Liveness Detection for Fingerprint Biometrics

Arunalatha G.[1, *], M. Ezhilarasan[2]

[1]Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India
[2]Department of Information Technology, Pondicherry Engineering College, Puducherry, India

Abstract

Biometrics refers to automated recognition of individuals based on their biological and behavioral characteristics. Biometric systems are widely used for security. They are used in forensic and commercial applications. Among all biometric techniques, fingerprint recognition is the most widely used for personal identification systems due to its permanence and uniqueness. But biometric systems are vulnerable to certain type of attacks. Spoofing refers to the fraudulent action by an unauthorized person into biometric systems using fake input that reproduces one of the authorized person's biometric input. Liveness detection provides extra level of authentication to biometrics. It is used to prevent forgeries. The fingerprint Liveness detection is performed by measuring the following quality features of fingerprint. They are Spatial Coherence, Gabor Features, Ridge frequency. This approach is based on fingerprint image quality. This technique is software based as it requires no external hardware. This approach is inexpensive.

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. Examples of behavioral characteristics include vocal patterns, keystrokes, handwriting and gait recognition. Among all biometric techniques, fingerprint recognition is the most widely used for personal identification systems due to its permanence and uniqueness Biometric systems are used for personal identification. Biometric systems provide several advantages when compared to classical methods such as passwords. For biometric systems it is not necessary to remember anything. Biometric systems have some drawbacks. Biometric trait 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.

Types of Attacks in Biometric System

There are 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. For direct attack, no knowledge is needed. 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. 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.

* Corresponding author
E-mail address: arunalathamaha@gmail.com (Arunalatha G.), mrezhil@pec.edu (M. Ezhilarasan)
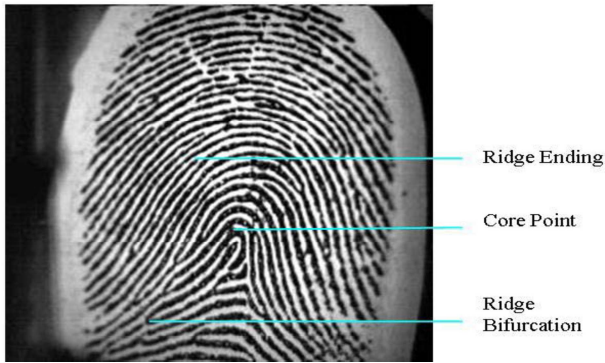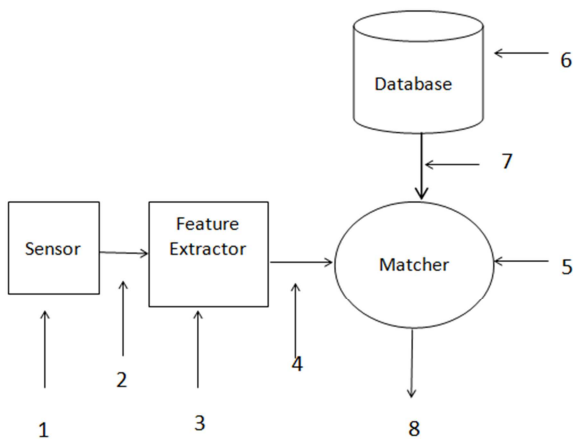
Fig. 1. Fingerprint image.

Fig. 2. 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.

The rest of the paper is organized as follows: Section II gives a brief overview of liveness detection systems. Section III presents the proposed system design for liveness detection.

Section IV gives the classifier. Section V gives experimental results. Finally, Section VI concludes the paper.

2. Liveness Detection

Differentiating a genuine biometric input from fake input is known as Liveness 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.

Fingerprint Liveness detection:

Fingerprint is a pattern of ridges and valleys on fingertip. The fake fingerprint can be made from gelatin, clay, play-doh, silicone, latex, rubber etc. with user's cooperation or without cooperation.

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, entropy, 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 detection method that using multiple static features is proposed [7]. These features extracted from one image are used determine the aliveness of fingerprints. The power spectrum, directional contrast, ridge 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 behavior 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. The important idea to detect liveness by checking quality was implemented in [12]. A fast and convenient wavelet-based algorithm based on the computation of the standard deviation of the fingerprint image is proposed.

3. Proposed System

The proposed system consists of three stages. In the first stage features are extracted from the input fingerprint image. In the second stage, features are selected. Then classifier classifies the fingerprint as real or fake.
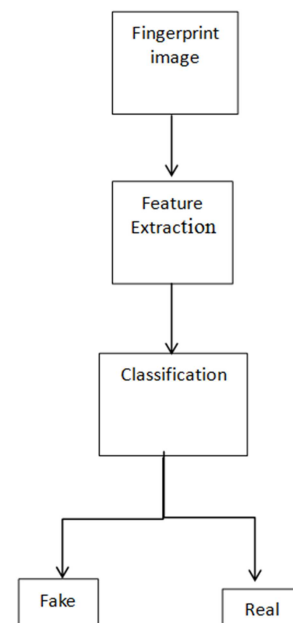

Fig. 3. Fingerprint Liveness Detection.

The following features are extracted from the fingerprint image. The fingerprint image is divided into nonoverlapped square blocks and then features are extracted from each block.

3.1. Ridge Clarity Feature: Spatial Coherence

It measures the local coherence of the intensity gradient [13]. It indicates the clarity of the local ridge-valley direction in each block. The fingerprint image is divided into foreground and background block. For foreground block, the covariance matrix of gradient vector is calculated.

The covariance matrix of gradient vector for an N point image can be expressed as

$$C = \frac{1}{N} \sum_N \left\{ \begin{bmatrix} dx \\ dy \end{bmatrix} [dx \quad dy] \right\} = \begin{bmatrix} C_{xx} & C_{xy} \\ C_{yx} & C_{yy} \end{bmatrix} \quad (1)$$

dx, dy-intensity gradient of each pixel calculated by sobel operator. The eigen values of Care denoted as

$$\lambda_a = \frac{c_{xx}c + c_{yy} + \sqrt{(c_{xx} - c_{yy})^2 + 4c_{xy}^2}}{2} \quad (2)$$

$$\lambda_b = \frac{c_{xx} + c_{yy} - \sqrt{(c_{xx} - c_{yy})^2 + 4c_{xy}^2}}{2} \quad (3)$$

$$\tilde{k} = \frac{(\lambda_a - \lambda_b)^2}{(\lambda_a + \lambda_b)^2} \quad (4)$$

If the region has distinct ridge-valley orientation, k=1. For poor quality image k=0.

3.2. Ridge Continuity Feature: Gabor Feature

Each block for the fingerprint image is filtered using a Gabor filter with m different directions [14]. Gabor filters optimally capture both local orientation and frequency information from a fingerprint image. By tuning a Gabor filter to specific frequency and direction, the local frequency and orientation information can be obtained. Thus, they are suited for extracting texture information from images. The core point is detected in the fingerprint. Core point is defined as the north most point of inner-most ridge line. The circular region is filtered using a bank of sixteen Gabor filters to produce a set of sixteen filtered images. Gabor filter-banks are a well-known technique to capture useful information in specific band pass channels. The average absolute deviation with in a sector quantifies the underlying ridge structure and is used as a feature. The feature vector (2048 values in length) is the collection of all the features, computed from all the 128 sectors, in every filtered image. The feature vector captures the local information and the ordered enumeration of the tessellation captures the invariant global relationships among the local patterns. For a high quality block, one of the filter output is larger than others. For a poor quality block, m filer output is same. The standard deviation of the m filter responses is used to determine the quality of each block. Gabor matrices are computed. Image is segmented as foreground or background.

The general form of 2D Gabor filter is defined by

$$h(x, y, \theta_k, f, \sigma_x, \sigma_y) = \exp\left[-\frac{1}{2}\left(\frac{x_{\theta_k}^2}{\sigma_x^2} + \frac{y_{\theta_k}^2}{\sigma_x^2}\right)\right] \times \\ \exp(i2\pi f x_{\theta_k}) \quad (5)$$

Where f is the frequency of the sine plane wave along the direction θ (0, 45, 90 and 135 degrees) from the x -axis, σ_x, σ_y are the space constants of the Gaussian envelope along X and Y axes, respectively.

The standard deviation value G is computed as follows:

$$G = \left(\frac{1}{m-1} \sum_{k=1}^{m} \left(g_{\theta_k} - \overline{g_\theta}\right)^2\right)^{\frac{1}{2}} . \overline{g_\Theta} = \frac{1}{m} \sum_{k=1}^{m} g_{\theta_k} \quad (6)$$

3.3. Ridge Strength Feature: Ridge Frequency

Ridge frequency [15] is used to detect abnormal ridges that are too close or too far. Fingerprint ridge distance is defined as the distance from a given ridge to adjacent ridges. It can be measured as the distance from the centre of one ridge to the centre of another. Fingerprint ridge distance is defined as the distance form a given ridge to adjacent ridges. It can be measured as the distance from the centre of one ridge to the centre of another. Both the pressure and the humidity of finger will influence the ridge distance. The ridge distance of high pressure and wet finger image is narrower than the low pressure and dry finger. Since the ridge frequency is the reciprocal of ridge distance and indicates the number of ridges within a unit length, Ridge frequency is the reciprocal of ridge distance and indicates the number of ridges within a unit length. Initially fingerprint image is divided into blocks of size 16X16. For each block orientation window is computed. The X signature of ridges is calculated within oriented window. The frequency of ridge is calculated from the x signature.

4. Classifier

The SVM is a powerful classifier with an excellent generalization capability that provides a linear separation in an augmented space by means of different kernels. The kernels map input data vectors onto a high-dimensional space where a linear separation is more likely, and this process amounts to finding a non-linear frontier in the original input space. Each input vector for the proposed quality estimation system consists of seven features.

$$V= [SC, GR, RF] \qquad (7)$$

SC stands for Spatial Coherence, GF stands for Gabor feature, and RF stands for Ridge Frequency.

5. Experimental Results

For each algorithm we calculated the False Acceptance Rate (FAR) that is the rate of live fingerprint images that are classified as spoof fingerprint images and False Rejection Rate (FRR) that is the rate of fake fingerprint images that are classified as live fingerprint images. 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). The material with which the different fake images are made is known. These fakes were created using the consensual method: a volunteer put his finger on a mould of plasticine like material, another material like gelatine or liquid silicon is poured over the mould. The result, after a certain time interval, is an artificial replica of the fingertip. The three features spatial coherence, Gabor Feature and Ridge Frequency are compared with Local Orientation Quality using False Acceptance Rate and False Rejection Rate. Among the features, Ridge frequency gives the better result than other features.
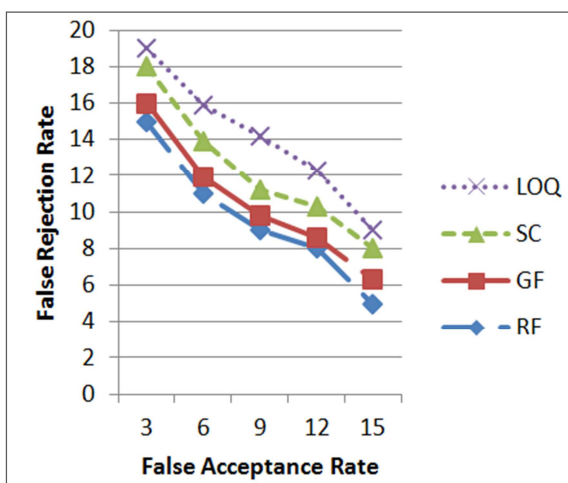

Fig. 4. Comparision of Ridge features –Local Orientation Quality (LOQ), Spatial Coherence, Gabor Feature (GF) and Ridge Frequency (RF).

6. Conclusion

Biometric systems are widely used for security. But biometric systems are vulnerable to certain type of attacks. The fingerprint spoof detection is performed by measuring the quality features of fingerprint. They are Ridge clarity features such as spatial coherence and clustering factor, Ridge continuity features such as gabor features and uniformity of frequency field and Ridge Strength features such as ridge frequency, contrast map and Direction map. This technique is software based as it requires no external hardware. The overall classification rate is good.

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] Y. Chen, S. Dass and A. Jain, Fingerprint quality indices for predicting authentication performance, in Proc. AVBPA: 160–170 (2005).

[14] L. Shen, A. Kot and W. Koo, Quality measures of fingerprint images, in Proc. Audio Video-Based Person Authentication: 266–271 (2001).

[15] E. Lim, X. Jiang and W. Yau, Fingerprint quality and validity analysis, in Proc. Int. Conf. Image Process, 469–472 (2002).

[16] C. Watson, M. Garris, E. Tabassi, C Wilson, R. McCabe, and S. Janet, User's Guide to Fingerprint Image Software 2-NFIS2 [Online]. Available: http:www//fingerprint.nist.gov/NFIS. NIST, (2004).