection; statistical correlation can be introduced by a lossy compression scheme through format based technique; camera based techniques exploit artifacts introduced by the camera lens, sensor, or on chip post processing; physical environment based techniques; and geometry based techniques make measurements of objects in the world and their positions relative to the camera.

i) Pixel based image forgery detection:

Pixel of the digital image can be emphasizing by Pixel-based techniques. These techniques are roughly categorized into four types. Pixel based techniques detect statistical anomalies introduced at the pixel level [1, 4]. In Figure 4 shows categorization of pixel based forgery detection techniques.



F

Figure-4: Pixel based image forgery detection

a. Cloning (Copy-Move):

Cloning is also known as copy-move forgery and this is one of the most common type of image forgery. Digital image of copy move forgery is a kind of image where we can copy a section from the image and then paste to the same section to another image. This technique may be performed with some wrong intension and basically it is used to make fake image.

b. Splicing:

Another type of image forgery is splicing .This technique is used to copy and paste two or more images and combine to make a fake image [18]. Suppose we have two images (1 & 2), as shown in Figures 5 and 6 both images are spliced into a single composite image (Figure 7).

Figure-5: Image-1

Figure-6: Image-2

Figure-7: Single composite image

c. Image Re-sampling

To make forged image, there are some selected regions which have to undergo geometric transformation like rotation, stretching, skewing, flipping, scaling and so forth. For photo editing this technique is very popular. This type of image forgery technique used in almost all magazine covers to enhance certain features of an image so that the image is more attractive [21].

Figure-8: Example of image retouching

III. COPY-MOVE IMAGE FORGERY

In literature, image forgery can be defined in number of ways, adding, changing, or deleting some important features characterized by picture altering from an image without leaving any obvious trace. Different techniques have been utilized for an image forging. Taking into account the methods used to make forged images, digital image forgery can be separated into three primary classifications: copy-move forgery, image splicing and image resampling but we have discussed only copy-move forgery detection in this paper.

The copy-move forgery is one of the most common types of image forgery or it is also known as cloning. In copy-move forgery type technique, the original part of the image is copied and paste to another image. The example of copy-move type is shown in the following figures. The original image contains only three missiles and coy moved version on the right has four missiles [19].

Figure-9: Example of copy-move forgery [19]

Basically Copy- Move Forgery Detection (CMFD) is a passive method which rely on the assumption that tempering is expected to change the elementary statistics even when it may not leave visual clues behind such inconsistencies which are used in copy-move forgery detection algorithms. CMFD techniques are forgery dependent techniques which are specially designed for this cloning detection. Generalized Framework used for CMFD is as follows:

(a) Image pre-processing:
The image on which we are going to process the method, it has to be preprocessed in which resizing, cropping, and gray-scale conversion from RGB color space etc has been done on the test image.

(b) Feature extraction:
For every class feature set is extracted which is helpful in distinguishing it from other classes and being essentially to all the differences in attributes from the host tampered data within a class.

(c) Classifier selection and feature pre-processing
A suitable classifier needs to be developed or chosen on the bases of the feature extraction. For the classifier's training is selected of large set of digital images and obtained some salient parameters of the chosen classifier that can be exploited for this classification.

(d) Classification
A classifier is broadly grouped into two classes: genuine and tampered digital image. A suitable classifier is further designed or chosen on the basis of feature extraction.

(e) Post-processing
Post-processing is a final step which involves the morphological operation and intent to lower false positive rate which are performed. Matching patches belonging to equal shift vectors to discriminate various copy-move patches and shift vectors are marked the same color and to visually locate the duplicate areas, usually white are used.

IV. CMFD (Copy- Move Image Forgery Detection) TECHNIQUES:

CMFD techniques divided into two categories: Block-based CMFD techniques and the Key-point based CMFD techniques. Given image is divided by the point of block-based CMFD techniques into either overlapping or non-overlapping tiles followed by the application on each tile of any transform. On the basis of some similarity criterion, similar blocks are computed. However, the extraction of interest points of an image involves by the key-point based CMFD method. For the identification of the duplicated regions, they make of local features of the interest points. Host image is segmented into image blocks in hybrid CMFD algorithms before key-point extraction. In addition to the less computational burden, these types of techniques are quite robust to the various geometrical attacks.

Block-Based CMFD Techniques:
Block Based technique was the first attempt for determination of tempered regions. To extract the features of host image the researchers divided the host image into overlapping files followed by the application of DCT (discrete Cosine Transform) to every image title. To reduce the computational complications lexicographical representation used. For better outcomes, Histogram was determined which is counting the matching blocks that even equal distance apart. And in final step a pre-defined threshold value is used in order to discard false alarms and determine the duplicated patches. Following method is one of the best techniques to solve complexity and performance issues but it is not able to detect small replicated regions.

Key point Based CMFD Techniques:
It is the best method to utilize Scale Invariant Feature Transform (SIFT) feature extraction along with key-point matching. Cloning can be detected by clustering of key-points, tempering detection and the next step estimated the occurrence of geometrical attacks. This method opted fine accuracy on various kinds of operation including JPEG compression, scaling, noise, rotation and exhibited robustness against the compound attacks in the post processing operations. In addition to this method it identifies the patches of replicas and also deduces the type of geometric transformation used for performing that forgery.

Hybrid CMFD Techniques:
Hybrid CMFD technique integrates both block based and key-point based detection algorithm. This method is introduced by Pun. Segment the test image into irregular and non-overlapping patches in an adaptive manner. Feature extraction was done by SIFT and then matched to determine labeled key feature points. Hybrid CMFD technique showed better detection precision and recall as compared to other methods. Li segmented a test image into non-overlapping independent patches. Then SIFT is used for key-point detection and extraction on each patch. Kl tree as constructed and K nearest neighbor search was performed for each extracted key-point.

CMF Attacks:
A number of image handling operations are grouped broadly into two classes: intermediate and post-processing. In the replicated regions and their neighbors, Intermediate processes are used in mainly providing the homogeneity and spatial synchronization. These intermediate operations include rotation, mirroring, scaling, chrominance modifying, or illumination modifying.

FLOW CHART OF COPY-MOVE FORGERY DETECTION

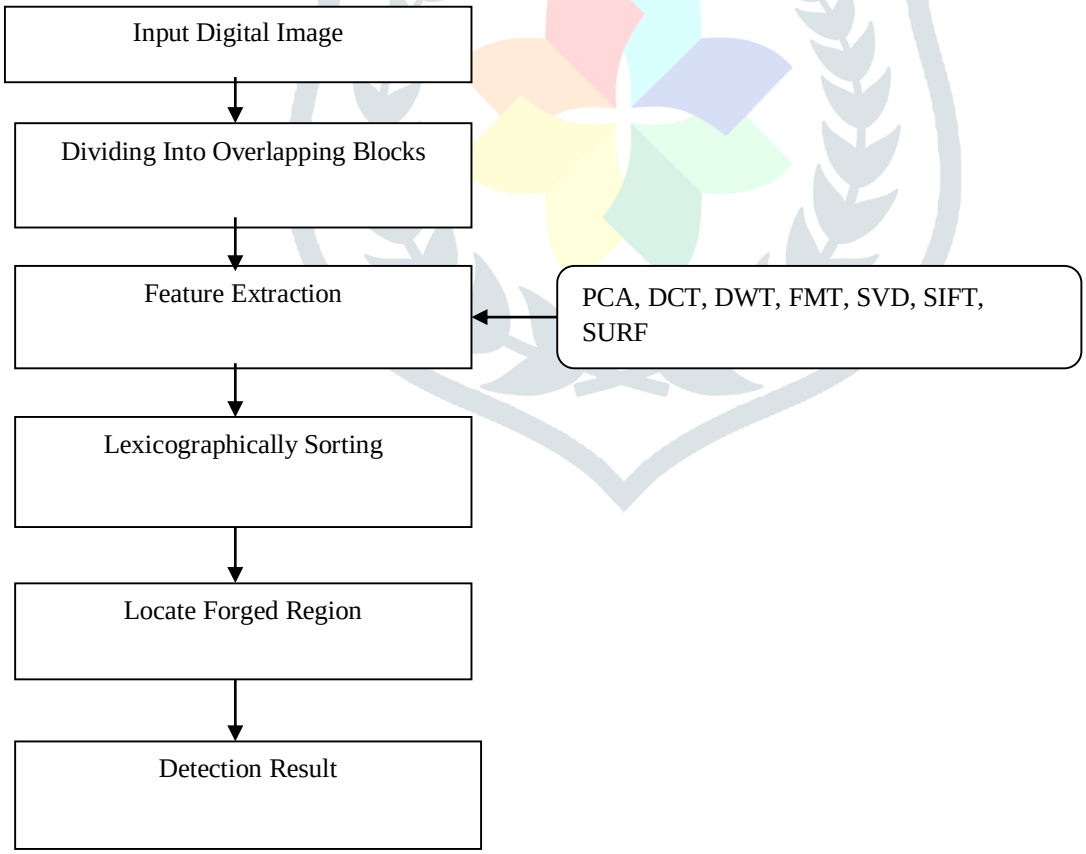


Figure-10: Block diagram of copy-move image forgery detection

V. LITERATURE REVIEW

[1] Jessica Fridrich, David Soukal and Jan Lukas proposed two techniques for detection, exact match and the approximate match. One method is based on the exact match and another one is based on an approximate match. For identifying segments in the image that are matched exactly by ordering and matching of pixel representation of the blocks. Robust match is similar to the exact match behind the approximation of this technique. But robust depiction that consists of quantized DCT coefficients. These are some method which is successfully detect the forged part in the image even the forged area is modified to merge it with the background and then the forged picture is saved in a distortion format such as JPEG.

[2] Alin C Popescu and Hany Farid proposed an algorithm which is based on the PCA (Principal Component Analysis), small fixed size image block which is applied to analyze and to obtain a reduced dimension representation. This are the representation is strong to predict minor variation in the image due to noise and lossy JPEG compression. The image which is based on the alphabetical order of their component letters sorting all the image blocks which is easily detect the duplicated regions. Additive noise and lossy LPEG compression is more reliable in this technique.

[3] Chi-Man Pun, et al. proposed a novel copy move forgery detection scheme which is used adaptive over segmentation and feature point matching. The proposed scheme integrates both the methods block based forgery detection method and the key point based forgery detection method. The proposed copy move forgery detection can achieve much better detection results compared with the existing state of the art copy move forgery detection methods.

[4] M. K. Bashar, Member, et al. proposed a duplication technique based on DWT (Discrete Wavelet Transform) and KPCA (kernel Principal Component Analysis). Both DWT and KPCA schemes provide excellent representations of the image data for robust block matching. For lexicographic sorting, multi resolution wavelet coefficients and KPCA based projected vectors corresponding to image blocks are arranged into a matrix form. For making a list of similar point pairs and computing their offset frequencies, sorted blocks are used.

[5] Jian Li, Xiaolong Li, Bin Yang and Xingming Sun proposed a framework copy move forgery detection which is classified into the two stages in which the image is first segmented into non-overlapped patches. In first strategy to find the suspicious matches by matching patches, and then a transform matrix is estimated. Then in the second stage, confirm the existence of copy move image forgery by refining the transform matrix. The key point based methods are much faster and favorable than the block based method, but it poses faster detection compared with existing block based algorithms.

[6] Gajanan K. Birajdar, et al. has presented the digital image tempering and the existing references on blind methods for image forgery detection. Different image forgery detection are classified and then presented the generalized structure of image forgery detection.

[7] Y. Wang, et al. proposed a wavelet-based region duplication forgery detection in 2012. The image is divided into overlapped blocks with fixed size and then applied multilevel 2D discrete wavelet transform to each block.

[8] Anuja Dixit et al. proposed copy move image forgery detection using frequency based techniques in 2016. Image is divided in blocks and the then the feature vectors are extracted corresponding to different blocks of image. To find out the similarity between blocks, sorting techniques are applied. In case of natural images, shift vectors are calculated to decrease false matches. In future hybrid techniques can be applied for achieving more accurate results with less computational cost.

[9] Dijana Tralic, et al. developed new database for copy move forgery detection in 2013, which consist of 260 forged image sets. Every image set includes forged image, two masks and original image. According to applied manipulation, images are grouped in 5 categories: translation, scaling, rotation, combination and distortion.

[10] Xiu-Li Bi, et al. proposed over segmentation image forgery detection in 2015. Firstly the Adaptive over Segmentation algorithm is proposed adaptively segment the host image into an irregular and non-overlapping blocks. Feature points are then matched and extracted with each to locate feature points which can approximately indicate the suspected forgery regions. Finally processed the labeled feature points and to generate the detected forgery regions is applied by morphological operation. The proposed CMFD indicate the good performance by experimental results.

Table-1: COMPARISION BETWEEN EXISTING TECHNIQUES

S. No	Author/Year	Methodology	Advantage
1	H. Huang, 2008[11]	SIFT	Detected copy-move region
2	M. Bashar 2010[13]	DWT	Exploring duplicated regions in natural images.
6	M. Ghorbani, 2011[14]	DWT-DCT(QCD)	Detected the forged region
7	G. Muhammad, 2011 [15]	DYWT	DYWT is a shift invariant and therefore more suitable than DWT for data analysis
8	SAH Tabatabaei, 2015[16]	AMACs	AMACs combine error-correcting codes with cryptographic primitives such as message authentication codes and symmetric encryption algorithms
9	Pun[3] 2015	Fixed	The average precision is 95.92%, recall is 97.22% and F1 is 96.91%.
10	Pun[3] 2015	Adaptive	The average precision is 96%, recall is 100% and F1 is 96.91%.
11	Dhania VS, 2016[17]	SIFT	This method integrates both block based and key-point based forgery detection.
12	A Thakur [12] 2018	SVM	Precision is 97.25% and recall is 100% and F1 is 98.53%

VI. CONCLUSION

Copy-move forgery has become one of the most common and easy to carry technique to manipulate images. This paper has presented a detailed review of copy-move forgery and its different detection techniques. In this paper a comparison between existing techniques is also done to achieve better detection results. Also Machine Learning can also be implemented for copy- move image forgery detection.

VII. REFRENCES

[1] Jessica Fridrich, David Soukal, and Jan Lukas," Detection of Copy-Move Dorgery in digital Images", in Proc. Digit. Forensic Res. Workshop, Cleveland, OH, Aug.2003.
[2] A.C.Pospescu and H. Farid,''Exposing digital forgeries by detecting duplicated image regions,'' Dept. Comput. Sci., Dartmouth College, Hanover, NH, USA, Tech. Rep. TR2004-515, 2004.
[3] Chi Man pun, Senior Member, IEEE, Xiao-Chen Yuan, member, IEEE, and Xiu-Li Bi "Image Forgery Detection Using Adaptive Over segmentation and Feature Point matching ", IEEE Transactions on Information Forensics And Security, Vol. 10, No. 8, August 2015.
[4] M. K. Bashar, Member , IEEE, K. Noda, Non-member, N. Ohnishi, and K. Mori, member, IEEE,'' Exploring Duplicated Regions in Natural Images'', IEEE.
[5] Jian Li, Xiaolong Li, Bin yang and Xingming Sun,'' Segmentation-Based Image Copy-Move Forgery Detection Scheme,'', IEEE Transactionson Information Forensics and Security, Volume:10, dec 2014.
[6] Gajanan K. birajdar a, Vijay H. Mankar, " Digital image forgery detection using passive techniques: A survey'', Elsevier, DOI: 10.1016/j.diin.2013.04.007.
[7] y. wang, K. Gurule, J. Wise, and J. Zheng,''wavelet based region duplication forgery detection,'' in Proc. Of the 9th International Conference on information Technology, pp.30-35, 2012.
[8] Anuja Dixit and R. K. Gupta, "Copy-Move Forgery detection using Frequency based Techniques: A Review", International journal of signal Processing, Image Processing and Pattern recognition, Vol.9, No.3 (2016), pp.71-88.
[9] Dijana Tralic,Ivan Zupancic, Sonja Grgic, Mislav grgic, ''CoMoFoD-New Database for Copy Move Forgery detection'', 55th International Symposium ELMAR-2013, 25-27 September2013, Zadar, Croatia.
[10] Xiu-Li Bi, Chi-Man Pun, and Xiao-Chen Yuan,'' Over-Segmentation Image Forgery Detection,'' in Proceedings of international Conference on Electronics and Automation Control,2015.
[11]W. Luo, J. Huang and G. Qiu, "Robust detection of region-duplication forgery in digital images", International Conference on Pattern Recognition, vol. 4,2006.
[12]Thakur, A. & Jindal, N. Multimed Tools Appl (2018). https://doi.org/10.1007/s11042-018-5836-5.

[13]M. Bashar, K. Noda, N. Ohnishi, and K. Mori, "Exploring duplicated regions in natural images," IEEE Transactions on Image Processing, 2010.
[14]M. Ghorbani , M. Firouzmand, and A. Faraahi, "DWT-DCT (QCD) based copymove image forgery detection," in Proc. of the 18th International Conference on Systems, Signals and Image Processing, pp. 1–4, 2011.
[15]G. Muhammad, M. Hussain, K. Khawaji, and G. Bebis, "Blind copy move image forgery detection using dyadic undecimated wavelet transform," in Proc. of the 17th International Conference on Digital Signal Processing, pp. 1–6, 2011.
[16]Seyed Amir Hossein Tabatabaei, Obaid Ur-Rehman, Natasa Zivic, and Christoph Ruland, "Secure and Robust Two-Phase Image Authentication", IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 17, NO. 7, JULY 2015.
[17]Dhania V S, Harish Binu K P, "Exposing Digital Image Forgeries Using Feature Extraction and Adaptive Over Segmentation", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 5, Issue 8, August 2016.
[18] Mohd Dilshad Ansari, S. P. Ghrera & Vipin Tyagi, IETE Journal of Education, "Pixel- Based Image Forgery Detection: A Review", IETE Journal of Education,| VOL 55, No 1,| JAN- JUN 2014.
[19] V. Tyagi, "Detection of forgery in images stored in digital form," Project report submitted to DRDO, New Delhi, 2010.
[20] Amanpreet Kaur, Richa Sharma: "Copy-Move Forgery Detection using DCT and SIFT", International Journal of Computer Applications (0975 – 8887) Volume 70– No.7, May 2013.
[21] L. Kang, and X.-P. Cheng, "Copy-move forgery detection in digital image," 3rd IEEE International Congress on Image and Signal Processing (CISP 2010), 2010, pp. 2419-2421.
[22] J. C. Lee, C. P. Chang, and W. K. Chen, "Detection of copy move image forgery using histogram of orientated gradients," Inf. Sci. (Ny)., vol. 321, pp. 250–262, 2015
[23] Bayram S., Avcibas I., Sankur, and B. Memon N.,"Image manipulation detection," Journal of Electronic Imaging – October - December 2006 – Volume 15, Issue 4, 041102 (17 pages), vol. 15(4), 2006.