International Journal of Security and Its Applications
Vol.9, No.10 (2015), pp.83-94
http://dx.doi.org/10.14257/ijsia.2015.9.10.07

# Fingerprint Spoof Detection Using Quality Features

Arunalatha G, M. Ezhilarasan

*Research Scholar, Department of Computer Science and Engineering*
*Professor, Department of Information Technology*
*Pondicherry Engineering College, Puducherry*
*arunalathamaha@gmail.com, mrezhil@pec.edu*

## *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. Spoof detection provides extra level of authentication to biometrics. It is used to prevent forgeries. The fingerprint spoof detection is performed by measuring the following quality features of fingerprint. They are Spatial Coherence, Clustering Factor, Gabor Features, Uniformity of Frequency field, Ridge frequency, Direction map and Contrast map. This approach is based on fingerprint image quality. This technique is software based as it requires no external hardware. This approach is inexpensive.*

***Keywords:*** *fingerprint, liveness, fake, real, spoof*

## 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.

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.

ISSN: 1738-9976 IJSIA

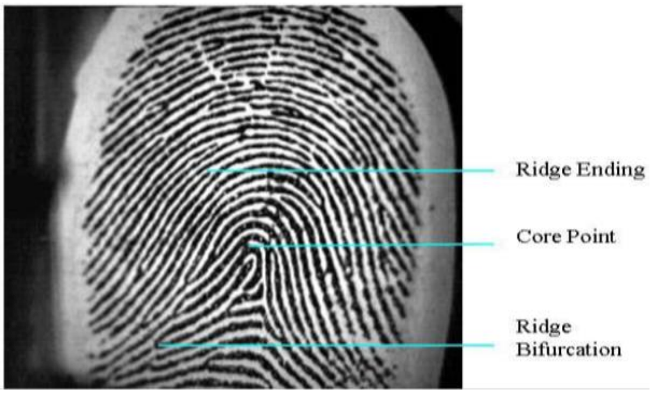

**Figure 1. Fingerprint Image**

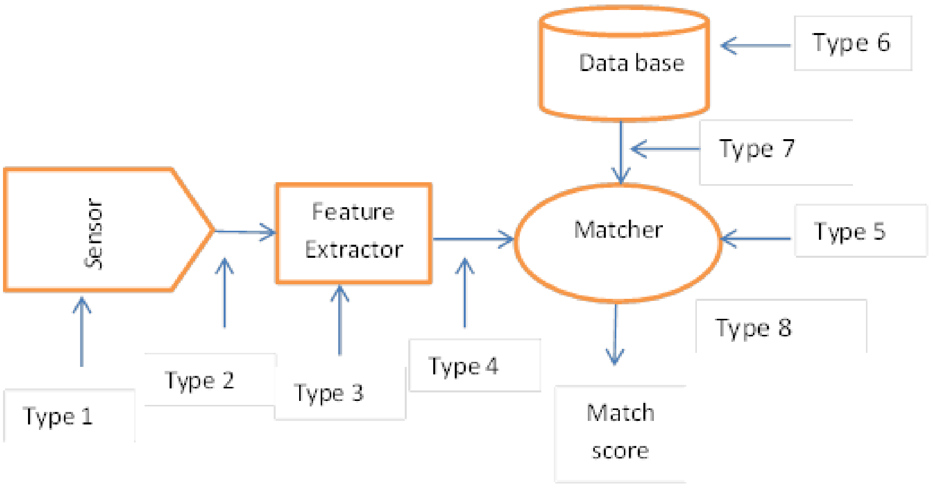

**Figure 2. Types of Attacks in Biometric System**

## 2. 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.

## Fingerprint Spoof 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.

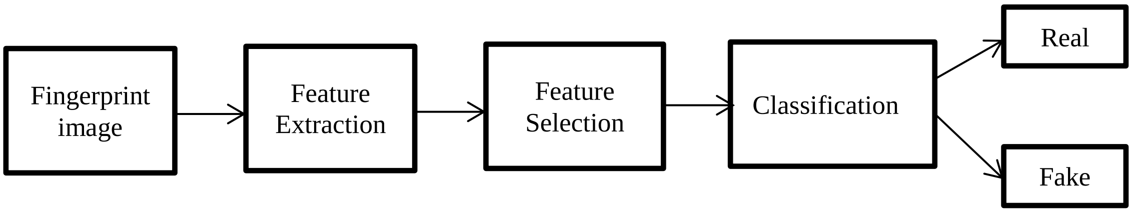

**Figure 3. Fingerprint Liveness Detection**

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 Features:

### 3.1.1 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

$$C=\frac{1}{N}\sum_{N}\left\{\begin{bmatrix}dx\\dy\end{bmatrix}\begin{bmatrix}dx & dy\end{bmatrix}\right\}=\begin{bmatrix}C_{xx} & C_{xy}\\C_{yx} & C_{yy}\end{bmatrix} \tag{1}$$

dx,dy-intensity gradient of each pixel calculated by sobel operator.

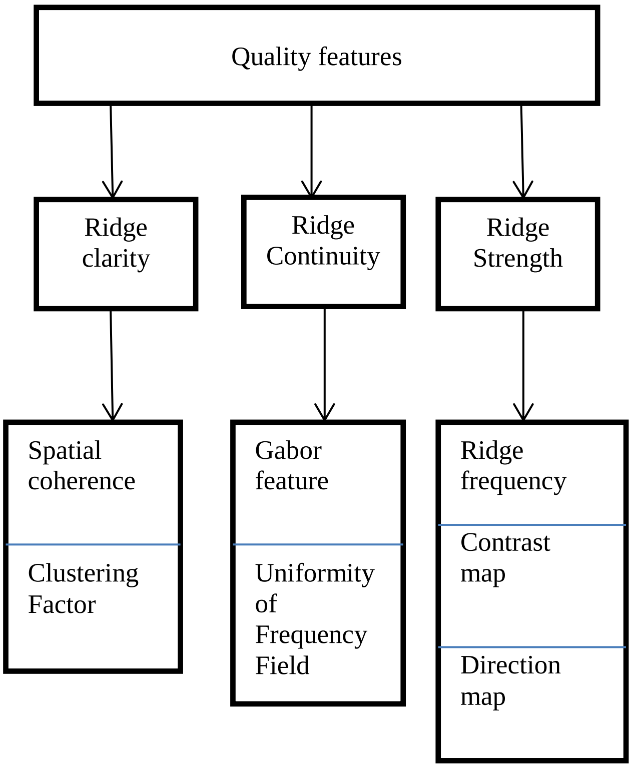

**Figure 4. Fingerprint Quality Features for Spoof Detection**

The eigen values of C are

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

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

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

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

**3.1.2 Clustering Factor:** It is used to calculate the consistency of ridges. The fingerprint image is binarized. A 3x3 mask is moved over fingerprint image. The clustering factor [14] is calculated for black and white pixel. Among 9 pixels if more than 4 contain black, a 1 is returned. If less than 4 pixels carry black, value returned is n. A circular region around the core point is located and tessellated into 128 sectors. The pixel intensities in each sector are normalized to a constant mean and variance.

A signature along the ridge-valley (x) direction, centered at the center of each sub-block can be as shown below.

$$\mathrm{T(x)} = \frac{1}{2\mathrm{r}+1}\sum_{\mathrm{k}=-\mathrm{r}}^{\mathrm{r}} \mathrm{D(x,k)} \qquad (5)$$

The first output is the frequency index Fmax corresponds to maximum amplitude in frequency domain. The second output being image quality measure computed by

$$\mathrm{IQM} = \frac{\{\mathrm{A}(\mathrm{F}_{\mathrm{max}})\mathrm{x} + 0.3[\mathrm{A}(\mathrm{F}_{\mathrm{max}} - 1) + \mathrm{A}(\mathrm{F}_{\mathrm{max}} + 1)]\}}{\sum_{\mathrm{F}=1}^{26} \mathrm{A(F)}} \qquad (6)$$

### 3.2 Ridge Continuity Features

**3.2.1 Gabor Features:** Each block for the fingerprint image is filtered using a Gabor filter with m different directions [15]. 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

$$\mathrm{h}(\mathrm{x},\mathrm{y},\theta_{\mathrm{k}},\mathrm{f},\sigma_{\mathrm{x}},\sigma_{\mathrm{y}}) = \exp\left[-\frac{1}{2}\left(\frac{{\mathrm{x}_{\theta_{\mathrm{k}}}}^2}{{\sigma_{\mathrm{x}}}^2} + \frac{{\mathrm{y}_{\theta_{\mathrm{k}}}}^2}{{\sigma_{\mathrm{x}}}^2}\right)\right] \times \exp(\mathrm{i}2\pi \mathrm{f}\mathrm{x}_{\theta_{\mathrm{k}}}) \qquad (7)$$

The magnitude Gabor feature at the sampling point (X, Y) can be defined as follows:

$$(\mathrm{x},\mathrm{y},\theta_{\mathrm{k}},\mathrm{f},\sigma_{\mathrm{x}},\sigma_{\mathrm{y}}) = \left|\sum_{\mathrm{x}=-\frac{\mathrm{w}}{2}}^{\frac{\mathrm{w}}{2-1}} \sum_{\mathrm{y}=-\frac{\mathrm{w}}{2}}^{\frac{\mathrm{w}}{2-1}} \mathrm{I}(\mathrm{X}+\mathrm{x},\mathrm{Y}+\mathrm{y})\mathrm{h}(\mathrm{x},\mathrm{y},\square_{\mathrm{k}},\mathrm{f},\sigma_{\mathrm{x}},\sigma_{\mathrm{y}})\right| \qquad (8)$$

The standard deviation value G is computed as follows:

$$\mathrm{G} = \left(\frac{1}{\mathrm{m}-1}\sum_{\mathrm{k}=1}^{\mathrm{m}}(\mathrm{g}_{\theta_{\mathrm{k}}} - \overline{\mathrm{g}_{\theta}})^2\right)^{\frac{1}{2}} \cdot \overline{\mathrm{g}_{\square}} = \frac{1}{\mathrm{m}}\sum_{\mathrm{k}=1}^{\mathrm{m}} \mathrm{g}_{\theta_{\mathrm{k}}} \qquad (9)$$

**3.2.2 Uniformity of Frequency Field:** There are two features to analyze the global structure [16] of a fingerprint image. Both of them use the local direction information provided by the direction field, which is estimated in nonoverlapping blocks. The first feature checks the continuity of the direction field. Abrupt direction changes between blocks are accumulated and mapped into a global direction score. The ridge direction changes smoothly across the whole image in case of high quality. The second feature checks the uniformity of the frequency field. This is accomplished by computing the standard deviation of the ridge-to-valley thickness ratio and mapping it into a global score, as large deviation indicates low image quality.

### 3.3. Ridge Strength Features

**3.3.1 Ridge Frequency:** Ridge frequency [16] 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 center of one ridge to the center 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 center of one ridge to the center 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.

**3.3.2 Direction Map:** The quality of each block is assessed by computing Direction map [17]. The direction map is indicating areas of the image with sufficient ridge structure. It describes the behavior of fingerprint ridge orientation.

Well-formed and clearly visible ridges are essential to reliably detecting points of ridge ending and bifurcation. In addition, the direction map records the general orientation of the ridges as they flow across the image. To locally analyze the fingerprint, the image is divided into a grid of blocks. All the pixels within a block are assigned the same results. Therefore, in the case of the direction map, all the pixels in a block will be assigned the same ridge flow direction. Several considerations must be made when using a block-based approach. First, it must be determined how much local information is required to reliably derive the desired characteristic. This area is referred to as the window. The characteristic measured within the window is then assigned to each pixel in the block. It is typically desirable to share data used to compute the results assigned to neighboring blocks. This way some of the image that contributed to one block results is included in the neighbouring blocks results as well. This helps minimize the discontinuity in block values as you cross the boundary from one block to its neighbor. This smoothing can be implemented using a system where a block is smaller than its surrounding window, and windows overlap from one block to the next. As a result, the image is divided up into a grid of 8×8 pixel blocks with each block being assigned a result from a larger surrounding 24×24 pixel window, and the area for windows of neighboring blocks overlap by up to 2/3.in practice. Designating the address of a block by its (row index, column index), the left frame is the first block (1,1) being computed. The next frame advances to the next adjacent block to the right, block (1,2). Correspondingly, its window is shifted 8 pixels, and the new block receives its results. Note that there are two copies of the image being used. Each window operates on the original image data, For each block in the image, the surrounding window is rotated incrementally and a Discrete Fourier Transform (DFT) analysis is conducted at each orientation. When determining the direction of ridge flow for a block, each of its window orientations is analyzed. Within an orientation, the pixels along each rotated row of the window are summed together, forming a vector of 24 pixel row sums. The 16 orientations produce 16 vectors of row sums. Each vector of row sums is convolved with 4 waveforms of increasing frequency.

**3.3.3 Low Contrast Map:** The low contrast map[17] is marking blocks with weak contrast, which are considered background blocks. An image map called the low contrast map is computed where blocks of sufficiently low contrast are flagged. This map separates the background of the image from the fingerprint, and it maps out smudges and lightly-inked areas of the fingerprint. Minutiae are not detected within low contrast blocks in the image. One way to distinguish a low contrast block from a block containing well-defined ridges, is to compare their pixel intensity distributions. By definition, there is little dynamic range in pixel intensity in a low contrast area, so the distribution of pixel intensities will be very narrow. A block containing well-defined ridges will have a considerably broader range of pixel intensities as there will be pixels ranging from very light in the middle of valleys to very dark in the middle of ridges. In order to determine if a block is low contrast, this software computes the pixel intensity distribution within the block’s surrounding window. A specified percent of the distribution is high and low tails are trimmed, and the width of the remaining distribution is measured. If the measured width is sufficiently small, then the block is flagged in the map as having low contrast.

## 4. Feature Selection

In order to find the optimal feature subsets, the classification performance of each of the possible feature subsets was computed using the leave-one-out technique (i.e., all the samples in the dataset are used to train the classifier except the one being classified).

## 5. 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 [13]. 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.

$$V= [SC, CF, GR, UFF, RF, DM, LCM] \tag{10}$$

SC stands for Spatial Coherence, CF stands for Clustering Factor. GF stands for Gabor features, UFF Stands for Uniformity of Frequency Field, RF stands for Ridge Frequency, DM stands for Direction map, LCM stands for Low Contrast Map.

## 6. Experimental Results

All the algorithms were tested using the four datasets collected for the Second International Fingerprint Liveness Detection Competition (LivDet 2011) by four optical sensors (Biometrika, Italdata, Digital Persona, Sagem). Each dataset is divided in two parts, one used to train a classifier and the other to test the classifier performances. Both parts consist of around 1000 “live” and 1000 “fake” fingerprint images. 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. For each algorithm we calculated the Equal Error Rate (EER) that is the value for which the percentage of misclassified live fingerprints (False Positive Rate) is equal to the percentage of misclassified fake fingerprints (False Negative Rate).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.

**Table I. The combination of different fingerprint image quality features and corresponding Avarage Classification Error. A 1 means the corresponding feature is included. A blank space means the feature is discarded.**

| No.of Features | SC | CF | GF | UF | RF | DM | LCM | ACE |
|---|---|---|---|---|---|---|---|---|
| 1 | | | | 1 | | | | 15.6 |
| 2 | | 1 | | 1 | | | | 13.5 |
| 3 | 1 | | | | 1 | 1 | | 11 |
| 4 | | 1 | 1 | | 1 | | 1 | 9.6 |
| 5 | 1 | | 1 | 1 | 1 | 1 | | 6.8 |
| 6 | 1 | 1 | 1 | | 1 | 1 | 1 | 3.5 |
| 7 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2.1 |

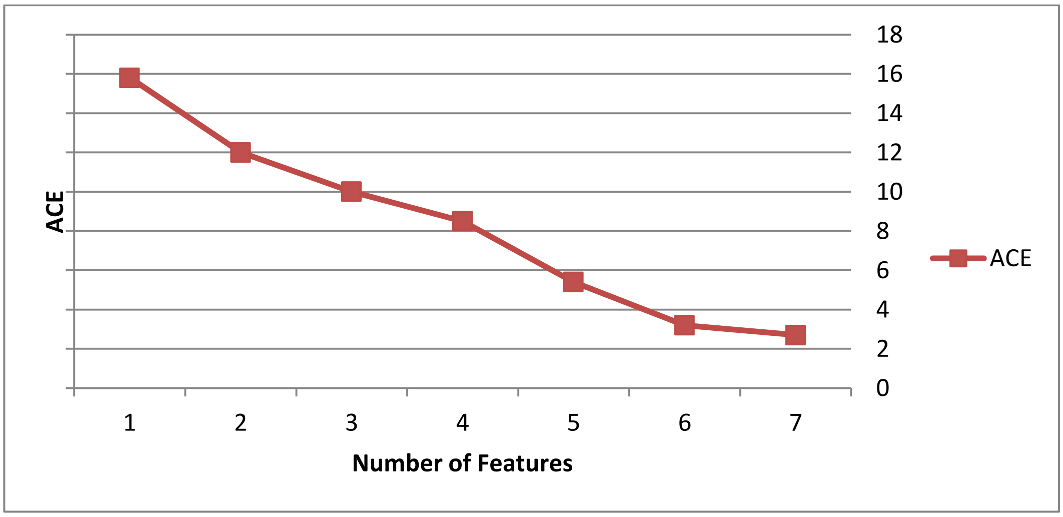

**Figure 5. Evolution of Average Classification Error for Different Number of Features**

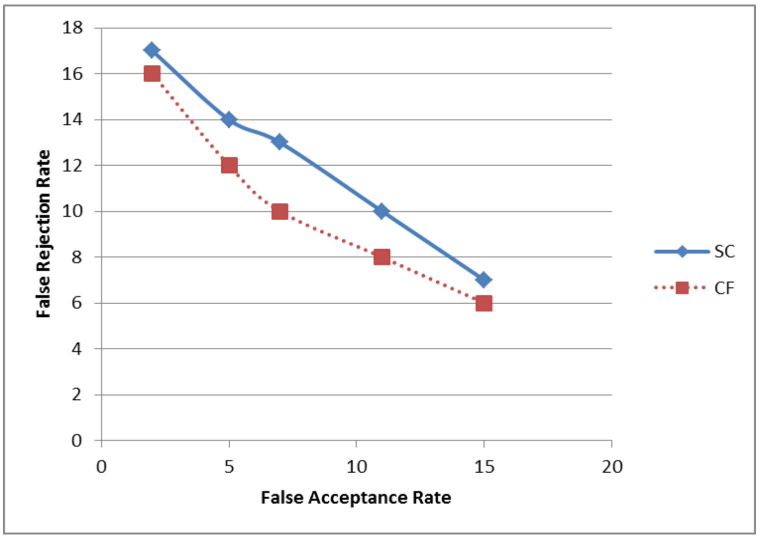

**Figure 6. Comparison of Ridge Clarity Features –Spatial Coherence (SC) and Clustering Factor (CF)**

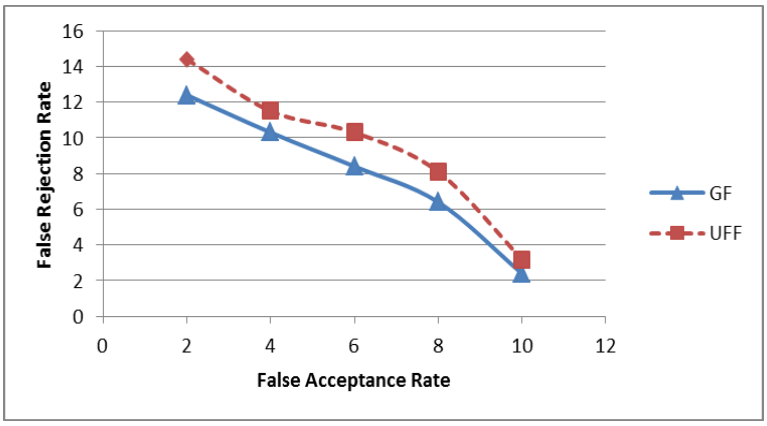

**Figure 7. Comparison of Ridge Continuity Features -Gabor Feature (GF) and Uniformity of Frequency Field (UFF).**

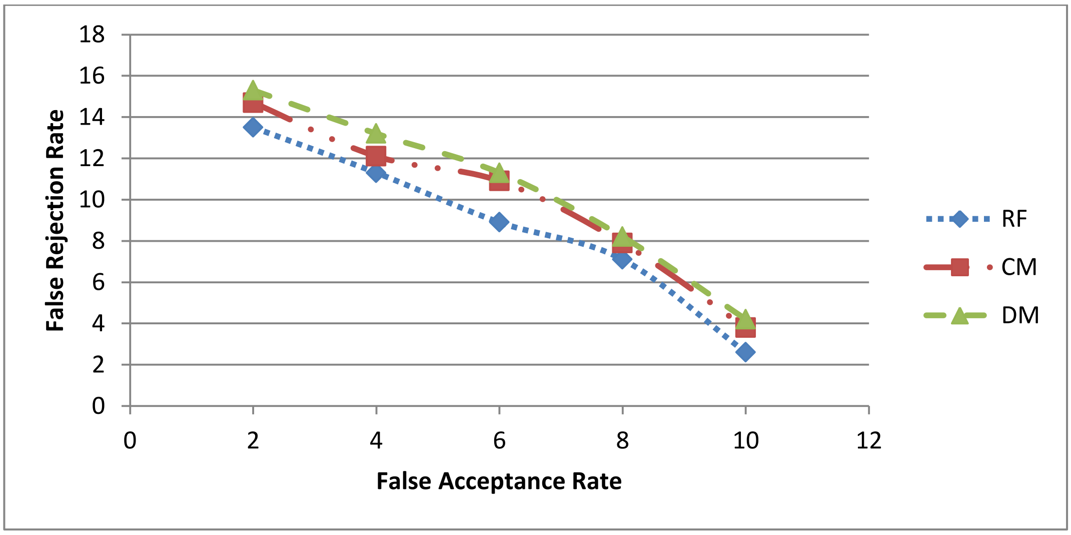

**Figure 8. Comparison of Ridge Strength Features – Ridge Frequency (RF), Contrast Map (CM) and Direction Map (DM).**

## 7. 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] Lim, E. K. Toh, P. Suganthan, X. Jiang, X. and W. Yau, Fingerprint image quality analysis, in Proc. ICIP: 1241–1244**(2004)**

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

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

[17] 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)**