Prevention of Spoof Attack in Biometric System Using Liveness Detection

Sanjeevakumar M. Hatture

Department of Computer Science and Engineering,
Basaveshwar Engineering College, Bagalkot, Karnataka State, India.

Nalinakshi B. G

Department of Computer Science and Engineering,
Basaveshwar Engineering College, Bagalkot,Karnataka State,India.

Rashmi P. Karchi

Research Scholar, Department of Computer Science,
Bharthiar University, India.

Abstract- Biometric system has gained wide range of motivations and applications in security domain. Biometric systems relay on the biometric characteristics/data taken from the user for authentication. Unfortunately such biometric data is stolen or duplicated by the imposters/unauthorized users. Most of the biometrics systems depend purely on identifying the physiological characteristics of the user. It becomes easier to spoof in these biometric systems with the aid of fake biometric; it further reduces the reliability and security of biometric system. Spoof fools the system through the process of deception and impersonating others to make out that they are authorized in order to gain access in to the biometric system. Now a day's spoofing has become very common on the internet which thus leads to identify theft and fraud. There are several level of spoofing attacks such as placing fake biometrics on the sensor, replay attack, Attacking the enrolment centre Corrupting the matcher, Attacking the application etc, these in turn will reduce the level of security and reliability of biometric system. Liveness identification using the facial features also has been receiving more attention compared to other biometric modalities. Prevention of spoof attack in biometric system can be done by detecting the liveness of the user with the help of local facial features like eye blinking, lip movement, forehead and chin movement pattern of the face detected with real-time generic web-camera. In the proposed work, an effective authentication system using face biometric modality by developing the liveness detection model using the variations in the facial movements. The developed method is evaluated for 50 users, with severe variation in pose and expressions. With own database face recognition accuracy is around 86% and Liveness detection performance for the 50 authenticated users is around 88% is achieved.

Keywords – Biometrics, Face Recognition, Liveness detection, Template matching, Spoof attack

I. INTRODUCTION

In tightly connected networked society, personal identification has become critically important. Biometric identifiers are replacing traditional identifiers, as it is difficult to steal, replace, forget or transfer them. A 2D-image based facial recognition system can be easily spoofed with simple tricks and some poorly-designed systems have even been shown to be fooled by the imposters. Spoofing with photograph or video is one of the most common manners to circumvent a face recognition system.

Liveness detection using facial features in biometric system is a method to capture the image of the person and test for his/her liveness after getting authenticated. Automatic extraction of human head and face boundaries and facial features is critical in the areas of face recognition, criminal identification, security and surveillance systems, human computer interface, and model-based video coding. In general, the computerized face recognition includes four steps. First, the face image is enhanced and segmented. Second, the face boundary and facial features are detected. Third, the extracted features are matched against the features in the database. Fourth, the classification or reorganization of the user is achieved. Further, liveness of the user is to be tested in-order to prevent the spoof attack. Providing reliability and security in the biometric system has become a "need of an hour". Since the existing biometric systems designed using several methods and algorithms fails to overcome the fraud and theft identity. It becomes necessary to build a highly secure and reliable biometric system which is spoof free. The proposed works employs the facial characteristics variations of person to overcome spoof attack by detecting the liveness. It uses the aliveness detection process which in turn uses methods like Viola Jones for face detection, LBP for feature extraction and Manhattan Distance classifier to identify the genuineness of the user and variations in the facial features to prevent spoof attack.

User authentication is the basic requirement of any security system. Facial biometrics is highly demanding biometric modality as face is acquired remotely. The liveness detection using facial movements to prevent the spoof attack is also emerging technique. Most of the researchers are making their efforts to design such systems. The literatures available for these are summarized below;

The identity spoofing is a contender for high-security face recognition applications. With the advent of social media and globalized search, face images and videos are wide-spread on the internet and can be potentially used to attack biometric systems without previous user consent [1]. Facial recognition system for automatically identifying or verifying a person from a digital image or a video frame from a video source. Euclidean distance test is used for checking a person's aliveness which ensures the detection of fake/dummy images [2]. Face recognition systems are not able to work with arbitrary input images taken under different imaging conditions or showing occlusions and/or variations in expression or pose. To support face recognition one has to perform a face image alignment (normalization) step that takes occlusions/variations into account. [3] The face detection technique is based on skin color information and fuzzy classification. A new algorithm is proposed in order to detect automatically face features (eyes, mouth and nose) and extract their correspondent geometrical points. [4]).It is exploited for motion analysis onsite to verify "Liveness" as well as to achieve lip reading of digits. A methodological novelty is the suggested quantized angle features ("quangles") being designed for illumination invariance without the need for preprocessing (e.g., histogram equalization). [5] There is lot of security threat due to spoofing. Spoofing with photograph or video is one of the most common manners to attack a face recognition system.[6] Automatic facial feature extraction, is one of the most important and attempted problems in computer vision.[7] . Liveness detection is the ability to detect artificial objects presented to a biometric device with an intention to subvert the recognition system. The paper presents the database of iris printout images with a controlled quality, and its fundamental application, namely development of Liveness detection method for iris recognition. [8] Single image-based face Liveness detection method for discriminating 2-D masks from the live faces. Still images taken from live faces and 2-D masks were found to bear the differences in terms of shape and detailedness. [9] Face Liveness detection from a Single Image with sparse low rank bilinear discriminative model. Spoofing with photograph or video is common method to circumvent a face recognition system. A real-time and non-intrusive method to address face Liveness is based on individual images from a generic web camera. [10] A real-time Liveness detection approach against photograph spoofing in face recognition, by recognizing spontaneous eye blinks, which is a non-intrusive manner. The approach requires no extra hardware except for a generic web camera. Eye blink sequences often have a complex underlying structure. [11]

II. Proposed Algorithm

The proposed model provides the security to biometric system by authenticating the user with face trait along with liveness detection using variations in facial eye, lip, chin and forehead movements. The designed model is strengthened by providing the security in two phases i.e. performing authentication and Liveness checks. The designed system for the proposed system is as shown in the Fig.1. First step in the proposed model is acquiring the image of face biometric modality. Further, localization of facial portion is to be carried using Viola Jones method. The feature extraction is the important steps in any biometric system. Extract the local regions of the detected face and locate eyes, lips, forehead and chin locations to extract the features using Local Binary Pattern (LBP) operator. The extracted feature vectors i.e. template are to be stored securely in the database. Hence, construct the templates from extracted features separately. During identification,compare the stored template from the database with the generated feature vector of the user using template matching i.e. with Manhattan distance. If matching is successful then perform the Liveness check using the variations in local regions of facial features like eyes, lips, forehead and chin. If there is a variation in these local features, then user is alive else user is not alive.

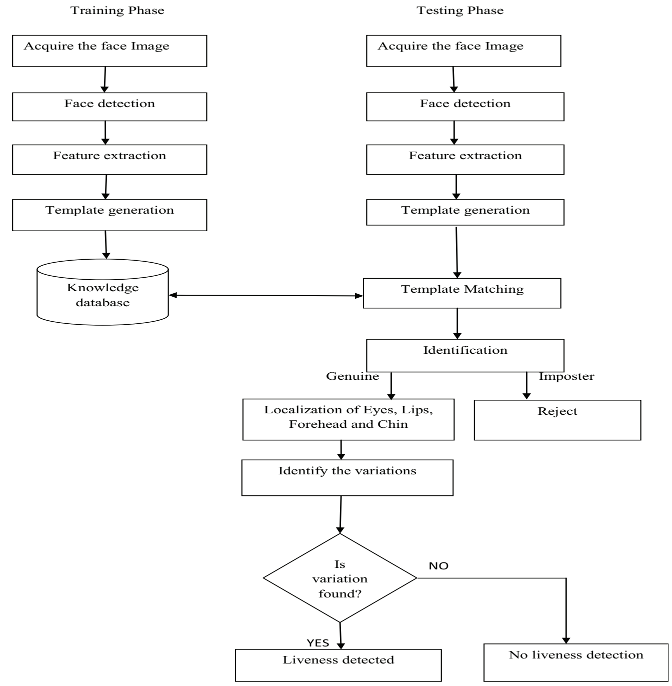


Figure 1. Propsed Model

A. Image Acquisition-

Acquire the facial image of the user using the web camera. This phase is mainly needed since it acts as an input for the registration phase. Sample face images registered in the database is shown in Figure 2.

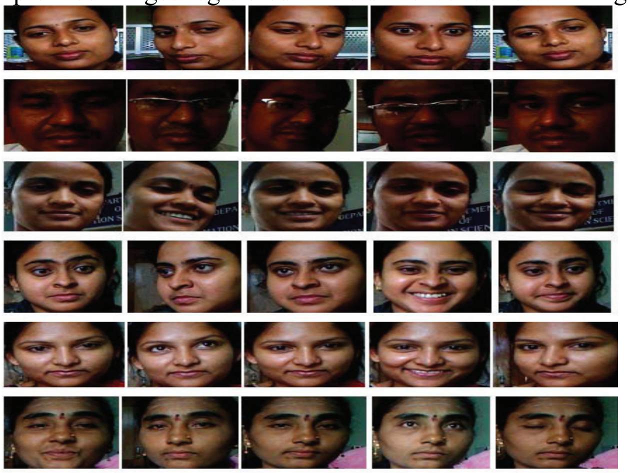


Figure 2. Image Acquisituion

*B. Face Detection and Alignment***-**

The basic need for face recognition is face detection. Face detection takes place as the camera detects the image of the user. System object is created to detect the location of a face in an input face image. The cascade object detector uses the Viola-Jones detection algorithm for face detection. By default, the detector is configured to detect faces. Using cascade object face region is tracked and with the help of additional properties like bounding box, tracked face region is bounded with rectangle box. Face Detection and tracking is shown in figure.3.Face alignment is shown in figure 4.

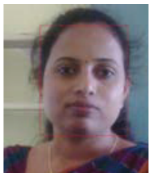


Figure 3. Face Detection and Tracking

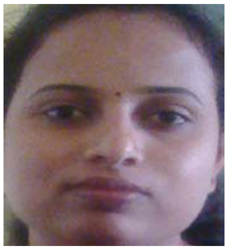


Figure 4. Face Alignment

C. *Feature Extraction-*

The features are extracted using LBP method where each facial image i.e. 256x256 pixel resolutions is divided into 256 cells (16x16 rows and columns respectively). The LBP function is applied to each block of the face image. The feature vector is constructed from all the 256 gray values computed from the histogram generated by the individual instances of the face images. From every user six instances of face images are used for training. Hence, the size of template for 100 users is 600x256. The histogram of the face image is shown in Figure 5.

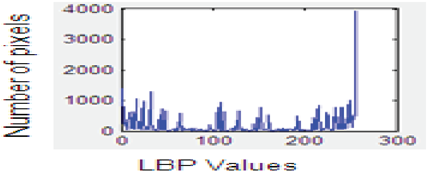


Figure 5. Feature Extraction

D. Matching-

Once face detection, alignment and features extraction are done successfully, the authentication is employed with matching the user's facial feature vector with the template from the stored database. As the user identification is one-to-many matching, the feature vector of the individual are compared with the feature vectors of every individual stored in the template database with Manhattan distance. Finally the Best Matching facial image is identified using the minimum Manhattan distance. The Manhattan distance is computed using following equation,

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

Where n=256 is the dimension of the feature vector, x_i is the i^{th} component of the sample feature vector, and y_i is the i^{th} component of the template feature vector. Further the liveness check is carried for authenticated user. If the user's authentication is failed, no liveness check is performed.

E. Aliveness detection-

The main aim of this work is identify the liveness detection to avoid the spoof attack on the biometrics system. Hence, to detect the liveness the movements of the local regions of the facial features is calculated by taking mean and standard deviation of each of the local regions i.e. eyes, lips, chin and forehead. The proposed algorithm considers all the movements of the local features to decide whether the user is alive or not. Once a movement is detected in these local facial features, it can be concluded that the person is alive. If there is no movements are found in these local facial features then the person is not alive. The movements are calculated by taking mean and standard deviation of each of the local facial feature.

Local Binary Pattern (LBP) Algorithm

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

Step 2: For each pixel in a cell is compared with its 8 neighboring pixels along a circle in clockwise or counter-clockwise direction.

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

Step 4: Compute the histogram, over the cell, of the frequency of each "number" occurring (i.e., each combination of which pixels are smaller and which are greater than the center).

Step 5: Normalize the histogram.

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

Algorithm for Liveness Detection

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

Step2: Locate the facial centre by placing a sort of marker

Step3: Draw the virtual line along the centre

Step4: Locate local eye region of face using equations (Refer figure 6.)

i) Estart = ceil(x/2-(x-0.8*x) where the value of x=100

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

Step 5: Locate local lip region of face using equations (Refer figure 7.)

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

ii) Lend = ceil(x-20)

Step 6: Locate local forehead region of face using equations (Refer figure 8.)

i) Fstart = Estart

ii) Fend = 20

Step 7: Locate local chin region of face using equations (Refer figure 9.)

i) Cstart=Lend

ii) Cend=ceil(x)

Step 8: Convert each rgb local facial feature into gray image

Step 9: Set the threshold value for each local facial feature

Step 10: Extract the edges of each local facial feature

Step 11: Find the mean and standard deviation of each feature using below equations

$$\text{Mean} = \frac{\sum(X)}{N} \qquad (2)$$

Where, $\Sigma =$ Sum of

X = Individual data points

N = Sample size (number of data points)

$$\text{Standard Deviation}=\sqrt{\frac{\sum X-\overline{X}}{n-1}} \qquad (3)$$

Where, n is the number of elements in the sample

X is a vector $\overline{X}$ is a mean of vector.

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

Step 13: Stop

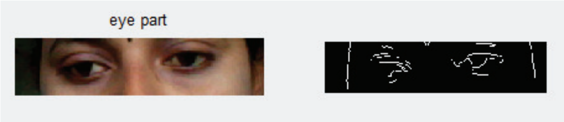


Figure 6. Localization of Eye and its variations

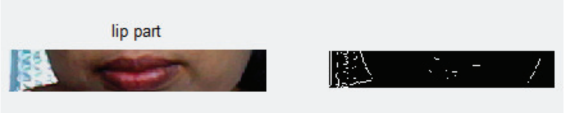


Figure 7. Localization of Lip and its variations

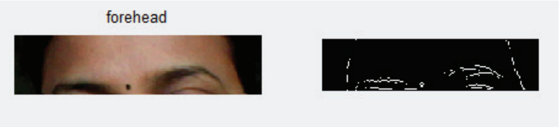


Figure 8. Localization of Forehead and its variations

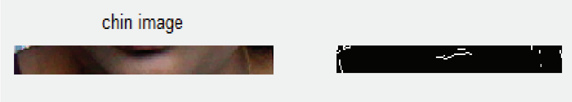


Figure 9. Localization of Chin and its variations

III. Experiments and Results

The developed method is evaluated by testing with four face images taken from every user with severe variation in pose and expressions. With the manually created database face recognition performance is considered as, the Correct Identification Rate (CIR) of around 86% ,false rejection rate is around14% and the false acceptance rate is around 16% is achieved. Face recognition performance for own databases is depicted in Table-1. The Liveness detection performance for the 50 authenticated users is considered as, the Correct Identification Rate (CIR) of around 88%; false rejection rate is around12%.The performance of the proposed model is measured using CIR, FAR and FRR.

$$\text{CIR}= \frac{\text{Number of Correctly Identified Users}}{\text{Total Number of Users}} \, x\, 100\% \qquad (4)$$

$$\text{FAR}= \frac{\text{Number of Wrongly Identified Users}}{\text{Total Number of Users}} \, x\, 100\% \qquad (5)$$

$$\text{FRR}= \frac{\text{Number of wrongly rejected Users}}{\text{Total Number of Users}} \, x\, 100\% \qquad (6)$$

Table- 1 Face Recognition Performance

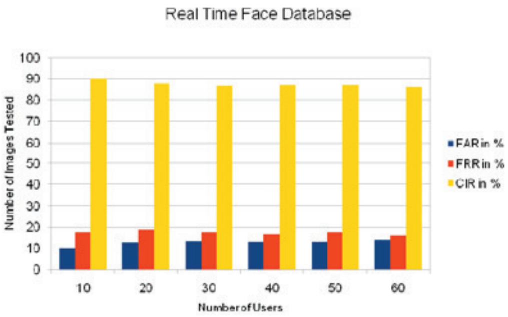
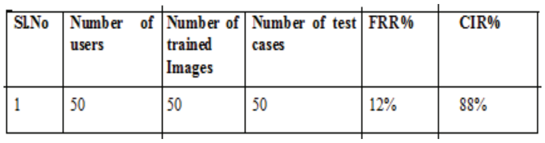


Table-2 Face Recognition Performance Analysis

SI.No	Number of users	Number of Images Tested	Number of wrongly Identified Images	Number of Wrongly Rejected Images	Number of Correctly Identified Images	FAR in %	FRR in %	CIR in %
1	10	40	4	7	36	10	17.5	90
2	20	80	10	15	70	12.5	18.75	87.5
3	30	120	16	21	104	13.3	17.5	86.7
4	40	160	21	27	139	13.1	16.8	86.9
5	50	200	26	35	174	13	17.5	87
6	60	240	33	38	207	13.7	15.8	86.3

Table 3- Liveness Detection Performance



Sl.No	Number of users	Number of trained Images	Number of test cases	FRR%	CIR%
1	50	50	50	12%	88%

IV.CONCLUSION

The developed system identifies the user being genuine or not, in face biometric security systems. The proposed system is implemented by integrating standard algorithm like Voila Jones algorithm for face detection, LBP method for feature extraction, Manhattan Distance classifier for matching. The developed system is tested for 50 persons from own database (viz. real time database). The accuracy of 86.3% and for the authenticated users the accuracy of Liveness Detection is around 88% is achieved. Thus the designed system provides higher rate of performance in terms of security. In future, different biometric modality can be used for user identification to increase the accuracy of the developed system. The other issues and challenges of the face modality like occluded face, variation in illumination and face acquired from the large distance etc. are to be addressed.

REFERENCES

[1] Andre Anjos, Murali Mohan Chakka and S´ebastien Marcel,”Motion- Based Counter-Measures to Photo Attacks in Face Recognition “,Idiap Research Institute - Centre du Parc, rue Marconi 19, 1920 Martigny, Switzerland,pp.1-27,2013.

[2] Annu, Dr. Chander Kant," Liveness Detection in Face Recognition Using Euclidean Distances” , International journal for advance research in engineering and technology, Vol. 1, Issue IV, ISSN 2320-6802,pp.1-5, May 2013.

[3] Martin Urschler, Markus Storer, Horst Bischof, Josef A. Birchbauer, “Robust Facial Component Detection for Face Alignment Applications”, Institute for Computer Graphics and Vision Graz University of Technology, Austria and Siemens Biometrics Center Siemens IT Solutions and Services, Siemens Austria ,pp.1-12, 2009.

[4] Yousra ben jemaa, Sana khanfer, “Automatic local Gabor features extraction for face recognition” (IJCSIS) International Journal of Computer Science and Information Security,Vol. 3, No. 1,pp.1-7, 2009.

[5] Klaus Kollreider, Hartwig Fronthaler, Maycel Isaac Faraj, and Josef Bigun, Fellow, IEEE,”Real-Time Face Detection and Motion Analysis with Application in “Liveness” Assessment”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 2, NO. 3, pp.548-558, 2007.

[6] Dr. Chander Kant Nitin Sharma,” Fake Face Detection Based on Skin Elasticity”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, ISSN: 2277 128X,pp.1048-1051, May – 2013.

[7] Bhumika G. Bhatt, Zankhana H. Shah,” Face Feature Extraction Techniques: A Survey”, National Conference on Recent Trends in Engineering & Technology, pp.13-14, 2011.

[8] Adam Czajka,” Database of Iris Printouts and its Application: Development of Liveness Detection Method for Iris Recognition”, Institute of Control and Computation Engineering Warsaw University of Technology, ul. NowowiejskaWarsaw, Poland, pp.26-29, Aug 2013.

[9] Gahyun, Sungmin, Jae, Dong, Kang and Jaihie, "Face Liveness Detection Based on Texture and Frequency Analyses", Research Institute of Automotive Electronics and Control, Hanyang University, Republic of Korea, pp.1-5, 2012.

[10] Hui Zhang, Zhenan Sun, Tieniu Tan, Jianyu Wang, "Learning Hierarchical Visual Codebook for Iris Liveness Detection", Shanghai Institute of Technical Physics, Chinese Academy of Sciences, pp.1-5, 2011.

[11] Yuqing He1 Yushi Hou Yingjiao Li Yueming Wang, "Liveness iris detection method based on the eye’s optical features", Key Laboratory of Photoelectronic Imaging Technology and System, Ministry of Education of China, Proc. of SPIE Vol.7838, pp.1-7, 2010.

[12] Gang Pan,Lin Sun, Zhaohui Wu, Shihong Lao, “Eyeblink-based Anti-Spoofing in Face Recognition from a GenericWebcamera”, Department of Computer Science Zhejiang University, China &Sensing&Control Technology Lab.OMRON Corporation, Japan, pp. 978-1-4244-1631,2007.

[13] P.Bhardwaj, Swapan Debbarma, Suman Deb, Nikhil Debbarma, Jayanta Pal ,”Liveness Detection Using Eye Blink A case Study”, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 1, Issue 3, ISSN 2319 – 4847,pp.21-28, November 2012.

[14] Hyung-Keun Jee, Sung-Uk Jung, and Jang-Hee Yoo, "Liveness Detection for Embedded Face Recognition System", World Academy of Science, Engineering and Technology, pp.941-943, 2008.

[15] Xiaoyang Tan, Yi Li, Jun Liu and Lin Jiang, "Face Liveness Detection from A Single Image with Sparse Low Rank Bilinear Discriminative Model", Dept. of Computer Science and Technology Nanjing University of Aeronautics and Astronautics, China, pp.1-12, 2011.

[16] Zhiwei Zhang, Dong Yi, Zhen Lei, Stan Z. Li, “Face Liveness Detection by Learning Multispectral Reflectance Distributions”, Center for Biometrics and Security Research & National Laboratory of Pattern Recognition Institute of Automation, Chinese Academy of Sciences,pp.1-6,2011.

[17] Frank Y. Shih, Chao-Fa Chuang, “Automatic extraction of head and face boundaries and facial features”, Information Science an International Journal Vol.158, pp.117–130, 2004.

[18] Hua Gu Guangda Su Cheng Du,” Feature Points Extraction from Faces”, Research Institute of Image and Graphics, Department of Electronic Engineering, pp.154-158, 2003.

[19] Ying-li Tian Takeo Kanade Jeffrey F. Cohn,” Recognizing Facial Actions by combining Geometric Features and Regional Appearance Patterns”, Robotics Institute, Carnegie Mellon University,pp.1-31, 2001.

[20] Athanasios Nikolaidis, Ioannis Pitas, “Facial feature extraction and pose determination”,Journal of Pattern Recognition Society, Vol.33, pp.1783-1791, 2000.

[21] Indian Face Database: http://vis-www.cs.umass.edu/~vidit/AI/dbase.html.

[22] Shanumukhappa A Angadi, Sanjeevakumar M Hatture, 2011, “A Novel Spectral Graph Theoretic Approach To User Identification Using Hand Geometry”, International Journal of Machine Intelligence ISSN: 0975–2927 & E-ISSN: 0975–9166, Volume 3, Issue 4, pp.282-288, December 2011.