AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com

Liveness Detection of Fingerprint Biometrics using Local Derivative Pattern

[1]Arunalatha G and [2]M. Ezhilarasan

[1]Research Scholar, Dept. of CSE, Pondicherry Engineering College Puducherry, India.
[2]Professor, Dept. of Information Technology, Pondicherry Engineering College Puducherry, India.

Address For Correspondence:
Arunalatha G, Research Scholar, Dept. of CSE, Pondicherry Engineering College Puducherry, India
E-mail: arunalathamaha@gmail.com

ARTICLE INFO

Article history:
Received 26 April 2016
Accepted 21 July 2016
Published 30 July 2016

Keywords:
Biometrics, Fingerprint, Liveness, Local Derivative Pattern

ABSTRACT

Biometrics are used for authentication. It is used to recognize a person based on their unique characteristics. Among several biometrics, Fingerprint is the most widely used and acceptable biometrics. Biometric system has several advantages over traditional methods. But it can be affected by several attacks. In this paper the type1 attack is discussed which is performed at the sensor level. Differentiating a genuine biometric input from fake input is known as Liveness detection. Local Derivative Pattern(LDP) is a gray-scale texture pattern. LDP assigns an 8 bit binary code to each pixel of an input image. It characterizes the spatial structure of a local image texture. The Local Derivative pattern texture feature is extracted for fingerprint image. It is used to check whether the fingerprint is real or fake.

INTRODUCTION

There are 3 levels of authentication for personal identification. They are using something you have (key, card), something you know (password, PIN) and something you are (biometrics).If we use card, it can be stolen by someone. If we use password it can be cracked or forgotten. Because of these disadvantages present in the conventional security system, we are going for biometrics. Biometrics is the automated recognition of a person based on their biological and behavioral characteristics such as fingerprints, iris, face, signature and voice Biometric systems can be used in two different modes. Identity verification occurs when the user claims to be already enrolled in the system (presents an ID card or login name); in this case the biometric data obtained from the user is compared to the user's data already stored in the database. Identification occurs when the identity of the user is a priori unknown. In this case the user's biometric data is matched against all the records in the database as the user can be anywhere in the database or he/she actually does not have to be there at all.

There are seven basic criteria for biometric security system: uniqueness, universality, collectability, performance, permanence, acceptability and circumvention Uniqueness indicate how uniquely and differently the biometric system will be able to recognize each user among groups of users. Universality indicates requirements for unique characteristics of each human being in the world which cannot be replicated. Permanence parameter is required for every single characteristic or trait which is recorded in the database of the system and needs to be constant for a certain period of time period. This parameter will be affected by the age of the user. The collectability parameter requires the collection of each characteristic and trait by the system in order to verify their identification. Performance outlines how well the security system works. The robustness and accuracy are main factors for the biometric security system. These factors will decide the performance of the biometric security system. The acceptability parameter will choose fields in which biometric technologies are acceptable. Finally, circumvention will decide how easily each characteristic and trait provided by the user

To Cite This Article: Arunalatha G and M. Ezhilarasan., Liveness Detection of Fingerprint Biometrics using Local Derivative Pattern. ***Aust. J. Basic & Appl. Sci.,*** *10(12): 188-195, 2016*

can lead to failure during the verification process.

There are seven basic criteria for biometric security system: uniqueness, universality, collectability, performance, permanence, acceptability and circumvention Uniqueness indicate how uniquely and differently the biometric system will be able to recognize each user among groups of users. Universality indicates requirements for unique characteristics of each human being in the world which cannot be replicated. Permanence parameter is required for every single characteristic or trait which is recorded in the database of the system and needs to be constant for a certain period of time period. This parameter will be affected by the age of the user. The collectability parameter requires the collection of each characteristic and trait by the system in order to verify their identification. Performance outlines how well the security system works. The robustness and accuracy are main factors for the biometric security system. These factors will decide the performance of the biometric security system. The acceptability parameter will choose fields in which biometric technologies are acceptable. Finally, circumvention will decide how easily each characteristic and trait provided by the user can lead to failure during the verification process.

Fig. 1: Fingerprint Image

A fingerprint is a flowing pattern on the fingertip of a person consisting of ridges and valleys. Ridges are black lines. Valleys are white space between ridges. We can represent fingerprint using local information or global information. Global information refers to fingerprint ridges. Local information refers to characteristics derived from ridges.

Ridge details can be represented in 3 levels: Level 1, Level 2 and Level 3. At level 1(global level) pattern type of ridges are described. They are loop, delta and core.

At level 2(local level) Galton characteristics like ridge ending, ridge bifurcation are described. They are called as minutiae. Each minutiae is represented by its position and ridge direction (angle). At level 3(Fine level) Sweat pores and incipient ridges are described.

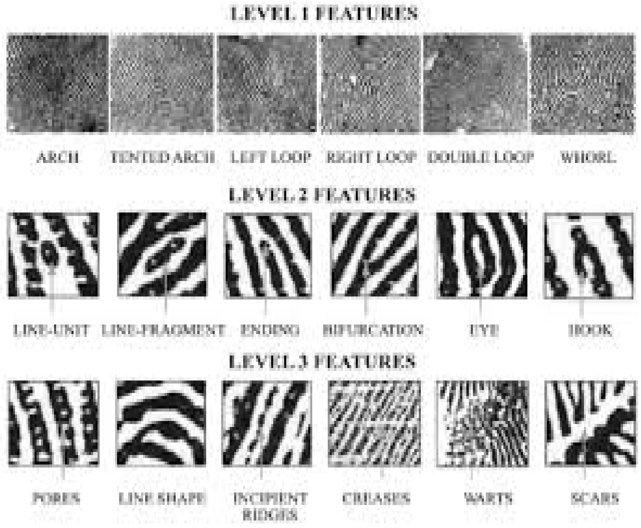


Fig. 2: Fingerprint Level1, level2 and level3 Features

A biometric system is designed using the following four main modules 1) Sensor module-It captures the biometric input of an individual. An example is a fingerprint sensor that images the ridge and valley structure of a user’s finger. 2) Feature extraction module-It processes the acquired biometric input to extract a set of salient or discriminatory features. For example, the position and orientation of minutiae points in a fingerprint image are extracted in the feature extraction module of a fingerprint-based biometric system. 3) Matcher module- It compares the features extracted during recognition against the stored templates to generate matching scores. For example, in the matching module of a fingerprint-based biometric system, the number of matching minutiae between the input and the template fingerprint images is determined and a matching score is reported. V) Decision making module, in which a user’s claimed identity is confirmed (verification) or a user’s identity is established (identification) based on the matching score. 4) System database module, which is used by the biometric system to store the biometric templates of the enrolled users. The enrollment module is responsible for enrolling individuals into the biometric system database. During the enrollment phase, the biometric characteristic of an individual is first scanned by a biometric reader to produce a digital representation of the characteristic. The data capture during the enrollment process may or may not be supervised by a human depending on the application.

Fingerprint System Security:

A. Attacks in Biometric System:

Uludag and Jain (2004) stated that there are two types of attacks in biometric system. I).Direct attacks. (type1) II). Indirect attacks. Direct attack can be carried out in the sensor level. To perform direct attack, knowledge is not necessary. To avoid direct attacks vitality detection techniques are used to differentiate between fake and real biometric input.

Presentation attack (Type 1): Fake input samples are given as input to the biometric Sensor.

Biometric signal replication (Type 2): The channel between Sensor and Feature Extractor is hacked. Previously stored biometric data is resubmitted.

Modifying Features (Type3): The features are preselected by the attacker using a Trojan horse.

Replacing features (Type 4): The set of features extracted by the feature extractor are modified using duplicate set of features.

Overriding the matcher (Type 5): The matcher module is corrupted to produce the preselected match scores preselected by attacker.

Replacing templates (Type 6): The templates stored in the template database are modified.

Modifying the channel data (Type 7): The data flowing through the channel between matcher and template database are modified by the attacker.

Altering the Decision ((Type 8): The result of the matcher is overridden by the attacker.

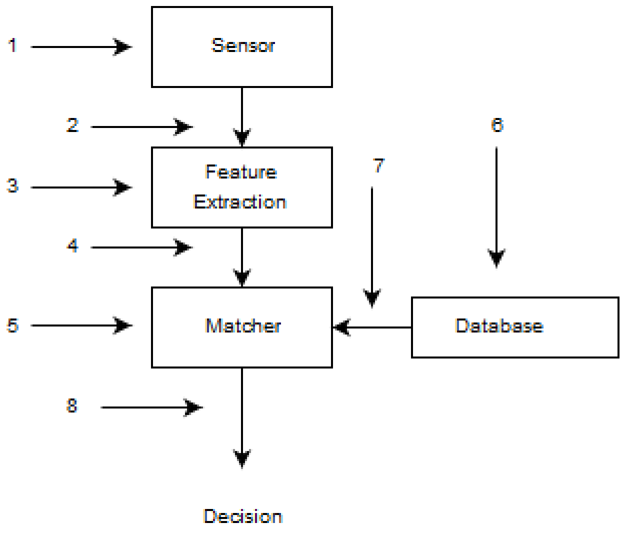


Fig. 3: Attacks in a Biometric system

B. Liveness Detection:

Spoof detection refers to the ability of the system to determine whether the input given to the sensor belongs to a live finger or not. 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 vitality 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.

There are two types of techniques for Liveness detection. (i) Software-based techniques: In this type, no special hardware device is added to the sensor. The biometric features extracted from the feature extractor are used to distinguish between real and fake biometric input. (ii) Hardware-based techniques: In this type a special hardware device is added to detect whether the biometric input is real or fake.

Artificial fingerprints are created using material like clay, plastic, clay, playdoh and silicon gelatin, wax, and silicon. They can be created in a cooperative or non_cooperative type. In the Cooperative type, artificial fingerprint is created with the cooperation of the user. In the non-cooperative type, the artificial fingerprint is created without the knowledge of the user.

Fingerprint Liveness detection:

Abgyankara and Schuckers(2004) proved Spoof detection using texture features. The first order statistics such as entropy, energy, median, variance, kurtosis, skewness and coefficient of variations are measured to detect the fake fingerprint. This method produces False Reject Rate as 5.1 and False Acceptance rate as 7.69. The evaluation of the ISO matcher is done with FVC2006 DB2 Database. Three quality measures based on ridge clarity and ridge strength are evaluated.

Jain *et al*. (2005) stated the distortions due to the rotation and pressure of the finger on a sensor produce different elastic characteristics of the materials. Vitality can be detected by comparing these distortions through static features. The elastic deformation occurs by the contact of the fingertip with a plane surface, since a fake fingerprint presents different deformations than a real fingerprint. The elastic behavior was analyzed for a live and a fake finger by using a mathematical model relying on the extraction of a specific and ordered set of minutiae points. Chan *et al*. (2005) designed a model named as Biometric Security Functional Model to provide security. Biometric system is represented for identification, verification and enrollment. The error rate given by this method is 2.32%.

Tan and Schuckers (2008) proposed a novel fake fingerprint identification method using multiple static features. These features extracted from one image are used determine the vitality of fingerprints. The power spectrum, ridge thickness, directional contrast, ridge signal and histogram of each fingerprint image are used as static features. The proposed method produces an EER of approximately 0% for capacitive sensor and 1.6% for optical sensors.

Abhyankara Schuckers(2009) proposed Fingerprint vitality detection based on quality measures for software based method. From feature extractor fingerprint quality measures based on ridge strength, ridge clarity and ridge continuity are extracted. The Feature vector is taken from best quality features. Fingerprint is classified as fake or real using classifier. The performance of the method is evaluated on databases LivDet 2009 and ATVS group. This method correctly classifies maximum 90% of the fingerprint images. The optimal ACE value is 6.56%.

Heeseung *et al*. (2009) prop0seda new vitality detection method for fingerprint images. The live fingers have a clear ridge-valley structure. But fake fingers have a distinct noise distribution because of the material's properties when placed on a biometric scanner. Using wavelet decomposition technique, statistical features are extracted in multiresolution scales. Based on these features, vitality detection is performed using neural networks and classification trees. This method produced approximately 90.9-100% classification of spoof and live fingerprints.

Tan and Schuckers (2010) proposed a new method by combining ridge signal and valley noise analysis for spoof detection in fingerprint sensors [9]. This method estimates perspiration patterns along ridges in live images and noise patterns along valleys in spoof images. The signals representing grey level patterns along ridges and valleys are explored in frequency, spatial and wavelet domains. Based on these features, separation between live and spoof images is performed using standard pattern classification tools including neural networks and classification trees. This method produces an EER of 0.9% for an optical scanner.

In general, a fake fingerprint image does not have a good quality as a live one. Galbally *et al*. (2012) proposed an important idea to detect vitality by checking quality. A fast and convenient wavelet-based algorithm based on the computation of the standard deviation of the fingerprint image is proposed. Chaudhari and Deore (2012) proposed vitality detection based on wavelet features. The coefficients are altered using the zoom-in property of the wavelets. Wavelet packet analysis and multiresolution analysis are used to get information from high frequency and low frequency content of the images respectively. Daubechies wavelet is implemented for wavelet analysis. This algorithm is tested for training set and it differentiates live fingerprints from fake fingerprints.

Hassan and Bhram (2012) proposed a wavelet based approach to detect vitality, integrated with the fingerprint matcher. Vitality is determined from perspiration changes in the fingerprint ridges. The proposed algorithm is applied to a data set of approximately 58 live, 28 cadaver and 50 spoof fingerprint images. This system of fingerprint matcher and vitality module reduces EER to 0:03%.

Cappelli *et al*. (2010) evaluated direct attacks for fake fingers that are generated from ISO templates. Fingerprint image is reconstructed from minutiae templates to perform vulnerability evaluation against direct attacks by fake fingers.

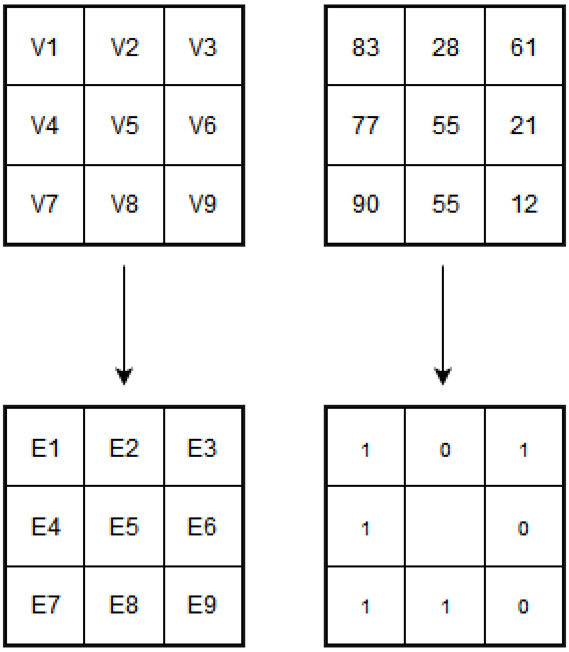
Proposed Work:

Local Derivative Pattern (Ldp):

Local Binary Pattern and Local Derivative Pattern [13] are Local Pattern Descriptors used for biometric recognition. LBP is used to represent the spatial structure of an image. Local Binary Pattern is used to capture small texture details. LBP gives the first order intensity pattern change.

LBP is a gray-scale invariant texture measure. It is used to model texture images. LBP represents the spatial structure of an image. The LBP operator considers 8 neighborhood pixels around a center pixel. It takes the value of center pixel s threshold value. and produces the results as a binary number. An LBP code for a neighborhood was produced by multiplying the threshold values with weights given to the corresponding pixels, and summing up the result.

$$E_i = \begin{Bmatrix} 0 & if\ V_i < V_0 \\ 1 & if\ V_i < V_0 \end{Bmatrix} \quad for \quad i = 1,2,\ldots.8 \qquad (1)$$



(a) (b)

Fig. 4: (a) LBP representation
(b)Example of obtaining the LBP

It is efficient and robust to monotonic illumination variation. But LBP is more sensitive to non-monotonic illumination changes. It fails to extract detailed information. LDP is a high-order texture descriptor.LBP operator extracts the first order pattern information. But LDP operator extracts second order pattern information. It is used to encode directional pattern features based on local derivative variations.

The nth-order LDP is proposed to encode the (n - 1) th -order local derivative direction variations. It contains more detailed information than the first-order local pattern used in local binary pattern. LDP is a 8 bit binary code descriptor. The code is assigned to each pixel of an image. It can be calculated by comparing the relative edge response value of a pixel in eight different directions. LDP captures curves, edges and texture characteristics. Edge responses are more illumination insensitive and noise insensitive than intensity values.

Zhang *et al.* (2010) stated that LDP is a gray-scale texture pattern. LDP assigns an 8 bit binary code to each pixel of an input image. It characterizesthe spatial structure of a local image texture. Local direction pattern method encodes the directional information of the textures and produces a more discriminative code. It encodes the structural information and the intensity variations of the texture. It gives the structure of a local neighborhood by taking its directional information. The edge responses are computed in the neighborhood, in eight distinct directions using a compass mask at each pixel. Then, from all the directions, the top positive and negative directions are selected to produce a meaningful code for different textures with similar structural patterns. This approach allows us to differentiate intensity changes in the texture. Since the edge responses are more illumination and noise insensitive than intensity values, the LDP feature describes the local primitives including different types of curves, corners, and junctions, more stably and retains more information. Given a central pixel in the image, the eight directional edge response values {mi}, 0, 1,7 are computed by Kirsch masks in eight different orientations centered on its position. Since the presence of an edge or corner shows high response values in some particular directions,thus, most prominent directions of k number with high response values are selected to generate the LDP code. In other words, k top-directional bit responses are set to 1, and the remaining bits are set to 0. After computing the LDP code for each pixel (,) r c, the input image I of size M N × is represented by a LDP histogram H.

$$\begin{bmatrix} -3 & -3 & 5 \\ -3 & 0 & 5 \\ -3 & -3 & 5 \end{bmatrix} \begin{bmatrix} -3 & 5 & 5 \\ -3 & 0 & 5 \\ -3 & -3 & -3 \end{bmatrix} \begin{bmatrix} 5 & 5 & 5 \\ -3 & 0 & -3 \\ -3 & -3 & -3 \end{bmatrix} \begin{bmatrix} 5 & 5 & -3 \\ 5 & 0 & -3 \\ -3 & -3 & -3 \end{bmatrix}$$

East M_0 North East M_1 North M_2 North West M_3

$$\begin{bmatrix} 5 & -3 & -3 \\ 5 & 0 & -3 \\ 5 & -3 & -3 \end{bmatrix} \begin{bmatrix} -3 & -3 & -3 \\ 5 & 0 & -3 \\ 5 & 5 & -3 \end{bmatrix} \begin{bmatrix} -3 & -3 & -3 \\ -3 & 0 & -3 \\ 5 & 5 & 5 \end{bmatrix} \begin{bmatrix} -3 & -3 & -3 \\ -3 & 0 & 5 \\ -3 & 5 & 5 \end{bmatrix}$$

West M_4 South West M_5 South M_6 South East $_{M7}$

Fig. 5: Kirsch edge masks in all eight directions

M3	M2	M1
M4	X	M0
M5	M6	M7

Fig. 6: Edge Response

b3	b2	b1
b4	X	b0
b5	b6	b7

Fig. 7: LDP Binary bit positions

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.

Experimental results:

For each algorithm we calculated the False Acceptance Rate (FAR) that is equal to the percentage of misclassified live fingerprints and False Rejection Rate (FRR) is equal to the percentage of misclassified fake fingerprints. 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 gelatin or liquid silicon is poured over the mould. The result, after a certain time interval, is an artificial replica of the fingertip.

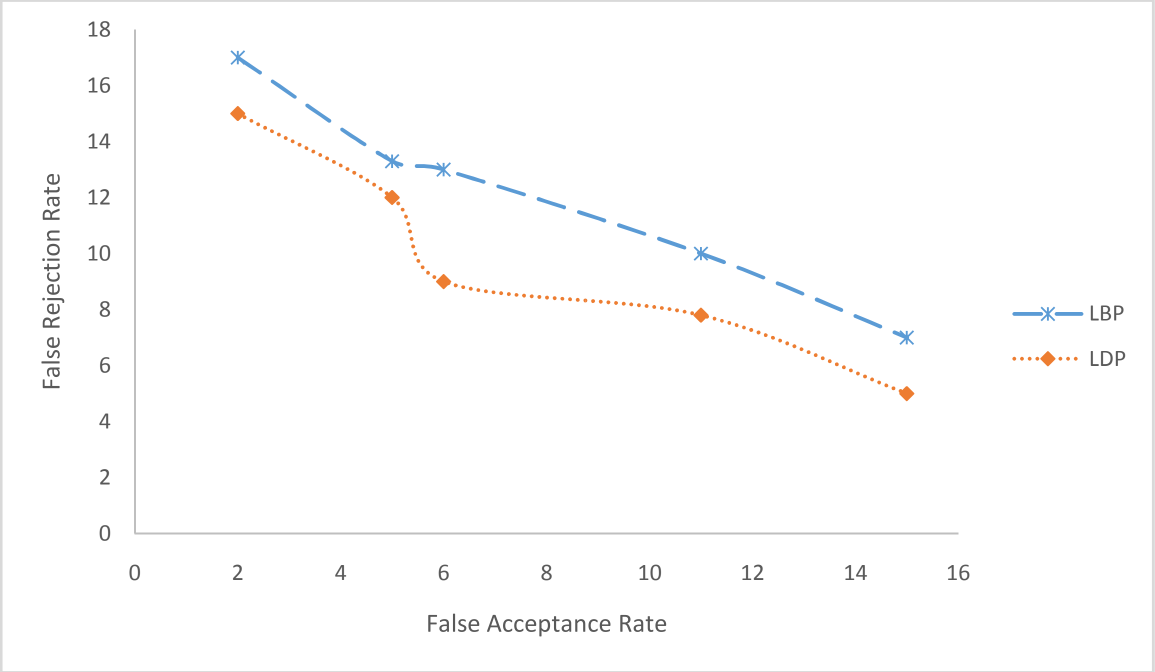


Fig. 8: Comparison between LBP and LDP- Dotted line represents LDP and dashed line represents LBP.

Conclusion:

Biometrics identify people by measuring physiological characteristics. Biometric system has several advantages over traditional methods. But it can be affected by several attacks. In this paper the type1 attack is discussed which is performed at the sensor level. Differentiating a genuine biometric input from fake input is known as Liveness detection. The Local Derivative pattern texture feature is extracted which is better than Local Binary Pattern. It is used to check whether the fingerprint is real or fake.

REFERENCES

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

Aditya Abhyankara and Stephanie Schuckers, 2004. A wavelet based approach to detecting liveness in fingerprint scanners, SPIE Proceedings, 5404: 278-286.

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

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

Tan, B. and S. Schuckers, 2008. 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

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

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

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

Baochang Zhang, Yongsheng Gao, Sanqiang Zhao and Jianzhuang Liu, 2010. Local Derivative Pattern Versus Local Binary Pattern: Face Recognition With High-Order Local Pattern Descriptor, IEEE Transactions On Image Processing, 19(2): 533-544.

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

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

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

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