International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 02 | Feb -2017 www.irjet.net p-ISSN: 2395-0072

Prevention of Spoofing Attacks in Face Recognition System Using Liveness Detection

Kewal Bhat[1],Suryapratap Chauhan[2],Gopal Benure[3],Prafulla Ambekar[4],Prof. 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 - *Biometric system has gained wide selection of motivations and applications in security domain. Biometric systems relay on the biometric characteristics/data taken from the user for authentication. sadly such biometric information is stolen or duplicated by the imposters/unauthorized users. Most of the biometry systems rely strictly on distinguishing the physiological characteristics of the user. It becomes easier to spoof in these biometric systems with the help of faux biometric it any reduces the dependability and security of biometric system. Spoof fools the system through the method of deception and impersonating others to create out that they're licensed so as to achieve access in to the biometric system. Now a day's spoofing has become quite common on the net that therefore ends up in determine stealing and fraud. There are several level of spoofing attacks like putting faux biometry on the detector, replay attack, attacking the entrance centre corrupting the intermediator, attacking the application etc. These successively can cut back the extent of security and dependability of biometric system. liveness identification using the facial expression also has been receiving a lot of attention compared to other biometric modalities. prevention of spoof attack in biometric system is done by detecting the liveness of the user with the assistance of native facial expression like eye blinking, lip movement, forehead and chin movement pattern of the face detected with real-time generic web-camera. within the planned work, a good authentication system using face biometric modality by developing the aliveness detection model using the variations within the facial movements.*

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

1.INTRODUCTION

In this 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.

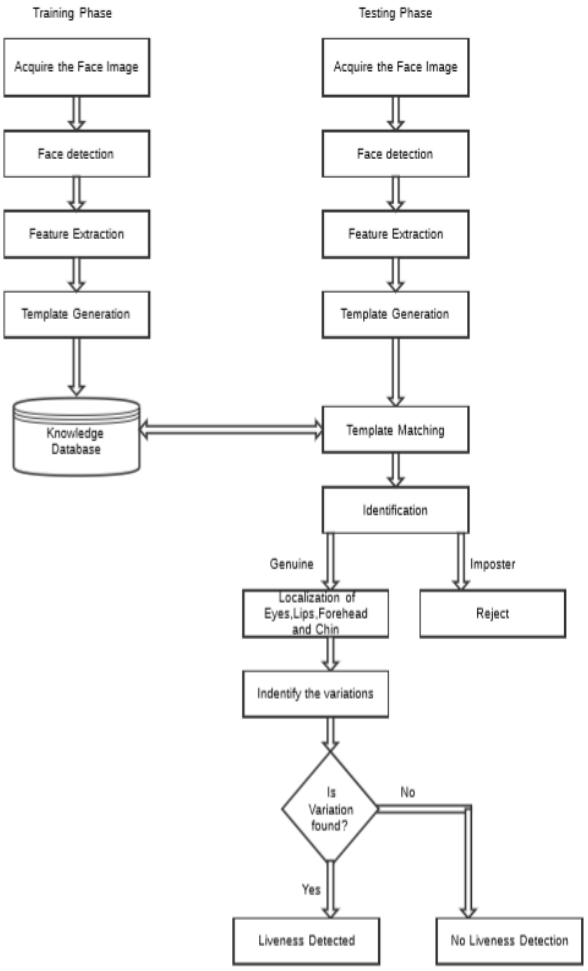
Liveness detection mistreatment facial expression in biometric system may be a technique to capture the image of the person and take a look at for his/her aliveness when obtaining documented. Automatic extraction of caput and face boundaries and facial features is vital within the areas of face recognition, 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 an

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 coloring 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 preprocessing (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 2-D 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 Proposed System:

The proposed model provides the protection to biometric system by authenticating the user with face attribute along with aliveness detection using variations in facial eye, lip, chin and forehead movements. 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, lips, forehead and chin 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 i.e. with Manhattan distance. If matching is successful then perform the aliveness check using the variations in native regions of facial features like eyes, lips, forehead and chin. If there's a variation in these native features, then user is alive else user isn't alive.



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.

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. Face alignment is shown in figure 4.

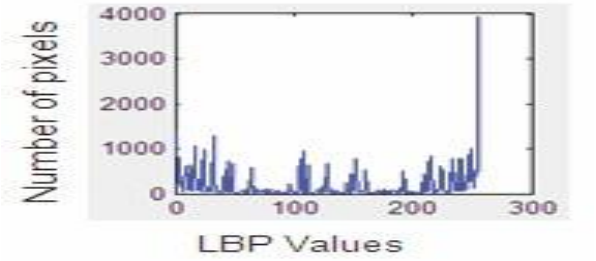
Fig.3.Face Location and tracking

Fig.4.Face Alignment

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 5.



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. because the user identification is one-to-many matching, the feature vector of the individual are compared with the feature vectors of each individual hold on within the model database with Manhattan distance. Finally the simplest Matching facial image is known using the minimum Manhattan distance. The Manhattan distance is computed using following equation

$$d = \sum_{i=1}^{n} | xi - yi |$$

Where n=256 is that the dimension of the feature vector, xi is the i-th element of the sample feature vector, and yi is the I the element of the model feature vector. more the aliveness check is carried for genuine user. If the user's authentication is failing, no aliveness check is performed.

C. Liveness Detection

Local Binary Pattern (LBP) algorithmic program:

Step 1: Divide the aligned face image into 256 cells. (e.g. 16x16 pixels for every cell).

Step 2: for every component in a very cell is compared with its eight neighbouring pixels on a circle in clockwise or counter clockwise direction.

Step 3: If the middle pixel's value is larger than its neighbour, then label with "1" otherwise, label with "0" i.e. 8-digit binary range (converted to decimal for convenience).

Step 4: reason the bar chart, over the cell, of the frequency of every "number" occurring (i.e., every combination of that pixels area unit smaller and that area unit larger than the center).

Step 5: Normalize the bar chart.

Step 6: Concatenate normalized histograms of all cells to get the feature vector for the window.

Algorithm for aliveness Detection:

Step1: Acquire the input as face image and localize the face i.e. observe face

Step2: find the facial centre by putting a kind of marker

Step3: Draw the virtual line on the centre

Step4: find native eye region of face using equations (Refer figure half dozen.)

i) Estart = ceil(x/2-(x-0.8*x) wherever the worth of x=100

ii) end = ceil(x/2+5)

Step 5: find native lip region of face using equations (Refer figure seven.)

i) Lstart = ceil(x-x/4) wherever x=100

ii) Lend = ceil(x-20)

Step 6: find native forehead region of face using equations (Refer figure eight.)

i) Fstart = Estart

ii) Fend = twenty

Step 7: find native chin region of face using equations (Refer figure nine.)

i) Cstart=Lend

ii) Cend=ceil(x)

Step 8: Convert every RGB native facial feature into grey image.

Step 9: Set the threshold worth for every native facial feature.

Step 10: Extract the perimeters of every native facial feature.

Step 11: notice the mean and variance of every feature using below equations

Mean = (X) / N

Where,

X = Individual knowledge points

N = Sample size (number of information points)

Standard Deviation= $\sqrt{\frac{X!\bar{X}'}{n!1}}$

Where, n is that the range of parts within the sample
X could be a vector X could be a mean of vector.

Step 12: If there's a variation in native facial features i.e. eyes, lips, forehead and chin then the person is alive else not alive.

Step 13: Stop

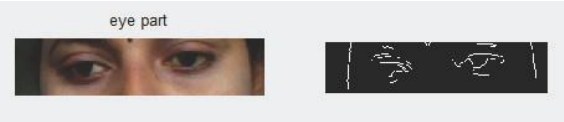


Fig.6.Localization of eye and its variation

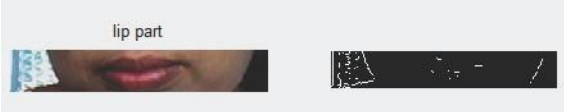


Fig.7.Localization of lips and its variation

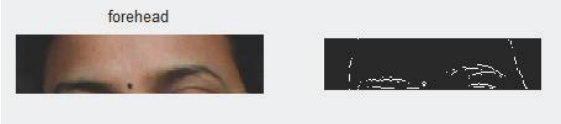


Fig.8.Localization of forehead and its variation

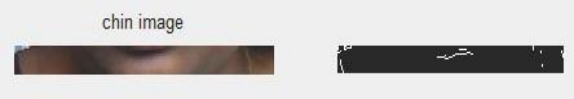


Fig.9.Localization of chin and its variation

3. CONCLUSION

Hence, by introducing liveness detection in face recognition system, we will be able to overcome the drawbacks of conventional face recognition system and provide access to legitimate users only.

REFERENCES

[1] 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] [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.