Saarth E-Journal

Saarth E-Journal of Research

E-mail : sarthejournal@gmail.com
www.sarthejournal.com

ISSN NO : 2395-339X
Peer Reviewed
Vol.8 No.19

Impact Factor
Quarterly
Jan-Feb-Mar 2023

A Depth Analysis on Forgery Detection in Case of Copy-Move Image Forgery

Mr. Jaynesh Desai, Dr. Sanjay Buch

Abstract

Since there are so many effective methods for manipulating photos, their authenticity is becoming a subject of debate, especially when those images have a lot of sway. utilized for news reports, insurance claims, and in court as examples of this. The integrity of images is established by picture forensic procedures using a variety of high-tech mechanisms that have been found in the literature. The internet has recently been overrun with billions of digital photographs, making it the main source of knowledge in many fields. Given how far technology has come, image fraud could seem easy to do. Digital photo copy-move forgeries, in which one or more objects or regions are copied or replicated, are the most common sort of image tampering. Digital forensics has given more focus to a crucial study field called forgery detection and localization.Numerous papers have been produced and a number of strategies have been proposed to recognise fraudulent photos. In order to emphasise the most recent methods for detection, this work reviewed research papers on copy-move image forgery that were published in reputable journals between 2017 and 2020. It then discussed numerous fraud picture-related strategies. In order to create new and more effective copy-move image detection algorithms, researchers will benefit from understanding the existing methods and methodologies in this field.

Keywords—Image forensics; copy-move forgery detection (CMFD); conventional techniques;

1. Introduction

Images in communication media are now very helpful. There is a sense that the visual conveys more significance about the incident or circumstance than the words do. In the current technological world, digital photographs are crucial in many different industries. They are primarily featured in journalism, news, defence, and health-related employment. Due to advancements in digital image technology, including advances in camera equipment, software, and computer systems, as well as the expanding popularity of internet media, a digital image can presently be considered as a crucial piece of information.

Images in communication media are now very helpful. There is a sense that the visual conveys more significance about the incident or circumstance than the words do. In the current technological world, digital photographs are crucial in many different industries. They are primarily featured in journalism, news, defence, and health-related employment. Due to advancements in digital image technology, including advances in camera equipment, software, and computer systems, as well as the expanding popularity of internet media, a digital image can presently be considered as a crucial piece of information.

There are two types of the active methods that are digital watermarking and digital signature [27]. Adigital watermark is added to the photo to identify copyright. It is the process of hiding special information(series of bits) in a digital image. The special information may be the author's serial number, company logo,meaningfultext,andsoon.

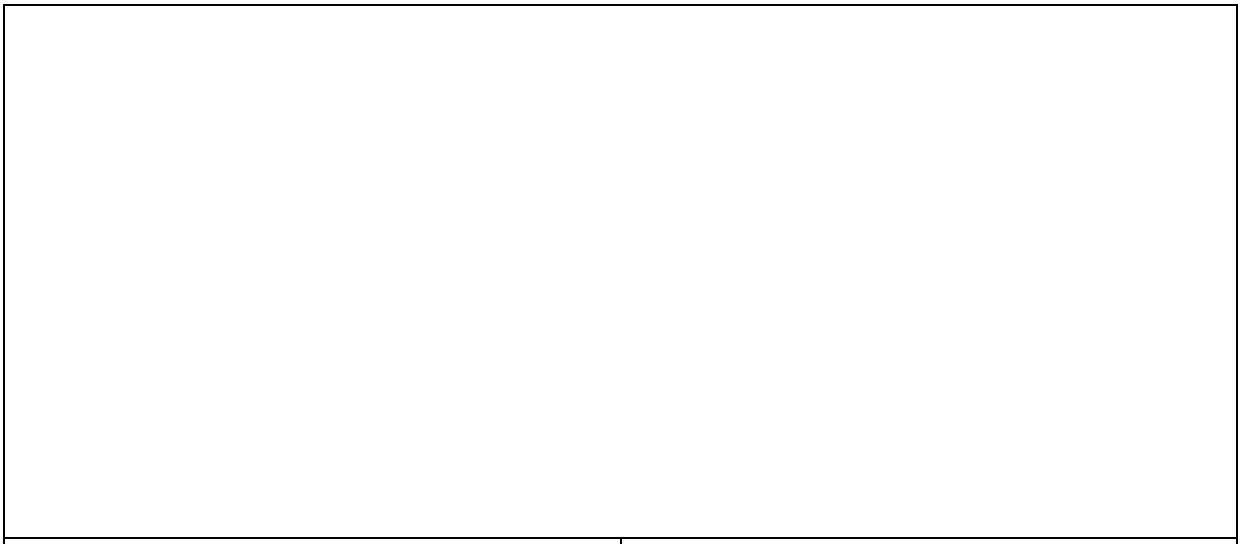
Type of image forgeries

Digital images can be used as a proof against crimes, and any person can make changes in digital image to hide or remove important information with the help of different types of editing soft wares available like Adobe Photoshop, Corel draw etc. Changes that can be made on images are given below:

1) Image Retouching,
2) Image Splicing,
3) Image Morphing,
4) Image Enhancing,
5) Copy move,
6) scaling ,
7) cropping,
8) geometric transformation,
9) selective color change,
10) merging another image or a part of same or different image.

The most common type among various forms of falsification of images is a copy-move forgery. In thedigital image copy-move forgery, one or more regions are repeated at different locations within the sameimage. Often duplicate dregion sareen larged, shrank,

orrotated to make forgery more convincing, making it more difficult to detect forgery images [28]Figure1 points to the exampleof copy – move forgery.



Original Image	ForgeryImage

[Figure 1: Example of copy-move forgery]

Related Work

Intense literature review has been done in the paper from year 2015 to 2019 to bring in light different techniques, algorithms and tools used by different authors.

Various CMFD techniques have been proposed so far to effectively address the region duplication problem. In this regard, the research is intended towards the representation of image regions in a more powerful way to accurately detect the duplicated regions. In [11], Fridrich et al. for the first time presented the copy-move forgery detection technique using DCT on small overlapping blocks. The feature vectors are formed using DCT coefficients. The similarity between blocks is analyzed after sorting the feature vectors lexicographically. In [13], image blocks are represented through principal component analysis (PCA). Exploiting one of the features of PCA, the authors used about half of the number of features utilized by [11]. It makes this technique effective but failed to detect copy-move forgery with rotation. In [15], a sorted neighborhood technique based on Discreet Wavelet Transform (DWT) is proposed. The image is decomposed into four subbands and applied the Singular Value Decomposition (SVD) on low frequency components for getting the feature vector.

The technique is robust to JPEG compression up to the quality level 70 only. In [16], a technique based on blur moment invariants up to seventh order for extracting the block features and kd-tree matching is introduced. In [12], the application of scaling and rotation invariant Fourier-Mellin Transform (FMT) is suggested in combination with bloom filters on the image blocks for detecting the image forgery. In [14], an improved DCT-based technique is proposed by introducing a truncating process to reduce the dimension of feature vector for forgery detection. In [17], a solution through DCT and SVD is proposed for detecting image forgeries. The algorithm is shown to be robust against compression, noise, and blurring but fails when images are even slightly rotated. In [18], an efficient expanding block technique based on direct block comparison is proposed. In [19], circle block extraction is performed and the features are obtained through rotation invariant uniform local binary patterns (LBP).

The technique is robust to blurring, additive noise, compression, flipping, and rotation. However, this technique failed to detect forged regions rotated with arbitrary angles. In [20], the authors employed a new powerful set of keypoint-based features called MIFT for finding similar regions in the images. In [21], the authors extracted feature vectors from circular blocks using polar harmonic transform (PHT) for detecting image forgeries. In [22],

an adaptive similarity threshold based scheme is presented in the block matching stage. The detection of forged regions is determined using thresholds proportional to blocks standard deviations. In [23], a method using the Histogram of Oriented Gradients (HOG) is suggested to detect the copy-move forged regions. In [24], the multiscale Weber's law descriptor (multi-WLD) and multiscale LBP features are extracted for image splicing and copy-move forgery detection from chrominance components. The authors employed SVM for classifying an image as authentic or forged.

With the advancements in imaging technologies, the digital images are becoming a concrete information source. Meanwhile, a large variety of image editing tools have placed the authenticity of images at risk. The ambition behind the image content forgery is to perform the manipulations in a way, making them hard to reveal through the naked eye, and use these creations for malicious purposes. For instance, in 2001, after the 9/11 incident, several videos of Osama bin Laden over the social media were found counterfeited through the forensic analysis [1]. In the same way, in 2007, an image of tiger in forest forced the people to believe in the existence of tigers in the Shanxi province of China. The forensic analysis, however, proved the tiger to be a "paper tiger" [2]. Similarly, in 2008, an official image of four Iranian ballistic missiles was found to be doctored, as one missile was revealed to be duplicated [3]. Hence, the famous saying "seeing is believing" [4, 5] is no longer effective. Therefore, ways that can ensure the integrity of the images especially in the evidence centered applications are required.

In recent years, an exciting field, digital image forensics, has emerged which finds the evidence of forgeries in digital images [6]. The primary focus of the digital image forensics is to investigate the images for the presence of forgery by applying either the active or the passive (blind) techniques [2]. The active techniques such as watermarking [7] and digital signatures [6] depend on the information embedded a priori in the images. However, the unavailability of the information may limit the application of active techniques in practice [8]. Thus, passive techniques are used to authenticate the images that do not require any prior information about them [8]–[10].

Images are usually manipulated in two ways such as image splicing and region duplication through copy-move forgery. In image splicing, regions from multiple images are used to create a forged image. However, in copy-move forgery, image regions are copied and pasted onto the same image to conceal or increase some important content in the pictured image. As copied regions are apparently identical with compatible components (i.e., color and noise), it becomes a challenging task to differentiate the tempered regions from authentic regions. Furthermore, a counterfeiter applies various postprocessing operations such as blurring, edge smoothing, and noise to remove the visual traces of image forgeries. An example of copy-move forgery is shown in Figure 6.

The original images **The copy-move forged images**

[Figure 2 : An example of copy-move forgery]

In the present work copy-move forgery detection is addressed through the discrete cosine transform (DCT) and Gaussian RBF kernel PCA that are used to investigate the similarity between duplicated regions. The benefits of our algorithm compared against several existing CMFD methods are(i)utilization of the lower length of feature vectors;(ii)lower computational cost;(iii)robustness against various postprocessing operations over the forged regions;(iv)ability to detect multiple copy-move forgeries.

2.COMPARATIVE ANALYSIS

Comparing accuracy of the different methods published in the papers in recent years are summarized in Table1. Inaddition, the advantages and disadvantages of the semethods alsos hown in the table.

Reference	Method	Forgerydetection	Characteristics	Publisheyear
[29]	Detection image forgery using a pixel-base dalgorithm	Detection Copy-move and splicing image forgery	This method has good accuracy and higher liability. On the otherside, this method needs more time and has less accuracy to detect forgery from the noisy image.	2017
[30]	Combi net wotechniques ; key-point based and block-based	Copy-move image forgery	It is a robustmethod with less complexity. However, it is less accurate and did not work well with complicated back ground and texture.	2017
[31]	Deep learning mechanism	Copy-move image detection	It is a highly efficientmethod with fewer false positives. However, the accuracy is less.	2018

[32]	Using LCA and algorithm forb lock matching.	Detect image forgery based on analyzing the problem of the hypothesistest.	It is more efficient with lesscomplexity. However, it is not aproper method for the noisy image. The estimate derror will in crease.	2018
[33]	Passive digital Image forensic approaches	Image forgeries detected by using the artifacts.	This method consumes minimum time and has a good ability for generalizing. Despite it suffers from performance degradation and faces difficulties in most forgery cases.	2018
[34]	Using CNN and support vectormachine, K near estneighborand Naïve Bayes	Detecting Spliced image forgery	Has good accuracy and ability to find the location of the forgery region. However, it does not work well for copy move image forgery and requires asystemwith high performance to handle this algorithm.	2019
[35]	Convolution alneural network (C2RNet) and diluted a daptive Clustering	Detect Splice dimage forgery	It decreases the time and complexity. One of the disadvantages of this method is poorer in Recall than many other comparisonal gorithms.	2019
[36]	Deep learning and wavelet transformation.	Detect forgery	This method in creases accuracy an dreduced computation alcost. However, it is notrobust, with high time complexity.	2019
[37]	Mathematical morphological filter detector	Detect splicing image forgery	It is highly accurate and robust to image compression. Nevertheless, has complexity for mathematic caland time.	2020
[38]	Attention DM for CISDL	Detect splicing image forgery	This algorithm improved the performance and computational. At the sametime, it reduces the detectionrate.	2020
[39]	CNN	Image spliced tection and local ization scheme	It is highly accurate and robustto image compression (JPEG). The disadvantage is very high complexity.	2020

In addition, Table 2 summarized the accuracy of detection copy-move forgery, whenusing 40% forgery images out of the tested images. Comparing precision forseveral methods summarizedin

Table 3.

Methods	MaximumDetectionAccuracy(%)
BusterNet	93.02
SPT	96.99
PCA	97.7945
EnhancedSURF	98
SVD	98.8730
PCA-DCT	98.9776
DCT	98.0624
ImprovedDCT	98.5882
EfficientDCT	98.5934
DyWT	98.7438
CNN	99.03

[Table 2 :
Detection accuracy for various method susedin detection copy - move image forgery.]

Reference	**Method**	**Precision %**	**Fmeasure %**
[40]	Convolution alneural networks	94.89	
[41]	FASTER RCNNWITHELA (Error Level Analysis)	90	
[42]	Combined features	81.82	87.83
[43]	A-KAZE and SURF Features	91.76	94.54
[50]	Deeplearning approach	95.38	96.75
[28]	Fourier-Mellin and scale-invariant feature transforms	94.12	96.97
[44]	Ow SURF	96	
[45]	Speeded-Up Robust Feature (SURF) and Binary Robust Invariant Scalable Keypoints (BRISK)	94.03	
[48]	Using various texture descriptors (LBP, LPQ, Binary Statistical Image Features, and Binary Gabor Pattern)	94.39	
[46]	SURF	93.3	90.3
[47]	Mirror-SIFT		89.4
[49]	Deep neural network	78.22	75.98

[Table 3:
comparing the precision for different recent methods.]

Conclusion

In this paper, we focused on finding the ways through which we can assure the detection of copy-move forgery in digital images. The main consideration of this paper was to reduce the dimension of the feature length and find the forged objects in the suspected image. Therefore, we have applied DCT and kernel PCA for feature extraction, which considers the identical objects found in the forged image. Furthermore, this technique does not require any prior information embedded into the image and works in the absence of digital signature or digital watermark. From the results, a conclusion can be drawn which is that the proposed technique not only effectively detects multiple copy-move forgeries and precisely locates the forged areas but also has nice robustness to post processing operations such as Gaussian blurring, AWGN, and compression. Moreover, comparing the detection performance of the proposed technique with existing standard copy-move forgery systems [11]–[14], the results of our technique are reasonably good in terms of average TPR and FPR.

- Copy move forgery type is most commonforgery type used
- Key point forgery detection techniques are better than block based forgery detection techniques
- Non-blind algorithms give more accuracy as compared to blind image forgery detection algorithms
- Use of effective clustering may lead to improved image forgery detection

References:

1. N. Krawetz, “A pictures worth digital image analysis and forensics,”BlackHat Briefings, 2007.
2. S. Lian and Y. Zhang, “Multimedia forensics for detecting forgeries,” in Handbook of Information and Communication Security, pp. 809–828, Springer, New York, NY, USA, 2010.
3. Y. Li, “Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching,” Forensic Science International, vol. 224, no. 1–3, pp. 59–67, 2013.
4. H. Farid, “Digital doctoring: how to tell the real from the fake,” Significance, vol. 3, no. 4, pp. 162–166, 2006.
5. B. B. Zhu, M. D. Swanson, and A. H. Tewfik, “When seeing isn't believing [multimedia authentication technologies],” IEEE Signal Processing Magazine, vol. 21, no. 2, pp. 40–49, 2004.
6. H. Farid, “Image forgery detection: a survey,” IEEE Signal Processing Magazine, vol. 26, no. 2, pp. 16–25, 2009.
7. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, Morgan Kaufmann, Burlington, Mass, USA, 2007.
8. M. A. Qureshi and M. Deriche, “A bibliography of pixel-based blind image forgery detection techniques,” Signal Processing: Image Communication, vol. 39, pp. 46–74, 2015.
9. T. Qazi, K. Hayat, S. U. Khan et al., “Survey on blind image forgery detection,” IET Image Processing, vol. 7, no. 7, pp. 660–670, 2013.
10. T. Mahmood, T. Nawaz, R. Ashraf et al., “A survey on block based copy move image forgery detection techniques,” in Proceedings of the International Conference on Emerging Technologies (ICET '15), pp. 1–6, Peshawar, Pakistan, December 2015.
11. J. Fridrich, D. Soukal, and J. Lukáš, “Detection of copy-move forgery in digital images,”

in Proceedings of Digital Forensic Research Workshop, Cleveland, Ohio, USA, August 2003.

12. S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '09), pp. 1053–1056, April 2009.

13. A.C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Tech. Rep. TR2004-515, Dartmouth College, Hanover, NH, USA, 2004.

14. St´ephaneDerrode and FaouziGhorbel "Robust and efficient Fourier-Mellin transform approximations for gray-level image reconstruction and complete invariant description".

15. Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images," Forensic Science International, vol. 206, no. 1–3, pp. 178–184, 2011.

16. G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in Proceedings of IEEE International Conference on Multimedia and Expo (ICME '07), pp. 1750–1753, IEEE, Beijing, China, 2007.

17. B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants," Forensic Science International, vol. 171, no. 2-3, pp. 180–189, 2007.

18. J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD," Forensic Science International, vol. 233, no. 1–3, pp. 158–166, 2013.

19. G. Lynch, F. Y. Shih, and H.-Y. M. Liao, "An efficient expanding block algorithm for image copy-move forgery detection," Information Sciences, vol. 239, pp. 253–265, 2013.

20. L. Li, S. Li, H. Zhu, S.-C. Chu, J. F. Roddick, and J.-S. Pan, "An efficient scheme for detecting copy-move forged images by local binary patterns," Journal of Information Hiding and Multimedia Signal Processing, vol. 4, no. 1, pp. 46–56, 2013.

21. M. Jaberi, G. Bebis, M. Hussain, and G. Muhammad, "Accurate and robust localization of duplicated region in copy-move image forgery," Machine Vision and Applications, vol. 25, no. 2, pp. 451–475, 2014.

22. L. Li, S. Li, H. Zhu, and X. Wu, "Detecting copy-move forgery under affine transforms for image forensics," Computers and Electrical Engineering, vol. 40, no. 6, pp. 1951–1962, 2014.

23. M. Zandi, A. Mahmoudi-Aznaveh, and A. Mansouri, "Adaptive matching for copy-move Forgery detection," in Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS '14), pp. 119–124, Atlanta, Ga, USA, December 2014.

24. J.-C. Lee, C.-P. Chang, and W.-K. Chen, "Detection of copy-move image forgery using histogram of orientated gradients," Information Sciences, vol. 321, pp. 250–262, 2015.

25. M. Hussain, S. Qasem, G. Bebis, G. Muhammad, H. Aboalsamh, and H. Mathkour, "Evaluation of image forgery detection using multi-scale weber local descriptors," International Journal on Artificial Intelligence Tools, vol. 24, no. 4, Article ID 1540016, 2015.

26. Pooja Bhole, Dipak Wajgi, 2020, An Image Forgery Detection using SIFT-PCA, International Journal of Engineering Research & Technology.

27. Akram Hatem Saber, Mohd Ayyub Khanl, Basim GalebMejbel, 2020, A Survey on Image Forgery Detection Using Different Forensic Approaches, Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 3, 361-370 (2020).

28. Kunj Bihari Meena and Vipin Tyagi, A hybrid copy-move image forgery detection technique based on Fourier-Mellin and scale-invariant feature Transforms, Multimedia Tools and Applications, 2020, DOI: https://doi.org/10.1007/s11042-019-08343-0.
29. A. Kashyap, R. S. Parmar, M. Agrawal, and H. Gupta, "An Evaluation of Digital Image Forgery Detection Approaches," arXiv preprint arXiv:1703.09968, 2017.
30. N. K. Gill, R. Garg, and E. A. Doegar, "A review paper on digital image forgery detection techniques," in Computing, Communication and Networking Technologies (ICCCNT), 2017 8th International Conference on, 2017, pp. 1-7.
31. T. M. Mohammed, J. Bunk, L. Nataraj, J. H. Bappy, A. Flenner, B. Manjunath, et al., "Boosting Image Forgery Detection using Resampling Detection and Copy-move analysis," arXiv preprint arXiv:1802.03154, 2018.
32. O. Mayer and M. C. Stamm, "Accurate and Efficient Image Forgery Detection Using Lateral Chromatic Aberration," IEEE Transactions on Information Forensics and Security, 2018.
33. X. Lin, J.-H. Li, S.-L. Wang, F. Cheng, and X.-S. Huang, "Recent Advances in Passive Digital Image Security Forensics: A Brief Review," Engineering, 2018.
34. Ankit Kumar Jaiswal and Rajeev Srivastava, "Image Splicing Detection using Deep Residual Network," 2nd International Conference on Advanced Computing and Software Engineering (ICACSE-2019).
35. Bin Xiao, Yang Wei, Xiuli Bi, Weisheng Li, andJianfeng Ma, "Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering " Elsevier Information Sciences, 2019.
36. Thuong Le-Tien, Hanh Phan-Xuan, Thuy Nguyen-Chinh, and Thien Do-Tieu, " Image Forgery Detection: A Low Computational-Cost and Effective Data-Driven Model " International Journal of Machine Learning and Computing, Vol. 9, No. 2, April 2019.
37. Giulia Boato, Duc-Tien Dang-Nguyen, and Francesco G. B. Denatale, " Morphological Filter Detector for Image Forensics Applications" IEEE Access 2020.
38. Yaqi Liu, and Xianfeng Zhao, "Constrained Image Splicing Detection and Localization With Attention-Aware Encoder-Decoder and Atrous Convolution" IEEE Access2020.
39. Yuan Rao, Jiangqun Ni, and Huimin Zhao, "Deep Learning Local Descriptor for Image Splicing Detection and Localization" IEEE Access2020.
40. Younis E. Abdalla, M. T. Iqbal, and M. Shehata, Image Forgery Detection Based on Deep Transfer Learning, EJECE, European Journal of Electrical and Computer Engineering Vol. 3, No. 5, September 2019, DOI: http://dx.doi.org/10.24018/ejece.2019.3.5.125.
41. Robin Elizabeth Yancey, Norman Matloff, Paul Thompson, MULTI-STREAM FASTER RCNN WITH ELA FOR IMAGE TAMPERING DETECTION, arXiv:1904.08484v2 [cs.CV] 20 Jun 2019
42. Lin, Cong, et al. "Copy-move forgery detection using combined features and transitive matching." Multimedia Tools and Applications 78.21 (2018): 30081-30096.
43. Wang, Chengyou, Zhi Zhang, and Xiao Zhou. "An image copy-move forgery detection scheme based on akaze and surf features." Symmetry 10.12 (2018): 706.
44. D. Mistry and A. Banerjee, "Comparison of Feature Detection and Matching Approach: SIFT and SURF," GRD Journals- Global Research and Development Journal for Engineering, vol. 2, no. 4, pp. 7-13, 2017.
45. Soad Samir, Eid Emary, Khaled Elsayed, Hoda Onsi, Copy-Move Forgeries Detection and Localization Using Two Levels of Keypoints Extraction, Journal of Computer and Communications, Vol.7 No.9, September 2019, DOI: 10.4236/jcc.2019.79001.
46. Zhang W, Yang Z, Niu S, Wang J. Detection of copy-move forgery in flat region based on feature enhancement. In: Shi Y, Kim H, Perez-Gonzalez F, Liu F, editors. Digital

Forensics and Watermarking, IWDW 2016. Lecture Notes in Computer Science, vol 10082. Springer, Cham; 2017. 2017:159–171.
47. Abdul Warif NB, Abdul Wahab AW, Idna Idris MY, Fazidah Othman RS. SIFT-Symmetry: A robust detection method for copy-move forgery with a reflection attack. J Vis Commun Image Represent, 2017;46:219–232.
48. Divya S. Vidyadharan and Sabu M. Thampi, Digital image forgery detection using compact multi- texture representation, Journal of Intelligent & Fuzzy Systems 32 (2017) 3177–3188 DOI:10.3233/JIFS-169261.
49. Yue Wu, Wael Abd-Almageed, and Prem Natarajan, BusterNet: Detecting Copy-Move Image Forgery with Source/Target Localization, European Conference on Computer Vision, ECCV 2018: Computer Vision – ECCV 2018 pp 170-186.
50. Allu Venkateswara ,Chanamallu Srinivasa , Dharma Raj Cheruku, An Innovative And Efficient Deep Learning Algorithm For Copy Move Forgery Detection In Digital Images, International Journal of Advanced Science and Technology Vol. 29, No. 05, (2020), pp. 10531 – 10542.

Mr. Jaynesh Desai
[Asst. Prof., Bhagwan Mahavir
College of Computer Application, BMU SURAT]
Dr. Sanjay Buch
[Dean, Bhagwan Mahavir
College of Computer Application, BMU SURAT]