Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
ISSN NO. 2320-5407
Article DOI: 10.21474/IJAR01/5291
DOI URL: http://dx.doi.org/10.21474/IJAR01/5291

RESEARCH ARTICLE

FACIAL VERIFICATION ALONG WITH SPOOF ATTACKS.

Jherna Devi[1], Sajida Parveen[2], Nadeem Naeem[3] and Nida Husan Abbas[4].

1. Department of Information Technology, Quaid-e-Awam univertersity of Engineering, Science and Technology, Nawabshah, Pakistan.
2. Department of Computer Systems Engineering, Quaid-e-Awam univertersity of Engineering, Science and Technology, Nawabshah, Pakistan.
3. Department of Electronic Engineering, Quaid-e-Awam univertersity of Engineering, Science and Technology, Nawabshah, Pakistan.
4. Department of Computer and Communication Systems Engineering Universiti Putra Malaysia (UPM), Serdang, 43400, Selangor Darul Ehsan, Malaysia.

……………………………………………………………………………………………………....

Manuscript Info

Manuscript History

Received: 28 March 2017
Final Accepted: 30 April 2017
Published: May 2017

Key words:-
Face anti-spoofing; Fake Faces; Database; Texture.

Abstract

Face biometrics assumes an essential part in different authentication applications. Yet, there is a design issues exists to ensure the genuine person along with its originality being alived. For the improvement of such kind of robust framework of face verification along with anit-spoofing, the database should include three kinds of data i.e. Genuine, Fake and Imposter. In this paper, a database is designed to work for face verification and anti-spoofing technique. The Local Binary Pattern is adopted to extract the features and calculate the scores for genuine, fake and imposter attacks. This research would provide a more realistic and challenging platform for facial anti-spoofing and verification research.

……………………………………………………………………………………………………....

Introduction:-

Currently, due to the advancement of electronic gadgets and easy availability of social media, fake facial specimen on different material can easily reproduced and breaches the facial biometric security [1].

To overcome such situation, it is essential to incorporate the anti-spoofing algorithm within face biometric such that the system is able to differentiate between live and spoof face specimen. The appearance of a fake face as a real face is affected by a number of factors, including some life signs such as motions and texture of real skin. To measure the impact of spoofing attacks, face anti-spoofing algorithm need to be trained and tested on a realistic and challenging database that should cover all sort of possible face spoofing attacks for face biometric systems. Also there is need of facial verification database along with its spoof attacks for complete performance evaluation of verification system under the spoof attacks.

In this paper, our previously published and designed UPM face spoof database and UPM verification database is utilized for complete modeling of verification system along with anti-spoof countermeasure.

Corresponding Author:- Jherna Devi[1].
Address:- Department of Information Technology, Quaid-e-Awam univertersity of Engineering, Science and Technology, Nawabshah, Pakistan.

The organization of the rest of the paper is as follows: In this paper, we reviewed the publicly available anti-spoofing databases in section II and identify the necessary data collection gaps. In Section III we present the methodology used in the collection of our own face spoofing database which should addressed several of the previously identified gaps. The need of face anti-spoofing system is examined by using both verification and spoof database in section IV. The conclusion of our work is given in the last section V.

I. Literature review:-

Recently, the most common databases which have been used in a numerous anti-spoofing algorithms are NUAA, CASIA and Reply attack database [2, 3, 4]. These databases consist on images of both real client and fake attacks. The summery of reported database along with the detail of types of attacks and number of participants is presented in table 1.

It is observed that no database has encompassed the variety in texture based specially in still photo attacks. Because in most of the applications, attackers are not bound to use a limited type of photo papers in the attacks. As it can be seen from the literature that current research uses the databases of fake faces with limited variations in texture patterns for face anti spoofing techniques. Therefore, we motivated to collect our own face imposter database in which we have considered significant improvements in both the photograph and digital display devices for our spoof attacks to make it more challenging in non intrusive methods.

TABLE I. PUBLICLY AVAILABLE DATABASES.

Name	Participants	Paper types	Digital display
NUAA	15	2	-
PRINT-ATTACK	50	1	-
CASIA	50	1	1

II. OUR APPROACH:-

1. UPM face Database

This database was collected mainly for face verification with its one-to-one comparison. There is a need of face verification database along with the face spoof database. For collecting the genuine samples of users, the single view camera was used for recording at 50 frame rates per second, with resolution of 1440×1080 pixels. The collected high resolution images were too large for the process of algorithm calculation and memory storage; therefore face images were cropped by frontal view of 345×400 resolution. The maximum quality for printing photographs is retained and will be used in next step for producing spoof attacks. For verification, the sample images were collected with different clothing, eye glasses, hair styles and makeup. The 60 subjects have participated, in which 30 were set as genuine access and 30 for imposter attempt in UPM-FDB. During each session variability is considered in terms of facial expressions, eye blinks and wearing a scarf. There is no restriction for participants to wear same cloths, makeup and hair style as shown in Fig 1.

2. UPM FACE SPOOF DATABASE

This database consists of 30 participants from different races, between the ages of 20 and 50. From all volunteers, the male participants were 18 and 12 female participants. Facial images are the frontal shots with high quality color images of 1440 x 1080 pixels in size. The database took two months to compile the genuine part. The imaging and recording conditions is indoor environment under uncontrolled illumination. The setting of camera parameters and distance is calibrated to ensure that setting should be identical across subjects. The process of collecting spoof database is divided into 3 sessions at two week intervals.

In this database four types of paper material in photo attacks such as common A4, Glossy, Matt, and Laminated and without lamination paper and different digital screens like mobile, laptop and a tablet for different resolution quality attacks are collected. To make collected database more challenging in terms of attacks, the images are captured from different distances. Tilted and bended images were also captured in order to increase the level of difficulty. The details of textures of the fake face introduced in our spoof database are shown in Fig. 2

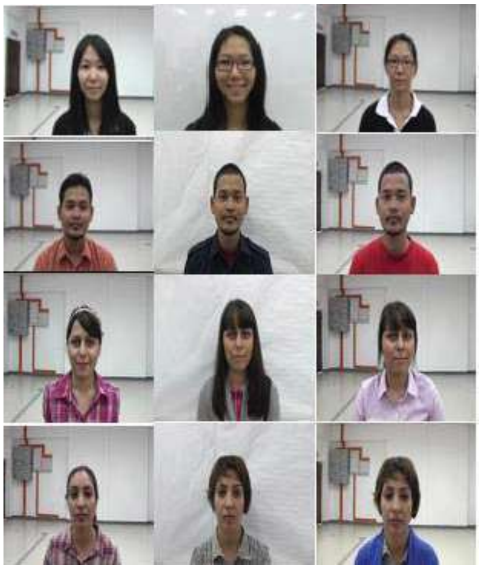

Fig 1:- Samples of UPM Face database

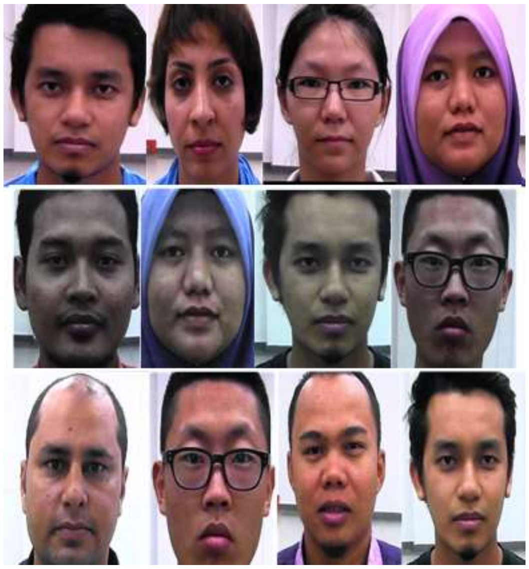

Fig 2:- Samples of UPM spoof database

3. DATA ORGANIZATION:-

There is a total of 2,7000 genuine image samples in proposed database in which we took 900 samples of each participant. The total number of fake sample images from all types of attack is 57450. Our database mainly considers the possible effects of textures in various fake face attacks. In doing so, we can select the images for training set and testing set from both positive (genuine) and negative (fake) images randomly from all three sessions.

4. LOCAL BINARY PATTERN

In local binary pattern (LBP) [5] descriptor each pixel of an image is labeled a decimal number, which encode the small patch size window placed on center pixel. In each patch its neighbors compared the values by its center value. The mathematical expression of LBP is given below:

$$LBP_{P,R} = \sum_{p=0}^{P-1} s(w_p - w_c) \times 2^p \qquad (6)$$

Where w_c, w_p and p are already defined in equation (2), (3) and (4) . And *P, R* is the number of neighbors or samples and radius of the circle respectively.

III. Face Verification Uner Spoofing Attacks

In this paper, the combined database for face verification and anti-spoofing was developed. In this section we find out that how much the face spoof attacks deceives a face verification system without implementing any anti-spoofing countermeasure. Local Binary Pattern (LBP) texture descriptor is adopted to extract the features for this experiment. The verification system obtained the scores by matching the client's images with genuine samples of corresponding client for verification and obtained the score sets for legitimates and imposters, The verification scores are plotted in Fig 3, which shows the three types of samples scores those are genuine user, imposter and spoofing attacks. It is clear from the distribution of the scores that, major part of spoof attacks overlap the genuine score area, which means spoof attacks mostly bear a resemblance to the genuine access. It is examined that face verification system is easily deceived when exposed to face spoof attacks. Approximately 90% of the face spoof attacks of UPM Face Spoof Database (UPM-FSDB) get successful access into the system.

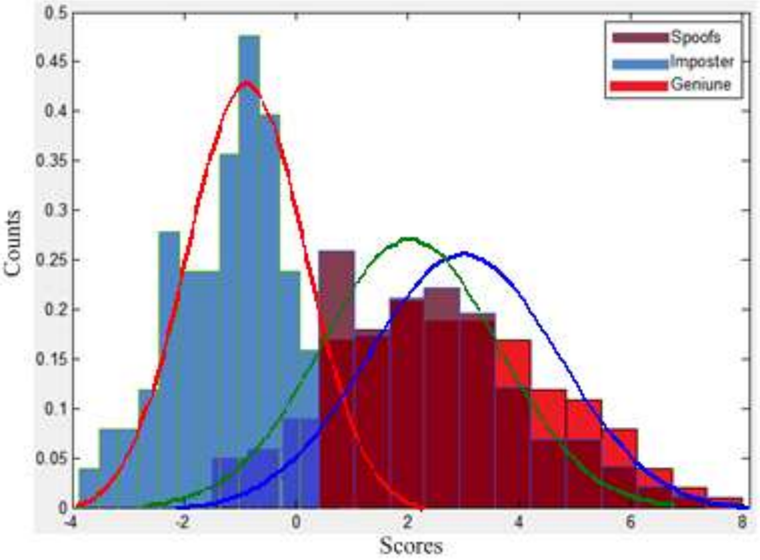

Fig 3:- Score distribution without face anti-spoofing

This is obvious because of overlay of score distribution of spoof over genuine which lead no proper separablity between the spoof and licit in the situation where face verification system is free from face anti-spoofing.

To observe the importance of face anti-spoofing countermeasure for face verification systems, the experiment was conducted in which a face anti-spoofing method is applied and calculates the score distribution again. It can be observed from the calculated scores after applying face anti-spoofing method in Fig 4 that there is a prominent shift in spoof attacks scores with clear margin towards the imposter score. This means implementing the face anti-spoofing method creates the clear discrimination between the valid user and imposter along with non-live faces.

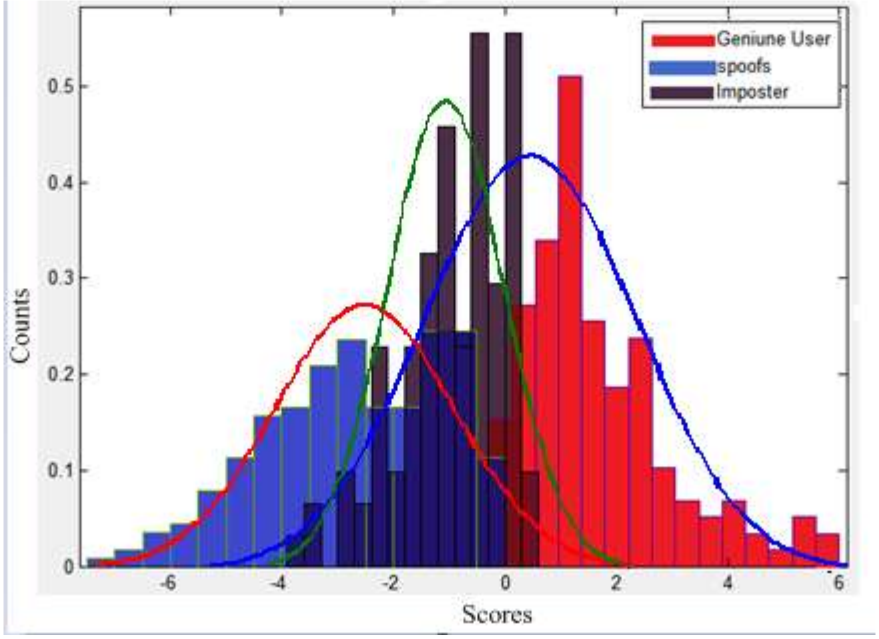

Fig 4:- Score Distribution with anti-spoofing system

The ROC curve of verification system is plotted under the two conditions, one without anti-spoofing and one with applying anti-spoofing system on verification system in Fig 5. The curve shows that if there is no anti-spoofing system applied on face verification, facial spoof attacks get access easily. While lower curve of ROC is because of the detection of such spoof attacks. The reason of higher ROC of face spoof attacks is because of overlay of score distribution of spoof over genuine which lead no difference between the spoof attack and genuine face in the situation where face verification system is free from face anti-spoofing system.

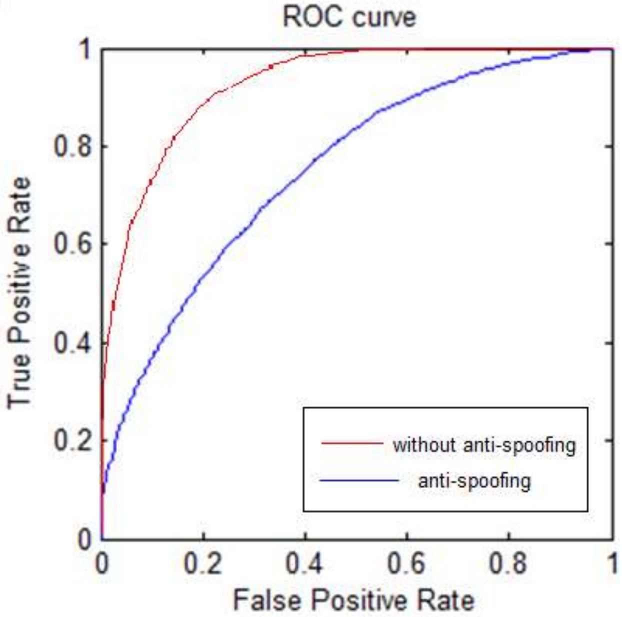

Fig 5:- ROC curve of facial biometircs with and withoud face anti-spoofing system

Conclusion:-

In this paper, a framework is portrayed in which the system can be viewed with and without spoof attacks. Local binary pattern (LBP) was utilized to extract feature of genuine and various spoof attacks. Moreover, the main objective of this paper is to introduce a database of a variety of textures that does not offered by other existing available databases in the market and evaluating the effectiveness of anti-spoofing system by implementing facial database for verification system. For making UPMFSDB more challenging, we have maintained the same trends for fake attacks which were introduced in the previously available databases, like rotating and moving the photographs back and forth, using A4 paper and digital display devices as used in NUAA and CASIA databases. Our intention is to introduce more challenging attacks in terms of textures in still images or photographs with the help of different kind of papers and different resolutions. Because attacker can spoof the face biometric system by using different papers and high tech devices that resembles the same properties which are related to real face. In this manner we can evaluate the performance of verification system under the spoofing attacks and reduce the risk of spoofing by utilizing these both databases. It can be verified from the calculated score distributions and ROC curve of the facial biometric system that how much it is necessary to protect the system by implementing the security layer of face anti-spoofing system.

References:-

1. Nixon, Kristin Adair, Valerio Aimale, and Robert K. Rowe. "Spoof detection schemes." In *Handbook of biometrics*, pp. 403-423. Springer US, 2008.
2. Hadid, Abdenour. "Face Biometrics Under Spoofing Attacks: Vulnerabilities, Countermeasures, Open Issues, and Research Directions." In *Computer Vision and Pattern Recognition Workshops (CVPRW), 2014 IEEE Conference on*, pp. 113-118. IEEE, 2014.
3. Tan, Xiaoyang, Yi Li, Jun Liu, and Lin Jiang. "Face liveness detection from a single image with sparse low rank bilinear discriminative model." In *Computer Vision–ECCV 2010*, pp. 504-517. Springer Berlin Heidelberg, 2010.
4. Anjos, André, and Sébastien Marcel. "Counter-measures to photo attacks in face recognition: a public database and a baseline." In *Biometrics (IJCB), 2011 International Joint Conference on*, pp. 1-7. IEEE, 2011.
5. Ojala, T., Pietikainen, M., & Maenpaa, T. (2002). Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on pattern analysis and machine intelligence*, *24*(7), 971-987.