Liveness Detection: An Overview

Sonal Girdhar[1] Dr. Chander Kant[2]
[1]Research Scholar [2]Assistant Professor
[1,2]Department of Computer Science and Application
[1,2]Kurukshetra University, Kurukshetra, India

Abstract— Biometric system provides a mechanism to identify or verify every individual on the basis of their biometric traits. As every system is prone to attack by intruders so this system can also be breached by an imposter by gaining access to the personalized data of a legitimate user and getting unauthorised access. The biometric system needs to become more secure by using different techniques and one such technique is liveness detection. Liveness Detection can be used to detect whether the input is being given by a live user or some imposter is providing non-live or fake data. This paper presents a brief overview about some techniques which can be used to detect liveness in the different input samples being presented.

Key words: Biometrics, Biometric Technologies, Liveness Detection.

I. Introduction

Biometrics can be defined as the science of physiological or behavioral characteristics to identify or verify an individual. There are three different types of authentication that are commonly used these days i.e. Something we know, something we have, and something we are [1].

The first type of authentication, something we know, basically makes use of passwords or PINs (Personal Identification Number). Even though people are generally required to use this type of authentication to access some particular information, these passwords or PINs can easily get compromised.

The second type, something we have, is a smart card or token based. These are the items that we would have to carry with ourselves to use as identification. These items are relatively more risk prone, since they can be easily lost or stolen.

The third type of authentication, something we are, is generally based on our biometric traits. This is the most secure type of authentication as it cannot be easily lost, stolen, or forgotten. It is also the most feared by the general public as can be forged by the intruder. Several methods have come up that can be used to bypass biometric based security access.

So, liveness detection can be used as a technique to secure the biometric system by detecting the non-live biometric sample presented by the intruder to gain access to it. Different biometric technologies may require different liveness detection methods for security. Some of these biometric technologies are discussed in section 2.

II. Biometric Technologies

Different techniques are available to identify/verify an individual based on the biometric traits which can be divided into physical and behavioral characteristics [2] as shown in figure 1.

1) Physiological characteristics - These are based on information retrieved directly from a measurement of the human body. For example fingerprint recognition, facial recognition, optical recognition (iris or retina), or hand geometry recognition. They do not change with time and hence are used for verification as well as identification purposes.
2) Behavioral characteristics – These are based on information retrieved from an indirect measurement of the human body. For example voice recognition, keystroke recognition, signature recognition, odour or gait recognition. They can be changed forcefully and hence are used only for verification but not for identification purposes.

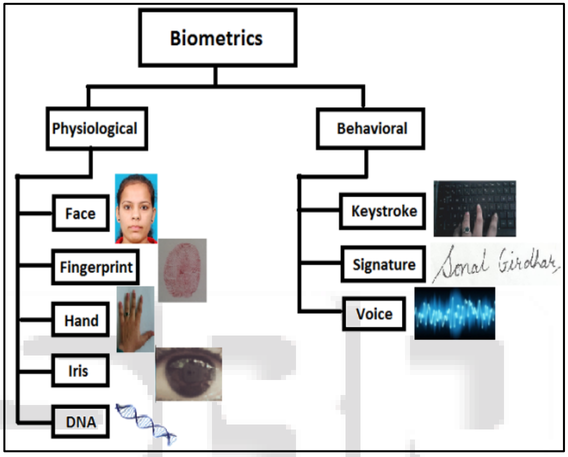

Fig. 1: Different Biometric Technologies

Each biometric trait has its own strengths and limitations; hence cannot satisfy the needs of all applications and accordingly, each trait is more suitable to a particular user application than others. These technologies can also be divided into two categories on the basis of their position required at the time of authentication which are:

A. *Contact Based Biometric Technologies:*

A biometric technology that requires the user to make direct contact with the surface of the scanner is known as a contact based biometric technology. Some of the commonly used contact based biometric technologies are [3]:

1) *Fingerprint Recognition:*

Fingerprints are the pattern of ridges and valleys present on the surface of fingertips which are captured to identify an individual uniquely.

2) *Palmprint Recognition:*

The palm of a human hand not only consists of unique features such as principal lines and wrinkles in addition to ridges and valleys similar to a fingerprint but also the area of the palm is much larger hence they are considered to be more distinct than fingerprints.

3) *Hand Geometry Recognition:*

In this, the physical characteristics of the hand and fingers are measured from a three dimensional perspective such as its shape, size, length and width.

4) Signature Recognition:

Signature recognition is the most common type of recognition which has been used in the government, legal and commercial sectors for decades.

5) Keystroke Recognition:

In this, the individual must be able to type in the same manner so that the time interval between letters or numbers must be same at different times.

B. Contactless Biometric Technologies:

A biometric technology that does not requires the user to make direct contact with the device but the required information can be extracted from a distance is termed as a contactless biometric technology. Some of these are [3]:

1) Face Recognition:

A digital camera is used to capture an image of the facial features in order to authenticate the user based on either the location and shape or the distance between two facial features.

2) Iris Recognition:

The iris carries very discrete information even in case of identical twins which can be used to uniquely identify an individual with a very high accuracy and speed than any other biometric trait.

3) Voice Recognition:

Voice recognition may be text dependent or text independent. The former type recognizes the individual independent of what he speaks while the latter is constrained with a particular text for recognition.

4) Gait Recognition:

Gait refers to the way in which a person walks and it can be used to recognize people at a distance.

Any security system is not completely fool proof. In spite of their various advantages, biometric systems are vulnerable to attacks, which can decrease their security. These attacks have been illustrated in section 3.

III. Attacks on Biometric Systems

Biometric-based systems also have some limitations that may have adverse implications for the security of a system [4]. Although a careful system design is necessary to overcome the limitations of a biometric system, it is important to understand that fool proof personal recognition systems do not really exist.

A. Basic Security Threats:

A biometric system is liable to various types of threats. Some of these threats are [5]:

1) Denial of Service:

An intruder willingly corrupts the system and its resources by sending a large number of fake requests so that the legitimate users can no longer have access to the system.

2) Circumvention:

An intruder gains access to the personalized data of a legitimate user and gets unauthorized access to the system by deceiving it.

3) Repudiation:

A legitimate user accesses the facilities of a system and then later claims that an intruder might have circumvented the system.

4) Covert acquisition or Contamination:

An adversary deceives the means of identification without the knowledge of a legitimate user.

5) Collusion:

When a user with super-user privileges such as an administrator misuses his privileges and deliberately modifies the biometric system's parameters to permit invasion by a collaborating intruder.

6) Coercion:

When an intruder forces a legitimate user to authenticate the system by giving his details. For example, an ATM user could be forced to give away his ATM card and PIN at gunpoint.

B. Biometric System Attack Points:

The various attacks in a biometric system are categorized into eight types [5]. Figure 2 shows these different types of attacks.

1) Type 1:

In this the intruder gives a fake biometric (e.g., synthetic fingerprint, face, iris) input to the sensor or may physically destroy the scanner.

2) Type 2:

This point of attack is known as "Replay Attack". In this the intruder interrupts the channel between the scanner and feature extractor to steal the biometric data and then replays it at a later time for authentication to bypass the scanner.

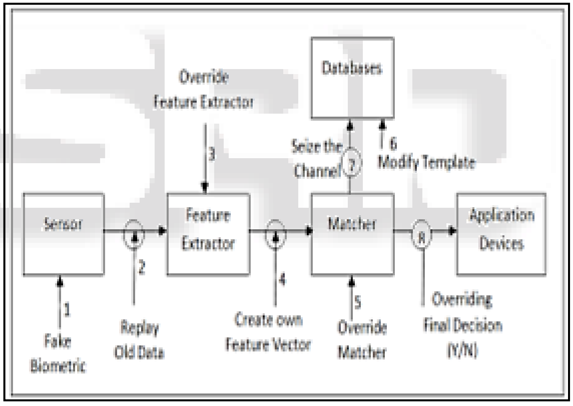

Fig. 2: Different Attack Points in Biometrics [5]

3) Type 3:

In this the feature values extracted by the feature extraction module are replaced by the feature values selected by the attacker.

4) Type 4:

In this the feature values of a legitimate user are stolen by the intruder from the channel between the feature extractor and matcher module to replay them to the matcher at a later time to bypass the feature extractor.

5) Type 5:

In this the attacker can modify the output of the matcher to an artificially high matching score to bypass the biometric.

6) Type 6:

In this the template database is attacked by the intruder such as adding a new template, modifying an existing template, removing templates, etc.

7) Type 7:

In this the attacker interrupts the transmission medium between the template database and matcher in order to steal or alter the transmitted templates.

8) Type 8:

In this the intruder overrides the matcher result (accepts or reject) being transmitted to the application by interrupting the channel between the matcher module and the application device.

The biometric system must be secure enough to deal with all these types of attacks. Many security techniques exist for this purpose as described in section 4.

IV. Biometric System Security through Liveness Detection

Security is a risk management strategy that identifies, controls, eliminates, or minimizes uncertain events that may adversely affect system resources and information assets. A biometric system deals with identifying individuals with the help of their physiological and behavioural data such as fingerprints, face, iris, signature, voice, etc. Since intruders provide the system with a large number of spoofed biometrics for authentication. Therefore, Liveness detection is one such technique that can be used to secure the biometric system from the intruders.

A. Liveness Detection:

The aim of liveness detection is to determine that whether the input data is being acquired from a genuine, live user who is physically present at the point of acquisition or an imposter who is trying to fool the system by providing fake biometrics to get access to the system. Liveness detection can be performed either at the acquisition or at the processing stage. It can be implemented in the following three ways [6]:

1) By adding 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 fingerprint of the legitimate user to the fingerprint scanner while his own real fingerprint to the hardware that just detects the liveness of the finger.

2) Using information already captured by the device

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.

3) Using liveness information inherent to the biometric

This method is very effective for facial thermogram and iris recognition but it cannot be used for fingerprint recognition as the outer layer of a finger, the epidermis, is necessarily dead, hence no inherent liveness information is present.

Basically, all liveness detection techniques lie between three categories [7]:

1) Intrinsic Properties of a Living Body:

These properties are further categorised as:

1) Physical Properties
- Density
- Elasticity

2) Electrical Properties
- Capacitance
- Resistance
- Permittivity

3) Spectral Properties
- Reflectance
- Absorbance

4) Visual Properties
- Colour
- Opacity

5) Body Fluid Analysis
- Oxygen
- DNA
- Blood constituents

2) Involuntary Signals of a Living Body:

Involuntary signals can be the characteristics of the autonomic nervous system. These constitute the dynamic liveness tests. A living body consists of certain involuntary considerable signals which are:

1) Pulse:

The pulse at the tip of finger can be measured to detect liveness.

2) Blood Pressure:

The blood pressure in the trait can be determined to check whether it is live or not.

3) Hippus:

The fluctuations in the pupillary size can be used to detect liveness in the input without any change in the illumination condition.

4) Perspiration:

The skin capacitance varies with time due to perspiration in fingers and it can be measured to detect whether the presented finger is live or dead.

5) Blood flow:

The blood flow level in the trait presented can be measured to assure of its liveness.

6) Brain Wave Signals (EEG):

Brain wave signals cannot be generated in a fake or dead trait. Hence the system cannot be fooled by an imposter easily.

7) Electrical Heart Signals (ECG or EKG):

A combination of pulse oximetry, ECG and temperature can be used to make the spoofing more complex.

3) Bodily Responses to External Stimuli:

These methods are based on challenge-response techniques which may require user cooperation (voluntary) or not (involuntary).These are also known as dynamic liveness tests.

1) Voluntary or Behavioral

These methods prompts the users to give a response to the system when asked to do so such as blinking or smiling in face recognition and looking left and right or up and down in iris recognition.

2) Involuntary or Reflexive

These methods do not require any response from the user as these are measured automatically by the system such as pupil dilation and knee reflex by changing the illumination levels.

B. Existing Liveness Detection Techniques:

There are many existing solutions to detect liveness of a biometric trait i.e. the user presenting the trait is live or not. Some of these solutions are:

1) Liveness Detection in Fingerprint Recognition:

Fingerprint is one of the most commonly used biometric and has been widely used in forensics for decades due to its uniqueness. But a fingerprint recognition system can be fooled by using gelatine, gum and play-doh to create synthetic fingerprints.

Figure 3 shows a comparison of fake fingerprints constructed using cadaver, clay, play-doh and real fingerprints formed using the capacitive scanner. Fake finger can be detected on the basis of:

1) Skin elasticity:

In this method when a person puts his finger on the scanning device, a sequence of fingerprint images will be captured which shows the deformation process of the finger.

2) Pulse Oximetry:

Pulse oximetry is based on different absorption levels of two wavelengths of light protruding through the finger. While blood oxygen content is neglected, the pulse information retrieved is used to detect liveness.

3) Skin resistance:

The electrical resistance of human skin with pre-specified range is used to detect degree of liveness. In this method skin resistance of user's finger is measured using ohmmeter or millimeter. The conductivity of human skin is based on humidity which varies among different people due to their biological characteristics.

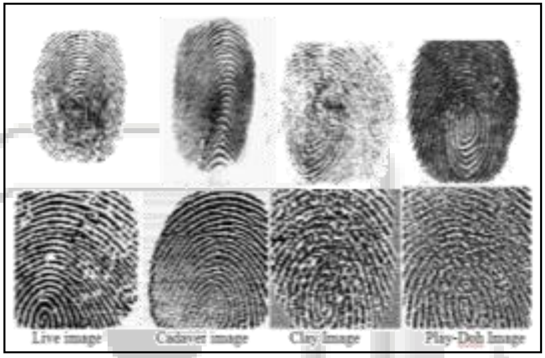

Fig. 3: Comparison of Real Fingerprint Image with Fake Images [8]

4) Laser System:

The laser system can be used to acquire the information from a distance and it can be integrated with a standard optical fingerprint sensor. We assume that expansion and contraction occurs in the volume due to heart activity, which causes fine movements of the skin. The laser sensor is capable of measuring very small changes in distance such as in terms of µm. The comparison of the computed curve and a normalized standard curve (the template) is used to detect whether the measured heart activity indicates a fake finger or not.

5) Finger Skin Temperature:

The human skin's temperature can be measured by using a thermo-camera. This method detects temperature of the outer layer of the skin, the epidermis which typically is in the range of 25-30 degree centigrade. Main drawback of this method is vulnerability increases as the range of operating temperature increases [8].

6) Thermal Imaging and Ultrasound:

In this a thermal pattern is generated using thermal camera to detect liveness. Ultrasound can also be used for liveness detection.

2) Liveness Detection in Iris Recognition:

The iris of every individual is unique and is composed of pigmented vessels and ligaments forming unique linear marks, frail ridges, grooves, furrows, vasculature, and other similar features and marks [9]. Figure 4 shows images of real and fake iris image.

1) Papillary reflex method:

This method uses the variation in pupil size with time due to flashlight illuminations.

2) Eye gaze detection method:

In this method user has to focus on the marker present on system screen and user has to move their eyes along with the position of the marker.

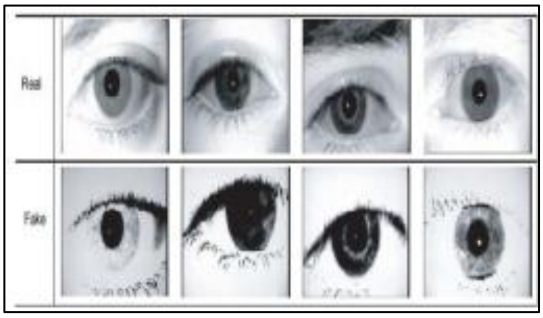

Fig. 4: Images of Real and Fake Iris [10]

In [9] Daugman proposes some eye features that could be used as countermeasures against direct attacks. Among these characteristics some spectrographic properties of different parts of the eye (tissue, fat, blood and melanin pigment), the coaxial retinal back reflection (the red eye effect) and the four Purkinje reflections caused by each of the four optical surfaces comprised inside the eye have been mentioned. These reflections can be noticed only with a very high quality camera not used in common iris identification systems.

3) Liveness Detection in Face Recognition:

The facial features of the users such as its valleys, peaks and landmarks are used by the system to authenticate the user by comparing them with the templates stored in the database. Face recognition system can be breached by three ways:

- Photograph of a valid user
- Video of a valid user
- 3D model of a valid user

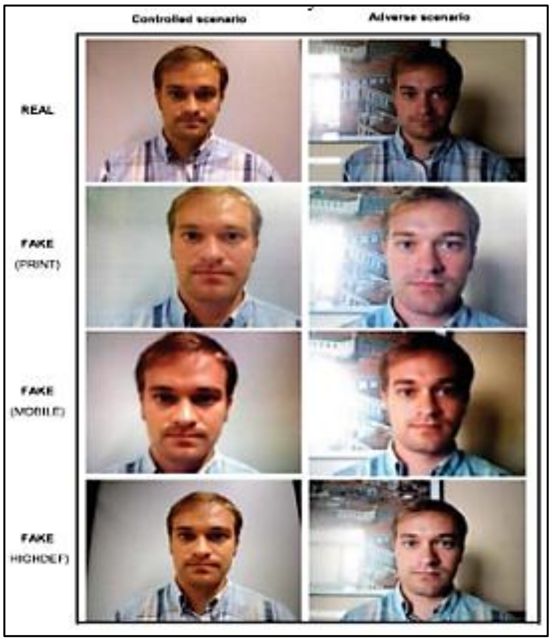

Fig. 5: Some Real and Fake Face Images [10]

Some examples of real and fake face images are shown in figure 5. Different methods to detect liveness in face recognition are:

1) Optical flow field:

It is a common method to use a photograph to fool the face recognition algorithm. As there are differences in optical flow fields generated by movements of two-dimensional planes and three-dimensional objects, a new liveness detection method has been proposed such that the test region is a two-dimensional plane; a reference field can be obtained from the actual optical flow field data. Then the degree of differences between two fields can be used to distinguish between a three-dimensional face and a two-dimensional photograph [11].

2) SVM Based algorithm:

This method describes illuminative variations on the face, which is especially applicable in artificial shadow estimation. Face authentication should also use a one-against many classification algorithm based on support vector machine (SVM) to obtain individual subsets, then estimate authenticated performances [12].

4) Liveness Detection in Palmprint Recognition:

Palmprints are considered to be more distinct and unique but they can also be spoofed by the intruder. Liveness detection in palmprint recognition can be performed by thermal imaging, ultrasound, infrared and multi spectrum approaches [13]. Figure 6 shows images of a human hand in different positions.

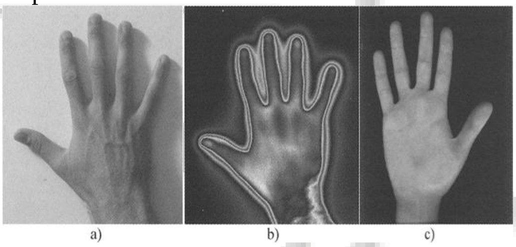

Fig. 6: A) Typical Position Of The Human Hand During The Acquisition Procedure; B) Thermal Image Of The Abaxial Surface Of The Hand Acquired By An Infrared Camera; C) Visible-Light Image Of The Palm Surface Of The Hand Scanned By The Optical Scanner [13].

5) Liveness Detection in Voice Recognition:

Voice recognition is used to translate the spoken word into a specific reaction, while voice verification verifies the vocal characteristics with those of the enrolled user. Voice verification systems can be text dependent, text independent, or their combination. Text dependent systems require a person to speak a predetermined word or phrase such as a name, birth city, favourite color, common idiom or a number sequence. It is then compared to a sample captured in the database during enrollment. Text independent systems recognize a user without requiring a predefined phrase. It operates on longer duration speech inputs so that it has a greater opportunity to identify the distinctive vocal characteristics (i.e., pitch, rhythm, tone). One of the main risks that both text-dependent as well as text-independent voice biometrics systems face is the risk of intruders using voice recordings of legitimate speakers. These can be acquired by interception or "Vishing" (Voice Phishing). To avoid this we use liveness detection in voice recognition. Liveness detection in voice recognition system is done by comparing the text independent audio sample collected at verification stage with text dependent audio sample received at enrollment stage [14].

V. Conclusion

Security of biometric system from fraudulent attacks is the biggest challenge nowadays. One of the negative impacts of increased technological achievement is the ease with which, one can spoof into a biometric system. The increasing attacks using fake biometric reduces reliability and security of biometric system. As general biometric algorithms are not able to differentiate "live" biometric from "not live" biometric, liveness detection is highly desirable so that these attacks may become more difficult to be performed.

References

[1] Sakshi Goel, Akhil Kaushik, Kirtika Goel, "A Review Paper on Biometrics: Facial Recognition", International Journal of Scientific Research Engineering & Technology (IJSRET) , ISSN 2278 – 0882, Vol 1 , Issue 5 , pp 012-017 August 2012.

[2] Anil K. Jain, Arun Ross and Salil Prabhakar, "An Introduction to Biometric Recognition", Appeared in IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

[3] Anil K. Jain, Arun A. Ross, "Introduction to Biometrics", Handbook of Biometrics, Springer, New York, USA, 2008.

[4] A. Vetro and N. Memon. Biometric System Security. Tutorial presented at Second International Conference on Biometrics, Seoul, South Korea, August 2007.

[5] Mrs. U. Latha , Dr. K. Rameshkumar, " A Study on Attacks and Security Against Fingerprint Template Database", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), ISSN 2278-6856, Volume 2, Issue 5, September – October 2013.

[6] S. A. C. Schuckers, "Spoofing and anti-spoofing measures". Information Security Technical Report, Vol. 7, No. 4, pages 56– 62, 2002

[7] J. D. Woodward, J.M. Orlans, P.T. Higgins, "Biometrics", Identify Assurance in the Information Age, 2003.

[8] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of Fourier spectra," appeared in Biometric Technology for Human Identification, SPIE, vol. 5404, pp. 296-303, 2004

[9] Daugman J., "How iris recognition works" , IEEE Transactions on Circuits and Systems for Video Technology 14, 21–30 , 2004.

[10] Pradnya M. Shende, Dr.Milind V. Sarode, Prof. Mangesh M. Ghonge, "A Survey Based on Fingerprint, Face and Iris Biometric Recognition System, Image Quality Assessment and Fake Biometric", International Journal of Computer Science Engineering and Technology (IJCSET), ISSN 2231-0711, Vol 4, Issue 4,129-132, April 2014.

[11] Saptarshi Chakraborty and Dhirubajyoti Das, "An overview of face liveness detection", Appeared in internation journal on information (IJIT), Vol 3, No. 2, April 2014.

[12] Cheng-Ho Huang, Jhing-Fa Wang, "SVM-based One-Against-Many Algorithm for Liveness face Authentication", Conf. on Man and Cybernetics 2008, pp 744-748, 2008.

[13] Swati Verma and Pomona Mishra, "A survey on Palm Prints Based Biometric Authentication System", International Journal of Electrical and Electronics Engineering (IJEEE), ISSN (PRINT): 2231 – 5284, Vol-1, Iss-3, 2012.

[14] Rozeha A. Rashid, Nur Hija Mahalin, Mohd Adib Sarijari, Ahmad Aizuddin Abdul Aziz, "Security System Using Biometric Technology: Design and Implementation of Voice Recognition System (VRS)", Proceedings of the International Conference on Computer and Communication Engineering 2008 May 13-15, 2008.