International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-12 Issue-9, August 2023

A New Efficient Forgery Detection Method using Scaling, Binning, Noise Measuring Techniques and Artificial Intelligence (Ai)

Mahesh Enumula, M.Giri, V.K. Sharma

Abstract: ***In the market new updated editing tools and technologies are available to edit images and with help of these tools images are easily forged. In this research paper we proposed new forgery detection technique with estimation of noise on various scale of input image affect of noise in input image, frequency of images are also changed due to noise, noise signal correlated with original input images and in compressed images quantization level frequency also changed due to noise. We partition input image into M X N blocks, resized blocks are proceed further, image colors are also taken into consideration, each block noise value is evaluated at local level and global level. For each color channel of input image estimate local and global noise levels are estimated and compared using binning method. Also measured heat map of each block and each color channel of input image and all these values are stored in bins. Finally from all noise values calculate average mean value of noise, with these values decide whether input image is forgery or not, and performance of proposed method is compared with existing methods.***

Keywords: Image Processing, Machine Learning, Retouching, Binning, Forgery, Water Marking.

I. INTRODUCTION

With latest development tools and technology, an image can be easily editable, untrained peoples may not in a position to differentiate original and forged images[1], many image processing tools are available to detect such a forgery images, all these tools are giving clues to detect forgery, a window sized boxes will scan entire images based on clues, and all these image forgery detection techniques are suffering with boundary problems. Authors in [3] introduced image locations technique to detect forgery within segments, image localization is done with noise and photo response technique, taken homogeneity of local region to detect forgery based on small clues, and authors[3] combined localization technique and window based frame work to detect forgery images.

Manuscript received on 18 July 2023 | Revised Manuscript received on 05 August 2023 | Manuscript Accepted on 15 August 2023 | Manuscript published on 30 August 2023.
*Correspondence Author(s)
Mahesh Enumula*, Research Scholar, Department of Electrical Communication Engineering, Bhagwant University, Ajmer (Rajasthan), India. E-mail: researcher.mahesh@gmail.com, ORCID ID: 0009-0009-5931-3830
Dr. M. Giri, Professor, Department of Computer Science and Engineering, Siddharth Institute of Engineering and Technology, Puttur (Karnataka), India. E-mail: dr.m.giri.cse@gmail.com
Dr. V. K. Sharma, Professor, Department of Electrical Communication Engineering, Bhagwant University, Ajmer (Rajasthan), India. E-mail: viren_krec@yahoo.com

Median filtering is widely used in multi-media-based applications like steganography, image forensic, security filtering approach is mostly nonlinear technique and as well as data also preserving using this technique. Earlier researcher on image processing proposed various types of techniques to handle images based on median filtering approach, handle low resolution images and due to compression not possible to restore complete data. Detecting forgery from large volume of data is a challenging task [16]. Authors in [6], introduced new method of forgery detection based median filtering to handle compressed data images, in their model they used regression techniques and Markov chain model, these two methods in turn use dimensionality reduction while detecting image forgery.

Image forgery can be detected using forensic techniques. It can be useful in many legal service oriented applications, and in turn these techniques resolve many criminal cases. In court of criminal laws separating original and duplicate images is more important task. Taxonomy of various forensic techniques is listed in Figure 1.

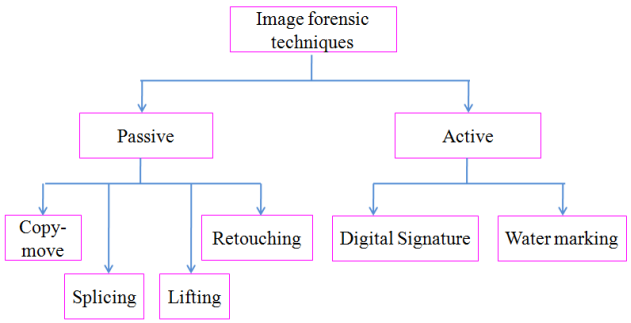

Figure 1: Classification of Image Forensic Techniques

Now a day's number of tools are available to change original images, with help of these tools one sub area of an images easily tampering with other, original and duplicate images are at most similar, and distinguish both images are one of the challenging task. To identify image forgery two active approaches are used is digital signature and other one is water making.

In digital signature (DS) image are partitioned in to 16*16 parts, for each sub area apply discrete wavelet transform, trace out DS, calculate hash code of traced out DS, compared received and calculated hash code, and with that identify forgery if any one of the signature mismatch. In water making technique check sum is added at LSB position, add length of input image, also calculate correlation coefficient of water maker images, and water marked images are not visible scanners or humans.

To identify image forgery three passive approaches are used and they are retouching, splitting and copy move method. Copy move forgery is one of the special categories of image forgery in which some area of an image is copied and replicated in the same image with an intention to hide valuable feature [10] of the image. In retouching forgery method image features are changed by rotating original image, resizing by changing resolution, and modify original image by stretch. In image splicing mostly used high contrast to modify edges of an image, apply image smoothing technique to smooth sub parts of an image or its corners.

II. RELATED WORK

In the market new updated editing tools and technologies are available to edit images and with help of these tools images are easily forged. Authors in [4] introduced forgery detection based on "copy-move" concept. They used many feature of images to detect forgery with high speed and also used exponential transform technique. Authors in [4] first partitioned image into small size blocks (b_1,b_2,…….b_n) using segmentation technique, and all these blocks are divided into two types. One is smooth and second is texture, images are compared for matching, and identify false or fake or forgery detection using proposed method.

In image processing area detecting forgery images under cut and paste mechanism is more complex than other image editing techniques. Authors in [5] proposed texture based method to detect forgery images, they divide images into different local regions, for each local region calculated median and entropy values, they used morphology technique to identify features, and they used new used kind of support vector machine to improve performance of forgery detection algorithm. In their research they have taken images of different types, they used window size of 3*3 and 5*5, all images are compressed before applying it to their method, and authors in [5] proved that their method will detect forgery even they used cut-paste mechanism to edit images.

Authors in [7] used median filtering to handle images of compressed, it is more important in image forgery detections or detection of fake video. Authors in [7] used machine learning technique (CNN) to handle input image, it is one of the self train and learning method. Their method resolve over filtering process and their method detect forgery even in compressed images. Image sharpening is a technique to enhance image visuals, if images are edited it is not possible to authenticate, the main goal of image forensic is to identify editing images, and to resolve this issue authors in[8] proposed new technique for image forgery based on image globalization. To analyze image pixels authors in [8] used more than ten different sets to extract features of input image, these features are useful to detect image forgery and performance of their method is evaluated with various types of data sets.

Due to limited availability of resources majority of deep learning techniques accept input images of small size and also these images are used resizing function to resize. Now a day images with high resolutions are available when applying resizing its quality will impact and it will degrade overall performance of a deep learning algorithms. Authors in[2] proposed CNN based forgery detection of images , processed images as patch, all high resolution are accept by their method, used check point method to train data samples, all parameters are restricted to use less memory space and take decisions with high resolution images whether it is forgery or original.

Morphology is more popular non linear functions, and widely used in many applications to discover features, to enhance images, and also useful to remove noise from images. Morphology based filtering approach useful to detect artifacts from edited images, and this method is used in image forensics. Authors in [9] extended deterministic model to detect forgery and used SVM for classification to extract image features. Authors in [12] conducted survey on image forgery problem, identification of resizing of original image, taken images without compressed, analyzed background of images, if the data is multimedia then detection of fake videos takes more time and they identify resizing of images using CNN method.

Now a day's information posted in the form of blogs, articles and libraries in various social media networks. Modern tools or software are available to edit images and it is difficult to identify original and duplicated or edited images. Earlier researchers on forgery detection proposed methods mostly based on handcraft mechanisms, problems facing by these methods are they will identify image forgery on a particular domain, and they are incapable to detect on all categories of images. Authors in [16] conducted detailed survey on forgery using deep learning technique with various types of image datasets. Forensics is now mostly used in many criminal cases to identify fake images to solve cases. Authors in [11] proposed a technique to detect tampered image, verifies authentication of images, and calculate hash code to detect image tampering.

III. PROPOSED METHOD

In this research paper we proposed new forgery detection technique with estimation of noise on various scale of input image affect of noise in input image occur several times, frequency of images are also changed due to noise, noise signal correlated with original input images and in compressed images quantization level frequency also changed due to noise. Overall idea of proposed forgery detection method is shown in Figure 2.

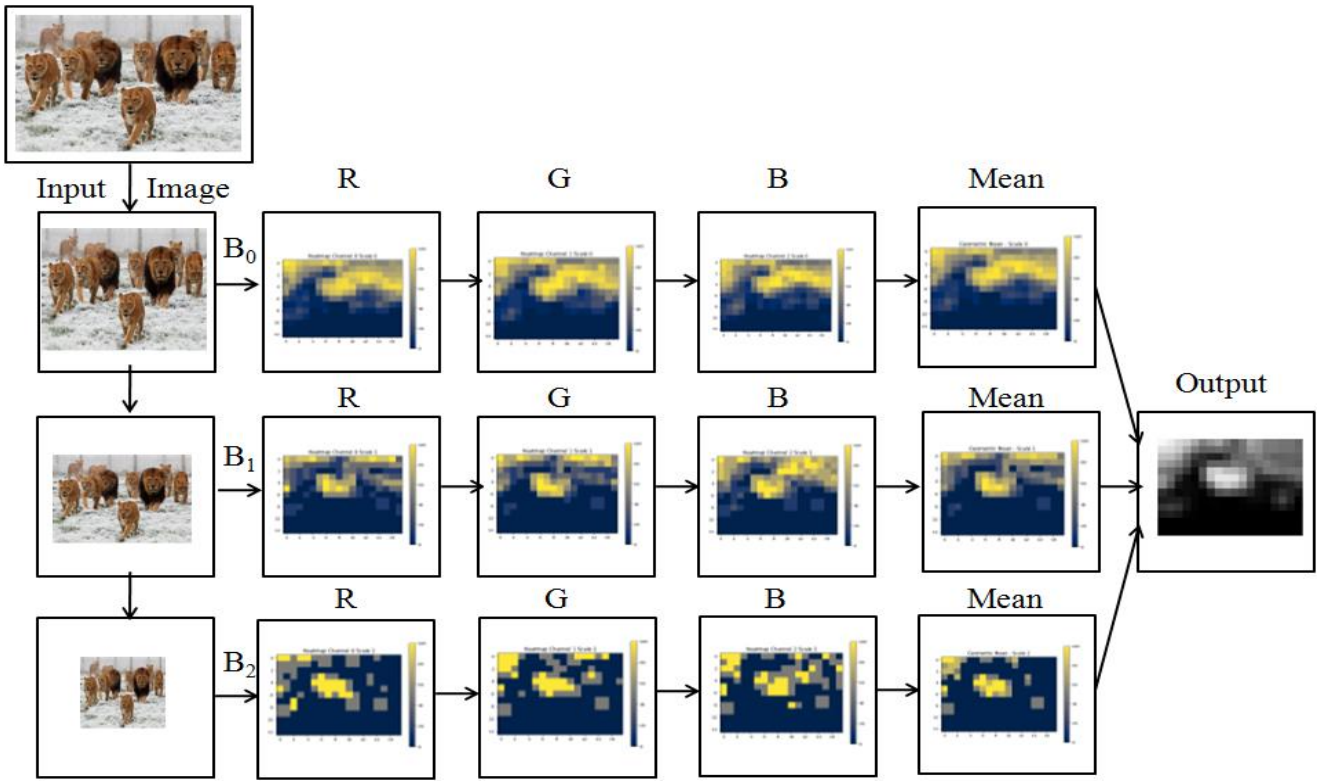

Figure 2: Forgery Detection Process

In this situation calculation of noise at local and goal level is more important in forgery detection method. For example input image (I) has C number of colors on image channels. We partition input image into M X N blocks, resized blocks are proceed further, image colors are also taken into consideration, each block noise value is evaluated at local level and global level. For each color channel of input image estimate local and global noise levels are estimated and compared using binning method. Also measured heat map of each block and each color channel of input image and all these values are stored in bins. Finally from all noise values calculate average mean value of noise. Algorithm is proposed to detect image forgery is as follows.

Algorithm:

Step 1: Select image which is suspect of forgery. Sample input image is shown in Figure 3.

Figure 3: Suspected Input Sample Image

Step 2: Fix block size and partition input image into smaller blocks based on block size.

$I = Input\ Image\ consist\ of\ (M_x, M_y)\ Blocks$

$C = Color\ Channel$

$$H_x = \left[\frac{M_x}{B\ X\ S}\right] - 1, Number\ of\ Horizantal\ Blocks.$$

$$H_y = \left[\frac{M_y}{B\ X\ S}\right] - 1, Number\ of\ Vertical\ Blocks.$$

Step 3: For each small block analyze color level, analyze histogram level at image boundaries, observe colors of block image and also calculate noise level of each smaller block and as well as global noise level of suspected image of forgery.

Step 4: Calculate heat map of each color channel of input block image and it is scaled to (0,255). To get output at the end merge all heat maps of individual smaller blocks.

Step 5: Noise level of image at global level is minimum then image is not tampered and if noise is high then decide image is tampered.

IV. PERFORMANCE EVALUATION

We executed proposed model, results are evaluated using scaling techniques, results are compared by varying one scale (B0), double scale (B1) and triple scale (B2), and also results noise values of blocks of proposed method compared with existing methods like splicing, retouching, and so on. To analyse performance of proposed method CG1050 dataset is used, these database has at most 1050 images, all these images are classified into four categories, images of this dataset are taken in different locations, all these images are captured with high resolution, all images are stored in two different forms one is colour and other one is gray [13], actually compressed version of images are stored in dataset, and for all these images original and as well as duplicate images are stored in the dataset.

Forgery detection is a binary classification technique, number of class label present is two (positive (yes or forged), negative (no or not forged), performance of a proposed method is measured with help of confusion matrix [14] [15]. Confusion matrix format to eavaluate performance of proposed algorithm is shown in Table 1.

Table 1: Confusion Matrix

		Predicted	
		P	N
Actual	P	True +ve	False -ve
	N	False +ve	True -ve

Let 'a' is a pixel, H is heat map value, M is mask of forgey, and four possible combination of confusion matrix values are calculated using following equations.

$$TP_I = \sum_a H(a) * M\ (a)$$

$$TN_I = \sum_a \big(1 - H(a)\big) * (1 - M\ (a))$$

$$FN_I = \sum_a H(a) * (1 - M\ (a))$$

$$FP_I = \sum_a (1 - H(a)) * M\ (a)$$

Let 'r' correlation coefficient, 'b' true positive, 'c' true negative, 'd' false negative, 'e' false positive, connection by Joining (J) and F1 is a score. These three performance evaluation metrics are used to proposed forgery method and are defined as follows.

$$r = \frac{b * c - d * e}{\sqrt{(b+e) * (b+d) * (c+e) * (c+d)}}$$

$$F_1 = \frac{2 * b}{2 * b + d + e}$$

$$J = \frac{b}{b + d + e}$$

Input image is scaled to one scale (O), double scale (D), Triple scale (T), correlation coefficient value (r) is measured using different forgery detection methods (Splicing (S), Coloring (CR), Retouching (R), and Copy move (CM)), and results are shown in Figure 4.

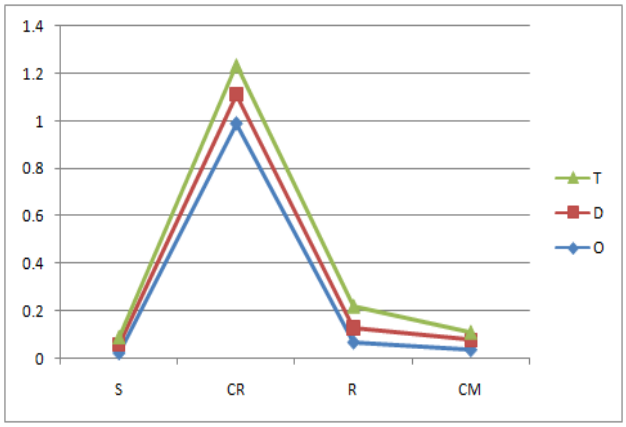

Figure 4: Forgery methods Vs. Correlation coefficient

Input image is scaled to one scale (O), double scale (D), Triple scale (T), correlation connection by Joining (J) is measured using different forgery detection methods (Splicing (S), Coloring (CR), Retouching (R), and Copy move (CM)), and results are shown in Figure 5.

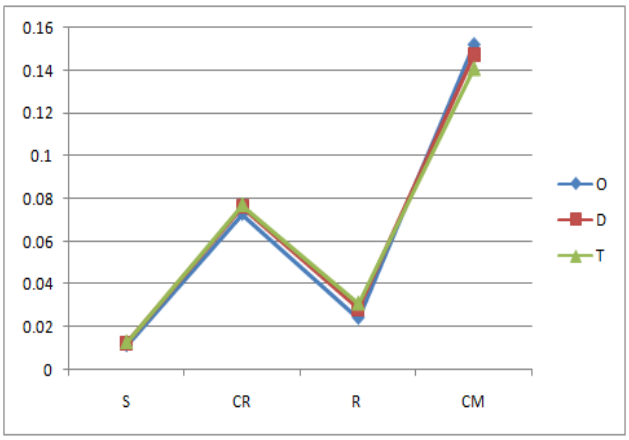

Figure 5: Forgery methods Vs. connection by Joining

Input image is scaled to one scale (O), double scale (D), Triple scale (T), correlation F_1 Score is measured using different forgery detection methods (Splicing (S), Coloring (CR), Retouching (R), and Copy move (CM)), and results are shown in Figure 6.

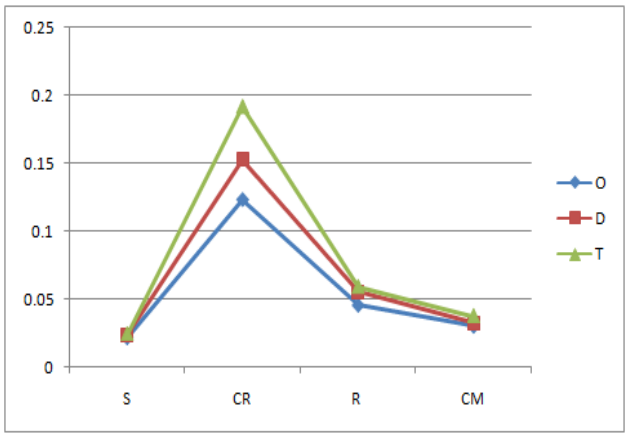

Figure 6: Forgery methods Vs. F1 Score

V. CONCLUSION

With latest development tools and technology, an image can be easily editable, untrained peoples may not in a position to differentiate original and forged images, many image processing tools are available to detect such a forgery images, all these tools are giving clues to detect forgery, a window sized boxes will scan entire images based on clues, and all these image forgery detection techniques are suffering with boundary problems. In this paper we proposed new forgery detection method to detect tampered images. Images are fitted into three different scales, color of the images and heat map of each channel are calculated, noise level are measured local areas and global areas of images, and from these values easily identify tampered images. Performance of proposed method is analyzed by using correlation coefficient, connection by Joining, and F_1 Score.

Retrieval Number: 100.1/ijitee.I97030812923
DOI: 10.35940/ijitee.I9703.0812923
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

DECLARATION

Funding/ Grants/ Financial Support	No Funding.
Conflicts of Interest/ Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	All authors having equal contribution for this article.

REFERENCES

1. B. P. Das, M. Biswal, A. Panigrahi, M. Okade, "CNN Based Image Resizing Detection and Resize Factor Classification for Forensic Applications", 2021 2nd International Conference on Range Technology (ICORT), pp. 1-6, 2021.
2. F. Marra, D. Gragnaniello, L. Verdoliva, G. Poggi, "A Full Image Full-Resolution End-to-End-Trainable CNN Framework for Image Forgery Detection", IEEE Access, vol. 8, pp. 133488-133502, 2020. https://doi.org/10.1109/ACCESS.2020.3009877
3. K. H. Rhee, "Detection of Spliced Image Forensics Using Texture Analysis of Median Filter Residual", IEEE Access, vol. 8, pp. 103374-103384, 2020. https://doi.org/10.1109/ACCESS.2020.2999308
4. C. Wang, Z. Zhang, Q. Li, X. Zhou, "An Image Copy-Move Forgery Detection Method Based on SURF and PCET", IEEE Access, vol. 7, pp. 170032-170047, 2019. https://doi.org/10.1109/ACCESS.2019.2955308
5. D. Wang, T. Gao, Y. Zhang, "Image Sharpening Detection Based on Difference Sets", IEEE Access, vol. 8, pp. 51431-51445, 2020. https://doi.org/10.1109/ACCESS.2020.2980774
6. X. Lin, C.T. Li, "PRNU-Based Content Forgery Localization Augmented With Image Segmentation", IEEE Access, vol. 8, pp. 222645-222659, 2020. https://doi.org/10.1109/ACCESS.2020.3042780
7. S. Luo, A. Peng, H. Zeng, X. Kang, L. Liu, "Deep Residual Learning Using Data Augmentation for Median Filtering Forensics of Digital Images", IEEE Access, vol. 7, pp. 80614-80621, 2019. https://doi.org/10.1109/ACCESS.2019.2923000
8. A. Peng, S. Luo, H. Zeng, Y. Wu, "Median Filtering Forensics Using Multiple Models in Residual Domain", IEEE Access, vol. 7, pp. 28525-28538, 2019. https://doi.org/10.1109/ACCESS.2019.2897761
9. Q. Yin, J. Wang, X. Luo, J. Zhai, S. K. Jha, Y. Q. Shi, "Quaternion Convolution Neural Network for Color Image Classification and Forensics", IEEE Access, vol. 7, pp. 20293-20301, 2019. https://doi.org/10.1109/ACCESS.2019.2897000
10. K. T. Ahmed, S. Jaffar, M. G. Hussain, S. Fareed, A. Mehmood, G. S. Choi, "Maximum Response Deep Learning Using Markov Retinal & Primitive Patch Binding With GoogLeNet & VGG-19 for Large Image Retrieval", IEEE Access, vol. 9, pp. 41934-41957, 2021. https://doi.org/10.1109/ACCESS.2021.3063545
11. Z. J. Barad, M. M. Goswami, "Image Forgery Detection using Deep Learning: A Survey", 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2020, pp. 571-576. https://doi.org/10.1109/ICACCS48705.2020.9074408
12. W. Wang et al., "Anomaly detection of industrial control systems based on transfer learning", Tsinghua Science and Technology, vol. 26, no. 6, pp. 821-832, Dec. 2021. https://doi.org/10.26599/TST.2020.9010041
13. G. Boato, D. Dang-Nguyen, F.G.B. De Natale, "Morphological Filter Detector for Image Forensics Applications", IEEE Access, vol. 8, pp. 13549-13560, 2020. https://doi.org/10.1109/ACCESS.2020.2965745
14. Jing Dong, Wei Wang, Tieniu Tan, "CASIA Image Tampering Detection Evaluation Database", IEEE China Summit and International Conference on Signal and Information Processing, 2013. https://doi.org/10.1109/ChinaSIP.2013.6625374
15. B. V. Somasundaran, R. Soundararajan, S. Biswas, "Image Denoising for Image Retrieval by Cascading a Deep Quality Assessment Network", 2018 25th IEEE International Conference on Image Processing (ICIP), pp. 525-529, 2018. https://doi.org/10.1109/ICIP.2018.8451132
16. M. Giri, S.Jyothi, "Big Data Collection and Correlation Analysis of Wireless Sensor Networks Yielding to Target Detection and Classification", Springer Lecture Notes on Data Engineering and Communications Technologies, Vol. 9, ISSN: 2367-4512, print ISBN: 978-981-10-6318-3, pp. 201-213, 2017. https://doi.org/10.1007/978-981-10-6319-0_18

AUTHOR PROFILES

Mahesh Enumula is currently pursuing Ph.D in Bhagwanth University, Ajmer, Rajasthan, India on the research topic Image forgery detection using Artificial Intelligence. He did Bachelors and Masters in Technology on Electronics and Communication Engineering from JNTU, Andhra Pradesh, India. He is holding a patent on Image forgery detection topic from the Government of Australia. Apart from Artificial Intelligence his interests are Embedded systems and VLSI Design. He is having 9 international journal papers and 4 conference papers.

Dr. M. Giri Professor, Department of CSE, Siddharth Institute of Engineering and Technology, Puttur. He did his B.Tech in Computer Science & Engineering from Sree Vidya Nikethan Engineering College, Tirupati, affiliated to JNTU, Hyderabad, in 2001. He did his M.Tech in Computer Science & Engineering from School of IT, JNTU Hyderabad campus, Hyderabad in 2009. He did his Ph.D in Computer Science & Engineering from Raalaseema University, Kurnool, in 2018. He is having 22 years of teaching experience. He organized and participated in various Workshops, FDPs, Seminars in different areas of Computer Science during his tenure. He has published 68 papers in various reputed International/National journals and Conferences. He is a member of IEEE, MCSIT, MIAENG and MCSTA. His research area includes Data Mining, Wireless Sensor Networks, Artificial Intelligence, Cryptography, Network Security, Cloud Computing and IoT.

Dr. V. K. Sharma received his B.E. degree in Electrical Engineering from KREC (NIT), Surathkal, India in 1984 and received his M.Tech degree in Power Electronics from IIT Delhi, India in 1993. He received his Ph.D. degree in the field of Electric Drives from IIT Delhi, India in 2000 and he has done one year stint as Post-Doctoral Fellow in Active Filters from ETS, Montreal Canadain 2001. Presently, he is a Vice-Chancellor of Bhagwant University, Ajmer, India and he is also Professor in the department of EEE since 2014. He is having total 36 years of teaching experience. He has authored or co-authored over more than 200 papers in various SCI, SCOPUS Indexed and other national, international journals. He completed major projects sponsored by public funding agencies like AICTE, DST etc. He received various awards like Railway Board Medal, Lions Award, and UGC Research Associate etc. His research interests include Electric Drives, Active Filters, Antennas and Renewable energy conversion techniques. He is a senior member of IEEE, Fellow IETE and Member IE (I).