A Survey on Facial Spoofing Detection

Shyama V S, Mary Linda P A

***Abstract*— Spoofing attacks to the biometric systems has greatly effected in verifying the identity of an individual. Detection of the spoofing attacks is a serious problem whereas face recognition systems and voice authentication systems are mostly vulnerable to spoofing. Traditional spoofing detection methods are not up to the mark due to the rapid increase in the hacking methodologies. Several spoofing attack detection methods have been proposed and few of which have been summarized below. The basic method used in detection of spoofed video uses prior knowledge regarding live face images such as eye blinking and lip movements since attack types are often unknown and very different from each other. Due to the lack of efficiency and accuracy whereas handling excessive attacks, specific cue which is peculiar to the attack must be developed. Thus a data driven approach with high accuracy and efficiency was developed. A combination of Dynamic Mode Decomposition, Local Binary Patterns, and Support Vector Machine were introduced for identifying print attacks and replay attacks. It results in better security, scalability, efficiency and accuracy.**

***Index Terms*—Dynamic Mode Decomposition, Local Binary Patterns, Spoofing, Support Vector Machine**

I. INTRODUCTION

Biometrics is a technology that can measure and analyze the human body characteristics. It involves both Physical characteristics such as fingerprints, faces or iris patterns and behavioral characteristics such as voice, signature [1]. One of the main challenge that the biometric recognition systems faces today is the unauthorized access of the individuals and thereby the efficiency, accuracy and effectiveness of the system is hampered. Spoofing attacks is one among the cause for illegitimate actions in the biometric systems. Spoofing attacks can be defined as the method of falsifying the biometric system by an unauthorized system such as the use of artificial fingers, contact lens with retinal patterns and recorded voice etc. Among them liveness facial biometrics based spoofing detection is to be considered seriously as it is highly prone to spoofing attacks. Facial biometrics spoofing techniques involve placing genuine photographs or dummies, playing video recording etc. in front of the camera.

Liveness face detection can be either positive class or negative class. Positive class have limited variations and negative class includes the spoofed faces on photographs, dummy or recorded videos. Detection may be influenced by the lighting, picture quality etc. Other than these, in liveness detection for facial biometrics, there are limitations such as lack of accuracy and efficiency in identifying the presentation attacks, replay attacks and print attacks, lack of extracting the unique features that distinguish a valid and spoofed videos, lack of providing the three dimensional (3D) information. To overcome these limitations, a data driven approach is considered called Dynamic Mode Decomposition (DMD) [2] combined with Local Binary Patterns [3] and Support Vector Machine [4] so as to provide efficient liveness detection of the facial biometrics.

Extraction of the unique features and relevant modes from videos in face recognition can provide a good separability between valid videos and the spoofed ones. DMD has the capability of capturing and discovering the important signs of valid face videos and at the same time artefacts of spoofed videos such as moiring and planar effects are also being extracted. Thus it is computationally efficient in handling the large sized videos as it considers the deep and accurate complex flow behavior of the features that can tackles both photo based and video based spoofing attacks.

II. LITERATURE SURVEY

Most of the work on the facial spoofing detection focus on the outline structure of facial expressions such as eye blinking, lip movement, and head movement. It is hopeful that a detailed description of the features can be extracted to detect the spoofed sample and valid sample.

Xiaoyang Tan [5] proposes a method for face liveness detection against photo spoofing by using sparse bilinear discriminative model for a single image. In this method real time and non intrusive method is used to distinguish the distinct surface properties of a photograph and a real human face. Firstly, by using the Lambertian model that focus on the reflecting surface of the image, two strategies were proposed to extract the essential information in the given image, in terms of latent samples. Several illumination invariant face recognition algorithm are used to collect the needed latent samples.

Tan uses Variational Retinex based Method and Difference of Gaussian Method for collecting the samples. In Variational Retinex Based Method the face image is decomposed into reflectance part and illuminance part and thereby the centered Fourier spectra of the raw image is analyzed. Then, Difference of Gaussian method (DoG) is used to filter the raw image being analyzed. Finally by using the sparse nonlinear/bilinear discriminative model upon this filtered image, the spoofed samples can easily be detected.

The proposed method has the advantages of real time testing, non intrusion and no extra hardware requirement. But this method holds some disadvantages like it cannot handle various texture based images for analyzing the spoofed samples, it cannot change the dynamic range of the whole image and also an illumination change will have a

Manuscript received Dec, 2015.

***Shyama V S**, Department of Computer Science and Engineering, KMCT College of Engineering, Calicut University Calicut, India*

***Mary Linda P A,** Department of Computer Science and Engineering, Calicut University, Calicut, India.*

ISSN: 2278 – 7798

negative impact on the results made. Moreover this method require more time to perform the operations.

B. Pexito [6] proposed a method to detect the spoofed sample under bad illumination conditions. It is an extension to the method developed by Tan [5]. This method mainly focus on the spoofing detection of high quality and recaptured printed images. It also works for a single image. Various databases are being used for the detection.

In this method firstly the image is analyzed by using Difference of Gaussian filter which is a bypass filter. As a result, high middle frequencies are identified and it helps to detect the borders of the image. But under bad conditions it fails to detect the borders. So the method uses Contrast Limited Adaptive Histogram Equalization (CLAHE) [20] method is adopted. This method operates on the small regions of the image that are called as tiles and various distributions such as uniform distribution exponential distributions are also used so that it works under bad illumination conditions.

The advantages of this proposed method is that it does not require any extra devices or user involvement and thereby it provides good classification results with low false positive and false negative rates even for dark images. But the disadvantage is that it does not consider about the spoofing that are entering from the cell phone screens and also dimensionality reduction problem. The method has a future work of implementing a binary classifier for the detection of spoofed sample and actual sample.

Li [7] cross examined the Fourier spectra of the image for the live face detection and ensured more correctness of authentication new method for live face detection. The method can distinguish the spoofed and original sample by analyzing the Fourier Spectra of a single face image or face image sequences. Li focused on the two principles for the detection of spoofed samples. Firstly the high frequency components of the photo images is less than the real face images and secondly the standard deviation of the frequency components in the sequence must be small.

At first a subset of images are constructed by extracting image from an input image sequence of every four images. An energy value is computed for every image in the subset. From the subset three images are randomly selected and corresponding High Frequency Descriptor (HFD) is calculated. If the median of the HDD is smaller than threshold value, then it can be concluded that it is a fake face. Otherwise the Frequency Dynamic Descriptor (FDD) is computed and then it is compared with the threshold value. If the FDD is less than the threshold value then it is a spoofed sample otherwise the sample is a live face.

The Li's method has an advantage of effectively preventing the spoofing of small size fake image with the help of high frequency descriptor and frequency dynamic descriptor helps in identifying the motion of large size fake images in a camera. It takes less computational time and provides easiness. This method also has several disadvantages such as the algorithm does not work with low quality images and illumination change can damage the system performance.

W. Bao [8] proposed a method by analyzing the optical flow field. In this method, the region to be tested is a two dimensional plane, and a reference field is obtained from the actual optical flow field data. In order to distinguish a three dimensional and two dimensional images it uses the degree of differences between the two fields. This method showed a better performance in detecting the spoofed samples. But it has the drawback that illumination change can have a great impact and this method will work only for the face image on a plane. Also it won't work with the three dimensional face model or bended or folded face images.

K. Kollreider [9] proposed a technique for evaluating the liveness in the short facial image sequences. This method also uses the Optical Flow Lines and detect the spoof samples based on the structure tensor. This method uses Gabor decomposition and SVM classifier to detect the facial images. These helps to extract the features powerfully. The combination of optical flow estimation and face part detection determines the score called liveness score and by analyzing this score and the unique trajectory of the facial parts discriminate the samples against the spoofed ones. The major drawback of the method is that the computational time for performing this algorithm is much higher.

M. Chakka [10] proposed a method as an extension to the method specified in [8]. Here a photo attack dataset that contains a diverse set of spoofing attacks under diverse conditions are considered. With the help of this dataset, the spoofing detection is carried out for the motion analysis. It considers foreground or background motion correlation using optical flow and direction oriented features on the target images.

The direction θ of motion for every pixel in the input image is computed by using the horizontal and vertical orientations according to a simple Cartesian to polar coordinate transformation by discarding the magnitude components. Histograms are then created for the face and background regions and chi square distance between the angle histograms of the regions are computed. There exists a windowing unit in the system that has the capability to average the chi square distance over a window size of N frames. The average scores calculated from the windowing unit are fed to the binary classifier and detects whether the input image is a spoofed sample or not.

In this research work researchers found difficult in identifying the spoofed samples which has poor lighting, non stationary backgrounds, and also combination of both magnitude and direction could also not be identified.

The texture of the facial images using multi scale local binary patterns (LBP) were analysed by J. Maatta, A. Hadid [11] to detect the spoofed samples. At first the input image is cropped and normalized into a 64 x 64 pixel image, that is, texture of the input image is analysed. Local Binary Pattern operator is applied on the normalized image and the resulting image is divided into 3x3 overlapping regions. Histograms corresponding to the images are considered and concatenated to form the feature histogram. Finally the results are fed in to a Support Vector Machine, a binary classifier. It determines whether the input image corresponds to a live face or spoofed face.

The proposed technique is robust, fast and it does not require any user cooperation. It focus on the texture features for the detection. This method failed to detect the spoofing attacks using masks or 3D models of the face because skin has a very particular texture.

ISSN: 2278 – 7798

Most of the face liveness detection algorithms require user cooperation for adopting the behavioral features. Z. Zhang [12] proposed a system of multispectral face liveness detection method which does not require the user cooperation. In this method, the multispectral properties of the human skin versus non skin are analyzed by using Lambertian model. After that two discriminative wavelengths are extracted. Zhang also used trained SVM classifier for identifying the genuine and fake images. The advantages of this proposed method is that it makes the liveness detection more user friendly and fast. Also it considers the user system distance factor which results into better performance. But this method faces major drawbacks as it does not adopt time consuming and user unfriendly interactions. Also it does not detect the mask faces and thereby the accuracy of the algorithm is reduced.

G. Pan [13], [14] established a method for the liveness detection especially for the eye blink sequences. In this method spontaneous eye blink is detected and modelled as the inference in a Conditional Random Field (CRF) [19] framework which contains variable nodes and factor nodes. For the computational efficiency and accuracy a discriminative measure known as the eye closity is derived and it is enclosed in to the contextual model. The major advantages of this method is that it does not require extra hardware other than a webcam, it is a non intrusion method and Pan proved that it has high performance in detecting the spoofed facial images. But on the other side it holds various disadvantages such as the spoofing detection is highly affected by strong glasses reflection that can cover the eyes partially or fully, also this algorithm does not works for the video spoofing.

Two dimensional facial spoofing attack detection were studied by R. Tronci [15] as a combination of both static and dynamic (video) analysis of the scenes. The static analysis considers to work upon the photo attack and the noise introduced during those attacks. In the case of dynamic analysis, it examine the human facial physiological characteristics this method can easily identify the features about the motion, texture and the liveness of the input scenes.

In this proposed method, each image is represented with feature spaces by using JPEG histogram, texture histogram and many others so that the dynamic features are extracted accurately. After obtaining the features a classifier is trained so that for each frame of a video, a score is obtained. By comparing these scores with the threshold values the method easily detects whether the input sample is a spoofed sample or actual sample. Here for N frames it has N scores and N number of visual features are being used.

This method proves to have better performance but it also faces various disadvantages such as detection of the photo within the context of automatic face verification system is difficult. It is a time consuming process and could not be applied on three dimensional attacks for face spoofing.

W. R. Schwartz [16] proposed an anti spoofing method to discriminate the valid and non valid videos by considering both spatial and temporal informations with the help of Partial Least Squares regression method. Firstly, a video containing N frames are divided into m parts such that the feature extraction process is done at every i^{th} frame. Descriptors are extracted from each frame and are concatenated to form the resultant feature vector. This methods uses various databases and the sample videos are being trained and tested. In the training stage, the face regions are analyzed from the videos. The color frequency, histogram of oriented gradients, and histograms of shearlet coefficients of the image are integrated to yield better performance. Upon this integrated component, Partial Least Squares Regression method is carried out and thereby, the samples are being tested and the spoofed ones are detected. The major drawback of this method is that it does not focus on the specific features of a face image like eyes, lips etc. an overall face image is considered from a video and it is being processed.

A. da Silva Pinto [17] proposed a method in detecting the video based spoofing attacks based on the visual dynamics. In this method a training set consist of valid videos and spoofed videos. Firstly noise signatures of every videos are extracted and then the Fourier Spectrum on logarithmic scale is computed for each and every frame. In the next stage the visual rhythms for each video is created and training is provided to the classifier by using pixel intensities or gray level occurrence matrices. In the testing phase a visual dynamic for a given video under examination is taken out and discriminated whether it is a valid access or spoofed access. This method has a disadvantage that it cannot extract the unique features that are included in the facial images.

Norman Poh [18] proposed a method that has the capability to extract the unique features which can discriminate the valid video and spoofed videos from print attacks, replay attacks and presentation attacks that contains the authenticated face. A newly developed algorithm called Dynamic Mode Decomposition is used that focus on the data driven approach to extract the features. In this method not only DMD but also a combination of Linear Binary Patterns and Support Vector Machine is considered with the histogram intersection kernel for identification purpose. It can effectively detect the eye blinks, lips movement, and the facial dynamics.

In this method firstly, 1-N video frames are developed from a single video. On to these video frames Dynamic Mode Decomposition Algorithm is applied and it results into 1 to (N - 1) Dynamic Modes. Eigen values for each frames are computed. Among these modes, a mode with phase angle zero or closest to zero is selected as the first dynamic mode. LBP histogram is constructed for the mode and finally with the help of SVM classifier it identifies whether the input video is a valid one or spoofed one.

DMD has the ability to capture the changes, fluctuations in the intensities and variations in the videos, that is., DMD can reduce the background information captures the changes, fluctuations in intensities, and small variations obtained by suppressing the stable information present within the videos. Hence, in this case, DMD is able to suppress the background information and noises. It not only captures the movement characteristics in a face but also the facial textures of a person in a video frame. This proposed method provides better accuracy, high performance, less time consuming and highly efficient and effective in detecting the spoofed samples. It can capture both planar and moiring effects. At the same time it can acquire both liveness cues and attack specific artefacts.

ISSN: 2278 – 7798

III. DETECTION OF FACE SPOOFING USING VISUAL DYNAMICS

The use of Dynamic Mode Decomposition (DMD) with a combination of Dynamic Mode Decomposition, Local Binary Patterns and Support Vector Machine is used for the effective spoofing detection. This provides an efficient way of identifying the spoofed samples. The novel framework consists of mainly three stages

- Dynamic Mode Decomposition
- Construction of the LBP Histogram
- Classification using SVM classifier

At first, the input video is converted into (1 - N) video frames. Upon these video frames the DMD algorithm is applied.

A. *Dynamic Mode Decomposition*

The Dynamic Mode Decomposition (DMD) algorithm is applied on a set of frames that is constructed from an input video frame. Eigen values are computed for the frames and the thereby dynamic modes are thus created. Among them a single dynamic mode image is selected whose phase angle is equal to 0 or closest to it.

B. *Construction of the LBP Histogram*

The Local Binary Patterns helps in representing the image texture in a more powerful way. The histogram corresponding to the dynamic mode whose phase angle equal to 0 or closest to it is constructed. This is done by dividing the selected dynamic mode image into different blocks. Histograms are constructed for each. By considering all the histograms and concatenating the features, a feature histogram corresponding to the dynamic mode is created.

C. *Classification using SVM Classifier.*

The SVM classifier which is a binary classifier helps in discriminating the valid videos and spoofed videos. The classification is based on the threshold value set in the system. The distance of the test sample from the SVM decision hyper plane is computed and if the resultant value is positive then it is a valid video. In case if the resultant value is negative then the sample will be a spoofed one. Fig. 1 shows the spoofing detection using Dynamic Mode Decomposition.

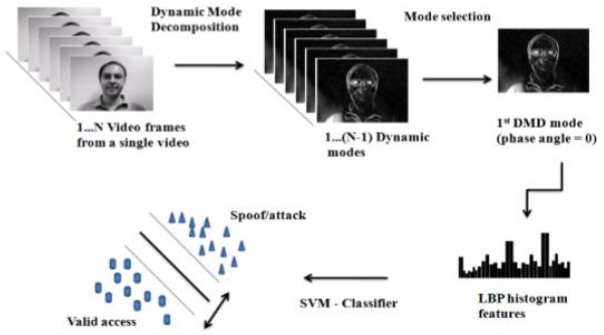

Fig. 1 Spoofing detection using Dynamic Mode Decomposition

IV. CONCLUSION

In this paper various spoofing detection methods were analyzed and among them Norman Poh's [17] method which combines the Dynamic Mode Decomposition, Linear Binary Patterns and Support Vector Machine performs well for identifying the spoofed videos and valid videos. It has the capability to simultaneously extract the liveness characteristics and attack specific artefacts. The DMD helps in extracting the unique features of the facial expressions in the video frames and easily discriminates the valid video from the spoofed video. It has an advantage of providing better security, efficiency, performance and accuracy. As a future work, voice recognition system and the typing behavior characteristics of individuals can also be taken into consideration for providing a better security and authentication thereby the spoofed and valid speaker recognition can be examined.

ACKNOWLEDGMENT

I am thankful to my project guide and Head of the Department Ms. Mary Linda P.A for her support, remarks, and suggestions for providing all the important facilities like Internet access and important books, which were essential to carry out the survey. I am also grateful to all the staff members of the Department of Information Technology and Computer Science & Engineering of KMCT College of Engineering and Technology, Calicut for their assistance in improving the survey paper significantly.

REFERENCES

[1] Biometrics: A Tool For Information Security Anil K. Jain, Fellow, Ieee, Arun Ross, Member, Ieee, And Sharath Pankanti, Ieee Transactions On Information Forensics And Security, Vol. 1, June 2006

[2] P. J. Schmid, K. E. Meyer, and O. Pust, "Dynamic mode decomposition and proper orthogonal decomposition of flow in a lid driven cylindrical cavity," in 8th International Symposium on Particle Image Velocimetry, pp. 25–28, 2009.

[3] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti spoofing," in Biometrics Special Interest Group (BIOSIG), IEEE 2012

[4] N. Cristianini and J. Shawe Taylor, An introduction to support vector machines and other kernel based learning methods. Cambridge university press, 2000

[5] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," in Computer Vision–ECCV 2010, pp. 504–517, Springer, 2010.

[6] B. Peixoto, C. Michelassi, and A. Rocha, "Face liveness detection under bad illumination conditions," in Image Processing (ICIP), 2011 18th IEEE International Conference on, pp. 3557–3560, IEEE, 2011.

[7] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of fourier spectra," in Defense and Security, pp. 296–303, International Society for Optics and Photonics, 2004.

[8] W. Bao, H. Li, N. Li, and W. Jiang, "A liveness detection method for face recognition based on optical flow field," in 2009 International Conference on Image Analysis and Signal Processing. IEEE, 2009

[9] K. Kollreider, H. Fronthaler, and J. Bigun, "Evaluating liveness by face images and the structure tensor," in Automatic Identification Advanced Technologies, Fourth IEEE Workshop on, IEEE, 2005.

[10] A. Anjos, M. M. Chakka, and S. Marcel, "Motion based countermeasures to photo attacks in face recognition," IET Biometrics, vol. 3, no. 3, pp. 147–158, 2013

[11] J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using micro texture analysis," in Biometrics (IJCB), 2011 International Joint Conference on, pp. 1–7, IEEE, 2011.

ISSN: 2278 – 7798

[12] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li. Face liveness detection by learning multispectral reflectance distributions. In International Conference on Face and Gesture, pages 436–441, 2011.
[13] G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink based anti spoofing in face recognition from a generic webcamera," in Computer Vision, 2007. ICCV 2007. IEEE 11th International Conference on, IEEE, 2007.
[14] G. Pan, Z. Wu, and L. Sun, "Liveness detection for face recognition," Recent advances in face recognition, pp. 109–124, 2008
[15] R. Tronci, D. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia, M. Ristori, and F. Roli, "Fusion of multiple clues for photo attack detection in face recognition systems," in Biometrics (IJCB), 2011 International Joint Conference on, IEEE, 2011
[16] W. R. Schwartz, A. Rocha, and H. Pedrini, "Face spoofing detection through partial least squares and low level descriptors," in Biometrics (IJCB), 2011 International Joint Conference on, pp. 1–8, IEEE, 2011.
[17] A. da Silva Pinto, H. Pedrini, W. Schwartz, and A. Rocha, "Video based face spoofing detection through visual rhythm analysis," pp. 221–228, IEEE, 2012.
[18] Detection of Face Spoofing Using Visual Dynamics Santosh Tirunagari, Norman Poh, David Windridge, Aamo Iorliam, Nik Suki, and Anthony T.S. Ho.,IEEE 2015
[19] K.Zuiderveld,"Contrast limited adaptive histograph equalization.," Graphic Gems IV, pp. 474–485, 1994.

Shyama V S is pursuing her M.Tech degree in Computer Science and Engineering from KMCT College of Engineering, Calicut University. She obtained her B.Tech Degree in Computer Science and Engineering from Calicut University Institute of Engineering And Technology, in 2014.

Mary Linda P.A. is Assistant Professor, Department of Computer Science and Engineering, KMCT College of Engineering, Calicut University. Her research focuses on Image processing, Internet security. She obtained her B.Tech degree in Information Technology from KMCT College of Engineering in 2007. She completed her M.Tech degree in Image processing from Model Engineering College, CUSAT in 2012.

ISSN: 2278 – 7798