A Novel Approach for Detecting Fingerprint Liveness

Sonal Girdhar¹, Dr. Chander Kant²
¹Research Scholar, DCSA, Kurukshetra University, Kurukshetra, India
²Assistant Professor, DCSA, Kurukshetra University, Kurukshetra, India

Abstract: A biometric system is the most secure type of authentication system as it identifies an individual based on the physical or behavioral characteristics of the person. Fingerprints are most commonly used in authentication but an intruder can fraudulently get access to the system by using different hacking technique. Therefore, securing a fingerprint biometric system becomes crucial and important. Liveness detection is used as a countermeasure to such spoofing attacks by detecting physiological life signs in the sample to distinguish a real fingerprint from a fake one. In this paper a novel approach has been used to enhance the security of a fingerprint biometric system by applying a challenge response mechanism to detect liveness in the sample being acquired.

Keywords: Attacks, Biometrics, Involuntary technique, Liveness Detection

1. INTRODUCTION
Fingerprint recognition systems are vulnerable to spoofing attacks with synthetically generated artifacts made from plastic, wax, clay, play-doh, silicone or gelatine materials. Robust performance of the existing fingerprint detection techniques has contributed to the ease of spoofing attacks on fingerprint biometric systems. Further, the latent fingerprints which are leftover on an object when touched once by the user, can easily be taken by the imposter to get fraudulent access to the system. Fingerprints are made up of ridges and valleys. They are most commonly represented by a set of minutiae points. Fingerprint recognition systems are based on minutiae matching. Minutiae are generally marked at ridge terminations and bifurcations. A fingerprint biometric system can be generally divided into two parts namely

- Enrollment
- Identification or Verification

In the enrollment phase, the fingerprint of an individual is first acquired by a biometric scanner and then features are extracted to generate a template. It is used to register individuals into the biometric system. Fingerprint verification is to verify the authenticity of the user by acquiring his fingerprint and matching it with the template stored in the database.

In this paper a new model has been proposed to enhance the security of a fingerprint biometric system by acquiring fingerprint of each of the five fingers of the right hand of the user at the time of enrollment to be stored in the database. The system then asks for any three random fingerprints at the time of authentication to be compared with the templates stored in the database.

The organization of this paper is as follows: threats to a biometric system in section 1.1, sensor attacks in a fingerprint biometric system in section 1.2, liveness detection in section 1.3, related work in section 2, problem with the existing techniques in section 3, proposed model in section 4, followed by conclusion and future scope in the last section.

1.1 THREATS TO A BIOMETRIC SYSTEM
A biometric system may be attacked at different modules which are classified into eight attack points [1]. These vulnerability points, as shown in Figure 1, can broadly be categorised into two main types:
(i) **Direct Attacks:** The sensor is attacked with fake biometric samples, such as synthetically generated fingerprints (point 1 in Figure 1). In this type of attack no internal knowledge of the system is needed. Liveness Detection deals with this type of attacks because digital security mechanisms such as watermarking, digital signature, etc cannot be used to prevent them.

![Figure 1: Attack points in a biometric system](image)

(ii) **Indirect Attacks:** All the remaining seven points of attack in figure 1 are known as indirect attacks. Attacks at points 3 and 5 are carried out by means of a Trojan horse that bypasses the system modules (Feature extractor and matcher module). In attack 6, the knowledge database is manipulated by adding, deleting and modifying templates. The remaining attack points (2, 4, 7 and 8) take place at the communication channels between the system modules. Unlike direct attacks, here the impostor needs to have some extra information about the internal processes of the system.

### 1.2 SENSOR ATTACKS IN A FINGERPRINT BIOMETRIC SYSTEM

A fingerprint biometric system can easily be spoofed by presenting fake biometric samples due to its inability to ensure liveness and are vulnerable against various types of attacks. Some of the possible attacks [2] are described as follows:

i) **The registered (legitimate) finger:** Fingerprint of a legitimate user can be stolen and then used by casting it into a mould, or forcing the user to present it to the sensor either directly or indirectly.

ii) **The unregistered (imposter’s) finger:** In this, the intruders use their own fingers to try to log in as another user.

iii) **A genetic clone of the registered finger:** Fingerprints of identical twins are almost similar to each other. In the same way, genetic clone of the fingerprints of a legitimate user can be used to fool the system.

iv) **Artificial fingerprint:** A real fingerprint can be artificially copied with gelatine, wax, silicone, clay, plastic or other materials. The attacker only needs to have the original fingerprint either by directly making a mould, or by collecting latent fingerprints of the user.

The biometric system must be made robust enough to deal with all these types of attacks. Liveness Detection acts as a countermeasure to these spoofing attacks in the fingerprint biometric system as described in section 1.3.

### 1.3 LIVENESS DETECTION

Liveness detection ensures that the input data is being provided by a genuine live user and not an imposter who is trying to spoof the system by providing fake or dead biometrics to the scanner. Liveness detection in a biometric system can be performed either at the acquisition stage or at processing stage. It can be implemented by (i) Adding extra hardware to the system, (ii) Using information already captured by the device or (iii) Using liveness information inherent to the biometric, but the outer layer of a finger, the epidermis, is requisitely dead, hence no inherent liveness information can be used in a fingerprint recognition system [3]. There are many techniques which are used to detect the liveness of the data acquired and hence, reduce spoofing at the sensor level. All these techniques are categorised into three types [4]:

---

**Sonal Girdhar, Dr. Chander Kant**
(i) Intrinsic properties of a Living body
Some characteristics of a living human body can be used to detect liveness in the biometric sample. These are categorised into different types as shown in figure 2. In a fingerprint biometric system the properties of various skin layers or body fluids can be used.

![Fig 2: Intrinsic properties](image)

(ii) Involuntary signals of a living body
A living body consists of certain involuntary considerable signals which constitute the dynamic liveness tests. Some of these properties are pulse, blood pressure, hippus (variation in the pupil size without illumination changes), perspiration, blood flow, brain wave signals (EEG) and electrical heart signals (ECG or EKG) as shown in figure 3.

![Fig 3: Involuntary Signals](image)

(iii) Bodily Responses to External Stimuli
Figure 4 shows that these methods are based on challenge-response techniques which may be either voluntary (user’s response is needed) such as eye blinking and smiling, or involuntary (without user’s cooperation) such as pupil dilation and knee reflex. These are also used as dynamic liveness tests.

![Fig 4: Challenge-response techniques](image)

2. RELATED WORK
This section reviews the related literature on involuntary techniques based on automatic (without user intervention) acquisition of data from the user’s body. These are:

i) Temperature
The temperature difference between the epidermis (about 26-30°C) and silicone artificial fingerprint (max 2°C less than the real finger’s temperature) is measured to detect liveness in the sample but this difference is so small that it is not easy to detect the wafer-thin silicone rubbers [5].

ii) Pulse
The pulse in the tip of a real finger can be detected and used as a liveness detection method but as the imposter’s finger is covered with a wafer-thin artificial fingerprint, the underlying finger’s pulse will however be sensed by the device [5].

iii) Heartbeat
This method senses the heartbeat present in the user’s finger to detect liveness. The problem that arises in this technique is the variability in the heart rhythm of a user due to user’s emotional condition and level of physical activity [5].
iv) Blood pressure
This method measures the heartbeat at two different parts of the body to determine the propagation speed of heart pulse but it is not liable to a wafer-thin silicone rubber glued to a finger as the underlying finger's blood pressure gets sensed [5].

v) Conductivity
In this technique, liveness is detected by measuring the conductivity of the finger, which ranges from 200 kΩ, during sweaty summer to several MΩ during dry freezing winter weather. The system can be easily fooled by applying some saliva on the silicone artificial fingerprint accepting it as a live finger [5].

vi) Relative Dielectric Constant
It measures the extent to which the material concentrates the electrostatic lines of flux. RDC of human skin is different from that of silicone material and is influenced by the humidity of the finger but it can also be fooled by applying some spirit on the silicone rubber so that it comes under the range of the RDC of a human finger [5].

vii) Detection under Epidermis
This technique measures the pattern of lines underneath the epidermis. The pattern of these lines is identical to the fingerprint pattern. It can also be easily fooled by making a wafer-thin silicon layer having the two lines pattern in exact matching positions [5].

viii) Pulse Oximetry
This technique is used to measure arterial oxygen saturation of haemoglobin in the pulse. The technology involved is based on two physical principles. First, a pulsatile signal is generated by arterial blood which is independent of non-pulsatile blood, capillary blood and other tissues. Second, oxy-haemoglobin and reduced haemoglobin absorb light differently at different wavelengths depending on the degree of oxygenation [6]. This technique can be fooled by using a translucent artificial fingerprint such as gelatin which covers only the fingerprints of a live user as the pulse oximeter will measure the saturation of oxygen of haemoglobin in the intruder’s finger’s blood.

ix) Optical properties
This technique measures the difference between absorption, reflection or scattering of the human skin from other materials such as silicone, wax, etc under different illumination conditions. However, gelatine material has optical properties almost similar to human skin [7].

x) Fine movements of the fingertip surface
This method is based on the analysis of fine movements of fingertip surface, which is produced by volume changes caused by the blood flow. There are two optical solutions to measure fine movements of papillary lines [8]. The first system is based on a close image of the fingertip acquired with a CCD camera along with a macro objective while the other one uses The second is based on a triangulation of a distance laser sensor and variation of the distance to fingertip maps, to variation in fingertip volume with blood flow.

xi) Surface coarseness
This approach is based on analyzing the surface coarseness of the fingertips in three steps. Firstly, a fingertip image is denoised using wavelet- based approach. Next, the noise residue (original image minus denoised image) is calculated and coarser surface texture results in a stronger fluctuation in the pixel value of the noise residue. Finally, standard deviation of the noise residue can be used to mark the texture coarseness [9] but this method is not compatible with all the sensors as it is dependent on high-resolution fingerprint.

xii) Perspiration
This technique is based on detecting the perspiration phenomenon between the human skin and other material under different conditions but its limitation is that it may not be used to detect liveness in users with low moisture or high perspiration-saturated fingers due to the requirement of specific changes in the moisture [10].
xiii) Sweat Pores
In this technique, a very high resolution fingerprint image sensor can be used to acquire the details in the fingerprint, such as sweat pores that can be used as a liveness detection method. These fine details might be difficult to copy in artificial fingerprints and hence spoofing can be reduced to a great extent [11].

3. PROBLEM ANALYSIS
A strong biometric system is required for user authentication and more secure biometric system can be achieved by applying the involuntary techniques discussed in section 2 by detecting fingerprint liveness and hence reducing spoofing attacks to a great extent but their operation margins have to be adjusted so radically to effectively operate indoors, outdoors, summer and winter that a wafer-thin silicone rubber that is glued to a real finger easily passes these additional tests of scanners [5]. Therefore, a novel voluntary approach has been proposed in section 4 so that no additional efforts are required to detect liveness in fingerprints.

4. PROPOSED WORK
In this paper, a new voluntary (challenge-response) liveness detection model has been proposed to make the fingerprint biometric systems more secure. Proposed model (as shown in figure 5) works in two phases by first enrolling the user into the system by acquiring the fingerprints of all the five fingers (Thumb, Index Finger, Middle Finger, Ring Finger and Little Finger) of the right hand starting from the thumb as shown in figure 6. After that the minutia points are extracted as the feature set of the fingerprints. Each finger is assigned a number according to the order in which it is located in the hand, beginning with the thumb as number 1 and ending with the little finger as number 5 for storing them into the database. This marks the completion of first phase. Next the system performs the authentication process by asking the user to put the fingerprint of any random finger by randomly generating a number between 1 and 5 corresponding to a particular finger of the right hand of the user. Feature set is extracted and template generated to compare it with the template of the finger stored at that particular number in the database. Based on this, a match score is generated and if its value is equal to or above the threshold then the number of acquisitions is determined to decide whether the input being provided is live or not.

There are a number of advantages of proposed model over the conventional system, as described below:

i) Fingerprint of the second finger is acquired if and only if the first finger matches with the existing database template and user is not declared as an imposter.

ii) No additional hardware is required to detect liveness in the sample.
iii) Accuracy of the system will improve.

Fig 6: Sequence of fingerprints

The algorithm for the proposed model is described in two phases as:

**First Phase: Enrollment**
1. Acquire the fingerprint of each of the five fingers of the right hand one by one.
2. Extract the feature set of the fingerprint.
3. Generate the template.
4. Create the Database.

**Second Phase: Verification / Identification**
1. System asks to put the fingerprint of any random finger from the right hand of the user.
2. Acquire the fingerprint by using a fingerprint scanner.
3. Extract the feature set of the fingerprint.
4. Generate the template.
5. Compare with the template stored in the database.
6. If (match score >= threshold)
7. If (no. of acquisitions >= 3)
8. Identified as genuine.
9. Else
10. Goto step 1
11. End If
12. Else
13. Identified as fake.
14. End If
15. End

The proposed scheme is not free from all drawbacks,
(i) It requires extra storage space to store the template of all the five fingers of a user instead of one.
(ii) Total response time of the system increases if the user is genuine.

(iii) May not be user convenient at all times.

5. CONCLUSION AND FUTURE SCOPE
As the spoofing attacks in a biometric system are increasing at a very fast pace so there is an emerging need to make biometric devices more robust and secure. Liveness detection has been a very powerful technique to differentiate between the real and fake samples being presented to the system but it also have some limitations like every other technique. Our proposed technique requires more storage space and thereby consuming more time. Hence, continued research is needed in this direction to make liveness detection more efficient for providing security.

REFERENCES
Department of Anaesthetics, Oxford Radcliffe NHS Hospitals Headington, 2000


