Spoofing Technique for Fingerprint Biometric system

Tanisha Aggarwal[1] Dr. Chander Kant Verma[2]
[1]M.Tech. Scholar [2]Assistant Professor
[1, 2] Department of Computer Science and Application
[1, 2] Kurukshetra University, Kurukshetra, India

Abstract--- A spoof is a counterfeit biometric that is used in an attempt to circumvent a biometric sensor. Differentiating a genuine biometric trait presented from a live person versus some other source is called spoof detection (anti-spoofing). The fingerprint liveness detection refers to the inspection of the finger characteristics to ensure whether the input finger is live or artificial. There are two major approaches for liveness detection, which are reported in literature are using the additional hardware and software based techniques. In this paper, various fingerprint liveness detection methods, which are categorized as voluntary and involuntary, are explored. The main objective of this paper is to propose a method to spoof a fingerprint sensor using a mold made by a material i.e. fevicol.

Keywords: Biometrics, Biometric threats, Fingerprints, Liveness Detection, Spoofing.

I. INTRODUCTION

A biometric is defined as a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being. These days, biometric technologies are typically used to analyze human characteristics for security purposes. The uses of biometric systems are growing every day. Fingerprint scanning is the one biometric identification method available today that is mostly used. The security of fingerprint scanners has however been questioned and previous studies have shown that fingerprint scanners can be fooled with artificial fingerprints, i.e. copies of real fingerprints or artificial fingerprints. An artificial fingerprint, is a fingerprint made to imitate a real (living) fingerprint. It can be made of gelatin, silicone, play-doh, clay, or other materials. There are two ways to make an artificial fingerprint; either by directly making a mold of the legitimate user's finger, or by using a residual fingerprint to produce an artificial fingerprint. To improve security for the biometric systems, liveness detection (or vitality detection) is proposed to defeat this kind of spoof attacks. In this paper, first some of the well-known eminent threats and attacks on the fingerprint algorithms are explored. Secondly, some countermeasures and techniques to overcome such problems are discussed. In the last, a method is proposed to spoof the fingerprint system easily.

A. Threats to Biometric System

1) Generic Security Threats:

In addition to above identified attacks, Jain et al [2] list a number of other types of attacks as follows:

(1) Denial of Service: Slowing and stopping of system via an overload of network requests or by degrading performances.This attack prevent the legitimate use of the biometric system.(2) Circumvention: An adversery gain access to data or computer resources that he may not be authorised to access.(3) Repudiation: a legitimate user accesses the resources and then claim that intruder had circumvented the system.(4) Covert acquisition: the use of biometric information captured from legitimate users to access a system.(5) Collusion: Access to the system by way of collusion between administrator (super user) and other users to overrule the decision made by system.(6) Coercion: Access to the system as genuine users by forcing the user to identify themselves to system.

Scenarios 2 and 4 can be classified as unregistered fingerprint, while 3 and 6 can be labeled as registered fingerprint attack as detailed above. In the case of denial of service (scenario 1), since every fingerprint sensor has individual acquisition technologies and related durability (e.g. surface of optical sensors can be easily broken), any offered solutions must depend on the especial investigation of each sensor. Furthermore, in scenario5, the offer of any solution raises the demand of implementation details based on application requirements.

2) Biometric security threats:

Ratha et al. [1] identified several different levels of attacks that can be launched against a biometric system (Figure 1):

(i) a fake biometric trait such as an artificial finger may be presented at the sensor, (ii) illegally intercepted data may be resubmitted to the system, (iii) the feature extractor may be replaced by a Trojan horse program that produces pre-determined feature sets, (iv) legitimate feature sets may be replaced with synthetic feature sets, (v) the matcher may be replaced by a Trojan horse program that always outputs high scores thereby defying system security, (vi) the templates stored in the database may be modified or removed, or new templates may be introduced in the database, (vii) the data in the communication channel between various modules of the system may be altered, and (viii) the final decision output by the biometric system may be overridden.

II. SENSOR ATTACKS IN BIOMETRIC TRAITS

There are number attacks and there remedial solutions

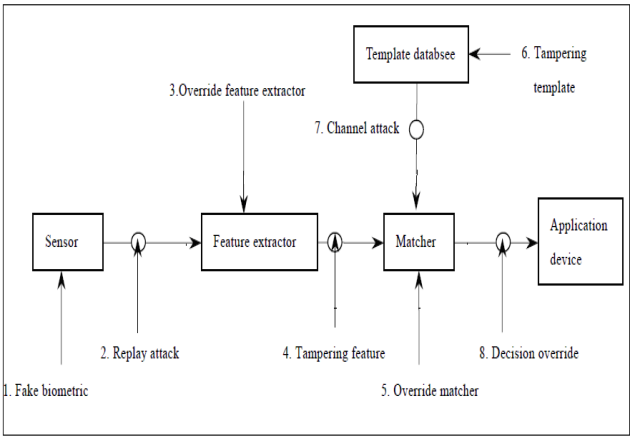

Fig. 1: Attack points in biometric system

discussed in the literature on different modules of biometrics system and communication links among them. But still the researchers are not able to secure every module of a biometric system against these attacks.

A. Facial Recognition

Commercial facial recognition system most often are based on digital images collected using visible or near infrared light. These system can be broadly divided in two categories: 2-D and 3-D facial recognition.The 2-D facial recognition system can be able to be spoofed using a simple photograph of the enrolled person's face. One can also use make-up or plastic surgery as other means of spoofing, photographs are probably the most common sources of spoofing attacks because one can easily download and capture facial images. Typical countermeasure against spoofing is liveness detection that aims at detecting physiological signs of life such as eye blinking, facial expression changes, mouth move- ments etc. Another existing countermeasure to spoofing attacks consists of combining face recognition with other biometric modalities such as gait and speech.

B. Iris Recognition

Iris recognition is based on discriminating the fine texture of the textured area of the eye that surround the pupil. A straightforward method that has been used to spoof an iris sensor is based on a high quality photograph of the eye. Another method used to successfully spoof some iris sensor is to use contact lense on which an iris pattern is printed. Even more sophisticated and three dimensional artificial irises may also be produced to spoof a sensor. Iris spoof detection may be accomplished in variety of ways. Involuntary motion of the pupil at rest or in reaction to changing ambient light condition may be checked to determine if a live eye is in sensor's field of view. Another method is that person under the test may be asked to blink or move their eyes in a certain direction to ensure liveness.

C. Voice recognition

In voice recognition the spoofing attacks generally happens at the two points: sensor level and transmission of the sensed signal. At the sensor level, imposter could deceive the system by impersonating someone at the microphone and at the transmission time the acquired voice signal could be replaced by synthetically generated signal or imitated voice.to Speaker verification system is used to automatically accept or reject the claimed identity of a speaker.

D. Fingerprint

The possibility of defeating a fingerprint biometric system due to its inability to ensure liveness through fake biometric samples, make fingerprint authentication systems vulnerable against various possible attacks. In this section, these possible attacks [1] are explored in different schemes as follows:

1) The registered finger:

i. Stealing fingerprint of a user by casting it into a mold, or causing user to press against sensor either directly or indirectly by way of drugs.

ii. Separating finger from legitimate user's body.

2) The unregistered (illegitimate) finger:

This is another kind of attack known as unregistered finger that attackers use their own fingers to try to log in as another user.

3) A genetic clone of the registered finger:

Another type of the attack on the not robust system is genetic clone of the fingerprint or using the similarity of identical twins fingerprints. Therefore, it raises the demand of carefully designed systems with capability to detect even slightly different fingerprints, since twins fingerprints are not identical. In the case of genetic cloned, this attack cannot be successful by employing a liveness detection mechanism in the system. Although, protection against the identical twin is not as easy as protection against a genetic clone, but combination with another authentication method can be a helpful countermeasures [1].

4) Artificial fingerprint:

This attack is made by duplicating a real fingerprint with gelatine, silicone, copier, clay, or other materials. In this method, attacker should have the original fingerprint either by directly making a mould of user's finger, or by using a residual fingerprint to make an artificial one. The useful countermeasures against this are liveness detection or combination with other authentication methods [1].

III. Liveness Detection As Countermeasures In Fingerprint

Academic and industry experts have been researching methods to counter the threat of physical spoofing of biometric samples. Since every type of fingerprint sensor has individual acquisition and related tenability, the protection solutions must take into account the special characteristics of these sensors. Liveness detection in a fingerprint system ensures that only "genuine" fingerprints are capable of generating templates for enrollment, verification, and identification. In particular various liveness detection methods have been conceived and indeed implemented in some devices.

Liveness detection can be performed in a biometric devices either at the acquisition stages or at processing stage. There are many techniques pointed out in literature to recognize the liveness of the presented data and hence, reduce vulnerability to spoof attacks at sensor level [3, 4, 5]. These techniques are explored in two different approaches as voluntary (acquisition of life signs by measuring the voluntary properties of users' body or users' response) and involuntary (acquisition of life signs by measuring the involuntary properties of users' body or users' response) **.**This section reviews the published literature on involuntary techniques based on automatic (without intention) acquisition of data from the user's body. Some well-known methods evaluated by other researchers are described in this section.

A. Temperature

This technique is based on extracting the temperature difference between the epidermis (about 26-30° C) and silicone artificial fingerprint (max 2°C). Lack of ability to detect the wafer-thin silicone rubbers is the main weakness of this technique [3].

B. Pulse

The pulse in the tip of the finger can be detected and used as a liveness detection method. With a wafer-thin artificial fingerprint, the underlying finger's pulse will however be sensed.

C. Heartbeat

This method is accomplished by sensing the finger pulse as liveness detection method. This technique has practical problems with diversity in the heart rhythm of a user. In addition, user's emotional condition and level of activity will affect the heartbeat [3].

D. Blood pressure

This method is not susceptible to a wafer-thin silicone rubber glued to a finger. It can be bypassed by using underlying finger's blood pressure [3].

E. Pulse Oximetry

Pulse oximetry is used in the medical field to measure the oxygen saturation of haemoglobin in a patient's arterial blood. A pulse oximeter also measure the pulse rate. The technology involved is based on two basic principles. First, haemoglobin absorbs light differently at two different wavelengths depending on the degree of oxygenation. Second, the fluctuating volume of arterial blood for each pulse beat adds a pulsatile component to the absorption [7].

Detection of pulse oximetry can be fooled using a translucent artificial fingerprint (e.g. gelatin) which covers only the live finger's fingerprint. The pulse oximetry will measure the saturation of oxygen of haemoglobin in the intruder's finger's blood. [6]

F. Optical properties:

These techniques are based on the different absorption, reflection or scattering between the human skins versus other materials under different lighting conditions. However, gelatine artificial fingerprint has optical properties very similar to human skin [4].

G. Fine movements of the fingertip surface:

This method is based on the analysis of fine movements of fingertip surface, which is induced by volume changes due to the blood flow. There are two approaches to measure fine movements of papillary lines [8], both based on optical principles. The first solution is based on a close-up view of the finger- tip acquired with a CCD camera; the second one is the triangulation distance measurement with a laser sensor. In spite of the advantages, more investigation needs to be done to evaluate the effectiveness and feasibility of such methodology. In addition, matching techniques needs to be improved (for instance in the case of presenting similar patterns to real heart activity curve, measuring curves of camera and the laser is solution) [8].

H. Surface coarseness:

This new liveness detection approach is based on analyzing an intrinsic property of fingertips: surface coarseness. Firstly, a fingertip image is denoised using wavelet- based approach. In second step, noise residue (original image minus denoised image) is calculated and coarser surface texture tends to result in a stronger pixel value fluctuation in noise residue. Finally, standard deviation of the noise residue can be used as an indicator to the texture coarseness [9]. Feasibility of such method is dependent on high-resolution fingerprint, which is not compatible with all current sensors.

I. Perspiration

This method is developed by Biomedical Signal Analysis Laboratory. When user's finger is put on the sensing area it is relatively dry, which results in a pale captured image. The finger is perspiring and the sweat is distributed along the ridges into the originally dry areas, hence the captured image becomes darker during some time. This process is clearly illustrated in Fig 2 below. But user with low moisture may not be able to use a fingerprint scanner, and highly perspiration fingers may nor exhibit liveness.

J. Conductivity

In this technique, liveness detection is made by checking the conductivity of the finger skin, which is from 200 kΩ (dependent on the type of sensor) to several MΩ respectively, depending on whether we are during dry freezing winter weather or during summer. The simple attack in this system can fool the sensor by some saliva on the silicone artificial fingerprint to be accepted as live finger [3]. The Table 1. Below shows the limitation of the liveness detection methods which are discussed in this paper.

K. Pores detection method

By using a fingerprint sensor which can acquire an image of the print with a very high resolution, it is possible to use details in the fingerprint, such as sweat pores, as a liveness detection method . These fine details might be difficult to copy in artificial fingerprints.

Table 1. Liveness detection techniques and their limitations

Liveness Detection Techniques	**Limitations**
Epidermis Temperature	Lack of ability to detect the wafer thin silicone rubber
Pulse	With a wafer-thin artificial fingerprint, the underlying finger's pulse will however be Sensed
Heartbeat	Practical problems with diversity in heart rhythm of a user
Blood Pressure	Can be fooled by using underlying finger's blood pressure
Pulse Oximetry	Can be fooled using a translucent artificial fingerprint (e.g. gelatin).
Optical properties	Gelatine artificial fingerprints has optical properties similar to human skin.
Skin Conductivity	Can be by some saliva on the artificial fingerprints.
Perspiration	User with low moisture may not be able to use a fingerprint scanner, and highly Perspiration fingers may nor exhibit liveness.
Surface Coarseness and detection of fine-movements of fingertip surface	More investigation needs to be done to evaluate the effectiveness and feasibility of such methodology

Fig. 2: Perspiration: change of captured fingerprint in time

IV. Proposed Method For Spoofing

The spoofing attack in fingerprint detection system attack is made by duplicating a real fingerprint with gelatine, silicone, clay-doh etc. In this paper a new method is proposed to make an artificial fingerprints. The artificial fingerprints are made by creating a mold by using fevicol. The process of creating mold is described as below:

- Take some heated wax (molten) in a container and leave it undisturbed for some time and after that make depression of finger in the wax (Figure 3).
- A thin layer of fevicol is applied on the depression created by fingers in the wax and removed properly after 15-20 minutes.
- The pattern of ridges and valleys get printed on the fevicol covering (figure 4) .

Fig. 3: Depression of finger in the wax

Fig. 4: Artificial fingerprints using fevicol

This wafer thin layer is used as an artificial fingerprint to spoof the sensor. At the time of enrollment person uses his live finger. But at the time of verification, if intruder uses this artificially created mold in the biometric device, the device will match this artificial finger print with the enrolled live fingerprints. The fingerprints which are made using fevicol can easily spoof the fingerprint sensor.

V. Conclusion

In this paper various spoofing and anti-spoofing methods are explored. The new method is also proposed to spoof the fingerprint system which increases the emerging need to find the method to protect the finger print system from this spoofing attack. As, security is the major concern in the biometrics, so the researchers should focus their efforts to make biometric devices more roburst and secure and the research must be ongoing.

References

[1] T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, "Impact Of Artificial "Gummy" Fingers On Fingerprint Systems", In Proceedings Of Spie Vol. #4677, Optical Security And Counterfeit Deterrence Techniques Iv, Yokohama National University, Japan, January 2002.

[2] A. K. Jain, A. Ross, U. Uludag, "Biometric Template Security: Challenges And Solutions," In Proceedings Of The European Signal Processing Conference (Eusipco '05), Antalya, Turkey, September 2005.

[3] T. V. Putte, J. Keuning, "Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned", In Proceedings Of Ifip Tc8/Wg8.8 Fourth Working Conference On Smart Card Research And Advanced Applications, September 2000.

[4] International Biometric Group, "Liveness Detection In Biometric Systems", White Paper, 2003.

[5] S. A. C. Schuckers, "Spoofing And Anti-Spoofing Measures", Information Security Technical Report, Clarkson University And West Virginia University, December 2002.

[6] S. A. C. Schuckers. Spoofing And Anti-Spoofing Measures. Information Security Technical Report, 7(4):56–62, December 2002.

[7] Dr. E. Hill And Dr. M. D. Stoneham. Practical Applications Of Pulse Oximetry, 2000.

[8] M. Drahansky, R. Notzel, W. Funk, " Liveness Detection Based On Fine Movements Of The Fingertip Surface", In: 2006 Ieee Information Assurance Workshop, June 21-23, 2006, Pp. 42–47 (2006).

[9] Y.S. Moon, J.S. Chen, K.C. Chan, K. So, K.C. Woo, "Wavelet Based Fingerprint Liveness Detection", Electronics Letters 41(20), 1112–1113 (2006).

[10] S.Memon, Member, Ieee, N. Manivannan, Member, Ieee, W. Balachandran Fellow, Ieee, "Active Pore Detection For Liveness In Fingerprint Identification System", 19th Telecommunications Forum Telfor 2011, Serbia, Belgrade, November 22-24, 2011.

