Study and Analysis of Copy-Move Forgery Detection in Digital Image: A Review

Rachana[1], Ashok Kumar[2], H.L.Mandoria[3], Binay Pandey[4]

[1]M.Tech Student, Dept. of Information Technology
G. B. Pant University of Agriculture & Technology, Pantnagar, India
[2, 4] Assistant Professor, Department of Information Technology
G. B. Pant University of Agriculture & Technology, Pantnagar, India
[3] Professor and Head of Information Technology
G. B. Pant University of Agriculture & Technology, Pantnagar, India

---***---

Abstract - *In today's digital age, Digital image forgery becomes a common information falsification trend. This is generally done due to the largely available contemporary editing software and superior digital cameras. Authenticity of images becomes a more imperative issue while transferring data from one place to another place. Trustworthiness of photograph has a significant role in many areas - forensic investigation, criminal investigation, surveillance system, intelligent system, medical imaging and Journalism. Digital Image forensics finds the authenticity of the images. Different techniques are used to create forgery in the digital image. More regular type of digital image forgery is copy move forgery in which a part of an image itself is one copied and pasted into another location of the same image to conceal or alter the meaning. Post processing operations like resizing, blurring, rotation, JPEG compression etc has been done which makes digital image forgery detection difficult and hence an efficient approach is needed to detect the forgery into digital images. Copy Move forgery detection technique is grouped into two methods: Block based and Key Point based. In this paper, we have presented the various block based copy move forgery detection techniques. Image forensics is a fast growing research field and promises a convincing improvement in forgery detection.*

***Key Words*: Digital image, Digital Image Forgery, Copy-move forgery, Authenticity, Block-based methods.**

1. INTRODUCTION

Digital images in the current era play very important role in various fields. They are used in different applications in the area of military, news, medical diagnosis and media. Due to the development in technology of digital image, for example, cameras, software, and computers and the wide spread via the internet, digital image can be considered a premier source of information this time. With the enrichment of technology and availability of low-cost hardware and software editing tools, it is not crucial to change or forge the digital images without any visible traces [9]. Digital image forgery and manipulation of digital images in many cases is to intentionally affect the awareness of the recipient. In this situation Digital image forgery detection plays an important role in image forensics to provide authenticity of the image. There are many detection techniques are classified into two approaches [11] as shown in (figure 1): a) active; and b) passive techniques.

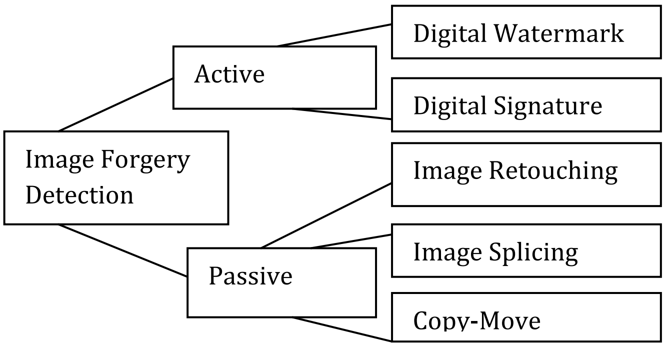
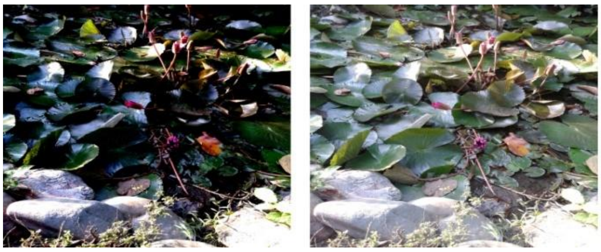


Figure 1: Image Forgery classification

For authenticity of a digital image, digital watermarking and digital signature have been proposed which are known as active techniques. In the active approach require some pre-processing operations, like attaching watermark and signature when producing digital images, thus limiting their applications in practice [14] not like the watermark and signature-based method, the passive techniques does not require any digital signature to be generated or to be inserted any watermark.

Passive authentication is the procedure of authenticating digital images without using any auxiliary information apart from the pictures themselves. Passive approaches are further grouped into two categories: 1) source device identification; and 2) tamper detection. Source device identification: It is based on identifying camera fingerprints, which are the clues that are left by the image acquisition steps and the storage phases. Tamper detection: Tamper detection approaches are devised for particular types of forgeries, like copy-move or image splicing [26].

Image Retouching: It can be treated to be the less harmful/fatal kind of digital image forgery. Image retouching does not greatly transform or alter an image, but instead, enhances (or reduces) feature of an image. (Figure2)[10] Shows image retouching, and the difference between left image and right images (enhanced) clearly.



(a)Original Image (b) Image Retouching

Figure 2: Image Retouching

Image Splicing: This is another type of forgery. Image splicing is an approach that involves a composition of two or more images which are joined together to create a forgery as shown in (figure3) [17].This type of forgery is executed carefully; the border between the spliced regions can be hardly optically noticeable.

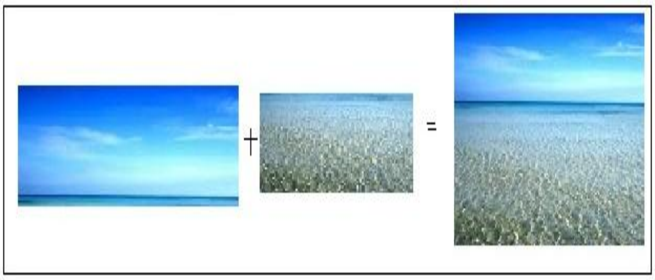
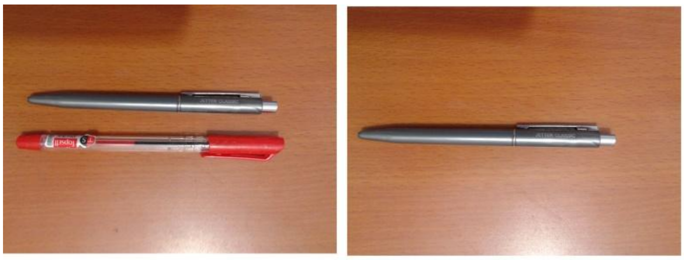


Figure 3: Image Splicing

Copy Move Forgery: Copy move forgery is more or less alike to image splicing. In this type of image forgery a part of an image itself is copied, moved to a desired location and pasted within the same image. (Figure 4) shows a red pen has been removed from the original image in part (a), by covering some of the region by background of the same image to produce forged image (b) [4]. There are many types of copy move forgery as follows: 1) just Copy-move;2) Copy-move with reflection; 3) Copy-move with different scaling; and 4) Copy-move with rotation[21].



(a) Original Image (b)Forged Image (Copy-Move)

Figure 4: Copy –Move Forgery

From the literature survey, copy move forgery detection techniques is further grouped into two methods as shown in (figure5): 1) Block based Method; and 2) Key point based Method

Block based Methods:

In Block based method divide the input image into overlapping or non-overlapping blocks of equal size. Then the feature is calculated for each block in order to detect duplicated regions. And matching is done to detect duplicated region in the image [21, 22].

Key Point-based Method:

Key point-based methods operate on whole image. Instead block based methods, Key point based methods compute their features only on image regions with high entropy. Key point based method can be further classified into two methods: SIFT (scale invariant feature transform) and 2) SURF (SpeededUp Robust Features) methods. [5, 3, 22]

2. GENERAL WORKFLOW OF COPY MOVE FORGERY DETECTION

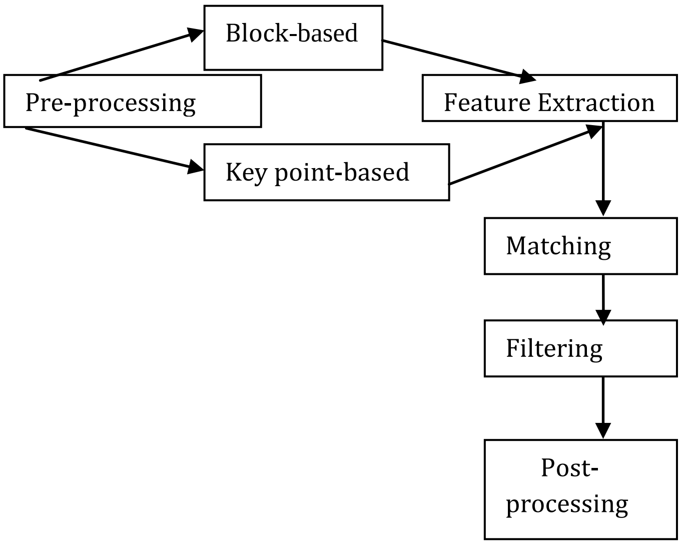


Figure 5: General Copy Move Forgery Detection

2.1 EXISTIN BLOCK BASED IMAGE FORGERY DETECTION TECHNIQUES

A large number of techniques have been proposed for detecting copy move forgery. A typical procedure has been followed as shown in figure 5.Copy Move Forgery Detection method can either block based and keypoint based approach. In block based approach, Most of the time in block based method needs gray scale images so the RGB image is first converted into a gray-scale image. For feature extraction, this gray scale image is divided into non overlapping/overlapping block of same size. From each block, a unique representation as a feature vector is computed. And then detect the copy move forgery by looking for the similar blocks [31].

Fridrich et. al [4] first analyzed the exhaustive search and then suggested a block matching method to espy copy move forgery. This method was based on Discrete Cosine transformation (DCT). Lexicographic Sorting is used and neighboring blocks are taken as possibly forged area. Thus these considered neighbor region are compared in the matching step .This technique in some complicated manipulation techniques like blurring or random noise addition it is not easy task to detect the forgery.

To make the computation faster, Popescu et. al [1] proposed a method based on Principal Component analysis (PCA).Due to the characteristics of PCA the number of features required to present a block were reduced as the half of the numbers of the features used by Fridrich. But this method is not robust to enough adequate small rotation of duplicated regions.

Li et. al [5] proposed a method based on (Discrete Wavelet transform) and Singular Value Decomposition (SVD). Discrete Wavelet Transformation (DWT) has been used to low frequency coefficients to reduce the feature vector representation and then SVD is applied on each sub blocks of low energy coefficient. This method works well even if the image is extremely compressed.

Myna et al. [2] proposed a method based on log-polar coordinate and Discrete Wavelet Transform (DWT). For the dimension reduction DWT is applied on the input image. And then sub blocks of the images are mapped on the log-polar coordinate to acquire a matrix corresponding to each block. Lexicography sorting is used to bring similar rows closer. Phase correlation was employed for similarity criterion. This method has lower time complexity. but not robust against geometric operation.

Q.Wu and S.Wang [26] attempted to make robust against post processing operation like scaling and rotation. Method was based on log-polar Fast Fourier Transformation (LPFFT).

Mohamadian and Pouyan [15] proposed a new method of detecting copy move forgery which is based on SIFT (scale invariant feature transform) algorithm along with the Zernike Moments. SIFT algorithm is used to perform detection but cannot detect flat copied region. To resolve this issue Zernike moments are used.

A method proposed by Bayram et al. [3] was based on Fourier-Mellin Transformation (FMT). By employing FMT on overlapping blocks of images, Features are extracted. These obtained features are robust to rotation and scaling, blurring, noise addition and JPEG compression. Lexicography sorting is used to neighboring the alike block and Counter bloom filter are used inspite of lexicography sorting to compare the blocks.

S.-jin Ryu and M.-jeong Lee [27] Zernike moments based detection approaches the flat copied region is detected and also invariant to different operations like JPEG compression, rotation, blurring and AWGN. The algorithm exhibited robustness against different degrees of rotation and high detection rate but not for the scaling.

Muhammad et al.[16] proposed a method based on Dyadic Wavelet Transform (DyWT) . Due to the characteristics of DyWT (shift invariant) is used. So, it is more applicable than discrete wavelet transform (DWT) for data analysis. In this method, decomposes the input image into approximation (LL1) and detail (HH1) subbands. Further those subbands(LL1 and HH1) are divided into overlapping blocks and after that measure the similarity between blocks. A method based on Dyadic Wavelet Transform (DyWT) in which both the LL and HH sub bands are used to find the similarity between the blocks of image.

Later on, same author Muhammad et al. [14] proposed a method to detect copy move forgery was based on undecimated wavelets and Zernike moments. UWT is translation invariant, although Zernike moments are scale and rotation invariant. Firstly undecimated wavelet transform is applied to find its approximation. After that Zernike Moments are calculated from the approximation. To find similarity of the moments between the blocks of image Euclidean distance is used. This algorithm is robust against different degree of rotation and high detection rate but not for the scaling.

A method to detect copy-move forgery using Discrete Wavelet Transform (DWT) and Principal Component Analysis-Eigenvalue Decomposition (PCA-EVD) is proposed by M. Zimba and S. Xingming [18]. DWT is applied on the image to reduce the size and obtained the low approximation coefficients. Principal component analysis to yield a reduced dimension representation .This technique accurately detects such specific image manipulations as long as the copied region is not rotated or scaled. Later on, by the same author [19] a fast and robust approach is presented to detect copy move forgery. This method is based on block characteristics of DWT coefficients. Fixed window is then move over the sub-band, pixel-by-pixel, and a feature vector is obtained at each location. Thus these obtained Feature vectors, are sorted using radix sort. This method is robust to JPEG compression, noise addition and rotation through some fixed angles, the algorithm has good precision ration in detection of copy move forgery.

A method based on Discrete Wavelet Transform (DWT) and Kernel Principal Component Analysis (KPCA) is proposed by Bashar et al. [20]. In this method input image is splited into small overlapping blocks. Each block of input imge is transformed by DWT or KPCA. DWT is applied on the image to minimize the size and obtained the low approximation coefficients. KPCA is used for feature collection and lexicographic sorting is used to cluster the alike feature blocks. This method is robust to manipulations such as translation-flip and translation-rotation of duplicate region

Yanping Huang et al. [34] An improved DCT-based method is developed to detect copy move forgery. Firstly, Discrete Cosine Transformation (DCT) is applied on fixed-size overlapping blocks of input image.DCT coefficient are obtained from each block to represent its features. To reduce the dimension of the features, Truncation is performed. Lexicography sorting is performed on calculated feature vectors. Duplicated region blocks are compared in the matching step. This improved DCT-based method is able to detect the duplicated regions even when suspected image was deformed by JPEG compression, blurring or additive white Gaussian noise.

Y. Cao and T. Gao [33] Firstly, Input image is divided into fixed-size blocks, and discrete cosine transform (DCT) is employed to each block, thus, the DCT coefficients is obtained for each block. Secondly, each cosine transformed block is presented by a circle block and four features are calculated to minimize the dimension. After that, Lexicography is used to sort the feature vectors, and duplicated region in the image is matched by predefined shift frequency threshold. The technique not only minimize the feature length but showed robustness against detection of multiple copy move forgeries, noise and blurring, but not robust to JPEG compression, rotation and scaling.

Sridevi, Mala and Sandeep [29] proposed a method for detection of copy move forgery in parallel environment. The methods begin with dividing the image into several blocks. Feature extraction is done for every block using intensity. The last two locations of the feature vectors store the block position. They established one more algorithm for parallel sorting. Lexicography sorting is done using radix sort method in a parallel way. They found the duplicated regions in the image by matching of features and these blocks are mapped on to the image using the location stored in the vector. This method shows improvement in performance over other conventional techniques.

Nguyen and Katzenbeisser [24] proposed a method which is based on radon transformation and phase correlation. In this method, Feature extraction is done by using Radon transform and phase correlation is used to match duplicated blocks. This proposed method is robust against rotation with angles smaller than 4◦ and Gaussian noise addition with SNR values larger than 35 db.

L. Li et al. [13] suggested a method in which image is first filtered and divided into overlapping circular blocks and then the features of the circular blocks are extracted by applying rotation invariant uniform local binary patterns (LBP). Feature vectors are obtained and then compared. And the forged regions can be located by tracking the corresponding blocks. This method is robust to JPEG compression, noise contamination and blurring, and also robust to rotation and flipping. The limitation of the proposed method is that when the region is rotated by common angles, it is difficult to detect the forgeries.

J. Zhao et al. [35] propose a method using Discrete Cosine Transformation and Singular Value Decomposition. In this method, 2D-DCT is employed to fixed-size overlapping blocks of input image. DCT coefficients are determined for each block. Further, each quantized block is divided into non overlapping sub-blocks and Singular Value Decomposition is used to each sub-block, then features are extracted to minimize the dimension using its greatest singular value. Finally, Lexicography is used to sort the feature vectors, and duplicated image blocks are matched by predefined shift frequency threshold.

Sunil Kumar et.al [28] suggests a method using PCA on DCT. Firstly DCT is practiced to calculate DCT coefficient for feature extraction and PCA to yield a reduced dimension representation respectively. Features, invariant to local change of intensity are created using down sampling of low frequency DCT coefficients. The method is robust against manipulation techniques like added noise and JPEG compression and also attend invariance to illumination, but it is fails in case of contrast variations. To overcome this limitation (contrast variations), same author [12] 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. After that binary DCT features are extracted using sign of the DCT coefficients. Coefficient of correlation is used to match resulting binary vectors. This approach is robust against many manipulation techniques such as Gaussian noise addition, compression and minor rotation and scaling.

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

S. No.	Techniques	Method Used	Merits / Demerits
1	[4]	DCT	will not work in AWGN
2	[1]	PCA	robust against AWGN and JPEG compression
3	[5]	DWT-SVD	lower time complexity
4	[2]	DWT-log Polar coordinates	lower time complexity but the geometric operations are not discussed
5	[15]	SIFT	robust to geometric transformation
6	[3]	FMT	robust to scaling bussing, noise addition & SEEG compression
7	[6]	Zernike	high detection rate but not for the seating
8	[18]	PCA – EVD	will not work in rotation & scaling
9	[34]	Improved DCT	will not work in image distorted by JPEG compression ,blurring or AWGN
10	[28]	PCA on DCT	robust to against noise, IPEG compression and also achieve invariance to illumination

3. CONCLUSIONS

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 further research effort is still needed to develop an appropriate algorithm that can detect the copy move. From the literature survey, we observed that the big problem with the copy move forgery in digital image is the detection of duplicated region processed by some common post processing operations such as compression, noise addition, rotation, scaling, flipping etc. The other concern is the time complexity of detection technique of copy move forgery in digital image. Motive of this paper was to give a brief comprehensive review about various techniques for copy-move forgery detection in digital images. A very common type of forgery i.e. copy move forgery detection is discussed. This paper presented a study on various detection techniques which is based on block method.

REFERENCES

[1] **A.C. Popescu and H. Farid** (2005) ***"Exposing digital forgeries by detecting traces of resampling".*** *IEEE Transactions on Signal Processing, vol. 53(2),* pp. 758–767.

[2] **A. Myna, M. Venkateshmurthy, and C. Patil**, 2007. ***"Detection of region duplication forgery in digital images using wavelets and log-polar mapping".*** in Conference on Computational Intelligence and Multimedia Applications. International Conference on, 2007, pp. 371-377.

[3] **Bayram, S., Sencar, H. T., & Memon, N.** (2009). ***"An efficient and robust method for detecting copy-move forgery".*** Paper presented at the Acoustics, Speech and Signal Processing. ICASSP 2009. IEEE International Conference on.

[4] **Fridrich, A. Jessica, B. David Soukal, and A. Jan** Lukáš. 2003. ***"Detection of copy-move forgery in digital images".*** in Proceedings of Digital Forensic Research Workshop. 2003.

[5] **G. Li, Q. Wu, D. Tu, and S. Sun**. 2007. ***"A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD".*** in Multimedia and Expo,IEEE International Conference on, 2007, pp. 1750-1753.

[6] **G. Muhammad and M. S. Hossain.** (2011). ***"Robust copy-move image forgery detection using undecimated wavelets and Zernike moments".*** in Proceedings of the Third International Conferenc on Internet Multimedia Computing and Service, 2011, pp. 95-98.

[7] **H. Farid** . 2009. ***"A Survey of Image Forgery Detection".*** Signal Processing Magazine, vol. 26, no. 2, pp. 16–25

[8] **Himanshu Sharma, Ashok Kumar and H.L.Mandoria** ***"Study and Comparison Analysis of a Video Watermarking Scheme for different Attacks"*** International Journal for

Research in Management and Technology, Volume-4, Issue-9, September-2015:pp. 51-56.

[9] **Harpreet Kaur, Jyoti Saxena.** 2015. **"Key-point based copy-move forgery detection and their hybrid methods: A Review"**. Journal of The International Association of Advanced Technology and Science: ISSN-4265-0578.Vol.6

[10] **J. A. Redi, W. Taktak, and J.-L. Dugelay**.2011. ***"Digital image forensics: A booklet for beginners"*** .Multimedia Tool Appl., Vol. 51, no. 1, pp. 133_62.

[11] **Jiming Zheng and Liping Chang** .2014.*"**Detection of Region-duplication Forgery in Image Based on Key Points' Binary Descriptors**"*, Journal of Information & Computational Science, vol. 11, no. 11, pp. 3959-3966, Jul, 2014.

[12] **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.

[13] **L. Li, S. Li and H. Zhu** .2013. ***"An Efficient Scheme for Detecting Copy-Move Forged Images by Local Binary Patterns"***, Journal of Information hiding and Multimedia Signal Processing, vol. 4, Jan., pp. 46-56.

[14] **M. Hussain,K. Khawaji,G. Bebis and G. Muhammad** . 2012. ***"Passive Copy Move Image Forgery Detection Using Undecimated Dyadic Wavelet Transform".***Digital Investigation, vol. 9, pp. 49-57.

[15] **Mohamadian, Z., & Pouyan, A. A.** (2013). ***"Detection of Duplication Forgery in Digital Images in Uniform and Non-uniform Regions***". Paper presented at the UKSim 15th International Conference on Computer Modeling and Simulation.

[16] **Muhammad G, Hussain M, Khawaji K, Bebis G.** (2011) "***Blind copy move image forgery detection using dyadic undecimated wavelet transform***". In: Proc. 17th digital signal processing (DSP) conference, Corfu, Greece; July.

[17] **M. P. Gomase and M. N. Wankhade** .2014. ***"Advanced Digital Image Forgery Detection: A Review***". International Conference on Advances in Engineering & Technology (ICAET), pp. 80-83.

[18] **M. Zimba, S. Xingming** .2011. ***"DWT-PCA (EVD) based copy-move image forgery detection".*** Int. J. Digital Content Technol. Appl. 5 (1) 251–258.

[19] **M. Zimba and S. Xingming**.2011.***"Fast and robust image cloning detection using block characteristics of DWT coefficients".*** JDCTA: International Journal of Digital Content Technology and its Applications, vol. 5, pp. 359-367.

[20] **M. Bashar, K. Noda, N. Ohnishi and K. Mori** . 2010. ***"Exploring duplicated regions in natural images".***IEEE Trans Image Process, (2010), pp. 1–40.

[21] **M. D. Ansaria, S. P. Ghreraa and V. Tyagi** .2014. ***"Pixel-Based Image Forgery Detection: A Review".*** IETE Journal of Education.

[22] **Mariam Saleem** *.2014.* ***"A Key-Point Based Robust Algorithm for Detecting Cloning Forgery".*** *| International Journal of Current Engineering and Technology, Vol.4, No.4.*

[23] **Mohd Dilshad Ansari** .2014. ***"Pixel-Based Image Forgery Detection: A Review".***IETE Journal of Education, vol 55, no.1

[24] **Nguyen HC, Katzenbeisser S.**(2012). ***"Detection of copy-move forgery in digital images using random transformation and phase correlation".*** Proceedings of the 2012 8th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP '12); July; IEEE; pp. 134–137.

[25] **P.Sabeena Burvin** *.2014.* ***"Analysis of Digital Image Splicing Detection".*** *IOSR Journal of Computer Engineering (IOSR-JCE) Vol. 16, Issue 2, PP 10-13*

[26] **Q. Wu, S. Wang, and X. Zhang.** 2011. ***"Log-polar based scheme for revealing duplicated regions in digital images".*** Signal Processing Letters, IEEE, vol. 18, pp. 559-562, 2011.

[27] **S.-J. Ryu, M.-J. Lee, and H.-K. Lee** . 2010. ***"Detection of copy-rotatemove forgery using zernike moments".*** in Information Hiding, pp. 51-65.

[28] **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-

Vol II. Springer International Publishing.

[29] **Sridevi, M., Mala, C., & Sandeep, S.** (2012). ***"Copy–move image forgery detection in a parallel Environment"***. Computer Science & Information Technology (CS & IT), 52, 19-29.

[30] **Sekhar Resmi and A S Chithra**.2014. ***"Recent Block based Methods of Copy-Move Forgery Detection in Digital Images"*** .International Journal of Computer Applications, vol. 89, no. 8, pp- 28-33.

[31] **Salam A.Thajeel, Ghazali Bin Sulong** .2013. ***"State of the art of copy-move forgery Detection Techniques: a review"*** .IJCSI Issues, Vol.10, Issue 6, No 2.

[32] **V. Tyagi** . 2010. ***"Detection of forgery in images stored in digital form".*** Project report submitted to DRDO, New Delhi

[33] **Y. Cao, T. Gao, L. Fan, and Q. Yang**. 2012. ***"A robust detection algorithm for copy-move forgery in digital images".*** Forensic science international, vol. 214, pp. 33-43.

[34] **Y. Huang, W. Lu, W. Sun, and D. Long** .2011 ***"Improved DCT-based detection of copy-move forgery in images".*** Forensic science international, vol. 206, pp. 178-184.

[35] **Zhao J, Guo J** .2013. ***"Passive forensics for copy-move image forgery using a method based on DCT and SVD".*** *Forensic Science International*; 233(1–3):158–166.

AUTHORS

Ms Rachana is pursuing her M.Tech From the Govind Ballabh Pant University Agriculture & technology Pantnagar, Uttarakhand, India in Information Technology, She received her B.Tech. Degree in Computer Science & engineering from Uttaranchal Institute of Technology Dehradun, Affiliated to Uttarakhand Technical University Dehradun, India in 2012. Her interest includes Image Processing.

Mr. Ashok Kumar is currently working as an Assistant Professor in the Department of Information Technology College of Technology, GB Pant University of Agriculture & Technology. His area of interest includes Software Engineering, Software Testing & Software Analytics.

Dr. Hardwari Lal Mandoria is currently working as a Professor & Head in the Department of Information Technology, College of Technology GB Pant University of Agriculture & Technology, Pantnagar. His areas of Interest are Computer Networks, Network Security Wireless Communication, Mobile Computing, Information Security, information communication Technology

Mr. Binay Kumar Pandey is currently working as an Assistant Professor in the Department of Information Technology College of Technology, GB Pant University of Agriculture & Technology. His areas of interest includes High Performance computing, Bio-informatics, Cloud-Computing.