A Machine Learning Based Classifier for Automated Detection of Image Forgery

Urvashee Bhawsar[1] Prof.Ashish Tiwari[2]

***Abstract*—**With social media making its presence felt wide and far, its consequences are also far reaching at least in the context of imagery. The amount of information that can be shared by images is enormous as compared to test data. However, there remains a chance of fake and forged image data that can be circulated which can result in disastrous consequences for individuals, firms or communities at large. With the advancements in image editing tools, it is practically impossible to detect fake or forged images by the naked human eye. Moreover, the number of images shared specifically on social media platforms is so large that human intervention is practically infeasible. In this paper, image forgery detection has been carried out using artificial neural networks and image processing techniques. The configuration of the neural networks is the ada-boost network. The performance index is the classification accuracy. It has been shown that the proposed technique achieves higher classification accuracy compared to previously existing methods for the same dataset.

Keywords—Image Processing, Image Forgery, Artificial Neural Network (ANN), Ada-Boost Network, Classification Accuracy.

I. INTRODUCTION

With the ever increasing growth and popularity of social media platforms resorting to visual imagery, the chances of forged images doing the rounds have also increased [1]. Moreover, as the tools used for image forgery have become more advanced, the perceptibility of forgery being done has also become very less. With the enormous amount of data being shared on social media platforms, it is nearly impossible to make humans recognize forgery in images in real time critical applications[2]-[3]. Hence, it becomes mandatory to design automated systems which can detect image forgery with high accuracy, which is the most stringent need to be met [4].

Digital images can be morphed or manipulated in several forms such as splicing, retouching etc. Every forgery technique needs a different approach to be detected. In general, for artificial intelligence to work, it is necessary to train the system with large enough data sets so as to learn from the features of forged and unforged images. Hence, the training data set is critical and so is the choice of features to distinguish a forged image from an unforged one [5]. In this paper, an image forgery mechanism is put forth with a cascaded back to back connection of neural networks called the ada-boost neural architecture. The substantiated discussions follow in the subsequent sections.

II. CHALLENGES PERTAIING TO IMAGE FORGERY DETECTION

There are fundamental challenges pertaining to image forgery detection among which the most prominent ones are [6]-[7]:

1. Similarity in Pixel Value Distribution: The pixel values of forged and unforged images often bear stack similarity thereby making conventional techniques fail.
2. Effect of Noise and Disturbances: Images are extremely prone to blurring, noise and disturbance effects while capturing, storage and sharing, Hence, it becomes almost impossible to detect whether the noise is injected intentionally or is naturally present. Mathematically, the blurring and degradation effects also make the recognition difficult. Let the original image be designated by I, then,

$$I' = I + N(f) \quad (1)$$

Here,
I represents the original image
I' is the degraded image
N is the noise affecting the image
f is the frequency metric

3. The accuracy of classification is extremely challenging to be high since the previous two factors make the classification problem challenging [8].

III. ADA-BOOST NETWORK DESIGN

Due to the size and complexity of the data, neural network design to address the problem becomes almost invariable. In such a case, a neural network model is needed which can address the classification problem with high accuracy. The mathematical model of the neural network is shown in figure 1.

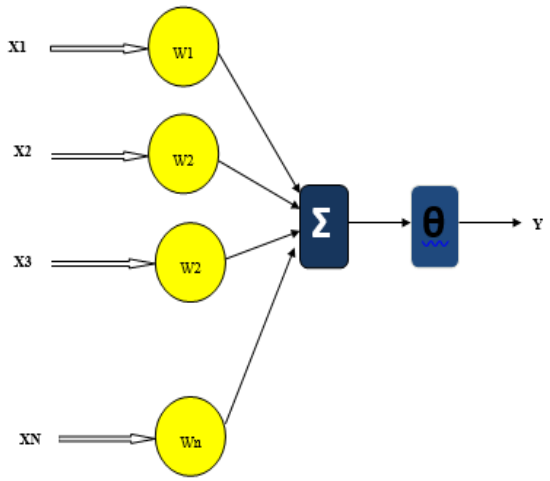


Fig.1 Mathematical Model of ANN

Here,
X represents the parallel input data stream to the ANN
Y represents the output of the ANN
W represents the dynamic weights of the system
θ represents the logic for analysis or bias of the network [9].

Next, for the purpose of image forgery detection, two critical aspects need to be understood.

(i) Neural networks need to be fed with numerical features which have to be extracted from the raw data set.
(ii) The network should be able to train or learn from the highly uncorrelated data
(iii) The neural classifier needs to have a holistic approach in regards to classification.

For this purpose, the cascade ada-boost neural architecture is chosen. It is depicted in the figure below:

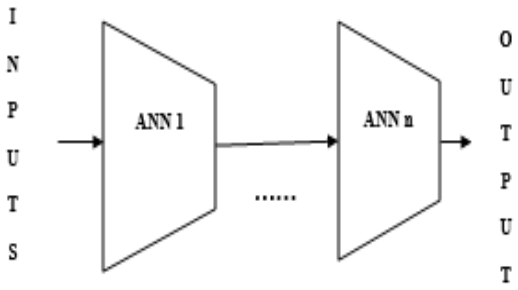


Fig.2 Ada-Boost Architecture

It can be seen from the above figure that the neural networks are connected in cascade and the output of one neural network is fed as the input to the other neural network. Such a strategy is employed for complex classification problems, where the data format is different from the extracted feature values.

IV. DATA PRE-PROCESSING

As discussed earlier, the images are prone to noise and disturbance effects while capturing, storage and transfer. Hence, it is necessary to remove the effects of noise and disturbance [10]. The sub-techniques used are explained below:

a) RGB to Gray Scale Conversion: In this method, the colour or R,G,B image is converted to a grayscale image in which the pixel values are functions of intensity alone i.e.

$$I(R,G,B) \xrightarrow{Transform} I(intensity) \quad (2)$$

Thus, the transform removes the R,G,B values separately existing to a combined intensity values in binary or 2 state values.

b) Binarization: In this case, the image is converted to a binary form of image in which all the pixel values.

c) The Wavelet Transform: The wavelet transform is an effective tool for image noise removal. Images generally are not smooth in nature if the pixel variations are considered [11]. Hence conventional Fourier methods do not render good results for image based data sets. This can be understood as:

$$X(f) = \int_{-\infty}^{+\infty} x(t)e^{-j\omega t}dt \quad (3)$$

Here,
X(f) is the signal in the frequency domain
x(t) is the signal in time domain
It can be seen that the kernel of the transform comprises of smooth signals since:

$$e^{-j\omega t} = cos\omega t - jsin\omega t \quad (4)$$

Both sin and cos being smooth in nature are incapable of handling non-smooth variations in the pixels of the images. Hence the Wavelet Transform is to be used.

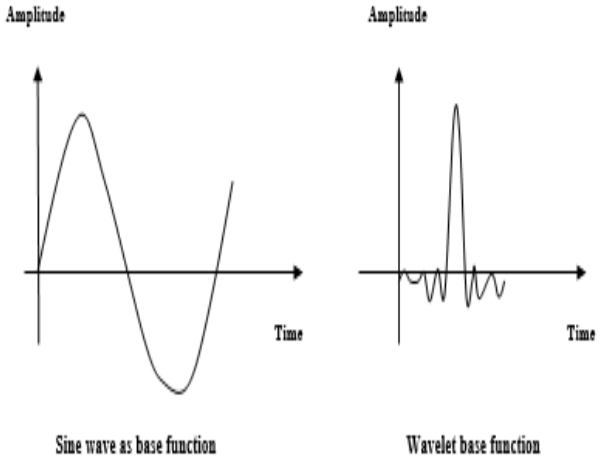


Fig.3 Fourier and Wavelet Base Functions

The difference between the base functions makes it possible for wavelet analysis to cater to the image de-noising approach.

Mathematically, the wavelet transform can be given as:

$$Z(S, P) = \int_{-\infty}^{\infty} z(t)\,((S, P, t))dt \quad (5)$$

Here,
S denotes the scaling operation
P denotes the shifting operation
t denotes the time variable
Z is the image in transform domain
z is the image in the spatial domain

The major advantage of the wavelet transform is the fact that it is capable of handling fluctuating natured signals and data and removes noise effects and also local disturbances. The scaling operator is defined for the Wavelet Kernel as:

$$W\Phi\,(Jo, k) = \frac{1}{\sqrt{M}} \sum_n S(n).\Phi(n)_{jo'k} \quad (6)$$

Subsequent to the pre-processing, the feature extraction is done which is explained below.

V. FEATURE EXTRACTION

The neural network understands or is intelligible for numerical data only [12]. Hence it becomes mandatory to feed the neural network with numerical data corresponding to the forged and unforged images. The numerical features computed are:

1. Contrast
2. Correlation
3. Energy
4. Homogeneity
5. Mean
6. Standard Deviation
7. Entropy
8. RMS value
9. Variance
10. Smoothness
11. Kurtosis
12. Skewness

The salient features are different for the forged and unforged data. Hence it allows the neural networks to classify. The features extracted are then fed to the neural architecture shown in the subsequent figure.

VI. TRAINING AN ADA-BOOST NETWORK

The neural architecture used is the ada-boost whose mechanism can be understood using the figure given below.

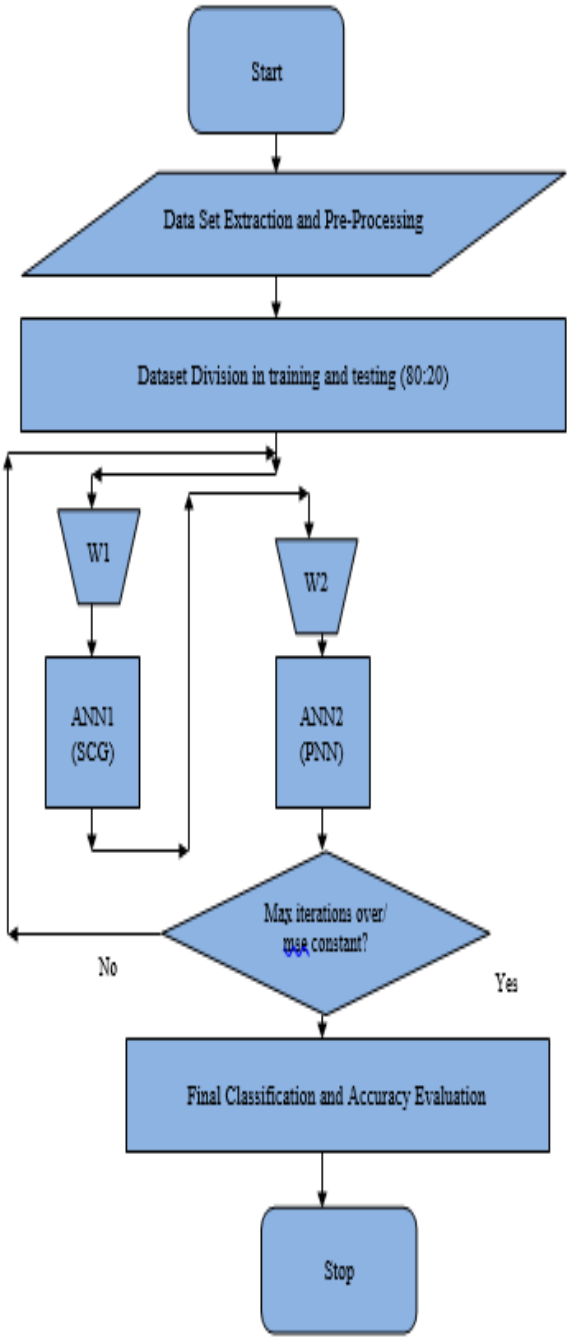


Fig.4 System Flowchart

It can be clearly seen that the proposed approach uses two ANN architectures for the final classification. The first one is the scaled conjugate gradient (SCG) and the other is the Probabilistic Neural Network (PNN). The essence of the SCG is the fact that it uses least space complexity for implementation and is also fast. The PNN is a very effective probabilistic classifier. They are discussed subsequently. The weights are updated as follows

$$x_{k+1} = x_k + \alpha_k g_k \quad (7)$$

Where, $\alpha_k$is the determined step size and

$$P_k = -g_k + \beta_k P_{k-1} \quad (8)$$

Here p is search direction vector and g is gradient direction vector. For SCG, β_k factor calculation and direction of the new search can be shown as in following equations.

$$\beta_K = \frac{(|g_{k+1}|^2 - g_{k+1}{}^T g_k)}{g_k{}^T g_k} \quad (9)$$

$$P_{k+1} = -g_{k+1} + \beta_k P_k \quad (10)$$

The probabilistic neural network works on the principle of the Baye's Theorem pertaining to conditional probability of associated random events. The theorem is defined as:

$$P\left(\frac{A}{B}\right) = \frac{P\left(\frac{B}{A}\right)P(A)}{P(B)} \quad (11)$$

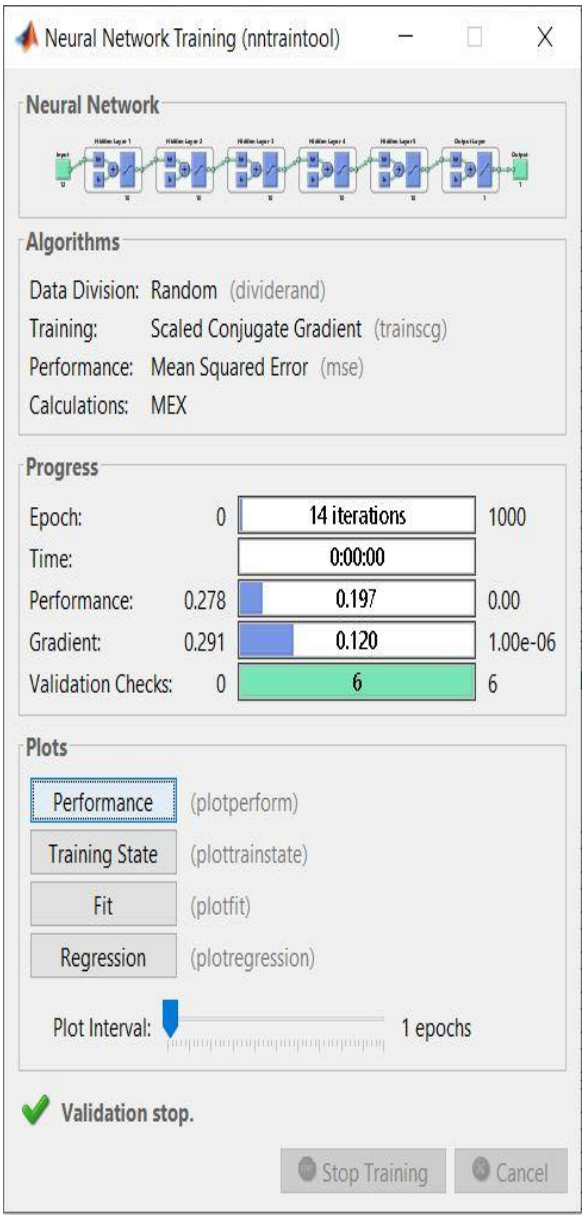
Here:
P(A) is the individual probability of event A
P(B) is the individual probability of event B
P(A/B) is the probability of A given B is true
P(B/A) is the probability of B given A is true
The probabilistic neural network is specifically used for applications where there is a sense of uncertainty in computing the output. The PNN computes the cost function of the event A with respect to event B.

$$P_A C_A f_A > P_B C_B f_B \quad (12)$$

Here,
P_A represents probability of A
P_B represents probability of B
C_A represents the cost function for event A
C_B represents the cost function for event B
F_A represents the probability function for event A
F_B represents the probability function for event B
The PNN is used for the final classification.

VII. RESULTS

The results obtained are depicted sequentially in this section,



Fig, 5 ANN1:SCG Training

The first neural network is the 1-5-1 Scaled conjugate gradient (SCG) Network. It takes around 14 iterations to train and subsequently send its output to the next neural network which happens to be the probabilistic neural network (PNN) for the final classification.

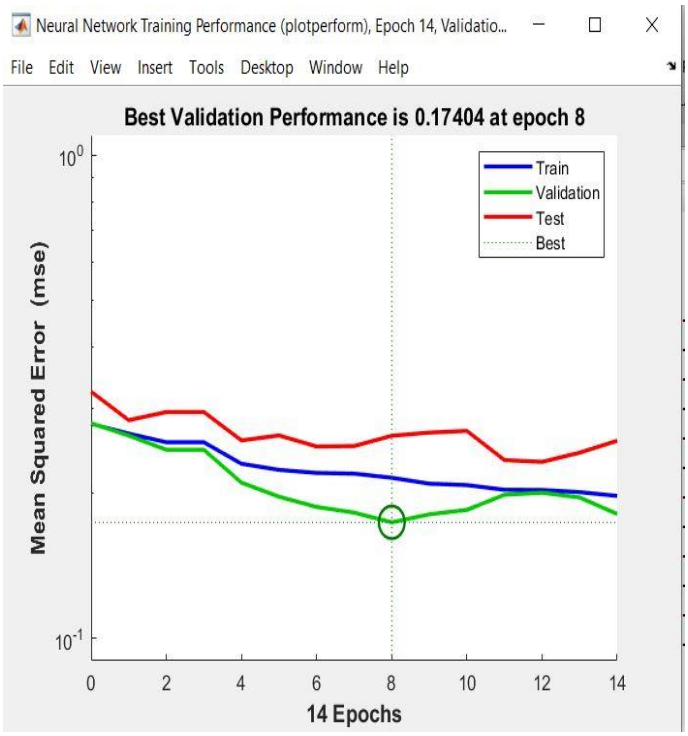


Fig.6 Variation of MSE w.r.t. epochs

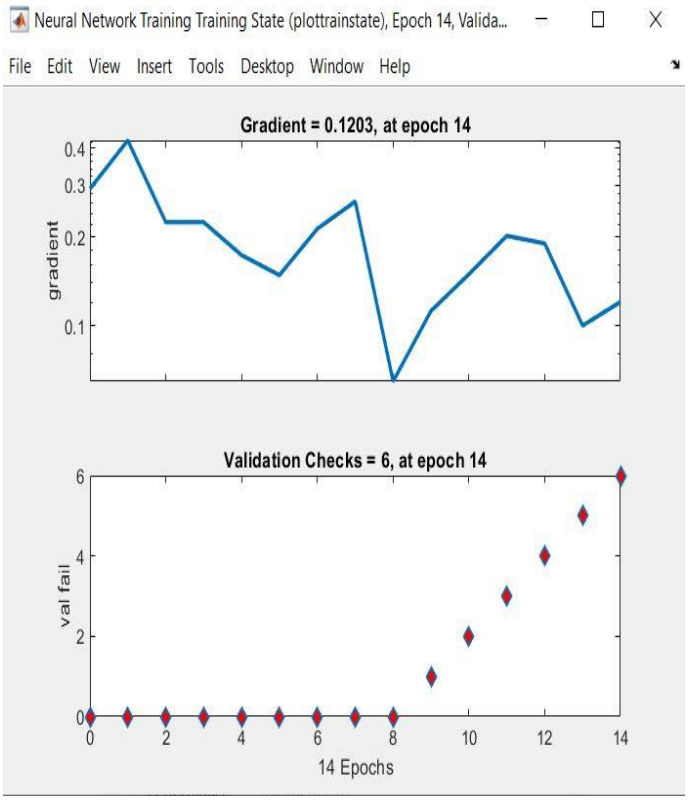


Fig.7 Training States w.r.t. epochs

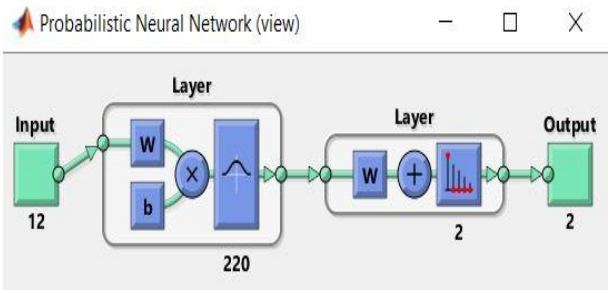


Fig.8 ANN2: PNN

The final classification is carried out by the 12-220-2 PNN. 12 in the input layer signifies 12 neurons, 22o signifies the number of neurons in the hidden or pattern layer and 2 at the output signifies the number of neurons in the output layer.

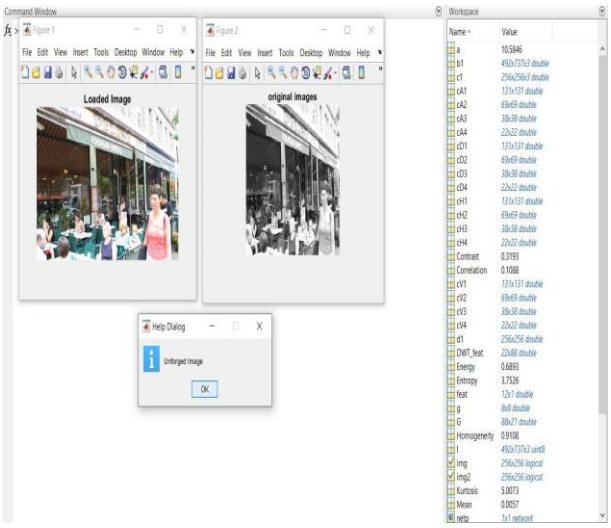


Fig.9 GUI for Non-Forgery Detection

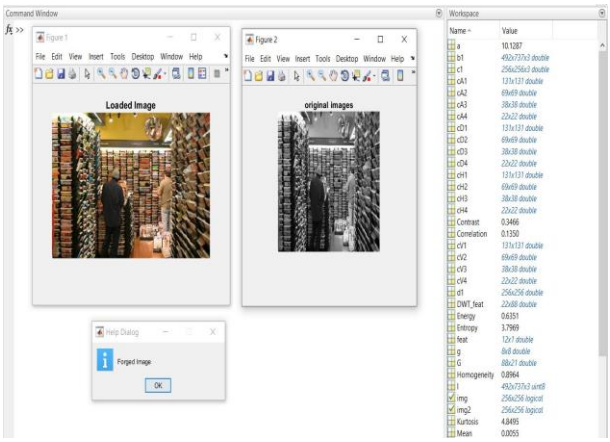


Fig.10 GUI for Forgery Detection

The accuracy of the system for the tested data set is found to be:

$$Ac = \frac{True\ Classifications}{Total\ Cases}$$

$$Ac = \frac{210}{220} = 95.45\%$$

Thus the accuracy of the proposed system is found to be 95.45%.

CONCLUSION: It can be concluded from the previous discussions that the process of image forgery detection is complex in nature owing to the complexity and size of the data for real time critical applications, Hence the need for artificial intelligence based techniques is invariable. The proposed approach presents an ada-boost ANN architecture which uses both the scaled conjugate gradient (SCG) and the Probabilistic Neural Network (PNN) for the image forgery detection approach. The performance of the proposed system is better compared to previous work [1].

References

[1] H. Wu, J. Zhou, J. Tian, J. Liu and Y. Qiao, "Robust Image Forgery Detection Against Transmission Over Online Social Networks," in IEEE Transactions on Information Forensics and Security, 2022, vol. 17, pp. 443-456.

[2] Abhishek, N Jindal, “Copy move and splicing forgery detection using deep convolution neural network, and semantic segmentation”, Multimedia Tools and Applications, Springer 2021, vol.80., pp. pages3571–3599.

[3] Z. J. Barad and 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.

[4] R. Agarwal, D. Khudaniya, A. Gupta and K. Grover, "Image Forgery Detection and Deep Learning Techniques: A Review," 2020 4th International Conference on Intelligent Computing and Control

Systems (ICICCS), Madurai, India, 2020, pp. 1096-1100.

[5] R. Thakur and R. Rohilla, "Copy-Move Forgery Detection using Residuals and Convolutional Neural Network Framework: A Novel Approach," 2019 2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC), 2019, pp. 561-564

[6] Araz Rajab Abrahim, Mohd Shafry Mohd Rahim, Ghazali Bin Sulong "Splicing image forgery identification based on artificial neural network approach and texture features", Springer 2018

[7] T Pomari, G Ruppert, E Rezende "Image Splicing Detection Through Illumination Inconsistencies and Deep Learning", IEEE 2018

[8] J Bunk, JH Bappy, TM Mohammed, "Detection and Localization of Image Forgeries Using Resampling Features and Deep Learning", IEEE 2017

[9] C Seibold, W Samek, A Hilsmann, P Eisert., "Detection of Face Morphing Attacks by Deep Learning", Springer 2017

[10] Yuan Rao ; Jiangqun Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images", IEEE 2016

[11] Belhassen Bayar, Matthew C. Stamm, "A Deep Learning Approach to Universal Image Manipulation Detection Using a New Convolutional Layer", IEEE 2016.

[12] Jiansheng Chen ; Xiangui Kang ; Ye Liu ; Z. Jane Wang, "Median Filtering Forensics Based on Convolutional Neural Networks", IEEE 2015.

[13] Chi-Man Pun , Xiao-Chen Yuan , Xiu-Li Bi, "Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching",IEEE 2015.

[14] Davide Cozzolino ; Diego Gragnaniello ; Luisa Verdoliva, "Segmentation-Based Image Copy-Move Forgery Detection Scheme", IEEE 2014

[15]Davide Cozzolino ; Diego Gragnaniello ; Luisa Verdoliva, "Image forgery detection through residual-based local descriptors and block-matching", IEEE 2014

[16] GK Birajdar, VH Mankar, "Digital image forgery detection using passive techniques: A survey", Digital investigation , Elsevier 2013, vol.10., no.3. pp. 226-245.

[17] G Lynch, FY Shih, HYM Liao, "An efficient expanding block algorithm for image copy-move forgery detection", Information Sciences, Elsevier 2013, vol.293, pp. 253-265.