IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-12 E-ISSN: 2347-2693

A New Approach of copy move Forgery Detection using Rigorous Preprocessing and Feature Extraction Imulation Based Exploration

A.K. Chakraverti[1*] and V. Dhir[2]

[1*]RIC (Computer Science and Engineering), IKG-Punjab Technical University, Jalandhar, India
[2] Department of Computer Science and Engineering, M.K. Group of Institution, Amritsar, India

[*]*Corresponding Author: ashish.me08@gmail.com, Tel.: +91-9717978667*

Available online at: www.ijcseonline.org

Received: 17/Nov/2017, Revised: 29/Nov/2017, Accepted: 15/Dec/2017, Published: 31/Dec/2017

Abstract— these days, advanced pictures are being used in an extensive variety of uses and for numerous reasons. They additionally assume an imperative part in the capacity and exchange of visual data, particularly the mystery ones. With this far reaching utilization of advanced pictures, notwithstanding the expanding number of devices and programming of computerized pictures altering, it has turned out to be anything but difficult to control and change the real data of the picture. In this way, it has turned out to be important to check the credibility and the respectability of the picture by utilizing present day and advanced methods, which add to examination and comprehension of the pictures' substance, and after that ensure their trustworthiness. There are many sorts of picture imitation, the most critical and prominent sort is called duplicate glue fabrication, which utilizes a similar picture during the time spent falsification. This sort of fraud is utilized for one of two things, first to cover a protest or scene by replicating the region of the picture and gluing it on another zone of a similar picture. In this paper we have presented a new approach of copy move forgery detection. proposed scheme uses Oriented FAST and rotated BRIEF(ORB) alternative of scale invariant feature transform (SIFT) technique which is integrated with modified local contrast modification-contrast limited adaptive histogram equalization(LCM-CLAHE). Experimental results shows that proposed scheme is more promising in terms of false positive rate(FPR) and true positive rate(TPR) compare to state of the art techniques.

Keywords— Image Processing, Image Enhancement, Histogram Equalization, SIFT, TPR, FPR, Copy move forgery, ORB

I. INTRODUCTION

In this Digital era, Photographs are most dominant and dependable media for exchanging thoughts, emotions or message. Each and every state of affairs or scenario can e reflected even with only a single image. Digital image alteration and manipulation tool are now very advance now days and are being developed very fast for last few years. Image manipulation software is available either at nominal rate or free of cost [5]. Digital image forgery is the amendment of an digital image available in any format. Growing advancements in the photo editing soft-wares and technology of image capturing devices have provided the easy way to forge the images. Among all available image forgery technique Copy move forgery is the most common image forgery [6]. Digital image forensics is a stream that analyzes images of a exacting scenario, in order to establish the trustworthiness and genuineness (or otherwise), through a variety of means. It is attractive and a popular field because of its prospective applications in many domains like intelligence, sports, law firm, news preparation, medical imaging and insurance claim investigations. With the ever rising reliance on digital media, the need to ensure its genuineness and trustworthiness is of vital importance. The formation and manipulation of digital images, with no clear tampering, is becoming easier with each passing day [7]. Conventional copy move forgery detection methods for digital images are mainly focused on finding of duplicate regions in an image. In the area of digital image forensics we have seen lot of research progression since last decade, where by the examination for possible forgeries is solely based on post-processing of images [15].

Histogram equalization (HE) is the most fundamental and popular technique of pre-processing and key feature enhancement. This technique is used to enhance the contrast of image to analyze the image efficiently. Digital image forensic, medical image processing and satellite data processing deals with image feature enhancement for better analysis.

There are two classes of Digital image forensics: first active approach and second passive approach. In the active approach, a digital watermark or signature verifies the integrity and validity of digital images. A watermark or signature is embedded into the image while it is acquired, and any spiteful tampering of the image can be detected through examination of the value of a digital watermark or

signature. However, a most important shortcoming is that the digital imprison devices do not contain the unit to insert watermarks or signatures. To conquer this problem, passive approaches which do not need any previous information about image to notice traces of tampering [11].

Sunil V. Dahale et. al.[26] proposed a image retrieval method based on colour histogram by using fuzzy logic inference system. This method may also provide some room for research in area of feature extraction.

The preliminary objective of the SIFT method is to evaluate two images (or two image parts) that can be deduced from each other (or from a common one) by a rotation, a translation, and a zoom. The process turned out to be also robust to great enough changes in view point angle, which explains its achievement. In this method, following a classical model, stable points of interest is thought to lie at extrema of the Laplacian of the image in the image scale-space illustration [1, 2]. Counterfeit detection can be done by two method block method [3, 4] and key point attribute extraction method [12].

Original Images Copy move forged images

Figure 1: Some example images of CoMoFoD[25]

In our work we have found that most of the copy move forgery technique does not give attention to pre-processing of images for forgery detection purpose. In our research work we have applied rigorous pre-processing using modified LCM CLAHE and then applied the SIFT to detect the localization. We have break rest of our manuscript as follows. Section 2 contains the examination of existing conventional technique. In section 3 we presented our method to improve copy move forgery detection technique. Section 4 has the detail about planned method and related algorithms. Implementation, Experiment and results are elaborated in section 5. Finally we have compiled our conclusion and possible potential work in this area in section 6.

II. RELATED WORK

In one of the great finding in this area, Luca DAmiano et al. [8] given a method to recognition and localization of copy-move forgeries. To reliably detect both additive and occlusive copy moves author uses a dense-field approach, with invariant features that guarantee robustness to several post-processing operations. Mahmoud Emam et.al.[9] propose a robust region duplication forgery detection method based on extracting local extrema points from Difference of Gaussians (DoG) operator. As per author he uses DoG because it is a good approximation for the Laplacian of Gaussian (LoG) and much faster to calculate. By author to extract the descriptive features and hence improve the matching performance, Multi-support Region Order-based Gradient Histogram (MROGH) descriptor is adopted.

Mona F. Mohamed Mursi et. al. [10] proposed a blind copy-move tampering detection and localization method. As per author statement its novelty lies in the combination of SIFT, PCA and DBSCAN techniques. As per author the proposed method shows its potential to disclose and localize tampered regions of different sizes and shapes. Furthermore, as per author, method requires no prior information about the image or the manipulation operations carried on it.

Nor Bakiah Abd. Warif et. al.[12] presented a new method by combining Scale Invariant Feature Transform (SIFT)-based CMF recognition method and symmetry-based identical both at once as a robust CMF detection method, called SIFT-Symmetry. In the rigorous evaluation process of this method authors found that their method is more productive in comparison of conventional methods those are based on SIFT, multi-scale analysis, and patch matching. Author uses two new datasets covering simple alteration and reflection based attacks.

Rajan CRISTIN & Velankanni CYRIL RAJ [13] developed a new method that uses a feature based neural network to detect the image counterfeit either in reflection or shadow. In author's projected method of image counterfeit detection, three essential steps are used first segmentation, second feature mining and third detection. Map-based segmentation and Fuzzy c-Mean (FCM) clustering is used to

identify mirror image point and shade points in segmentation step. After that LVP operator is used to extract feature point from reflective and shade part of image considering texture consistency and strength stability. In final step Artificial Bee Colony and Levenberg-Marquardt (ABCLM) is design to detect forgery by using feed forward neural network. ABCLM is used for training of neural network weights.

Rahul Dixit et.al.[16] presented a new advancement for revealing of copy-move forgery using stationary wavelet transform (SWT) which, is shift invariant, in contrast of most wavelet transforms (e.g. discrete wavelet transform), , and helps in investigating the similarities, i.e. matches and differences, i.e. noise, between the blocks of an image, in result of blurring. In author's method the blocks are constructed by features extracted using singular value decomposition (SVD) of an image. Also, the concept of colour-based segmentation used in this work provides easyness to achieve blur invariance. Sundus Farooq et. al.[17] propose a scheme for the detection of multiple types of image forgeries. In this research author proposed a generic passive image forgery scheme using spatial rich model (SRM) in blend with textural feature i.e. local binary pattern (LBP). Moreover, different sub-model selection strategies are implemented and analyzed to investigate the performance-to-model dimensionality trade-off. Ensemble multi-class classifier is used for classifying the features into different forgery classes.

Somayeh Sadeghi et. al. [18] suggested SIFT based technique to detect copy-move counterfeit in digital image as a successful technique. The planned technique will correctly attest digital image and find group of pixel that are forged with. The formula starts by victimization SIFT to take out native image options that are called key points, so searches for similar key points supported their geometrician distances. At last, the harmonized key points, that signify the derived and glued areas, are related to one and an additional to point that elements of the image are counterfeit with. Author verified and validated his method in terms of usefulness against different attack. In this experiment author also enumerated its power against post processing.

Toqeer Mahmood et. al. [19] developed an economical method to detect copy move forgery based on associative degree. Authors have taken the help of native binary pattern variance (LBPV) over the less calculated elements of the stationary wavelets. In this method author tackle the possible post-processing operations. This CMFD method is applied over the circular regions. Author has used CoMoFoD and kodak lossless true color image (KLTCI) data sets. Author have examined proposed method in presence of different post processing attack like flipping blurring, scaling. Color diminution, and manifold forged region in image.

V. T. Manu and B. M. Mehtre [20] developed a method by conservation of affine transformation property of clustering feature point of image. These property conservation involves test for co-linearity and distance ration. Author claimed that their technique ia also capable to analyze the image having multiple copy-move forged regions.

V. Thirunavukkarasu et. al. [21] has used DSWT and MDS to develop a powerful non-intrusive forensic analysis technique. DSWT and MDS are attribute descriptor. These descriptors can routinely recognize the copy move forged area even in absence of image content property. Very few features are used by this algorithm to describe all blocks. In outcome of proposed method author shows that this technique can discover forged areas which are very small and no regular. This method can also multiple tampered region as well as forged area distorted by irregular average filter blurring, brightness and color decline in different level.

Xiuli Bi, and Chi-Man Pun [22] proposed another and quick intelligent balance subordinate searching technique down picture duplicate move fake recognition. Amid the instatement organize, the traits are separated and haphazardly relegated highlight correspondences to get the early mapping balances. In the seeking stage, the sagacious balances are registered to estimate whether the mapping balances are duplicate move fraud mapping balances. At that point, the proposed need based trademark coordinating to quickly spread the duplicate move imitation mapping counterbalances and upgrade the mapping and canny balances. At long last, just a couple of emphases can recognize the fake districts totally from the mapping balances.

Yuecong Lai et. al.[23] proposed an enhanced block-based matching algorithm (IBMA) to solve the this problem. At first, creator put the aggregate of highlight vectors in the main segment to get another grid. Besides, the grid substance of framework is arranged according to the substance of first section. At long last, every line of the framework will investigate the accompanying lines until the point that the qualification in the primary segment is bigger than the limit esteem.

ZHAO Fei et. al. [24] proposed a successful strategy in light of picture division and swarm intelligence (SI) calculation. In this procedure creator sectioned picture into little non-covering squares. An estimation of even degree is given for each square. Test picture is divided into independent layers as per the smooth degree. SI calculation is connected in choice the ideal location parameters for each

layer. These parameters are utilized to recognize each layer by scale invariant highlights change (SIFT)- based plan, which can find an aggregation of key points.

In exhaustive literature survey we found that very few researchers have considered the pre-processing as critical step in copy move forgery detection techniques. In our research work we have pre-processed the image to de-noise and then we have applied feature based copy move forgery technique. For feature based techniques we have used Binary Robust Independent Elementary Features (BRIEF) and Oriented FAST and rotated BRIEF (ORB) because SIFT and SURF are patented and paid services. BRIEF and ORB are alternative of SIFT and SURF.

III. METHODOLOGY

A. Proposed LCM CLAHE for pre-processing

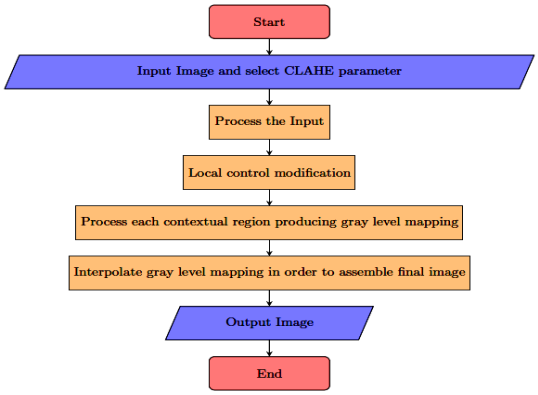

Figure 2: Operational Flow Chart of CLAHE

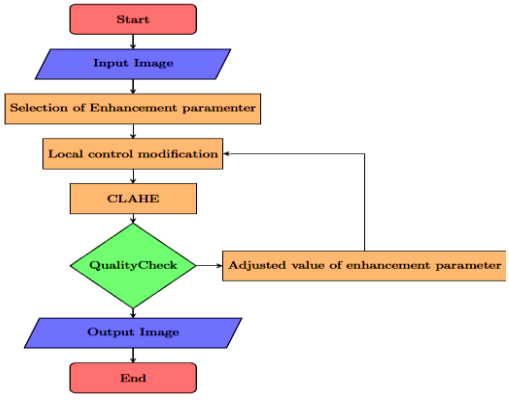

Figure 3: Operational Flow Chart of LCM-CLAHE

In this section we present details of proposed method of HE for de-noising non monotonous image. Image categories taken for the experiments are shown in Fig 1[25]. Fig 2 and Fig 3 show the CLAHE and LCM-CLAHE operation flow chart.

B. Selection of enhancement parameter in pre-processing step

This step involves the selection of parameter of image to be enhanced like contrast, brightness etc. here in our example we have taken contrast as enhancement parameter. In image processing contrast enhancement is very common operation and it is very use full to process scientific images like satellite images and X-rays images. This is also use full in forgery detection where images are enhanced to improve the details up to desired level. HE is one of the most common method to enhance the contrast.

C. Local contrast modification

In this step local contrast enhancement on input image is applied. The function [14] of this step is designed in such a way that it takes global and local information both to produce the enhanced image. Transformation functions are as follows.

$$T = \frac{E * M}{\sigma} \quad (1)$$

$$g = T * (f - m) + m \quad (2)$$

Where f and g are input image and LCM enhanced image correspondingly. E is enhancement parameter; M and m are global and local mean of image respectively. Now here we have presented the expression for local mean and standard deviation for the user defined local window of size n * n.

$$m(x,y) = \frac{1}{n*n} \sum_{x=0}^{n-1} \sum_{y=0}^{n-1} f(x,y) \quad (3)$$

$$\sigma = \sqrt{\frac{1}{n*n} \sum_{x=0}^{n-1} \sum_{y=0}^{n-1} \left(f(x,y) - m(x,y)\right)^2} \quad (4)$$

After the calculation of local mean m and standard deviation σ from equation 3 and 4 for all windows defined by user, average of these values is used to get the finer details of image by equation 1 and 2. Image with finer details is given as input to modified CLAHE which will use LCM-CLAHE to optimize the contrast of image up to threshold value during HE.

D. Pre-process image up to threshold contrast by using LCM-CLAHE

In our research work we found very interesting fact that there a remarkable relationship between contrast and copy

move forgery detection. We first pre-process the image up to desired contrast then applied copy move forgery detection.

E. Algorithm

We have named proposed method as adaptive copy move forgery detection since it uses varying contrast. Contrast in our proposed method is not fixed for all images. These are decided on the basis of categories of images based on feature distribution and noise. Algorithmic representation of proposed method is given as follows.

Result: HE Image
Inputs: Fine detailed image from LCM, Enhancing parameter ;
begin;
Step1: Obtain inputs like number of regions, dynamic range and clip limit;
Step2: Calculate threshold contrast;
Step3: Process the inputs;
Step4: Process each contextual region producing gray level mapping ;
Step5: Interpolate gray level mapping in order to assemble final image;
end;

Algorithm 1: LCM-CLAHE

F. Applying ORB

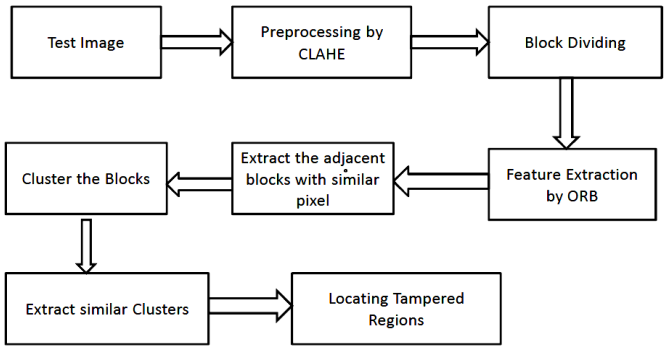

Figure 4: Flow Graph of proposed method

Relevant details should be given including experimental design and the technique (s) used along with appropriate statistical methods used clearly along with the year of experimentation (field and laboratory).

IV. Results and Discussion

We have implemented our proposed method in Python 3.6 and Image packages of Python like skimage, opencv and other science packages, ubuntu 16 operated on i3 core system as hardware platform. We have used CoMoFoD [25] database for evaluation of proposed scheme. Experimental results show the promising improvements in compassion of state of the art techniques. Performance comparison is done on the basis of TPR, FPR, and F_score.

$$TPR=(imgfd/imgf) \quad \textbf{(5)}$$

$$FPR=(imgod/imgo) \quad \textbf{(6)}$$

$$F\_score=(TPR/(TPR+FPR))*100 \quad \textbf{(7)}$$

Where imgfd=images detected as forged being forged
imgf=number of forged images
imgod=images detected as forged being original
imgo=original images

Table 1: Detection results of the proposed method and state of art method using 1000 images from CoMoFoD[25] data base.

S.NO.	Methods	TPR%	FPR%	F_score%
1	Nor Bakiah Abd, et.al. [12]	91.20	7.12	92.75
2	Somayeh Sadeghi, et.al.[18]	98.15	8.15	92.33
3	V. T. Manu1, and B. M. Mehtre [20]	95.65	6.14	93.96
4	Proposed Method	99.25	6.00	94.29

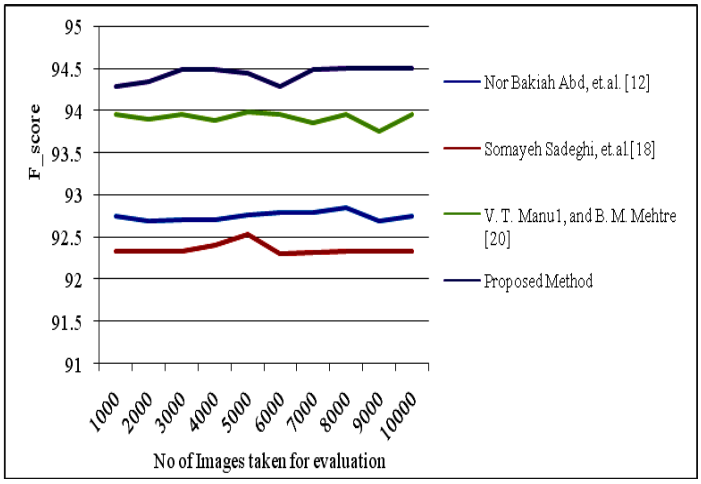

Figure 5: Graph showing performance of proposed method

A. Improvements

As we have promised in section of proposed method for remarkable improvements in F_score. So it is clear from performance comparison table Table 1, Fig 5 shows the rigorous evaluation evidence for improvement in proposed method that our proposed method has remarkable positive

improvements. Existing techniques[12, 18, 20] have F_scores 92.75, 92.33, and 93.96 respectively. Our proposed method shows 94.29 F_score. More F_score promise robust detection technique.

V. CONCLUSION and Future Scope

In our research work, we aimed to developed a new approach of copy move forgery detection and have developed it, and same is presented in this paper. Our method is based on integration of pre-processing and feature extraction and rigorous pre-processing of image before applying detection method. In our experiment we have evaluated our proposed method by using CoMoFoD image data base. Results show promising improvement in terms of TPR, FPR, and F-score. In our experiment we have compare three states of art techniques [12, 18, 20]. Our method shows better performance in comparison of these state of art techniques.

In future this research may be carried forward towards making automatic detection of image forgery that depends on feature of input image and use of proposed method in pre-processing phase of copy move forgery detection to improve the performance of state of art techniques.

VI. REFERENCES

[1] J. M. Morel and G. Yu. "On the consistency of the SIFT *Method"*. Lecture notes, August 11, 2008.

[2] D. G. Lowe. *"Distinctive image features from scale-invariant keypoints"*. International Journal of Computer Vision, 60, 2, pp. 91-110, 2004.

[3] A. C. Popescu and H. Farid. *"Exposing Digital Forgeries by Detecting Duplicated Image Regions"*. 6211 Sudikoff Lab, Computer Science Department, Dartmouth College, Hanover, NH 03755 USA.

[4] J. Fridrich, D. Soukal, and J. Luk. *"Detection of Copy-Move Forgery in Digital Images"*. Department of Electrical and Computer Engineering, b Department of Computer Science SUNY Binghamton, Binghamton, NY 13902-6000

[5] J. Yaduwanshi, and P. Bansal. *"A Novel Approach for Copy Move Forgery Detection Using Template Matching"*. Proceedings of International Conference on Communication and Networks, Advances in Intelligent Systems and Computing 508, India,Springer Nature Singapore Pte Ltd., pp. 711-721, 2017, DOI 10.1007/978-981-10-2750-5 72.

[6] K. Sachdev, M. Kaur, and S. Gupta. *"A Robust and Fast Technique to Detect Copy Move Forgery in Digital Images Using SLIC Segmentation and SURF Keypoints"*. Proceeding of International Con-ference on Intelligent Communication, Control and Devices, Advances in Intelligent Systems and Computing 479, Springer Science+Business Media Singapore, pp. 787-793, 2017, DOI 10.1007/978-981-10-1708-7 91.

[7] K. Hayat, and T. Qazi. *"Forgery detection in digital images via discrete wavelet and discrete cosine transforms"*. Computers and Electrical Engineering 0 0 0 (2017) 111, 2017.

[8] L. D. Amiano, D. Cozzolino, G. Poggi, and L. Ver-doliva. *"A PatchMatch-based Dense-field Algorithm for Video Copy-Move Detection and Localization"*. Cornell University Library,2017, arXiv:1703.04636v1 [cs.CV].

[9] M. Emam, Q. Han, Q. Li, H. Zhang, and M. Emam. *"A Robust Detection Algorithm for Image Copy-Move Forgery in Smooth Regions"*. International Conference on Circuits, System and Simulation (ICCSS),London, UK, IEEE, 2017, DOI: 10.1109/CIRSYS-SIM.2017.8023194 .

[10] M. F. Mohamed Mursi, M. M. Salama, and Md. 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, pp. 23-28, 2017.

[11] N. Kaur. *"A Review Paper on Copy Move Forgery Detection Techniques"*. International Journal of Advanced Research in Computer Science,Volume 8, No. 7, pp. 157-161, 2017. DOI:10.26483/ijarcs.v8i7.4146.

[12] N. B. Abd. Warif, A. Wahid, Mohd. Y. I. Idris, R. Salleh,and F. Othman. *"SIFT-Symmetry: A Robust Detection Method for Copy-Move Forgery with Reflection Attack"*. J. Vis. Commun. Image R., 2017, DOI: 10.1016/j.jvcir.2017.04.004.

[13] R. CRISTIN, and V. CYRIL RAJ. *"Consistency features and fuzzy-based segmentation for shadow and reflection detection in digital image forgery"*. SCIENCE CHINA Information Sciences, Vol. 60 082101:1082101:18, 2017, DOI: 10.1007/s11432-016-0478-y.

[14] S. Mohan and M. Ravishankar. *"Modified Contrast Limited Adaptive Histogram Equalization BAsed on Local Contrast Enhancement for Mammogram Image"*. In: Das V.V., Chaba Y. (eds) Mobile Com-munication and Power Engineering. Communications in Computer and Information Science, vol 296. Springer, Berlin, Heidelberg , pp 397-403, 2013

[15] R. Dixit, and R. Naskar. *"Review, analysis and parameterisa-tion of techniques for copymove forgery detection in digital images"*. IET Image Processing, 2017, DOI: 10.1049/iet-ipr.2016.0322.

[16] R. Dixit, R. Naskar, and Swati Mishra. *"Blur-invariant copy-move forgery detection technique with improved detection accuracy utilising SWT-SVD"*. IET Image Processing, 2017, DOI: 10.1049/iet-ipr.2016.0537.

[17] S. Farooq, M. Haroon Yousaf, and F. Hussain. *"A generic passive image forgery detection scheme using local binary pattern with rich models"*. Computers and Electrical Engineering 0 0 0 (2017), pp. 114, 2017, DOI: 10.1016/j.compeleceng.2017.05.008.

[18] S. Sadeghi, H. A. Jalab, K. Wong, D. Uliyan, and S. Dadkhah. *"KEYPOINT BASED AUTHENTICATION AND LOCALIZATION OF COPY-MOVE FORGERY IN DIGITAL IMAGE"*. Malaysian Journal of Computer Science. Vol. 30(2), pp. 117-133, 2017.

[19] T. Mahmood, A. Irtaza, Z. Mehmood, and Md. T. Mahmood. *"Copy-move forgery detection through stationary wavelets and local binary pattern variance for forensic analysis in digital images"*. Forensic Science International, DOI:10.1016/j.forsciint.2017.07.037.

[20] V. T. Manu, and B. M. Mehtre. *"Copy-move tampering detection using affine transformation property preservation on clustered keypoints"*. SIViP, 2017, DOI 10.1007/s11760-017-1191-7.

[21] V. Thirunavukkarasu, J. S. Kumar, G. S. Chae, and J. Kishorkumar. *"Non-intrusive Forensic Detection Method Using DSWT with Reduced Feature Set for Copy-Move Image Tampering"*. Wireless Pers Commun, 2017, DOI 10.1007/s11277-016-3941-1.

[22] X. Bi , and C. Pun. *"Fast Reflective Offset-Guided Searching Method for Copy-Move Forgery Detection"*. Information Sciences, 2017, DOI: 10.1016/j.ins.2017.08.044.

[23] Y. Lai, T. Huang, and J. Lin H. Lu. *"An improved block-based matching algorithm of copy-move forgery detection"*. Multimedia Tools Appl, 2017, DOI 10.1007/s11042-017-5094-y.

[24] Z. Fei, S. Wenchang, Q. Bo, and L. Bin. *"Image Forgery Detection Using Segmentation and Swarm Intelligent Algorithm"*.

Wuhan University Journal of Natural Sciences, Vol.22 No.2, pp. 141-148, 2017.

[25] D.Tralic , I. Zupancic , S. Grgic, and M. Grgic. *CoMoFoD - New Database for Copy-Move Forgery Detection"*. in Proc. 55th International Symposium ELMAR-2013, pp. 49-54, September 2013

[26] Dahale Sunil V, Thorat S.B., P.K. Butey, and M.P. Dhore. "*Efficient Content Based Image Retrieval Using Fuzzy Approach*". International Journal of Computer Sciences and Engineering, Volume-5, Issue-10, pp. 38-43, 2017.

Authors Profile

Mr. Ashish Kumar Chakraverti pursued Bachelor of Technology from IEC College of Engineering and Technology, Greater Noida UP india in 2005 and Master of Technology from RGPV Bhopal MP India in year 2010. He is currently pursuing Ph.D from IKG-PTU Jalandhar Punjab India, and currently working as Assistant Professor in Department of CSE , IEC College of Engineering and Technology, Greater Noida UP since 2015. He is a member of IEEE & IEEE computer society since 2013, ACM since 2014. He has published more than 10 research papers in reputed international journals including Thomson Reuters (ESCI & Web of Science) and conferences including IEEE and it's also available online. His main research work focuses on Big Data Analytics, Image Processing, Digital Forencics and Parallel Computing. He has 12 years of teaching experience and 2 years of research experience.

Dr Vijay Dhir pursued Bachelor of Technology, Master of Technology, and PhD from PTU Jalandhar. He is member of board of study in department of CSE IGK-PTU, Jalanadhar. He is a member of IEEE & IEEE computer society since 2009, ACM since 2010. He has published more than 50 research papers in reputed international journals including Thomson Reuters (ESCI & Web of Science) and conferences including IEEE and it's also available online. His main research work focuses on Big Data Analytics, Image Processing, Digital Forencics and Parallel Computing. He has 17 years of teaching experience and 3 years of research experience.

