International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 05, May 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

PREVENTION OF FACE SPOOFING ATTACKS AND ITS DETECTION USING LBP

Mr. Kaustubh D.Vishnu[1], Dr. R.D.Raut[2], Dr. V. M. Thakare[3]

SGBAU, Amravati, Maharashtra (India)

ABSTRACT

Preventing personal data from attackers is most challenging task. System which uses face for authentication purpose must be robust against face spoofing attacks. This paper aims to provide a method to detect such attacks and prevent system from spoofing attacks. Proposed method identifies the face from the input image and extracts information and compares the extracted information with database to detect whether input image is authorized or it's a spoof attack. This paper proposes a technique for face detection using LBP which is ultimately preventing system from the spoof attack by identifying the authorized face image. The proposed method gives the easy and effective method to detect spoofing attacks and increase security of system.

Index Terms— Face detection, LBP, Spoofing attack, Security

I. INTRODUCTION

Security against the spoofing attacks is most needed feature to increase system's robustness against various attacks. Face spoofing is one of attacks which threaten the security of system. Preventing the system from spoof attack is a process of automatically detecting whether two faces are of same person or not. Number of factors makes this a challenging for computer. Faces in images and video are mostly captured with different cameras with different imaging properties and also it may be captured at various resolutions, quality, and lighting conditions. Most of the system uses digital images and video for authentication and processing purposes thus digital images and videos are important in the multimedia information era. The human face is one of the most important objects in an image or video. Detecting the location of human faces and then extracting the facial feature in an image is an important ability with wide range of applications, such as human Face Spoofing, surveillance systems, human computer interfacing, video-conferencing etc. In process of detecting whether two faces are of same person or not, the texture features of the images must be taken into consideration[1].Distortion of image while extracting image properties must be analysed properly to extract more and more information from the image[2].Obtaining the feature space for coupling spoofing detection and face recognition is done by encoding the micro-texture pattern of the image using LBP[3].Extracting the useful information from the image and collecting them to use them for detecting the legal face for access is also a effective method to prevent spoofing attacks[4].Data driven method for spoof detection is mostly used, thus the effective method should be

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

used to extract useful information from the input image. Dynamic mode description and LBP features makes the system data rich which is very useful in preventing system from spoofing attacks[5].

In this paper we have proposed a method for prevention of Face Spoofing that is robust, reasonably simple and accurate with a relatively simple and easy to understand algorithms and techniques. With the given image, the goal of face detection algorithm is to detect the face and extract the features from given image and then extracting LBP patterns and executing LBP matching is done and matching of extracted information is performed with given database of face images which will be useful to identify real and spoofed image.

II. BACKGROUND

Most of the existing face recognition systems are vulnerable to spoofing attacks. The facial appearance analysis based methods are referred to as texture or image quality analysis based techniques. Face Spoofing Detection Using Colour Texture Analysis explore the facial colour texture content using four descriptor which are ,the local phase quantization(LPQ), the co-occurrence of adjacent local binary patterns(CoALBP), the binarized statistical image features(BSIF) and the scale-invariant descriptor(SID) Colour texture based approach provides an in depth analysis on the use of colour texture analysis for face spoofing detection[1].

Real time face spoof detection requires a decision to be made based on a limited numbers of frames. Thus a method is proposed with a discriminating features that is capable of differentiating between real and fake face image. Face spoofing detection approach based on Image Distortion Analysis(IDA) is proposed which is effective in grasping the intrinsic distortions of spoof face images with respect to the genuine face images[2].Current face biometric system are vulnerable to spoofing attacks, by falsifying data attacker thereby gains illegitimate access to private information. Such problem of face spoofing detection is handled from texture analysis point of view. Printing quality defects can be easily detected using texture analysis and local shape analysis. A method is proposed to analyse the texture and gradient structures of the facial images using a set of low-level feature descriptors, fast linear classification scheme and score level fusion[3].A method for extracting temporal and spectral information from face biometric samples, referred to as time-spectral descriptors. The visual codebook model also referred to as Bag-of-Visual-Word model, for creating a mid-level representation from time-spectral descriptors, referred to as time-spectral visual words which works best while gathering important knowledge[4]. The exploitation of the facial dynamic information is a completely data-driven fashion, rather than using prior knowledge regarding live face images such as eye-blinking and lip-movements. In order to extract facial dynamic information reliably ,a method gives a modified version of Dynamic Mode Decomposition (DMD) which helps to detect a print and replay attacks from live (valid) videos containing an authentic face[5].

This paper presents the brief introduction of face spoofing prevention and its detection in section I. Section II discusses background. Section III discusses previous work. Section IV discusses existing methodologies. Section V describes proposed methodology. Section VI discusses analysis and discussion. Section VII discusses the possible outcomes and result. Finally section VIII concludes this paper.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

III. PREVIOUS WORK DONE

Zinelabidine Boulkenafet et.al (2016) [1] proposed method to detect morphed face while preventing from spoofing. A statistical analysis is done on datasets and histograms is done for both real and fake image using texture of image. The proposed method aims to investigate the effectiveness of different texture descriptors more closely in detecting various kinds of face spoofs by extracting holistic face representation from luminance and chrominance image in different colour spaces.

Di Wen et.al (2015) [2] proposed method feature set based on image distortion analysis (IDA) with real time response and better performance in cross database scenario. Proposed method try to capture the face image quality differences due to the different reflection properties of different materials. Proposed method aims to design discriminative features that are capable of differentiating between genuine and spoof faces based on a single frame. Proposed method try to differences genuine face image and fake face image which mainly occurs in Print photo Attack and Replay Video Attack.

J. Maatta et.al (2012) [3] proposed method which adopts complementary properties of two powerful texture descriptors, since LBP encodes the micro-texture patterns and Gabor filters more macroscopic information. In addition, HOG-based local shape description provides additional information to the face description. A homogeneous kernel map is applied on each resulting feature vector transforming the data into compact linear representation and reproducing an accurate approximation of the desired kernel function. This representation enables then to use fast linear support vector machine (SVM) classifiers. The final decision, whether there is a live person in front of the camera or not, is based on the score level fusion of the individual SVM outputs. Extensive experiments on three publicly available database (NUAA Photograph Imposter Database , Yale Recaptured Database and Print-Attack Database) containing several real and fake faces showed excellent result compared to many previous works.

Allan Pinto et.al (2015) [4] proposed method can be explained in three proposed forms which are low-level descriptor extraction, mid-level descriptor extraction, and classification. Low-level descriptor extraction contains calculations such as calculation of residual noise videos. Next step is mid level descriptor extraction which involves visual codebook generation , coding which performs point wise transformation and then pooling which summaries the collected information. After this the classification is done using available functions (PLS) and (SVM).

Santosh Tirunagari et.al. (2015) [5] proposed method which is concerned with rendering a face recognition system robust against presentation attacks; and specifically, print attacks based on printed facial images, and replay attack that is carried out by replaying a video sequence using a tablet or a mobile phone. Proposed system is pipelined, consisting of DMD, LBP and SVM. This combination is ideal because DMD captures the visual dynamics in the form of a fixed-size image, LBP can effectively capture the dynamic patterns, and SVM is known to be an ideal general-purpose classifier that minimizes the empirical risk of classification error.

IV. EXISTING METHODOLOGY

There are various approaches proposed by various researchers for image based Face Spoofing. Description of those few approaches are as follows,

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

A. Colour Texture Analysis Approach:

Comparison of performance of the colour texture features and gray scale counterparts is basic of colour texture analysis approach. The model parameters are trained and tunes using a subject-disjoint cross validation on training sets and the result is reported in terms of Equal Error Rate (EER).Then combine complementary facial colour texture representation to form the final face description used in anti-spoofing method and compares its performance. Cross database testing improves reliability of method.

B. Distortion Feature Extraction Approach:

Image distortion feature extraction is done using four different features such as Specular reflection Feature, Blurring Feature, Chromatic moment Feature, Colour Diversity Feature. Concatenation of feature happens. It is desirable to have a efficient classifier for the extracted IDA features. Construction of group of training samples firstly divides spoof samples into K training sets according to attack type then a specific training set is constructed by combining all genuine samples and a single group of spoof samples .Multi-Frame fusion is then executed.

C. Texture and Local Shape Analysis Approach:

Low-level feature extraction and Classification are the basic execution modules of Texture and Local Shape Analysis approach. In low level feature extraction The LBP texture analysis operator is defined as a gray scale invariant texture measure derived from local image neighbourhood. In addition to the LBP-based texture analysis, this method also uses Gabor wavelet features to enhance the texture representation of the facial image. The basic idea is to extract features at multiple scales and orientation using a Gabor wavelet decomposition. For classification purposes, a feature vector is constructed using the mean and standard deviation of the magnitude of the transform coefficients at different scales and orientations. The local shape characteristics are introduced to the face representation using HOG which captures the edge or gradient structures of the facial image. HOG representation is invariant to local geometric transformations if translations or rotations are much smaller than the local spatial or orientation bin size. And in classification section the desired kernel can be approximated to a very good level by linear ones using suitable explicit feature map which transform the data into a compact linear representation. SVM classifier and conventional Z-score normalisation technique and weighted score level fusion are used for combining the outputs of the individual SVMs to determine whether the input image corresponds to a live face or not.

D. Spectral Temporal Cubes Approach:

Low-level descriptor extraction, mid-level descriptor extraction, and classification are the three execution forms of the spectral temporal cubes approach. This approach performs the analysis which are done using Low-Level Descriptor Extraction Parameter Analysis (LGF and M) and Mid-Level Descriptor Extraction Parameter Analysis (CS, SDD, DS, and CP) and Classification Step Parameter Analysis (C).Algorithm takes advantage of noise and artifacts added to the synthetic biometric samples during their manufacture and recapture is improving the performance of an approach.

E. Visual Dynamics Approach:

Visual Dynamics Approach presents the pipeline mechanism of method which consist of DMD, Local Binary Pattern histogram and kernel based SVM. This approach processes a image or video using the DMD algorithm in order to output dynamic mode images. From which, a single dynamic mode image is selected, then the LBP

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

histogram features are processed for dynamic mode image. And finally the produced LBP code is fed into a trained SVM classifier in order to classify whether the processed video is a valid access or spoof.

V. ANALYSIS AND DISCUSSION

Lot of researchers have worked on effectiveness of face recognition techniques and methods to detect and prevent spoofing attacks. Most of the current Face Spoofing systems presume that faces are readily available for processing. However, in reality, we do not get images with just faces. We need a system, which will detect the face in image, so that this detected face can be given as input to Face Spoofing systems. The goal of a face detection algorithm is to identify the location and scale of all the faces in image. The task of face detection is so trivial for the human brain, yet it still remains a challenging and difficult problem to enable a computer to do face detection. This is because the human face changes with respect to internal factors like facial expression, beard and moustache, glasses etc and it is also affected by external factors like scale, lightning conditions, contrast between face and background and orientation of the face. Digital images and video are becoming more and more important in the multimedia information era. The human face is one of the most important objects in an image or video. Detecting the location of human faces and then extracting the facial feature in an image is an important ability with wide range of applications, such as human Face Spoofing, surveillance systems, human computer interfacing, video-conferencing etc

Effectiveness of detecting faces using a view based approach is implemented. The neural networks are powerful tool to solve pattern recognition problems, and can potentially be applied at each stage of a Face spoofing system. Firstly the pre-processing of face image is gone through the various steps like enhancement of image, segmenting the image, then these pre-processed images are fed to the trained neural network. After that the initial network connection weights are optimized. In testing process, this neural network tests the input images with the given or template images. If it is matched then show the accurate face and display their characters, otherwise test will continue. If all images are scanned, then end otherwise scanning will be continue. It gives the correct recognition rate

Face spoof detection and prevention technique	Advantages	Disadvantages
Colour Texture Analysis Approach	1.conducts a cross database evaluation with stable performance.	1.Sensors must be powerful and effective. 2.expensive or impractical requirements
Distortion Feature Extraction Approach	1.Low Cost of launching. 2.Result within a single frame of image.	1.HTER increases under cross-database scenarios

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Texture and Local Shape Analysis Approach	1.robust and does not require user co-opration.	1.It requires high resolution input image. 2.Low cost devices does not gives accurate results.
Spectral Temporal Cubes Approach	1.Low cost solutions for spoofing detections. 2.Does not rely on user interaction or on extra hardware.	1.Attacks with high quality samples are hard to detect.
Visual Dynamics Approach	1.Pipeline of DMD+LBP+SVM proves to be efficient, convenient to use and effective.	1.Co-ordinating complexities of the outputs of pipelined classifiers.

Table 1: Comparison Between Different Anti Face Spoofing Techniques

VI.PROPOSED METHODOLOGY

A method of Face Spoofing that is fast, robust, reasonably simple and accurate with a relatively simple and easy to understand algorithms and techniques. Given an image, the goal of face detection algorithm is to detect the face and extract the features from given image and to recognize the detected face with given database of face images which finally help to decide whether the input image is of same person or not which ultimately helps to prevent system from spoofing attacks. Effective use of available resources is making the method more co-operative to implement. Framework of proposed method can be understood using following diagram

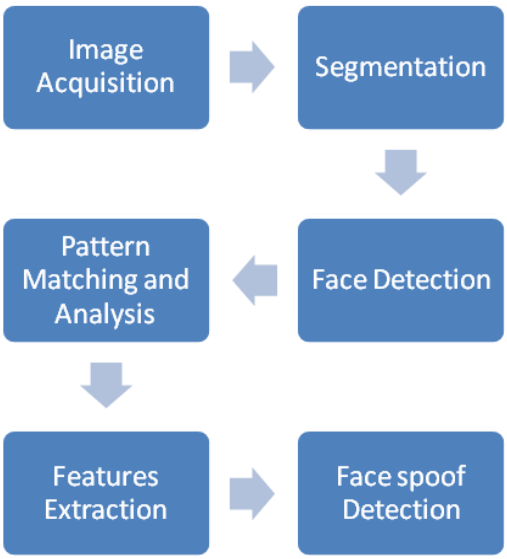

Figure: Proposed Framework For Face Recognition & Detection Of Spoofing Attack.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Algorithm proposed is as follows:

Algorithm:

1. Input Face
2. Detect Skin Colour from input Face
3. If Skin Colour Present then algorithm will go for face detection else discard input image.
4. Face Detection will be done where features are detected with reference distance .
5. if face present , face features like (eyes, nose, mouth) will be extracted else input image discarded.
6. Selected Face Features play an important role in Face Spoofing

Face recognition is important part of spoof detection and proposed method uses efficient way to detect face portion within the image and extracts information from that selected portion only so that unnecessary extraction gets eliminated from execution. Then discriminate analysis is performed along with information extraction. Available database is used for information matching purpose. This complete execution helps to detect genuine and fake face used for authentication, which prevents system from spoof attack.

VII. POSSIBLE OUTCOMES AND RESULT

Effectiveness of detecting faces using a view based approach is implemented. Various techniques are used to propose a method to solve pattern recognition problems, a technique for face detection and recognition using LBP is proposed which is expected to produces reliable and robust outcomes against face spoof attack.

Proposed method excludes unnecessary portion from information extraction process, which definitely improves response time. And simple execution of proposed method reduces complexities in proposed method. Less complications and quicker response time gives the best result for proposed method.

VIII. CONCLUSION

This paper proposed a method which explains the effectiveness of first detecting face region from the image and then extracting the information from image to match the faces for preventing system from spoof attacks. Objective of this method is that it gives a simple and robust method to detect face and checks for spoof attacks. Using LBP techniques this method helps system to prevent from face spoofing attacks.

With less user interaction and less complex execution proposed method gives more user friendly experience. Proposed method does not demands for external hardware supports or costly sensors thus cheaper execution model is proposed.

REFERENCES

[1] Zinelabidine Boulkenafet, Jukka Komulainen, and Abdenour Hadid, “Face Spoofing Detection Using Colour Texture Analysis” IEEE Transactions On Information Forensics and Security. Volume 11, Issue No. 8, PP 1-13 August 2016

[2] Di Wen, Hu Han and Anil K. Jain, “Face Spoof Detection With Image Distortion Analysis” IEEE Transactions On Information Forensics and Security. Volume 10, Issue No. 4, PP 746-761April 2015

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

[3] J. Maatta, A. Hadid, M. Pietikainen, "Face spoofing detection from single images using texture and local shape analysis" Published in IET Biometrics. Volume 1, Issue No. 1, PP 3-10 February 2012

[4] Allan Pinto, Helio Pedrini, William Robson Schwartz and Anderson Rocha, "Face Spoofing Detection Through Visual Codebooks of Spectral Temporal Cubes" IEEE TRANSACTIONS ON IMAGE PROCESSING. Volume 24,No 12,PP 4726-4740 December 2015

[5] Santosh Tirunagari, Norman Poh, David Windridge, Aamo Iorliam, Nik Suki, and Anthony T S. Ho, "Detection of face spoofing using visual dynamics". IEEE Transactions On Information Forensics and Security. Volume 10, Issue No. 4, PP 762-777, April 2015