Improving Sensor Interoperability for Fingerprint Biometric Systems

Varnika
M.Tech Scholar, Department of Computer Science & Applications, Kurukshetra University, Kurukshetra, Haryana
Email: varnikachawla29@gmail.com
Chander Kant
Assistant Professor, Department of Computer Science & Applications, Kurukshetra University, Kurukshetra, Haryana
Email: ckverma@rediffmail.com

Abstract

Interoperability refers to the system's ability to work with various set of devices. Fingerprints of a person are the oldest biometric identifiers and are most widely used for authentication purposes. The advances in sensor technology allow us to acquire fingerprint data of a person through variety of fingerprint sensors. The manufacturing technologies of these sensors are different. With the advancing technology, it is common to replace older designs with newer ones. So, the sensors used at the time of fingerprint enrollment and identification can be different. Different types of sensors can induce different types of variations in resolution, scanning area etc. So, there should be interoperability between sensors otherwise the performance of recognition system will be affected. The system should be able to handle the variations induced by different sensors used. This problem is discussed and a solution to overcome this problem is proposed in this paper.

Keywords - Biometric System, Design Diversity, Fingerprint Sensors, Quality Measures, Sensor Interoperability.

1. Introduction

Our society has become electronically connected through internet and digital devices. The technology is advancing and in today's digital world, it has become crucial to provide a highly secure and reliable environment. Biometric is increasingly used in number of applications where identity assessment of persons is needed. Biometric Technology refers to the technique of identifying an individual based on their distinguishing biological characteristics. These characteristics can be behavioral (like voice, gait, gesture, keyboard typing, signature) and can be physiological (like fingerprint, hand geometry, face, retina, iris of a person). A biometric system can either be a verification system i.e. 'whether the person is who that he/she claims to be' or an identification system i.e. 'whether the person is identified as an authorized person' [1]. Despite of various benefits like fraud detection, improved security, there are various challenges faced by biometric systems. Sensor Interoperability is one of the very challenging problems for biometric systems. The sensor interoperability issues may arise when a biometric sensor is replaced without recapturing the corresponding templates.

Interoperability is how system works when different set of devices are used. Sensor Interoperability in biometric systems is the ability of the system to adapt to the data acquired from variety of sensors [2]. Today, most biometric systems are designed with the assumption that the data collected for enrollment and for identification or verification of biometric trait of a person is obtained from same type of sensor [3]. According to [4], there are many face verification algorithms that makes it mandatory to capture the images with same camera. But it is not guaranteed that same sensor that has been used for the enrollment of the modality will also be used during recognition process. The sensors used in the system greatly affect the captured raw data. If the nature of this data is affected, then it will also affect the feature set. Thus, the matching score will be subsequently affected and the performance of the matcher decreases. Different types of sensors induce different types of variations in the data such as variations in the resolution of the image, sensor area, sensor's position with respect to the user, gray level, distortion effects etc. Since the matching module cannot handle variations in the feature set, there will be an impact on the matching scores if different sensors are used during enrollment mode and recognition mode. In [2], authors used two different sensors (optical sensor and solid state capacitive sensor) for capturing the fingerprint image and obtained significantly different images.

For a secure and reliable access, biometrics is now being used at variety of places. Due to this rapid growth in the usage of biometric systems in various fields, there is a diverse set of sensors available in the market which emphasizes the importance of sensor interoperability in biometrics. For example, to capture iris images, sensors used are distance based and wavelength based [5]. Similarly, signature of a person can be captured through various electronic devices like pen table, grip pens, smart phones, Personal Digital Assistants (PDAs) etc. People can use any of the available sensors to interact with the biometric system which is good for the consumers. Moreover, with the increasing number of new sensors, old ones are to be replaced with new ones and it is not feasible to re-enroll the modalities every time the sensor changes. Thus, if a biometric trait is enrolled with one device is matched with the data captured from other device then there will be chances of getting error if interoperability issue is not considered.

2. Fingerprint Acquiring Technology

2.1 What is a fingerprint?

Finger skin is made of friction ridges which are created during the fetal live and are in genetically defined shape. The fingerprints of the person remain the same in the entire life (only grows to adult size). Basically, there are three basic patterns of fingerprint ridges that are arch, loop, and whorl. On the basis of these patterns we can easily differentiate between the identities of individuals and these are shown below:

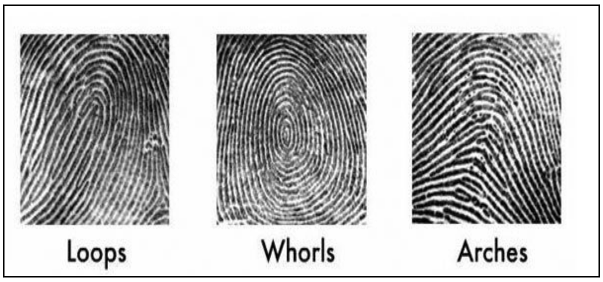

Figure 1: Fingerprint Patterns

2.1.1 Arch: In this pattern the ridge runs along the fingertip and curves up in the middle.

2.1.2 Loop: Loops basically have a stronger curve rather than arches and they enter and exist on the same side. Radial loops slant toward the thumb & Ulnar loops loop away from the thumb impression.

2.1.3 Whorl: An oval arrangement of ridge lines, often making a spiral pattern around a central point. Principal types are a Plain Whorl, Central Pocket Loop Whorl, Double Loop Whorl & Accidental whorl.

2.2 Fingerprint Sensors

Fingerprint sensors are used to detect the minutiae points i.e. ridge ending, bifurcation, dot or an island [6]. Various types of fingerprint sensors available today are shown in fig. 2 [7, 8] and explained below:

2.2.1 Offline fingerprint Acquisition: This includes Ink Technique. These are the first fingerprint scanners which are still used in some applications. In this technique, firstly the finger is smeared with ink and then the finger is pressed against a paper to get the patterns of valleys and ridges on a paper. This is then converted into digital form by means of paper scanner. It is simple but slow technique.

2.2.2 Optical Sensors: Optical sensor captures a digital image of the fingerprint using visible light. The finger is placed on the touch surface which is the top layer of the sensor. A light-emitting phosphor layer is used below it that illuminates finger surface. A charged couple device is used to capture the light reflected from the finger and thus visual image of the fingerprint is captured.

2.2.3 Solid State Sensors: These are silicon based sensors and that consists of an array of pixels where each pixel is itself a tiny sensor. So, this has reduced the problem of size as these can be easily implemented in cell phones, laptops etc.

2.2.4 Ultrasound Sensors: It works on the principle of acoustic signals. This consists of 2 components-transmitter and receiver. The acoustic signal is generated by the transmitter is sent to the finger surface. The receiver detects the echo when the signal bounces off the fingerprint surface. This echoed signal is used to determine the fingerprint pattern. This method can image the fingerprint even through a thin layer.

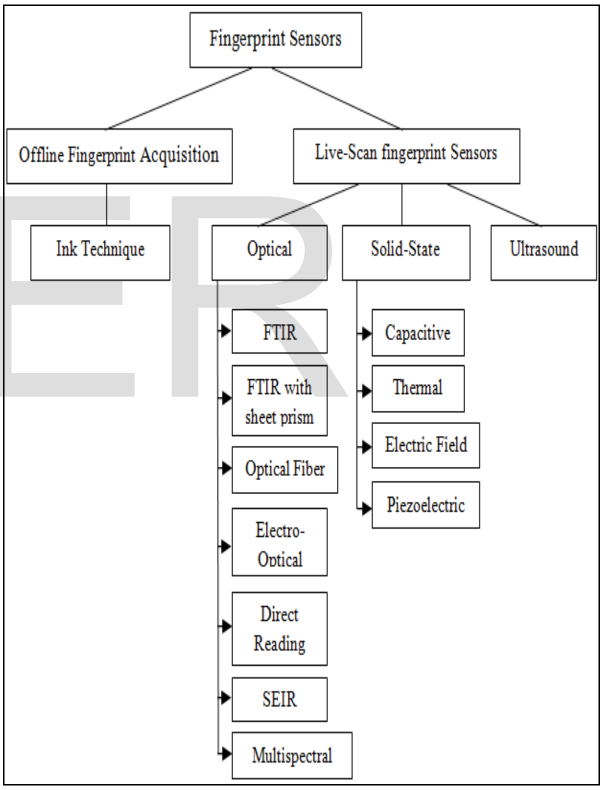

Figure 2: Types of fingerprint sensors

3. Related Work

Problem of sensor interoperability cannot be solved by using only common biometric data exchange formats. There are various works that points out the importance of sensor interoperability in biometric system as discussed below:

The matching performances of a fingerprint system when different types of sensors were used was analyzed [2]. They considered that the issue of interoperability is related to the variations induced in the feature set when different sensors are used for sensing. The experiment was conducted using 2 different fingerprint sensors i.e. Optical sensor and solid-state capacitive sensor. The Equal Error Rate (EER) of 23.13% was reported when matching images are acquired by Optical and Solid-State sensors while EER was 6.14% and 10.39% when using only Optical and Solid-State sensors, respectively. It was also reported that the optical sensors results in the extraction of more minutiae points as compared to solid-state sensor.

The authors in [9] analyzed image quality of the fingerprint images. The fingerprints of 494 participants were taken using 4 different biometric fingerprint devices. 10 fingerprints of each of 494 participants were collected and the data was taken twice per person: one used at the time enrollment and other for authentication or identification. They found that the genuine matching scores were higher when same device was used to capture the samples compared with the case that different devices were used. It was also found that the FRR was affected when data capturing devices were different. It was also reported that the similarity scores were much more sensitive to the quality of the captured data when devices used for sensing were different than when same device was used.

In [10], the authors proposed a classification scheme that combines the extracted features and match scores. Approximately 500 subjects were taken and the data was captured using 4 different optical sensors and scanned rolled ink prints to evaluate classification performance of a set of fingerprints. The experiment shows a significant impact on match rates when the interoperability is low. The approach used reduces the cross-device match error rates by a large margin.

The authors in [11], analyzed the problem of device interoperability for dynamic signature verification. The authors proposed a two-staged approach: the first was preprocessing stage where the data captured from different devices is processed and the signals were normalized in similar ranges, the second stage was based on feature selection where the selection of best features which were robust in conditions when different devices were used occurs. They applied these two stages on global features based and time function based systems and concluded that there was an average improvement of 40.5% EER in global features based and 14.0% EER in time function based systems. Finally, fusion of global features based and time function based systems was done and by applying their proposed approach there was an improvement of 27.7% EER as compared to best performance of time function based system.

In [12], the paper discusses the relationships among individual, sensor and features. The impact of feature selection on sensing device interoperability in biometric systems was illustrated. The experiment shows that different features put different sensor interoperability on different sensors. They argued that sensor interoperability results mainly because of two factors: one is due to inherent performances gap between two sensing devices and second factor is performance drop caused due to coordinating two sensors.

The authors in [13] proposed a superpixel based finger vein region of interest (ROI) extraction with sensor interoperability in biometric systems. Finger boundaries were firstly determined by tracking superpixels. Then the middle points of detected finger boundaries were used to adjust the finger directions. Finally, internal tangents of finger boundaries were used to localize ROI. It was found that this method extracts ROI accurately from the images acquired using multiple sensors.

The authors in [14] proposed a compensation algorithm to improve sensor interoperability for fingerprint recognition. Two methods: Common resolution method and Relative resolution methods were proposed for compensating resolutions of fingerprint images that were acquired by different sensors. The average EER of 8.62%, improved to 5.37% by applying Relative resolution compensation and improved to 6.37% by Common resolution compensation method.

4. Proposed Work

There are various types fingerprint sensors used today and sensing mechanism of each device is different. The type of sensor used produces fingerprint images with different characteristics which prevent them from being interoperable. Sensor interoperability can be achieved by discarding the impact of the sensor before the feature extraction process. This is to be done so that variation induced by a particular type of sensor does not affect the features to be extracted for template generation and hence the matching score will not get affected due to sensor variation. In this work we start by analyzing the different measures that defines the quality of the fingerprint images. Quality-based processing has been used in various works to increase the interoperability between devices but in this approach we apply selective operations depending upon the sensor used for enhancing a fingerprint image. For this firstly training of the biometric system is required.

4.1 Fingerprint Quality Measures

Various parameters like resolution, sensing area, aspect ratio, gray level, distortion etc.,[8, 15] and other quality measures that are needed be considered regarding a fingerprint are discussed below:

4.1.1. Resolution: It is density of pixels i.e. pixels per inch (ppi) or dots per inch (dpi). Maximum and minimum allowed resolution of biometric sensor is 500dpi±10%.

4.1.2. Gray scale: Value of gray scale range used by the sensor.

4.1.3. Sensing area of the sensor**:** A rectangular type area (height*width) that senses the fingerprint. If sensing area is large, more ridges and valleys can be captured and hence we get good quality. But more sensing area poses problem of incorporation in small devices and cost of sensor is also increased.

4.1.4. Geometrical accuracy: It is the introduction of maximum geometric distortion by an acquisition device is known as geometrical accuracy. It is expressed in the form of percentage with respect to x and y direction. The distortion in fingerprint alignment causes interoperability issues when different sensors are used for acquisition.

4.1.5. Signal/Noise ratio: It is defined as the ratio of signal power to noise power. Practically, S/N ratio is 500±2%. Correlation between the noise pattern and sensor reference pattern for a particular type of sensor should be analyzed.

4.1.6. Dynamic range or depth: It is the number of bits used to encode the intensity value of each pixel. Its value is generally taken as 8.

4.1.7. No. of pixels: It is determined using the value of resolution and acquisition area. Let resolution is denoted by 'R' dpi and area as 'height (h)*width (w)' then (Rh*Rw) gives the total number of pixels.

4.1.8 Image Quality: This is the measure that tells how useful a biometric sample is. It tells the utility of the image. For image quality assessment, divide the fingerprint image into blocks of equal size. Assign weight (W_i) to each i^{th} blocks according to the equation 1 as given below [16]:

$$W_i = \exp\left(\frac{-\| l_i - l_c \|^2}{2r^2}\right) \tag{1}$$

Here, $l_c = [A_c , B_c]$ which is the centroid of the fingerprint image, $l_i = [A_i , B_i]$ is center of each i^{th} block and 'r' is the normalization constant. Blocks near the center are assigned higher weights. The image quality of the fingerprint is measured by determining the ratio of total weights of directional blocks to the total weight of all the blocks.

4.1.9 Minutiae Count: It tells the total number of minutiae that can be extracted from an image. The number of minutiae depends upon how the user interacts with a particular sensor. For accurate matching of results more minutiae points are to be extracted.

4.1.10 Intensity Statistics: Intensity parameter of a particular image can be obtained directly from the histogram of the image.

4.2 Fingerprint Sensor Estimation

Consider two set I and S, where $S = \{S_1, S_2, S_3, ..., S_n\}$ be the set of 'n' fingerprint sensors used for image acquisition and $I = \{I_1, I_2, I_3, ..., I_m\}$ be the set of 'm' images acquired by any sensor $S_i \in S$ There should be the one-to-one correspondence between captured image and the sensor used i.e. $I_j \leftrightarrow S_i$, $\forall I_j \in I$. This means that an image is captured using a particular sensor. For sensing device estimation, various combinations of above quality measures are to be taken into consideration. Let 'k' be the number of quality measures taken for device estimation, the set is defined as $Q = \{Q_1, Q_2, Q_3, ..., Q_k\}$. For learning process, images captured from different sensors are used to train the biometric system. Let 't' be the set of images used during training phase, the correspondence is established as:

$$I_j \leftrightarrow S_i : I_{train} = \{I_1, I_2, I_3, ..., I_t\}$$
$$\exists \{ I_j \leftrightarrow S_i \}, \forall I_j \in I_{train}, S_i \in S$$

The quality measures considered for each device is given as:

$$Q_d = \{Q(I_1), Q(I_2), Q(I_3), ...Q(I_t)\}; \forall I_j \in I_{train}$$

For training process, Q_d is used to by the learner to map the fingerprint images to the camera that has captured it. It can use classifiers like Support Vector Machines, Nearest Neighborhood classifier etc.

4.3 Selective Operations

Let $O = \{O_1, O_2, O_3, ..., O_s\}$ be the set of 's' different operations. The aim is to select one or more of these operations for each fingerprint sensor. So, there is one-to-many correspondence between sensing device and operations $S_i \rightarrow O_q$, where $O_q \in O$; $\forall S_i \in S$.

Let the set of operations corresponding to each sensing device S be represented as OP_i so that we have a one-to-one correspondence $S_i \leftrightarrow OP_i$ and $OP_i \in OP$. Suppose given a raw image with unknown correspondence $I_j \leftrightarrow S_i$, let $I_j \in I$ and suppose 'I_r' is used to represent it and O_r be its quality measures. The trained Leaner is used to map the raw image I_r with sensor $S_{selected}$.

$$S_{selected} = \{S_i\}$$
$$\exists \{\text{Learner}(Q(I_r)) \rightarrow S_i\}, \exists S_i \in S$$

i.e. depending upon the device used selected operation is to be applied.

The variety of techniques can be applied depending upon various quality parameters like image quality, distortion, blurriness, noise etc. These include applying techniques or operations like Weiner Filter Morphological Processing, Genetic Algorithms, Contrast Enhancement, Histogram Equalization etc. Thus, in this way the variations induced by the sensor can be overcome before being used for cross-sensor fingerprint recognition.

4.4 Image Normalization

Linear Normalization of the digital image is performed. The image is normalized with the intensity values in the range {Min, Max}. The linear normalization can be applied using the equation 2:

$$I_N = (I - Min)\,\frac{newMax - newMin}{Max - Min} + newMin \qquad (2)$$

4.5 Architecture of the system

4.5.1 Training Phase

In the training phase, the system is provided with the test images taken from the various fingerprint sensors. The system learns from the quality measures that which type sensor has been used to take a particular image. After estimating the device used to capture the image, the selective operations or techniques can be applied on the raw image depending upon the quality measures. The basic steps involved in the training of the system are shown in fig. 3.

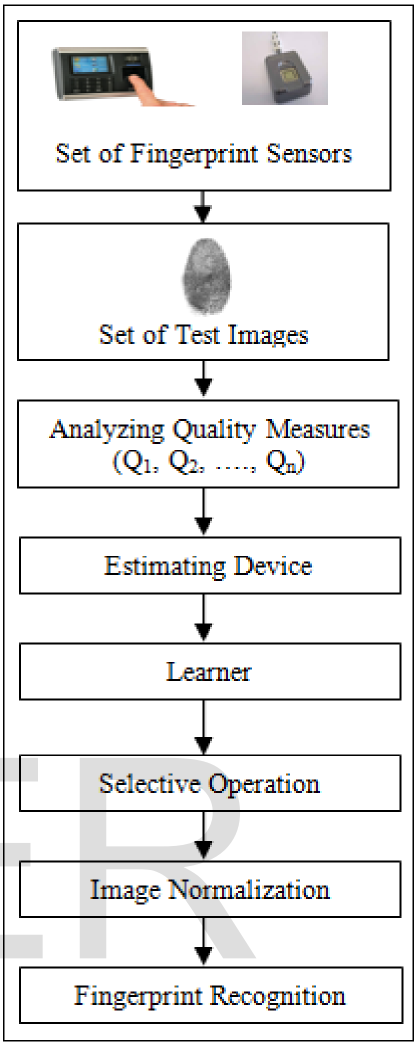

Figure 3: Training Phase of the system

4.5.2 Enrollment/ Recognition Phase

The system has been trained with the type of operation to be performed on the raw image captured from a particular device depending upon the quality measures. After the feature extraction and the template generation, the template is matched with the enrolled templates. If the calculated match score is greater than equal to the predefined threshold value then the fingerprint image is accepted as of the genuine user otherwise rejected. The threshold can be Bayes Threshold whose values depends upon the prior probabilities of the hypothesis p(A) and p(B), where ‘A’ is the target hypothesis that the image came from same person and ‘B’ is the non-target hypothesis that the image came from different persons. The process is shown in fig. 4.

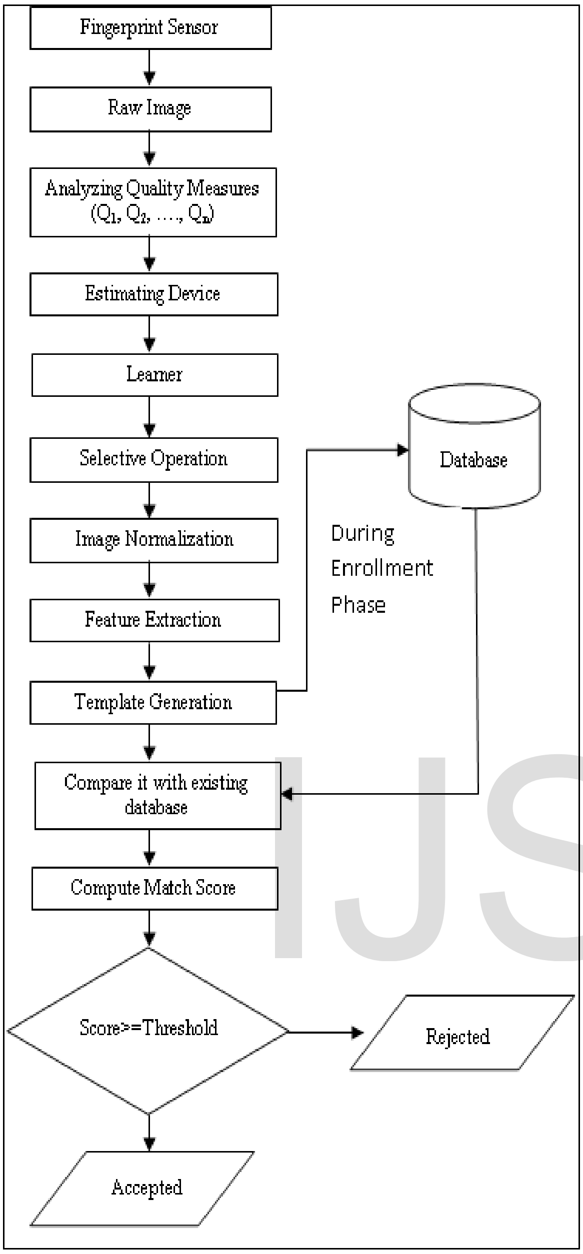

Figure 4: Enrollment/ Recognition Phase of the system

5. Conclusion

There are a variety of fingerprint sensors available today and different sensors put different types of variations on the raw fingerprint data like blurriness while capturing image, pixel density, gray scale, distortion etc. These in turn affects the match scores of the biometric trait. So in the proposed approach these variations are removed before the recognition process so that these will not put any effect on the matching scores of the fingerprint image. For this, the system is firstly trained to apply selective operations on the captured raw image by determining the device used depending upon various quality measures. This is done to reduce the impact of the sensor during the cross-sensor recognition process. The approach can improve interoperability among fingerprint sensors. In the future the approach can be enhanced to be applied on all the biometric sensors.

References

[1] Renu Bhatia, "*Biometrics and Face Recognition Techniques*," International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Vol. 3, Issue 5, pp. 93-99, May 2013.

[2] Arun Ross, Anil Jain, "*Biometric Sensor Interoperability: A Case Study In Fingerprints*," Appeared in Proc. of International ECCV Workshop on Biometric Authentication (BioAW), Springer, LNCS Vol. 3087, pp. 134-145, May 2004.

[3] Anil Jain, Arun A. Ross, Karthik Nandakumar, *Introduction to Biometrics*, Springer, Chapter 1, pp. 37.

[4] Phillips, P.J., Martin, A. Wilson, C.L., Przybocki, M, "*An introduction to evaluating biometric systems*," IEEE Computer 33, pp. 56–63, 2000.

[5] Gursimarpreet Kaur, Dr. Sheetal Verma, Dr. Chander Kant Verma "*Classification Of Fingerprint, Iris And Facial Sensors*," IJSRD - International Journal for Scientific Research & Development, Vol. 2, Issue 03, ISSN (online): 2321-0613, 2014.

[6] Shweta Gaur, Mannish Thakker, "*Biometric Recognition Techniques: A Review*," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE), Vol. 1, Issue 4, pp. 282-290, October 2012.

[7] Salil Prabhakar, Alexander Ivanisov, and Anil Jain, "*Biometric Recognition: Sensor Characteristics and Image Quality*," IEEE Instrumentation & Measurement Magazine, pp. 1094-6969, June 2011.

[8] Davide Maltoni, Dario Maio, Anil Jain, Salil, *Handbook of Fingerprint Recognition*, Chapter 2.
[9] Luca Lugini, Emanuela Marasco, Bojan Cukic, Ilir Gashi, "Interoperability in Fingerprint Recognition: A Large-Scale Empirical Study," IEEE, 2013.

[10] Emanuela Marasco, Luca Lugini, Bojan Cukic, Thirimachos Bourlai, "*Minimizing the Impact of Low Interoperability between Optical Fingerprints Sensors*," IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), Arlington, VA, pp. 1-8, September 29 2013-October 2 2013.

[11] Ruben Tolosana, Ruben Vera-Rodriguez, Javier Ortega-Garcia, Julian Fierrez, "*Preprocessing and*

Feature Selection for Improved Sensor Interoperability in Online Biometric Signature Verification," IEEE, Vol. 3, pp. 478-489, May 2015.

[12] Chunxiao Ren, Yilong Yin, Jun Ma, Gongping Yang, "Feature Selection For Sensor Interoperability: A case Study in Fingerprint Segmentation," IEEE International Conference on Systems, Man and Cybernetics, pp. 5202-5207, October 11-14, 2009, proceedings.

[13] Lu Yang, Gongping Yang, Lizhen Zhou, Yilong Yin, "*Superpixel based Finger Vein ROI Extraction with Sensor Interoperability*," IEEE International Conference on Advances in Biometric (ICB) 2015, pp. 444-451, May 19-22, 2015.

[14] Jihyeon Jang, Stephen J. Elliott, Hakil Kim, "*On Improving Interoperability of Fingerprint Recognition using resolution Compensation Based on Sensor Evaluation*," International Conference on Advances in Biometrics(ICB) 2007, Seoul, Korea, pp. 455-463, August 27-29, 2007, proceedings.

[15] Davide Maltoni and Matteo Ferrara, "*On the Operational Quality of Fingerprint Scanners*," BioLab- Biometric System Lab Biometric System Lab University of Bologna University of Bologna – ITALY, Nov 7, 2007.

[16] Anil Jain, Arun A. Ross, Karthik Nandakumar, *Handbook of Multibiometrics*, Springer, Chapter 5, pp. 150.