Prevention of Spoofing attacks in FR based Attendance System using liveness detection

Kewal Bhat[1], Suryapratap Chauhan[2], Gopal Benure[3] , Prafulla Ambekar[4], Sagar Salunke[5]

[1,2,3,4] BE Students, Dept. of Computer Engineering, PCCOE, Pune, Maharashtra, India
[5] Professor, Dept. of Computer Engineering, PCCOE, Pune, Maharashtra, India

Abstract - *Face recognition systems are user friendly and easy to use compared to other biometric methods. These systems are susceptible to spoof attacks. Deciding on a specific method is often a difficult task because each method has its disadvantages. In this paper we present a survey on various face liveness detection techniques. We used face recognition and authentication using web cam. After having images from Web-Cam, the image is cropped into square shape. We also focus on the special characteristics of human facial aspects such as eye, nose. In this recognition different control points are detected. The input image goes through the recognition system for facial identification. In some cases where the input image from the Web-Cam does not exist in the database, the user will get some error. However, in cases where the image exists in the database, that image will be computed for similarity measurement using. Distance between control point measures from the input image. The result of our experiment indicate that the recognition process. It is easy to spoof face recognition systems by using photographs. It is important to incorporate face liveness detection algorithms into these systems to make it more secure.*

Key Words: Biometrics, Face Recognition, Liveness detection, Template matching, Spoof attack

1.INTRODUCTION

In tightly connected networked society, personal identification has become critically necessary. Biometric identifiers are commutation ancient identifiers, because it is troublesome to steal, replace, forget or transfer them. A 2D-image primarily based facial recognition system will be simply spoofed with straightforward tricks and a few poorly-designed systems have even been shown to be fooled by the imposters. Spoofing with photograph or video is one among the foremost common manners to circumvent a face recognition system.

Liveness detection mistreatment facial expression in biometric system may be a technique to capture the image of the person and take a look at for his/her aliveness when obtaining documented. Automatic extraction of caput and face boundaries and facial features is vital within the areas of face recognition, criminal identification, security and police investigation systems, human pc interface, and model-based video writing. In general, the processed face recognition includes four steps. First, the face image is increased and segmental. Second, the face boundary and facial expression square measure detected. Third, the extracted options square measure matched against the options within the information. Fourth, the classification or reorganization of the user is achieved. Further, aliveness of the user is to be tested in-order to forestall the spoof attack. Providing dependableness associate degreed security within the biometric system has become a "need of an hour". Since the present biometric systems designed mistreatment many strategies and algorithms fails to beat the fraud and larceny identity. It becomes necessary to make a extremely secure and reliable biometric system that is spoof free employs the facial characteristics variations of person to beat spoof attack by detecting the aliveness. It uses the aliveness detection method that successively uses strategies like Viola Jones for face detection, LBP for feature extraction and Manhattan Distance classifier to spot the genuineness of the user and variations within the facial expression to prevent spoof attack. User authentication is that the basic demand of any security system. Facial biometrics is very difficult biometric modality as face is acquired remotely. The aliveness detection using facial movements to stop the spoof attack is also rising technique. Most of the researchers are creating their efforts to style such systems. The literatures available for these are summarized below. The identity spoofing may be a competitor for high security face recognition applications. With the appearance of social media and globalized search, face pictures and videos are wide-spread on the web and might be probably used to attack biometric systems while not previous user consent. Biometric authentication system for mechanically identifying or verifying an individual from a digital image or a video frame from a video supply. Euclidian distance take a look at is used for checking a person's aliveness that ensures the detection of fake/dummy pictures. Face recognition systems don't seem to be able to work with arbitrary input pictures taken below completely different imaging conditions or showing occlusions and/or variations in expression or cause. To support face recognition one must perform a face image alignment (normalization) step that takes occlusions/variations into consideration. The face detection technique is based on colouring data and fuzzy classification. A replacement algorithmic rule is projected so as to discover automatically face options (eyes, mouth and nose) and extract their correspondent geometrical points. It is exploited for motion analysis onsite to verify "Liveness" likewise on accomplish lip reading of digits. A methodological novelty is that the recommended quantized angle options being designed for illumination invariance without the requirement for pre-processing (e.g., bar chart equalization). There's ton of security threat because of spoofing. Spoofing with photograph or video is one among the foremost common manners to attack a face recognition system. Automatic facial feature extraction, is one of the foremost necessary and tried issues in computer vision. Aliveness discovering is that the ability to detect artificial objects given to a biometric device with

Associate degree intention to subvert the recognition system. The paper presents the information of iris output signal pictures with a controlled quality, and its basic application, specifically development of aliveness detection technique for iris recognition. Single image-based face aliveness detection technique for discriminating 2-D masks from the live faces. Still pictures taken from live faces and 2D masks were found in reality the variations in terms of form and detailed. Face Liveness detection from one Image with thin low rank additive discriminative model. Spoofing with photograph or video is common technique to avoid a face recognition system. A real-time and non-intrusive method to handle face aliveness relies on individual pictures from a generic web camera. A real-time Liveness detection approach against photograph spoofing in face recognition, by recognizing spontaneous eye blinks that may be a non-intrusive manner. The approach needs no additional hardware aside from a generic net camera. Eye blink sequences usually have a fancy underlying structure.

1.1 OPERATION OF SPOOFING PREVENTION USING LIENESS CHECK IN ATTANDANCE SYSTEM :-

The system provides the protection to FR based attendance system by authenticating the user with face attribute along with aliveness detection using variations in eye movements i.e. blinking. The designed model is reinforced by providing the protection in 2 phases i.e. performing authentication and aliveness checks. The designed system for the projected system is as shown within the Fig.1. Commencement within the planned model is getting the image of face biometric modality. Further, localization of facial portion is to be carried using Viola Jones methodology. The feature extraction is that the vital steps in any biometric system. Extract the native regions of the detected face and find eyes locations to extract the options using native Binary Pattern (LBP) operator. The extracted feature vectors i.e. template are to be hold on firmly within the information. Hence, construct the templates from extracted options individually. Throughout identification, compare the stored template from the information with the generated feature vector of the user using template matching. If matching is successful then perform the aliveness check using the variations in native regions of eyes. If there's a variation in these native features, then user is alive else user isn't alive.

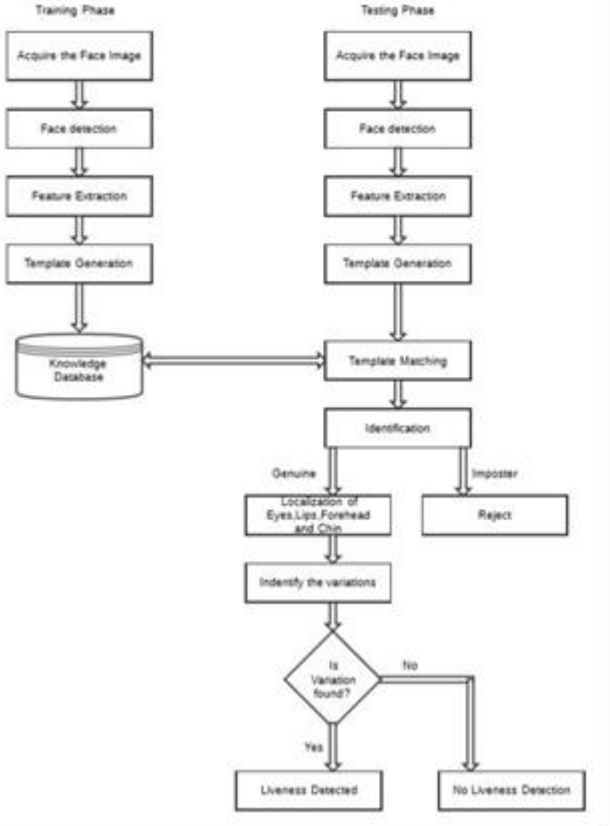


Fig. Operation flow

A. Image Acquisition

Acquire the facial image of the user using the web camera. This section is especially required since it acts as an input for the registration section. Sample face pictures registered within the database is shown in the below figure.

Fig 1. Flow Diagram

B. Face Detection and Alignment

The basic need for face recognition is face detection. Face detection takes place because the camera detects the image of the user. System object is formed to observe the placement of a face in an input face image. The cascade object detector uses the Viola-Jones detection algorithmic program for face detection. By default, the detector is designed to detect faces. Using cascade object face region is tracked and with the assistance of extra properties like bounding box, tracked face region is delimited with parallelogram box. Face Detection and tracking is shown in figure.3. Eye localization is shown in figure 4.

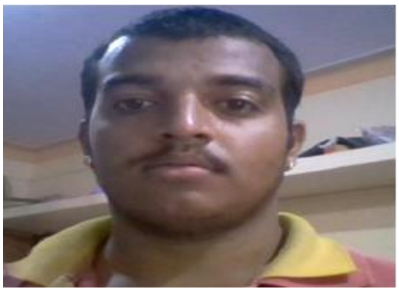


Fig.3.Face Detection Location and tracking

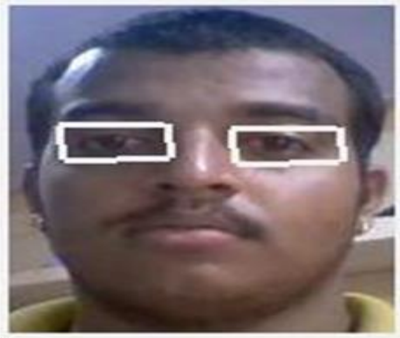


Fig.4.Eye localization

C. Feature Extraction

The features area unit extracted using LBP methodology wherever every facial image i.e. 256x256 component resolutions is split into 256 cells (16x16 rows and columns respectively). The LBP operate is applied to every block of the face image. The feature vector is made from all the 256 grey values computed from the bar chart generated by the individual instances of the face pictures. From each user six instances of face pictures area unit used for coaching. Hence, the dimensions of model for one hundred users is 600x256. The bar chart of the face image is shown in Figure five.

D. Matching

Once face detection, alignment and options extraction are done successfully, the authentication is used with matching the user's facial feature vector with the model from the stored database.

2. SOSTWARES AND TOOLS USED :-

1. Netbeans
2. MySQl
3. SQL query browser
4. OpenCV

1.OpenCV:- OpenCV is released under a BSD license and hence it's free for both academic and commercial use. It has C++, C, Python and Java interfaces and supports Windows, Linux, Mac OS, iOS and Android. OpenCV was designed for computational efficiency and with a strong focus on real-time applications. Written in optimized C/C++, the library can take advantage of multi-core processing.

2.Netbeans:- NetBeans is a software development platform written in Java. The NetBeans Platform allows applications to be developed from a set of modular software components called modules. Applications based on the NetBeans Platform, including the NetBeans integrated development environment (IDE), can be extended by third party developers. The NetBeans IDE is primarily intended for development in Java, but also supports other languages, in particular PHP, C/C++ and HTML5.

3. SQL Query Browser :-

MySQL Query Browser, one of the open source MySQL GUI tools from MySQL AB, is used for building MySQL database queries visually. In MySQL Query Browser, you build database queries using just your mouse—click, drag and drop. MySQL Query Browser has plenty of visual query building functions and features.

3. SIMULATION AND RESULTS :-

The control panel can be interpreted as different parts; the Web-Cam control I/O and the processing unit. The first part receives an input image through the camera, which is further described in Fig. 4 as a Start-up GUI.The Selection of device from the list indicates Web-Cam activation.The square frame is design to surround the facial area as to relocate the prospective area and separate the facial area. After the "Capture" button is pressed, the interrupt signal is sent to our Web-Cam, which has now stopped its task since the prospective image is obtained.

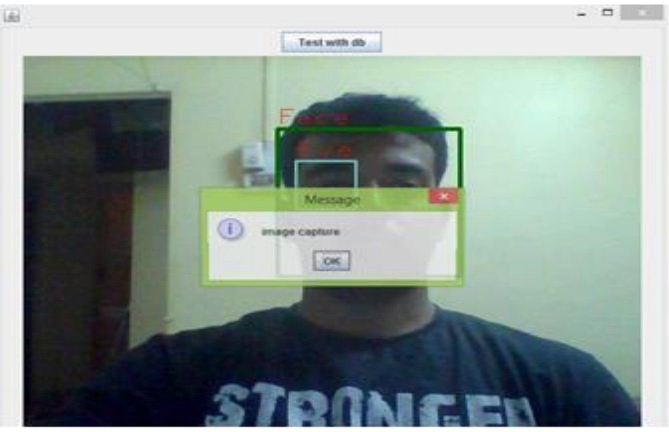
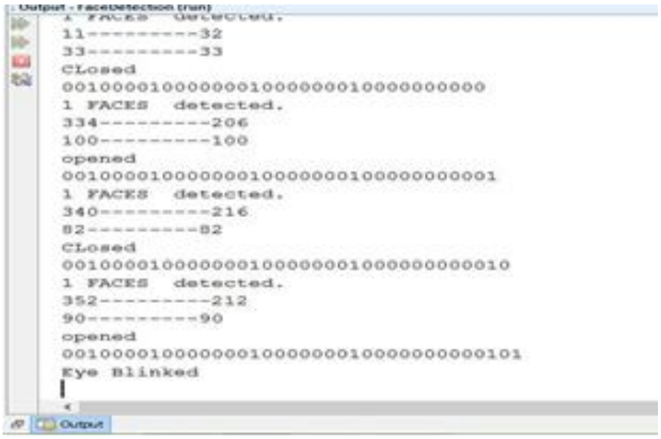


Fig. Image Capture



```
1 FACES  detected.
11----------32
33----------33
CLosed
0010000100000000100000000100000000000
1 FACES  detected.
334----------206
100----------100
opened
00100001000000001000000001000000000001
1 FACES  detected.
340----------216
82----------82
CLosed
001000010000000010000000010000000000010
1 FACES  detected.
352----------212
90----------90
opened
0010000100000000100000000100000000000101
Eye Blinked
```

Fig. Liveness check (eye blinking)

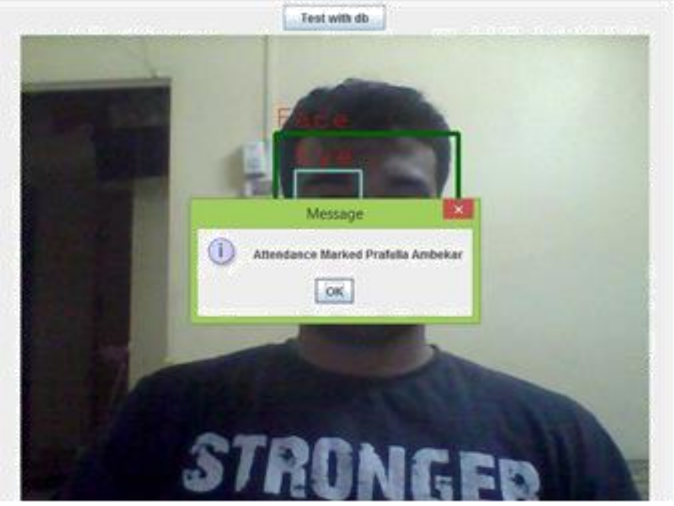


Fig. Attendance marked

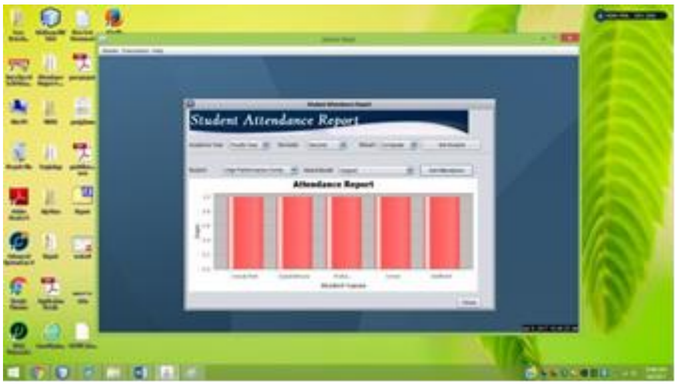


Fig. Attendance Report

4. CONCLUSION AND FUTURE SCOPE :-

This work provided a detailed view of face liveness detection using eye blinking. The most common problems that have been observed in case of many liveness detection techniques are the effects of illumination change, effects of amplified noise on images which damages the texture information. For blinking and movement of eyes based liveness detection methods, eyes glasses which causes reflection must be considered for future development of liveness detection solutions. Our main aim is to give a clear pathway for future development of more secured, user friendly and efficient approaches for face liveness detection.

REFERENCES

[1] D. Kornack Liveness Detection in Biometrics By Maximilian Krieg and Nils Rogmann.

[2] A Leap Password based Verification System Aman Chahar *, Shivangi Yadav *, Ishan Nigam, Richa Singh, Mayank Vatsa IIIT-Delhi, New Delhi.

[3] An Embedded Fingerprint Authentication System, Ms. Archana S. Shinde, Prof. Varsha Bendre, Dept. of E&TC, Pimpri Chinchwad College of Engineering Pune, India.

[4] The Leap Motion controller: A view on sign language.

[5] Prevention of Spoof Attack in Biometric System Using Liveness Detection by Sanjeevankumar M. Hatture, Nalinakshi B. G, Rashmi P. Karchi.

[6] Corneal Topography: An Emerging Biometric System for Person Authentication By Nassima Kihal, Arnaud Polette, Salim Chitroub, Isabelle Brunette and Jean Meunier.

[7] A Basic Design for Adaptive Corneal Topography H.J.W. Spoelder', F.M. Vos2, D.M. Germans' 1 .Division of Physics and Astronomy Faculty of Sciences,Vrije Universiteit, De Boelelaan

[8] Liveness Detection Technique for Prevention of Spoof Attack in Face Recognition System Nalinakshi B. G1, Sanjeevakumar M. Hatture2, Manjunath S.Gabasavalgi3, Rashmi P. Karchi4.

[9] Automated Attendance Management System Using Face Recognition