Volume 3, Issue 5, May 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Fake Face Detection Based on Skin Elasticity

Dr. Chander Kant
Assistant Professor,
Department of Computer Science and applications
K.U. Kurukshetra, INDIA

Nitin Sharma
M.Tech. Student,
Department of Computer Science and applications,
K.U. Kurukshetra, INDIA

Abstract*— Biometric system provides a way of automatic verification or identification a person. But nowadays due to lack of secrecy, 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. Liveness detection is a technique that can be used for validating whether the data originate is from a valid user or not. Liveness detection can be hardware based or software based or a combination of both. In this paper, we present a non intrusive and real time method to address this problem, based on skin elasticity of human face. In this technique user is asked to do some movement like chewing and forehead movement simultaneously, so that a full movement to face skin can be given and then sequence of face images is captured with a gap of few milliseconds. Then by applying correlation coefficient between images and then discriminate analysis using some method, face skin is discriminate from the other materials like gelatin, rubber, cadaver, clay etc. In comparison to other face liveness detection, this method will be much user friendly. On the other hand, one of the images captured for liveness detection can be used for face recognition.

Keywords*— Biometrics, Face Recognition, Fake Face Detection, Liveness Detection, Skin Elasticity,

I. INTRODUCTION

Face recognition is a process of identifying and verifying a person by recognizing his face. Face recognition has become an important issue in many applications such as security systems, credit card verification, criminal identification etc [1]. One of the negative implications of increased technological advancement is the ease with which, one can spoof into a biometric identification system. The increase of attack using fake biometric reduces reliability and security of biometric system. Because general biometric algorithms cannot be able to differentiate 'live' biometric from 'not live' biometric, the research on liveness detection is highly desirable, yet rather unexplored anti-spoofing measure in biometric identity authentication [2]. In face recognition, the usual attack methods may be classified into several categories. The idea of classifying is based on what verification proof is provide to face verification system, such as a stolen photo, stolen face photos, recorded video, 3D face models with the abilities of blinking and lip moving, 3D face models with various expressions and so on [3]. To resist these attack methods, a successful live face detection system should have one or more anti-imposture abilities to expose them. The vein map of the faces using ultra-violet cameras is a most secure method of identifying a live individual, but it needs special expensive devices.

In this paper, a novel approach of liveness detection based on skin elasticity is proposed. In which a set of face images, as in fig 1 is shown, is captured after asking the user to do some face movement activities. Then correlation coefficient is calculated and images are discriminate using some discriminant analysis. Since this approach is software based, so it will be less cost method for liveness detection.

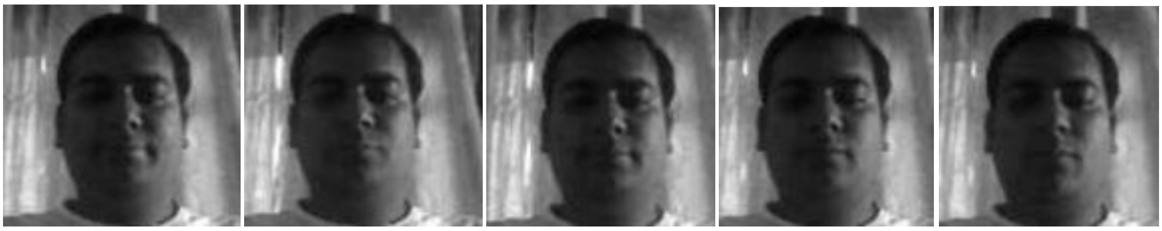

FIG 1 SET OF FACE IMAGES CAPTURED IN AN INTERVAL OF FEW MILLISECONDS

In section II some related work done in this field is discussed. Then in the next session, proposed method of liveness detection is given base on skin elasticity and in last section conclusion is described.

II. LIVENESS DETECTION IN FACE RECOGNITION

In a biometric system there are three ways for introducing liveness detection:

A. Using extra hardware: This approach is an expensive approach. In this approach extra hardware is used to acquire the life signs.

B. Using software: In this approach some software is used to classify the fake and real images. It is done at processing stage.
C. Using combination of hardware and software: in this approach a combination of hardware and software is used to classify the fake and real images.

In these approaches first approach is an expensive but fast approach. Second approach is relatively less costly but takes much time in comparison to first. Last approach is a combination of these two so it is expensive as well as time consuming. But it provide a good high end solution for livens detection which is difficult to breech.

Before dealing with this, we will know about way of spoofing Face recognition system can be spoofed by three ways:

A. Photograph of a valid user
B. Video of a valid user
C. 3D model of a valid user

Some examples of the fake face image are shown in the figure 2. In this example, faces made of material like silica gel, rubber, photo and video replay are shown [4]. In general, fake faces have two main properties:

A. Large variations. Although the positive class, namely the genuine face, has limited variation (all genuine faces are human skins), the negative class, i.e., the fake faces, can range from photos, videos to masks and so on. When it comes to material level, the variety is even larger: take face mask for example- there are rubber mask, plastic mask, silica gel mask, etc. It’s almost impossible to give a complete list. Some examples of fake faces are shown in Fig.2.

B. Indistinguishable under visible light. Fake is, by its definition, indistinguishable for human eyes. Therefore, without extra aid, only visual face images are insufficient and impossible for the detection of fake faces.

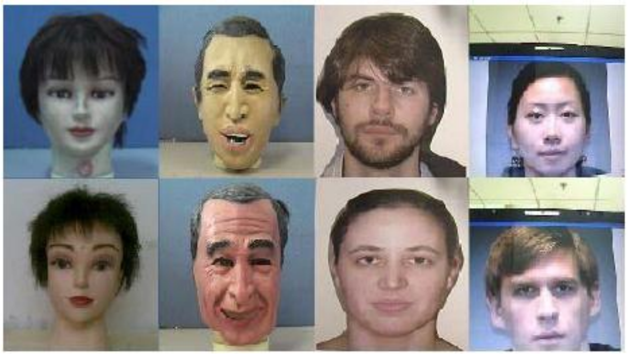

Fig 2: Some Fake face examples. Materials from left column to right are:
silica gel, rubber, photo and video replay

Two of the most important challenges nowadays refer to: (1) the need of designing and deploying non-intrusive methods without extra devices and human involvement; and (2) designing detection methods robust to changes in pose and illumination. 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 still 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 conducted no 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 is tried by Frischholz et al, requiring user to act an obvious response of head movement [8]. Compared with photographs, another prominent characteristic of live faces is the occurrence of the non-rigid deformation and appearance change, such as mouth motion, 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 uses the micro texture analysis of Face Image for spoofing detection [9]. Kollreider et al applies the optical flow to the input video to obtain the information of face motion for liveness judgments [10], but it is vulnerable 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 collaboration. With thermal infrared imaging camera, face thermo gram also could be applied in to 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 [13]. Some uses the analysis of frequency spectrum of a live face. 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. In another work Aruni et al. has provide a method of detecting a tempered face image detection based on second order gradient technique[14].

These anti-spoofing clues, in terms of quality, Hardware and user collaboration have been summarized in table 1.

Table 1: COMPARISON OF ANTI-SPOOFING CLUES FOR FACE RECOGNITION

Clues	Data Quality	Additional Hardware	User Collaboration
Facial Expression	High	No	Middle
Depth Information	High	No	Low
Mouth Movement	Middle	No	Middle
Head Movement	High	No	Middle
Eye Blinking	Low	No	Low
Degradation	High	No	Low
Multi-Modal	-	Yes	Middle/High
Facial Thermogram	-	Yes	Low
Facial Vein Map	-	Yes	Middle
Interactive response	-	No	High

III.PROPOSED WORK

When a user stands in front of camera, user is asked to do some activities like chewing and forehead movement simultaneously. Using flowchart a complete illustration of process is shown. Then at the same time camera captures a sequence of face images at a certain frame rate. For example, when the frame rate is 20 fps (frames per second) and the capturing duration is 1.5 second, the image number of every sequence is 30.

In this method, firstly user is asked to do some simple mouth movement activities like chewing, forehead movement etc simultaneously. At the same time a set of face images is captured. Then after applying pre-processing techniques, feature extraction is done using correlation coefficient and image extension feature. Using some discriminant analysis method, images are discriminate and skin elasticity is calculated. Then output is compared with the stored database. If output is less than the stored value then image captured is a fake image else it is a real image.

Since age factor plays a significant role in skin elasticity so threshold value can be according to ages. On the other hand, age can be used as a soft biometric for classifying the face database. In this method user intervention is minimum, so it will provide a very good non intrusive solution against fake faces. On other way it is a user friendly method, so its acceptance criteria among users will be more. Also as it is a software base liveness detection method so it will be easily applicable on all pre-established face database.

A. Proposed Algorithmic Approach:

Step 1. Request the user to perform live activities like chewing, smile, forehead movement etc.
Step 2. Now capture a sequence of face images with a gap of few milliseconds.
Step 3. Perform correlation coefficient method on set of sequence of face images.
Step 4. Perform “Discriminant Analysis” method like “Fisher linear discriminant Analysis” on the set of images.
Step 5. Calculate the skin elasticity value and compare it with stored database.
Step 6. If output is below threshold value then the image captured is “Fake Image”.
Step 6. Else if output is greater than threshold value, then the image captured is from live person.
Step 7. Now perform face recognition process.

B. Flowchart for above proposed algorithm has been shown in figure 3.

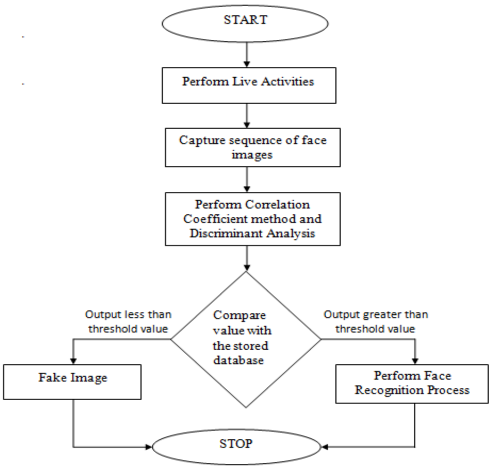
START
Perform Live Activities
Capture sequence of face images
Perform Correlation Coefficient method and Discriminant Analysis
Compare value with the stored database
Output less than threshold value
Output greater than threshold value
Fake Image
Perform Face Recognition Process
STOP

Fig 3 Flowchart of different phases of proposed work

IV. CONCLUSIONS

Spoofing is the real concern with regard to the security of the biometric system. In this paper we have discussed face liveness detection, in which spoofing can be controlled in a smart way. In this paper, a novel approach of liveness detection based on skin elasticity is proposed. In which a set of face images is used for liveness detection based on their correlation coefficient and their discriminant analysis. Since it requires a less user intervention, so it will be more user friendly and acceptable among no of users.

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, Aug-2010

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

[3] 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.

[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), 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), 2011 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),2012 5th IAPR, pp 67-72, April 2012

[8] Frischholz, R.W. & Dieckmann, U. (2000). 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), 2011 International joint conference, pp. 1-7, October 2011

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

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

[12] Socolinsky, D.A.; Selinger, A. & Neuheisel, J. D. (2003). Face Recognition with Visible and Thermal Infrared Imagery, Computer Vision and Image Understanding, vol.91, no. 1-2, pp. 72-114, 2003

[13] Li, J.; Wang, Y. & Tan, T. & Jain, A. (2004). Live Face Detection Based on the Analysis of Fourier Spectra, Biometric Technology for Human Identification, Proceedings of SPIE, Vol. 5404, pp. 296-303, 2004

[14] 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