Novel Copy Move Forgery Detection Based on Repeated Feature Extraction and Delaunay Triangulation

Dhanya R, Kalaiselvi R

Abstract*: Nowadays new and creative methods of forging images are developed with the invention of sophisticated softwares like Adobe photoshop. Tools available in such softwares will make the forged image look real which cannot be even identified by a naked eye. In this paper, key point based approach of taking out features using Scale Invariant Feature Transform (SIFT) is used. The feature points thus extracted are then modeled to get a set of triangles using Delaunay Triangulation method. These triangles are matched using mean vertex descriptor and the removal of false positives is done using the method of Random Sample Consensus (RANSAC). Implementation show that the proposed approach outdoes the equivalent methods

Keywords: Forensic Image Processing, Forgery detection, Delaunay Triangulation, Copy-Move Forgery.

I. INTRODUCTION

In the current scenario, digital images play an inseparable part in human life. The invention of strong editing softwares has made the process of counterfeiting and tampering the images a child's play. This has led to the distrust of photos in every area including law. This proves the significance of image forensic tools to differentiate the original with the fake one. Although the existing methods are effective against some kind of attacks, the accuracy is not enough in practical scenario.

Two approaches are mainly there in Forensic digital image processing [1], Active and Passive methods. Active method forms the act of embedding additional information on the images whereas analyzing the contents of the image to find whether it is tampered or not forms the passive method [2].

The forgery method copy-move is where portion of the image is copied and inserted onto alternative portion of that itself. It is done for concealing or overemphasizing something in the image. It forms an advanced version of the splicing attack in which two image parts are fused to form a fresh image. The forgery done desperately will not be easily identified by the detectors as the inconsistencies are usually exploited of the local statistical features of different parts of the same image. But the copied regions in this case show consistency with the other parts [3]. Many researches have been carried out to find the forgery of copy move.

Revised Manuscript Received on January 06, 2020.
***** Correspondence Author
Dhanya R*, Research Scholar, Department of Computer Applications, Noorul Islam Centre for Higher Education, Kumaracoil, Tamil Nadu, India. Email: dhanyamanoj2003@gmail.com
Kalaiselvi R, Associate Professor, Department of Computer Science & Engineering, Noorul Islam Centre for Higher Education, Kumaracoil, TamilNadu, India. Email: kalaiselvir32@gmail.com

It is not rare to discover identical areas as the copied parts. Later, there comes the necessity for a filtering phase to remove false matches. Geometrical mismatches are utilized for this purpose which suffers from high computational cost. Higher rate of exclusive areas bring about low incompatible sections [4]. Thus, numerous false matches will lead to low performance if that image is with highly homogenous parts. Hence in order to achieve better results, some of the methods omit these homogenous regions. A number of highly impressive approaches were suggested to check the images having even regions, it is still puzzling when the image is extremely large.

Here we are proposing a new method wherein the entire area of the image is covered adaptively based on distinctiveness metric. The density of the key points is also adjusted adaptively such that the suspected forged areas can be more concentrated. Later triangles are formed with these interest points using Delaunay Triangulation method and after that an iterative enhancement method is designed to improve the accuracy based on pixels. The iterative method will help to focus only on the suspected regions and the less number of triangles form decreases the computational cost. Thus the proposed method shows merit accuracy wise as well as computational cost wise.

The article is structured in the subsequent way. Section II reviews the formerly conducted methods of CMFD. Section III elaborates the method proposed and the experimental analysis of the method proposed and the recent CMFD approaches is done in section IV.

II. LITERATURE SURVEY

Numerous methods have been suggested to identify the copy move method of forgery. Mostly they are characterized into two: key point based and block based. Features are extracted, local features are described and the similarity is evaluated. For each point, a feature vector is taken out in block based method where as a key point descriptor is got for each relevant point in key point method.

The common framework for copy move forgery detection is shown in Fig.1. Christlein et al presented a stretched version [5]. Improvement of efficiency is the primary objective of the first stage. Computational complexity is

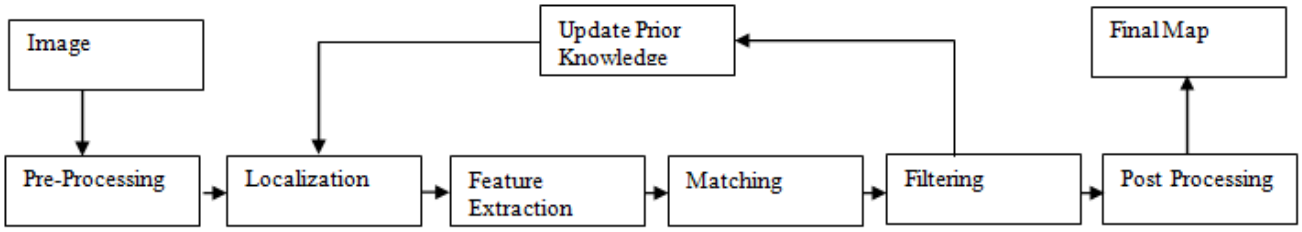

Fig. 1. Copy-move forgery detection method - Common Framework

Reduced with segmentation. The centres of local patches are determined in the localization phase. For each region, feature vector is computed. In the matching stage, identical blocks are found. Spurious pairs are avoided in the filtering phase. In the post-processing stage, some morphological operations are employed. The matching information is updated using attained facts from the earlier iterations.

The researches on CMFD was started by Fridrich et. al. From all overlapping blocks, they extracted coefficients of Discrete Cosine Transform. Principal Component Analysis and Singular Value Decomposition are also used which were found to be vigorous to JPEG compression, blurring and noise addition[6-7]. For those images which suffered geometric conversions, features not variant to rotation using Fourier Mellin Transform (FMT)[8] and Local Binary Patterns (LBP)[9] were also used. But they were limited to special degrees [5]. Polar Cosine Transforms (PCT) and Zernike moments represented circle blocks as polar co-ordinates [10-11]. In the filtering phase, Random Sample Consensus (RANSAC) was engaged in estimating affine conversions between duplicated regions. In [12], for each block, a matching threshold is adapted.

Methods that are sparsely sampled uses feature point extraction techniques. To detect salient points Scale Invariant Feature Transform (SIFT) [13-15] and Speeded Up Robust Features (SURF) [16,17] are used. These methods are found to be robust against geometric transformations and they also impose low computational cost due to the lower number of points compared. Feature point indicators found suitable to one application will not effective for another problem as each application has its own constraints. Indicators of Interest point focuses on parts with large info content and so as a consequence they may avoid the areas unevenly shielded by interest points, similar to low contrast areas.

Two methods which use segmentation are proposed recently. In [18], an expectation-Maximization method is used to reduce the error of affine estimation. But then again the cost of computation is high on big images.

Next section proposes an algorithm that integrate the benefits of key-point and block-based methods. Even when the image is fully enclosed in this approach, the number of chunks which are scrutinized is very less. Hence it exploits more resultive procedures that have high computational cost. Further it allows concentrating more on the suspected area in the successive Iterations to give more perfect result.

III. PROPOSED METHOD FOR CMFD

Image is covered entirely and adaptively in the proposed method, even the low contrast regions. Interest points are detected using SIFT and then an improved adaptive matching is used. The false positives are rejected by an operative filtering algorithm. Based on the previous info the process is iterated to enhance the outcomes.

A. Feature Extraction

For the images, their self-similarity, makes the amount of patches measured as matching especially in low entropy areas. Hence, using all the probable blocks will likely reduce the recognition. The possibility of pseudo equivalent is large in areas with low distinctiveness as it raises the discrimination [19]. This has inspired us to selecting more exclusive portions which are not as much of prospective to be unequal. On the contrast, the entire image is to be enclosed sufficiently with points of interest in the detection of Copy-Move Forgery. The proposed scheme offers an entire exposure of points of interest which adapts the density grounded on the resident distinctiveness. Less possibility of detecting a spot shows the more distinctiveness. Through extensive experiments, in [20], they have defined uniqueness metric considering the nearby blocks. Moreover to fine-tune the compactness of the points of interest, based on the certainty level and uniqueness, they also defined a local capacity. During the initial iteration, for every points, the certainty levels are set equal. On increasing the image resolution, there is restriction to the local variations and hence the primary value of the certainty level should be reliant on the image size. For further iterations, it is accustomed grounded on the formerly attained outcomes.

More exclusive points are carefully chosen first. If the dimensions are considerably larger than the local density, then a point is taken as a point of interest. For each point, the local density is found by the Gaussian window. The smaller the distance weights, the more sensitive will be the close points and this will scatter the interest points. The projected method identifies the points of interest that cover the entire image in a solid way. The method also makes use of the preceding info in distinction of other algorithms that make the decision just based on the operational data. The tampered regions may not be identical and it will be distorted when compared to the real equivalents. The achievement of extraordinary amount of uniqueness and invariance concurrently is very difficult whose unsuitable level may result in a reverse effect.

Polar Cosine Transforms (PCT) and Zernike moments show most precise tampering detection in the case of CMFD [5, 11]. There are some other techniques which are proposed in the phase of filtering where transformations are estimated.

Affine transformations where in the uneven points or outliers are rejected employing Random Sample Consensus (RANSAC). In [12], adaptive matching threshold is used for every block whereas in [20, 21] Patch Match is suggested.

For its maximal discrimination property, PCT is utilized [22]. For a continuous image, PCT features, *g*, with order *n* repeated *l* times are calculated as :

$$f = \{|M_{i,l}| such\ that\ n+1 \leq 3, 0 \leq n, l < 3 \quad (1)$$

where

$$M_{i,l} = \Omega_n \int_0^{2\pi} \int_0^1 [H_{n,l}(r,\theta)]\, g(r,\theta) r dr d\theta \quad (2)$$

$$\Omega_n = \begin{cases} 1/\pi & n = 0 \\ 2/\pi & n \neq 0 \end{cases}, H_{n,l}(r,\theta) = \cos(\pi n r^2) e^{jl\theta} \quad (3)$$

The representation of the image as polar coordinate is indicated as $g(r,\theta)$. The definition of the interest points which are selected is done by a B × B block surrounding every point of interest converted to feature region using (1). f depicts the complete feature set which also includes the complete selected point representation. Along with that the angle of rotation between the two patches is also found using the phase of the PCT.

Scale Invariant Feature Transform (SIFT) method projected by Huang et. al [24] is experimentally found out to be invariant to rotations, noise, resizing and adjustments of lightings. It is also found to deal with with JPEG compression and Gaussian noises.

All the features extracted from the region may be characterized by a collection of related triangles. The model which is applied mainly in the area of computer graphics is also employed here in the case of images. From the image, the features are extracted. Delaunay triangulation is used to connect those featured points. Thus, the image is characterized by feature points is subdivided into triangles whose contents are pixels with identical features. This method is selected in place of Voronoi tessellation for its minute element will not contain the edges and its contents may be considered as consistent. The triangles thus obtained are matched with each other using their mean vertex descriptors.

B. Triangle Matching

Mean Vertex Descriptor of each triangle built against the geometric vertices of the triangles is calculated as the average value of the feature vectors.

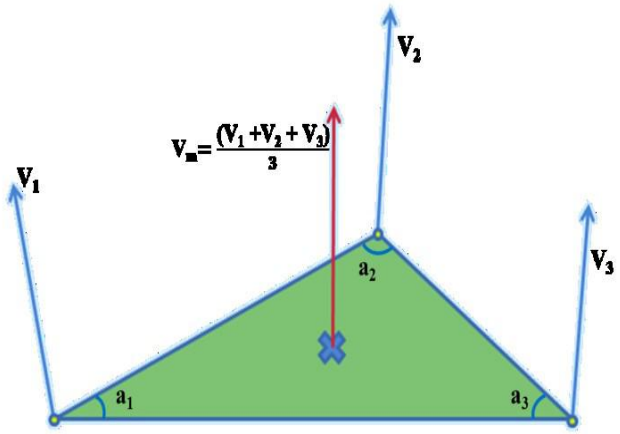

Fig. 2. Mean Vertex Descriptor

The Vertex mean V_m of each triangle is given by:

$$V_{mi} = (V_{1i} + V_{2i} + V_{3i}) / 3$$

where the feature vectors extracted is given by i ranging from 1 to N, given N is the number of Delaunay triangles that are formed in the image. Then to find the suspected copied regions, the triangles are sorted on account of their L1 norm of Mean Vertex Descriptors (MVDs) and these MVDs from every triangle is matched with each other ones in the queue using a static sized window rather than an adaptive window. Two triangles are considered to be matching if the L1 relative displacement with their equivalent MVD is less than a threshold value. x and y being the indices for the pair of triangles that are equated and if V_{mx} and V_{my} are the corresponding Mean Vertex Descriptors, then

$$|Vmx - Vmy| \leq THv\,(y - x) < ws$$

Where, THv is the threshold value and ws is the fixed window size.

C. Outlier Detection

False assignment of the candidate matched pairs is very common in the case of real images due to its intrinsic self-similarity. It is common that the regions that originated from the same action of copy-move shows identical behavior which in turn will help in discarding the pseudo matches. The common relationship between the two is estimated using affine transforms. High computational cost is the problem of most of filtering algorithms. Outliers are handled effectively by Random Sample Consensus (RANSAC) method, but it false pairs will incorrectly represent the correct matches. Identified points of interest being denser than the key points, its clustering, which greatly enhances the probability of identifying the exact pairs cannot be performed for its raised computational complexity.

IV. EXPERIMENTAL SETUP

This section deals with the experimental analysis of proposed system matched with the most efficient copy move forgery detection methods. Experiments are done using MATLAB R2017a with Intel Core i3-5005U CPU@ 2GHz using 4GB RAM and 64-bit Operating System.

We evaluated this method by means of different subsets of the database. The subsets range from simple ones, with operations on rotation, resizing, compression, multiple forgery and the combination of these operations.

A. Datasets

The dataset we used for assessing the proposed method compared with the existing one is MICC – F220 proposed in the paper [14], which comprises of 110 original and tampered images each.

B. Metrics

Evaluation is done on the images at pixel level rather than at image level. The following metrics were used: -

Table 1: Evaluation Metrics

Serial No.	Parameter Name	Formulas	Description of Parameter
1.	True Positive Rate	(TPR)= (TP)/(TP+FN)	TP - True Positive or Forge part identified as forge part on Tampered image FN - False Negative or Forge part does not identified as forge part on Tampered image
2	True Negative Rate	(TNR)= (TN)/(TN+FP)	TN - True Negative or Original part identified as original part on Tampered image FP - False Positive or Original part identified as forge part on Tampered image
3	Accuracy	(TP+TN)/ (TN+FP+TP+FN)	Accuracy in numeric form.
4	False Negative Rate	(FNR)= FN /(FP+TN)	Represent rate of false matching or wrong output
5	False Positive Rate	(FPR)=FP/ (FP+TP)	Represent rate of true matching or correct output

Precision: It is given by the number of correctly classified forged pixel in the total number of copy move pixels
TPR / (TPR+FPR).
Recall: It is the ratio of the true positives to the predicted results
F1-Measure: It is the harmonic mean on the precision and recall with its extreme at 1 and worst at 0.

$$F_1 \text{ Score} = 2 \times \frac{P \times R}{P + R}$$

V. RESULTS AND DISCUSSIONS

The comparison and evaluation of the method proposed with the efficient algorithms is done under this section. Experimental results show that the localization of the duplicated region is done more accurately in the proposed system. F1-score is more accurate in most of the cases. The iterative improvement elevates the recall rate as a consequence of not missing out any copied region. The hierarchical search for the forged regions has also decreased the execution time.

Fig 3. Original Image

Fig 4. Grey Image

Fig 5. SURF matched features

Fig 6. SIFT matched features

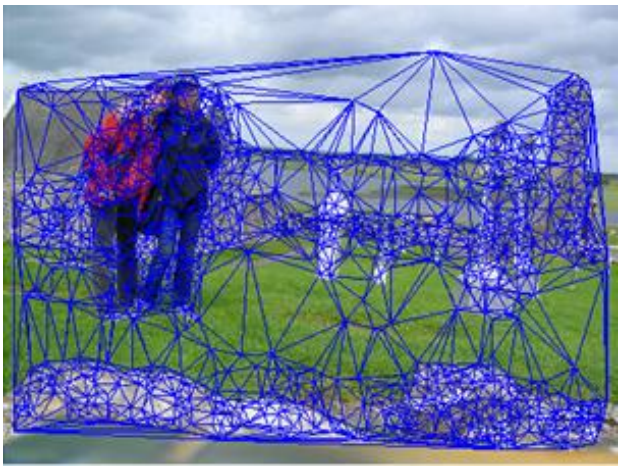

Fig 7. Delaunay Triangulation

Fig 8. Delaunay Features matched

Fig 9. Tampered region identification

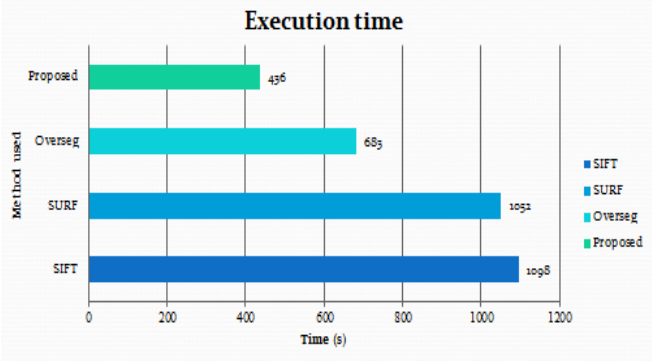

Fig 10. Comparison of execution time

Method	Precision	Recall
SIFT	0.69	0.91
SURF	0.65	0.73
Proposed Method	0.93	0.90

Fig 11. Precision and Recall

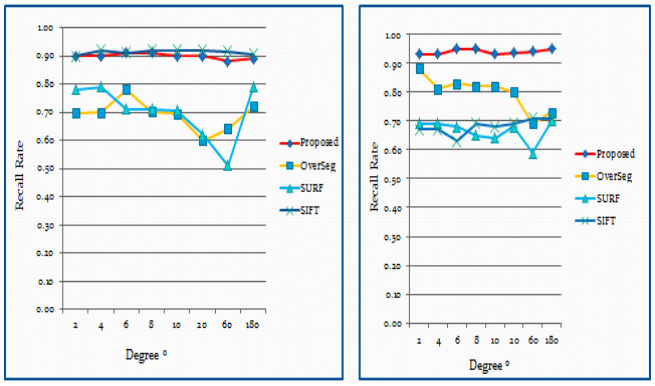

Fig 12. Rotation – Recall and Precision

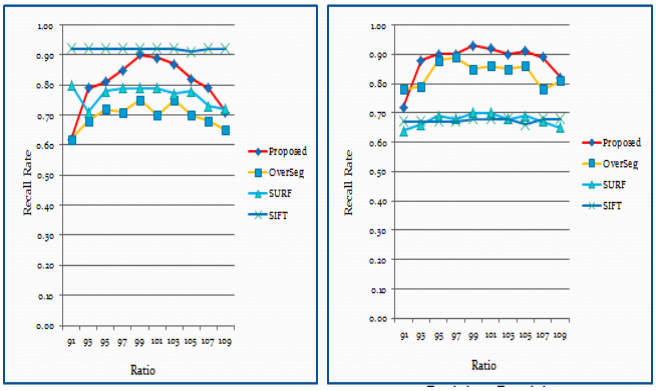

Fig 13. Resizing – Recall and Precision

VI. CONCLUSION

A novel CMFD method is suggested in this paper. For unique areas, the density of the points of interest will be considerably large and this will in effect increase the probability of finding the forged regions more accurately. The whole process is iterated upon which the points of interest concentrate more on the significant regions of suspicion based on the information collected from the previous iterations. The method proposed is a way in between the less sampled and the over sampled methods. Experimental results prove that the suggested method is efficient under many conditions like rotation, scaling and multiple pastes.

The forthcoming work on copy move forgery detection methods will concentrate more with JPEG compression and multiple paste situations.

REFERENCES

1. H. Farid, " Image Forgery detection," IEEE Signal Process Magazine, Vol.26, pp.16-25, 2009
2. P. Bestagini, M Fontani, S. Milani, M Barni, A Piva, M.Tagliasacchi, " An overview on video forensics," in Proc European Signal Process. Conf., 2012, pp,1229-1233
3. N. Hieu Cuong and S. Katzenbeisser, " Security of copy-move forgery detection techniques," in IEEE ICASSP, 2011, pp 1864-1867
4. S. Bravo.Solorio and A.K Nandi, " Exposing duplicated regions affected by reflection, rotation and scaling," in IEEE ICASSP, 2011, pp. 1880-1883
5. V. Christlein, C Riess, J. Jordan and E. Angelopoulou, " An evaluation of popular copy-move forgery detection," in IEEE In. Workshop on Information Forensics and Security, 2010, pp, 1-6
6. M. Bashar, K.Noda, N.Ohnishi ad K Mori, "Exploring duplicated regions in natural images", IEEE Transactions in Image Processing, pp. 1-1, 2010
7. L. Guohui, W.Qiong, D.Tu and S.Shaojie, " A Sorted neighbourhood approach for detecting duplicated regions in image forensics based on DWT and SVD," IEEE International Conference on Multimedia and Expo, 2007, pp.1750-1753
8. S. Beyram, H.T.Sencar and N. Memon," An Efficient and robust method for detecting copy move forgery," IEEE ICASSP, 2009, pp. 1053-1056
9. S. L.Leida Li Hancheng Zhu, " An Efficient scheme for detecting copy move forged images by local binary patterns," Journal of Information Hiding and Multimedia Signal process., Vol 4, pp,46-56, 2013
10. S.J Ryu, M.J.Lee and H.K.Lee, "Rotation invariant localization of duplicated image regions based on zernike moments," IEEE Transactions on Information Forensics Security , VOl.8,pp.1355-1370, 2013

11. Y.Li, “Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching,”, Forensic Science Int., Vol 224, pp.59-67, 2013
12. M. Zandi, A. Mahmoudi-Anaveh and A. Mansouri, “Adaptive matching for copy-move forgery detection,” in IEEE International Workshop on Information Forensics and Security, Atlanta, GA, 2014, pp.119-124
13. D.G.Lowe, ”Distinctive image features from scale invariant keypoints,” International Journal of Computer Vision, VOl.60,pp.91-110,2004
14. I.Amerini, L. Ballan, R.Caldelli, A.DelBimbo and G.Serra, “ A SIFT based forensic method for copy-move attack detection and transformation recovery,” IEEE Transaction of Information Forensics Security, Vol.6, pp. 1099-1110, 2011
15. P.Xunyu and L.Siwei,”Detecting image region duplication using SIFT features,” IEEE ICASSP, 2010, pp. 1706-1709
16. H. Bay, A,Ess, T.Tuytelaars, and L.Van Gool, “Speeded up Robust features (SURF),” Computer Vision and Image Understanding, Vol. 110, pp. 346-359, 2008
17. B. Shivakumar and L.D. S.S Baboo,”Detection of region duplication forey in digital images using SURF,” International Journal of Computer Science Issues, Vol.8, 2011
18. J.Li,X.Li, B. Yang and X.Sun, “Segmentation based Image copy-move forgery detection scheme”, IEEE Transactions on Information Forensics and Security, Vol.5, 2014
19. T Khadir and M. Brady, “Saliency, scale and image description”, International Journal of Computer Vision, Vol.45, pp. 83 – 105, 2001
20. Zandi, M., Mahmoudi-Aznaveh, A., & Talebpour, A..” Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector. IEEE Transactions on Information Forensics and Security, 11(11), 2499–2512. doi:10.1109/tifs.2016.2585118, 2016
21. C. Barnes, D.B.Goldman, E. Scechtman, and A. Finkelstein, “ The PatchMatch: a randomized correspondence algorithm for structural image editing,” ACM Trans. Graph, Vol. 28, pp. 1-11, 2009
22. C. Barnes, D.B.Goldman, E. Scechtman, and A. Finkelstein, “The PatchMatch randomized matching algorithm for image manipulation,” Communicatio ACM, Vol.54, pp.103-110, 2011
23. Y. Pew-Thian, J.Xudong and A.C.Kot, “Two dimensional polar harmonic transforms for invariant image representation, “IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 32, pp.1259-1270, 2010.
24. H. Huang, W.Guo, Y Zhang, “ Detection of Copy-Move forgery in digital Images using SIFT algorithm”, Pacific-Asia Workshop in Computational Intelligence and Industrial Application(PACIIA), Computer Society, 2008, pp. 272-276

AUTHORS PROFILE

Dhanya R, is a Research Scholar in the Department of Computer Applications at Noorul Islam Centre for Higher Education, Kumaracoil, Thuckalay, Tamil Nadu. She is currently working as an Assistant Professor in the Department of Computer Applications, St. Teresa’s College, Ernakulam, Kerala. She is an MCA graduate with research interest in Digital Image Processing and Digital Electronics. She has presented and published papers in International Conferences and Journals

R. Kalaiselvi, is currently working as an Associate Professor in the Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, Kumaracoil, Thuckalay, Tamilnadu, India. She has more than eighteen years of teaching experience. She obtained her B.E (Electronics and Communication Engineering) from M.S University, Tirunelveli, and her ME (Computer Science and Engineering) from Anna University, Chennai, India.and her Ph.D from Anna University Chennai. Her research interests include Network Security, Cloud Computing and Distributed Computing. She has published many research papers in National/International Conferences and Journals. She has attended several seminars and workshops in the past ten years. She is an IEEE member.