IJCSC 0973-7391 Volume 8 • Issue 2 March 2017 - Sept 2017 pp. 66-71 available online at www.csjournals.com

Minimizing Sensor Interoperability Problem using Euclidean Distance

Himani[1], Parikshit[2], Dr.Chander Kant[3]
M.tech Scholar[1], Assistant Professor[2, 3]
[1,2]Doon Valley Institute of Engineering and Technology, Karnal, India
[3]Department of Computer science and Application, Kurukshetra University, Kurukshetra, India
[1]himanisaluja26@gmail.com, [2]par7901@gmail.com , [3]ckverma@redifmail.com

Abstract: Fingerprint is one of the best apparatus to identify human because of its uniqueness, hard to change and long-term indicators of human identity. Biometric System suffers a significant loss of performance when the sensor is changed during enrollment and authentication process. 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. Euclidean distance helps in recognition of fingerprint images depends upon the threshold value. Euclidean distance calculated between the feature vectors. The algorithm is also capable of comparing and producing matching scores between two fingerprint images obtained from two different sensors, hence is sensor interoperable. In this paper, fingerprint matching Using Euclidean distance gives accurate matching results.
Keywords: Biometrics, fingerprint Sensor, Sensor Interoperability, Euclidean distance.

1. Introduction:

Biometrics is the use of physical or behavioral traits to verify personal identity. Biometrics is automated methods of recognizing a person based on a physiological or behavioral characteristic. Many physical body parts and personal Characteristics have been utilized to biometric systems: fingers, hands, irises, faces, ears, voices, gaits, odors, feet, signatures, and DNA [1, 2]. A biometric system contains mainly a sensor module, a feature extraction module and a pattern matching module. A Sensor module acquires the raw biometric data of a person. Feature extraction module improves the quality of the captured image. Database module saves the biometric format data from claiming selected Persons. Pattern matching module compares the present input with the saved template, which in-turn generates match score [3].

A fingerprint image is one of the noisiest of image types. This is due predominantly to the fact that fingers are our direct form of contact for most of the manual tasks we perform: finger tips become dirty, cut, scarred, creased, dry, wet, worn, etc. The image enhancement step is designed to remove this noise and to enhance the definition of ridges against valleys. In an identification system, the system conducts one to-many comparison to establish the identity of the individual. The individual to be identified does not have to claim an identity (Who am I?)[4]. In a verification system (Authentication System), the individual to be identified has to claim his/her identity (Am I whom I claim to be?) and this template are then compared to the individual's biometric characteristics. The system conducts one-to-one comparisons to establish the identity of the individual.

Fingerprint-based identification is one of the most important biometric technologies. Humans have used fingerprints for personal identification and the validity of fingerprint identification has been well established. Segmentation is an important pre-processing step in fingerprint recognition system. In segmentation image is segmented into background and foreground region so that the irrelevant data in background region can be ignored. After enhancement recognition of input image is done. Recognition includes the feature extraction of fingerprint. The recognition is done with the help of Euclidean distance algorithm. Euclidean distance helps in finding out the position of the core points in fingerprint images which can also called reference point. And last to match fingerprint after recognition. There are many methods, which can be used for accurate results of fingerprint matching. Euclidean distance simply refers to the distance between two points as measured in a straight line.

1.1. Fingerprint Sensors:

Fingerprint sensors come in various shapes and sizes, but generally into two categories [5]:

- Touch sensor: The user hold the finger on the sensor surface.
- Swipe sensor: The user slides a finger vertically over the sensor surface.[6, 7]

There is the various acquisition technologies used in fingerprint sensors: optical, capacitive, thermal, and ultrasonic [8].

1.1.1. Optical Sensor: It capturing the digital image formed by the reflection of light from the points where ridges touches the sensors touch surface. Optical finger impression followers contain of a light sensor, touch surface and a capture device which can be a Charge Coupled Device.

1.1.2. Capacitance Sensor: Fingerprint sensors consist of an array of capacitive plates on a silicon chip. One plate of capacitor is formed by the finger; other plate holds a minor region from claiming metallization on the chip. Small electrical charges are created between the surface of the finger and each of these plates when the finger will be put on the chip [9].

1.1.3. Thermal Sensor: Fingerprint sensors are made from the silicon die tiled by pixels of pyro-electric material that is sensitive to detect temperature differences. This sensor scans the surface of the finger, measuring the heat transferred from sensor to fingerprint.

1.1.4. Ultrasonic Sensor: The ultrasonic method is based on sending acoustic signals toward the finger tip and capturing the echo signal [10]. Those sensor needs two fundamental parts are: sender, that generates short acoustic pulses, and the receiver, that detects the responses obtained when these pulses bounce off the fingerprint surface.

Figure 1: Fingerprint Sensors

Sensor Interoperability:

Sensor interoperability is the ability of a biometric framework to adapt to the raw data obtained from a variety of sensors. Practically biometric frameworks would intended with look at information originated starting with the same sensor, but fail to give a good performance when the acquisition device is changed between the enrolment and the

authentication phase. Fingerprint sensor interoperability is the process of matching fingerprints collected from different sensors [11].

2. Related Work:

Chunxiao Ren et al. [12] discussed the relationship among individual sensor and features. The impact of feature selection on sensing device interoperability in biometric systems is illustrated in it. The experiment in the paper 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.

Lugini et al [13] statistically analyzed how match scores change across different optical devices. Results of the Kendall's rank correspondence test pointed out that there is a significant difference between sensor pairs and that those change will not symmetric when inverting those two devices.

Arun Ross et al.14] matching performances of a fingerprint system when different types of sensors were used was analyzed. 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.

Shimon Modi et al. [15] report performance evaluations of FR of different sizes and with different sensors, minutiae count, FNMR, FMR, image quality scores. The result shows Fingerprint images above or at level 5 are acceptable.

Jain et al [16] proposed a filter bank matching algorithm that employs Gabor filters to obtain both local and global information which in turn becomes a Finger Code. Matching is based on comparing the Euclidean distances between two such Finger Codes.

3. Proposed Framework:

A fingerprint sensor is to obtain a good quality image of the ridge pattern. The quality of a fingerprint image depends on sensor characteristics and the condition of the finger surface. Sensing mechanism of each device is different and images with different sizes, resolution, feature distribution, gray level are produced.

In this work, the fingerprint images captured using the different sensor. 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, technique can be applied on the input image depending upon the quality measures.

Fingerprint matching Using Euclidean distance gives accurate matching results. Euclidean distance helps in recognition of fingerprint images depends upon the threshold value. Euclidean distance calculated between the feature vectors. The algorithm is also capable of comparing and producing matching scores between two fingerprint images obtained from two different kinds of sensors.

Architecture of the proposed scheme:

In this proposed architecture when a user place its finger over a sensor surface then it would capture the data and then extract the features set from the sample. After that apply Euclidean Distance for fingerprint matching and then compute matching score. A match score between two fingerprints declared as matched or not matched. The architecture of proposed approach described in figure 2.

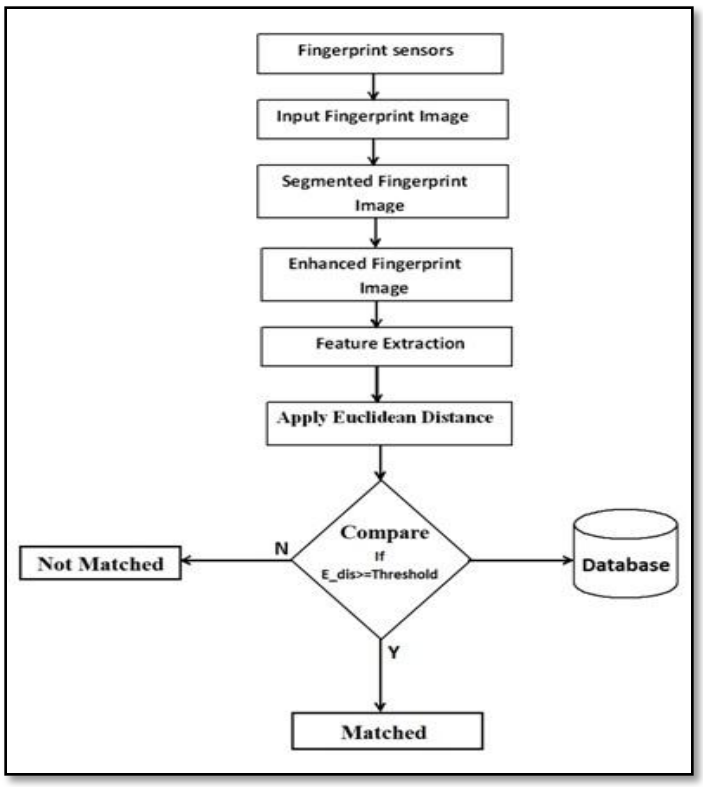

Figure 2.Architecture of the proposed scheme

A. **Image Acquisition**: This module is used to read fingerprint images using different fingerprint sensors.

B. **Fingerprint Image Segmentation:** Fingerprint image Segmentation is an important pre-processing step in fingerprint recognition system. In segmentation image is segmented into background and foreground region so that the irrelevant data in background region can be ignored.

C. **Fingerprint Image Enhancement:** Fingerprint image enhancement is to improve the quality of fingerprint image. It is used to make the fingerprint image clearer for easy further operations. This technique is useful tools to process an image so that the result is more suitable than the original image.

D. **Fingerprint feature extraction:** Fingerprint feature extraction consists of extracting the feature vector from the available raw data obtained from the sensor level. Feature extraction of fingerprint takes place at feature extraction level.

E. **Euclidean Distance:** There are two fingerprint images are matched using Euclidean distance then compare the similarity between two fingerprint images. Depending upon the obtained matching score; two fingerprints are declared as matched or not matched. This technique is to check the validity how efficient it is in matching the fingerprint images.

4. Results:

MATLAB 2013 is used to analyze the efficiency of proposed approach. The fingerprint database was taken from FVC 2004. The ROC (Receiver operating characteristics) curves for the proposed system are obtained by plotting the false accept rate versus false reject rate with different value of thresholds. FRR measure the proportion of positives that are correctly identified. FAR measure the proportion of positives that are incorrectly identified.

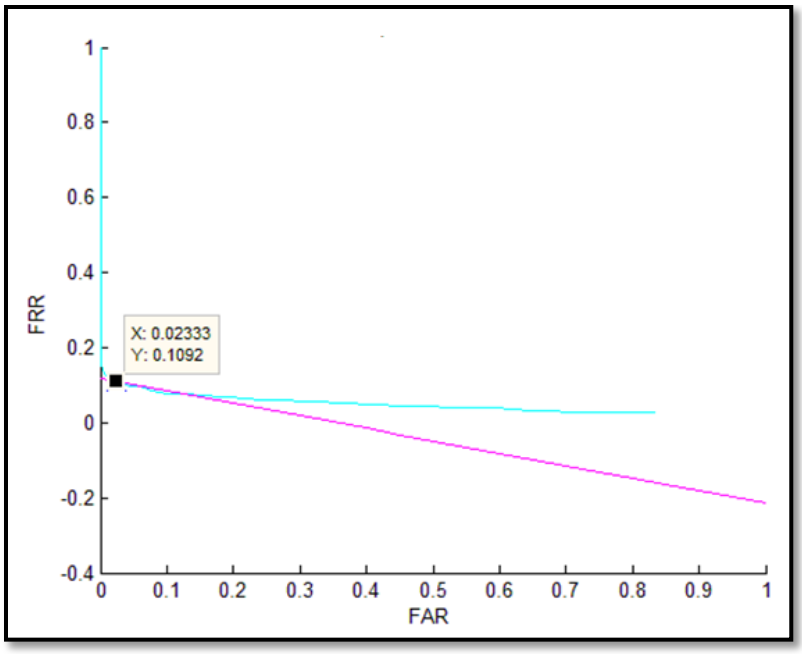

Figure 3: Roc curve of proposed approach

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. A significant performance improvement is observed when the proposed scheme is utilized to compare fingerprint images obtained from two different kinds of sensors. In this paper the problem of sensor interoperability can be overcome by using Euclidean distance. Fingerprint matching Using Euclidean distance gives accurate matching results. 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] R Raghavendra, Rao Ashok, and G Hemantha Kumar, "Multimodal biometric score fusion using gaussian mixture model and monte carlo method", Journal of Computer Science and Technology, 25(4):771–782, 2010.
[2] Renu Bhatia, "Biometrics and face recognition techniques," International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), vol. 3, issue5, pp. 93-99, May 2013.
[3] Al-Ani M. "A Novel Thinning Algorithm for Fingerprint Recognition" International Journal of Engineering Sciences, vol. 2(2), pp. 43-48, 2013.
[4] A. Bansal, R. Agarwal and R. K. Sharma, "FAR and FRR based analysis of iris recognition system,"IEEE International Conference on Signal Processing, Computing and Control, Waknaghat Solan, pp. 1-6, 2012.
[5] Shahzad Memon, Mojtaba Sepasian, Wamadeva Balachandran, "Review of Fingerprint Sensing Technologies", Conference Paper Jan. 2009.
[6] Salil Prabhakar, Alexander Ivanisov, and Anil Jain, "Biometric recognition: sensor characteristics and image quality," IEEE Instrumentation & Measurement Magazine, pp. 1094-6969, June 2011.
[7] Emanuela Marasco, Zachary Chapman, Bojan Cukic, "Improving Fingerprint Interoperability by Integrating Wavelet Entropy and Binarized Statistical Image Features", 2016.
[8] Marasco, E.; Lugini, L.; Cukic, B.: Automatic Enhancement of Interoperability between Optical Fingerprint Sensors. NIST International Biometric Performance Testing Conference (IBPC), 2014.
[9] J.Nam, S. Jung, M.Lee"Design and implementation of a capacitive fingerprint sensor circuit in CMOS technology" sensors and actuators, 2006.

[10] M. S. Ennis, R. K. Rowe, S. P. Corcoran, and K. A. Nixon, "Multispectral sensing for high-performance fingerprint biometric imaging," White Paper, Lumidigm Inc, 2012.
[11] Emanuela Marasco, Zachary Chapman, Bojan Cukic, "Improving Fingerprint Interoperability by Integrating Wavelet Entropy and Binarized Statistical Image Features", 2016.
[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, 1114, Oct. 2009.
[13] Lugini, L.; Marasco, E.; Cukic, B.; Gashi, I.: Interoperability in Fingerprint Recognition: a Large-Scale Study. Workshop on Reliability and Security Data Analysis (RSDA), Budapest, pp. 1–6, June 2013.
[14] 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.
[15] S. Modi, A. Mohan, B. Senjaya, and S. Elliott, ―Fingerprint recognition performance evaluation for mobile id applications, IEEE, 2010.
[16] A.K.Jain, S.Prabhakar, L.Hong, S.Pankanti, "Filter bank based Fingerprint Matching," IEEE Transactions on Image Processing, vol. 9, no. 5, May 2000.