Spoof Detection of Fingerprint Biometrics based on Local and Global Quality Measures

Arunalatha G.
Research Scholar,
Dept. of CSE,
Pondicherry Engg. College,
Puducherry.

M. Ezhilarasan
Professor,
Dept. of IT,
Pondicherry Engg. College,
Puducherry.

ABSTRACT

Biometrics is used for authentication purpose. Among the various types of biometrics, fingerprint is the most widely accepted biometrics. Biometric systems have several advantages when compared to classical methods such as passwords. Biometric system is vulnerable to various types of attacks. This paper proposes a method to avoid the sensor level attack. This method uses limited ring wedge spectral energy, Inhomogenity and Directional Contrast. The limited ring wedge spectral density is the global quality measure.
Inhomogenity and Directional Contrast are the local quality measures.

Keywords

Spoof, fingerprint, Spectral energy,inhomogenity,directional contrast.

1. INTRODUCTION

The Biometrics refers to automatic recognition of identifying a person based on physiological or behavioral characteristics. Biological traits include fingerprint identification, facial recognition, iris recognition, palm prints and vein patterns. Vocal patterns, keystrokes, handwriting and gait recognition are some of the behavioral characteristic .Fingerprint recognition is the most widely used biometric technique than the rest of the techniques for personal identification systems due to its permanence and uniqueness. Biometric systems are used for personal identification. Biometric systems have several advantages when compared to classical methods such as passwords. It is not necessary to remember anything for biometric systems. Biometric systems do have some drawbacks. Biometric traits cannot be replaced. In a traditional password system a new password can be given if the existing password is traced by intruder. But in a biometric system a new fingerprint cannot be given. Because it is unique.

2. ATTACKS IN BIOMETRIC SYSTEM

The following are the two types of attacks in biometric system. [1] I).Direct attacks. (type1) II). Indirect attacks. Direct attack can be carried out in the sensor level. Knowledge is not needed for direct attack. To avoid direct attacks liveness detection techniques are used to differentiate between real and fake biometric input. Example presenting fake biometrics at the sensor: In this mode of attack, a possible reproduction of the biometric feature is presented as input to the system. Examples include a fake finger, a copy of a signature, or a face mask. Indirect attack can be done at the internal elements of the biometric system. For indirect attack the person should have some knowledge about the operation of biometric systems. Type 2-Resubmitting previously stored digitized biometrics signals: In this mode of attack, a recorded signal is given to the system, bypassing the sensor. Examples include the presentation of an old copy of a biometric data or the presentation of a previously recorded audio signal. Type 3- Overriding the feature extraction process: The feature extractor is attacked using a Trojan horse, so that it produces feature sets preselected by the intruder.

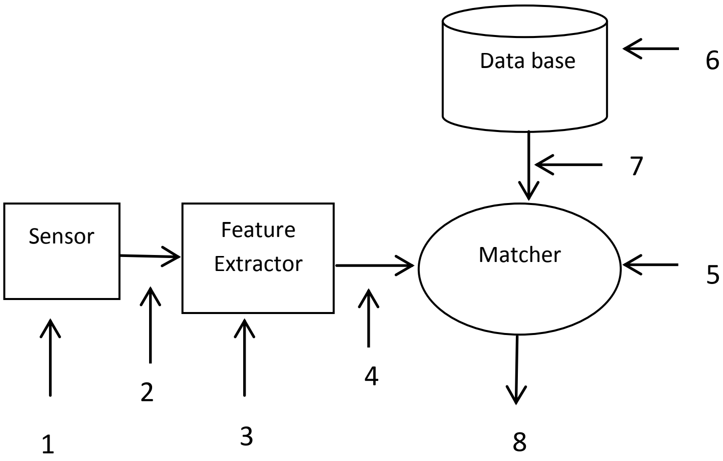

Fig.1. Types of attacks in biometric system.

Type 4-Tampering with the biometric feature representation: The features extracted from the input signal are replaced with a different set of fraudulent feature Type 5-Corrupting the matcher: The matcher is attacked and corrupted so that it produces preselected match scores Type 6-Tampering with stored templates: The database of stored templates could be either local or remote. The data might be distributed over several servers. The attacker can try to modify the templates in the database, resulting in either a fraudulent individual is authorized or service is denied to the persons associated with the corrupted template. Type 7-Attacking the channel between the stored tem plates and the matcher: The stored templates are sent to the matcher through a communication channel. The data travelling through this channel can be intercepted and modified. Type 8-Overriding the final decision: If the final match decision can be overridden by the hacker, then the authentication system has been disabled. Even if the actual pattern recognition framework has excellent performance characteristics, it has been rendered useless by the simple exercise of overriding the match result.

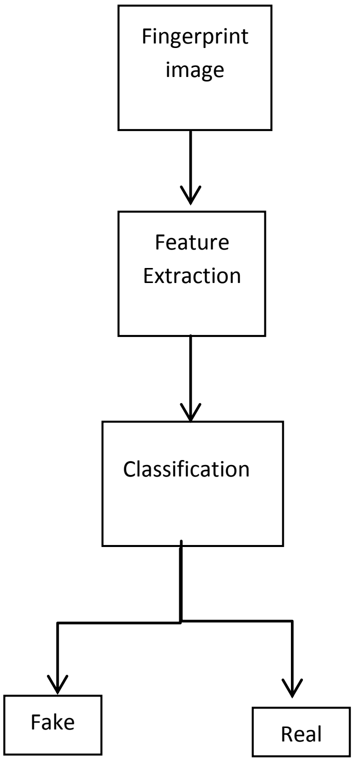

Fig. 2. Fingerprint Spoof Detection.

The rest of the paper is organized as follows: Section III gives a brief overview of spoof detection systems. Section IV presents the fingerprint Spoof detection. Section V gives Features for spoof detection. Section VI gives experimental results. Finally, Section VI concludes the paper.

3. SPOOF DETECTION

Differentiating a genuine biometric input from fake input is known as spoof detection. Liveness detection is a measure that determines whether or not the source of the image presented to a biometric sensor is from a living individual. The main reason for conducting liveness detection signs in fingerprint biometrics is to ensure that the sensor is capturing an image from real fingertip. It provides an extra level of security to the biometric system by working cooperatively with a matching algorithm that recognizes an enrolled user. The methods for liveness assessment represent a challenging engineering problem as they have to satisfy certain requirements (i) non-invasive, the technique should in no case penetrate the body or present and excessive contact with the user; (ii) user friendly, people should not be reluctant to use it (iii) fast, results have to be produced in very few seconds as the user cannot be asked to interact with the sensor for a long period of time; (iv) low cost, a wide use cannot be expected if the cost is very high; (v) performance, it should not degrade the recognition performance of the biometric system. There are two types of techniques for liveness detection. (i) Software-based techniques: In this case no special hardware device is added to the sensor. The features extracted from the feature extractor are used to distinguish between real and fake biometric input. (ii) Hardware-based techniques: In this case a special hardware device is added to detect whether the biometric input is real or fake.

4. FINGERPRINT SPOOF DETECTION

In [2] Fingerprint liveness detection based on quality measures for software based method is proposed From feature extractor 10 fingerprint quality measures based on ridge quality, ridge strength and ridge clarity are extracted Feature vector is formed form best quality features. Fingerprint is classified as real or fake using classifier. The performance of the method is evaluated on databases LivDet 2009 and ATVS group. This method correctly classifies almost 90% of the fingerprint images. The optimal value of ACE is 6.56%. Spoof detection using texture features is presented in [3]. The first order statistics such as energy, entrophy, median, variance, skewness, kurtosis and coefficient of variations are measured to detect the fake fingerprint. This method produces False Acceptance rate as 7.69 and False Reject Rate as 5.1. A model named as Biometric Security Functional Model is presented to provide security [4]. Biometric system is represented for identification, enrollment and verification. The error rate produced by this method is 2.32%. Direct attacks are evaluated for fake fingers which are generated from ISO templates [5]. Fingerprint image is reconstructed from ISO minutia templates to perform vulnerability evaluation against direct attacks by fake fingers. The evaluation of the ISO matcher is performed with FVC2006 DB2 database. Three quality measures based on ridge strength and ridge clarity are evaluated. Liveness detection based on wavelet features is presented [6]. The coefficients are changed using the zoom-in property of the wavelets. Multiresolution analysis and wavelet packet analysis are used to get information from low frequency and high frequency content of the images respectively. Daubechies wavelet is designed and implemented for wavelet analysis. This algorithm is applied to a training set and it differentiates live fingerprints from non live fingerprints. A novel fake-fingerprint detectionmethod that usingmultiple static features is propose [7]. These features extracted from one image are used determine the aliveness of fingerprints. The power spectrum, directional contrast, thickness, histogram and ridge signal of each fingerprint image are used for static features. The proposed method produces an EER of approximately 1.6% for optical sensors and 0% for capacitive sensor. A wavelet based approach to detect liveness, integrated with the fingerprint matcher [8]. Liveness is determined from perspiration changes along the fingerprint ridges. The proposed algorithm was applied to a data set of approximately 58 live, 50 spoof and 28 cadaver fingerprint images. The integrated system of fingerprint matcher and liveness module reduces EER to 0:03%. A new method by combining ridge signal and valley noise analysis is proposed for anti-spoofing in fingerprint sensors [9]. This method quantifies perspiration patterns along ridges in live subjects and noise patterns along valleys in spoofs. The signals representing grey level patterns along ridges and valleys are explored in spatial, frequency and wavelet domains. Based on these features, separation (live/spoof) is performed using standard pattern classification tools including classification trees and neural networks. Results show that this method produces an EER of 0.9% for an optical scanner. A new liveness detection method based on noise analysis along the valleys in the ridge-valley structure of fingerprint images is proposed [10]. Unlike live fingers which have a clear ridge-valley structure, artificial fingers have a distinct noise distribution due to the material's properties when placed on a fingerprint scanner. Statistical features are extracted in multiresolution scales using wavelet decomposition technique. Based on these features, liveness separation (live/non-live) is performed using classification trees and neural networks. Results show this method produced approximately 90.9–100% classification of spoof and live fingerprints. Distortions due to the pressure and rotation of the finger on a sensor produce different elastic characteristics of the materials. Liveness can be detected by comparing these distortions through static features. The elastic deformation due to the contact of the fingertip with a plane surface was studied in [11], since a fake fingerprint presents different deformations than a live one. The elastic behaviour of a live and a fake finger was analyzed by using a mathematical model relying on the extraction of a specific and ordered set of minutiae points. In general, a fake fingerprint image does not have a good quality as a live one. A fast and convenientwavelet-based algorithm[12] based on the computation of the standard deviation of the fingerprint image is proposed.

5. FEATURES FOR SPOOF DETECTION

5.1 Limited Ring-Wedge Spectral Energy

It measures the entropy of the energy distribution in the frequency domain[13]. A directional wave images can be represented by the Fourier spectrum . The FFT spectrum can be expressed in polar coordinates. The spectrum can be represented with the function S(r, θ), where r is the radial distance from the origin and θ is the angular variable. If fft2 represents the 2-D discrete Fourier transform function and fftshift moves the origin of the transform to the center of the frequency rectangle, then the FFT spectrum S(r, θ) can be expressed as follows:

S(r, θ) = log(1 + abs(fftshift(fft2(img)))) (1)

The global index measures the entropy of the energy distribution of 15 ring features. They are extracted using Butterworth low-pass filters. We convert S(r, θ) to 1-D function s_θ(r) for each direction, and analyze s_θ(r) for a fixed angle. Therefore, we can obtain the spectrum profile along a radial direction from the origin. A global descriptor can be achieved by summing for discrete variables:

$$s(r) = \sum_{\theta=0}^{\pi} s_\theta\,(r) \qquad (2)$$

The difference between quality and low quality images is indicated by the existence of strong principal feature peak (the highest spectrum close to the origin is the DC response) and major energy distribution.

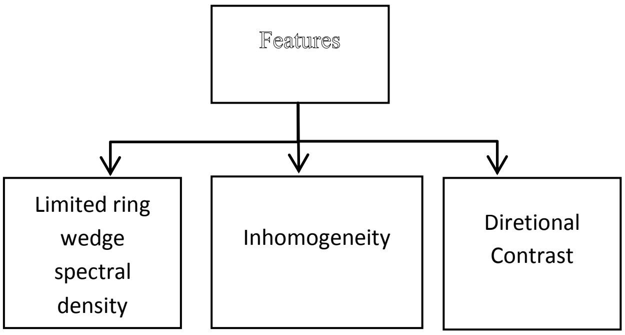

Fig. 3. Features for Spoof Detection.

5.2 Inhomogeneity:

The local texture[13] of the fingerprint images can be quantified by statistical properties of the intensity histogram . Let *I*i, L, and h(I) represent gray level intensity, the number of possible gray level intensities and the histogram of the intensity levels, respectively.Mean(m), standard deviation(σ) smoothness(R) and uniformity(U). We define the block Inhomogeneity(inH) as the ratio of the product between mean and Uniformity and the product between standard deviation and smoothness.

$$M = \sum_{i=0}^{l-1} Iih(\,Ii) \qquad (3)$$

$$\sigma = \sum_{i=0}^{L-1} (Ii - m)^2\, h(Ii) \qquad (4)$$

$$R = 1 - \frac{1}{1+\sigma^2} \qquad (5)$$

$$U = \sum_{i=0}^{l-1} h(I_i)^2 \qquad (6)$$

$$inH = \frac{mXU}{\sigma XR} \qquad (7)$$

5.3 Directional contrast:

Directional contrast reflects the certainty of local ridge flow orientation. It was used to measure the distinctness and clarity between the ridges and the valleys. This is because the blocks near to ridges and valleys in live images are well separated and display high directional contrast. The following procedure was devised to measure the level of directional contrast. A fingerprint image is partitioned into 8X8 blocks. A 3X3 four-directional mask is created to extract each directional value. The function $S_j(x, y)$ *j*=1,2,3,4 at the *x, y* position is described

$$s_j(x,y) = \sum_{k-1}^{2} I\big(P_{jk}\big) \qquad (8)$$

where $I\big(P_{jk}\big)$ denotes the intensity value of the pixel that corresponds to the position *Pjk* in the filter. For each block, the local directional gray value *Dj* is calculated as

$$D_j = \sum_{x=1}^{8}\sum_{y=1}^{8} s_j(x,y) \qquad (9)$$

6. EXPERIMENTAL RESULTS

The database used in the experiments is the development set provided in the Fingerprint Liveness Detection Competition, LivDET 2009. It comprises three datasets of real and fake fingerprints (generated with different materials) captured each of them with a different optical sensor. The Biometrika FX2000 (569 dpi) dataset comprises 520 real and 520 fake images. The fake images were generated with gummy fingers made of silicone.The CrossMatch Verifier 300CL (500 dpi) dataset comprises 1,000 real and 1,000 fake images. The fake were generated with gummy fingers made of silicone (310), gelatin (344), and playdoh (346). The Identix DFR2100 (686 dpi) dataset comprises 750 real and 750 fake images. The fake images were generated with gummy fingers made of silicone (250), gelatin (250), and playdoh (250).

S.No.	Feature	FAR
1	Limited ring-wedge spectral density	6.7
2	Inhomogenity	5.6
3	Directional Contrast	12.3

Table I. False Acceptance Rate for various features.

7. CONCLUSION

The Biometrics refers to automatic recognition of identifying a person based on physiological or behavioral characteristics. Biometric systems have several advantages when compared to classical methods such as passwords. Biometric system is vulnerable to certain types of attacks. Direct attack can be carried out in the sensor level. No Knowledge is not needed for direct attack. To avoid direct attacks spoof detection techniques are used to differentiate between real and fake biometric input. This method uses limited ring wedge spectral energy, Inhomogenity and Directional Contrast as features for spoof detection.

8. REFERENCES

[1] U. Uludag and Anil K. Jain, Attacks on biometric systems: A case study in fingerprints, Proc. SPIE, 5306: 622–633, 2004.

[2] Javier Galbally, Fernando Alonso-Fernandez, Julian Fierrez and Javier Ortega-Garcia, A high performance fingerprint liveness detection method based on quality, Future Generation Computer Systems, 28: 311–321, 2012.

[3] Ankita Chaudhari and P. J. Deore, Spoof attack detection in fingerprint biometric system using histogram features, Proc.World Journal of Science and Technology, 2(4): 108–111, 2012.

[4] Ahmad A. Hassan and Ahmad M. Bhram, Enhancing the Security of Biometric Systems on View of BioFM, Proc. ICCIT 2012.

[5] Galbally Javier, Raffaele Cappelli, Alessandra Lumini, Guillermo Gonzalez-de-Rivera Davide Maltoni, Julian Fierrez, Javier Ortega-Garcia and Dario Maio, An evaluation of direct attacks using fake fingers generated from ISO templates, Pattern Recognition Letters, 31: 725–732, 2010.

[6] Aditya Abhyankara and Stephanie Schuckersa, A wavelet based approach to detecting liveness in fingerprint scanners, SPIE Proceedings, 5404: 278–286, 2004,

[7] Heeseung Choi, Raechoong Kang, Kyoungtaek Choi, Andrew, Teoh Beng Jin and Jaihie Kim, Fake-fingerprint detection using multiple static features, Proc. Optical Engineering, 2009.

[8] Aditya Abhyankar and Stephanie Schuckers, Integrating a wavelet based perspiration liveness check with fingerprint recognition, Pattern Recognition, 42: 452–464, 2009.

[9] B. Tan and S. Schuckers, Spoofing Protection for Fingerprint Scanner by Fusing Ridge Signal and Valley Noise, Pattern Recognition, 4(8): 2845–2857, 2010.

[10] S. Tan and S. Schuckers, A New Approach for Liveness Detection in Fingerprint Scanners Based on Valley Noise Analysis, Journal of Electronic Imaging, 17(1): 011009-1 to 011009-9, 2008.

[11] A. Jain, Y. Chen and S. Dass, Fingerprint deformation for spoof detection. Biometric Symposium, 2005.

[12] K. C. Chan, K. So, Y. S. Moon, J. S. Chen and K. So Woo, Wavelet based fingerprint liveness detection. Electronic Letters, 41(20): 1112–1113, 2005.

[13] ChaohongWu, Sergey Tulyakov and Venu Govindaraju, Image Quality Measures for Fingerprint Image Enhancement,LNCS,215-222, 2006