International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 07, July-2015

3D Facial Recognition Integrated with Human DNA Analysis

Sangamithra. K
M.Tech Applied Electronics& Instrumentation
Department of ECE
Younus College of Engineering& Technology,
Kollam, Kerala

Mr. Safuvan. T
Asst.professor,
Department of ECE
Younus College of Engineering& Technology,
Kollam, Kerala

***Abstract*— Spoofing attack is the act of outwitting a biometric system by presenting fake evidence in order to gain authentication. Recognition system's vulnerability to presentation attacks is still an open security issue in biometrics domain and among all biometric traits, face is exposed to the most serious threat, since it is particularly easy to reproduce and access. A well deserved popularity has been recently gained for the problem of detecting spoofing attacks. With the help of some printed photos or replaying recorded video on mobile devices, used for the forged 2D attacks. Many different types of face spoofing attacks are examined and for detecting them, various algorithms have been proposed. The flatness of the spoofing material in front of the sensor is a significant portion of these studies. This assumption is no longer maintained, due to the advancements in 3D reconstruction and printing technology. This paper aims to inspect the spoofing potential of a subject-specific 3D facial mask for different system along integrated with human DNA analysis. Since every individual has unique DNA structure; hence it increases the accuracy of the system.**

Keywords- Spoofing, Vulnerability, Local Binary Pattern, Linear Discriminant Analysis, Support Vector Machine.

I. INTRODUCTION

Nowadays, with growing populations and their increasing mobility, for identity management, we use biological characteristics for human recognition. For human, face recognition is used as a common biometric trait, and also it become an active research topic, it has found great application. While comparing with any other biometric traits like finger print or iris, face recognition owns it reputation by being easily accessible. But due to this attacker can create copies and spoofing face recognition system easily in some malicious circumstances. Spoofing is an attempt to gain authentication through a biometric system by presenting a counterfeit evidence of a valid user [1]. A numerous papers have been published in countermeasure studies due to this vulnerability of face, which has evoked significant attention in the biometric field. With the available database and reproducible analysis of several methods, we can refer it. The most common types of spoofing methods being focused are printed photos and video attacks, due to their convenience and low cost. Mainly, proposed anti-spoofing approaches against these spoofing attacks, broadly classified into three groups: motion analysis, texture analysis, liveness detection. Also human DNA analysis is very efficient biometrics, which together makes a multi-modal biometric sensor; it will increase the accuracy of the system.

In the first group, the motion of the scene is analyzed by examining the object in front of sensor, whether it is moving or not, by that it expose the spoofing attacks [2]. The movement of the face is differing greatly with the movement of the planar objects like papers or screens. The trajectories of small regions in the face image is analyzed and classified as fake or genuine Also, to detect the attacks, a set of facial points are located automatically and utilized their geometrical invariants. In the second group, here conduct an examination on the texture of the face image to find the spoofing clues like printing artifacts [3] and/or blurring [4]. Micro texture analysis is also applicable alternatively in a recent paper, where it utilized multi-scale local binary patterns (LBP) [5].The third group is to detect the liveness of the face image based on live-face specific gestures such as eye-blinking or lip movements. A substantial portion of these approaches for 2D anti-spoofing are rendered inoperative when 3D face mass are introduced. By an example, it is shown that a liveness detection system relying on eye-blinking and lip movements can be defeated by using photographic masks which are actually high resolution facial prints worn on face, where there will be a cut out in the eyes and mouth region. Similarly, motion based countermeasure that depend on the shape difference between real and fake faces are not able to operate as intended, by using facial masks instead of using photos or screens. By employing additional sensors, affordable consumer depth camera like KINECT which is use to utilize to localize face and test its "fakeness", would become futile. In conclusion it is clear that 3d masks introduce new challenges to face anti-spoofing domain. To our knowledge, very few studies have been published addressing them.

II. RELATED WORKS

The first papers published in mask anti-spoofing can be list by the work of an author named Kim. Mainly it aims to distinguish between the facial skins and mask materials by exploiting the difference between their reflectance characteristics. A set of albedo values for illumination at various wavelengths are analyzed for this purpose to see how they are differently behavior in reflectance, facial skin and mask material. Due to this, it results a 2D feature vector presents a new method capable of accurately distinguishing the consisting of 2 radiance measurements under 850 and 685 nm, Fisher linear discriminant is used for the classification of these selected illumination. By this proposed method, it reported to have 97.78% accuracy in fake face detection. The experiments are done directly on the mask material instead of real mask in that paper, hence it is not included all the spoofing performance. Moreover, for mask detection, exactly

30 cm are required for the measurement to be done and on the region of forehead. This occlusion possibility in forehead together with range limitations makes the method quite impractical.

A multi-spectral analysis is proposed claiming the fake, therefore, it is not possible to detect attacks using only visual fade image, by its definition, is indistinguishable for human eye. By measuring the albedo curves of facial skin and mask materials with varying distance two discriminative waves (850 and 1450 nm) are selected. A SVM classifier is used to train between genuine and fake attempts for discriminate them. There conduct an experiment on a database of 20 masks of different materials: 4 sponges, 4 plastic, 6 silica gel, 4 paper pulp, and 4 plaster. As a result, it achieves 89.18% accuracy by this method. By eliminating the range limitation and experimenting on real facial masks, the authors bring the state of the art one step further, but still no analysis of how well the spoofing attacks work is presented.

Above briefed two papers are handled the mask attack rather than spoofing in an evasion context. In that, they do not examine the impersonated masks that are the replicas of real subjects. We need a 3D scanner and with the use of 3D printing services, the masks were manufactured. Along with the texture images, the database includes range image for both fake samples and real one. By applying an LBP-based method on both color and depth channels and claim 88.12% and 86% accuracy, respectively, this is proposed by the authors. There are two main short comings in this study: Initially, the authors unfortunately do not report on the spoofing performance of the printing masks, which is certify the alleged thread is nearly as important as to counter it. Secondly and more importantly, it poses a barrier to comparative and reproducible research, since the utilized database is not public.

We have three main purposes, in this paper:

- Introducing the first public spoofing database with facial masks, called 3D Mask Attack Database (3DMAD).
- Along presenting with Baseline analysis on its spoofing performance against 2D face recognition.
- The effectiveness of Local Binary Patterns (LBP) based features extracted from color and depth image to detect the mask attacks is studying.

Purpose for reproducibility, both the database and source code to generate the reported results are made freely public availability. The rest of the paper is organized as follows: In Section 3, MORPHO database is briefed. In Section 4, 3DMAD database is described in detail. In Section 5, the studied countermeasure techniques are explained. Experimental results face recognition system and anti-spoofing performances of the LBP-based methods are provided in Section 7. Finally, in Section 8, the paper is concluded with remarks .

III. MORPHO DATABASE

The non-public database which was collected by MORPHO is called Morpho database. With the help of a 3D printer, subject-specific masks used for spoofing attempts are manufactured, with a scanner; it acquires facial models of 16 different users. Their shapes are accurate replicas of the targeted clients and grayscale is the texture of the mask.

With the employed 3D scanner during acquisition process, it is really sensitive to movement. It needs the co-operation of the clients that become a crucial to the mask manufacture for the attackers.

IV. 3D MASK ATTACK DATABASE

With the help of a Microsoft Kinect sensor, the 3D MAD is mainly composed of real access and mask attack video of 17 different subjects which are recorded. Following subsections, the database recording is explained in detail and to evaluate the mask spoofing performance, the baseline 2D recognition is implemented and presented.

A. 3D Mask Manufacturing

According to Zhang, The massive usage of masks does not exist in the literature, to produce client-like masks is too expensive is the main reason. But this becomes popular recently by the introduction of the 3D printing services. It has become very high potential and is expected to continue growing rapidly in market. For alternates, many available options are there, ThatsMyFace.com which specializes in facial; reconstruction and it create 3D sculpture instead of 2D portraiture. It constructed 3D face is displayed for inspection, even after seconds of uploading frontal and profile face images of a person. The customer get satisfied, then it get printed and in several forms such as ahead on an action figure or a wearable life-size mask in hard resin or a paper cut.

The possibility of utilizing facial images to create a 3D model, is the mainly advantage of this service over the others. Here it use a 3D printing services, there used to create the database in require the 3D models to be obtained by the user and for printing purpose, it should be uploaded to their system, still the advancements in 3D scanner technologies are remarkable, it requires user co-operation and all they still have range limitation. Because of this reason, obtaining proper 3D data from a distance or from unaware subject is highly dramatic. But in other words, through social networks or via internet, the photographs of the users can be easily captured from a distance and hence obtained.

We uploaded one frontal and two profile images of 17 different subjects on ThatsMyFace.com, for our database and ordered a life-size useable mask and a paper-cut mask for each. But in this paper, they are not included. In Fig 1, we used 17 wearable masks made up of a hard resin composite in full 24-bit color with holes at the eyes and nostrils are shown. Due to the high cost of the 3D facial masks, the size of the database is limited to 17 subjects. In other hand, we can collected more samples from the same masks, also by using paper-cut files, it can be use extend.

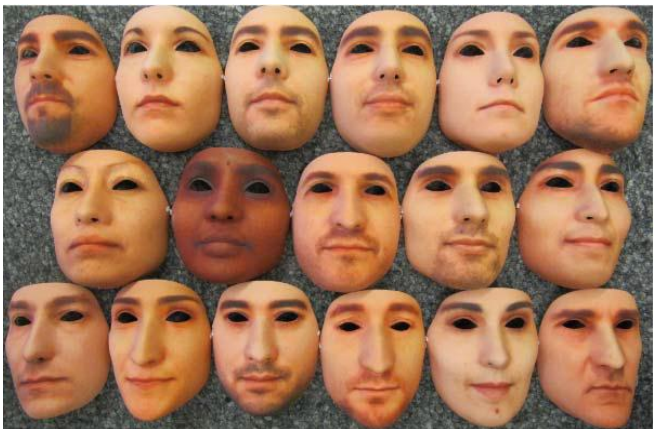

Fig .1. 17 facial masks obtained from ThatsMyFace.com

B. *Recording Settings*

By using Microsoft Kinect for X360, here for the dataset, all recording are done. The sensor provides both RGB (8-bit) and depth data (11 bit) of size 640x480 at 30 frames in every second. Main reason behind this selection is twofold. Primarily, with the available depth images, it possible to explore attacks and 3D information devise countermeasures. Secondary, it would be interesting to explore the vulnerability of 3D face recognition system to mask attacks, this work will use as a future extension. There are three different sessions in the collected videos: Among this, two real access sessions held two weeks apart and a third session in which mask attacks are performed by an attacker. Every each session and for each person, they captured 5 videos of 10 seconds length. Totally, 255 color and depth videos of 300 frames are recorded.

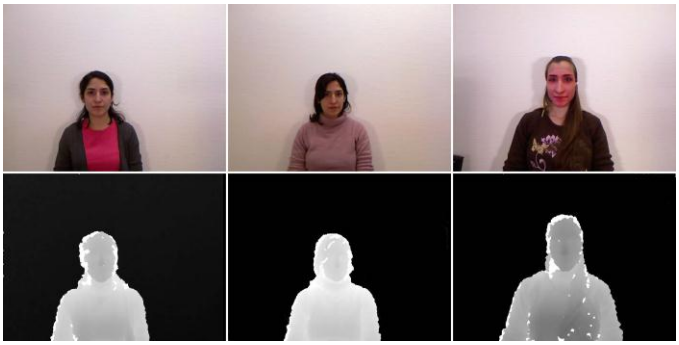

Fig..2. Example color (top row) and depth (bottom row) images from three different sessions for a user in 3DMAD. The first two are real accesses while in the third, an attacker is wearing the user's mask.

In all three sessions, the recording conditions are well controlled: The scene's background is uniform and to minimize the shadows cast on the face, by adjusting the lighting. In Fig 2, three sample frames from three sessions for the same subject can be seen. Along with that, eye positions for each video are included in the database which are annotated manually at every 60th frame and for these are linearly interpolated.

V. BASELINE FACE RECOGNITION ALGORITHMS

Using a 2D face recognition algorithm that is based on Inter Session Variability (ISV) modeling method, we have examined the spoofing performances of a subset of masks in 3DMAD. Because of that fact, the dataset was divided into non-overlapping set for training, development and testing, for evaluate every mask, it was not possible.

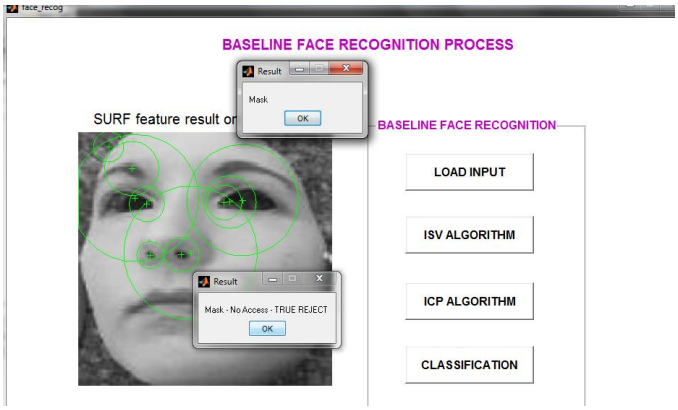

Fig.3. Detect fake mask attempt using Base line face recognition algorithm

A. *ISV method for 2D and 2.5D face recognition*

Inter session variability modeling (ISV) method is implemented as an algorithm of baseline face recognition. Inter session variability is an extension of the Gaussian Mixture Models (GMM) approach which estimates more reliable client models by removing within client variations and explicitly modeling. The identity models are adapted from a Universal background Model (UBM) and built on Discrete Cosine Transform (DCT) block features.

B. *ICP model for 3D face recognition*

Iterative closest point (ICP) algorithm is a well-established techniques used for registration of 3D surface. It is used to establish point-to-point correspondence between two face models. It cannot handle non-rigid transformation which is crucial in the presence of surface deformation, such as occlusion or facial expressions and it needs a good initialization for an accurate result, there are two main shortcoming of ICP. The following results show in Fig 3, mask spoofing is classified, which is done by using an artificial neuron network classifier.

VI. ANTISPOOFING ALGORITHMS

We discussed previously, to detect 3D mask attacks liveness detection and motion analysis methods are bound to fail. One reliable approach which is texture analysis is the solution for the 3D mask detection. Its optical characteristics, such reflectance, scattering etc which differs the human skin from the mask material, and help to discriminate between real access and spoof attacks, possible by using the texture properties.

For both 2D and 3D face spoofing attacks, Local Binary Pattern (LBP) and its variations have been proven to be successful. From this study, we are analyzing the discriminative properties of texture feature extracted from various LBP operators in 'real face' or' 3D mask' classification using the proposed MAD3D database. Each frame of each video is processed separately to extract the LBP

histograms, which is similar to recognition tests. The countermeasure analysis is performed per video. All histograms from each video are computed and classification experiments are done on these average features by this end.

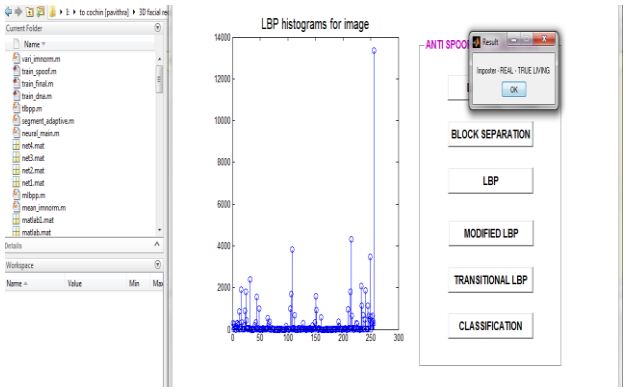

Fig. 4. Detect enrolled face using anti-spoofing algorithm.

A. Feature Extraction by LBP

The basic LBP value for a pixel is computed as a binary number by comparing the intensity of that pixel to the intensities of the adjacent pixels in 3x3 instead of the center pixel. Transitional compares two consecutive neighborhoods (LBP 3x3). The histogram of these 2^8 different labels is then used as a feature vector. An extension called uniform patterns with more than two bitwise transitions.

Along with LBP, three more extensions are evaluated: modified (mLBP), transitional (tLBP), and direction-coded (dLBP). Modified LBP compares the pixel in 3x3 neighborhoods to their average instead of the center pixel. Transitional LBP compares two consecutive neighboring pixels circularly in direction of clock-wise. Direction-coded LBP compare our adjacent pixels only but also includes the direction information in an extra bit. By dividing the face image into blocks, we assess the influence. In each LBP type, the image is broken into 3x3 blocks, and LBP histograms are calculated for each block separately and the final feature vector is concatenated to form. It is reported that, in the block processing methodology. It can improve the performance.

B. Classification

In LBP histograms, the feature vectors are extracted, so firstly $\chi 2$ histogram matching is applied to compare to compare test sample with a reference histogram, by taking the average of all real access samples in the training set which is simply calculated. . The following results show in Fig 4, genuine face is classified using anti-spoofing algorithm. Also, two more complex classifiers are tested, one is linear and other non-linear. In the linear classification, Linear Discriminant Analysis (LDA) is used. Principal Component Analysis (PCA) is applied for dimensionality reduction in which 99$ of the energy is preserved, before computing the scores for the extracted features. In finally, for non-linear classification, support vector machine (SVM) with radial kernel basis function is employed.

After the classification, we can determine whether it is real access or mask attempt. For ensuring the security of the system, we introduce on addition feature called micro array DNA analysis of the user. We already we have a database, which have the sample DNA of the enrolled client. After the face recognition, the DNA is also verified for the system to be got access. The following results show in Fig 5, we got the classification of Human DNA as an unauthenticated one. For that we use a probe, for scribe the skin from the person. Here the main and most important matter is that, the probe only decided where it has to scribe, it will neglect the chance of being duplicating the DNA of the enrolled client.

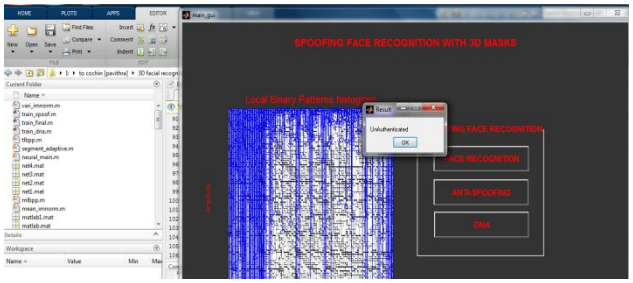

Fig. 5. Detect the unauthenticated DNA sample.

VII. RESULT ANALYSIS

Initially, all the color and depth images are preprocessed. That is it is converted into grey image, the cropped and by using annotated eye position it is normalized to 64X64. Recently lots of works has been done in face recognition. But majority of the works are doing for fining the spoofing with non-public database like MORPHO database.

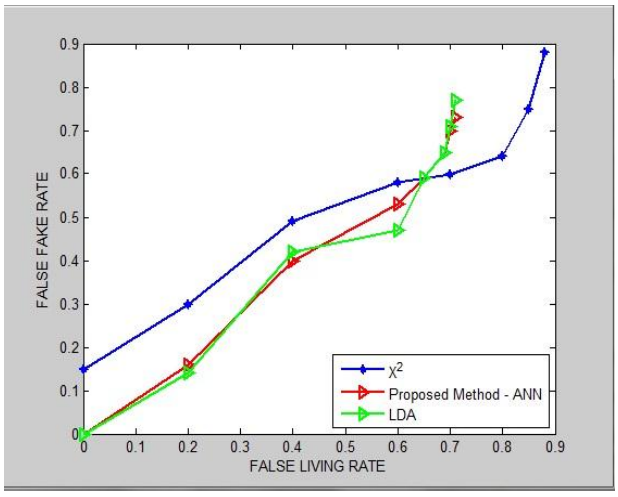

Fig. 6.Graph obtained on classification: false fake rate v/s false living rate.

For the accuracy calculation, Equation 1 is utilized where τ is the decision threshold and *Nr* and *Nm* are number of real access and mask attack attempts.

$$\text{Acc} = \max\tau\,(1 - (\text{FFR}(\tau) \cdot Nm + \text{FLR}(\tau) \cdot Nr) \quad (Nm + Nr)) \qquad (1)$$

Here a new method for recognition of mask spoofing with a public database 3DMAD is proposed. It also includes the base line face algorithm and anti-spoofing algorithm using texture analysis. It gives accuracy result which is integrated with the analysis of the individual. As we know that each individual has the unique DNA, hence it will increase the accuracy of the detection. The following results show in Fig 6, we got the classification, which help to find out the best accuracy of the system while we are doing it in artificial neural network than any other classifier. Also we analysis the DNA of the individual with the Database already had and got the result which is fake or genuine attempt of the person.

VIII. CONCLUSION

With the advancement of 3D printing technology, the manufacturing of 3d mask is quite cheaper and also easy .We aim to contribute to the current state of research in this domain, by providing the public 3d mask database and analysis it by baseline face recognition algorithm. To reduce it vulnerary, also use the anti-spoofing algorithm. In order to increase the accuracy of the system we need DNA analysis, which is integrated to it.

REFERENCES

[1] K. Nixon, V. Aimale, and R. Rowe, "Spoof detection schemes, in *Handbook of Biometrics*, A. Jain, P. Flynn, and A. Ross, Eds. New York, NY, USA: Springer-Verlag, 2008, pp. 403–423.

[2] B. Biggio, Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Security evaluation of biometric authentication systems under real spoofing attacks," *IET Biometrics*, vol. 1, no. 1, pp. 11–24, Mar. 2012.H. Simpson, *Dumb Robots*, 3rd ed., Springfield: UOS Press, 2004, pp.6-9.

[3] J. Bai, T.-T. Ng, X. Gao, and Y.-Q. Shi, "Is physics-based liveness detection truly possible with a single image?" in *Proc. IEEE ISCAS*, May/Jun. 2010, pp. 3425–3428.

[4] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of fourier spectra," *Proc. SPIE*, vol. 5404, pp. 296–303, Aug. 2004.

[5] J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," in *Proc. IEEE IJCB*, Oct. 2011, pp. 1–7.