Asian Journal of Multidisciplinary Research (AJMR) 2016

E-ISSN: 2395-1710

P-ISSN: 2395-1729

Volume 02- Issue 03-, pp-84-91

Research Paper Open Access

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

Anandhi.K[1], NizreenaBanu.A2, Selvarani.B3, Rahin BatchaR[4]

M. Tech Student, Department of Computer Science and Engineering

Sri ManakulaVinayagar Engineering College,

Anandhi.11593@gmail.com[1],banunizreena@gmail.com3,manipremi648@gmail.com[2],batcha35@gmail.com

Abstract

Biometrics is employed for authentication purpose. Among the assorted styles of biometry, fingerprint is that the most generally accepted biometry. Biometric systems have many blessings when put next to classical strategies like passwords. Biometric system is susceptible to varied styles of attacks. This paper proposes a technique to avoid the device level attack. This technique uses restricted ring wedge spectral energy, Inhomogenity and Directional distinction. The restricted ring wedge spectral density is that the world quality live. Inhomogenity and Directional distinction area unit the native quality measures.

Keywords: Spoof, fingerprint, Spectral energy, Inhomogenity, directional contrast**.**

1. Introduction

The biometry refers to automatic recognition of distinguishing individual supported physiological or behavioural characteristics. Biological traits embody fingerprint identification, automatic face recognition, iris recognition, palm prints and vein patterns. Vocal patterns, keystrokes, handwriting and gait recognition area unit a number of the behavioural characteristic .Fingerprint recognition is that the most generally used biometric technique than the remainder of the techniques for private identification systems owing to its length and individuality. Biometric systems area unit used for private identification. Biometric systems have many blessings in comparison to classical ways like passwords. It is not necessary to recollect something for biometric systems. Biometric systems do have some drawbacks. Biometric traits can't be replaced. in an exceedingly ancient Arcanum system a replacement Arcanum will be given if the present Arcanum is derived by trespasser. However in an exceedingly biometric system a replacement fingerprint can't be given. As a result of its distinctive.

2. ATTACKS IN BIOMETRIC SYSTEM

The following areas are the 2 kinds of attacks in biometric system. [1]

I) Direct attacks. (type1)

II) Indirect attacks.

Direct attack is administered within the device level. Information isn't required for direct attack. To avoid direct

attacks aliveness detection techniques area unit won't to differentiate between real and pretend biometric input. Example presenting pretend biometry at the sensor: during this mode of attack, a doable copy of the biometric feature is conferred as input to the system. Examples embrace a pretend finger, a replica of a signature, or a mask. Indirect attack is done at the inner components of the biometric system. For indirect attack the person ought to have some information concerning the operation of biometric systems. Sort 2-Resubmitting antecedently keep digitizedbiometry signals: during this mode of attack, a recorded signal is given to the system, bypassing the device. Examples embody the presentation of an recent copy of a biometric knowledge or the presentation of a antecedent recorded audio signal. Sort 3- preponderating the feature extraction process: The feature extractor is attacked employing a bug, in order that it produces feature sets preselected by the persona non grata.Type 4-Tampering with the biometric feature representation: The options extracted from the signalling area unit replaced with a distinct set of dishonest feature sort 5-Corrupting the intermediator:
The matcher is attacked and corrupted in order that it produces preselected match scores sort 6-Tampering with hold on templates: The information of hold on templates might be either native or remote. The information may be distributed over many servers. The offender will try and modify the templates in the information, leading to either a dishonest individual is authorized or service is denied to the persons associated with the corrupted template. sort 7-Attacking the channel between the hold on tem plates and also the intermediator: The hold on templates area unit sent to the matcher through a communication. The information move through this channel is intercepted and changed. Sort 8-Overriding the ultimate call: If the ultimate match decision is overridden by the hacker, then the authentication system has been disabled. Although the particular pattern recognition framework has wonderful performance characteristics, it's been rendered useless by the easy exercise of preponderating the match result. The rest of the paper is organized as follows: Section III provides a quick summary of spoof detection systems. Section IV presents the fingerprint Spoof detection. Section V provides options for spoof detection. Section VI provides experimental results. Finally, Section VI concludes the paper.

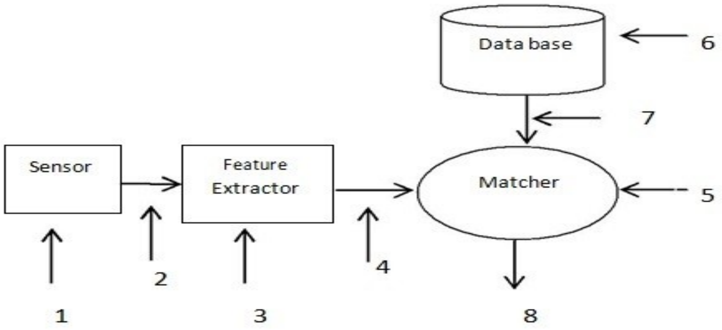

Fig.1. Types of attacks in biometric system.

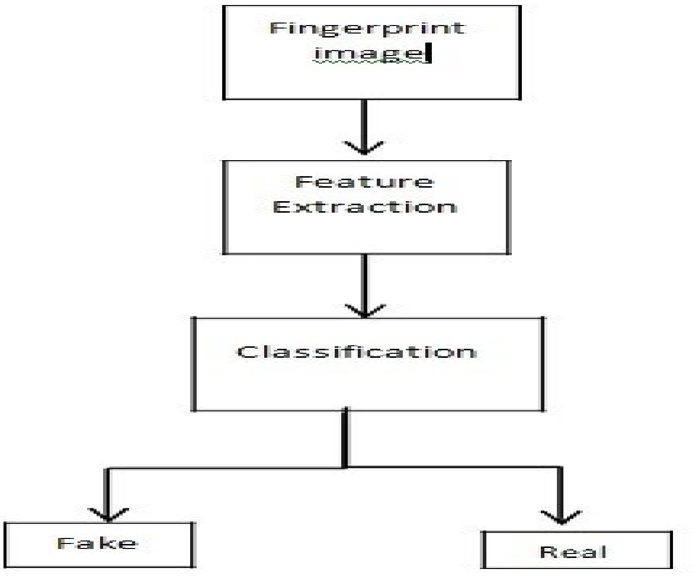

Fig. 2. Fingerprint Spoof Detection.

3. SPOOF DETECTION:

Differentiating a real biometric input from faux input is understood as spoof detection. Physiological property detection could be a live that determines whether or not or not the supply of the image conferred to a biometric device is from a living individual. The most reason for conducting physiological property detection signs in fingerprint biometry is to confirm that the device is capturing a picture from real tip. It provides an additional level of security to the biometric system by operating hand in gloved glove} with anidentical rule thatacknowledges a list ed user.The ways for physiologicalproperty assessmentrepresenta difficult engineering d rawback as theyneed to satisfy sure needs (i) non-invasive, the technique ought to in no case penetrate the body or gift and excessive contact with the user; (ii) user friendly, folks shouldn't be reluctant to use it (iii) quick, results ought to be made in only a few seconds because the user can not be asked to move with the device for an extended amount of time; (iv) low value, a good use can not be expected if the price is incredibly high; (v) performance, it shouldn't degrade the popularity performance of the biometric system. There area unit 2 kinds of techniques for physiological property detection. (i) Software-based techniques: during this case no special hardware device is supplementary to the device. The options extracted from the feature extractor area unit wont to distinguish between real and faux biometric input. (ii) Hardware-based techniques: during this case a special hardware device is additional to find whether or not the biometric input is real or faux.

4. FINGERPRINT SPOOF DETECTION

In[2]Fingerprint animateness detection supp orted quality measures for software system primarilybasedmethodology is plann ed Fromfeatureextractor ten fingerprintqualit ymeasures supported ridge quality, ridge strength and ridge clarity area unit extracted Feature vector kinded|is made|is created} form very best quality options. Fingerprint is classed asrealor pretend victimisation classifier. The performance of the strategy is evaluated on databases LivDet 2009 and ATVS cluster.This methodology properly classifies virtually ninetieth ofthefingerprint pictures. The optimum price of ACE is half-dozen.56%. A spoof detection victimisation texture option is given in [3]. The primary order statistics like energy, entropy, median, variance, skewness, kurtosis and constant of variations area unit measured to discover the pretend fingerprint.This methodology produces False Acceptance rate as seven.69 and False Reject Rate as five.1. A model named as Biometric Security purposeful Model is given to produce security [4]. Biometric system is delineating for identification, enrolment and verification. The error rate made by this methodology is two.32%.Directattacks areaunit evaluated for pretend fingers that area unit generated from ISO templates [5]. Fingerprint image is reconstructed from ISO detail templates to perform vulnerability analysis against direct attacks by pretend fingers. The analysis of the ISO marriage broker is performed with FVC2006DB2 info. 3 quality measures supported ridge strength and ridge clarity areaunitevaluated. an animateness detection supported riffle option is given [6]. The coefficients area unit modified victimisation the zoom-in property of the wavelets. Multiresolution analysis and riffle packet analysis area unit accustomed get info from low frequency and high frequency content of the photographs severally. Daubechies riffle is meant and enforced for riffle analysis.

This algorithmic program is applied to a coaching set and it differentiates live fingerprints from non live fingerprints. a completely unique fake-fingerprint detection method that using multiple static options is propose [7]. These options extracted from one image area unit used verify the aliveness offingerprints. thefacility spectrum, directional distinction, thickness, bar graph and ridge signal of every fingerprint image area unit usedforstatic options.The planned methodology produces AN EER ofroughlyone.6% for optical devices and 1/3 for electrical phenomenon sensor.A riffle primarily based approach to discover animateness, integratedwiththefingerprint marriagebroker [8]. animateness isdecided from perspiration changes on the fingerprint ridges. The planned algorithmic program was applied to a knowledge set of roughly fiftyeight live, fifty spoofand twenty eight remains fingerprint pictures.Theintegratedsystemoffingerprint marriagebroker and animateness module reduces EER to 0:03%. a brand new methodology by combining ridge signal and depression noise analysis is planned for anti-spoofing in fingerprint sensors [9].This methodology quantifies perspiration patterns on ridges in live subjects and noise patterns on valleys in spoofs. The signals representing gray level patterns on ridges and valleys area unit explored in abstraction, frequency and riffle domains. Supported these options, separation (live/spoof) is performed victimisation customary pattern classification tools as well as classification trees and neural networks. Results show that this methodology produces AN EER of zero.9% for AN optical scanner. a brand new animateness detection methodology supported noise analysis on the valleys within the ridge-valley structure of fingerprint pictures is planned [10]. in contrast to live fingers that have a transparent ridge-valley structure, artificial fingers have a definite noise distribution attributable to the material's properties once placed on a fingerprint scanner. Applied math options area unit extracted in multi resolution scales victimisation riffle. Decomposition technique supported these options, physiological property separation (live/non-live) is performed exploitation classification trees and neural networks. Results show this methodology created or so ninety.9–100% classification of spoof and live fingerprints. Distortions as a result of the pressure and rotation of the finger on a detector manufacture completely different elastic characteristics of the materials. physiological property may be detected by scrutiny these distortions through static options. The elastic deformation as a result of the contact of the tip with a plane surface was studied in [11], since a faux fingerprint presents completely different deformations than a live one. The elastic behaviour of a live and a faux finger was analyzed by employing a mathematical model looking forward to the extraction of a particular and ordered set of trivialities points. In general, a faux fingerprint image doesn't have an honest quality as a live one. a quick and convenient wavelet-based algorithm[12] supported the computation of the quality deviation of the fingerprint image is projected.

5. FEATURES FOR SPOOF DETECTION

5.1 Limited Ring-Wedge Spectral Energy

It measures the entropy of the energy distribution within the frequency domain [13]. A directional wave pictures are often delineate by the Fourier spectrum. The FFT spectrums are often expressed in polar coordinates.Thespectrum areoften delineate withthe operate S(r,), wherever r is that the radial distance from the origin and is the angular variable. If fft2 represents the 2-D discrete Fourier rework operate and fft shift moves the origin of the transform to the middle of the frequency parallelogram, then the FFT spectrum S(r,) can be expressed as follows:

$$S(r, \theta) = \log(1 + \mathrm{abs}(\mathrm{fftshift}(\mathrm{fft2}(img)))) \quad (1)$$

The global index measures the entropy of the energy distribution of fifteen ring options. they're extracted exploitation Butterworth low-pass filters. We tend to convert S(r,) to 1-D function (r) for every direction, and analyze (r) for a set angle. Therefore, we will get the spectrum profile on a radial direction from the origin. a world descriptor is achieved by summing for distinct variables:

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

The distinction between quality and calibre pictures is indicated by the existence of robust principal feature peak (the highest spectrum near the origin is that the DC response) and major energy distribution.

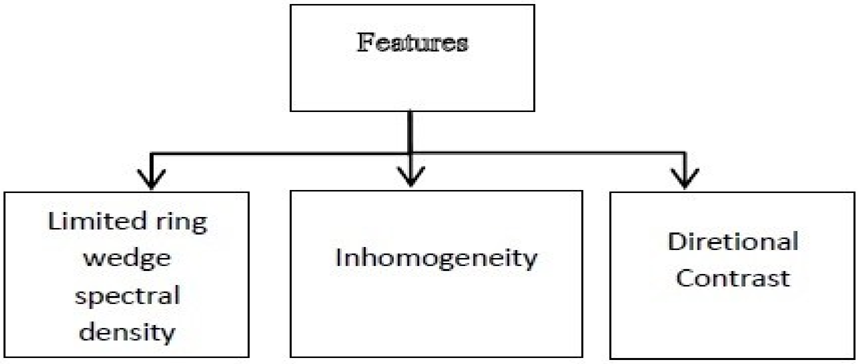

Fig. 3. Features for Spoof Detection.

5.2 Inhomogeneity:

The native texture[13] of the fingerprint pictures are often quantified by applied math properties of the intensity bar chart . Let Ii, L, and h(I) represent grey level intensity, the amount of potential grey level intensities and also the bar chart of the intensity levels, severally. Mean(m), normal deviation(smoothness(R) and uniformity(U). we have a tendency to outline the block Inhomogeneity(inH)because the magnitude relation of the merchandise between mean and Uniformity and also the product between variance 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 distinction reflects the knowledge of native ridge flow orientation. It had been accustomed live the distinctness and clarity between the ridges and therefore the valleys. This can be as a result of the blocks regarding ridges and valleys in live pictures square measure well separated and show high directional distinction. The subsequent procedure was devised to live the amount of directional distinction. A fingerprint image is partitioned off into 8X8 blocks. A 3X3 four-directional mask is made to extract every directional price. The perform Sj(x, y) j=1,2,3,4 at the x, y position is delineated

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

where I(P_{jk}) denotes the intensity price of the element that corresponds to the position Pjk within the filter. For every block, the native directional grey price Dj is calculated as

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

6. EXPERIMENTAL RESULTS

The information utilized in the experiments is that the development set provided within the Fingerprint animateness Detection Competition, LivDET 2009. It includes 3 datasets of real and pretend fingerprints (generated with completely different materials) captured every of them with a unique optical sensing element. The Biometrika FX2000 (569 dpi) dataset includes 520 real and 520 faux images. The pretend pictures were generated with viscous fingers manufactured from siloxane.The CrossMatch friend 300CL (500 dpi) dataset includes 1,000 real and 1,000 pretend pictures. The pretend were generated with viscous fingers manufactured from siloxane (310), gelatin (344), and playdoh (346). The Identix DFR2100 (686 dpi) dataset includes 750 real and 750 pretend pictures. The pretend pictures were generated with viscous fingers manufactured from siloxane(250), gelatine(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.