International Journal of Future Generation Communication and Networking
Vol. 13, No. 2s, (2020), pp. 543–546

Image ForgeryDetection using Passive Image Splicing Method

ShraddhaChore[1] Preeti R. Komati[2] Mansi Sonkusare[3] Pratiksha Hulsure[4]

[1, 3, 4] *UG student, Dept. of E & TC Engg ,SKNCOE, SPPU, Pune.*
[2] *Assistant Professor, Dept. of E & TC Engg , SKNCOE, SPPU, Pune.*

[1] *shraddhachr486@gmail.com*
[2] *pvjannu12@gmail.com*
[3] *mansisonkusare11@gmail.com*
[4] *pratikshahulsure44@gmail.com*

Abstract

We are certainly living in an era where we are susceptible to a fantastic array of visual imagery. Image forgery recognition is developing together of the main research topic among researchers within the area of image forensics. This image forgery detection is addressed by dividing an image into blocks. In this system, efficient forgery detection and classification technique is proposed by three different stages. At first stage, we have carried out preprocessing by using bilateral filtering o remove noise. At second stage, extract unique features from forged image by using efficient feature extraction technique namely DWT. Finally, forged image is detected by classifying the type of image forgery using Artificial Neural Network (ANN). Also, the performance of the proposed method is analyzed using the subsequent metrics: accuracy, sensitivity and specificity.

Keywords- *DWT, ANN, Forgery Detection*

.

I. INTRODUCTION

Presently days, pictures have gotten extremely helpful in correspondence media. There is a conviction that the picture talks more truth about the occurrence or the circumstance caught than the words. Before, proficient information was required to control the pictures created by conventional film cameras with refined dull room gear, which is hard to do as such for normal clients. The pictures are anything but difficult to gain these days with the cheap gadgets. The way toward recording, putting away and sharing of enormous number of pictures is conceivable by everybody. With the time of advanced pictures the vast majority of the picture handling systems have been proposed. In this unique circumstance, the picture altering programming apparatuses expanded step by step prompting the fabrication of advanced pictures. Pictures altered utilizing the product instruments are exposed to a few preparing stages and are photorealistic to such an extent that, the imitation in a picture can never be identified by the human vision. As a result, the controlled pictures are showing up at an expanding rate prompting the abatement of trust in the visual substance. Subsequently, the legitimacy of the picture isn't taken as conceded. With the improvement of fabrication devices, innovation has been advanced to check the inventiveness of the picture data.

So the exploration network has discovered an elective method for verifying the pictures and named it as advanced picture criminology. Forgery detection strategy is one of the confirmation techniques, which accept that the first picture has some intrinsic examples, which are presented by the different imaging gadgets or handling. These examples are constantly steady in the first picture and adjusted after some forgery activities. The picture forgery detection has gotten perplexing, due to the progressed and advanced preparing devices.

II. LITERATURE SURVEY

A short overview of picture altering and forgery detection is displayed and the techniques have been arranged in this idea. An endeavor is made to acquire different potential calculations that imply improvement in picture validation procedures. From the information on the picture validation methods we construe that Passive or visually impaired strategies which need no earlier data of the picture viable

ISSN: 2233-7857 IJFGCN

have a critical favorable position of no necessity of extraordinary types of gear to implant the code into the picture at the hour of age, over dynamic procedures [1].

Presented a summary study of various splicing image forgery detection techniques. The spliced images are produced from different images there by the discrepancies of the image features or camera characteristics are the main source in detecting the forged regions of the images. Among the pixel-based and statistical based techniques we classify further into illumination color estimation, statistical characteristics of the image, noise inconsistency and finally presented other feature based methods. There may be several techniques found in the literature but, each one has its limitations. Image forensics is a burgeoning research field and despite the limitations, it promises a significant improvement in forgery detection with competition among forgery creators and detectors [2].

Due to the advancement in the digital software's manipulation of digital images has become easy. As incredible powerful computers photograph altering programming bundles and high goals catching gadgets are designed. Out of all the cases of digital image forgery, they can be categorized into two major groups as active and passive approaches, based on the process involved in creating the fake image [3].

III. METHODOLOGY

We have developed a detection technique to detect forgery image, The figure shows the block diagram of methodology used in the paper. Consider the block diagram shown in figure initially an input image is divided into a number of blocks. The main technique is feature extraction of those divided blocks. We are using DWT techniques for feature extraction. Images has information or features not visible to eye of human. With the assistance of feature extraction techniques, we extract this important features.

Next the Artificial Neural Network (ANN) algorithm is used for feature matching. The output of this matching is the probability of the matched blocks. Then a threshold value is applied and blocks having probability greater than the edge value are considered to be tampered. At last using all feature like DWT and ANN whether an image is forgery or not is detected.

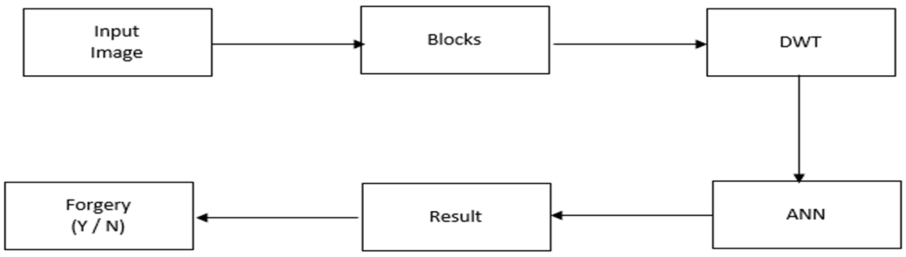

Figure 1. System Architecture

DWT: The DWT represents the signal in dynamic sub-band decomposition. Generation of the DWT during a wavelet packet allows sub-band analysis without the constraint of dynamic decomposition. The discrete wavelet packet transform (DWPT) performs an adaptive decomposition of frequency axis. The specific decomposition are going to be selected consistent with an optimization criterion.The Discrete Wavelet Transform (DWT), supported time-scale representation, provides efficient multi-resolution sub band decomposition of signals. It has become a strong tool for signal processing and finds numerous applications in various fields like audio compression, pattern recognition, texture discrimination, special effects etc. Specifically the 2-D DWT and its counterpart 2-D Inverse DWT (IDWT) play a big role in many image/video coding applications.The DWT architecture, the input image is decomposed into high pass and low pass components using HPF and

ISSN: 2233-7857 IJFGCN

LPF filters giving rise to the primary level of hierarchy. The process is sustained until multiple hierarchies are obtained. The approximation and detail filters are as A1 and D1.

ANN:A man-made neural network is an interconnected group of nodes, inspired by a simplification of neurons during a brain. Here, each circular node represents a man-made neuron and an arrow represents a connection from the output of 1 artificial neuron to the input of another.
Preprocessing is the first step in image processing chain. Preprocessing can be defined as an operation in which the input consists of sensor data and output is a full image. Role of Artificial Neural Networks in these three preprocessing categories are discussed below. ANNs can be applied directly to pixel data as well as features.Image compression and feature extraction are two of the most important applications of data reduction. An image compression algorithm, used for storing and transmitting images, generally contains two steps: encoding and decoding. ANNs were used to implement both these steps.

IV. RESULTS

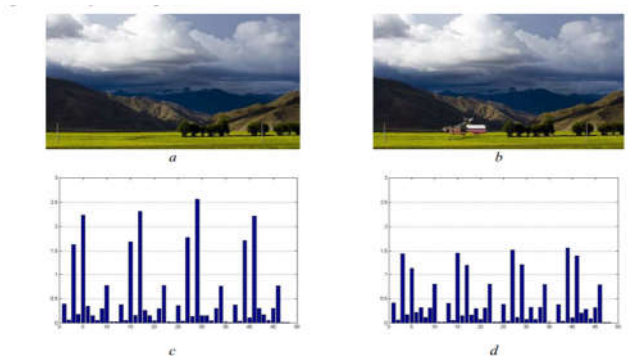

Figure 2(a)
Original image

Figure 2(b)
Forged image

Figure 3(a) above image: original
Figure 3(b) below image: forged

Figure 4(a)
Original image

Figure 4(b)
Forged image

Figure 5(a)
Original image

Figure 5(b)
Forged image

ISSN: 2233-7857 IJFGCN

Shape Features	Size Features	Intensity Features
Circularity	Area	MinIntensity
Roughness	ConvexArea	MaxIntensity
Elongation	Perimeter	MeanIntensity
Compactness	ConvexPerimeter	SDIntensity
Eccentricity	EquivDiameter	MinIntensityBG
Solidity	MajorAxisLength	MaxIntensityBG
Extent	MinorAxisLength	MeanIntensityBG
RadialDistanceSD		SDIntensityBG
		IntensityDifference

Texture Features
11 Haralick features calculated from co-occurrence matrices (Contrast, Correlation, Entropy, Energy, Homogeneity, 3rd Order Moment, Inverse variance, Sum Average, Variance, Cluster Tendency, Maximum Probability)

s

V. CONCLUSION

Hence, this system would help to recognize people.Thus, this framework present a proficient forgery detection utilizing DWT and Artificial Neural Network calculation. We are certainly living in a period where we are defenseless against an amazing exhibit of visual imagery. Picture fake affirmation is making as one of the significant investigate subject among researchers in the region of picture wrongdoing scene examination. This picture forgery area is tended to by isolating an image into blocks. In this system, productive distortion disclosure and request technique is proposed by three distinct stages. From the beginning sort out, preprocessing is finished using particular isolating to evacuate commotion. At second stage, remove uncommon features from delivered picture by using effective element extraction strategy specifically DWT. Finally, delivered picture is perceived by characterizing the kind of picture adulteration using Artificial Neural Network (ANN).

REFERENCES

[1] Saba Mushtaq and Ajaz Hussain Mir,"Digital Image Forgeries and Passive Image Authentication Techniques: A Survey", International Journal of Advanced Science and Technology Vol.73 (2014)
[2] Chandra Sekhar, Dr. T N Sankar,"Review of Image Splicing Forgery Detection Techniques",JETIR (ISSN-2349-5162),December 2016, Volume 3, Issue 12
[3] Snigdha K. Mankar,"Image Forgery Types and Their Detection: A Review",International Journal of Advanced Research in Computer Science and Software Engineering, 2015.
[4] Shwetha B and S V Sathyanarayana,"Digital image forgery detection techniques: a survey",ACCENTS Transactions on Information Security, Vol 2(5)ISSN (Online): 2455-7196, 2017.
[5] Meenakshi Sundaram A.,and C. Nandini, "Feature based Image Authentication using Symmetric Surround Saliency Mapping in Image Forensics," International Journal of Computer Applications,2014
[6] Chih-Chung Chang, Chih-Wei Hsu, and Chih-Jen Lin," The analysis of decomposition methods for support vector machines". IEEE Transactions on Neural Networks, 11(4):10031008, 2000
[7] T. Carvalho, F. A. Faria, H. Pedrini, R. da S. Torres, and A. Rocha, "Illuminant-based transformed spaces for image forensics," IEEE Transactions on Information Forensics and Security,Apr. 2016.
[8] D. Cozzolino, G. Poggi, and L. Verdoliva, "Splicebuster: a new blind image splicing detector," in 2015 IEEE International Workshop on Information Forensics and Security (WIFS), Nov. 2015.
[9] D. Cozzolino, D. Gragnaniello, and L. Verdoliva, "Image forgery detection through residual-based local descriptors and block-matching," in 2014 IEEE International Conference on Image Processing (ICIP), Oct.2014.
[10] M. Chen, J. Fridrich, M. Goljan, and J. Lukas, "Determining image origin and integrity using sensor noise,"IEEE Transactions on Information Forensics and Security, vol. 3, no. 1, pp. 74–90, Mar. 2008.

ISSN: 2233-7857 IJFGCN