Liveness and Spoofing in Fingerprint Identification: Issues and Challenges

MOJTABA SEPASIAN, CRISTINEL MARES, WAMADEVA BALACHANDRAN
School of Engineering & Design
Brunel University
Uxbridge, Moddlesex, UB8 3 PH
UK
Mojtaba.Sepasian@brunel.ac.uk, Cristinel.Mares@brunel.ac.uk,
Wamadeva.Balachandran@brunel.ac.uk

Abstract: - The fingerprint liveness detection refers to the inspection of the finger characteristics to ensure whether the 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. However, it is not declared by the manufacturers of these systems whether liveness detection is actually implemented. Possible measures to detect liveness are only proposed in patents and published literature. There are three major schemes, which are reported in fingerprint liveness literature. These coupled with the additional hardware, software, or combination of fingerprint with other identifications is aimed to verify the liveness in submitted fingerprints. The hardware-based methods use auxiliary sensors to detect the biological and physiological measurements from finger, whereas software-based methods utilize changes in physical properties that take place in early stages of pressing the finger. In this paper, various fingerprint liveness detection methods, which are categorized as voluntary and involuntary, are explored. These 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) liveness detections. The main objective of this paper is to critically review the voluntary and involuntary fingerprint liveness detection techniques proposed in the literature, and discuss their effectiveness and possible limitations.

Key-Words: - Liveness Detection, Spoofing, Fingerprint, Biometric Security, Voluntary and Involuntary Technique

1 Introduction

Today the employment of biometrics has increased considerably (with applications in different scenarios such as social identification, access control to the network, and obtaining permission to pass the border) and it has become accepted as very secure methods for identification and authentication of individuals. Some other techniques such as key distribution system, password and ID cards are currently used widely, but present specific deficiencies as being easily forged, lost, forgotten, and stolen. A solution to increase the security of these methods is that of using biometrics which has significant advantages compared with traditional methods, due to impossibility of lost or stolen identity. Many scientists believe already that in the very near future biometrics will play an important role in our lives (be it users entering an office or home, starting a vehicle, talking on a cellular phone, logging into a computer, or purchasing merchandise). The use of fingerprints as a biometric is most prevalent today in many commercial, civil, and forensic applications. Small size, low price, good performance, convenience, and user-friendliness are the key drivers for embedding fingerprint sensors in various applications. In the last decade, many hardware and software technologies have been designed and implemented to capture and process fingerprint. In spite of these advantages, detecting liveness of a presented fingerprint sample has become a challenging research issue [1] [2], due to the possibility of defeating the fingerprint authentication. Although some biometric technologies such as facial thermogram and vein pattern may be considered stronger and more difficult to simulate artificially, these technologies are not widely implemented and will need to be validated as reliable biometric identifiers [3].

Liveness detection (vitality detection) in a biometric system means the capability of the system to detect if a presented biometric sample is alive or not. In addition, to check that the sample belongs to the live enrolled and not just any live human being, it is necessary to guard against artificial fingerprints [4]. Liveness detection can be executed either at the acquisition or at processing stage in two approaches, liveness detection and non-liveness one (e.g. detecting bubbles in gelatine artificial fingerprints) [5]. The main concern in fingerprint techniques is at what level of security one can rely on fingerprint readers (e.g. travel authentication like passports or access to nuclear facilities). A fingerprint reader is the front end of a fingerprint authentication system. This unit captures the fingerprint image by a sensor, which is usually one of the optical or solid-state type. There are many techniques to recognize the liveness of presented data at sensor level. In this paper, various countermeasures to avoid spoof attacks at fingerprint sensor level are explored in voluntary and involuntary forms. These techniques are based on determining the presence of a user by different responses. This can be from either voluntary source such as passwords, smart cards, and multiple biometrics (which makes spoofing more difficult), or involuntary liveness detection such as pulse oximetry, blood pressure, and heartbeat. In the voluntary case, the required response is based on the reaction of the user to hearing, seeing or feeling something. Involuntary on the other hand is about the user automatically responding to a stimulus, such as muscles responding to electrical stimulation, or skin changing colour when pressure is applied.

Although many fingerprint liveness countermeasures to avoid spoof attacks are presented in the literature, the majority lack proven results and additional hardware requirements, and do not operate efficiently in different environments (such as indoors, outdoors, summer and winter). For instance, 3M Blackstone liveness testing project (measured electrocardiograph signals (ECG), blood oxygen levels and pulse rate) was discontinued because of the disrupting effects caused by user movements during the ECG synchronizing stage. It was also quite difficult for the users to remain motionless and hold their fingerprints in the required position for six to eight seconds [3]. In addition, there are a number of other limitations with the required hardware such as price, size, and inconvenience for the user and in some cases, the possibility to fool the system by presenting an artificial fingerprint. The list of possible attacks is continuously growing and not all the extra hardware systems, which are needed to test and analyze the data, are available as COTS (Commercial, Off-The-Shelf) items.

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. Amongst the recommended solutions, an attempt is made to select the most effective one.

2 Sensor attacks and possible tenability

Parallel to improving the fingerprint based system technologies, the various types of attack and forging are improving. Due to the new software and hardware technologies for editing (e.g. Adobe Photoshop), making an artificial fingerprint has become easier than ever. For instance, by using high-resolution camera, one can get better photographs of the fingerprints; or by adding a preservative to increase the usability of gelatine employed for storing fingerprints can last even longer than a week (artificial). 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:

The registered finger:

- Stealing fingerprint of a user by casting it into a mould, or causing user to press against sensor either directly or indirectly by way of drugs;
- Separating finger from legitimate user's body ;

In this case, combining the fingerprint scanner with another authentication method such as password or ID card can be used as a countermeasure. Alternatively, a control measure to alarm when under duress, or have supervision in place as one controls the other (two-person implementation where system requires fingerprint from two different people) are possible solutions. Obviously, this is not always feasible.

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. The probability of a successful attack is based either on the high FAR of the system, or in the case of categorized system as "loops", "whorls", or "arches", by presenting the similar unregistered pattern as registered finger. In this kind of attack, the countermeasures can be a) to reduce the FAR of the system; b) in the case of categorized systems, to evaluate both the categories of fingerprints and the fingers within each category [1].

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].

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].

The others: In addition to identified types of attack in fingerprint sensor level, there are various types of attacks such as flashing a light against scanner, heating up, cooling down, humidifying, impacting on, and vibrating the scanner outside its environmental tolerances. Moreover, using the residual fingerprint on the sensor surface by dusting graphite powder, pressing adhesive film on surface, and many other possible attacks in specific sensor type exist [1]. In addition to above identified attacks, Jain et al [6] list a number of other types of attacks as follows:

1. **Denial of service (DoS):** Damages the system by attacker while a legitimate user has no longer access to system;
2. **Circumvention:** Allows access to system and data by unauthorized user to get either access he may not be authorized to (privacy attack) or manipulate the system to be used for illegal activities (subversive attack);
3. **Repudiation:** Denies having accesses to system by authorized user to obtain double personal benefit;
4. **Contamination or covert acquisition:** Provides access to system by unauthorized user with compromised knowledge of a legitimate user (e.g. lifting the latent fingerprint of a user and making an artificial fingerprint by attacker, or recording the voice sample of legitimate user and playing it back);
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. Next section reviews various general protection schemes to find optimum solution to improve the security and accuracy of fingerprint systems at the sensor level.

3 Protection & Countermeasures

In the case of non-liveness detection fingerprint, verification system is very vulnerable against artificial fingerprint attacks from user leaving behind fingerprints every day everywhere without noticing. As a result, with possible attacks either identified above or any other method, employment of such systems is inappropriate for any application unless a preliminary investigation is carried out in order to assess the capacity of the system to ensure liveness. 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 addition, in a live biometric system, it is difficult for an individual to repudiate the executed transaction or access a secure facility or data. However, design decisions are based on the specific needs of a biometric application. 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 [2, 4, 5, 7, 9-20]. In this paper, 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). Furthermore, some of the well-known techniques in both will be dealt with briefly. For now, such techniques are based on determining the presence of user by different responses from either voluntary or involuntary source.

4 Involuntary captured information by biometric reader

The main problem with fingerprint scanner is distinguishing between real fingerprints (i.e. silicone rubber) and other not alive fake fingerprints such as epidermis of a finger [2]. This section reviews the published literature on involuntary techniques based on automatic (without intention) acquisition of data from the user's body. Generally, the involuntary techniques can be divided into the acquisition of data with additional hardware, and use of existing information in fingerprint without any hardware requirements. The main concern with using additional hardware is adjusting the scanners to operate efficiently in different environments (such as indoors, outdoors, summer and winter), leading to problems with using a wafer-thin artificial fingerprint glued onto a live finger [2]. In addition, there are a number of other limitations with this scheme such as price, size, inconvenience for the user, and possibility to fool the system by using an artificial fingerprint [5]. Although not all of the extra hardware systems available at COTS (Commercial, off-the-shelf) have disclosed characteristics, some well-known methods in both categories evaluated by other researchers are described in this section.

4. 1 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 [2].

4. 2 Blood pressure: This method is not susceptible to a wafer-thin silicone rubber glued to a finger. Excluding single point sensors that must be entered directly into the vein, other available sensors at COTS require measurements at two different places on the body (e.g. both hands). In addition, it can be bypassed by using underlying finger's blood pressure [2].

4. 3 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, which makes it virtually impossible to use in order to consider a person's heart rhythm when scanning the fingerprint (e.g. different rhythms for same user). In addition, user's emotional condition and level of activity will affect the heartbeat [2].

4. 4 Odor: In this scheme, detecting the liveness of fingerprint is based on the acquisition of the odor by means of an electronic nose, and discriminating between human skin with other material. In spite of the fact that this method is able to discriminate real fingerprints from artificial reproductions, creation of a single model of human skin, rather than a template, for each user is necessary [7].

4. 5 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 [2].

4. 6 Detection under epidermis: This is based on detecting fingerprint patterns in the epidermis and between epidermis and dermis as a sign of liveness. There are two types of sensors: ultrasonic sensor and electric field one. Ultrasonic sensors focus on the fact that the underlying layer is softer and more flexible than the epidermis. While electric field alternative are focusing attention on the higher electric conductivity of the layer underneath the epidermis as compared to the epidermis itself. Two different layers of artificial fingerprints with the appropriate characteristics could fool the scanner when the characteristics of sensor are known. For instance, in the case of using ultrasonic sensors made of flexible and soft print, a second regular artificial print can be attached to the first while making sure that the two line patterns are in exact matching positions. This can be achieved very easily by a dental technician [2].

4. 7 Relative Dielectric Constant: Other terms for this technique are relative static permitivity or dielectric constant. The dielectric constant of a specific material reflects the extent to which it concentrates the electrostatic lines of flux [8]. Measuring the distinct values of relative dielectric constant (RDC) between a live and an artificial fingerprint is the foundation for this method. However, RDC is influenced by the humidity of finger in different conditions, and fooling such sensor is possible by wetting the silicone rubber using alcohol/water mixture before it is pressed on the fingerprint scanner. Since the RDCs of alcohol and water are 24 and 80 respectively, and the RDC of a normal finger is somewhere between the two [2], it is easy to fool the sensor.

4. 8 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].

4. 9 Pulse Oximetry: This technique is based on measuring the arterial oxygen saturation of hemoglobin in a pulse [9, 10]. It can be deterred by using translucent artificial fingerprint (e.g. gelatine) [10].

4. 10 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. Two optical solutions are proposed for measuring characteristic periodic changes of the fingertip volume. The first is based on a system composed of a CCD camera and a macro objective to acquire images and analyze that with respect to fine movements of the papillary lines to draw on the volume changes. 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. 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) [11].

4. 11 Involuntary challenge-response: This technique is based on determining the presence of a user by automatically (without intention) responding to the requested challenge. For instance, user's response to a stimulus such as muscles' to electrical stimulation or change in the color of skin when pressure is applied [5]. An implemented instance of an involuntary challenge-response is found in the US patent detector, based on the finger's electrical reaction to the small impulse, which outranges response of predefined acceptable values assumed as fake [12]. There are two kinds of limitations with this technique: first lack of acceptability because of using the uncomfortable stimulus such as shocking. Second is difficulty with distinguishing between the challenged person and the true owner of the fingerprint presented to sensor [5].

4. 12 Surface coarseness: This new liveness detection approach is based on analyzing an intrinsic property of fingertips: surface coarseness (Figure 1). 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 [13]. However, experimental results demonstrate the effectiveness of this technique on high-resolution fingertip images (~1000 dpi) [13]. Feasibility of such method is dependent on high-resolution fingerprint, which is not compatible with all current sensors.

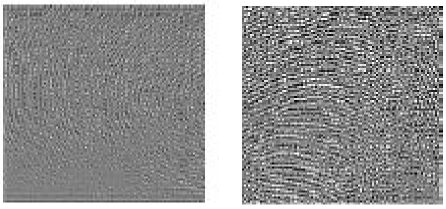

Figure 1 Using wavelet based denoising. For left noise residue Standard Deviation = 11.5 while right image has noise residue Standard Deviation = 36.5 [13].

4. 13 Underlying texture and density of the fingerprint images: In this approach, detecting "liveness" associated with fingerprint scanners is based on the underlying texture and density of the fingerprint images (Figure 2). As first step, multiresolution texture analysis techniques are used to minimize the energy associated with phase and orientation maps.

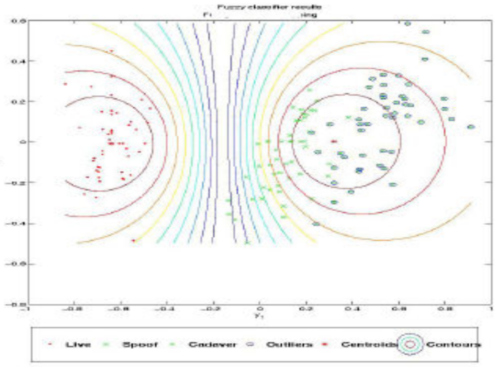

Figure 2 Result of the FCM classifier. The left centroid is for live fingerprints and right for not live [14].

Subsequently, cross ridge frequency analysis of fingerprint images is performed by means of statistical measures and weighted mean phase is calculated. As a final point, these different features along with ridge reliability or ridge center frequency are given as inputs to a fuzzy c-means classifier. Although, the algorithm has 95.36% classification for the limited data, more investigation with multiple scanners and different underlying technologies are required to validate the ability of such a scheme [14].

4. 14 Perspiration: This is based on detecting the perspiration phenomenon between the human skin and other material under different conditions. In spite of the advantages, it is usually possible to deceive fingerprint systems by presenting a well-duplicated synthetic or dismembered finger. However, Derakhshani et al [15] introduced one method to provide fingerprint vitality authentication in order to solve this problem. In their approach, vitality through fingerprint examination in conjunction with capacitive scanners (based on detection of the sweating pattern from two consecutive fingerprints), is captured during 5 seconds and a final decision about vitality is made by a trained neural network [12]. In addition, there are some other methods such as enhanced perspiration detection algorithm, which improves Derakhshani's work by including other fingerprint scanner technologies and use of larger, more diverse data sets along with shorter time windows [16]. Another technique is based on the statistics of wavelet signal processing to detect the perspiration phenomenon [17]. However, this technique has less ability for users with low moisture and highly perspiration-saturated fingers, and may not exhibit liveness due to the necessity of specific changes in moisture. Therefore, more investigations in terms of accuracy and environmental conditions are required to prove efficiency of such system [5].

4. 15 Valley noise analysis: This software-based method distinguishes between the live and artificial finger, using noise analysis along the valleys in the ridge-valley structure of the fingerprint images. The features are extracted in multiresolution scales using the wavelet decomposition technique, and liveness detection separation is performed using classification trees and neural networks. Dissimilar to live fingers which have clear ridge-valley structures; artificial fingers have a distinct noise distribution due to the material's properties when placed on a fingerprint scanner [18]. However, results show that this technique is very efficient (90.9–100%) for the capacitive, optical, and electro-optical scanners [18]. Efficiency of such method for all sensors though, needs especial investigation of each sensor specification.

4. 16 Spectrographic Properties: This technique is based on the analysis of the spectrographic properties of living human tissue (Figure 3 a) for fingerprinting. In this method, multispectral imaging technology (MSI) uses multiple illumination wavelengths rather than the monochromatic illumination used in total internal reflectance (TIR) imaging. In addition, polarizers can be utilized for the purpose of light penetrating surface that scatters several times by the time it leaves skin towards imaging array (Figure 3 b). Inexpensive films and materials are proved inefficient against this method [19]. Although, TIR image quality is poor for people with dry skin, it has little or no effect on an MSI sensor. This ability to detect subsurface features of the fingerprint, based on the difference optical properties of human skin and synthetic material observed with the MSI sensor, enables this technology to detect spoof material [19, 20]. Therefore, to enhance usability and security for a fingerprint system that incorporates an MSI-based sensor; more investigations need to be implemented [20].

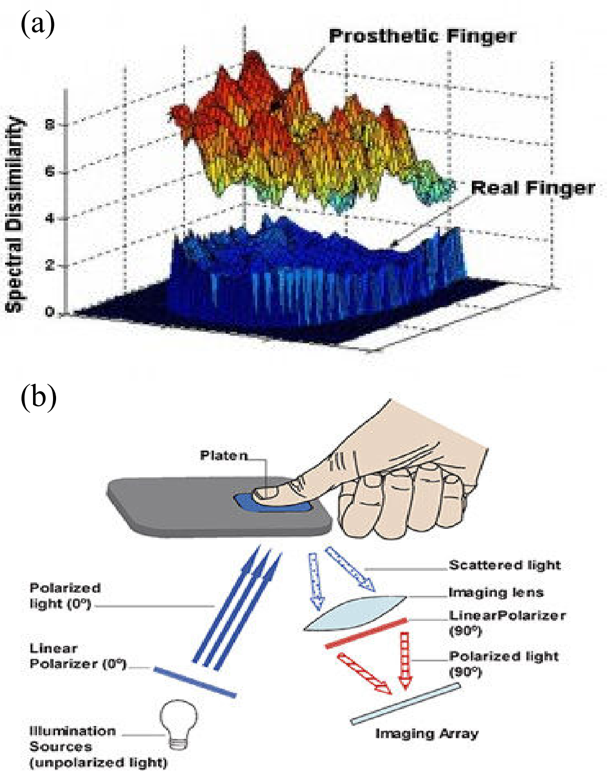

Figure 3 a: Spectral-characteristics-of-spoofs and real fingerprint [19] and **b**: Schematic of multispectral imaging elements [20]

4. 17 Skin deformation: This technique is based on the information about how the fingertip's skin deforms when pressed against a surface. For instance, there are non-linear distortions between fingerprint impressions of the users, who are required to touch the sensor twice or move it once it has been in contact with the sensor surface. However, artificial fingerprint with the same type of requirements will only give a rigid transformation between the two fingerprint impressions and produce quite similar non-linear deformations as a live fingerprint [22].

Methods	Liveness Detection Technique	Limitations
Involuntary Measurements	Epidermis Temperature	Lack of ability to detect the Wafer-thin silicone rubbers
	Blood Pressure	Can be fooled by using underlying finger's blood pressure
	Electrocardiogram (EKG)	Disrupting the system by user movement during the EKG synchronizing
	Pulse Oximetry	Can be deterred by using translucent artificial fingerprint
	Odor	Creation of a single model of human skin, instead of a template for each user is necessary
	Heartbeat	Practical problems with diversity in heart rhythm of a user
	Detection under Epidermis	Can be fooled by two different layers of artificial fingerprints with the appropriate characteristics
	Relative Dielectric Constant	Influenced by the humidity of the finger in different conditions and can be fooled by wetting the silicone rubber
	Optical Properties	Gelatine artificial fingerprint has optical properties very similar to human skin
	Skin Conductivity	Can be fooled by some saliva on the silicone artificial fingerprint
	Skin Deformation	Can be fooled by artificial fingerprint with the same type of requirements for original fingerprint
	Pores	Possibility to produce coarse reproduction of intra-ridge pores with gelatine artificial finger
	Perspiration	Users with low moisture may not be able to use a fingerprint scanner, and highly perspiration-saturated fingers may not exhibit liveness
	Involuntary Challenge-response	Lack of acceptability and difficulty when distinguishing between challenged person and true owner of the fingerprint
	Underlying Texture and Density	Lack of relevant independent studies based on a very large number of users and effects of long-term experience on FRRs and FARs
	Surface coarseness	
	Fine Movements of the fingertip surface	
	Valley noise analysis	
	Spectrographic Properties	

Table 1: Reported fingerprint involuntary liveness detection methods and limitations

4. 18 Pores: This is based on using a very high-resolution sensor to acquire a fingerprint image, and therefore, fingerprint details (e.g. sweat pores) can be used for liveness detection since they are more difficult to copy in artificial fingerprints [22]. However, it is possible to coarse reproduction of intra-ridge pores with gelatine artificial fingerprints [1].

4. 19 Other Claims: In addition to aforementioned liveness detection methods, there are several other claimed methods and techniques, which are neither well known due to commercial confidentiality or not properly validated yet (e.g. electrocardiography) [2]. The possible classification of involuntary liveness detection methods is shown in Table 1.

5 Measuring the voluntary properties of user's body or user's response

As discussed above, involuntary liveness detections are suffering from a number of limitations such as low acceptability, lack of proven established results and additional hardware requirements, and cannot operate efficiently in different environments. Therefore, in this section voluntary techniques will be investigated in order to address some of these limitations of involuntary approach. However, it is clear that voluntary techniques have higher acceptability rate due to the detection of life signs from user (with intention) manually at the requested challenge. A possible classification of voluntary liveness detection methods, available in the literature, is presented in the following:

5.1 Using multiple biometrics: Vulnerability against spoof attacks and liveness problems in unimodal biometrics can be addressed through multimodal biometric technique, which is based on the presence of multiple biometric traits by the user. Despite using the multiple evidence provision of the same identity through multimodal systems, it may resolve difficulties of individual match verification systems. Implementing such system is currently much more difficult than it seems due to environmental, cost, or equipment limitations. Multimodal biometric systems can be designed to operate in five different scenarios:

a. Multiple sensors: The information derived from various sensors for the same biometric are integrated. For instance the use of multiple fingerprint sensors (ultrasonic and optical) in order to capture different fingerprint features of user;

b. Multiple biometrics: Combining more than one biometric such as combining fingerprint and face. There will be more than one sensor in this scenario and each sensor is used to sense a different biometric trait. Therefore, it is more difficult for an attacker to create both an artificial fingerprint and another artificial biometric identifier such as iris, voice, or face;

c. Multiple units of the same biometric: Enrolling more than one finger can be used as identification/verification by either randomization of requested fingers (e.g. two fingerprints) to identify/verify, or requesting all fingers enrolled for identification/verification. This can reduce the likelihood of spoofed data being usable for verification;

d. Multiple snapshots of the same biometric: Multiple samples of the same finger are combined and each should be identified and verified correctly. This technique decreases the FAR and probably increases the FRR with artificial fingerprints. It suffers from low acceptability due to the inconvenience for users;

e. Multiple representation and matching algorithms for the same biometric: In this scenario, different approaches to feature extraction and matching of the biometric characteristic are combined [21].

5.2 Retention of identifiable data: Retaining image data (i.e. not destroyed data immediately after template generation) albeit posing substantial privacy and storage challenges may provide a means of resolving spoof claims [4].

5.3 Using multi-factor authentication: Although using biometrics with password-protected smart cards reduces the probability of biometric systems being spoofed, it can be lost or stolen and reduces the convenience provided by biometrics. In addition, it is not possible to employ such techniques in every application, especially in the case of availability of users in large numbers, which makes the template database much bigger than any allocated space in smart card [4].

5.4 Fingerprint with password: Using a password as identification is a very well known of the traditional methods. Besides, integration of password with fingerprint systems may reduce the associated security risk and possibility of forging with this traditional system. Such a system still suffers from lost or forgotten passwords. In addition, by using artificial fingerprint and stolen password, there is a high possibility to counterfeit such identification. However, this system is currently used in a number of applications such as wireless devices (e.g. laptop, mobile phone) due to affordability and high acceptability with user.

5.5 Supervision: This technique is based on surveillance identification, verification, and enrolment to increase the security. Hence, it is more difficult to circumvent a system when being watched. However, this technique suffers from difficulty for a supervisor to detect transparent gelatine artificial print glued onto a live finger [9].

5.6 Voluntary challenge-response: This technique is based on determining the presence of a user by a response to the requested challenge (e.g. place of birth). In voluntary case, required response is based on the reaction of the user to hearing, seeing, or feeling something. Dissimilar to involuntary, voluntary techniques do not suffer from the lack of acceptability from using uncomfortable stimulus such as shocking (e.g. ask the user to enter the pin code). However, distinguishing between the challenge-respond person and true owner of the fingerprint presented to the sensor is still a challenging issue in this technique [5, 9]. Table 2, illustrates the possible classification of voluntary liveness detection methods.

Methods	Voluntary Measurements	Limitations
Multiple biometrics	Multiple sensors	Increases the timing, measurement and cost
	Multiple biometrics	
	Multiple units of the same biometric	
	Multiple representation and matching algorithms for the same biometric	Increases the timing, measurement and complex algorithms
	Multiple snapshots of the same biometric	Increases the timing, measurement and decrease acceptability
Retention of data	Retaining image data	Increases the timing, measurement and cost
Multifactor authentication	Fingerprint with password	Can be fooled by artificial fingerprint and stolen password
	Fingerprint with password-protected smart cards	Can be lost or stolen and reduces the convenience provided by biometrics
Challenge response	Reaction of the user to hearing, seeing, or feeling something	Difficulty of distinguishing between the challenge-respond person and true owner

Table 2 Reported fingerprint voluntary liveness detection methods and limitations

4 SUMMARY AND DISCUSSION

Various methods in the public domain for artificial fingerprint attacks and countermeasures have been reviewed in this paper. Although these countermeasures have significant advantages for detecting artificial fingerprints, there are a number of limitations with them as a) the incompatibility of liveness techniques with some fingerprint sensors, which is increasing the measurement time, cost, and lack of proven results, b) there is no clear criterion for all sensors and scenarios, and none of available methods in the literature have the ability to cover all requirements independently. Therefore, any offered solutions for specific scenarios, and sensors, depend on especial investigation of that scenario, individual acquisition, and related tenability of each sensor. Different environments and conditions used depend strongly on each sensor specification and each application requirement. Furthermore, more work needs to be done to verify these claims and evaluate security levels of each of them. Generally, increase in the security of fingerprint system depends on the high recognition performance and liveness detection of user. However, many liveness detection techniques in the COTS (Commercial, Off-The-Shelf) and public domain claim to have had successful operations. Nevertheless, what is really not clear is proven efficient output (i.e. FRRs and FAR) in large number of users, and tenability experiences over long period of time. In this regard, using multibiometric have a number of advantages which includes higher recognition, liveness detection, higher acceptability, and lower possibility of defeat due to difficulty for attacker to create both an artificial fingerprint and another artificial biometrics. However, it can increase the additional cost of sensors and authentication time, which can cause inconvenience for the user. From the above review, one can conclude that the security represents in fact, the prioritization of risks followed by coordinated and economical application of resources to minimize, monitor and control the negative effects (or even to accept some or all of the consequences of a particular risk), which is similar to other published works in the field [22].

Although the purpose of this review was to present the particular liveness methods for use in fingerprint identification systems, a number of problems are preventing suggestions for perfect technique. The liveness technology market is changing rapidly, standards are not widely supported, and performance depends on the operational environment and life cycle cost of the technology. Furthermore, parallel to improving the liveness detection technologies, various types of attacks and forges are improving as well, and consequently the liveness detection systems should be one-step ahead in order to be efficient.

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] 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.

[3] J. Woodward, N. M. Orlans, P. T. Higgins, "Biometrics", New York, McGraw Hill Osborne, ISBN: 0072230304, December, 2002.

[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] 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.

[7] D. Baldisserra, A. Franco, D. Maio, D. Maltoni, “Fake Fingerprint Detection by Odor Analysis”, In D. Zhang and A.K. Jain (Eds.): ICB 2006, LNCS 3832, (2005) 265-272.

[8] S. E. Braslavsky "Glossary of terms used in photochemistry (IUPAC recommendations 2006)", Pure and Applied Chemistry 79: 293–465; see p. 32, 2007.

[9] M. SandstrÄom, “Liveness Detection in Fingerprint Recognition Systems”, Linkopings University, Master Thesis, Sweden, June 2004.

[10] E. Hill, M. D. Stoneham, “Practical applications of pulse oximetry”, Nuffield Department of Anaesthetics, Oxford Radcliffe NHS Hospitals Headington, 2000.

[11] 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).

[12] P Kallo, I. Kiss, A Podmaniczky, J Talosi, “Detector for recognizing the living character of a finger in a fingerprint recognizing apparatus”, Dermo Corporation, Ltd. US Patent, January 16,2001.

[13] 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 (2005).

[14] A. Abhyankar, S. Schuckers, “Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques,” 2006 IEEE International Conference on Image Processing, pp. 321-324, October, 2006.

[15] R. Derakhshani, S. Schuckers, L. Hornak, L. O'Gorman, “Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners”, Pattern Recognition. v36 i2. 383-396.

[16] S. Parthasaradhi, R. Derakshani, L. Hornak, S. Schuckers, “Time-series detection of perspiration as a liveness test in fingerprint devices”, IEEE Trans. Syst. Man Cybern. Pt. C: Appl. Rev. 36 (2) (2005), pp. 335–343.

[17] B. Tan, S. Schuckers, “Liveness Detection for Fingerprint Scanners Based on the Statistics of Wavelet Signal Processing”, In: IEEE CVPRW (June 2006).

[18] B. Tan, S. Schuckers, “New Approach for Liveness Detection in Fingerprint Scanners Based on Valley Noise Analysis”, SPIE Journal of Electronic Imaging 17(1) (2008).

[19] The page is available at “http://www.lumidigm.com/liveness-detection/”, last visit January of 2010.

[20] R.K. Rowe, K.A. Nixon, S.P. Corcoran, “Multispectral fingerprint biometrics”, Proceedings of the 2005 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY

[21] A. K. Jain, A. Ross, S. Prabhakar, “An introduction to biometric recognition”, IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image-and- Video-based Biometrics, January 2004, vol.14, p. 19-22.

[22] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, “Handbook of fingerprint recognition”, New York, Springer Verlag, 2003.