Detection of Face Spoofing Activities in Face Recognition and Verification System

D. Gowthami #1, T. Venipriya #2

1M.E student, Department of Computer Science, Arasu Engineering College, Kumbakonam,
2 Assistant Professor, Department of Computer Science, Arasu Engineering College, Kumbakonam.
1 gowthamidharmarajan@gmail.com
2 venipri@gmail.com

***Abstract*— Face Recognition and Verification system is the alternative and recently emerging method in biometric technique in order to provide high level security to the system or the organization. Spoofing is the act of masquerading as a valid user by falsifying data to gain an illegitimate access. Printed photo, mimic mask, video replay are some of the commonly used methods for spoofing. In this paper, we propose a real time ant spoofing measure in order to detect the liveness of the face. The proposed feature is developed using the spherical harmonic representation of the face texture-mapped onto a sphere. The texture map itself is generated by back-projecting the multi-view video data. Video plays an important role in this scenario. It provides an automatic and efficient way for feature extraction. The Viola Jones algorithm and Kanade-Lucas-Tomasi algorithm are used for face spoofing detection by measuring the difference between the live and fake faces. The proposed anti-spoofing measure provides efficient security to the biometric systems. The Experimental results on various datasets like NUAA, Replay attack and Morpho show that the proposed method is effective for face spoofing detection when compared with previous approaches.**

***Keywords*— Spoofing, masquerading, Viola Jones algorithm, Kanade-Lucas-Tomasi algorithm, anti-spoofing measures.**

I. INTRODUCTION

The mobile devices are provided with high level security using some biometric techniques such as Iris, Finger print, signature, hand gestures etc,. [1],[2]. The Iris and Finger print verification system is most commonly used biometric technique in order to provide security to the system. Vulnerability of face recognition and verification system to spoofing attacks is still an open security issue in biometrics domain. Even though they provide high level security, they need require close interaction with the user which is inconvenient to the user. The Face Recognition and Verification system is the alternative measure to these biometric techniques where our face is given as input. This is most popular method which is vulnerable to diverse spoofing attacks. Various spoofing activities using printed photo, mimic mask, screen shots, video replay attacks are shown in figure 1, in order to gain the access illegally. The attacker will also capture the video sequence such as eye blinking, head shake etc., and replay it in order to penetrate the security system. The input images and videos are analyzed for its texture, quality, pixel intensity, illumination and reflection characteristics to find spoofing attacks. Several researchers have addressed this problem based on three approaches namely motion, spectrum and image quality information.

First motion based approach, in which face motions are detected such as eye blinking [3],[4], and lip movement[5] and head rotation. Specifically in [3] the eye blinking is detected based on the undirected conditional graphical framework, in which a discriminative measure of eye state is incorporated. In [5], the optical flow line of the mouth region is detected to find the lip movement. They use velocity vector onto their intuitive stick-mouth model and extracted the statistics of the lip movement for face liveness detection.

Second the spectrum-based methods clearly explain the difference between the face and live face in spoofing attacks. In [6], the reflectance disparities between the live and fake faces are revealed based on the computed radiance under different illuminations, and these estimated values are then applied to Fisher linear discriminate. In[7] the albedo curves of different materials, i.e., skin and non skin are measured. This approach lead to correct face spoofing detection but requires some additional devices like near infrared sensor, which are not easily deployed in mobile systems.

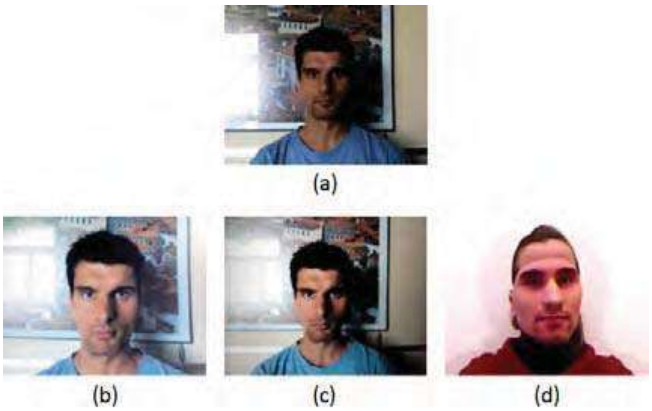

Fig. 1. A genuine face image (a) of a subject and three spoofs of the same subject using a (b) printed photo, (c) displayed photo (on a tablet screen), and (d) 3D face mask.

Third image quality-based approaches are used to detect some quality features from live face and fake face and compare them to find the spoofing attacks. The fake face does not have more quality features like the live face. In [8] the Fourier transform is used to identify the spoofing attacks by observing the lose details in fake faces. In [9] Multiple DoG filters is applied to extract the features to determine the liveness of the face. In [10] the DoG filter along with texture based analysis is used to detect the face liveness. Spoofing using mimic mask is detected using various approaches. In [11] 3D data acquired with a low-cost sensor is used to localize face and verify spoofing attacks. In [12] the planner surface for a fake face is rendered futile in case of 3D facial mask attacks. In [13], the authors conduct experiments on different mask materials like

silicon, latex or skin-jell to observe the reflectance difference when compared to facial skin from the fore head region. In [14] the albedo curves of facial skin and mask materials are examined with two discriminative wavelengths (850 and 1450 nm).

In existing techniques, Single-View based object recognition is inherently affected by information loss that occurs during image formation. Although there exists many works addressing this problem, pose variation remains as one of the major nuisance factors for face recognition. In particular, self-occlusion of facial features, as the pose varies, raises fundamental challenges to designing robust face recognition algorithms. A promising approach to handle pose variations and its inherent challenges is the use of multi-view data. In recent years, multi-camera networks have become increasingly common for biometric and surveillance systems. Having multiple viewpoints alleviates the drawbacks of a single viewpoint since the system has more information at its disposal. In the context of face recognition, having multiple views increases the chances of the person being in a favorable frontal pose.

To overcome the above discussed problem, we propose a novel method to detect the face spoofing activities using photo and mask from a single image. However, to reliably and efficiently exploit the multi-view video data, often need to estimate the pose of the person's head. While there are many methods for multiview pose estimation.The key idea of this method is to find the difference between live and fake face by analysing the surface properties of the image. The (VJ) viola-jones algorithm is used extract selected features from the original face image. This extracted features are mapped into a spherical harmonic structure and saved in the system. This spherical harmonic representation is compared with spherical harmonic representation of the input image at each time, using Kanade Lucas Tomasi (KLT) algorithm.When compared to previous approaches, the proposed method is more effective and performs well regardless of the image medium and under varying illuminations. This increases the robustness of face recognition and verification system in a wide environment. The experimental results using various datasets like NUAA, Replay attack and morpho shows reliable performance of face spoofing detection.

II. FACE SPOOFING DETECTION

A. *Motivation*

In proposed method, multiple images of the face in different poses can be obtained in at a time. Invariably these images could include a mix of frontal, non-frontal images of the face or in some cases, a mix of non-frontal images. This makes registration of the faces extremely important. Registration can be done once. It is decided to impose a three dimensional model onto the face. However, registration to a three dimensional model (essentially, aligning eyes to eyes, nose to nose, etc.) is very hard and computationally intensive for low-resolution imagery. Toward this end, it is chosen to use a spherical model of the face and a feature that is insensitive to pose variations. This proposed work proposes a robust feature for multi-view recognition that is insensitive to pose variations. A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database where web camera is used to capture the human face. Input given through web camera can be a live image of person or it can be a video. Then the face detection process is carried over the captured image. Features of the image extracted are compared with the features of the image already stored in the database. Then develops a new statistical

model that can be used to recover the three dimensional face shape from a single image taken under arbitrary lighting conditions. The proposed statistical model combines shape and image intensity information. The latter is represented by a spherical harmonics (SH) space. Given a training data set of aligned height maps of faces and their corresponding albedos, The input image is projected into the space spanned by the SH basis images of each member in the data set. The combined statistical model is obtained by performing the principle component analysis on both the SH projections and the height maps. Finally, the face is reconstructed by fitting the model to the input intensity image. In addition to the shape recovery, the proposed model can be used to recover the face albedo and to estimate the light direction. The Viola-Jones algorithm is used for converting image into spherical harmonic structure. The KLT algorithm is used to analyze the features of image and based on the analysis the input image will be identified as a live or a spoof image. The KLT algorithm is used to find spoofing attacks in face recognition and verification system. Thus, spoofing activities are detected and the access of spoof user is denied.

B. Viola-Jones Algorithm

The Viola–Jones object detection framework is the first object detection framework to provide competitive object detection rates in real-time. Although it can be trained to detect a variety of object classes, it was motivated primarily by the problem of face detection. This algorithm is implemented in OpenCV as *cvHaarDetectObjects()*. The problem to be solved is detection of faces in an image. A human can do this easily, but a computer needs precise instructions and constraints. To make the task more manageable, Viola–Jones requires full view frontal upright faces. Thus in order to be detected, the entire face must point towards the camera and should not be tilted to either side. While it seems these constraints could diminish the algorithm's utility somewhat, because the detection step is most often followed by a recognition step, in practice these limits on pose are quite acceptable. The algorithm has four stages:Haar Feature Selection, Creating an Integral Image, Adaboost Training and Cascading Classifiers.

C. Kanade-Lucas-Tomasi Algorithm

The Kanade–Lucas–Tomasi (KLT) feature tracker is an approach to feature comparision. It is proposed mainly for the purpose of dealing with the problem that traditional image registration techniques are generally costly. KLT makes use of spatial intensity information to direct the search for the position that yields the best match. It is faster than traditional techniques for examining far fewer potential matches between the images. Here it is used to compare the spherical harmonic representation of input image and image already stored in the database.

III. EXPERIMENTAL RESULTS

Here three bench marking datasets are used namely NUAA, Replay Attack and Morpho datasets. NUAA is most widely used in this field. The Replay attack dataset is composed of photo and video under different lighting conditions used in attack attempt against 50 clients. The Morpho is not a public dataset which consists of mimic mask for set of users.

A. Datasets

1) ***NUAA:*** This dataset is widely adopted in this field for evaluating face liveness in order to spoofing attacks. It consists of images of 15 subjects who were asked to frontally look at the webcam with neutral expression. None of the faces contains any apparent movement, such as eye blink or head movement. To create fake examples, the authors captured the pictures using usual cannon camera and printed them on a A4 paper respectively. These faces are detected using Viola-Jones detector and geometrically normalized based on the eye localizer. Finally, these images are resized to 64 x 64 pixels with gray scale representation.
2) ***Replay-Attack:*** This dataset consists of 1,300 video clips and photo images under various lighting conditions are used for spoofing attacks against 50 clients. Used to identify the spoofing medium such as printed paper, smart phone or high resolution screen (Tablet). Therefore the dataset is decomposed into three subsets, as for training, development, and testing. It is mostly applied to video based spoofing attacks.
3) ***Morpho Database:*** This is a non-public database which consists of 207 real access and 199 mask attack images in both 2D and 3D, i.e., facial images and 3D face models. It consists of masks of 16 clients that are used for spoofing attacks, created using 3D printer. The texture of the mask is in gray scale and the shapes are accurate as live faces. A 3D scanner uses a structural light technology to capture many different shots for each user. In each shot, three manually annotated points (two for outer eye corners and one for the nose tip) are included in the database.

B. Proposed methodology

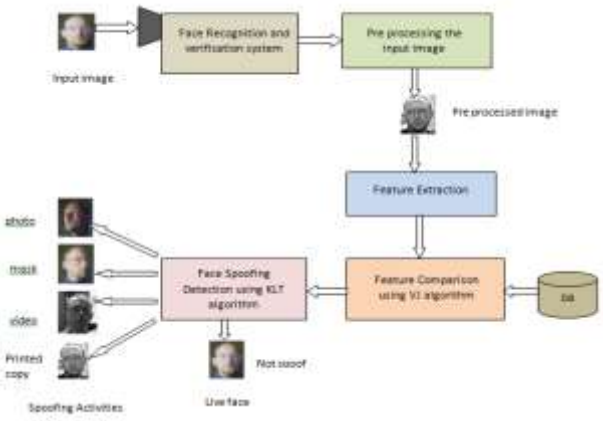

Fig. 2. The proposed system model.

In the Proposed methodology (Fig . 2), the input face image is given to the face recognition and verification system . the image is checked for spoofing attacks such as photo, video, mimic mask , etc.

1. *Preprocessing the image.*

Input to this module is a live face or a spoof one which involves printed photo, mimic mask, videos. The input image is involved with some preprocessing activities like noise removal, quality improvement feature extraction, etc. The given image is converted into gray scale image and then histogram for that image is generated. Dimensions of the face in various poses are noted and stored in the database. Input image is done these preprocessing activities and compared with the image that already exists in the database. Histogram for the input image is generated and the basic features are analyzed.

2. *Face Detection*

Input to this module is preprocessed image. In this module facial components such as eyes, nose and mouth are detected in order to recognize the face. A square box is used to indicate the detected area of the box. The size of the window varies on different faces as different scales. However, the ratio of the window remains unchanged. The face of the user is detected correctly even in varying the pose and quality. Here the face is detected even in different illumination conditions.

Fig. 3. Face is detected from input image

3. *Feature extraction*

In this module, the features such as surface, texture, shape, color, pose and dimension are extracted using Viola-Jones algorithm. The value of RGB image, gray scale images and Illumination & reflection properties of the image are noted. The extracted features are then mapped to a spherical harmonic structure here. Each and every time the input image is converted into a spherical harmonic structure and stored. This spherical harmonic structure is unique for each faces

.

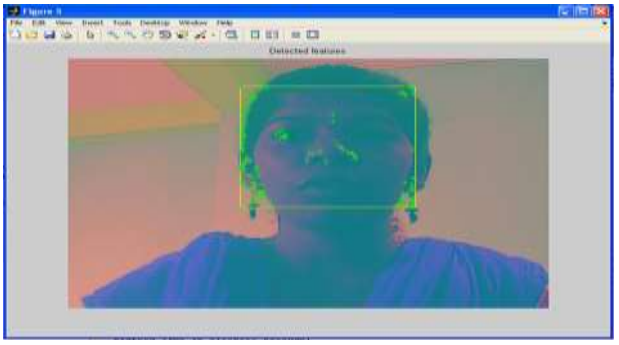

Fig. 4. Features extracted from face image

4. *Face Spoofing Detection*

Finally the spherical harmonic representation of the input image is compared with the spherical harmonic image already stored in the database using KLT algorithm. The difference between these two representations are analyzed and identified. If the images are similar and the features are matched then the image is determined as live face and the user is allowed to access the system. If the features are not matched, then the image is said to be spoofing activities such as photo, mask or video. Hence the spoofing activities are intimated to the admin and the user and the access is denied to the spoofed user.

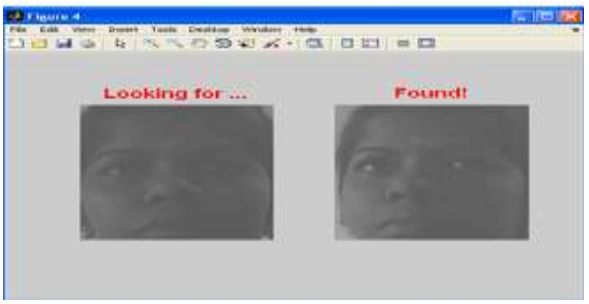

Fig. 5. Face found

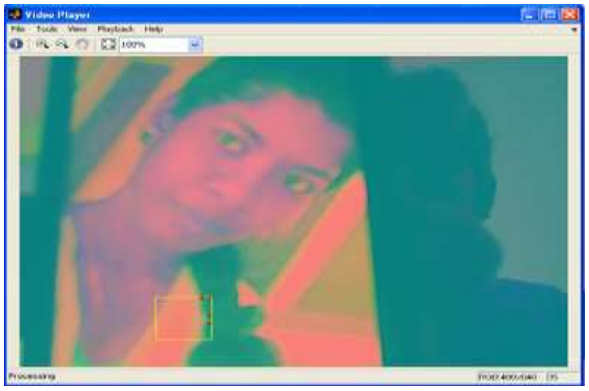

Fig. 6. Spoofing attacks using mobile

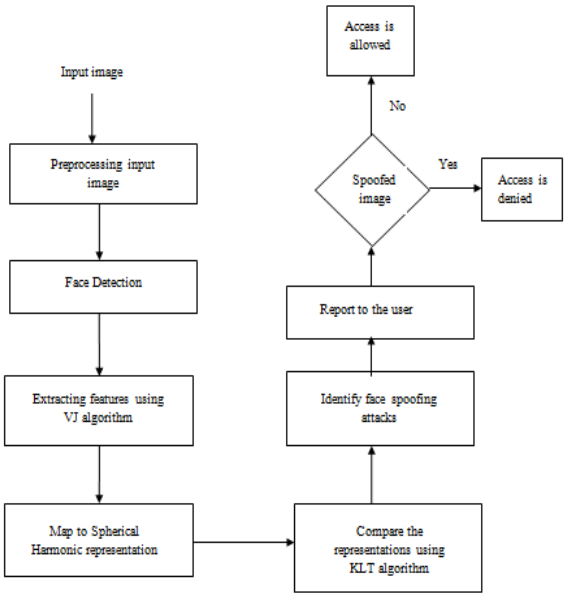

Fig. 7. Over all Block Diagram

C. *Performance Evaluation in NUAA Dataset*

The experiment is conducted with various time step values and iteration numbers. The image block of size 32 × 32 pixels is taken for implementation and the dimension of the feature vector is 59 × 9 = 531. These features are given as the input to the SVM classifier for training and testing. C is fixed as 100 for SVM in order to show good results on validating the proposed method of training set.

Table.1 Performance of NUAA compared with various approaches

Methods	DoG-F	DoG-M	DoG-S	DoG-L
Accuracy	84.5%	81.8%	87.5%	94.5%
Methods	MLBP	CP	Baseline	LSB-based
Accuracy	92.7%	97.7%	90.4%	98.5%

D. *Performance Evaluation in Replay Attack Dataset*

The Performance evaluation of Replay Attack Dataset is discussed in this subsection. This is mainly designed for diverse spoofing attacks and provides samples for both training and testing. The performance of evaluation of Replay-Attack Dataset is compared with various approaches such as Half total error rate (HTER), which is half of the sum of the false rejection rate (FRR) and false acceptance rate (FAR).

The threshold value for HTER is determined by computing the equal error rate (EER), which is defined in ROC curve where FAR values equal the FRR value. Hence the HTER Valus of the development and test is set as 13.72% and 12.50% respectively. The comparison of performance of Replay Attack dataset in various attacks is shown in Table .2.

Table.2 . Performance of Replay Attack dataset with various attacks.

Types	Print attack	Phone attack	Tablet attack	Total
Fixed-support	1.79%	0.63%	17.52%	12.88%
Hand-held	5.84%	2.18%	12.09%	13.97%

E. *Performance Evaluation with Morpho Dataset*

Face recognition and verification system consists of masked images of users in order to attack the security systems. The results of this morpho dataset are compared with LBP-2D, LBP-2.5 and TPS-3D algorithms. They are tested using various protocols in order establish the baseline system. The 2D mask attacks and 3D mask attacks are determined using two algorithms namely VJ and KLT approaches. The Performance of this technique to live and fake faces is shown in Figure .8.

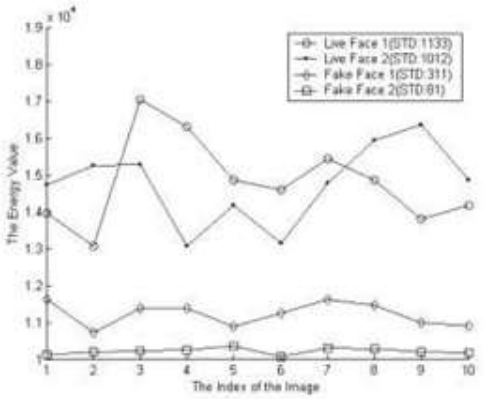

Fig . 8. The comparison results of live and fake faces.

IV.CONCLUSION

An effective and robust approach to detect the face spoofing activities is proposed in this project. Here we proposed an efficient approach for anti spoofing measure in order to reveal the difference between the live and fake faces. It is used to identify the spoofing attacks using printed photo, mimic mask or video clippings. The difference in the features extracted using VJ algorithm. The spoofing attacks are detected efficiently using KLT algorithm. Therefore it is concluded that, the proposed method will detect the spoofing attacks efficiently and can be used as an alternative method for biometric systems like, iris, fingerprint, etc.

To improve the rate of face detection, we need to combine face detection and skin tone mapping together to make better classifiers. Viola-Johns algorithm will only ensure we have the object with the correct shading, but it does not necessarily be human. Therefore to improve the result, a human skin classifier is necessary. Right now we are only using corner detection from the area that we are interested in. This is not entirely accurate due to different lighting conditions and different scales of the faces. In future, the database samples with various skin tones can be used for effective spoofing detection.

ACKNOWLEDGMENT

The research in this paper is used in Idiap Research Institude, Martigny, Switzerland. Various researches based on this face biometrics are proposed in order to provide security systems and also applied n mobile devices.

REFERENCES

[1] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, ―Filterbank-based fingerprint matching,‖ IEEE Trans. Image Process., vol. 9, no. 5, pp. 846–859, May 2000.

[2] Y. Wang, J. Hu, and D. Phillips, ―A fingerprint orientation model based on 2D Fourier expansion (FOMFE) and its application to singular-point detection and fingerprint indexing,‖ IEEE Trans. Pattern Anal. Mach Intell., vol. 29, no. 4, pp. 573–585, Apr. 2007.

[3] G. Pan, L. Sun, Z. Wu, and S. Lao, ―Eyeblink-based anti-spoofing in face recognition from a generic webcamera,‖ in Proc. IEEE 11th Int. Conf. Comput. Vis. (ICCV), Oct. 2007, pp. 1–8.

[4] L. Sun, G. Pan, Z. Wu, and S. Lao, ―Blinking-based live face detection using conditional random fields,‖ in Proc. Adv. Biometrics, Oct. 2007, pp. 252–260.

[5] K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun, ―Real-time face detection and motion analysis with application in ―liveness‘ assessment,‖ IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 548–558, Sep. 2007.

[6] W. Bao, H. Li, N. Li, and W. Jiang, ―A liveness detection method for face recognition based on optical flow field,‖ in Proc. IEEE Int. Conf. Image Anal. Signal Process., Apr. 2009, pp. 233–236.

[7] Y. Kim, J. Na, S. Yoon, and J. Yi, ―Masked fake face detection using radiance measurements,‖ J. Opt. Soc. Amer. A, vol. 26, no. 4,pp. 760–766, Apr. 2009.

[8] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, ―Face liveness detection by learning multispectral reflectance distributions,‖ in Proc. IEEE Int. Conf. Autom. Face Gesture Recognit. (FG), Mar. 2011, pp. 436–441.

[9] J. Li, Y. Wang, T. Tan, and A. K. Jain, ―Live face detection based on the analysis of Fourier spectra,‖ Proc. SPIE, Biometric Technol. Human Identificat., pp. 296–303, Aug. 2004.

[10] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, ―A face antispoofing database with diverse attacks,‖ in Proc. IEEE 5th IAPR Int. Conf. Biometrics (ICB), Mar./Apr. 2012, pp. 26–31.

[11] X. Tan, Y. Li, J. Liu, and L. Jiang, ―Face liveness detection from a single image with sparse low rank bilinear discriminative model,‖ in Proc. 11th Eur. Conf. Comput. Vis. (ECCV), 2010, pp.504–517.

[12] B. Peixoto, C. Michelassi, and A. Rocha, ―Face liveness detection under bad illumination conditions,‖ in Proc. 18th IEEE Int. Conf. Image Process. (ICIP), Sep. 2011, pp. 3557– 3560

[13] N. Erdogmus and S. Marcel, ―Spoofing 2dx face recognition systems with 3d masks,‖ in International Conference of Biometrics Special Interest Group, 2013.

[14] Y. Kim, J. Na, S. Yoon, and J. Yi, ―Masked fake face detection using radiance measurements,‖ Journal of the Optical Society of America A, vol. 26, no. 4, pp. 760–766, 2009

[15] Z. Zhang, D. Yi, Z. Lei, and S. Li, ―Face liveness detection by learning multispectral reflectance distributions,‖ in IEEE International Conference on Automatic Face Gesture Recognition and Workshops, March 2011, pp. 436 – 441.

