Fake Fingerprint Detection Methods

TanishaAggarwal[1] ,Dr.Chander Kant Verma[2]
[1]M.Tech. Scholar, DCSA, Kurukshetra University, Kurukshetra, India
[2]Assistant Professor ,DCSA, Kurukshetra University, Kurukshetra , India
[1]tanuaggarwal91@gmail.com, [2]ckverma@rediffmail.com

Abstract:-Security is a very important aspect in the biometric system. There are number attacks and there remedial solutions 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. Recently, research has shown that it is possible to spoof a variety of fingerprint scanners using some simple techniques with molds made from plastic, clay, Play-Doh, silicone or gelatin materials. To protect against spoofing, methods of liveness detection measure physiological signs of life from fingerprints ensuring only live fingers are captured for enrollment or authentication. This paper is devoted to various optical methods,which are supposed to be used for liveness detection on fingers.

Keywords: Biometrics, Fingerprints ,Liveness Detection.

1. INTRODUCTION

This paper discusses in brief about various methods to secure the biometric system from the fake fingerprints. Biometric systems are an emerging technology that enables the authentication of an individual based on physiological characteristics including face, fingerprint, iris, hand geometry, palm, or behavioral characteristics including voice, gait, keystroke dynamic and handwriting signature, etc .While biometrics may improve security, biometric systems are found to be vulnerable to attacks at the biometric sensor level, replay attacks on the data communication level, and attacks on the database . For example, previous studies have shown it is possible to fool a variety of fingerprint scanners using a well-duplicated synthetic finger made of silicone rubber, Play-Doh, wax, clay, gelatin, or in the worst cased, dismembered fingers . These materials are moisture based and most fingerprint scanners are able to image them . Face or iris recognition systems can be spoofed by static facial or iris images. To improves security for the biometric systems, liveness detection (or vitality detection) is proposed to defeat this kind of spoof attacks. Liveness detection is an anti-spoofing method ensuring that only the biometric from a live, authorized person is submitted for enrollment, verification and identification .

1.1Biometric Overview

Biometrics (also known as biometry) is defined as “the identification of an individual based on biological traits, such as fingerprints, iris patterns and facial features” [1].

1.2. Identification and Verification

Identification and verification (also known as authentication) are both used to declare the identity of a user. Since the two terms identification and verification are easily mixed up, definitions are given below [2]

- Identification: In an identification system, an individual is recognized by comparing with an entire database of templates to find a match. The system conducts one-to-many comparisons to establish the identity of the individual. The individual to be identified does not have to claim an identity (Who am I?). [2]
- Verification (authentication): In a verification system, the individual to be identified has to claim his/her identity (Am I whom I claim to be?) and this template is then compared to the individual’s biometric characteristics. The system conducts one-to-one comparisons to establish the identity of the individual. [2]

Before a system is able to verify/identify the specific biometrics of a person, the system requires something to compare it with. Therefore, a profile or template containing the biometric properties is stored in the system. Recording the characteristics of a person is called enrolment. [3]

1.3Biometric Techniques

Currently, there are many different techniques available to identify/verify a person based on biometrics [3]. These techniques can be divided into physical characteristics and behavioral characteristics. All techniques have in common that acquired data is compared with templates enrolled earlier.

1.3.1 Physical characteristics

The following are examples of biometric techniques based on physical characteristics [3]

- Fingerprint recognition: Fingerprint recognition systems scan the fingerprint pattern for recognition.

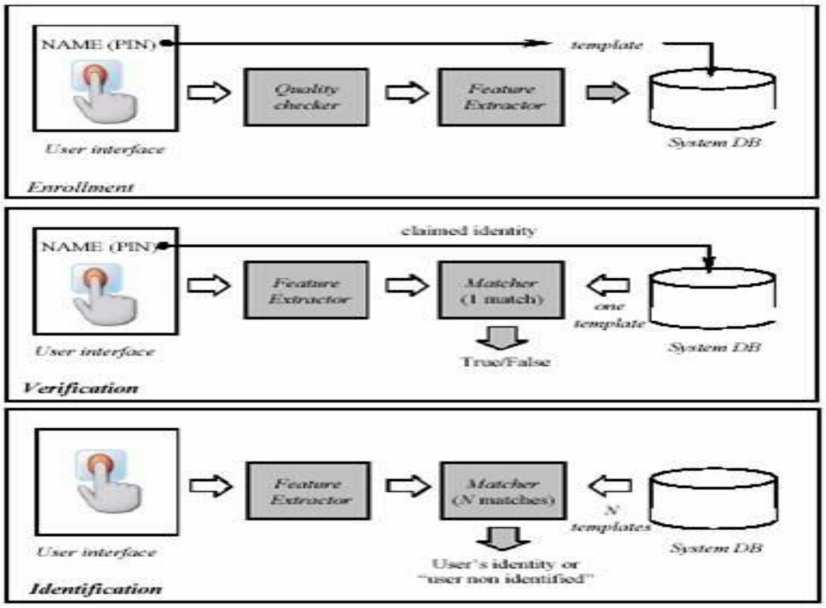

Fig.1 Enrollment, verification, and identification.

- Recognition of hand or finger: Recognition of hand or finger systems scan the entire hand or larger parts of the finger and makes a comparison of patterns in the skin (similar to fingerprint recognition systems). The difference between a fingerprint recognition system and a hand/finger recognition system, lie mostly in the size of the scanner and the resolution of the scanning array.
- Face recognition: Face recognition systems detect patterns, shapes, and shad- ows in the face.
- Face geometry: Face geometry systems work similar to face recognition sys- tems, but focus more on shapes and forms instead of patterns.
- Vein pattern recognition: Vein pattern recognition systems detect veins in the surface of the hand. These patterns are considered to be as unique as fingerprints, but have the advantage of not being as easily copied or stolen as fingerprints are.
- Retina recognition: Retina recognition systems scan the surface of the retina and compare nerve patterns, blood vessels and such features.
- Iris recognition: Iris recognition systems scan the surface of the iris to compare patterns.

1.3.2 Behavioral characteristics

The following are examples of biometric techniques based on behavioral character istics [4]

• Voice recognition: Voice recognition systems use characteristics of the voice, such as pitch, tone, and frequency.
• Signature recognition: Signature recognition systems measure pressure of the pen and frequency of writing to identify a person via a signature.
• Keystrokes dynamics: Keystrokes dynamics systems use statistics, e.g. time between keystrokes, word choices, word combinations, general speed of typing etc.

1.4 Attacks on Biometric Systems

1.4.1 Generic Security Threats

Any system (including biometric systems) is susceptible to various types of threats. These threats are discussed below:
i. **Denial of Service**: An adversary overwhelms computer and network resources to the point that legitimate users can no longer access the resources.
ii.Circumvention: An adversary gains access to data or computer resources that he may not be authorized to access.
iii.Repudiation: A legitimate user accesses the resources offered by an application and then claim that an intruder had circumvented the system.

iv. Covert acquisition: An adversary compromises and abuses the means of identification without the knowledge of a legitimate user.
v. Collusion: In any system, there are different user privileges. Users with super-user privileges have access to all of the system's resources. Collusion occurs when a user with super-user privileges abuses his privileges and modifies the system's parameters to permit incursions by an intruder [2].
vi.Coercion: A legitimate user is forced to give an intruder access to the system. For example, an ATM user could be forced to give away her ATM card and PIN at gunpoint [2].

1.4.1 Biometric security threats

i.Type 1: This point of attack is known as "Attack at the scanner". In this attack, the attacker can physically destroy or fake the recognition scanner and cause a denial of service as described in 1.4.1.

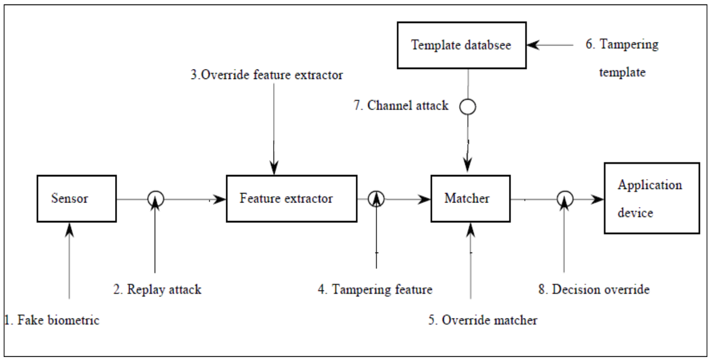

Fig.2: Attacks points in Biometrics Systems

ii. Type 2: This point of attack is known as "Attack on the channel between the scanner and the feature extractor" or "Replay attack". In this attack, the attacker intercepts the communication channel between the scanner and the feature extractor to steal biometric traits and store it somewhere. The attacker can then replay the stolen biometric traits to the feature extractor to bypass the scanner.

iii. Type 3: This point of attack is known as "Attack on the feature extractor module". In this attack, the attacker can replace the feature extractor module with a Trojan horse . Trojan horses in general can be controlled remotely. Therefore, the attacker can simply send commands to the Trojan horse to send to the matcher module feature values selected by him.
iv. Type 4: This point of attack is known as "Attack on the channel between the feature extractor and matcher". This attack is similar to the attack described in 1.4.1.
The difference is that the attacker intercepts the communication channel between the feature extractor and the matcher to steal feature values of a legitimate user and replay them to the matcher at a later time.
v. Type 5: This point of attack is known as "Attack on the matcher".This attack is similar to the attack described in 1.4.1. The difference is that the attacker replaces the matcher with a Trojan horse.
The attacker can send commands to the Trojan horse to produce high matching scores and send a "yes" to the application to bypass the biometric can also send commands to the Trojan horse to produce low matching scores and send a "no" to the application all the time causing a denial of service.
vi. Type 6: This point of attack is known as "Attack on the system database". In this attack, the attacker compromises the security of the database where all the templates are stored. Compromising the database can be done by exploiting vulnerability in the database software or cracking an account on the database. In either way, the attacker can add new templates, modify existing templates or delete templates.
vii. Type 7: This point of attack is known as "Attack on the channel between the system database and matcher". In this attack, the attacker intercepts the communication channel between the database and matcher to either steal and replay data or alter the data.
viii. Type 8: This point of attack is known as "Attack on the channel between the matcher and the application". In this attack, the attackers intercept the communication channel between the matcher and the application to replay previously submitted data or alter the data.
ix. Type 9: This attack is called "Attack on the application". Bugs are a consequence of the nature of the programming task that no one can deny. It is a fact that any software has at least one bug in it. Since biometric authentication systems are not 100% accurate, most of these systems use traditional authentication schemes as a backup.

1.5.Liveness Detection

Liveness detection (sometimes called vitality detection) in a biometric system means the capability for the system to detect, during enrollment and identifica- tion/verification, whether or not the biometric sample presented is alive or not. Furthermore, if the system is designed to protect against attacks with artificial fingerprints, it must also check that the presented biometric sample belongs to the live human being who was originally enrolled in the system and not just any live human being.

Silicon, gelatin, and rubber are the some of the materials that can be used to make fake fingers.

Liveness detection can be performed either at the acquisition stage, or at the pro- cessing stage. For example, an optical fingerprint scanner would create an image of an eraser, but not extract any features; the liveness detection takes place at the processing stage. A capacitive fingerprint sensor on the other hand, would not even create an image of the eraser; the liveness detection takes place at the acquisition stage[5].There are two approaches in determining if a finger is alive or not; liveness detection and non-liveness detection. The material or data used to spoof a system often have a number of different non-liveness characteristics that could be used to detect non- liveness.

An example of a non-liveness detection detection method would be to detect air bubbles in gelatin artificial fingerprints.

Most biometric systems today have a decision process which first checks liveness:

```
                    if data = live
            perform acquisition and extraction
                    else if data = not live
      do not perform acquisition and extraction
```

This means that an intruder has the simpler task of imitating a live finger than circumventing a non-liveness detection mechanism. In fact, any detection mechanism can and will be defeated according to [5].

There are essentially three different ways to introduce liveness detection into a biometric system [6]:

- Using extra hardware to acquire life signs.
- Using the information already captured by the system to detect life signs.
- Using liveness information inherent to the biometric.

The first of these methods introduces a few other problems; (1) it is expensive, (2) it is bulky, and (3) it could still be possible to present the artificial fingerprint to the fingerprint sensor and the real fingerprint of the intruder to the hardware that detects liveness. Also, in some cases it is still possible to fool the additional hardware with a wafer-thin artificial fingerprint. The second method does not have these disadvantages, except maybe that it could be possible to still fool with an artificial fingerprint. It is on the other hand a bit more complicated to extract the life signs using no additional hardware.The third method of using inherent liveness information to the biometric, is not applicable to fingerprint recognition.The main problem of distinguishing between an artificial fingerprint and a real fingerprint, is that the epidermis (outer skin) of the finger is in fact not alive either.

2. RELATED WORK

The two major approaches are there to implement liveness detection. The first is hardware based approach and the second is software based approach.

2.1. Using exta hardware

The main problem with liveness detection methods based on extra hardware, is that the scanners have to be adjusted to operate efficiently in different kinds of environments, leading to problems when using a wafer-thin artificial fingerprint glued on to a live finger. Furthermore, using extra hardware will in many cases be inconvenient for the user.

2.1.1 Temprature

The temperature of the epidermis is about 26–30◦C. When using a thin silicone artificial fingerprint, this results in a decrease by a maximum of 2◦C of the tem- perature transfer to the sensor. Obviously, it will not be difficult to have the temperature of the artificial fingerprint within the working margins of the sensor. Sensors that are used outdoors often have a broader working margin, giving the intruder even better prerequisites. [3]

2.1.2 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. Also, practical problems arise due to changes in the pulse. A person with a pulse of 40 beats per minute implicates that the finger must be held for at least four seconds on the sensor for the pulse to be detectable.

The same person could have a pulse of 80 beats per minute if he or she worked out immediately before the fingerprint scanning. The emotional state of the person also affects the pulse. [3]

A US patent entitled Anti-Fraud Biometric Sensor that Accurately Detects Blood Flow by SmartTouch LLC describes how two Light Emitting Diodes (LEDs) and a photo-detector are used to determine whether blood is flowing through the finger. Earlier similar solutions have been possible to fool by simulating blood flow (through the use of a flashing light or by moving the imposters finger). This patent declares to have solved these problems by checking if the background light level is above a threshold and by detecting movement of the finger. This liveness detection method basically implements pulse oximetry, but only uses the pulse rate information [8]

2.1.3 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 measures 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]

2.1.4 Blood Pressure Detection

Apart from the same disadvantages as with measuring the pulse, measuring blood pressure adds another problem. The sensors available today (excluding the single point sensors that must be entered directly in the vein),require measurement at two different places on the body, e.g. on both hands. Also, blood pressure measurement devices are easy to fool by using a wafer-thin artificial fingerprint and the underlying finger's blood pressure.

2.1.5 Skin Electric Resistance detection

The electric resistance of the skin can range from a couple of kilo-Ohms to several mega-Ohms depending on the humidity of the finger. With some people having dry fingers, and others being sweaty, it is easy to realize that the span of allowed resistance levels will be great enough for an intruder to easily fool the system. For example, by putting some saliva on the silicone artificial fingerprint, the system will be fooled into believing it is the live finger. [3]

In [10], the electric resistance was measured to 16 MOhms/cm in a live finger and 20 MOhms/cm for the corresponding gelatin artificial fingerprint. In other words, the difference is so small between the two that it would be impossible to create liveness detection with this method without getting a too high FRR(False Rejection Rate).

2.1.6Combining ECG, Pulse Oximetry and temprature

A US patent from 1998, suggests using one or preferably more biometrical features for liveness detection [10]. Many examples of non-specific biometric parameters are given, but most preferably a combination of pulse oximetry, electrocardiography(ECG), and a temperature sensor is used. A CCD camera is used for the fingerprint identification/verification, and the skin temperature, pulse (both from ECG and optical readings which should correlate), and oxygen saturation of haemoglobin in the arterial blood, are used for a liveness measurement.

As mentioned earlier, the temperature sensor can be easily fooled with an artificial fingerprint. Also, detection of pulsation, pulse oximetry, and electrocardiogram can be fooled using a translucent artificial fingerprint (e.g. gelatin) which covers only the intruder's live finger's fingerprint [6].

Additionally, because of the ECG sensor, the user has to hold his/her finger still for six to eight seconds. This is quite a long time when it comes to these types of applications. If the user moves the finger, the measurement has to be started all over again. Because of this and other various reasons, the project was discontinued.

2.2 Using software based approach

The software based approach is more complicated but does not require any additional accessories as in the hardware based approaches. Existing fingerp[rint sensor can easily use this approach by just modify the software. There are various method for this:

2.2.1 Persipiration based method

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 3 below.

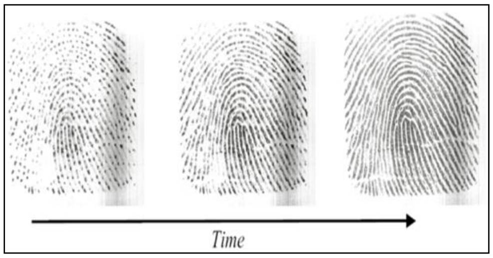

Fig.3. Perspiration: change of captured fingerprint in time [11]

2.2.2 Skin Deformation based method

This method is based on the difference of hardness (or elasticity). The difference of hardness will produce different deformations when pressing and rotating a finger on a sensor.

Liveness can be detected by comparing these distortions. The key point of this method is the difference of the material hardness. Thus, the method performs poorly when the hardness of fake material is similar to live skin, and users need some training process.

2.2.3 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 [2]. These fine details might be difficult to copy in artificial fingerprints.

According to [2], the work by Matsumoto et al. [9], showed that a coarse reproduction of intra-ridge pores is feasible with gelatin artificial fingerprints. The pores can however be coarsely reproduced, and even this should make you think twice before using a fingerprint device which uses the position and size of pores as liveness detection.

2.2.4 Image Quality based method

In fact, it is difficult to make a fake fingerprint image having the same or better image quality than that of live. In general, the quality of the fake fingerprint image is not good as live fingerprint image. Moon et. al. detected the liveness of a fingerprint by calculating the standard deviation of the fingerprint image using the wavelet transform. The advantage of this method is that it is fast and convenient to use. Although Moon’s work is only conceptual, it contributes an important hint that we can detect the liveness by checking the image quality.

But in [12] a method is applied by analyzing the finger prints with Discrete Wavelet Transformation(DWT).

The system is trained for certain fingerprint images and their rotated images and when the input image is given to the system ,it should recognize the person if there is a match. DWT is the transformation used for analysis and Canberra distance metric is used for similarity estimation.

The various phases include are:

A. 2D Discrete Wavelet Transformation
B. Feature extraction
C. Training
D. D.Texture Classification

2.2.5Detection of fine movements (based on Papillary Lines)[14]

One of the solutions is based on the analysis of fine movements of the pap- illary lines of the fingertips and on measurements of the distance of the fingertip surface to a laser sensor, respectively. The system is compact enough to be integrated with the optical fingerprint sensors.

There are two approaches to measure fine movements of papillary lines [13], 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 distance measurement with a laser sensor.

2.2.5.1 Camera System: An important aspect of the camera based liveness detection is analysis of the video stream. First of all, single frames of the video sequence are processed to find unique points (e.g. minutiae, sweat pores), which can be used as reference points to identify a region of the fingerprint that will be further analyzed.Human’s heartbeat causes small volumetric changes on the fingertip. As the fingertip expands, the distance between the papillary lines grows (Fig. 4). These fluctuations are small, but measurable and show similarities to a cardiogram. The video stream (or the sequence of images) is analyzed and filtered so that these movements can be observed. Cheating this method by applying a silicon layer (or another attack method) on the finger should change these characteristics considerably, so that such attack can be easily detected.

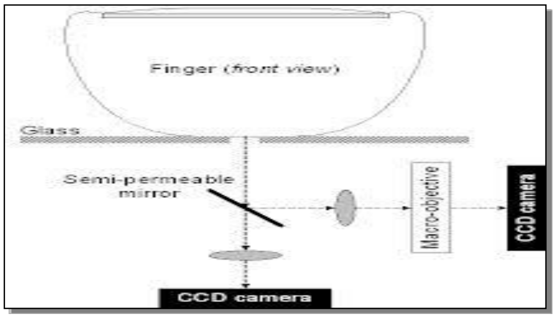

Fig. 4.Liveness detection with CCD camera[14].

Average volume changes of the fingertip (as measured by a laser range-meter) are 6.5 µm in the volume radius. According to the measured volume changes, the papillary lines move in average with a difference of 4.5 µm. The fingerprint (or the image respectively) must be zoomed so that the movements become detectable. Preliminary tests have been performed, but due to the low quality of the optics, the results are still ambiguous and the research is still going on.

The sequence of images captured by the camera has to be processed by various filters and edge detectors (e.g. Gaussian filter, Sobel and Laplace edge detector etc.). The edge detection algorithms sharpen the papillary lines and the Gaussian filter eliminates background noise and other unnecessary image information.

2.2.5.2. **Laser system**: The second optical method for liveness detection is a laser distance measurement, which is outlined in Fig. 5. The lens optical system and the CCD camera for acquisition of the complete fingerprint are the same as in Fig. 4.

In contrast to the solution,the laser distance measurement module, based on the triangulation principle, is placed to the right side of the glass plate, which is L- shaped here. The user places his finger such that it is in contact with the horizontal and the vertical side of the glass plate.

2.2.6.Band Selective Fourier Spectrum method[15]

The 2D spectrum of a fingerprint image reflects the distribution and strength in spatial frequencies of ridge lines. The ridge-valley texture of the fingerprint produces a ring pattern around the center in the Fourier spectral image and a harmonic ring pattern in the subsequent ring. Both live and fake fingerprints produce these rings, but with different amplitudes in different spatial frequency bands. Typically, live fingerprints show stronger Fourier spectrum in the ring patterns than the fake. This method classifies the live and the fake fingerprints by analyzing the band-selective Fourier spectral energies in the two ring patterns.

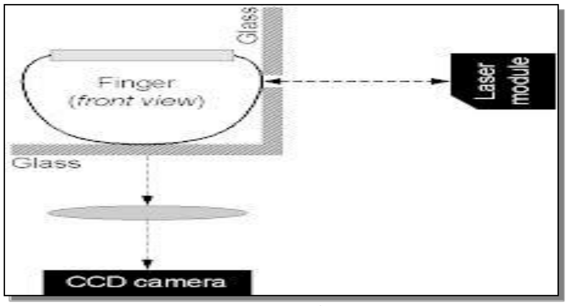

Fig. 5. Laser distance measurement for livenessdetection[14].

There are differences on overall spectral energy between live and fake spectral images. These differences are made by the size of the foreground of fingerprint image, the distribution of histogram, and the performance of the sensors. Figure1 depicts the computation of spectral energies in the inner and the outer rings. Figure 6 depicts the computation of spectralenergies in the inner and the outer rings.

The algorithm below describes the procedure for computing the energy in these three intervals. At first, the fingerprint image is converted into the spatial frequency domain using Fast Fourier Transform.

In order to avoid a big value contrast, logarithm operations are applied to the transformed image, and then the result image is normalized.

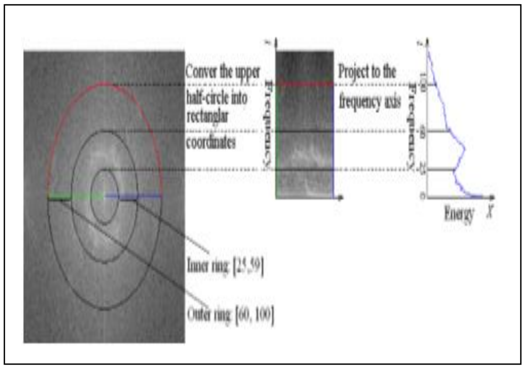

Fig. 6. The spectral image of fingerprint, the two ring patterns, and the computation of the Band-Selective energies[15]

The algorithm below describes the procedure for computing the energy in these three intervals. At first, the fingerprint image is converted into the spatial frequency domain using Fast Fourier Transform. In order to avoid a big value contrast, logarithm operations are applied to the transformed image, and then the result image is normalized. Subsequently, the upper half-circle of the spectral image is converted into a rectangular coordinate using the homogeneous rubber sheet model presented by Daugman and then projected to the frequency axis. Finally, these energies are accumulated on the three intervals: 25~59, 60~100, 1~100.

Algorithm:

1. 1.Transform the image using FFT(Fast Fourier Transform). Compute logarithm on FFT image and normalize it
2. 2.Convert polar coordinates to Cartesian coordinates
3. Project the rectangles onto the frequency axis.
4. Compute the Band-selective energy of inner, outer and overall rings.
5. Classify the fingerprint and detect the fake.

3. CONCLUSION

Spoofing is a real concern with regard to the security of biometric system. In this paper various methods are illustrated to prevent the attacker to fool the biometric system with fake fingerprints. More and more successful spoofing attempts are emerging and even though the sophistication of these attacks is on the rise and spoofing is still in its infancy.

Both industry and academia are focusing their efforts to make biometric devices more robust but every countermeasures can eventually be circumvented .Thus research and development efforts must be ongoing.

References

[1] P.McFedries. The word spy biometrics.Available at http://www.wordspy.com/words/biometrics.asp [accessed 12/05/04].

[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar. Handbook of Fingerprint Recognition. Springer Verlag, New York, NY, USA, June 2003.

[3] T. van der Putte and 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, pages 289– 303. Kluwer Academic Publishers, September 2000.

[4] J. Blomm´e. Evaluation of biometric security systems against artificial fingers. Master's thesis LITH-ISY-EX-3514-2003, Department of Electrical Engineer- ing, Link¨oping University, Link¨oping, Sweden, October 2003.

[5] International Biometric Group. Liveness detection in biometric systems, 2003. White paper. Available at http://www.biometricgroup.com/reports/public/ reports/liveness.html [accessed 12/05/04].

[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] P. D. Lapsley, J. A. Lee, Jr. D. F. Pare, and N. Hoffman. Anti-fraud biometric sensor that accurately detects blood flow. SmartTouch, LLC., US Patent #5,737,439, April 1998.

[9] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino. Impact of artificial "gummy" fingers on fingerprint systems. In Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, Yokohama, Japan, January 2002. Yokohama National University.

[10] D. Osten, H. M. Carim, M. R. Arneson, and B. L. Blan. Biometric, personal authentication system. Minnesota Mining and Manufacturing Company, US Patent #5,719,950, February 1998.

[11] S. Shuckers, L. Hornak, T. Norman, R. Derakhshani, S. Parthnasardi, "Issues for Liveness

[12] Detection in Biometrics", CEMR LDCSEE, West Virginia University, USA, 2006, p. 25.

[13] K.Thaiyalnayaki, S. Syed Abdul Karim P. VarshaParmar, "Finger Print Recognition using Discrete Wavelet Transform" ©2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 24.

[14] M. Drahansky, W. Funk, R. Nötzel, "Liveness Detection based on Fine Movements of the Fingertip Surface", Proceedings of IAW'06, IEEE, New York, USA, 2006, p. 19-21, ISBN 1-4244-0130-5.

[15] Martin Drahansky, Dana Lodrova," Liveness Detection for Biometric Systems Based on Papillary Lines" International Journal of Security and Its Applications Vol. 2, No. 4, October, 2008

[16] Changlong Jin, Hakil Kim, and Stephen Elliott," Liveness Detection of Fingerprint Based on Band-Selective Fourier Spectrum" ICISC 2007, LNCS 4817, pp. 168–179, 2007.