ISSN No:-2456-2165

Analysis on Capabilities of Artificial Intelligence(AI) Image Forgery Detection Techniques

Mahesh Enumula
Research scholar, Department of ECE,
Bhagwant University, Ajmer

Dr. M. Giri
Professor, Dept. of CSE, Siddharth Institute
of Engineering and Technology, Puttur, India

Dr. V. K. Sharma
Professor, Dept. of ECE, Bhagwant University Ajmer,

Abstract:- Cybersecurity has become a serious threat to society because of the revolution on the internet. Due to the internet revolution worldwide people are consuming quintillion bytes of data on daily basis. The data consumption over the internet may increase in the feature at the same time the threats to internet security posing new questions to the world. One of the major problems in cybersecurity is image forgery. An effective mechanism to detect image forgery is needed to avoid complications in various fields like medical imaging, space research, defense, etc., where even small details in the images are very crucial. In the present research by taking the advantage of Artificial intelligence an effective model is built. This model in the pre-processing stage of the image uses superpixels. These features will be provided as inputs to the deep neural network. Basically, the neural network acts as a classifier of the images. The convolutional neural networks are built and optimized according to the input data. The convolutional neural networks are being trained by a large number of image data set and will be tested for the results. When the trained CNN is supplied with the images which are needed to be detected for the forgery in the initial stages the images will be divided into blocks that are non-uniform and features will be extracted which consists of superpixels. These features will be supplied to the classifier. The classifier not only detects the forged image and non forged image but also indicates the location of the forgery.

The present research paper compares various methods of image forgery detection. In the comparison, the proposed method will enhance performance matrices in terms of accuracy, precession, Recall, etc.

Keywords:- *Forgery detection, Deep neural network, Artificial intelligence, Convolutional neural network, superpixels, Feature extraction, accuracy, precession, recall, confusion matrix.*

I. INTRODUCTION

Internet usage has increased drastically in the previous decade. The pandemic and lockdowns increased the consumption of internet data. In 2021 one report saying that people over worldwide are using 2.4 quintillion bytes of data on a day to basis. In the feature, it may reach new heights. Safety and security over the internet is a challenging task. Cybercriminals are posing a lot of questions to the world with their attacks. Thousands of people are becoming victims of cyberattacks. Governments are also trying to create awareness over cybersecurity.

One of the problems in cybersecurity is image forgery. The forged images are creating a serious threat to society. There are many fields like biomedical imaging, defense, space research, etc where even small detail in the image is very crucial. For example, if take biomedical imaging, an intruder may change small detail of patient data like x-ray or scan reports which may lead to false results. In the case of defense, the opponent areal images may mask or non-mask. In the case of space research, a forged image may be circulated over public platforms by creating wrong impressions. There are a lot of aspects relating to the children and women safety concerns when they use social networking platforms due to image forgery. A report says that daily 1.8 billion photos are being exchanged over the internet so there is a high risk of image forgery. mage Forgery Detection technique is one of the important research in image processing. Digital media is the leading technology in the present day. For a passive technique, a digital signature is inserted in the original image. The condition of the received image is used to evaluate the digital signature's performance. Active and passive image forgery detection approaches are divided into two categories (blind). The photos are protected against fabrication using the strong Secret Key technique [1]. Copy move forgery is a well-known and widely used method of copying and pasting in the same image. Forgers utilise image editing software such as Adobe Photoshop and GIMP to alter the contents of digital photos. Image tampering is not a new problem. The content of digital photographs is authenticated using digital signatures and digital watermarking [2]. To detect the modifications in the original image, a hybrid approach for Copy-Move Image Forgery is applied. Picture processing technologies are used to change the unique data, such as blurring and resizing the photographs, in order to alter the information. Non-copy and copy changes are the two types of image tampering [3]. Manipulation is used to remove images that have been hidden. Image forgery detection is an important and active technology in the study field. In the digital watermarking and digital signature techniques, active forgery detection approaches are applied [4] Semi-fragile image hashing.

The most difficult techniques in picture forensics are watermarking and passive procedures. The new image forgery detection uses Convolution Neural Network (CNN) algorithms [5]. In our daily lives, digital images and videos are extremely important. Digital photographs can be easily changed using image editing software such as Adobe

ISSN No:-2456-2165

Photoshop. Digital signature and watermarking systems are the most common active methods. The passive approaches do not require any explicit prior image information. Format-based, pixel-based, physic-based, camera-based, and geometry-based methods are the five basic categories of digital techniques. For detecting fraud in original photos, the Discrete Cosine Transform (DCT) approach is used [6]. The World Wide Web (WWW) now contains a large number of digital images for efficient communication. The most common image tampering operations are: I hiding or removing a region in the image; ii) adding a new object to the image; and iii) misrepresenting image information. One of the most common techniques for manipulating or hiding the content of an image is CM image manipulation. Feature extraction, copy decision, and matching algorithms are used to identify CM forgery [7]. The most frequent types of digital picture forgeries in image processing techniques are copy-move and splicing. Copy-move forgery is a photo modification technique that involves copying a section from an image and putting it in other places. When the forged area is not doubly compressed, edge information is employed to locate it [8].

Forgery of images is a common blunder. The pixel is the basic building element of a digital image in digital image forensics. In digital image forensics, pixels are the fundamental building blocks. Digital cameras nowadays contain a single CMOS or CCD sensor and employ Color Filters Array (CFA) [9]. Digital picture counterfeiting has become a big problem as a result of strong image altering tools. As a result, colour moments are employed in the original image to detect image counterfeiting. In today's world, low-cost digital cameras and cell phones are ubiquitous. Journalistic, criminal, medical imaging, and forensic investigations are just a few of the domains where it's applied. To overlap square blocks, the detecting copy-move forgery images are employed.The performance of the model will be evaluated with the True positive (TP), True Negative (TN), False Positive (FP), False Negative (FN), Precision (P), Recall (R), Similarity (S), False measure (FM), True Positive Rate (TPR), False Positive Rate (FPR) and accuracy.

II. TYPES OF IFD APPROACHES

Nowadays, removing and adding parts from an image for the purpose of manipulation and getting good results from image forgeries is simple. Different types of software are used in image processing. Some applications can alter a specific image block without altering the image's originality. This type of change is undetectable to the naked eye. The most important duty is to double-check the original photograph. Image manipulation techniques such as scaling, rotation, blurring, filtering, and cropping can all be used to manipulate an image. Image forgery detection is essential in a variety of image processing applications. Image forgery detection is a growing research subject with crucial implications for maintaining digital image trustworthiness.

Image forgery detection(IFD) can be classified into two approaches:

A. Active Approach

B. Passive Approach

- **Active Approach:** In the active approach, some digital image preparation, such as integrated watermark or signature production, is necessary at the time of creation, which limits the image's applicability. This method is not employed for the purpose of authentication.
- **Passive Approach:** The digital signature is not employed for authentication in the passive technique. Some assumptions are used in this technique, such as the fact that digital forensics may not leave any visual clues for image tempering. It has the potential to change the image's underlying statistics.

The image forgery detection tools can be grouped into five groups:

- Camera based technique
- Physically based technique
- Geometric based technique
- Pixel based technique
- Format based technique

III. TECHNIQUES IN ARTIFICIAL INTELLIGENCE

Machine learning(ML) and Deep learning(DL) are two equally important tools in Artificial intelligence. But when it comes to a problem related to digital image processing the techniques in deep learning are more suitable.The idea of Deep learning is mostly dependent on nueral networks.By taking the inspiration from biological neural networks the artificial neural networks were built to solve the problems.Depending upon type of the problem the particular type of neural networks can be utilized in the deep learning model.The deep learning models depending upon type of nueral networks can be broadly classified as:

A. Artificial Nueral Networks (ANN):

An ANN consists of three different types of layers called as input layers,output layers and hidden layers.Each layer consists of nodes.These nodes can be called as neurons which performs the similar operation of nuerons in biological human brain.Each and every node will be connected with the neighbor nodes.These connections makes the signal to travel in between the nodes. Each node will have some weight and will act as an activation function depending upon threshold of the input signal. The weight of the neuron may increase or decrease depending upon balancing of the weights in backpropogation. These ANNs will be trained with dataset until the weights are tuned for the problem. On the trained networks the real data will be applied which in the problem domain for the required results. In ANNs through testing of performance parameters the results will be optimized.The most important thing is care shuld be taken in size of the data set while training the model in order to avoid over tuning and under tuning.

ISSN No:-2456-2165

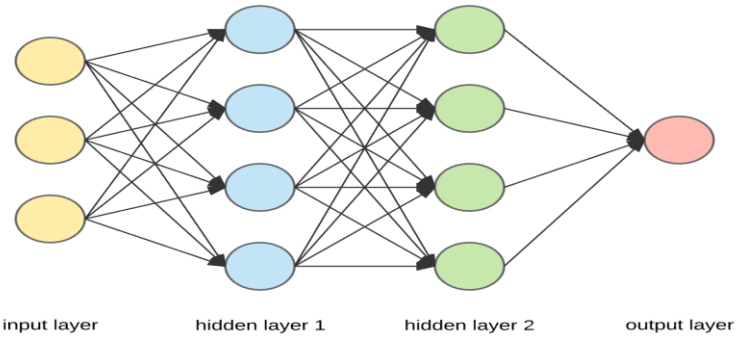

Fig. 1: Depiction of different layers in ANN

B. Convolutional Nueral Networks(CNN):

In deep learning, a convolutional neural network or ConvNet is a type of deep neural network. The frequent use of CNN is to solve the problems of images/videos. CNNs have applications in image and video recognition, image classification, , recommender systems, medical image analysis,image segmentation, brain-computer interfaces, financial time series and natural language processing.CNNs uses network as multilevel perceptrons. Multilevel perceptrons usually connects networks of nodes in all the possible paths.These networks makes them vulnerable to data overfitting.Regularization, or preventing overfitting, can be accomplished in a variety of methods, including punishing parameters during training (such as weight loss) or reducing connectivity (skipped connections, dropout, etc.) CNNs use a different method to regularisation: they take advantage of data's hierarchical pattern and piece it together. As a result, CNNs are at the lower end of the connectivity and complexity spectrum. Convolutional networks were motivated by biological processes because their connectivity pattern matches the arrangement of the animal visual cortex. Individual cortical neurons respond to inputs only in the receptive field, which is a small portion of the visual field. Different neurons' receptive fields partially overlap, allowing them to encompass the full visual area. In comparison to other image classification methods, CNNs require very little pre-processing. This means that the network learns to optimise the filters (or kernels) by automatic learning, as opposed to hand-engineered filters in traditional techniques. This lack of reliance on prior information or human intervention in feature extraction is a significant benefit.

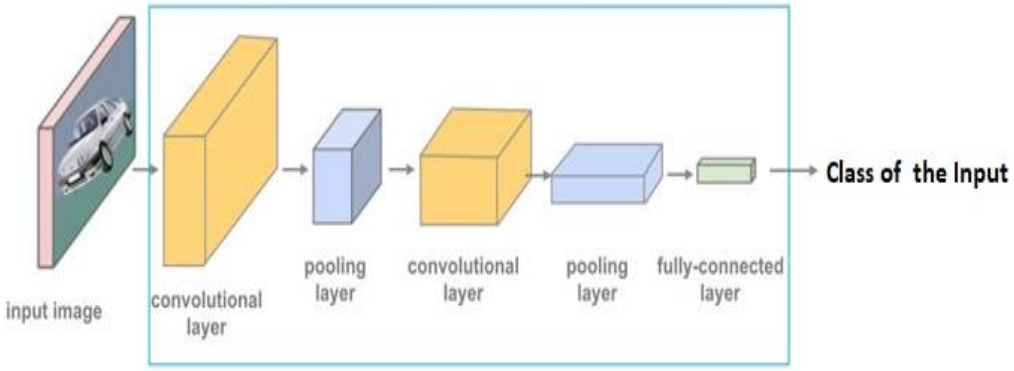

Fig. 2: Illustration of different stages in CNN

C. Recurrent Nueral Networks(RNN):

A recurrent neural network (RNN) is a type of neural network containing loops that allow data to be stored inside the network. Recurrent Neural Networks, in short, use their reasoning from prior experiences to predict feature events. Recurrent models are useful because they can sequence vectors, allowing the API to execute more complex tasks. Recurrent Neural Networks are a collection of networks that are linked together. They frequently feature a chain-like architecture, making them useful for tasks like speech recognition and language translation. An RNN can be programmed to work with vector sequences in the input, output, or both. A sequenced input, for example, might accept a text as input and return a positive or negative sentiment value.A sequenced output, on the other hand, may take an image as input and output a statement. Consider training an RNN to recognise the word "happy" using the letters "h, a, p, y." The RNN will be trained on four different examples, each of which represents the possibility that letters will fall into the correct order. For example, the network will be trained to recognise the likelihood that the letter "a" would appear after "h." The letter "p" should also appear after "ha" sequences. Following the sequence "hap," . probability will be calculated once again for the letter "p." The procedure will be repeated until probabilities have been computed to determine the possibility of letters falling into the desired order. As the network receives each input, it calculates the likelihood of the next letter depending on the previous letter's or sequence's probability. The network can be modified over time to offer more accurate findings. Machine translation is a popular application of Recurrent Neural Networks. A neural network, for example, could take a Spanish statement and convert it into an English sentence. The network calculates the probability of each word in the sentence. output sentence based on the word and the output sequence before it.

ISSN No:-2456-2165

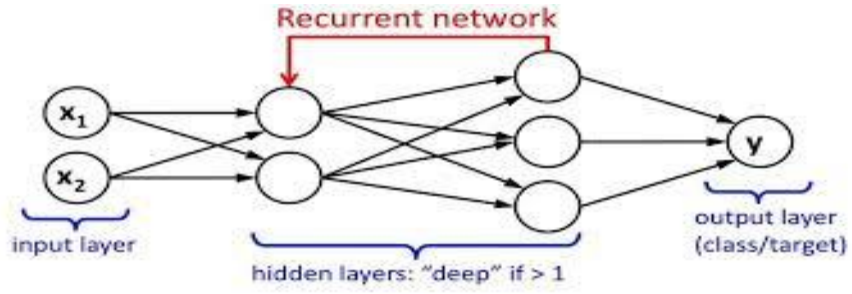

Fig. 3: Nuerons connection in RNN

IV. IFD USING AI METHOD

The IFD-AI method mainly consists mainly two stages.one is Feature Extraction and Second one is Neural network classifier. The raw image which is suspected for the forgery will be given as input to the initial stage.The classified image will be collected as output from the Neura Network classifier as shown in the FIGURE 4.

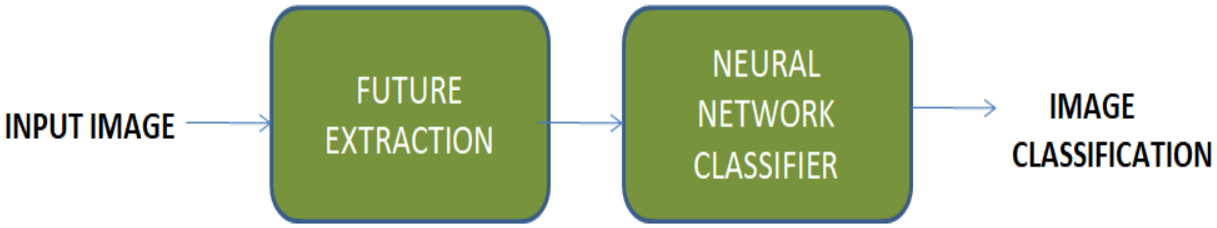

Fig. 4: Block Diagram of IFD using AI method

A. Feature Extraction:

Natural images have the property of being "stationary," which means that the statistics of one area of the image are the same as the statistics of any other section of the image. This implies that the features we learn in one portion of the image may be applied to other areas of the image, and that the same features can be used elsewhere. We can then use our learnt 8x8 feature detector wherever in the image after learning features across small (say 8x8) patches sampled randomly from the bigger image. In particular, we can "'convolve'" the learnt 8x8 features with the bigger image, yielding a distinct feature activation value at each place in the image. Consider the following scenario: you've learned features on 8x8 patches sampled from a 96x96 image. Assume that this was accomplished using an autoencoder with 100 hidden units. To retrieve the convolved features, take the 8x8 patch from each 8x8 section of the 96x96 image, starting at (1,1),(1,2),...(89,89), and run it through your trained sparse autoencoder to get the feature activations. As a result, there would be 100 sets of 89x89 convolved features.

B. Neural Network Classifier:

The massively parallel-disturbed structure of neural networks (NNs) is what gives them their processing capacity. Which have a tremendous capacity for learning complex and non-linear correlations involving noisy or less exact data. NNs are simple electronic networks of neurons based on the brain's neural organisation. They process records one at a time, learning by comparing their (mostly arbitrary) classification of the record to the known true classification of the record. The faults from the first record's initial categorization are fed back into the network and utilised to tweak the network's algorithm for subsequent rounds. There are two primary processes in the classifying process.

C. NN training:

The correct class for each record is known (this is referred to as supervised training), and the output nodes can be assigned proper values — 1 for the node matching to the correct class, and 0 for the rest. (In practise, values of 0.9 and 0.1 have been proven to produce superior outcomes.) As a result, the network's calculated output node values may be compared to these accurate values, and an error term can be calculated for each node (the Delta rule). These erroneous words are then utilised to change the weights in the hidden layers, presumably bringing the output values closer to the right values during the following iteration.

The initial task in the training phase is pre-processing, which entails resizing the input image to 512x512 pixels. The over segmentation algorithm was used to divide the scaled picture into small parts.. The next crucial stage in the feature extraction is to turn each segmented block into three planes, such as red, green, and blue. In this step, three different types of characteristics are extracted for each plane. Statistical features, DCT and SIFT features, as well as the features themselves, are saved in an array, which is then trained on a neural network. The training step saves the data in an array, which is then passed to the NN testing phase.

- *Neural network (NN) testing:*

The computational capacity of an ArtificialNeural network (NN) is derived from its massively parallel-disturbed structure, as shown in Fig.4. They have a remarkable ability to understand complex, non-linear relationships involving noisy or less exact data. ANNs are simple electronic networks of neurons based on the brain's neural structure. They process records one at a time, learning by comparing their (mostly arbitrary) classification of the record to the known true classification of the record. The faults from the first record's initial categorization are fed back into the network and

ISSN No:-2456-2165

utilised to tweak the network's algorithm for subsequent rounds.

The layers of neurons are input, hidden, and output. The input layer is made up of record values that are used as inputs to the next layer of neurons, rather than entire neurons. The hidden layer is the next layer. A neural network can have multiple hidden layers. The output layer is the final layer, with one node for each class. The record is assigned to the class node with the highest value after a single sweep forward across the network assigns a value to each output node.

Fig. 5: Copy move forgery images

V. PERFORMANCE EVOLUATION OF THE MODEL

The performance evaluation of a classification model can be done using confusion matrix.The confusion matrix can be represented as following.

Confusion matrix(C.M)=$\begin{bmatrix} W & X \\ Y & Z \end{bmatrix}$

W= True positive

X=False positive

Y=False negative

Z=True negative

A. Recall:

The number of True Positives divided by the number of True Positives and False Negatives is the recall. To put it another way, the number of positive forecasts divided by the number of positive class values in the test data equals the number of positive predictions divided by the number of positive class values in the test data. It's also known as the True Positive Rate or Sensitivity.This can be expressed as:

$$R.C = \frac{W}{W+Y}$$

B. Precision:

The number of True Positives divided by the total number of True Positives and False Positives equals precision. In other words, it's the total number of positive class values predicted divided by the total number of positive predictions. It's also known as the Positive Predictive Value (PPV).This can be expressed as:.

$$P = \frac{W+Z}{W+X+Y+Z}$$

C. False Measure:

The harmonic mean of accuracy and recall, also known as the classical F-measure or balanced F-score, is a metric that combines precision and recollection:

$$F.M = \frac{2(R.C)(P)}{R.C+P}$$

D. Sensitivity:

In the case of a medical test used to diagnose an illness, sensitivity refers to the test's capacity to correctly detect patients who do have the condition, and the sensitivity of the test is the proportion of persons who test positive for the disease among those who have the disease. Mathematically, this can be expressed as:

$$ST = \frac{W}{W+Z}$$

E. Specificity:

The test's ability to correctly discover people without a condition is referred to as specificity, often known as the true negative rate. Take, for example, a medical test for disease diagnosis. The specificity of a test refers to the percentage of healthy persons that test negative for the condition while not having it.Mathematically, this can also be written as:

$$SF = \frac{Z}{Z+X}$$

F. Accuracy:

The degree of conformance between a measurement of an observable quantity and a recognized standard or specification that indicates the true value of the quantity.

$$\mathrm{A} = \frac{W+Z}{W+X+Y+Z}$$

ISSN No:-2456-2165

VI. COMPARISION OF VARIOUS IFD TECHNIQUES

Table 1: Comparision of contribution towards image forgery detection in chronological order

S.No	Paper	Year	Target	Methodology	Perfarmance paramters
1	[9]	1999	Digital Forgeries	polyspectral analysis	
2	[12]	2003	Copy and Move Imgae forgery detection	Robust match	
3	[10]	2004	Image splicing digital photomontaging	bicoherence features, Support Vector Machine (SVM)	Accuracy=0.7148 Precision= 0.6814 Recall= 0.8098
4	[13]	2004	Image forgery for Pan Chromatic	SIFT,PCA algorithms in MATLAB	Accuracy=93.02
5	[11]	2005	Digital image forgery	Re-sampling	Accuracy=30-80
6	[33]	2006	Copy and move forgery	Blur moments	
7	[36]	2010	Region duplication	Feature Matching	
8	[30]	2011	Copy and move forgery	Multi resolution charecterstic of DWT	
9	[16]	2012	Image forgery	DWT	Accuracy=96-100
10	[17]	2012	Image forgery	pixel based	
11	[25]	2013	Copy and move forgery	Local Binary Pattrens	
12	[32]	2013	Copy and move forgery	Segmentation	
13	[15]	2014	Copy and Move Imgae forgery	Block representing	Accuracy=25-68
14	[19]	2014	Image forgery	Dyadic Wavelet Transform (DyWT) and Scale Invariant Feature Transform (SIFT	Precision=88
15	[20]	2014	Image forgery	Edge detection based salient Region detection	
16	[24]	2015	Image forgery	Scaled ORB	
17	[14]	2015	Cloning forgery images	Speed up Robust Feature (SURF),DWT	
18	[22]	2016	Copy and move forgery	SIFT with Particle Swarn Optimization Technique	
19	[27]	2016	Copy and move forgery	Fusion of block and key points	Precision=88.51 Recall=86.48 F-Measure=87.17
20	[28]	2016	Copy and move forgery	New interest point detector	
21	[31]	2016	Splicing and copy-move forgeries	Deep learning	
22	[35]	2016	Copy and move forgery	Block based	
23	[8]	2016	Image forgery	Superpixel by SIFT nd LFP	Precision=99 Sensitivity=84 Specificity=99
24	[26]	2017	Copy and move forgery	hybrid features(SIFT and Others)	Precision=90.27 Recall=78.61 F-Measure=84.04
25	[21]	2017	Image forgery	Single valued decomposition(SVD) cuckoo search algorithm	F1=94.18 Precision= 96.13 Recall= 92.3
26	[29]	2018	Copy and move forgery	Feature Matching,Deep learning	F-Measure=93
27	[23]	2019	Copy and move forgery	Deep learning	Precision=94.8 Recall=95.3 FMeasure=95.02
28	[34]	2021	Copy and move forgery	Rotation invariant features on dense field	

VII. CONCLUSION AND FEATURE WORK

Image forgery is a major threat not only to cybersecurity but also to mankind. The problem has to be addressed with a scientific approach. Many researchers are working on the same problem for years and have contributed much to solve the problem. In this particular paper, we review all the techniques used by the researchers to detect image forgery. With the advancement of Artificial Intelligence, there are a lot of frameworks available which can address problems in any domain efficiently. By taking the advantage of Artificial Intelligence in our feature work we want to address the problem of image forgery and to localize the detection with better performance indicators by overcoming the limitations of the existed methods.

REFERENCES

[1.] Singh, Sandarbh, and Rupali Bhardwaj. "Image forgery detection using QR method based on one-dimensional cellular automata." *Contemporary Computing (IC3), 2016 Ninth International Conference on*. IEEE, 2016.

[2.] Mahmood, Toqeer, et al. "A survey on block based copy move image forgery detection techniques." *Emerging Technologies (ICET), 2015 International Conference on*. IEEE, 2015.

[3.] Mangat, Sawinder Singh, and Harpreet Kaur. "Improved copy-move forgery detection in image by feature extraction with KPCA and adaptive method." *Next Generation Computing Technologies (NGCT), 2016 2nd International Conference on*. IEEE, 2016.

[4.] Tuba, Ira, Eva Tuba, and Marko Beko. "Digital image forgery detection based on shadow texture features." *Telecommunications Forum (TELFOR), 2016 24th*. IEEE, 2016.

[5.] Rao, Yuan, and Jiangqun Ni. "A deep learning approach to detection of splicing and copy-move forgeries in images." *Information Forensics and Security (WIFS), 2016 IEEE International Workshop on*. IEEE, 2016.

[6.] Moradi-Gharghani, Hajar, and Mehdi Nasri. "A new block-based copy-move forgery detection method in digital images." *Communication and Signal Processing (ICCSP), 2016 International Conference on*. IEEE, 2016.

[7.] Fadl, Sondos M., and Noura A. Semary. "A proposed accelerated image copy-move forgery detection." *Visual Communications and Image Processing Conference, 2014 IEEE*. IEEE, 2014.

[8.] Rad, Reza Moradi, and KokSheik Wong. "Digital image forgery detection by edge analysis." *Consumer Electronics-Taiwan (ICCE-TW), 2015 IEEE International Conference on*. IEEE, 2015.

[9.] Hany Farid "Detecting Digital Forgeries Using Bispectral Analysis" Perceptual Science Group, MIT, Cambridge, MA 02139

[10.] Tian-Tsong Ng, Shih-Fu Chang, Qibin Sun "BLIND DETECTION OF PHOTOMONTAGE USING HIGHER ORDER STATISTICS"

[11.] Alin C. Popescu and Hany Farid "Exposing Digital Forgeries by Detecting Traces of Re-sampling"

[12.] Jessica Fridrich, b David Soukal, and a Jan Lukáš "Detection of Copy-Move Forgery in Digital Images"

[13.] Shivani Thakur, Ramanpreet Kaur "Image Forgery Detection using SIFT and PCA Classifiers for Panchromatic Images" IJSTE - International Journal of Science Technology & Engineering | Volume 3 | Issue 01 | July 2016

[14.] Manpreet Singh, Er. Harpal Singh "Detection of Cloning Forgery Images using SURF + DWT and PCA" International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137 Volume – 01, Issue – 09, December – 2016, PP – 01-10

[15.] Rohini.A.Maind, Alka Khade, D.K.Chitre "Image Copy Move Forgery Detection using Block Representing Method "International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-4 Issue-2, May 2014

[16.] Preeti Yadav ,Yogesh Rathore ,Aarti Yadu "DWT Based Copy-Move Image Forgery Detection " International Journal of Advanced Research in Computer Science and Electronics Engineering Volume 1, Issue 5, July 2012

[17.] Pradyumna Deshpande , Prashasti Kanikar "Pixel Based Digital Image Forgery Detection Techniques" Pradyumna Deshpande , Prashasti Kanikar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp. 539-543

[18.] SHAHABUDDIN.S.K, DR. A.R.ASWATHA "An Efficient Image Forensic Mechanism using Super pixel by SIFT and LFP Algorithm" International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 07 | July -2017

[19.] Mohammad Farukh Hashmia , Vijay Anandb , Avinas G. Keskarc "Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform" 2014 AASRI Conference on Circuit and Signal Processing (CSP 2014)

[20.] K. Anitha, P. Leveenbose "Edge Detection based Salient Region Detection for Accurate Image Forgery Detection" 978-1-4799-3975-6/14/$31.00 ©2014 IEEE

[21.] Abhishek Kashyap , Megha Agarwal , Hariom Gupta "Detection of copy-move image forgery using SVD and cuckoo search algorithm" International Journal of Engineering & Technology.

[22.] SH Wenchang, ZHAO Fei, QIN Bo, LIANG Bin "Improving image Copy-Move Forgery Detection with Particle Swarm Optimization Techniques" Security schemes and solutions, China communications January 2016.

[23.] B. Rakesh Babu1 , Dr. S. Narayana Reddy "Copy – Move Forgery Detection in Digital Images Based on deep Learning" International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET) , Volume 10, Issue 2, February 2021

[24.] Ye Zhu & Xuanjing Shen & Haipeng Chen "Copy-move forgery detection based on scaled ORB" Multimed Tools Appl DOI 10.1007/s11042-014-2431-2
[25.] Leida Li , Shushang Li , Hancheng Zhu "An Efficient Scheme for Detecting Copy-move Forged Images by Local Binary Patterns" Journal of Information Hiding and Multimedia Signal Processing Volume 4, Number 1, January 2013
[26.] Fan Yanga , Jingwei Lia , Wei Lua,∗ , Jian Wengb "Copy-move forgery detection based on hybrid features"E ngineering Applications of Artificial Intelligence 59(2017)N73-83
[27.] Jiangbin Zheng · Yanan Liu · Jinchang Ren· Tingge Zhu· Yijun Yan· Heng Yang "Fusion of block and keypoints based approaches for effective copy-move image forgery detection" Multidim Syst Sign Process DOI 10.1007/s11045-016-0416-1
[28.] Mohsen Zandi, Ahmad Mahmoudi-Aznaveh, and Alireza Talebpour "Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector" 1556-6013 (c) 2016 IEEE.
[29.] Gul Muzaffer, Guzin Ulutas "A new deep learning-based method to detection of copy-move forgery in digital images" 978-1-7281-1013-4/19/$31.00 ©2019 IEEE
[30.] S Khan, A Kulkarni "Detection of Copy-Move Forgery Using Multiresolution Characteristic of Discrete Wavelet Transform" International Conference and Workshop on Emerging Trends in Technology (ICWET 2011) – TCET, Mumbai, India
[31.] Yuan Rao, Jiangqun Ni "A Deep Learning Approach to Detection of Splicing and Copy-Move Forgeries in Images" 2016 IEEE International Workshop on Information Forensics and Security (WIFS)
[32.] Jian Li, Xiaolong Li, Bin Yang, and Xingming "Segmentation-based Image Copy-move Forgery Detection Scheme" 1556-6013 (c) 2013 IEEE.
[33.] Babak Mahdian , Stanislav Saic "Detection of copy–move forgery using a method based on blur moment invariants" doi:10.1016/j.forsciint.2006.11.002
[34.] Davide Cozzolino, Giovanni Poggi and Luisa Verdoliva "Efficient dense-field copy-move forgery detection" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY
[35.] Hajar Moradi-Gharghani and Mehdi Nasri "A New Block-based Copy-Move Forgery Detection Method in Digital Images" International Conference on Communication and Signal Processing, April 6-8, 2016, India
[36.] Xunyu Pan, Siwei Lyu "Region Duplication Detection Using Image Feature Matching" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 4, DECEMBER 2010.

AUTHOR'S 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).