International Journal of Applied Science and Advance Technology (ISSN: 0973-7405)
Dec 2013, Vol. 2, No. 1, pp. 64-67

Making Biometric System more secure with Liveness Detection

Garima Yadav, Nikita Yadav
Research Scholar, School of Computer Science & IT, Singhania University,Rajasthan
garima.aky@gmail.com, aquanikita12@gmail.com

Abstract: Traditional user authentication/verification systems mostly rely on knowledge; like password or smart card. But they are not able to meet strict security performance of today's computer applications. That's why now biometrics-based authentication systems are good alternate to these traditional authentication methods. Biometric system works on the principle of recognizing individuals on the basis of their physical and behavioral characteristics. As biometric data cannot be lost or forgotten so biometric system is more reliable and user-friendly. However this widespread acceptance of biometrics technology also attracting the attention of attackers. Attackers for cracking biometric system security trying to use the artificial biometric trait, which are made up of silicon, gelatin etc. These synthetic biometric has same characteristics as of original biometric trait. So now biometric system required more secure system which able to differentiate between real and fake biometric. It can be done by liveness detection techniques. In this paper we are discussing some techniques for liveness detection for various biometric systems.
Keyword: Liveness detection, fingerprint, iris.

1. Introduction

Biometric is defined as an automated method of verifying or authenticating the identity of a living person on the basis of physiological or behavioral characteristics [1]. Biometric authentication uses biometric constraints which are taken from given user, like fingerprints, faces, irises etc. to identify individuals. Such data is unique for every individual. While many research has been done both to determine which traits can differentiate humans and for optimizing that differentiation, the problem of determining, if the presented trait originates from a living person has received relatively less attention. Between acquiring biometric data and giving a result, there are various points where the overall security of a biometric system can be compromised. The information flow of a biometric access system is simple. Biometric system uses physical and behavioral characteristics of an individual which are considered to be private and secret. But if we see in daily routine the biometric information which consists of fingerprints, voice pattern and iris etc are considered to private but they cannot be assumed as secret. Like 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 can be recorded. Fingerprints impression can be recorded from anything we touch for e.g. door by which we enter our own home, office etc. It's not possible to keep a track of the number of things touched by us or number of call we made to different numbers etc. So the availability of facial images, fingerprints, voice patterns etc. in public can not be restricted. Thus it is acceptable that biometric systems which use fingerprint, facial images, iris, voice pattern etc are sensitive to spoofing attacks [2]. These biometric identifiers can be copied and used for hacking many existing biometric systems. Therefore the challenge is to find suitable techniques for biometric traits for detecting that it is real or fake. That's why the application of liveness detection technique introduces. This technique should be implemented in all systems which required higher security requirements, such as border passport control systems, bank systems etc. The biometric systems without liveness detection techniques could be fooled very easily and hence unauthorized access can be done. Liveness detection technique is capable of sense that given biometric trait is of living human or synthetic made up of silicon, gelatin etc. It is difficult to perform lives test for open network where system operators can not control end user terminal and transmission channels.

2. SPOOFING IN BIOMETRIC SYSTEM

In any Biometric system mainly 5 stages are used [3]:

1. Image Acquisition
2. Image Processing
3. Feature Extraction
4. Template Creation
5. Template Matching

Attacker can attack at any of following stage for unauthorized access to system; some of those attacks are like biometric sensor attack which happens at the beginning of process. In this type of attack fake biometric data like artificial finger, a mask over a face or a contact lens on an eye etc. may be presented to the sensor. It is known as a spoof attack. Another type is replay attack which intercepts the output flow of a sensor and puts previously stored genuine biometric information (either in raw or extracted form) into the proper place in the processing chain. Following are some attacks that can be happen on biometric system [4].

- Fake biometric data to sensor: In this type of attack fake biometric trait like fake gummy finger, an iris printout or a face mask is used for unauthorized access.
- Resubmitting previously stored digitized biometric signals (replay attack). A digitized biometric signal, which has been previously enrolled and stored in the database, is again send to the system.
- Tampering biometric feature: In this attack extracted features of given biometric trait changed so that it can be accepted by matcher.
- Attack on enrollment: An enrollment database used in the verification/identification process can also be altered like by providing fake biometric traits.

These are some common attack mainly happened on biometric system. Some of attack can be resolved by maintaining some security like securing database from alternation. But some attacks like fake biometric data to sensor cannot be covered by strong security. It's not possible to check every person that he/she using its own biometric or artificial synthetic biometric of other person. So for this type of attacks Liveness detection technique is used, to ensure that the given biometric sample originates from a living person and is not artificial. A liveness detection method can help to protect the system against some types of spoofing attacks in which fake biometric used.

3. Liveness Detection in Biometric System

Biometric traits of any given person are private but it's not secure. There are many routine work in which we used them, for e.g. when we touch handle of door our fingerprint impression appeared on it. Similarly when we talk on phone our voice can be recorded by anyone. So one can record or copy biometric of any person and can use it further in biometric system for unauthorized access. Liveness detection techniques can be used for improving the biometric system for knowing that given biometric trait is from living person or artificial.
Liveness detection technique can be based on following types:

1. Hardware Based: In this an extra hardware will be connected with the biometric system for sensing suitable sign like temperature, pulse etc.
2. Software Based: In other method some different type of software can be used for liveness detection, which uses the image of biometric trait.

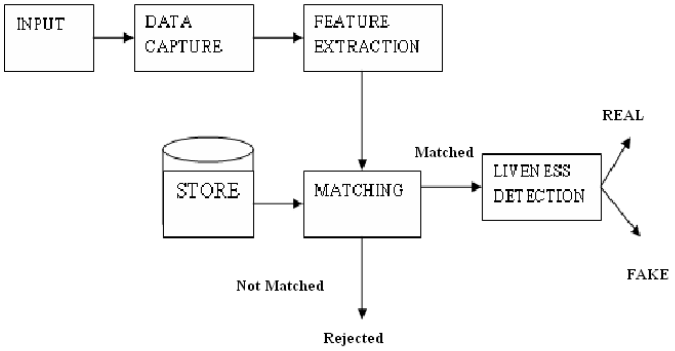

Figure1. Liveness Detection in Biometric System

Liveness detection techniques used different method for different biometric traits. Human body offers a great amount of different characteristic properties like pulse rate, temperature etc. Liveness detection technique choose some characteristic for verifying given sample is artificial or from living person. The properties usable for the liveness detection systems can be divided into following categories [5]. These are intrinsic properties of body, involuntarily generated signals and body responses to a stimulus.

1. Intrinsic properties: These properties include various characteristics of living human tissue, which can be based on thermal, optical, body fluid etc. One of the possibilities of utilization of the intrinsic properties is analysis of the spectral characteristics e.g. reflectance or absorbance. The characteristics of the skin are absorbance, transmittance and reflectance of the electromagnetic radiation of different wavelengths, which penetrate the skin surface to a different depth. Living human skin also has Electrical properties i.e. its conductance or dielectric constant [6].

2. Involuntarily signals: Involuntarily generated signals consist of living body uncontrollable generated signal like pulse, blood flow, blood pressure etc. The best known involuntarily generated signal is a

pulse. One of the approaches to measure pulse is based on the pulse oximetry, the pulsation differs from person to person and it is even not same for one person in various times. Perspiration is another good method this method is developed by Biomedical Signal Analysis Laboratory [7]. When user's finger is put on the sensing area it is relatively dry, which results in a pale captured image.

3. Body responses to stimulus: In this technique given person has to response to system for ensuring system that he is living person and not dummy. In it system interacts with user like asking user to raise his left/ right hand or to blink eyes. This technique mainly used in face recognition biometric system for liveness detection.

Liveness detection technique is now becomes a most important part for any biometric system. There are no. of biometric systems which required different types of biometric trait for authentication purpose, for e.g. fingerprint recognition system, iris recognition etc. Liveness detection technique can be used in any of following recognition system, by using suitable method for every system.

3.1 Liveness Detection in Fingerprint Recognition

The purpose of fingerprint recognition is to recognize a person on basis of his/her fingerprint image [8]. A fingerprint is believed to be unique to each person. Fingerprints of even identical twins are different. But with advancement of technology now attacker can make synthetic finger by using substances like gelatin. Such that given synthetic fingerprint has similar type of characteristics as that of real one. If given recognition system doesn't contain liveness detection system then attacker can access the system even by using synthetic finger. Therefore this system required more security so that attacker is not being able to fool the system by artificial finger. For this liveness detection technique can be used, which can detect some finger characteristics to ensure input finger is live or artificial. A number of fingerprint identification systems are used widely and implemented at various important places, such as border and immigration services. Therefore liveness detection is a necessary part of system to stop unauthorized access.

There are three major scheme reported in fingerprint liveness literature. It may include the additional hardware, software, or combination of fingerprint with other identifications scheme. The hardware-based methods use different sensors to detect the biological and physiological measurements from finger, like moisture, temperature etc. Whereas software-based methods detect changes in physical properties that take place in early stages of pressing the finger. Liveness detection technique categories are based on determining the presence of a user by different responses from either voluntary (e.g. passwords or multiple biometrics) or involuntary (e.g. pulse oximetry or blood pressure)[9].



Figure2. Artificial Finger

Artificial finger can be made by taking impression of real finger and then create a mold. Molds can also be created from latent fingerprints by photographic etching techniques. Use of play-doh, gelatin, or other suitable material can be used to cast a fake finger. In Worst-case scenario dead fingers is used.
There are different approaches for fake finger detection:

(a)Fake finger detection on basis of analysis of skin elasticity: In this approach fake finger is detected on basis of skin elasticity of finger. Such that when user put his finger on sensor, sequence of fingerprint images will capture which shows the deformation process of finger. After that suitable method used for detecting given finger is fake or real.

(b) In other approach some extra hardware used for detecting live finger on basis of some suitable sign like temperature, blood pressure etc.

3.2 Liveness Detection in Iris Recognition

Iris recognition biometric system recognize user on basis of iris pattern of user. If system is without liveness detection technique, then it can easily be fooled by using contact lenses or photograph image of iris of authenticated user. Liveness detection ensures that sample of iris at verification time is of living person and is not fake like contact lens or photograph.

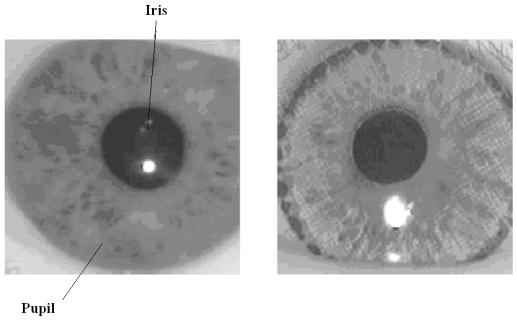

Figure3. Natural iris Fake iris (contact lens)

Iris recognition liveness detection method has different type of approaches:

(a) Pupillary reflex method: This method uses the variation in pupil size with time as result of flashlight illuminations [10].

(b) Eye gaze detection method: In this method user has to focus on marker present on system screen and user has to move their eyes along with movement of marker. Its very effective in

3.3 Liveness Detection in Face Recognition:

In face recognition biometric system without liveness detection technique, system can be fooled by mask. So for liveness detection in face recognition system, system may interact with the user and demanding real time responses for e.g. head movement blink eyes etc. Thermal cameras can be used for distinguish between living and dummy user.

Conclusion

With the advancement of technology even secured biometric system attacked by attacker. Now biometric system requires a more secure technique like liveness detection technique. Such that system not only verify that given biometric trait is from an authorized person, but also can get to know given biometric trait is real or fake. Therefore liveness detection technique make given system more secured from any unauthorized access. But this liveness detection scheme required extra hardware in addition to biometric system, that's why biometric system with liveness detection is costlier than simple one. Also there are still other biometric traits like hand geometry which is not comply with this technique. In brief liveness detection technique is now need of every biometric system for strong security.

References

[1] Anil K Jain, "Biometric Authentication: How Do I Know Who You Are", Proc. on Advances Pattern Recognition, pp.9-10, 2003.

[2] Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: Handbook of Fingerprint ecognition, Springer Verlag, New York, 2003, ISBN 0-387-95431-7.

[3] Biometrics -Identify Verification in a Networked World - Samir Nanavati, Michael Thieme, Raj Nanavati- WILEY-dreamtech .

[4]Galbally, J., Fierrez, J., Ortega-Garcia, J.: Vulnerabilities in Biometric Systems: Attacks and Recent Advances in Liveness Detection, Biometrics Recognition Group, Madrid, Spain, 2007, p. 8.

[5] Valencia, V.S., Horn, C.: Biometric Liveness Testing, In: Biometrics, Berkeley, CA: Osborne McGraw Hill, 2003, pp. 139-149.

[6] Kluz, M.: Liveness Testing in Biometric Systems, Master thesis, Brno, Masaryk University, Faculty of Informatics, CZ, 2005.

[7] Biomedical Signal Processing Laboratory, http://www.bsp.pdx.edu/.

[8] D.Maltoni, D. Maio, A. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer Verlag, Nu, USA, 2003

[9] Drahanský M.: Fingerprint Recognition Technology: Liveness Detection, Image Quality and Skin Diseases, Habilitation thesis, Brno, CZ, 2010, p. 153.

[10] Drahanský M.: Experiments with Skin Resistance and Temperature for Liveness Detection, In:Proceedings of the Fourth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Los Alamitos, US, IEEE CS, 2008, pp. 1075-1079, ISBN 978-0-7695-3278-3.