Survey on Secure Face: Spoof Detection

Priyanka Agarwal
Department of Computer Engineering
Pimpri Chinchwad College of Engineering, Pune

Shambhavi Joshi
Department of Computer Engineering
Pimpri Chinchwad College of Engineering, Pune

Kalyani Kamble
Department of Computer Engineering
Pimpri Chinchwad College of Engineering, Pune

Abstract

Spoofing attack against biometric systems is still an important issue. Face spoofing is a form of attack that is presenting a fake sample to the acquisition sensor with facial information of a valid user. Compared to various attacks against fingerprint, speech or iris recognition systems, the ubiquitous nature of image acquisition devices, such as cameras and smartphones, allows attackers to acquire facial images of a user easily and discretely. This paper presents a literature survey on spoof detection methods and proposes a method to detect whether the input face is spoofed or not. Edge Adaptive Hybrid Filter is used for image enhancement and Naive Bayes classifier is used for classification to detect spoofed face.

Keywords- Spoof Detection, Naive Bayes classifier, Edge Adaptive Hybrid Filter

I. INTRODUCTION

Today there are many applications which can fulfill the user's need in short period of time. So, to provide authorization and authentication so that unauthorized user will not get permission to enter into the system, Biometric technique is used. There are many biometric techniques like fingerprint, face, iris, palm,etc.So developer can provide security by making use of one of this biometric technique. However, one of the most challenging task is to identify the theft, which is conceptually known as spoofing attack.

As compared to other biometric systems, face recognition is a user convenient authentication technique because it it does not require any additional hardware as required for iris and fingerprint biometric system. So, most of the spoofing attacks is done on face biometric systems.

In this the spoofing attack will occur when someone tries to bypass a face biometric system by presenting a fake face in front of the camera. However, face recognition authentication system is vulnerable to several attacks like print attack, replay attack and 3D mask attack. Attackers can easily spoof the system by downloading a photo from the internet or by capturing a photo of the authenticated user. Also, the attacker can penetrate the system by replaying a recorded video in front of a camera. Also, the attacker can have a 3D masking and the he will sit in front of the camera for penetrating into the system.

In an attempt to address this issue, many researchers have proposed different methods to prevent the spoofing attacks. Broadly there are 2 methods: (1) Cue - based method and (2) Data Driven method. In Cue – based method liveliness of the user is detected using only the specific properties like eye blinking, lip movement, facial expression and in data driven method motion analysis and texture analysis is done.

Face spoof detection system can be used in applications like employee identification, in ATM's,in banking domain, also in attendance monitoring system. Over here security is the major concern as the unauthenticated user or the user who is authenticated but he is not present in that current situation are the spoofed users who can hack the system. So this as motivated us and so our primary goal will be to identify and detect the spoofed users in less response time.

II. LITERATURE SURVEY

Various spoof detection methods are proposed by many researchers. Detailed description of various methods is done.
The technique used in [1] to identify the liveliness detection of the user is DMD + LBP + SVM. Basically DMD (dynamic mode decomposition) algorithm is used to convert the n frames of a single video into one single image of the same dimension as that of the frames in input video. After that in the second stage, LBP (Local binary pattern) technique is applied on that image and the histogram is generated. Based on the histogram SVM (support vector machine) classifier gives result as whether the image is spoofed or not. The technique used is completely based on data driven approach. So, dynamic facial information can be extracted using data driven approach rather than using prior knowledge of live face images such as eye blinking and lip movements as that is used in Cue based methods. This method can be used for print attack and video attack. But as DMD is used so it can efficiently handle large sized videos for computation.

In [2] liveliness detection of the user is done based on colour texture analysis. The technique which is used over here is LBP (Local Binary Pattern) + SVM (Support Vector Machine).

The author has mainly focused on the analysis of the luminance information of the face images and discarding the Chroma component due to which fake images can be discriminated from genuine ones. In this technique the author has converted the input RGB image into YCbCr colour space instead of gray-scale colour space because the evaluation suggest that the facial colour texture representation is more stable in unknown conditions compared with its gray-scale counterparts. Then LBP technique is applied on three different colour channels i.e. Y,Cb and Cr and then the histograms which are being generated by using the LBP are concatenated and SVM classifier is applied to find whether the input image is spoofed or not.

The technique which the author has used in [3] deal not only with face liveliness detection but also recognition. The feature descriptors are defined using shear let transform and the stacked auto encoders and softmax classifier is used. The input image/video is given from which the features are extracted and stored in stacked autoencoders.Also the features which extracted are given to next stage where the detection is done whether is user is lively present or not. If the user liveliness is detected as valid, then the features which were stored in stacked auto encoders based on that the face recognition is done. The drawback which were there in using LBP and SVM classifier has been overcome by using feature descriptor based on shear let transform.

Aziz Alotaibi, AusifMahmood [4] proposed a deep convolution neural network to extract local and complex features of input diffused image. Here non-linear diffusion is used with large time size for obtaining sharp edges and preserving boundary locations of input image. This method uses only one frame of input image. When replayed video attack takes place, the proposed method utilizes only one frame from sequenced frames.

Here the frame is captured using various mediums such as printed photograph, mobile screens, and tablet screens. Method is tested over a dataset consisting of 1200 short videos containing real access and spoofing attack videos.
Proposed deep convolution consists of 6 layers. First 5 layers are convolution and subsampling layers and last layer is output layer. Here neural network concept is used to decide whether the input image is fake or real.

Fake facial images had shown fewer sharp edges and flattened surfaces around nose, lips, eyes and cheek regions. Whereas real facial image shows proper sharp edges around nose, lips, eyes and cheek region. In this way we can differentiate between fake and real facial images.

Quoc-Tin Phan, Duc-Tien Dang-Nguyen, Giulia Boato, Francesco G. B. De Natale [5] proposed novel face spoof detection technique using Local Derivative Pattern from 3 orthogonal planes (LDP-TOP).LDP-TOP is a data driven based method. Both spatial and temporal information is considered. LDP extracts high order local information so that subtle changes on the face can be highlighted. Proposed method consists of 3 steps:

1) Face Detection and normalization:

Each input video frame is grey-scaled and then passed through face detector. Normalization is performed on detected faces.

2) LDP-TOP histogram Extraction:

LDP operators are applied over 3 orthogonal planes intersecting at centre and then extracted histograms are concatenated.

3) Classification:

In this step, output of previous step is given as input to SVM classifier which determines whether the video is spoofed or not.
This method is simple and computationally efficient and so it is suitable for real time processing and low cost devices but it does not work well under different conditions.

Zinelabidine Boulkenafet derived [6] multiscale space to represent facial images before extraction of texture features. Variations in input image quality and resolution are considered. Following 3 types of multiscale filtering approaches are considered in this paper for detecting and characterizing edges of small and large structures.

1) Gaussian Scale Space:

Convolution with Gaussian kernels is helpful for reducing noise in input images which also emphasizes coarser structures.

2) Difference of Gaussian (DoG) scale space:

In this blurred image is subtracted from another image. It is equivalent to band pass filter.

3) Multiscale Retinex:

Here, image is considered as multiplication between illumination component and reflectance component. Each of these components are applied on each scale.

After that from each scale, textual histograms are extracted using LBP. These histograms are then concatenated and passed through SVM. Finally SVM decides whether the image is real or fake. DoG scale space image representation showed high performance.

In paper [7] liveliness detection of the user is done using Local Ternary Pattern. The proposed technique consider facial texture as a feature to extract from the input. Local ternary approach is used to extract the textural features and generate the ternary pattern. After this the upper pattern and lower pattern are extracted. The threshold value 5 is considered as it is optimum value. Upper patterns are the pixel values that are beyond the threshold value and lower pattern consists of pixel values which are below the threshold value. After the generation of patterns, histogram is generated and then SVM classifier is used to detect whether the image is spoofed or not.

III. PROPOSED SYSTEM

The proposed method consists of three main steps. Initially face is captured and face detection and normalization technique is applied. Each video frame is gray-scaled and passed through face detector. Then detected face is normalized.

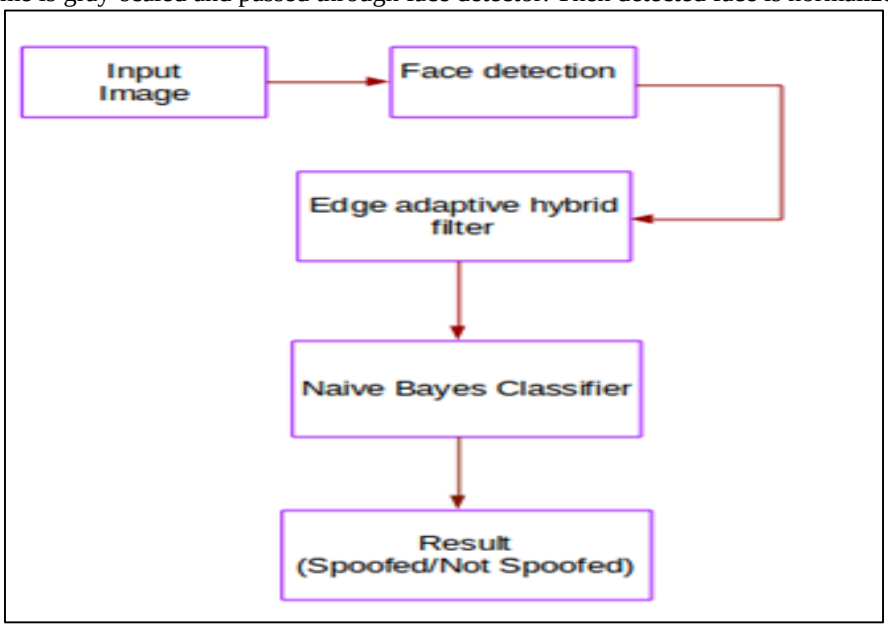

Fig. 1: Schema of proposed method

In the second step Edge Adaptive Hybrid Filter is applied for image inhancement.The image is converted into binary image and to improve the edges, high pass and low pass filter masking is applied. If the pixel I(i,j) is an edge then the high pass filter masking is applied and if it is not an edge the low pass filter masking is applied.

In the third step Naive Bayes classifier is applied. Input will be the feature vector, and it will classify whether the input image is spoofed or not.

IV. CONCLUSIONS

Thus there are many methods for checking liveliness of the user. Methods like visual dynamics, colour texture analysis, shear let transform, deep learning. In the proposed work, Edge Adaptive Hybrid Filter is used which gives better results than histogram processing.

ACKNOWLEDGMENT

We are thankful to our project guide Mrs. Santwana Gudadhe and Head of the Department Mrs. Rajeswari for her support, remarks, and suggestions for providing all the important facilities like Internet access which were essential to carry out the survey. I am also grateful to all the staff members of the Department of Computer Engineering of Pimpri Chinchwad College of Engineering for their assistance in improving the survey paper significantly.

REFERENCES

[1] Tirunagari, Santosh, et al. "Detection of face spoofing using visual dynamics." IEEE Transactions on Information Forensics and Security 10.4 (2015): 762-777.
[2] Boulkenafet, Zinelabidine, Jukka Komulainen, and Abdenour Hadid. "Face Spoofing Detection Using Colour Texture Analysis." IEEE Transactions on Information Forensics and Security 11.8 (2016): 1818-1830.
[3] Li, Yuming, et al. "Face liveness detection and recognition using shearlet based feature descriptors." 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2016.
[4] Alotaibi, Aziz, and Ausif Mahmood. "Enhancing computer vision to detect face spoofing attack utilizing a single frame from a replay video attack using deep learning." Optoelectronics and Image Processing (ICOIP), 2016 International Conference on. IEEE, 2016.
[5] Phan, Quoc-Tin, et al. "FACE spoofing detection using LDP-TOP." Image Processing (ICIP), 2016 IEEE International Conference on. IEEE, 2016.
[6] Boulkenafet, Zinelabidine, et al. "Scale space texture analysis for face anti-spoofing." Biometrics (ICB), 2016 International Conference on. IEEE, 2016.
[7] Diviya, M., and Susmita Mishra. "A novel approach for detecting facial image spoofing using local ternary pattern." Science Technology Engineering and Management (ICONSTEM), Second International Conference on. IEEE, 2016.