IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727

Liveness Detection for Face Recognition in Biometrics: A Review

Meenakshi Saini[1], Dr. Chander Kant[2]
[1,2](Department Of Computer Science and Applications, Kurukshetra University, Kurukshetra, India)
([1]minakshisaini26@gmail.com, [2]ckverma@rediffmail.com)

ABSTRACT : *A Biometric system recognizes an individual by measuring or analyzing his physical or behavioral body traits. In recent times, Facial recognition is one of the most commonly used biometric technology and is rapidly integrated in various applications such as security login or access to the buildings or surveillance etc. Facial recognition is also user friendly and cost effective solution than other technologies. Beside this, Face recognition system is also prone to the spoofing attacks such as placing photographs,playing video clips in front of camera and dummy faces.In order to guard the system against such spoofing attacks,liveness detection can be integrated into the system. Liveness detection in face recognition tests whether the face presented to the system is real face or a fake face.This paper presents the state-of-the-art of various liveness detection techniques in the area of face recognition technology along with their strengths and limitations.*

Keywords – *Face recognition, Liveness detection, Face spoofing, Biometrics*

I. INTRODUCTION

In modern scenarios, Biometrics is the need of almost all the security systems whose functionality depends upon the accurate recognition of an individual such as secure money transactions, granting access to shared networked resources etc. The primary reason for this is that unlike traditional methods of security such as ID cards or passwords, biometric data can't be easily forgotten, hampered, lost or stolen.[1] Biometrics is a technology of identifying or verifying a person by measuring or analyzing his body traits. These traits can be further classified into physical traits such as: fingerprint, face, retina, iris etc. and behavioral traits such as voice, signature, gait etc. These traits are also called biometric modalities, identification technologies or characteristics.

Among all these identification technologies, Face recognition technology is the one that has been recently evolved and it is more user friendly, cost effective and convenient solution than other recognition technologies. [2] Therefore face recognition technology has been integrated as a security component in most of the authentication systems. A Face recognition system recognizes an individual from a digital image or a video frame from a video source. In face recognition applications, the first step is to acquire the facial image of user from camera and at the second step, face is detected from the acquired image [3] and it can also be normalized or enhanced. At the third step, face recognition process takes place in which the desired facial features are extracted and then these extracted features are matched against the features stored in the database and finally, the output of face recognition process is used (if there is a match or not) to determine the identity of the person as shown in Figure 1.

However, the major challenge faced by most of the authentication systems [4] is the theft of identity or spoofing. There are various levels of spoofing attacks such as placing fake biometrics on sensor, replay attacks, attacking the enrollment database, corrupting the matcher and decision module or attacking the application etc. A face recognition system can also be spoofed easily because face recognition [5] algorithms don't have a mechanism to differentiate a live face from a fake (non real) face. A face recognition system can be spoofed by placing photographs or playing video recordings in front of camera and presenting dummy faces. Figure 2 shows the non real faces that are made of materials like silica gel, rubber, photo and video replay respectively. To avoid such problems, liveness detection technique is generally integrated just before the face recognition process which verifies whether the facial image presented to the authentication system is alive or has been reproduced synthetically or fraudulent. Liveness detection differentiates between a live feature set and non live feature set of face. Liveness detection is an active research area in fingerprint, face or iris recognition. With the help of liveness detection, the performance of a biometric system can be improved significantly.

This paper is organized as follows, section II gives the architecture of a face liveness detection system, section III gives review of related work, section IV describes the discussion and comparison of various face liveness detection techniques and finally the conclusion of the work is explained.

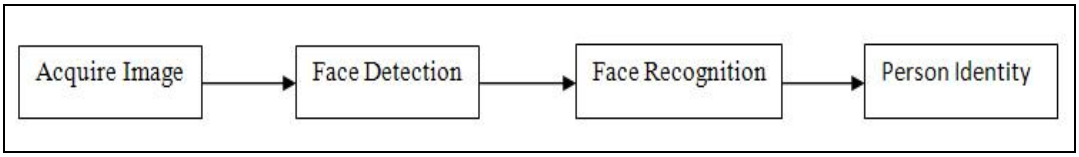

Fig. 1: Various steps in face recognition process

Fig. 2 : Examples of non real faces. From left to right columns, faces are made of silica gel, rubber, photographs and video replays respectively. [7]

II. ARCHITECTURE OF FACE LIVENESS DETECTION SYSTEM

Liveness detection process ensures that only live biometric samples will be processed for biometric identifications, whereas the non live samples are automatically rejected. In biometric recognition systems, there are three ways of introducing liveness detection: i) By using extra hardware to acquire the life signs, however, this is an expansive but fast method, ii) Using some software to acquire the life signs at the processing stage but it takes comparatively more time than the first method and iii) combination of both hardware and software. Various intrinsic properties of human body such as reflectance, resistance, absorbance, texture etc. and involuntary signals [6] of human body such as blood flow, pulse etc. can also be used for detection of life signs.

The basic components of a face liveness detection system are shown in Figure 3. Typically a face liveness detection system consists of following basic components:

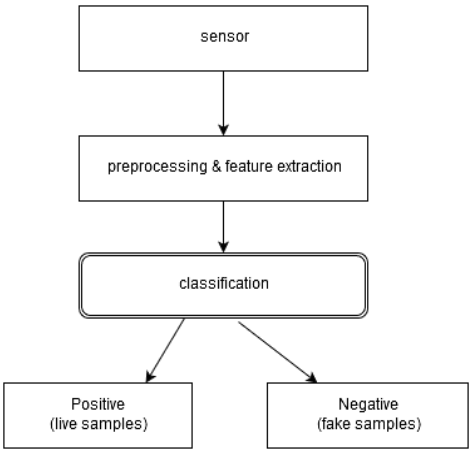

Fig. 3: Architecture of a Face Liveness Detection System

a) Sensor

Sensor is used to acquire the facial image of the user. e.g.: visible light camera, thermal camera, 3D sensors etc.

b) Preprocessing and feature extraction

Preprocessing involves removal of noise from the acquired image and to improve the visual quality of an image. Various techniques of preprocessing are: blurring, sharpening, edge detection or scaling etc. After

preprocessing, the samples are forwarded to the feature extraction module so that various salient features of face can be extracted to differentiate the live feature set from the spoofed feature set [7]. Various techniques of feature extraction are: local binary patterns (LBP), correlation coefficient and discriminative analysis etc.

c) Classification

Liveness verification is performed by matching the queried feature sets against their respective feature sets which are stored in the database during the enrolment phase. After matching, a binary response is generated which represents the status of liveness verification as live samples or the rejected spoofed samples.[8] Various examples of classifiers that can be used are: SVM classifiers, binary classifiers, Hamming distance, Manhattan distance, weighted fusion, difference degree calculation etc.

III. RELATED WORK

There are various approaches implemented in the face liveness detection systems. Basically, there are two types of approaches: Intrusive and Non-intrusive as shown in Figure 4. In the intrusive approach, system asks the user to perform some actions such as smiling, chewing, rotating head in a particular direction etc. On the other hand, there is no involvement of user in the non-intrusive approach. No user response is required.

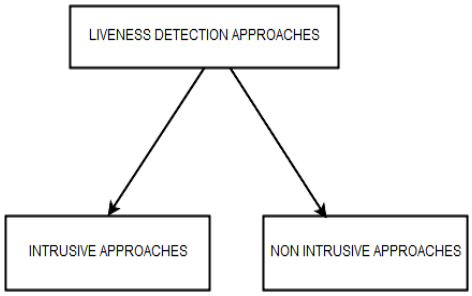

Fig. 4: Types of Liveness Detection Approaches

- Intrusive Liveness Detection Approaches

User response is required in the intrusive liveness detection approaches. Various kinds of intrusive approaches are presented in literature review and are explained below:

Frischholez and Werner in [9] have proposed an approach in which the user has to rotate his head in a particular direction on the basis of randomly generated instructions by the system. He proposed a pose estimation algorithm that compares the user movements with the respective instructions. This method is resistant to both photo and video replay attacks. The main disadvantage of this approach is that it is time consuming, cumbersome and the user attention is necessary.

Another approach proposed by Kollreider et al. in [10] is based on the lip movement. In their approach, user has to utter a random sequence of digits from 0 to 9 and his lip movement is recorded and then recognized sequentially.SVM classifier is used for classification of lip movements. This technique needs no preprocessing, hence less computation is required. Limitation of this approach is that it is without audio recording; therefore the system can be attacked by video or a sequence of photographs.

Chetty et al. in [11] proposed an approach for liveness detection which was based on cross modal fusion. The fusion of acoustic and visual speech correlation features were carried out. Voice and lips were extracted from the video and their degree of synchronization was measured. This approach removed the limitation of previous approach proposed by Kollreider in [10] and is resistant to both photos and video replay spoofing attacks.

The combination of one or more biometric traits can be integrated into the system to enhance the security of facial biometric systems. Chetty and Wagner in [12] proposed a framework of multilevel liveness verification which used the voice and face biometric traits and their relationships.

Likewise, Dr. Chander Kant et al. in [13] proposed a method based on fusion of elasticity and thermal imaging. In this approach user is asked to smile or chew or move forehead etc., then correlation coefficient and linear discriminant is applied on the facial image and then elasticity is computed. A thermal sensor is also used.

This approach was effective against both 2D photo attacks and video replays. This approach is affected by the effect of age factor on skin elasticity and use of extra hardware i.e. thermal sensor is also required.

- Non-intrusive liveness detection approaches

In non intrusive approach, various facial skin properties such as eye blinking, skin texture analysis, skin elasticity and thermography is used to detect life signs from the face of user. No user collaboration is required in these approaches. Techniques against photo spoofing attacks are based on the fact that photographs have 2D planar structure which is quite different from the live face having 3D structure.

Choudhry et al. in [14] has proposed an approach based on the structure from motion which yields the depth information of various features of face. Main drawback of this method is that it is difficult to estimate the in-depth information when the head is still and also, this method is sensitive to noise.

Lagorio et al. in [15] proposed an approach based on the properties of 3D structure of live face and a 3D scanner was used for this purpose. System cost is increased in this method because it requires an expensive 3D optoelectronic sensor.

Bao et al. in [16] has proposed a method of liveness detection which is based on optical flow fields. It was analyzed that there was a difference in optical flow fields generated by 2D planar objects and 3D objects. Various properties of translation, rotation, swing, moving forward and backwards were taken into account. This method was affected by illumination changes, sensitivity to background etc.

Lin Sun et al. in [17] proposed an approach for liveness detection based on blinking of an eye. Eye blinking is an operation of two continuous sub operations i) from opening to closing and ii) from closing to opening. They have used CRF (conditional random fields) model such that yt =X= {1, 2, .C}, t= {1, .T} and observations xt. C stands for closed state and NC stands for non closed state as shown in Figure 5.

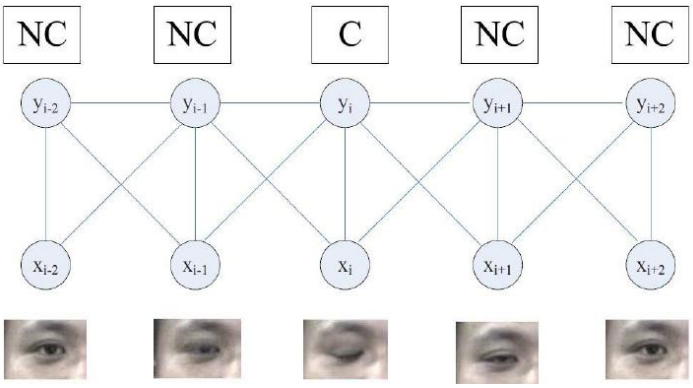

Fig. 5: CRF based eye blinking model [17]

Li et al. in [18] has proposed a method based on Fourier spectra. It was analyzed that live face has more number of frequency components than a fake image.

Another method is based on the texture analysis which was proposed by Kim et al. in [19]. In this method Local binary pattern (LBP) was implemented to analyze the texture pattern of facial images. Basic operation of LBP calculation is shown in Figure 6. It is a simple but effective texture operator. Another technique was proposed by Hadid et al. in [20] which was based on the micro texture analysis of facial image using LBP. It was based on analyzing the micro texture patterns in the live or fake facial image.

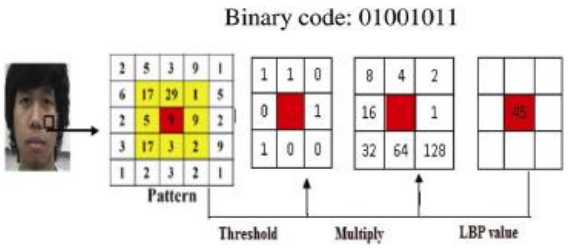

Fig. 6: Basic LBP texture operator calculation using threshold value=9 [19]

IV. DISCUSSION

From the reviewed literature work, it has been found that intrusive approaches are limited because these techniques are dependent upon the user involvement such as head movement, smiling etc. Non intrusive approaches are cost effective and user friendly than the intrusive approaches since they don't need any kind of user interaction.

There are three types of liveness indicators or clues: motion, texture and life sign. Various types of liveness indicators and their comparisons are shown in Table 1. First indicator is texture based analysis that works on the fact that faces printed on the paper produce higher frequency texture patterns than real face images. These methods are low cost, need no user interaction and they can be easily implemented. The main disadvantage of this method is that it can suffer from low texture attacks. Attack can be performed by using a photograph that produces very low texture information.

Motion based analysis, differentiates between the motion pattern of 2D and 3D faces. It is very difficult to spoof 2D face images in this method. Motion analysis needs video so it must be of high quality. It is a medium, cost intrusive and texture independent method. However, the method can suffer problem when there is low motion information. Illumination can also affect the system performance.

Life sign indicators are based on analyzing the life signs from the face of user such as eye blinking. They are texture independent and very hard to spoof. Cost of such systems is relatively high because they need additional hardware but these systems have a better performance but it may need user collaboration. These approaches generally focus on face part detection.

TABLE I

COMPARATIVE ANALYSIS OF VARIOUS LIVENESS DETECTION APPROACHES

Liveness indicators	Cost and method	Advantages	Disadvantages
1. Texture	Low cost, Non intrusive method	1. Simple implementation, 2. No user collaboration needed	1. Low image or video quality 2. Low textual attacks 3. Need diverse datasets
2. Motion	Medium cost, Intrusive Method	1.Texture independent 2. Hard to spoof 3. No user collaboration needed	1. Needs high quality data 2. Needs video 3. Difficult to use when Low motion information 4.Illumination problem
3. Life signs	High cost, Both intrusive(e.g. some motion activity on face) & Non intrusive(e.g. eye blinking)	1. Texture independent 2. Cover all attacks 3. Good performance under bad illumination conditions	1.Need extra hardware or 2.Sensor needs videos and may need user collaboration

V. CONCLUSION

This paper provides an overview of various liveness detection techniques implemented for face recognition. It may be concluded that there is a need of designing non intrusive approaches that uses no extra hardware and are able to guard the system against 2D photograph attacks, video replay attacks and the dummy faces. More life signs can be added in the liveness testing to improve the performance. The biggest challenges to the face recognition technology today is: i) The need of designing non intrusive techniques without using extra hardware and human interaction and ii) designing liveness detection techniques that are robust to change in pose and illumination. No system is completely free from spoofing however anti spoofing techniques simply makes it hard to attack the face biometric systems by the intruders. Hence, more user friendly, cost effective and more efficient approaches for liveness detection in face recognition are needed in future.

REFERENCES

[1] Anil Jain, Lin Hong and Sharath Pankanti, Biometric Identification,*white paper in Communications of the ACM*,43(2),February 2000.
[2] Anil K. Jain, Arun A. Ross, Introduction to Biometrics, *Handbook of Biometrics, Springer,* New York, USA, 2008.
[3] Anil K. Jain, Arun A. Ross and Salil Prabhakar, An Introduction to Biometrics Recognition, *IEEE Transactions on Circuits and Systems for Video Technology, Special issue on Image- and-Video-Based* Biometrics,14(1), January 2004.
[4] Chris Roberts, Biometric Attack vector and Defenses, Elsevier computers & Security, 2007, 14-25.
[5] Emanuela Marasco and Arun Ross, A Survey on Anti-Spoofing Schemes for Fingerprint Recognition Systems, *ACM Computing, 47(2),* Sept 2014, 1-36.
[6] Dr. Chander Kant and Nitin Sharma, Fake face detection based on skin elasticity, *International journal of advanced research in computer science and software engineering,3(5),*May 2013.
[7] Sajida Parveen, Sharifah Mumtazah Syed Ahmad, Marsyita Hanafi and Wan Azizun Wan Adnan, Face anti-spoofing methods, *Current science,108(8),* April 2015.
[8] Saptarshi Chakraborty and Dhrubajyoti Das, An overview of face liveness detection, *International journal on information theory, 3(2),* April 2014.
[9] Frischholz, R. W. and Werner, A., Avoiding replay-attacks in a face recognition system using head-pose estimation, *IEEE International Workshop on Analysis and Modeling of Faces and Gestures(AMFG'03)*, 2003,234–235.
[10] Kollreider, K., Fronthaler, H., Faraj, M. and Bigun, J.,Real time face detection and motion analysis with application in liveness assessment, *Trans. Infor. Forensics and Security, IEEE,* 2007, 548–558.
[11] Chetty, G., Robust audio visual biometric person authentication with liveness verification, Intel Multimedia Analysis for Security *Appl. SCI 282, Springer,* 2010, 59–78.
[12] Chetty, G. and Wagner, M., Multi-level liveness verification for face-voice biometric authentication,*Biometrics Symposium,* Baltimore, Maryland, 19–21, September 2006.
[13] Dr. Chandar Kant and Nitin Sharma, Fake face recognition using fusion of thermal imaging and skin elasticity, *IJCSCIJ, 4(1),* 2013, 65–72.
[14] Choudhury, T., Clarkson, B., Jebara, T. and Pentland, A., Multimodal person recognition using unconstrained audio and video,*International Conference on Audio- and Video-based Biometric Person Authentication (AVBPA'99),* Washington DC, 1999, 176–181
[15] Lagorio,A.,Tistarelli,M., Cadoni, M., Fookes,C., Clinton,B. and Sridha, S., Liveness detection based on 3D face shape analysis,*Proceedings of the 2013 International Workshop on Biometrics and Forensics (IWBF), IEEE,* Lisbon, Portugal, 2013,1–4
[16] Bao, W., Li, H., Li, N. and Jiang, W.,A liveness detection method for face recognition based on optical flow field. , *IEEE International Conference on Image Analysis and Signal Processing IASP,* 2009, 233–236.
[17] Lin Sun, Gang Pan, Zhaohui Wu and Shihong Lao, Blinking-Based Live Face Detection Using Conditional Random Fields, ICB 2007, Seoul, Korea, *International Conference,*252-260,August 27-29, 2007.
[18] Li, J., Wang, Y., Tan, T. and Jain, A. K., Live face detection based on the analysis of Fourier spectra, *Proceedings of Article SPIE 5404, Biometric Technology for Human Identification,* 25 August 2004,296–303.
[19] G. Kim, S.Eum, J. K. Suhr, D. I. Kim, K. R. Park, and J, Kim, Face liveness detection based on texture and frequency analysis, *5th IAPR International Conference on Biometrics (ICB),* New Delhi, India, March 2012,67-72.
[20] Maatta, J., Hadid and A. and Pietik ,Face spoofing detection from single images using micro-texture analysis, IEEE, Washington, DC, 2011, 1–7.