IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

Rotation Invariant ZLBP Features for Copy-Move-Rotation Based Image Forgery Detection System

Gurpreet Kaur[1*], Rajan Manro[2]

[1,2]Department of Computer Science, Desh Bhagat University, Mandi Gobindgarh, India

Corresponding author: ergurpreetkaur1@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i3.242247 | Available online at: www.ijcseonline.org

Accepted: 14/Mar/2019, Published: 31/Mar/2019

***Abstract*:** In this paper, an effective method for copy-move-rotation forgery detection is proposed which uses Zernike moments and local binary pattern (LBP) as feature extractors. First image is divided into overlapped blocks in which Zernike moments are calculated by rotating block pixels into different directions. Then rotated block with minimum value of Zernike moments is evaluated for which LBP features are extracted. Similar procedure is followed for all blocks. For matching process, mean value of block pixels is used after sorting them in an array. For similar mean value blocks, matching process is carried out by taking the variance difference of LBP features. Blocks with similar variance values are marked as forged pixels in the image. For decreasing the time complexity, edge detector is used which gives edge binary image for high gradient pixels in the image. First matching is carried out for edge pixel blocks only. In post processing, morphological operations are used and matching procedure is followed to get the forged pixels in the image. Experiment results are carried out on a standard dataset in which detection accuracy (DA) and false positive rate (FPR) are used for performance evaluation.

***Keywords*:** *forgery detection, Rotation invariant, LBP, Zernike moments etc.*

I. INTRODUCTION

In modern age, digital imagery and video forging have become the serious threats to security of data; This can be achieved using powerful digital image/ video processing programs and are o effective that they do not leave observable traces. In order to detect these forgeries, an increasing number of researchers have already proposed many detection methods [1]. For digital image forgery, there are mainly two types: copy-move forgery and splicing forgery. In this paper, we focus on the problem of copy-move-rotation forgery detection. The existing forgery detection methods, which generally follow a common procedure especially for copy-move forgery detection are: (1) pre-processing in which forged images are converted to gray space or color space (2) feature extraction in which where features are extracted from different image regions (e.g., overlapped blocks), (3) feature matching, which obtains matched features to determine the original, suspected forgery regions, and (4) post-processing, which discards inconsistently matched pixels or outliers from matched region and only uses the left pixels to obtain the final forgery detected output. As feature extraction majorly affects the accuracy of detection, such methods are generally categorized into three main types named as block-based methods, segmentation-based methods and key point-based methods. In block-based detection methods, the input image is divided into overlapping regular image blocks, and then a descriptor of each block is calculated by various transforms. To extract features that are not affected by normal distortions (e.g., JPEG compression and noise addition) or geometric-distortions (e.g., rotation and scaling), transforms such as the, Principle Component Analysis (PCA) , (PCET) Moment and YCbCr color, Discrete Wavelet Transform (DWT) , Histogram of Orientation Gradient (HOG) ,Discrete Cosine Transform (DCT), Zernike Moment , Krawtchouk Moment , Fourier–Mellin Transform, Signal Value Decomposition (SVD), Polar Cosine Transform (PCT) , and 1-D reflection/rotation-invariant descriptors are applied to blocks to calculate block features [2]. The main weakness of the block-based methods is that the computational complexity of the dense field CMFD method is relatively high because all pixels must be examined. In some recently proposed CMFD methods, the robustness problem has been solved to some extent but the computational complexity of CMFD methods, which consists mainly of the cost of calculating features and matching them has not proven yet. Almost all existing CMFD methods use exhaustive searching of the features to obtain matched features. Exhaustive searching can obtain exactly matched features that can easily generate the final detected regions in post-processing. However, the computational complexity of exhaustive searching is directly related to the number of features. Whether block-based, keypoint-based or segmentation- based, almost all CMFD methods aim to reduce the number of features to decrease the computational

time. However, as the number of features decreases, the difficulty of identifying forged regions increases. Therefore, to retain good detection results, few existing CMFD methods achieve near real-time performance. Some detection methods [3] proposed to use the approximately searching methods, which does not need to reduce the number of features, for achieving low computational time and good detection performance, which do not perform well in terms of accuracy but are not as fast as in desirable. Also CMFD methods fails when there is rotation of copy-move region which is major challenge among the researchers. In this paper, our aim is to detect copy-move-rotation based forgery along with reducing the complexity of the algorithm. To make features rotation invariant Zernike moments are evaluated first in eight different directions by dividing image into overlapping blocks. Then local binary pattern is evaluated for that direction which has minimum value of Zernike moments. Experimental results are carried out for standard CoMoFoD [4] dataset which has different types of forged images.

The organization of the paper is as follows, Section I contains the introduction of copy-move forgery and techniques, Section II contain the related work of methods and approaches used, Section III contain the architecture and essential steps of proposed forgery detection system, Section IV contain the metrics of accuracy check for forgery detection and results, Section V concludes research work with future directions.

II. RELATED WORK

B.A. Warif et al [5] provided a comprehensive overview of existing CMFD techniques for the entire process. Specifically, they discussed the importance of the CMFD techniques, and outlined the common process involved in the CMFD workflow. They classified the copied regions to determine their relevancy in existing CMFD techniques. They also discussed how advances in big data solutions could be influence and/or solve CMFD challenges.

D. Chauhan et al [6] has done survey on different copy-move forgery detection techniques using keypoint based methods on forged image. They have identified that some methods are not responsive for geometric transformation such as scaling and rotating. Also it has been noted that some methods give accuracy but has high computational complexity.

X. Bi et al [7] propose a method using the reflective offset that can be calculated from the mapping offset of the matched feature pair to estimate whether the mapping offset is in a copy-move forgery region; And Based on the reflective offsets and the positions of neighbor features, the feature candidates are sorted from high probability to low probability and matched with the goal of rapidly propagating the copy-move forgery mapping offsets in the feature matching process.

S. M. Fadl et al. [8] the Fourier transform is performed for each block column instead of performing 2D Fourier transformation. Columns are sorted and reshaped to a 1D vector with low frequencies at the beginning and high frequencies at the end. Correlation between similar blocks is performed for similarity matching with two thresholds to eliminate false positives.

A. Kuznetsov et al. [9] showed the application of preliminary image processing methods to solve the problem of transformed copy-move detection. The following methods of image preliminary processing were taken for research: image intensity range reduction, gradient calculation, expansion in orthonormal basis, ALC and LBP. The carried out research showed high quality of copy-move detection with intensity shift distortions

D. Vaishnavi et al. [10] proposed a new symmetry-based image features to detect the forgery and the proposed scheme is modified to detect multiple copy move forgeries also. Though the proposed scheme obtained a good forgery detection results, it needs to be enhanced.

Z. Xie et al [11] proposed copy-move detection based on multi-feature decision. This method uses C4.5 decision tree to deal with the result of other four methods that respectively use gammatone feature, MFCCs feature, pitch feature and DFT coefficients. By adding the noise to the audio, the performance of the proposed method remains almost consistent and the accuracy rate can reach 94.1%.

H. A. Alberry et al. [12] proposed optimized FCM technique for clustering the SIFT key points to decrease time complexity. This research detects also in the status of rotation, scaling and multiple Copy Move attacks.

M. S. Nair et al. [13] proposed a method to extract the keypoints and identify the matching points using the Binary Discriminant Features. The descriptor being binary and of low dimension, reduces the complexity of feature matching.

III. PROPOSED FORGERY DETECTION SYSTEM

Here, we present the proposed technique for region duplication forgery detection, exploiting statistical image features i.e. mean and variance, and based on ZLBP (Zernike LBP) of an image. Fig. 1 displays the flowchart of the proposed technique. Below, we present the steps included in the presented copy–move forgery detection algorithm, including the detailed feature extraction, similarity calculation and thresholding procedures.

Steps in the proposed algorithm adopted:

(1) Initially we take the forged image of size $R_{rows} \times C_{cols}$ pixels (say) as an input. If the image is RGB format, we convert it into grayscale using to following Eqn.:

$$\mathrm{Im}\, g_{gray} = 0.299 \times Red \text{ channel} + 0.587 \times Green \text{ channel} + 0.114 \times Blue \text{ channel} \quad (1)$$

(2) Applied Gabor filter twice to enhance the edge pixels in the image by taking grayscale image and its complement image together and merge the output from them and then sobel filter is applied in horizontal and vertical direction to get the improved edge image to which further thresholding is applied to get binary image.

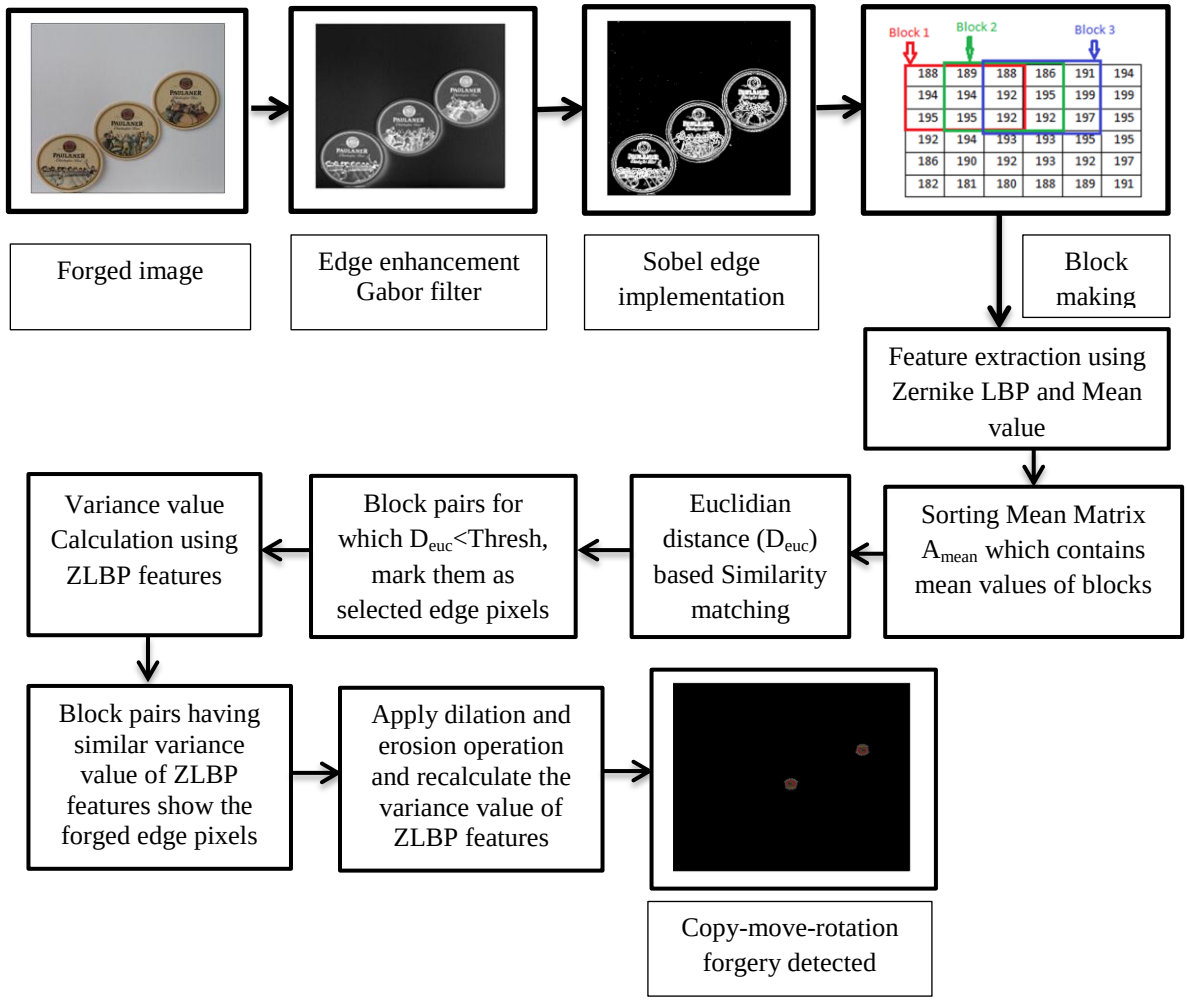

Figure 1: Flow chart of the ZLBP based forgery detection system

(3) Overlapping blocks of size $X \times X$ pixels has been obtained from the grayscale image, such that total size of obtained blocks is $(R_{rows} - X + 1) \times (C_{cols} - X + 1)$. The mean value sequence $M_1, M_2 \ldots M_{((W/2-P+1)\times(H/2-P+1))}$ is calculated from the corresponding blocks $B_1, B_2, \ldots B_{(R_{rows}-X+1)\times(C_{cols}-X+1)}$, as:

$$M_i = \frac{1}{X \times X} \sum_{j=0}^{X \times X} x_{ij} \quad (2)$$

Where M_i is the mean of pixel intensity of block B_i. The mean values are stored into a matrix, say A which is sorted in ascending order.

(4) To evaluate rotation-invariant features of image blocks a noble way is proposed in which first Zernike moments are calculated for the edge pixel blocks by taking eight different possibilities of rotation of a block. Then minimum value and location of Zernike value is finding and LBP feature is evaluated according to that rotation of pixel which has small value. By taking this effective rotation invariant LBP features are obtained [15].

(5) For calculation of similarity between blocks, we measure the following Euclidean distance:

$$D(x,\ y)' = \left(\sum_{i-1}^{(R_{rows}-X+1)} \left(A_{xi} - A_{yi} \right)^2 \right)^{1/2} \quad (3)$$

Where $D(x,\ y)$ is the Euclidean distance between a pair of rows of $A,\ A_x\ and\ A_y$, where $A_x = (A_{x1},\ A_{x2}, \ldots A_{x(M_{rows}-X+1)})$ and $A_y = \left(A_{y1},\ A_{y2}, \ldots A_{y(C_{cols}-X+1)} \right)$. Similarity check has been applied to only those pixels which come as edges in the soble edge binary image. It reduces the computation time as only high entropy pixels come as edge pixels.

(6) The block pairs for which $D(x,\ y) < T_s$, (where T_s is an empirically selected similarity threshold), are possibilities to be forged regions.

(7) For the selected edge pixel block check the similarity based on variance value of ZLBP features; two block-pairs which has similar variance values, mark them as forged edge pixels.

(8) As this produced only edge pixels in the copy move rotated area, morphological operations i.e. dilation and erosion is applied to the output, to which further similarity matching based on variance difference of ZLBP value is applied which results in whole forgery area detected in the image. The method is efficient and provides good results in Copy-move-rotation oriented forgery detection.

IV. PERFORMANCE EVALUATION

The number of pixels detected after presented forgery detection method and the ground truth image provides the effectiveness of the presented method based on sensitivity of forged pixels and specificity of rest of the image which considers as background portion [16]. Hence Detection Accuracy (DA) which defines sensitivity parameter and False Positive Rate (FPR), which defines background portion which comes as forged region, can effectively represent the accuracy of forgery detection by proposed method.

The formula for both DA and FPR is given as under .Detection Accuracy (DA) is the percentage of (actually) copy–move-rotated pixels in an image, which are accurately detected by a particular region duplication detection method to be copy–move-rotated. Higher efficiency implies higher detection accuracy [2].

$$DA = \frac{\#Correctly\,\det ected\ copy - move - rotation\ pixels}{\#actually\,copy - moved - rotaion\ pixels} \times 100\% \quad (4)$$

Or in terms of true positive, false positive, false negative parameters, these parameters can be defined as follows:

$$DA = \frac{\#True - Positive}{\#True - Positive + False - Negative} \times 100\% \quad 5)$$

False Positive Rate (FPR) is described as the total number of actual image pixels, incorrectly detected to be forged, and formulated as:

$$FPR = \frac{\#incorrectly\,\det ected\ copy - move - rotation pixels}{\#actually\,copy - moved - rotation\ pixels} \times 100\% \quad (6)$$

Similarly FPR can be defined as

$$FPR = \frac{\#False - Positive}{\#True - Positive + False - Negative} \times 100\% \quad (7s)$$

Where true positive is correctly detected pixels as forged, False-positive as incorrectly detected forged pixels and false negative as incorrectly detected non-forged pixels; Forgery detection results for tested images are shown below in figure 2.

Table 1: Detection accuracy (DA) and False positive rate (FPR) parameters for the tested images

Parameters Image	TP	TN	FP	FN	DA %	FPR

name						
42f	2994	258700	450	0	100	0.174
40f	1996	258964	1184	0	100	0.455
43f	7112	253300	1657	75	98.95	0.649
53f	7138	251933	2223	850	89.35	0.875
59f	6753	254836	538	17	99.74	0.211

The presented ZLBP and mean-variance based methodology has been implemented in MATLAB. Our test data consists of a set of 512 × 512 color as well as grayscale images; taken from the CoMoFoD [4] Database has been used for experimentation and performance evaluation which contains multi types of forged image. Only copy-move-rotated dataset from this database has been used in the experiments. For the sake of experimentation, we have selected test images with copy–move-rotated forgery induced into them. The DA and FPR results of the presented technique are presented in Table I.

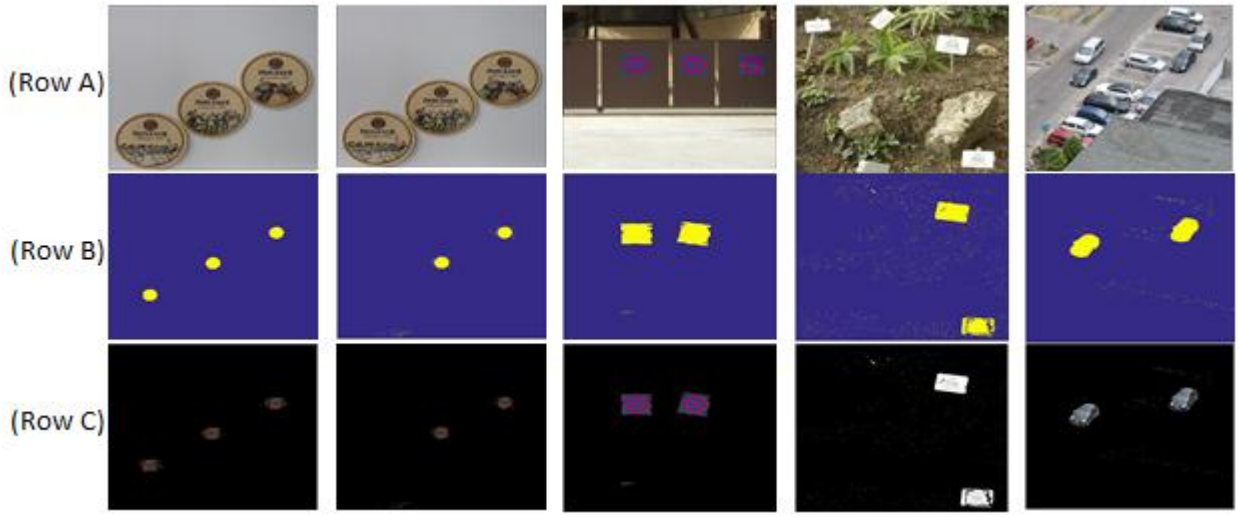

Figure 2: Image showing original forged images, binary ouput of forged region detected and forged pixels in original image

After optimizing the false matches, the false positive rate is minimized, which is now in the range of 0-2%. All the results presented in Table I are presented for all five test images shown in the figure below.

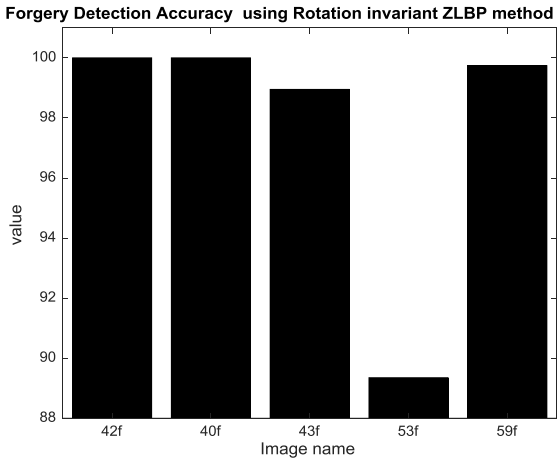

Figure 3: Bar graphs for Detection accuracy (DA)

Graphs show the efficiency of the presented method provides accuracy mainly on the principles of operation of LBP with Zernike moment [14]. The performance has been compared visually in terms of DA and FPR, in Figs. 3 and 4, respectively. From Figs. 3 and 4, it is evident that the presented algorithm achieves lower false positive rate and higher detection accuracy when copy-move-rotation forgery is induced in images.

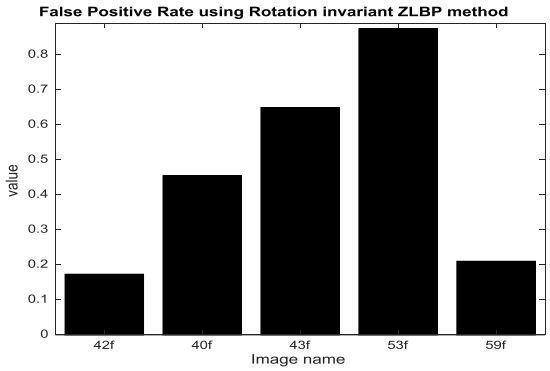

Figure 4: Bar graphs for false positive rate (FPR)

V. CONCLUSION

Proposed forgery detection method operates by carrying out edge detection so that only edge pixels can be used for pre-matching process. This reduces the computation time. Forged image is split into fixed size overlapped blocks for which rotation invariant features are extracted along with mean and variance values of pixels and features. Then matching process is carried out to get forged pixels with similar values of variance of LBP features. Post-processing is used to increase accuracy of segmentation results. For evaluating the performance of the proposed method, DA and FPR metrics are used which checks the output result with ground truth pixels of actual forged regions. Experimental results show approx. 98-100 % accuracy in forgery detection on most of the tested images. In future copy-move-scaling based duplication can be explored.

REFERENCES

[1] I. Amerini, L. Ballan, R.Caldelli, A. D. Bimbo, L.D. Tongo, G.Serra, "Copy-move forgery detection and localization by means of robust clustering with J-Linkage", Signal Processing: Image Communication, Vol. 28, Issue. 6, pp.659-669, 2013

[2] R. Dixit, R. Naskar and A. Sahoo, "Copy-move forgery detection exploiting statistical image features," International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, pp. 2277-2281, 2017

[3] D. Cozzolino , G. Poggi , L. Verdoliva, "Efficient dense-field copy–move forgery detection", IEEE Transactions on Information Forensics and Security, vol. 10, issue 11, pp. 2284-2297, 2015

[4] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, "CoMoFoD-New database for copy–move forgery detection," 55th IEEE International Symposium ELMAR, 2013.

[5] N. Warif, A.Wahab, M. Idris, R.Ramli, R.Salleh, S.Shamshirband, K. Choo, "Copy-move forgery detection: Survey, challenges and future directions" Journal of Network and Computer Applications, Vol. 75, pp.259-278, 2016

[6] D. Chauhan, D. Kasat, S. Jain, V. Thakare, "Survey on Keypoint Based Copy-move Forgery Detection Methods on Image", Procedia Computer Science, Vol. 85, pp. 206-212, 2016

[7] X. Bi, C. M. Pun "Fast reflective offset-guided searching method for copy-move forgery detection" Information Sciences, Vol. 418–419, pp. 531-545, 2017

[8] S. M. Fadl, N. A. Semary, "Robust Copy–Move forgery revealing in digital images using polar coordinate system", Neuro computing, Vol. 265, pp. 57-65, 2017

[9] A. Kuznetsov, V. Myasnikov, "A new copy-move forgery detection algorithm using image preprocessing procedure", Procedia Engineering, Vol. 201, pp. 436-444, 2017

[10] D. Vaishnavi, T.S. Subashini, "Application of local invariant symmetry features to detect and localize image copy move forgeries", Journal of Information Security and Applications, Vol. 44, pp. 23-3, 2019

[11] Z. Xie, W. Lu, X. Liu, Y. Xue, Y. Yeung, "Copy-move detection of digital audio based on multi-feature decision", Journal of Information Security and Applications, Vol. 43, pp. 37-46, 2018

[12] H. A. Alberry, A. A. Hegazy, G. I. Salama, "A fast SIFT based method for copy move forgery detection", Future Computing and Informatics Journal, Vol. 3, Issue 2, pp. 159-165, 2018

[13] P. M. Raju, M. S. Nair, "Copy-move forgery detection using binary discriminant features", Journal of King Saud University - Computer and Information Sciences, 2018

[14] J. Yang, P. Ran, D. Xiao, and J. Tan, "Digital image forgery forensics by using undecimated dyadic wavelet transform and Zernike moments", Journal of Computational Information Systems, vol. 9,Issue 16, 2008.

[15] Suma S L, Sarika Raga, "Real Time Face Recognition of Human Faces by using LBPH and Viola Jones AlgorithmReal Time Face Recognition of Human Faces by using LBPH and Viola Jones Algorithm", International Journal of Scientific Research in Computer Science and Engineering, Vol.6, Issue.5, pp.6-10, 2018

[16] Amey Samant, Sushma Kadge, "Classification of a Retinal Disease based on Different Supervised Learning Techniques", International Journal of Scientific Research in Network Security and Communication, Vol.5, Issue.3, pp.9-13, 2017

Authors Profile

Ms.Gurpreet Kaur is an Assistant Professor. She has more than 10 years of experience in academics. More than 5 papers are published in different international journals. Her research interest is in area of digital computing; CMFD and Copy-Move-Rotation based Forgery Detection.

Dr Rajan Manro is an Associate Professor. He is certified Oracle-9i (DBA) Professional. More than 14 papers are published in different international journals. His research interest is in the area of Cloud computing, Image Processing and A.I.

