IJCSC VOLUME 5 • NUMBER 2 JULY-SEPT 2014 PP. 134-137 ISSN-0973-7391

Towards more security in biometric system using Liveness Detection

Shiwani Goyal
Asst. Professor, Department of Computer Science, DAV, College, Yamuna Nagar

Abstract: With the advancement of technology, security has become the need of the hour for every system. Traditional security schemes like cryptography solve this issue to a great extent but still the security relies on size of secret keys. As the size of secret key increases the level of security also advances. The infeasibility to remember the large sized secret key is a problem for the users. To tackle this problem biometric System are used. Biometric System work on the principle of recognizing individuals based on their physiological and behavioral characteristics. Hence, any biometric recognition system requires a human trait. But what if these traits are artificial? i.e. the biometric traits are made up of silicon, gelatin, play-doh etc. With the widespread deployment of biometric systems in various applications, there are increasing concerns about the fraudulent attacks. Liveness detection is a solution to the above mentioned concern. Here in this paper, we focus on various biometric traits on which liveness can be performed and further how it can be performed.

1. Introduction

Biometric system uses physical and behavioral characteristics of an individual which are considered to be private and secret. But this is mere a dilemma as the biometric information which consists of fingerprints, voice pattern and iris etc are considered to private but they cannot be assumed as secret. As whenever we enter a shopping mall or a metro station our facial images are recorded. Even when we use any phone driven application our voice patterns are recorded. Fingerprints and DNA are recorded by anything we touch for e.g. a cup in which we had tea at neighbors home or door by which we enter our own home, office etc. It not even hard but impossible to keep a track of the number of things touched by us or number of call we made to different numbers etc. To consider that our biometric information will not be captured by an intruder for spoofing is playing with the security of any system where biometric information will be used. But the availability of facial images, fingerprints, voice patterns and DNA etc. in public can not be restricted. Thus it is acceptable that biometric technologies using fingerprint, facial images, iris, voice pattern etc are sensitive to spoofing attacks [1]. These biometric identifiers can be copied and used to destroy many existing biometric systems. Therefore the challenge is to find the biometric traits on which effective liveness detection can be performed and its mechanism. Liveness detection denotes the methods capable in discriminating real human traits (live or non live) from synthetic human traits made by silicon, gelatin or play-doh etc. It is difficult to perform lives test for open network where system operators can not control end user terminal and transmission channels. There are two types of spoofing attacks i.e digital or physical as shown in figure 1.

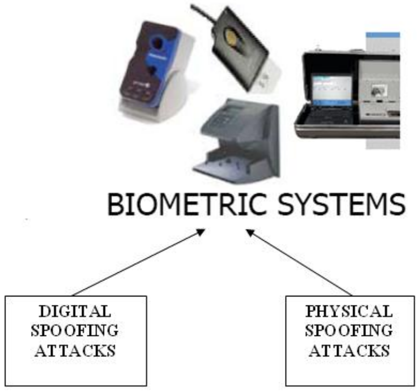

Figure 1: Types of spoof attacks in biometric systems

Digital attacks are defended against by authenticating the biometric reader sending the data and eliminating vulnerable data path [2]. In Physical attacks a clone is presented instead of legitimate user in order to gain access to biometric system. In this paper we will deal with physical spoofing attacks on various biometric traits.

Rest of the paper is organized as follows. Section 1 presents the importance of security of biometric system and importance of liveness detection on various biometric traits. Section 2 refers to the various biometric traits on which liveness detection is affective. Section 3 deals with mechanism by which liveness of biometric traits can be detected. Finally articles conclusion and future scope is presented in section 4.

2. Biometric Traits

Biometric traits are the human characteristics (physiological or behavioral) used by biometric based application like identity access management, access control, surveillance etc. The physiological traits are related to shape of the body for e.g. fingerprint, DNA, iris, face etc. and the behavioral traits are related to behavior of an individual for e.g. gait, voice, signature etc. The classification of biometric traits is well described in figure 2.

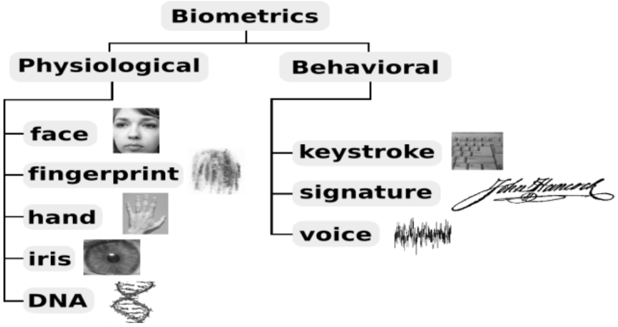

Figure 2 Classification of biometric traits

Liveness detection of biometric traits can take place either at acquisition stage or at processing stage. There are three ways in which it can be implemented in the system [3].

1. By adding extra hardware.
2. By using information already captured by the device.
3. By using liveness information inherent to the biometric in question.

All the three ways have their own advantages and disadvantages that we shall not discuss in this paper. Our concern lies in those biometric traits for which effective liveness detection can be performed by using any of the three mentioned ways. The biometric traits on which liveness testing can be done are fingerprint, iris, voice, face, hand and palm geometry. The mechanisms for liveness detection of these traits are explained in the section 3.

3. Liveness Detection

The schemes of liveness detection in biometric system depend upon the type of biometric trait. Largely liveness detection is covered under three categories as shown in figure 3.

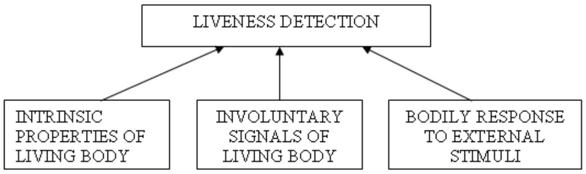
LIVENESS DETECTION
INTRINSIC PROPERTIES OF LIVING BODY
INVOLUNTARY SIGNALS OF LIVING BODY
BODILY RESPONSE TO EXTERNAL STIMULI

Figure 3: Categorization of Liveness Detection

1. **Intrinsic Properties of Living body –** This category includes thermal, electrical, optical, visual and body fluids properties. Liveness of any biometric traits can be detected using these intrinsic properties.
2. **Involuntary Properties of Living body-** Blood flow, precipitation, pulse, blood pressure, brain wave signal, electric heart signal and hippus are the examples of involuntary properties of living body. These properties are utilized for liveness detection and are known as dynamic liveness detection.
3. **Bodily Response to External Stimuli-** Finally bodily response to external stimuli can also be used for liveness detection. It requires user involvement for e.g. asking the user to blink the eyes, smile, show his/her various facial profiles etc. It is also dynamic scheme of liveness detection.

Finally we should state the mechanism used for liveness detection of biometric traits

1. **Fingerprint-** Liveness detection of fingerprint can be mainly performed using intrinsic properties i.e. by using touch less optical imaging from TBS and ultrasound imaging from ultra scan cooperation [4]. Also Electrical resistance can be used for the same purpose but this scheme is not that effective as liveness detection can be fooled by gummy cloned fingers. Precipitation patterns, pulse measurement can also be used for the same purpose.

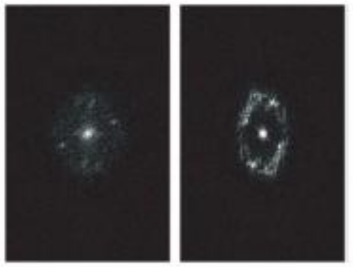

Figure 4: Computation of energy concentration in the power spectrum for two fingerprints of different quality

2. **Iris-** Iris liveness detection can be performed on the principle of red eye effect. This principle is effective when angle between light source, eye and camera is less than 2.5 degrees. Even involuntary property "hippus" can be used for live iris detection. Also user can be asked to blink the eyes and changing the level of illumination results in change of the size of pupil. This is a bodily response type of liveness detection.
3. **Face –** The best method for live face detection is based on bodily response to external stimuli. The user can be asked to show various profile

of his face at sensor. Image acquisition is another method which depicts the change in confidence level of a person than a dummy face. Involuntary properties involving pupil change, light level and response of muscles are also some of the documented methods.

4. Voice- Dynamic liveness is most effective method for liveness detection of this trait. In this we can match lip movement of the trait to that earlier recorded for verification. Also asking user to speak sentences and digits in varying speed help to detect spoof at identification.

Thus Liveness detection is a method to overcome spoof attack but still various biometric traits are present on which liveness detection cannot be performed.

4. Conclusion & Future Work

Security of biometric system from fraudulent attacks is the biggest challenge in front of us. With the advancement of technology, spoofing attacks are also increasing at an alarming rise. In this paper we have discussed Liveness detection which is a way in which spoofing can be controlled. But Liveness detection is not affective for all biometric traits. Even the extra hardware cost, user inconvenience and matching accuracy required for liveness detection need to be addressed. Also Liveness detection and multi-modal biometric system is still to be discovered. Both industries and academia should continue working in this direction to find more antispoofing techniques such that there is rise in difficulties for such types of attacks. Also, Research should be made to find more number of biometric traits which can undergo effective and feasible liveness detection and we will continue working in this area and come out with commercially accepted liveness detection schemes for more traits in near future.

References

1. T.Matsumoto, H.Matsumoto, K Yanada, S.Hoshino, “Impact of artificial ‘gummy’ fingers on fingerprint systems, Proceeding of SPIE, Vol 4077, January 2002.
2. West Virginia University, Biomedical Signal Analysis Laboratory, Spoofing Fingerprint Devices”. http:// people.clarkson.edu /~ biosal/research/spoofingfingerprint.html.
3. L. Thalhein, J.Krisseer, P-M. Ziegler, “Body check biometric access protection devices and their programs put to the test, c’t Magazine 11/2002. http://www.heise.de/ct/english/02/11/11
4. Boritoth, Deloitte, Biometric liveness detection, Information security bulletin,October 2005.
5. Javier Galbally, Frenando Alonso-Fernandez, Julian Fierrez, and Javier Ortega – Garcia.” Fingerprint Liveness Detection based on Quality measures.