International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 03 Issue: 10 | Oct -2019 ISSN: 2590-1892

Face Spoofing Detection in face recognition: A Review

1) Pooja Patil 2) Ashwini Khalangre 3) Rupali Bhagwat 4) Chaitrali Bankar 5) Arati Bachal

Under the guidance of Prof. K.S Bhagwat

Abstract: Face recognition systems is being widely used in various sector like in companies to identify the employee face, to unlock the cellular phones, etc. But criminals are developing various sophisticated techniques to gain the identity of valid user this is known as spoofing attack. face being a promising trait due to its convenience for users, universality and acceptability, traditional face recognition systems can be easily fooled with common printed facial photograph. To avoid such spoofing attacks a system should be developed and integrated with the traditional biometric system to minimize such frauds.Most of progressive anti-spoofing techniques for face recognition extracts texture options from pictures among them Local Binary Pattern(LBP) descriptor has been widely used in spoof detection systems.In most of the system for experimental purpose the NUAA PI DB, the YALE-RECAPTURED DB, the PRINT-ATTACK DB, the CASIA FAS DB, the REPLAYATTACK DB and the 3D MASK-ATTACK DB datasets has been used. This review considers various techniques and compares there accuracy to find out the best spoof detection method.

Keywords: Spoofing detection, deep texture features, Local binary pattern, Nanjing University of Aeronautics and Astronautics(NUAA).

1. INTRODUCTION:

Biometric models have been widely used in security system. Biometric system offers a great security and privacy than traditional methods. Biometric system is a pattern recognition system that identifies the valid user from their physiological and behavioral characteristics[1]. But criminals are developing various sophisticated techniques to get the valid user access. In biometric system majority of attack occurs by fooling capture sensors.

face recognition systems are the ones that suffer the most from spoofing attacks. Face recognition systems can be fooled by using printed photo attack, 3D mask attack, rely attack etc. To minimize such spoofing attack and keep users data safe various techniques have been developed by using various methods.

From the users point of view they are not interested in the technique that has been used for spoof detection rather they want the system that is highly reliable and trustworthy and recognizes the identity and accepts only when it is not a spoof. This paper explains about various types of

spoof and some commonly used spoof detection technologies.

In section 2 literature survey is explained. Section 3 explains about face spoofing and different types of spoofing attack. In section 4 system architecture has been explained in detail. Section 5 gives the conclusion of our work.

2. LITERATURE SURVEY:

Jamil Ahmad et al [9]Through there work they explained the advantages of deep learning and different categories of deep learning. The categories are

1 Deep Networks for Supervised Learning

For both classification and regression tasks, the network tries to get the expected output from the given input. They also explained commonly used architecture for supervised learning are DNN,CNN and RNN.

2. Deep Networks for Unsupervised Learning

In unsupervised learning the algorithm acts on the information without guidance without any training. The commonly used method for unsupervised learning is deep autoencoderand deep Boltzmann machines.

3 Hybrid Approach

In hybrid approach both supervised and unsupervised dataset is present the algorithm is used according to the dataset.

They concluded that the deep learning methods are used widely in various sector such as image detection,object detection,self-driving cars,disease detection etc,due to its high performance and effectiveness.

J.Maatta et al.[6] There proposed system detects whether there is a real live person in front of the camera or a face print[6]. In there system the technique used is multi-scale local binary pattern for analyzing the facial image texture which is integrated with micro-texture pattern to increase the feature of histogram and the result is given to the SVM which determines weather there is a live person or face print.

S. **Parveen et al.**[7] This paper introduced a new texture descriptor known as Dynamic Local Ternary Pattern (DLTP) in the face liveness detection method. By following Weber's law.

DLTP allow not only encoding important texture features but also reduction of the effect of noises for face recognition and verification.

Weber's law is adopted for tuning the threshold value dynamically for every image pattern in the Local Ternary Pattern (LTP).

Tibor et al.[2] They created the database of wild animals. This database consists of 500 different subjects (5 classes / 100 images for each class). The animal recognition system is divided as:

i]. Identification

ii]. Verification.

The overall performances were obtained using different number of training images and test images.

Sonali Swardekar and prof. Sowmiya Nair[3] They studied the facial expression using Local Binary Pattern(LBP) and using convolutional neural networks(CNN). They provided LBP feature map as the input to CNN to improve the understanding of CNN. They also expressed there experimental work which shows why LBP integrated with CNN is better than other techniques. They created a table of different emotion's like happy, angry, unhappy, fear, surprise,etc and the result is displayed explaining

the accuracy percent of each technique. This technique is used for treating patients in medical field, Human machine interaction and some of the application of facial expression recognition.

3. Face Spoofing:

Spoofing is tricking the computer system. Spoofing attack is done to get the access of valid users right without their permission. Such attacks can cause major loss if it is not fixed within time. Most of the attack occurs by fooling face recognition systems. The figure given below shows the classification of spoofing attack methods. Face spoofing is classified into two types 2D spoofing and 3D spoofing. In 2D spoofing printed photos and videos are used for spoofing attack and in 3D spoofing 3D mask has been used for spoofing attack.

3.1 *Methods for face spoofing detection*

There are three major methods used

i. Motion based methods

ii. Texture based methods

iii. Methods based on image qualityanalysis[5].

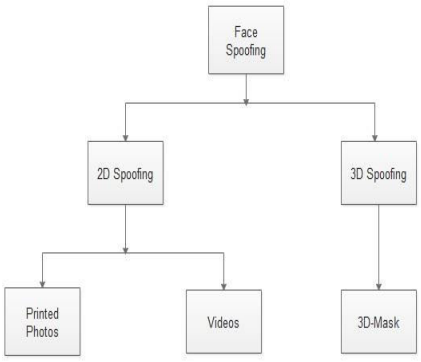

Fig:- Classification of face spoofing.

(1) Motion based methods:

Motion detection tells us the change in the position of object with respect to surrounding or the change in the surrounding with respect to object[4]. Intruder alarms, Automatic tickets gates, Automatic flusher, Hand dryer etc are the applications of motion based technologies

(2) Texture based methods:

Many of the spoof detection techniques are based on texture extraction. In texture descriptor the background texture of the image or video is considered to identify the spoofs like printed photo attack, 3D mask attack, rely attack etc.

(3) Methods based on image quality analysis.

To get the higher accuracy the quality of the image plays an important role. The factors that affects the image quality are noise, artifacts, spatial resolution, etc.

4. SYSTEM ARCHITECTURE:

In face spoofing detection system an image is taken as an input which is then passed to the pre-processing phase the output of pre-processing is sent to the feature extraction phase which then matches the image with the data set image. From the result of matching the decision is made weather the image is real or fake.

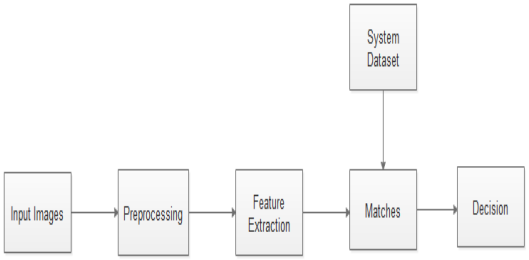

Fig 4.1: System Architecture.

4.1 Local Binary Pattern:

Local binary pattern has been most widely used for texture description. LBP operator replaces the value of pixels of an image with decimal numbers which is called as LBP codes.

Fig 4.1.1 shows the flow of LBP . LBP takes the image, generates the histogram and finally compares the input image with the dataset image to decide wheather the image is real or fake.

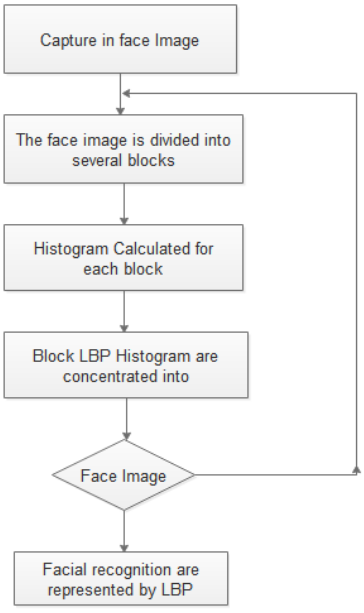

Fig 4.1.1:- Flowchart of LBP

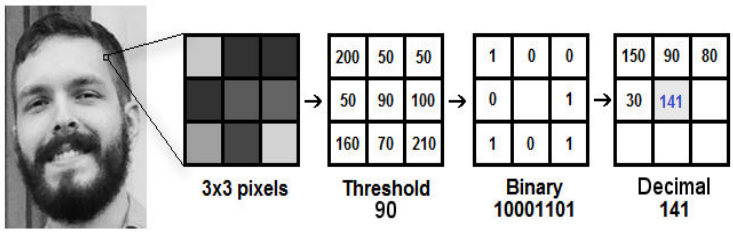

Fig4.1.2:- Working of LBP.

As shown in the fig 4.1.2 to generate the decimal value from the 3*3 matrix the middle value is compared with its eight neighbourhood values where 0 is written in the new matrix if the neighbour value is less than the middle and 1 is written when neighbour value is greater than middle value and a new matrix is generated with 0's and 1's. we convert this binary value to a decimal value and set it to the central value of the matrix. From original image grayscale image is generated from which a histogram of that image is drawn. Histogram gives an overall idea about intensity distribution of an image.

4.2 Convolutional Neural Network(CNN):

CNNis a type of artificial neural network and it has been widely used in image recognition area. CNN has proven itself successful in many machine learning tasks such as handwriting recognition, natural language processing, text classification, image classification, face recognition, face detection,object detection, video classification, object tracking, super resolution, human pose estimation and so on.

There are three layers present in CNN they are input layer, output layer and a hidden layer. Hidden layer contains multiple convolutional layer, ReLU layer, pooling layer, fully connected layer and normalized layer in it.

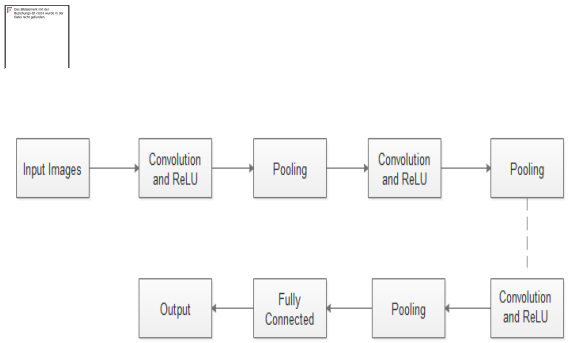

Fig 4.2.1: Working of CNN

In convolutional layer filters are applied on the input to minimize the size and the complexity of the input. Next is ReLU layer where the negative values in the matrix is replaced by zero. There are three types of pooling mean pooling, average pooling and max pooling. Most commonly max pooling is used. In max pooling the image size is reduced by finding the max value from 2 * 2 sized matrix, to reduce the number of parameters, memory and to control overfitting.

In fully connected layer connects all the neurons formed from the pixels into a single list. In Fully Connected layer softmax function is used to identify whether attack or not an attack.

Layer	Type	Properties
Layer1	Input	32*32
Layer 2	1 Convolutional	16 feature maps 3*3 kernel dimension
Layer 3	Pooling	2*2 kernel dimension probability 0.25
Layer 4	2 Convolutional	16 feature maps 3*3 kernel dimension
Layer 5	pooling	2*2 kernel dimension probability 0.25
Layer 6	Fully-connected	3000 neurons
Layer 7	Fully-connected (Softmax)	40 neurons(classes)

Fig 4.2.2: Layers of CNN

4.3 Dynamic Local Ternary Pattern(DLTP):

Local binary pattern has been most commonly used but LBP have certain limitations LBP operator becomes more sensitive to noise. To deal with this problem local ternary pattern(LTP) came into existence.

Unlike LBP, it does not threshold the pixels into 0 and 1, rather it uses a threshold constant to threshold pixels into three values 0,1 and -1.

1, if p>c+k
0, if p>c-k and p<c+k
-1, if p<c-k

Here, p is a neighbouring pixel, c is a center pixel and k is a threshold constant.

LTP have the fixed threshold value which might not be appropriate in many cases. To overcome this limitation of LTP, DLTP(dynamic local ternary pattern) came into existence. DLTP uses Weber's law for assigning the threshold value dynamically for every image pattern in LTP.

Algorithm[11]: Classification-feature generation

Input: Image pair {PA, PB}

Output: Classification-feature vector V **Begin**

Step 1. Divide PA and PB into n blocks Bi(PA), Bi(PB) respectively for i = 1, ..., n Step 2. Calculate histograms Hi(PA), Hi(PB) for each block Bi(PA), Bi(PB) respectively using DLTP, for i = 1, ..., n. Step 3. Calculate the square-root of χ 2 distances between histograms Hi(PA) and Hi(PB) (i = 1, ..., n) to obtain classification-feature vector V of length n.

End

Here, *PA* and *PB* are a face image pair. The algorithm is to produce a classification-feature vector for face verification.

RESULTS:

1. Result of LBP based system[12]

Methods	Performance
Local Binary Pattern(LBP)	89.3%

2 . Result of CNN based system[13]

Network Setups	Recogniti on Task	Corr.Recogni tion
1. Single CNN	Exp	68.5%

3 Result of DLTP based system[14]

Technique	HTER	RATE	AUC
Local Ternary Pattern(LTP)	15.81	84.18	0.785
Dynamic Local Ternary pattern(DLTP)	8.762	91.23	0.91

5. CONCLUSION:

In this paper we have explained various types of spoofing techniques which are used by criminals for spoofing attack. We have also explained the most commonly used technologies for spoof detection. In the results section we have observed that LBP has 89.3% performance rate, CNN has 68.5% performance rate whereas DLTP has 91.23% of performance rate. From the results we have concluded that DLTP(dynamic local ternary pattern) is the best from the remaining two technologies, i.e. LBP and CNN because of its high performance rate.

Therefore this dynamic local ternary pattern (DLTP)method will work best when compared to the other methods and will also provides the efficient result .

REFERENCES:

[1] Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). "*Biometric recognition: security and privacy concerns". IEEE Security & Privacy Magazine, 1(2), 33–42.*

[2] Tibor TRNOVSZKY, Patrik KAMENCAY, Richard ORJESEK, Miroslav BENCO, PeterSYKORA *"Animal Recognition System Based on Convolutional Neural Network"* Department of multimedia and information-communication technologies, Faculty of Electrical Engineering, University of Zilina, Univerzitna 8215/1, 010 26 Zilina, Slovakia

[3] Sonali Sawardekar, Prof. Sowmiya Raksha Naik*"Facial Expression Recognition using Efficient LBP and CNN"*
M. Tech Student, Dept. of Computer Engineering, VJTI College, Maharashtra, India 2Assistant Professor, Dept. of C.E.& I.T, VJTI College, Maharashtra, India.

[4] Shamir Alavi alavi1223@hotmail.com

Electrical Engineering *"Comparison of Some Motion Detection Methods in cases of Single and Multiple Moving Objects"* National Institute of Technology Silchar Silchar 788010 (Assam), India

[5]Ramandeep Kaur, P. S. Mann *"Techniques of Face Spoof Detection: A Review"*D.A.V. Institue of Engineering &Technology

[6] J. Maatta, A. Hadid, and M. Pietikainen, *"Face spoofing detection from single images using micro-texture analysis,"* in Proc. Int. Joint Conf. Biometrics, Washington, DC, USA, 2011, pp. 1–7.

[7] S. Parveen et al., *"Face liveness detection using dynamic local ternary pattern (DLTP),"*Computers, vol. 5, no. 2, p. 10, 2016.

[8] C. Cortes and V. N. Vapnik, *"Support-vector networks,"*Mach. Learn., vol. 20, no. 3, pp. 273–297, 1995.

[9]Ahmad.J, Farman.H,and Jan.Z,*"Deep learning: Methods and applications,"*Found. Trends Signal Process., vol. 7, nos. 3–4, pp. 197–387, 2014.

[10] Chingovska, I., Anjos, A. R. dos, & Marcel, S. (2014). *"Biometrics Evaluation Under Spoofing Attacks"*. IEEE Transactions on Information Forensics and Security, 9(12), 2264–2276.

[11] Mohammad Ibrahim, Md. Iftekharul Alam Efat, Humayun Kayesh Shamol, Shah Mostafa Khaled, Mohammad Shoyaib,*"Dynamic Local Ternary Pattern for Face Recognition and Verification"*. Institute of Information Technology, University of Dhaka, Bangladesh.

[12] TS Vishnu Priya, G.Vinitha Sanchez, N.R.Raajan*,"FacialRecognition System Using Local Binary Patterns(LBP)"*. School of Electrical & Electronics Engineering, SASTRA Deemed University, Thanjavur, India.

[13] Fasel, B. (n.d.).*"Robust face analysis using convolutional neural networks"*. Object recognition supported by user interaction for service robots.

[14] Sajida Parveen, Sharifah Mumtazah Syed Ahmad Abdul Rehman, Nadeem Naeem,Jherna Devi,Mukhtiar Ahmed. *"The Improved Complete Dynamic Local Ternary Pattern Texture Descriptor for Face Spoof Attacks"*.