Volume 8, No. 5, May – June 2017

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Liveness Detection in Different Biometric Traits: An Overview

Komal[1] and Dr. Chander Kant[2]
[1] P.hd Scholar, [2]Assistant Professor
Department of Computer Science and Application, K.U. Kurukshetra (Haryana), India

***Abstract*:** Biometrics is used as an alternative for password based authentication systems and it becomes increasingly attractive now a day. Despite of its popularity, biometric systems are vulnerable to spoof attacks, which can decrease the security of the system. In order to protect the system against spoof attacks, liveness detection can be integrated with biometric system and it can distinguish between real and fake sample at the very first sensor module level. Liveness detection has the capability to detect the biometric sample is alive or not. This paper includes basic introduction of liveness detection, various attack point in the biometric system and various techniques used in biometric traits to detect their life signs.

***Keywords*:** Biometrics, Liveness detection, Spoof attacks.

1. Introduction

Biometric system is an alternative for password or PIN based authentication system. This PIN/password based authenticating system has variety of problems, because password can be forgotten or guessed. Biometrics can address these problems in an effective way because it uses individual's physiological (fingerprint, face, iris etc.) and behavioural characteristics (voice, gait, signature etc.) that cannot be forgotten.

Different biometric system are used in various applications such as banking, passport, medical records management, sensitive government departments, cellular phones, border control systems etc. The biometric information is considered to be private but they cannot be secret. Fingerprint of any individual can be collected from the surface of drinking glass or from the touch screen of his Smartphone. Facial image of an individual can be recorded at the entry gate of metro station or shopping mall. When an individual use any phone driven application then voice pattern could be recorded. Therefore, biometric systems are very venerable to spoof attacks and there are many issues related to all biometric traits. These issues may affect the performance of the biometric system. By applying liveness detection technique these issues can be addressed and increase the performance of the system. Following pseudo code is applied for liveness detection: -

```
If (input = live) then
  Perform acquisition and extraction
Else if (input = not live)
  Do not perform acquisition and extraction
```

Biometric system has various attack points where intruder can attack and forge the system. Liveness detection can protect the system against these attacks because it can distinguish between real and fake sample at the very first sensor module level. Next section includes various attack points in the biometric system.

2. Attack Points in a Biometric System

Biometric systems are venerable to various spoof attacks which decrease the performance of the system. Sensor module and template database module are very prone to these spoof attacks. But there are eight attack points in the biometric system where intruder can attack. Brief descriptions of these attacks are as follows [1]: -

Type 1 is 'attack on the sensor module'. In this type of attack fake biometric sample is presented at the sensor by the imposter.

Type 2 is 'attack on communication channel between sensor and feature extractor module'. In this type of attack imposter can steal raw data of a person acquired by sensor and can use it somewhere else. Type 2 attack is also known as replay attack.

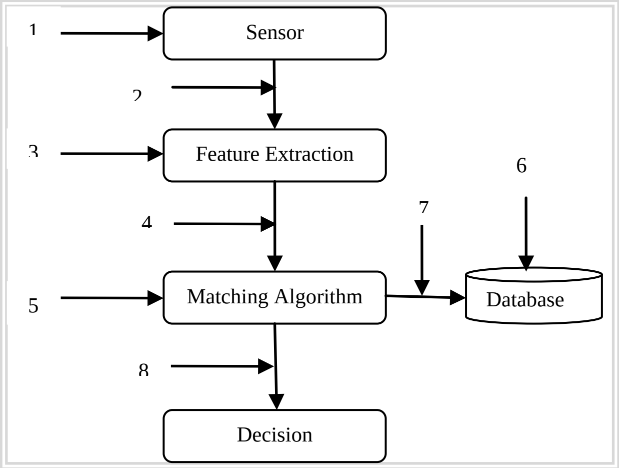

Fig 1: Attack Points

Type 3 is 'attack on feature extractor module'. In this type of attack imposter can generate fake feature value and can use these values instead of original feature values.

Type 4 is 'attack on communication channel between feature extractor and matching module'. This attack is similar to type

2 attack but in this imposter steal the feature values instead of raw data.

Type 5 is ‘attack on matcher module’. In this type of attack imposter can generate high matching score values for the fake sample [2]

Type 6 is ‘attack on template database’. In this type of attack imposter can add new template to the existing database, modify template database, remove template data etc.

Type 7 is ‘attack on communication channel between matching module and template database’. In this type of attack imposter can steal the template data which transmitted over communication channel.

Type 8 is ‘‘attack on communication channel between matching module and decision module’. In this type of attack imposter can tamper the match score values which are transmitted over communication channel.

Next section includes the basic introduction of the liveness detection and various techniques to detect life sign in human being. Liveness detection is one way to increase the performance of the system.

3. Liveness Detection

Liveness detection is used to address the problem of spoofing. Fig 2 shows the flow chart of the liveness detection in any biometric recognition system to check whether the input is alive or not:

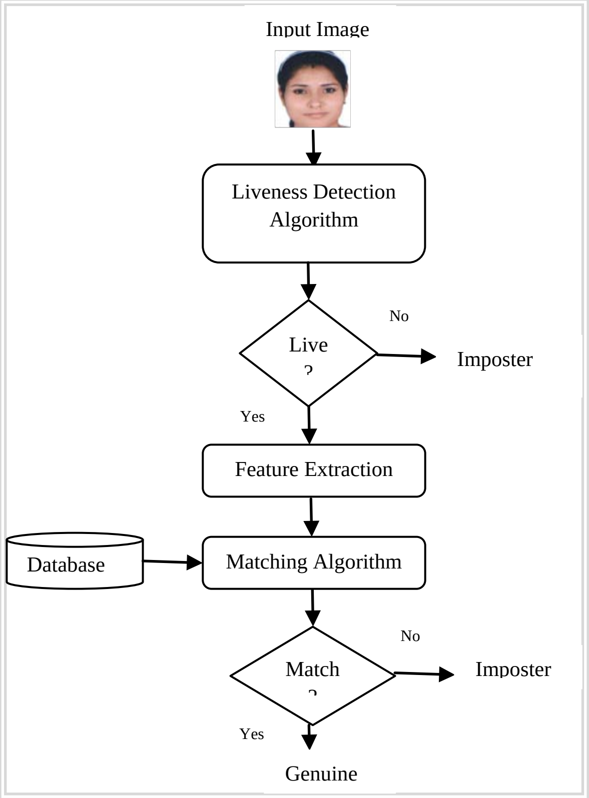

Fig 2: Flow Chart of Liveness Detection in Biometric System

Original input image is presented at the sensor level and then undergoes the process of liveness detection to check whether the sample is alive or not. Then feature extractor module extract the feature values from the input sample if the sample is alive. After then matching module matches the input feature module with the template stored in the database. If the input sample matches with the template data then it is declared as a genuine otherwise it is an imposter.

Basically there are three different ways to detect liveness in the biometric systems depend upon the type of biometric trait [3]:-

- **Intrinsic Properties of Living Body:** This category includes thermal, electrical properties of living body.
- **Involuntary Properties of Living Body:** This category includes blood flow, perspiration, pulse, blood pressure, brain wave signal, and electric heart signal are the examples of involuntary properties of living body.

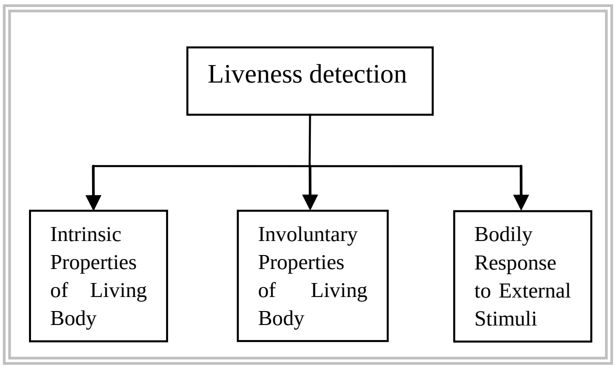
Liveness detection
Intrinsic Properties of Living Body
Involuntary Properties of Living Body
Bodily Response to External Stimuli

Fig. 3: Categorization of Liveness Detection

- **Bodily Response to External Stimuli:** This category requires user involvement for example: asking the user to blink the eyes, smile, moves his/her head etc.

Different traits use different techniques to capture the life sign of an individual.

3.1 Liveness Detection in Finger-print Recognition

Fingerprint is one of the oldest and most popular recognition techniques because of its high acceptability and performance. Every individual possesses unique fingerprint patterns, even two identical twins has different patterns of ridges and furrows [4]. Popular liveness detection techniques used in fingerprint recognition are as follows: -

- **Temperature Sensing: -**Temperature of the epidermis of finger is fixed and it is near about 26-30^{0}C. And thin silicon artificial fingerprints have lower temperature than normal range because thin silicon decreases the temperature transfer to the sensor. But the difference is not so much and it will not be difficult for the intruder to have the temperature within working range. So the outdoors sensor often has a broader working margin.
- **Pulse Detection: -** pulse in the finger tip can be used as liveness detection technique. But the pulse rate of a person is not fixed it can be changed due to fatigue, emotional state etc. A normal pulse rate of a person is 40 beats per minute and for the pulse detection the finger tip must be held for at least 4 seconds on the sensor. The pulse rate can be increased up to 80 beats per minute if he or she worked out before the fingerprint scanning [5].

  Anti-Fraud Biometric Sensor that Accurately Detects Blood Flow by Smart Touch LLC illustrated how two LEDs and a photo-detector are used to determine blood flow through the finger tip. Blood flow detection method basically implements Pulse Oximetry and it uses pulse rate information.

- **Pulse Oximetry: -** It is mostly used in medical field to measure the oxygen saturation level of haemoglobin in patient blood. Pulse Oximetry uses the pulse rate. This method is based on two principles: - 1. Haemoglobin absorbs light at different wavelength. 2. Fluctuating volume of blood for each pulse adds a pulse component to the absorption.

  Pulse Oximetry detection can be fooled by using artificial gelatine fingerprint. In this pulse Oximetry will also measure the oxygen saturation of haemoglobin of intruder's finger blood [3].
- **Electric Resistance: -** Electric resistance of a human skin ranges from several kilo-ohms to several mega-ohms. It may change depending on the humidity of the finger. Some people have dry finger and other have sweaty, so the range of resistance level is large enough for an intruder to easily fool the system. For example by using saliva on the artificial finger print, the system can be fooled into believing that the finger is live.

  Matsumoto and colleagues showed that the electric resistance of a live finger is 16 MOhms/cm and gelatine artificial finger is 20 MOhms/cm. The difference between live and artificial fingerprint is so small and it would be very easy for the intruder to fool the system. They also showed that live finger has moisture level of 16% while artificial finger has 23%. Since the moisture level affect the resistance, and difference in moisture level of live and artificial finger is very small. So the intruder can easily fool the system [6].
- **ECG: -** Electrocardiography can be used to detect the life sign in a finger. For ECG detection, the user has to hold his or her finger for 6 to 8 seconds. This is quit long time and if the user moves the finger in 6 to 8 seconds then measurement has to start all over again [7].
- **Skin Deformation:** - Fingertip's skin of a live person deforms when pressed against a sensor surface. And this information can be used as life sign. If the user is required to place his finger tip on the sensor surface twice, then there will be some non linear distortions between two fingerprint images while the artificial fingerprint produces the similar deformations.
- **Pore Detection: -** Sweat pores on fingertip can be used to detect life sign of a person. It might be difficult to copy the pores in artificial finger. Maltoni and colleague performed an experiment that showed it is difficult to reproduce the exact position and size of pores on the artificial fingerprint.

3.2 Liveness Detection in Face Recognition

Face recognition is widely used biometric technique and it is also very popular because of high acceptability [8]. Facial recognition is carried out by measuring facial metrics (e.g. measure distances between pupils or from nose to lip or chin).

Some liveness detection techniques in face recognition are as follows: -

- **Eye Blinking: -** Live body can be recognized by spontaneous eye blinks. Eye blink rate of a normal human is near about 15-30 per minute. Eye blinking based approach using Conditional Random Fields (CRFs) was introduced by Lun Sun and colleague [9]. Eye blinking operation consists of two sub operations: 1. From closing to opening and 2. From opening to closing. Eye blinking activity is an action represented by sequence of images which consists of close and non close state. Fig 4 shows the graphical structure of CRFs based blinking model.

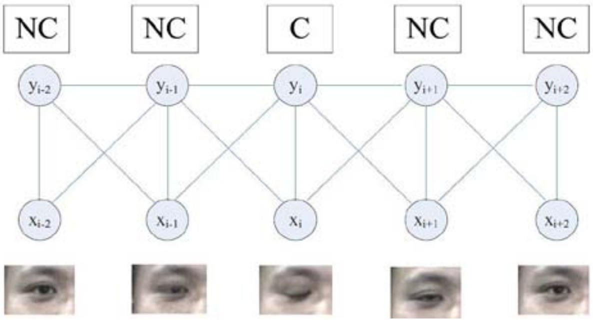

Fig 4: Graphical structure of CRFs based blinking model [9]

Here model is based on the observation of size 3. Label C stands for close state and NC stands for non close state. CRFs model has eye state label data y_t = {1, 2 ... c} and observation x_t.

Detection rate of the CRF based eye blinking model is shown in table 1. Detection rate is affected by strong glasses reflection, which covers eyes partially or totally.

Table 1: One eye blinking detection rate for CRF [9]

Different Styles	CRF
Without glasses	98.2%
With thin glasses	68.5%
With black frame glasses	75.0%

- **Movement of eye:** - Movement of eye based analysis was introduced by hyung-Keun Jee et al. for face recognition system. this method detect eyes in sequential images and then calculate the variations in each eye region and check whether the input face is live or not. In the eye detection process, first face region are normalized and then eye regions are extracted and binarized. Each eye regions are compared and variation is calculated. If result is higher than the threshold, then the input image is considered as live face otherwise it is considered as not live or photograph. Hyung Keun Jee and colleagues showed experimental results as given in table 2. Liveness score is measured using hamming distance, mean score value of live face is 30 and fake face is 17. It clearly shows that score value of live face is greater than the fake face.

Table 2: Hamming Distance of Eye Regions

	Hamming distance		
	Mean	Min	Max
Live Face	30	18	47
Fake Face	17	10	22

When threshold is set to the 21 then achieved FAR is 0.01 and FRR is 0.08.

- **Skin Texture:** - Micro skin texture can be extracted by using multi scale Local Binary Pattern (LBP). The LBP texture analysis operator is a gray-scale invariant texture measure, which is derived from a texture in a local neighbourhood. For each pixel in an input image, a binary code is produced by normalizing its value with the value of the center pixel. Fig. 5 shows an example of an LBP calculation.

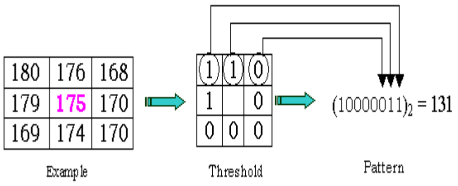

Fig 5: LBP Calculation

The operator $LBP_{P,R}$ refers to a neighbourhood size of P equally spaced pixels on a circle of radius R that form a symmetric neighbour set. The basic version of the LBP operator uses only the eight neighbour of pixel. LBP method has used in many applications like image retrieval, visual inspection, remote sensing, face image analysis, motion analysis etc.

Comparative analysis of these leveness detection techniques is shown in table 3 [10]. Some techniques are intrusive and other is non intrusive depending on the nature of the technique.

Table 3: Comparison of face liveness detection techniques

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 sign	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

3.3 Liveness Detection in Iris Recognition

It is the most correct biometric recognition system so it is called as king of biometrics. But because of low acceptability in daily life it is not so much popular as fingerprint or face recognition.

Some liveness detection techniques in iris recognition are as follows: -

- **Pupil Response: -** Living iris can be detected by measuring the pupil response to the effect of light. Size of pupil changes with the change in the illumination. Compare the size of the pupil of two eye samples of the same person that is acquired in two different illumination conditions. If the difference in the size of two pupil and is measured in the range of 5% - 15%, then it is considered as live or real eye sample otherwise fake sample [11].

  The percentage variation in size can be computed by the formula:

  $$((\text{First size} - \text{Second size}) / ((\text{First size} + \text{second size})/2)) * 100$$

- **Motions of Eye Retina: -** By detecting the motion of an eye ration one can capture the life sign and easily differentiate between real eye and artificial eye [12].
- **Reflection from Eye: -**Detection of Reflection from eye is very important as Dead Human's Eye does not give reflection.
- **Detecting Edge Sharpness: -** Iris edge sharpness is a possible way to measure the life signs. When contact lenses are used, fake iris edge is much sharper than the living iris edge [13].

3.4 Liveness Detection in Voice Recognition

Voice recognition is both physiological as well as behavioural trait. It focuses on the vocal features that produce speech and does not focus on the sound or the pronunciation of speech.

Some liveness detection techniques in voice recognition are as follows: -

- **Phoneme Localization Based analysis: -** Asking the user to repeat the sequence of phrases and digits. And captures time-difference-of-arrival (TDoA) changes in a sequence of phoneme sounds of two Sequences [14].
- **Detection of Pop Noise: -** Detect the pop noise caused by human breath in front of speaker. A Voice Liveness Detection (VLD) module is designed to reject the signals that do not have evidence of liveness. The human voice is result of shaping in the vocal tract of the airflow and it is produced by interaction between the vocal chords and lungs. Then the airflow is transformed into the acoustic signal when it is captured by the microphone. Acoustic airflow and strong breathing are considered as pop noise. Thus, by detecting pop noise, one can easily distinguish between live human voices or played back through loud speaker [15]. Fig 6 shows the recording process system using double channel algorithm. This algorithm detects the pop noise by using the procedure of subtraction between two channels.

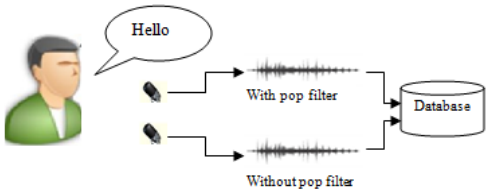

Fig 6: Recording Process System in double Channel Algorithm

This process requires two microphones, one with pop noise filter and another without pop noise filter. Finally the subtracted signal contains the information related to pop noise rather than background noise. Then this pop noise can be used to distinguish between real and fake sample.

4. CONCLUSION

We have discussed various attack points, liveness detection mechanism in biometric system. The life sign are used to distinguish between real and fake sensor inputs and hence elevate the security level in biometric field. Liveness detection can also be used with other security techniques like stenography, cancellable biometrics, watermarking, cryptography etc. to enhance the security and performance of the system in sophisticated areas.

REFERENCES

[1] U. Latha and K. RameshKumar, "A Study on Attacks and Security Against Fingerprint Template Database," *International Journal of Emerging Trends & Technology in Computer Science*, vol 2, no. 5, 2013.

[2] J. Mwemta, M. Kimwele and S. Kimani, "A Simple Review of Biometric Template Protection Schemes used in preventing Adversary Attacks on Biometric Fingerprint Templates", *IJCTT*, vol 20, no. 1, 2015.

[3] S. Schuckers, "Spoofing and Anti Spoofing Measures," *Information Security Technical Report*, vol 7, no. 4, pp. 56-62, 2002.

[4] A. Babu and D. Paul, "A survey on Biometric Liveness Detection Using Various Techniques," *International Journal of Innovative Research in Computer Science and Communication Engineering*, vol 4, no. 11, pp. 20055-20061, 2016.

[5] F. Fernandez, J. Fierrez, G. Javier and O. Javier, "Role of Biometrics in Healthcare Privacy and Security Management System," *Sri Lanka Journal of Bio-medical Informatics*, vol 2, no. 4, pp. 156-165, 2010.

[6] T. Keuning, "Biometric Fingerprint Recognition," *Fourth Working Conference On Smart Card And Advanced Applications*, USA., 2000

[7] J. Woodward, N. Orlands and P. Higgins, "Biometrics: Identity Assurance in The Information Age," McGraw-Hill, california, USA, 2003.

[8] T. Anjum and S. Sonekar, "Survey of Various Face Liveness Detection Techniques for Biometric Antispoofing," *IJECS*, vol 6, no. 4, 2017.

[9] L. Sun, G. Pan, and S. Lao, "Blinking-Based Live Face Detection Using Conditional Random Fields," *International Conference*, Korea, 2007.

[10] S. Chakraborty and D. Das, "An Overview of Face Liveness Detection," *International Journal on Information Theory*, vol 3, no. 4, pp. 220-225, 2014.

[11] R. Badode and S. Talbar, "Iris Analysis for Biometric Recognition Systems," Springer, new delhi, 2014.

[12] S. Javier Galbally, "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint and face Recognition," vol 23, 2011.

[13] Z. Wei, X. Qiu, Z. Sun and T. Tan, "Counterfeit Iris Detection Based on Texture Analysis," *International Conference on Pattern Recognition*, IEEE, 2008.

[14] L. Zhang, S. Tan, J. Yang and C. Yingying, "Voice Live: A Phoneme Localization Based Liveness Detection for Voice Authentication on smartphones," *ACM SIGSAC Conference on Computer And Communication Security*, New York, USA, 2016.

[15] S. Shiota, F. Villavicencio, J. Yamagishi, O. Nobutaka, I. Echizen and T. Matsui, "Voice Liveness Detection for Speaker Verification Based on a Tandem Single/Double-channel Pop Noise Detector," *international conference*, Spain, 2016.