ENHANCED PAD NEURAL BASED APPROACH FOR FORGERY DETECTION IN IMAGES

[1]Surinder Pal Kaur,[2]Anil Kumar

[1]Student,[2]Professor

Department of Computer Engineering and Technology

Guru Nanak Dev University,Amritsar,Punjab

ABSTRACT-Fraud detection is critical from the facial images. This paper presents a noval approach using presentation attack detection(PAD) mechanism for the detection of frauds from the image dataset. To detect the frauds Yale dataset is used. Pre-processing of the images is done using the linear learning color enhancement mechanism. For the purpose of classification neural network is used. The classification result will either be normal or abnormal images. The cumulative density function is applied to obtain the frauds using the fractions fetched from classification phase. Result in terms of false matching rate and false non matching rate is presented that is 0.489 and 0.455.   Hybridized PAD with neural network produces better result as compared to plan PAD approach and factor for improvement is 2%.

Keywords- PAD, Neural network, linear learning color enhancement, FMR, FNMR

I INTRODUCTION

Image processing advancement leads to the detection of forgery even within the images.(Zhou et al. 2009) Images can be used in order to encrypt the data and then transfer that information from source towards destination. Once the information is transferred, authentication of information depends on network media through which transmission occurred.(Gupta et al. 2015)proposed a DCT based approach for attack detection in watermarking images. The attack detection is generally slow and has high false matching and false non matching rate. To resolve the issue this paper present noval approach of presentation attack detection using neural network and neural network. The demonstration is done on Yale dataset. The proposed work is divided into two phases

- Training
- Testing

Training is done using the unsupervised learning mechanism. The original images are fed into the layers of neural network. Necessary features are extracted from the image and stored within .mat file. The hold out rate for the training images is 0.4.

Once training is complete testing process begin. The testing images are selected from the same source where testing images are present. The features are extracted using the neural network and then features are matched with the .mat file already prepared at training phase. The overall procedure first of all introduces noise within the Yale dataset images and then applies the proposed mechanism for the attack detection. The procedure for the detection of presentation attack is listed as

- Introduces noise within the images from the Yale dataset
- Applying the pre-processing mechanism using linear learning color enhancement.
- Extracting features using neural network
- Classification using cumulative density function
- Result in terms of FMR and FNMR

The detailed methodology is described in the section III. The existing literatures is discussed in section II, methodology is given in section III, performance analysis and results is given in section IV and conclusion is specified in section V.

II LITERATURE SURVEY

This section discusses techniques used in literatures for defining attacks from the images. The forgery detection mechanisms in general are discussed in this section.

(Mankar and Gurjar 2015) discussed image forgery detection mechanism and divide the overall techniques into two parts: first is active forgery detection mechanism and other is passive forgery detection mechanism. Copy move forgery is commonly employed to create attacks and application of support vector machine is discussed for the detection of forgery from the image.

(Birajdar and Mankar 2013) discussed forgery detection from the watermarked images. Passive detection mechanism is surveyed along with blind techniques for forgery detection from the watermarked images. The result is deviated when images are forged and peak signal to noise ratio is affected. Passive attack detection mechanism detects attack efficiently and PSNR increases.

(Yadav and Dongre 2017)proposed a copy move forgery detection mechanism. Block level and key point based mechanisms are discussed for forgery detection. The image forgery that is efficiently detected is copy move and result in terms of PSNR is presented.

 (Fei et al. 2017)proposed a image forgery detection using segmentation and swarm optimization mechanism. Segmentation divides the image into critical and non critical section. The features are extracted from the critical section and swarm optimization is applied to perform classification. Result is presented in terms of classification accuracy and peak signol to noise ratio.

(Pande 2014) proposed image tempering avoidance mechanisms. The image forgery detection and avoidance using pixel density based approach is discussed. Pixel based approach for feature extraction and classification is done. The object detection mechanism presents the result in terms of classification accuracy.

(Kaushik et al. 2015) proposed a image forgery detection mechanism two dimensional discrete cosine transformations and statistical moments are used for the detection of forgery from the images. This technique is effective enough to detect presentation attacks from the images. The result in terms of peak signal to noise ratio and classification accuracy is presented through this literature.

(Kaur and Kaur 2016) proposed image edge detection using artificial bee colony algorithm. This algorithm performs better as compared to genetic algorithm. The convergence of this approach is faster as compared to genetic approach. The overall overhead in terms of cost is minimized using the artificial bee colony algorithm.

The review of literature suggests that least amount of work has been done towards the detection of presentation attack. The attack detection using neural network and density function is also limited. Next section described the methodology followed in proposed work.

III Proposed Methodology

The methodology for the proposed literature is divided into phases. The first phase is of training mechanism. The training mechanism methodology is discussed as under

---

Training(Image$_i$)

- Receive image from the Yale dataset
  I=imread(Image$_i$)
- Define Layers of Neural Network
  Input Layer for filtering the image into distinct pixel set(X1,X2,----Xn)
  Processing layer defining weights(w1,w2,-----,wn)
  Output layer obtaining distinct features defined as Y
  Y$_i$=W1X1+W2X2+--------+WnXn
- Store Y in .mat file
- Repeat the above steps for i<N(where N is the total number of images)

Once training is complete, testing procedure can be performed. The images from the Yale dataset will be used for testing as well as training. The testing phase takes the image set and performs pre-processing mechanism. Once the pre-processing mechanism is finished then feature extraction using neural network initiates. As a last phase, density function is applied for classification. The algorithm used for testing is given as under

Testing (Images$_i$)

- Receive images from Yale dataset
  I=imread(Image$_i$)

- Introduce Noise within the image
  I=imnoise(I,'Gaussian')
- Define Layers of Neural Network
  Input Layer for filtering the image into distinct pixel set(X1,X2,----Xn)
  Processing layer defining weights(w1,w2,-----,wn)
  Output layer obtaining distinct features defined as Y
  Y_i=W1X1+W2X2+--------+WnXn(Density based Extraction)
- Extract the features stored within the .mat file during training
- Compare Y_i with Features from .mat file
- Predict result as normal and abnormal image

The proposed methodology produces effective result in terms of false matching rate and false non matching rate. The density based mechanism proves noval approach for the classification process. The result is demonstrated in the next section.

IV PERFORMANCE ANALYSIS AND RESULTS

The dataset used for the performance analysis is Yale dataset. The description of dataset is given in table 1.

Table 1: Yale dataset description

Images	Type	Size	Origin
	JPEG	300X300	Yale
	JPEG	300X300	Yale
	JPEG	300X300	Yale
	JPEG	300X300	Yale
	JPEG	300X300	Yale

The dataset used is of jpg format which is rgb in nature. The formatting and noise introduction does not impact the accuracy of the proposed system. The proposed system performance is compared with principal component analysis, discrete wavelet transformation and other primary feature extraction mechanisms. Results obtained are better as compared to existing system.

The result in terms of false matching rate and fasle negative rate is better as shown in figure 1
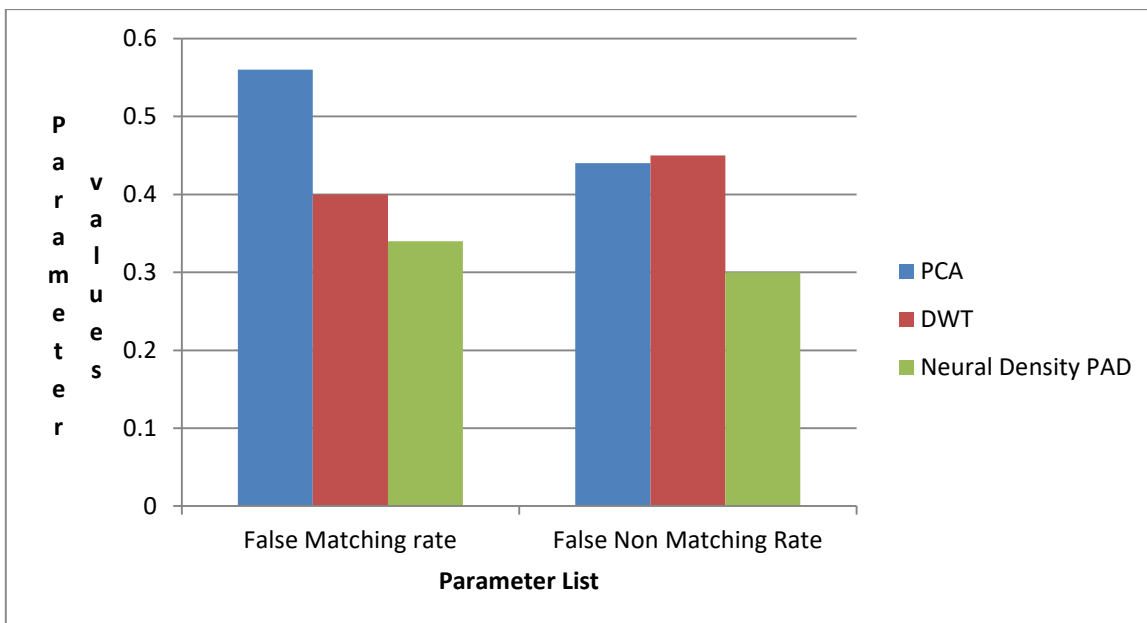

Figure 1: false matching rate and false non matching rate comparison with existing approaches such as PCA and DWT

The false matching and non matching rate of the proposed system is significantly lowered as compared to the existing system. The result is improved by 2%. The classification accuracy with which result is predicted through the proposed system is given in figure 2.
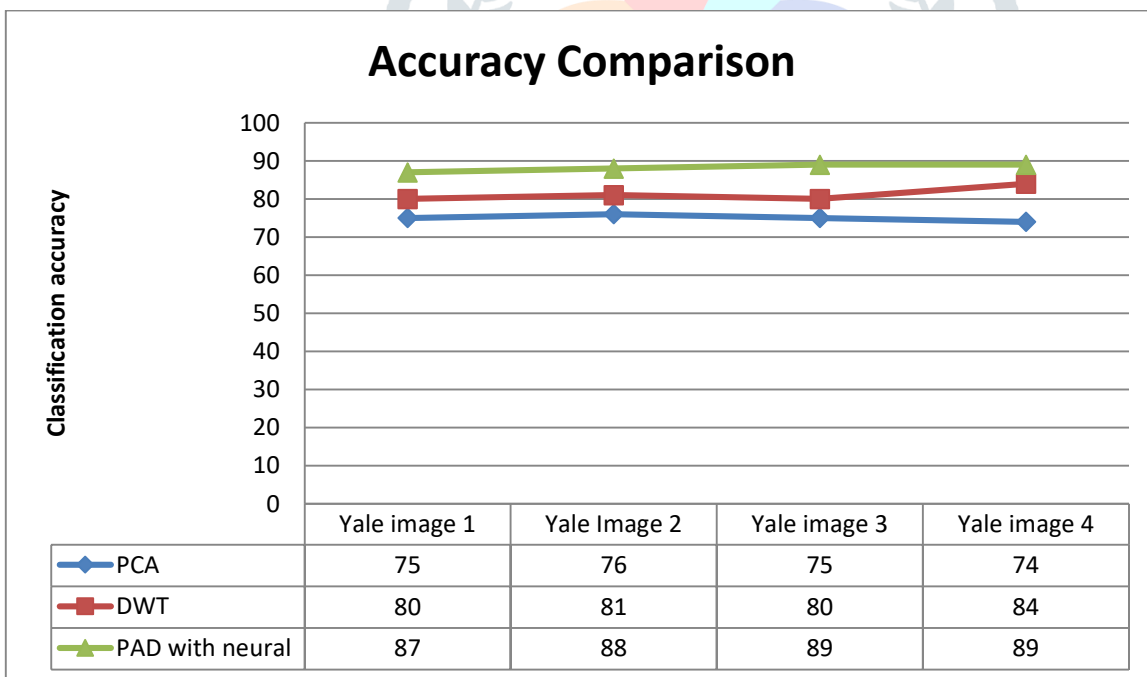

Figure 2: Classification accuracy comparison with proposed and existing PCA and DWT

The result is significantly better hence presentation attack is better detected by the use of neural based approach. The hold out rate can be varied further to improve the result. The hold out rate of 0.4 is maintained to obtained stable result.

V Conclusion and Future scope

The forgery detection from the image is critical since now a days images are used to transfer the information from source to destination. The network environment can cause the information to fluctuate from original and hence malicious information can

be incurred within the original image. To solve the problem this paper introduces a noval approach of PAD with neural network for better classification accuracy. Yale dataset is used and validity of the work is checked by introducing noise within the image set. The pre-processing mechanism is efficient enough to tackle noise as well as attack from the yale dataset. False matching and non matching rate is significantly lowered as compared to PCA and DWT approach.

In future PAD can be accommodated with region of interest to improve execution time while detecting forgery from the image dataset.

VI REFERENCES

[1]   Birajdar GK, Mankar VH (2013) Digital image forgery detection using passive techniques: A survey. Digit Investig 10:226–245 . doi: 10.1016/j.diin.2013.04.007

[2]   Fei Z, Wenchang SHI, Bo QIN, Bin L (2017) Image Forgery Detection Using Segmentation and Swarm Intelligent Algorithm. IEEE Access 22:141–148 . doi: 10.1007/s11859-017-1227-4

[3]   Gupta G, Joshi AM, Sharma K (2015) AN EFFICIENT ROBUST IMAGE WATERMARKING BASED ON AC PREDICTION TECHNIQUE USING DCT TECHNIQUE Watermarked image. 9102:1055–1059 . doi: 10.21917/ijivp.2015.0154

[4]   Kaur S, Kaur P (2016) An Edge Detection Technique with Image Segmentation using Artificial Bee Colony Optimization. IJORAT 1:20–24

[5]   Kaushik R, Kumar R, Mathew J (2015) On Image Forgery Detection Using Two Dimensional Discrete Cosine Transform and Statistical Moments. IEEE Access 70:130–136 . doi: 10.1016/j.procs.2015.10.058

[6]   Mankar SK, Gurjar PA a (2015) Image Forgery Types and Their Detection : A Review. IJARCSSE 5:174–178

[7]   Pande DN (2014) Detection of Image Tampering over Diverse information Security Schemata : A State-of-the-Art. IJCA 89:35–47

[8]   Yadav JA, Dongre N (2017) Analysis of Copy-Move Forgery Detection in Digital Image. IJEDR 732–736

[9]   Zhou Y, Panetta K, Agaian S (2009) Image encryption using binary key-images. 2009 IEEE Int Conf Syst Man Cybern 4569–4574 . doi: 10.1109/ICSMC.2009.5346780