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 the help of these tools, images can be easily forged. In this research paper, we propose a new forgery detection technique that estimates the noise on various scales of input images. The effect of noise on input images is also taken into account. Additionally, the frequency of images is altered due to noise. Furthermore, the noise signal is correlated with the original input images, and in compressed images, the quantisation level frequency is also changed due to noise. We partition the input image into M × N blocks. The resized blocks are then processed further, taking into consideration the image colours. The noise value of each block is evaluated at both local and global levels. For each colour channel of the input image, regional and global noise levels are estimated and compared using a binning method. Also, a heat map was measured for each block and each colour channel of the input image, and all these values were stored in bins. Finally, calculate the average mean value of noise from all noise values. With these values, decide whether the input image is a forgery or not. The performance of the proposed method is then compared with that of existing processes.***

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

I. INTRODUCTION

With the latest development tools and technology, an image can be easily edited, and untrained people may not be in a position to differentiate between 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 pictures based on clues, and all these image forgery detection techniques are suffering with boundary problems. Authors in [3] introduced an image locations technique to detect forgery within segments. Image localization is done with noise and photo response technique, taking the homogeneity of the local region to detect forgery based on small clues, and the authors[3] combined localization technique and window based frame work to detect forgery images. Median filtering is widely used in multimedia-based applications, such as steganography and image forensics. This filtering approach is mostly a nonlinear technique that also preserves data. Earlier researchers in image processing proposed various methods to handle images using the median filtering approach, which is effective for handling low-resolution photos. However, due to compression, it is not possible to restore complete data. Detecting forgery from a 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 helpful in many law service-oriented applications, and in turn, these techniques help resolve many criminal cases. In a court of criminal law, separating original and duplicate images is a more critical task. The taxonomy of various forensic methods is listed in Figure 1.

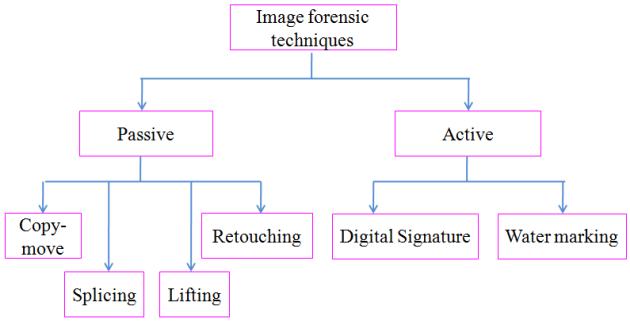

Figure 1: Classification of Image Forensic Techniques

Today, numerous tools are available to alter original images. With the help of these tools, one can easily tamper with an image's sub-area, making original and duplicate images appear similar. Distinguishing between the two images is a challenging task. To identify image forgery, two active approaches are used: digital signature and watermarking.

In a digital signature (DS) image, each 16x16 part is partitioned, and a discrete wavelet transform is applied to each sub-area. The DS is then traced out, and the hash code of the traced DS is calculated. The received and calculated hash codes are compared, and forgery is identified if any of the signatures mismatches. In the water making technique, a checksum is added at the LSB position. The length of the input image is also added. Additionally, the correlation coefficient of the water maker images is calculated. Watermarked photos are

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

invisible to scanners and humans.

To identify image forgery, three passive approaches are used: retouching, splitting, and the 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 to hide valuable features [10] of the image. In retouching forgery methods, image features are altered by rotating the original image, resizing it by changing the resolution, and modifying the original image by stretching or distorting it. In image splicing, high contrast is primarily used to alter the edges of an image, while image smoothing techniques are applied to smooth out subparts of an image or its corners.

II. RELATED WORK

In the market, new and updated editing tools and technologies are available to edit images, and with the help of these tools, images can be easily manipulated. Authors in [4] introduced forgery detection based on the "copy-move" concept. They utilised various image features to detect forgery at high speed and also employed the 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 the second is texture. Images are compared to identify matching and false or fake images using the proposed method.

In the image processing area, detecting forged images under the 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, using window sizes of 3x3 and 5x5. All images are compressed before applying them to their method, and the 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 critical 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 resolves the over-filtering process and detects forgery even in compressed images. Image sharpening is a technique used to enhance the visual quality of an image. If images are edited, it is not possible to authenticate. The primary goal of image forensics is to identify edited images and 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 helpful to detect image forgery and performance of their method is evaluated with various types of data sets.

Due to the limited availability of resources, the majority of deep learning techniques accept input images of small size, which are often resized using a specific function. Today, high-resolution images are available, and when resizing, their quality can impact and degrade the overall performance of 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 commonly used with non-linear functions and is widely employed in various applications to detect features, enhance images, and remove noise from images. A morphology-based filtering approach is practical for detecting artefacts in edited photos, and this method is commonly 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 photos, if the data is multimedia then detection of fake videos takes more time and they identify resizing of images using CNN method.

Nowadays, information is posted in the form of blogs, articles and libraries in various social media networks. Modern tools and software are available to edit images, making it difficult to distinguish between original and duplicated or edited photos. Earlier researchers in forgery detection proposed methods that were primarily based on handcrafted mechanisms. The problems facing these methods are that they identify image forgery in a particular domain and are incapable of detecting fraud in 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 primarily used in many criminal cases to identify fake images to solve cases. Authors in [11] proposed a technique to detect tampered images, verify the authentication of images, and calculate a 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. The overall idea of the proposed forgery detection method is shown in Figure 2.

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)

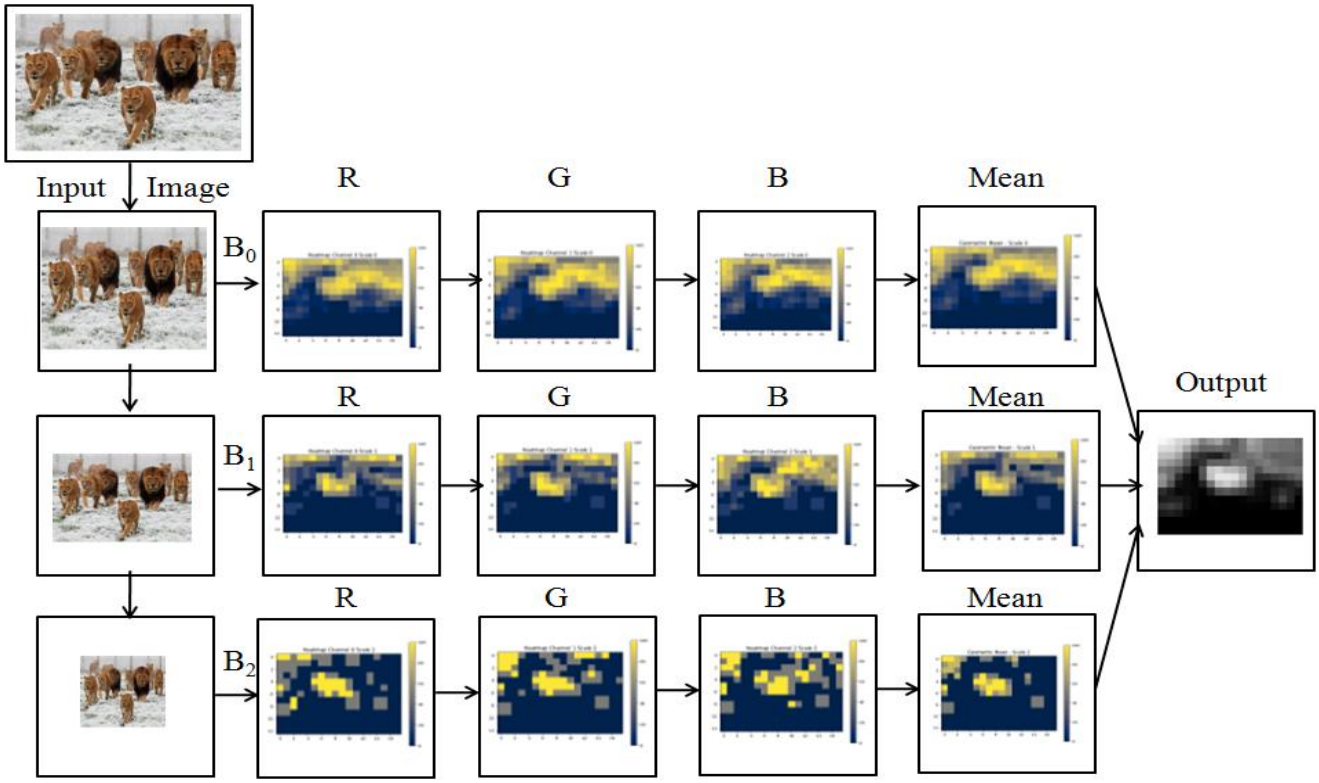

Figure 2: Forgery Detection Process

In this situation, calculating noise at both local and goal levels is crucial for effective forgery detection methods. For example, the input image (I) has C number of colours on its image channels. We partition the input image into M × N blocks. The resized blocks are then processed further, taking into consideration the image colours. The noise value of each block is evaluated at both local and global levels. For each colour channel of the input image, regional and global noise levels are estimated and compared using a binning method. Also, a heat map was measured for each block and each colour channel of the input image, and all these values were stored in bins. Finally, calculate the average noise value from all noise values. The proposed algorithm for detecting image forgery is as follows.

Algorithm:

Step 1: Select an image which is suspected of forgery. The sample input image is shown in Figure 3.

Figure 3: Suspected Input Sample Image

Step 2: Adjust the block size and partition the input image into smaller blocks accordingly.

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

$C = Color\ Channel$

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

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

Step 3: For each small block, analyse the colour level, examine the histogram level at image boundaries, observe the colours of the block image, and calculate the noise level of each smaller block as well as the global noise level of the suspected image of forgery.

Step 4: Calculate a heat map for each colour channel of the input block image, scaling it to (0, 255). To obtain the final output, merge all heat maps of the individual smaller blocks.

Step 5: The noise level of the image at the global level is minimum; then the image is not tampered with. If the noise level is high, then the image is likely tampered with.

IV. PERFORMANCE EVALUATION

We executed the proposed model, and the results are evaluated using scaling techniques. The results are compared by varying one scale (B0), double scale (B1), and triple scale (B2). Additionally, the noise values of blocks in the proposed method are compared with those of existing processes, such as splicing and retouching. 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

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

are stored in dataset, and for all these images original and as well as duplicate photos are stored in the dataset.

Forgery detection is a binary classification technique; the number of class labels present is two (positive (yes or forged), negative (no or not forged)). The performance of a proposed method is measured with the help of a confusion matrix [14] [15]. The confusion matrix, used to evaluate the performance of the 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' be a pixel, H be a heat map value, M be a mask of forgery, and four possible combinations of confusion matrix values are calculated using the 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' genuine 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 propose a 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.

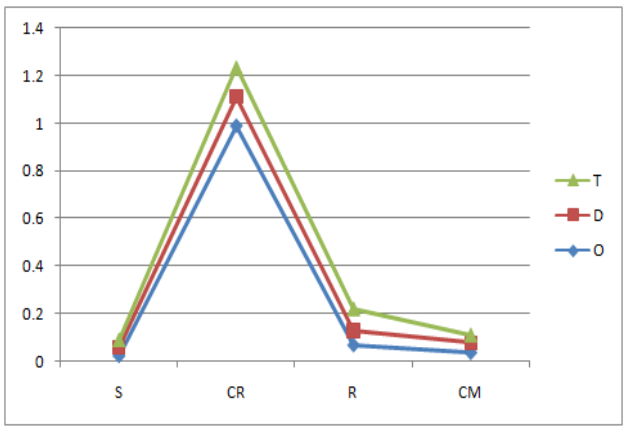

Figure 4: Forgery methods Vs. Correlation coefficient

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.

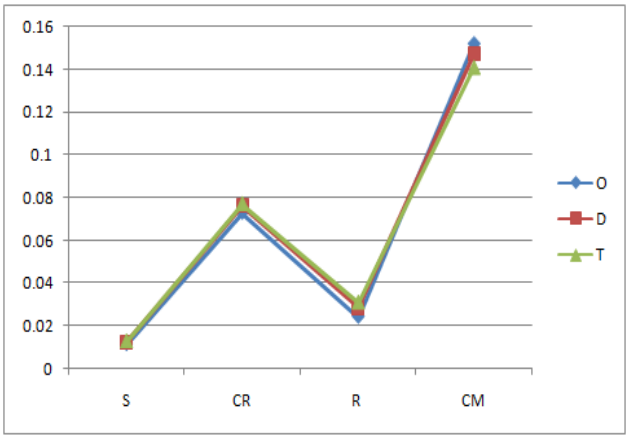

Figure 5: Forgery methods Vs. Connection by joining

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.

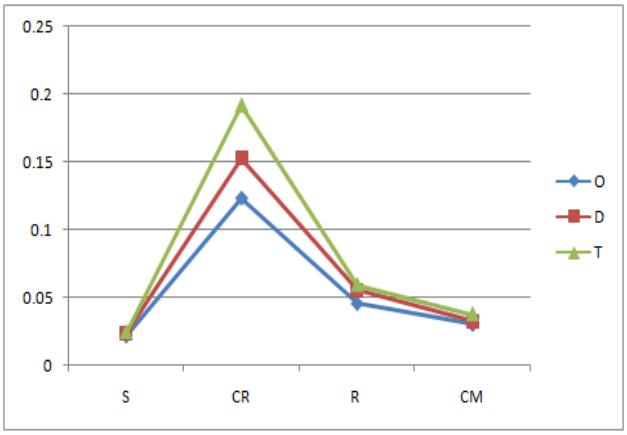

Figure 6: Forgery methods Vs. F1 Score

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 propose a novel forgery detection method for identifying tampered images. Images are fitted into three different scales. The colour of the images and the heat map of each channel are calculated. Noise levels are measured in both local and global areas of the images. From these values, it is easy to identify tampered images. The performance of the proposed method is analysed using the correlation coefficient, connection by Joining, and F_1 Score.

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 or consent to participate, as it presents evidence that is not subject to interpretation.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	All authors have equal contributions to 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 a Ph.D. at Bhagwanth University, Ajmer, Rajasthan, India, on the research topic of Image forgery detection using Artificial Intelligence. He obtained a Bachelor's and Master's degree in Technology with a specialisation in Electronics and Communication Engineering from JNTU, Andhra Pradesh, India. He holds a patent on the topic of image forgery detection from the Government of Australia. Apart from Artificial Intelligence, his interests include Embedded Systems and VLSI Design. He has nine international journal papers and 4 conference papers.

Dr. M. Giri Professor, Department of CSE, Siddharth Institute of Engineering and Technology, Puttur. He completed his B.Tech in Computer Science and Engineering from Sree Vidya Nikethan Engineering College, Tirupati, which is affiliated with JNTU, Hyderabad, in 2001. He completed his M.Tech in Computer Science and Engineering from the School of IT at the JNTU Hyderabad campus in Hyderabad in 2009. He completed his Ph.D. in Computer Science and Engineering from Raalaseema University, Kurnool, in 2018. He has 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 reputable international and national journals and Conferences. He is a member of IEEE, MCSIT, MIAENG and MCSTA. His research areas include 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 (now NIT), Surathkal, India, in 1984, and 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 spent one year as a Post-Doctoral Fellow in Active Filters at ETS, Montreal, Canada, in 2001. Presently, he serves as the Vice-Chancellor of Bhagwant University, Ajmer, India, and has been a Professor in the Department of EEE since 2014. He has a total of 36 years of teaching experience. He has authored or co-authored over 200 papers in various SCI and SCOPUS-indexed, as well as other national and international journals. He completed major projects sponsored by public funding agencies, such as AICTE and DST. He received various awards, including the Railway Board Medal, the Lions Award, and the UGC Research Associate award. His research interests include Electric Drives, Active Filters, Antennas and Renewable energy conversion techniques. He is a senior member of IEEE, a Fellow of IETE, and a Member of IE (I).