Volume 6, Issue 2, April-September 2015

ISSN: 0973-7391 Impact Factor: 2.5 Available at www.csjournals.com

IJCSC 0973-7391 International Journal of Computer Science & Communication

Improving Performance of a Face Liveness Detection System Using Soft Biometrics

Sonal Girdhar[1], Arun Kumar Yadav[2], Dr. Chander Kant[3]

[1,2] Research Scholar, Department of Computer Science and Applications, K.U., kurukshetra, INDIA

[3]Asst. Professor, Department of computer Science and Application, K.U., Kurukshetra, INDIA

Abstract: A biometric system identifies an individual based on physiological or behavioral characteristics. Face is one of the most commonly used biometric in authentication systems but nowadays there are a lot of security threats due to spoofing. A face recognition system can easily be spoofed with a photograph or a video of the legitimate user. Liveness detection is a technique to make sure that the data is being provided by a live user and not from artificial sources. Although soft biometric traits such as eye color, age, gender, ethnicity, etc. lack the ability to uniquely identify an individual, yet they provide some additional information about the user and may improve the efficiency of the system. Here in this paper, we have proposed a technique for integrating liveness detection with soft biometrics to improve the performance of the authentication system.

Keywords: Biometrics, Face Recognition, Liveness Detection, Soft Biometrics.

I. INTRODUCTION

Face recognition is a process of identifying and verifying an individual by recognizing his face. Face recognition has become an important aspect in security systems, credit card verification, criminal investigation and many other applications [1]. But with increasing technological advancement one can easily spoof a biometric identification system. Face recognition systems can be spoofed by static facial images. Several spoofing techniques have been developed to fool the biometric systems, and the security of such systems against attacks needs to be improved. Therefore, there is an increasing need to detect such attempts of attacks to biometric systems. Since the sensor is the most susceptible part, spoofing attacks have become easier for the intruders. Moreover, unlike the traditional authentication systems which are password or token based, some of our biometric data such as faces can be accessed from social networks, personal web sites, and can be easily sampled directly with a digital camera.

In face biometrics, an impostor tries to access the system as a valid user with three approaches [2]: (1) showing photograph of a legitimate user; (2) showing a video of a legitimate user, or (3) showing a 3D facial model of a legitimate user. Liveness detection can be used to prevent this kind of spoof attacks by ensuring that the biometric data is being presented from a live, authorized person and not from an imposter who is trying to fool the system by providing fake biometrics to get access to the system. Rest of the paper is organised as follows: liveness detection in face recognition in section II, related work in section III, proposed work in section IV, extraction of soft biometrics in section V, comparison of the proposed scheme with the existing techniques in section VI and finally conclusion and future prospects in the last section.

II. LIVENESS DETECTION IN FACE RECOGNITION

Liveness detection in a biometric system can be performed either at the acquisition or at the processing stage. It can be implemented in the following three ways [3]:

i) Using extra hardware

Adding new hardware adds extra cost to the system and also it can be easily fooled by an intruder. For example the intruder may present the artificial face image of the legitimate user to the face scanner while his own real face to the hardware that just detects the liveness of the face.

ii) Using software

This type of system is not easy to be fooled by the intruder but it becomes very complex to extract additional liveness information from already captured data without any extra hardware.

iii) Using combination of hardware and software

This method is very effective for facial thermogram but is expensive as well as time consuming. However it provides a good high end solution for liveness detection which is difficult to breech.

Basically, fake faces have two main properties:

a) Large variations: Although the affirmative class, i.e., the genuine user, has limited variation (all genuine faces are human skins), the harmful class, i.e., the fake faces, can range from photos, videos to masks and so on. The variety becomes even larger when it comes to material level. Face mask can be made of rubber, plastic, silica gel, etc. Some examples of fake faces are shown in figure 1 [4].

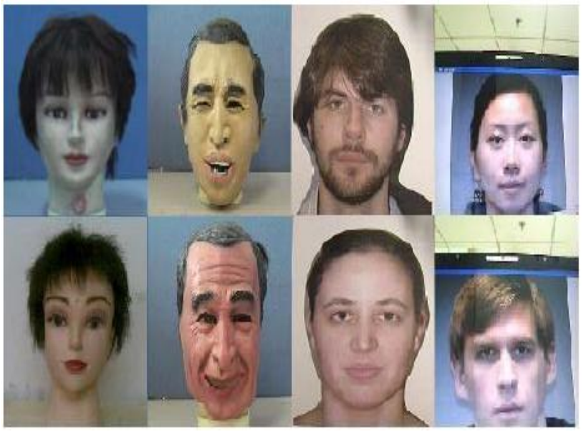

Fig. 1: Some Fake face examples made of silica gel, rubber, photo and video replay

b) Indistinguishable under visible light: Fake face is the one which is indistinguishable for human eyes. Therefore, without extra hardware, only visual face images are insufficient and impossible for the detection of fake faces.

Two of the most important challenges nowadays are: (1) the need of designing and deploying non-intrusive methods without extra hardware and human involvement; and (2) designing detection methods robust to changes in pose and illumination conditions.

III. RELATED WORK

In this section, we review the literature on some liveness detection techniques that can easily be integrated to existing face recognition systems. From the static view, an essential difference between a live face and a photograph is that a live face is a fully three dimensional object while a photograph could be considered as a two dimensional planar structure. With this natural trait, Choudhary et al employed the structure from motion yielding the depth information of the face to detect live person or motionless photo [5]. The disadvantages of depth information are that, firstly it is hard to estimate depth information when head is still. Secondly, the estimate is very sensitive to noise and lighting condition, becoming unreliable. Bruno et al presented a solution that works with both printed and LCD displayed photographs, even under bad illumination conditions without extra-devices or user involvement [6]. They performed number of tests on large databases that show good improvements of classification accuracy as well as true positive and false positive rates. G. kim et al has given a single image-based face liveness detection method for discriminating 2-D paper masks from the live faces [7]. In this still images taken from live faces and 2-D paper masks were found to bear the differences in terms of shape and detail. In order to effectively employ such differences, they exploit frequency and texture information by using power spectrum and Local Binary Pattern (LBP), respectively. An interactive approach was developed by Frischholz et al, requiring user to interact with the system by showing head movement [8]. Compared with photographs, another well-known characteristic of live faces is the occurrence of the non-rigid deformation and appearance change, such as mouth motion and expression variation. The accurate and reliable detection of these changes usually needs either the input data of high-quality or user collaboration. Jukka Matta et al used the micro texture analysis of face image for spoofing detection [9]. Kollreider et al applied the optical flow to the input video to obtain the information of face motion for liveness detection [10], but it is susceptible to photo motion in depth and photo bending. Some researchers use the multi-modal approaches of face-voice against spoofing [11], exploiting the lip movement during speaking. This kind of method needs voice recorder and user cooperation. With thermal infrared imaging camera, face thermogram could also be applied in liveness detection [12]. Besides, Li et al presented Fourier spectra to classify live faces or faked images, based on the assumption that the high frequency components of the photo is less than those of live face images [2]. The analysis of frequency spectrum of a live face is also being used by some researchers. They define two descriptors to measure the high frequency proportion and the temporal variance of all frequencies. Their method relies on both the lack of quality of a photograph and the change of pose in a live face. However, the above method will be defeated if a very clear and big size photo is used and there is no pose, expression change of user. Aruni et al has also provided a method of detecting a tempered face image detection based on second order gradient technique [13].

IV. PROPOSED WORK

In this paper, a new approach has been proposed to improve the system performance by using soft biometrics before the liveness detection in the face recognition system. The proposed approach (as shown in figure 2) works by first acquiring the facial image of the user using a sensor. Then, automatically extracting the soft biometric traits such as eye color, age, gender and ethnicity from that facial image. These extracted features are then compared with the existing database. If a match doesnot occurs then the user is rejected and no further processing takes place else the feature set of the face is extracted and template generated to compare it with the existing database. If the computed match score equals or exceeds the set threshold then the liveness is detected to finally authenticate the user otherwise the system denies the access and designates the user as an imposter.

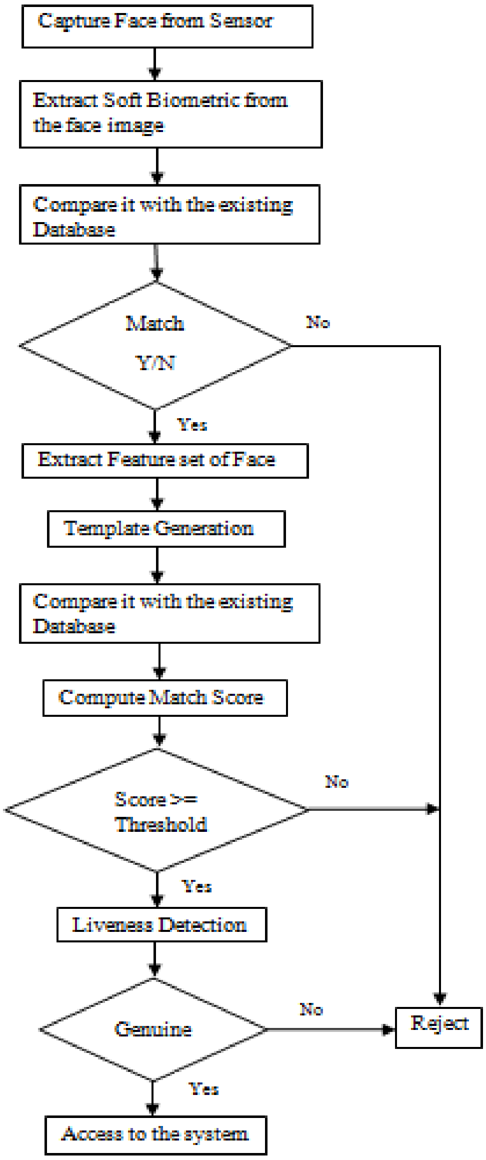

Fig 2: Flow Architecture of Proposed scheme

Algorithm for authentication in proposed scheme

```
1) Capture Face from Sensor
2) Extract soft biometric from the face image
3) Compare it with the existing database
4) If (soft trait feature matched)
5)          Extract feature set of face
6)          Generate template of feature set
7)          Compare it with the existing database
8)          Compute match score
9)          If (score >= threshold)
10)                  Apply Liveness detection technique
11)                  If (Identified as genuine)
12)                           Allow access to the system
13)                  Else
14)                           Reject user
15)                  End If
16)         Else
17)         Reject user
18)         End If
19) Else
20) Reject user
```

V. EXTRACTION OF SOFT BIOMETRICS

A mechanism should be there to automatically (without user intervention) extract the soft biometric features from the face image presented for the recognition [14]. This can be achieved by using a special system of sensors. For example, a camera can be used for obtaining the facial image of the user, which can be used to extract information like age, gender, eye color and ethnicity [15]. The information obtained from soft biometrics could then be used to decide whether the authentication process must be continued to detect the liveness in the sample or the user must be declared as imposter at this point of the algorithm. Several researches have been made to identify the gender, ethnicity and pose of the users from their facial images. The gender, ethnicity and pose of human faces are classified using a mixture of experts by radial basis functions [16]. This gender classifier classified users as either male or female with an average accuracy rate of 96%. Age determination is a more difficult problem because physiological or behavioural changes occur as the person moves from one age group to another [17]. No reliable biometric indicators have been developed for age determination yet.

VI. COMPARISON OF THE PROPOSED SCHEME WITH EXISTING TECHNIQUES

The proposed scheme presents a technique for liveness detection which uses the concept of soft biometrics. This technique ensures the detection of fake images and also verifies that the person is a legitimate user or not. But the traditional method does not use the concept of soft biometrics. Therefore, this method performs the liveness detection process even if the data is being presented by an imposter and hence is more time consuming. The main advantage of the proposed scheme is that if the person is found fake then it is detected at the soft biometric test module and the further computations are not performed. Hence, the performance of the system is improved.

VII. CONCLUSION AND FUTURE PROSPECTS

Spoofing is concerned with the security of the biometric system. Liveness detection can be used to detect a fake user by identifying the liveness of the sample being presented but is more time consuming and hence less efficient. Our proposed technique improves the performance of the liveness detection system by using soft biometrics at an early stage so that no system efforts are exhausted in ensuring the liveness of the sample being provided by an invalid user. Research in this area must be continued to develop a mechanism for automatic extraction of soft biometric traits.

REFERENCES

[1] Mayank Agarwal, Nikunj Jain, Mr. Manish Kumar and Himanshu Agrawal, “Face Recognition Using Eigen Faces and Artificial Neural Network”, IJCTE, Vol. 2, No 4, pp. 1793-8201, August, 2010.

[2] J. Li, Y. Wang, T. Tan, and A. K. Jain, “Live face detection based on the analysis of Fourier spectra,” In Biometric Technology for Human Identification, SPIE, Vol. 5404, pp. 296-303, 2004.

[3] S. A. C. Schuckers, “Spoofing and anti-spoofing measures”, Information Security Technical Report, Vol. 7, No. 4, pp. 56-62, 2002.

[4] Zhiwei Zhang, Dong Yi, Zhen Lei, Stan Z. Li, “Face Liveness Detection by Learning Multispectral Reflectance Distributions”, Automatic Face & Gesture Recognition and Workshops (FG 2011), IEEE, pp. 436-441, March 2011.

[5] T. Choudhury, B. Clarkson, T. Jebara, and A. Pentland, “Multimodal Person Recognition using Unconstrained Audio and Video”, International Conference on AVBPA, pp. 22-28, 1999.

[6] Bruno Peixoto, Carolina Michelassi, and Anderson Rocha, “Face Liveness Detection Under Bad Illumination Conditions”, Image Processing (ICIP), 18th IEEE Conference, pp. 3557-3560, Sep-2011.

[7] Gahyun Kim, Sungmin Eum, Jae Kyu Suhr, Dong Lk Kim, Kang Ryoung Park, Jaihie Kim, “Face liveness detection based on texture and frequency analyses”, Biometrics (ICB), 5th IAPR, pp 67-72, April 2012.

[8] R.W. Frischholz and U. Dieckmann, “BioID: A Multimodal Biometric Identification System”, IEEE Computer, Vol. 33, No. 2, pp.64-68, February 2000.

[9] Jukka Maatta, Abdenour Hadid, Matti Pietikainen, “Face Spoofing Detection From Single Images Using Micro-Texture Analysis”, Biometrics(IJCB), International joint conference, pp. 1-7, October 2011.

[10] K. Kollreider, H. Fronthaler and J. Bigun, “Evaluating liveness by face images and the structure tensor”, Fourth IEEE Workshop on Automatic Identification Advanced Technologies, pp. 75-80, Oct. 2005.

[11] G. Chetty and M. Wagner, “Multi-level Liveness Verification for Face-Voice Biometric Authentication”, Biometric Symposium, Baltimore, Maryland, Sep 2006.

[12] D. A. Socolinsky, A. Selinger and J. D. Neuheisel, “Face Recognition with Visible and Thermal Infrared Imagery”, Computer Vision and Image Understanding, Vol. 91, No. 1-2, pp. 72-114, 2003.

[13] Aruni Singh, Shrikant Tiwari and Sanjay Kumar Singh, “Face Tampering Detection from Single Face Image using Gradient Method”, International Journal of Security and Its Applications, Vol. 7, No. 1, pp. 17-30, January, 2013.

[14] X. Chen, P. J. Flynn, and K.W. Bowyer, “IR and Visible Light Face Recognition”, Computer Vision and Image Understanding, 99(3):332-358, September 2005.

[15] A. K. Jain, S. C. Dass, K. Nandakumar, “Can soft biometric traits assist user recognition?”, In Proceedings of SPIE International Symposium on Defence and Security, Biometric Technology for Human Identification, 2004.

[16] E. Erzin, Y. Yemez, and A. M. Tekalp, “Multimodal Speaker Identification Using an Adaptive Classifier Cascade Based on Modality Reliability”, IEEE Transactions on Multimedia, 7(5):840-852, October 2005.

[17] A. K. Jain, S. C. Dass, K. Nandakumar, “Integrating Faces, Fingerprints, and Soft Biometric Traits for User Recognition”, Proceedings of Biometric Authentication Workshop, LNCS 3087, pp. 259-269, Prague, May 2004.