IJITKM 0973-4414 Volume-9, Number-2 Jan-Jun 2016 pp. 21-25 **Impact Factor 2.8** available online at www.csjournalss.com

A Robust Approach for Biometric Security using Multibiometric System

Sonal , Dr. Pankaj Garg
Ph.D Scholar, Deptt. Of Computer Science, Uttarakhand Technical University, Dehradun, INDIA
Director, Dev Bhoomi Institute of Technology Dehradun
sonalkharb@gmail.com, hodpankajgarg@rediffmail.com

Abstract: Biometric system provides authentication to an individual by recognizing physiological or behavioral characteristics. Fingerprint is one of the most commonly used biometric for providing secure authentication, but nowadays spoofing has become an important issue to be taken into account. A fingerprint recognition system can be easily spoofed with the use of fake fingerprint of the legitimate user. But with the use of multiple instances, authentication level can be enhanced. Multi-Biometric System improves the capability of traditional biometric system. Here we have proposed a scheme by fusing different instances of a trait for raising the biometric system performance. The approach includes multiple instances of fingerprint at feature level fusion. The main purpose of the purposed scheme is to reduce the FAR (false acceptance rate), FRR (false reject rate) and total response time.
Keywords: Biometric Trait, Fingerprint, Fusion, Multiple Instances, Multi-biometric.

1. Introduction

Biometric system is regarded [1] as a technology to provide security using one's physiological traits (hand geometry, fingerprint, iris, retina, face, and palm print) and behavioral traits (signature, keystroke dynamics, gait pattern). The examples of different physiological and behavioral traits that are used in biometric system are shown in Fig1.

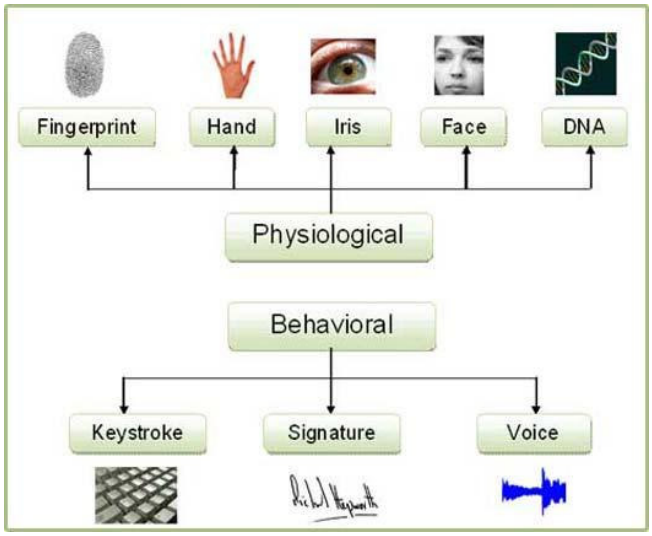

Fig1: Examples of Different Physiological and behavioral biometric traits

The main aim of the biometric system is to:

- Identify and verify an individual.
- Authenticate an individual to give appropriate rights to perform system operations.
- Keep the system safe and secure from unethical handling.

Traditional system provides authentication using single trait and is known as unibiometric system. As unibiometric system uses information about single biometric trait it has some drawbacks such as noisy data, inter and intra class variation, non universality, unacceptable error rates and spoof attacks. To overcome some of the limitations of traditional unibiometric system a multi-biometric system is designed.

A multi-biometric system can be categorized into one of the following:

- Multiple Sensors: Multiple sensors are used to capture a single biometric modality.
- Multiple Algorithms: In this a single biometric input can be processed by using different feature extraction algorithm for creating different information content.
- Multiple Instances: Multiple instances of a single biometric trait can be used.
- Multiple Samples: In this number of times same sensor can be used for acquiring the same biometric modality and instance.

The main aim of multi-biometric is to reduce one or more of the following:

- False Acceptance Rate (FAR)
- False Reject Rate (FRR)
- Failure to Enroll Rate (FTE)
- Susceptibility to Artifacts and Mimics

Reliability of multi-biometric system is more as compared to unibiometric system. Multi-biometric system includes two main drawbacks [2]:

1. Overall cost increases.
2. Verification time increases because comparison of information regarding multiple instances takes more time to provide verification.

Mainly there are four types of fusion techniques: sensor level fusion, feature level fusion, matching level fusion and decision level fusion. In biometric authentication system, second level of information fusion is feature level fusion. Feature level fusion occurs at feature extraction phase results in feature vectors which is a source of richest level of information as compared to the raw data captured through biometric sensors.

Less storage space is required to store feature vectors as compared to raw data captured from sensor. But feature vectors are of high dimensions and for storing feature vectors obtained from different modality more space is needed than storing a single modality. The total number of feature vectors originating from same feature extraction algorithm can be reduced by simple techniques like averaging or weighted averaging.

This paper presents an approach for combining the information provided by multiple instance of a biometric modality (fingerprint). The overall performance of the system is analyzed by integrating multiple instance of a fingerprint.

2. Related Work

The main motive to design a biometric system is to increase the success rate to provide authentication to an individual for that a system is designed that uses one's behavioral and physiological characteristics to provide the authentication.

2.1. Fingerprint extraction

There is necessity to enhance the fingerprint recognition as the quality of fingerprint images can degraded due to the presence of cuts and wounds and causes ridge discontinuities. Some of the techniques related to fingerprint enhancement are discussed [3] and Fast Fourier Transform is used for evaluating the performance. Feature of fingerprint were detected using the proposed smoothing algorithm [4].[5] Proposed minutiae based matching approach that considers the general minutiae distribution pattern between the two fingerprints. The proposed approach utilizes correlation scores between the local neighborhood areas and the edges that connect neighboring matched minutiae pairs. Here Boolean XOR function has been used for matching the fingerprints.[6] Fingerprint minutiae extraction algorithm has been proposed based on crossing number method for hardware implementation using FGPA devices. Here a simple fingerprint feature extraction algorithm is proposed and tested over PC and then this algorithm is implemented over FGPA devices. Their main aim is to develop and modify fingerprint feature extraction algorithm.

2.2. Feature level fusion

Fusion consists of different level of fusion techniques which are: sensor level fusion, feature level fusion, match score level fusion, rank level fusion and decision level fusion. Feature level fusion [7] is one which can be achieved by integrating the feature sets obtained from different sources and feature selection is performed on the obtained resultant vector.

In case of feature level fusion normalization [8] is done for obtaining the normalized score and then augmenting all the available normalized scores. Another technique [9] was proposed that deals in normalizing the feature vectors first and then NN classifier is used to select a candidate class having minimum distance as the class belonging to the testing sample. For multimodal biometric system the proposed [10] ensemble algorithm was used for feature level fusion. This fusion algorithm computes the normalized feature sets which were extracted individually from two traits of user and feature selection is done on the concatenation vector.

Image enhancement techniques [11] are used to preprocess the capture images. Curvelet Transform, Gabor Filter and Principal Component Analysis are used to extract the feature. Euclidean Distance is used to fuse the feature vectors which are matched later on. Feature extraction [12] is done based upon the high resolution fingerprint images. A new smoothing algorithm is used for efficiently detection of features of fingerprints. Ridges are determined with the help of eight different masks and a binary image of ridges is prepared from the grayscale fingerprint image.

3. Proposed Scheme

The proposed scheme integrates the multiple instances of fingerprints for getting faster response time and high reliability. The proposed method includes feature level fusion and mainly consists of two phase: enrollment phase and authentication phase.

Enrollment phase simply includes capturing multiple instances of fingerprints while enrolling with the system for first time. After that feature set of each instance is extracted separately by applying feature extraction. When feature sets of each instance get available then normalization (min-max) technique is applied to each separately and after it fusion process (simple sum rule) is applied to obtain fusion score as a

result. This fusion score is then stored in the retrievable database which can be used for authentication (verification/identification) purposes.

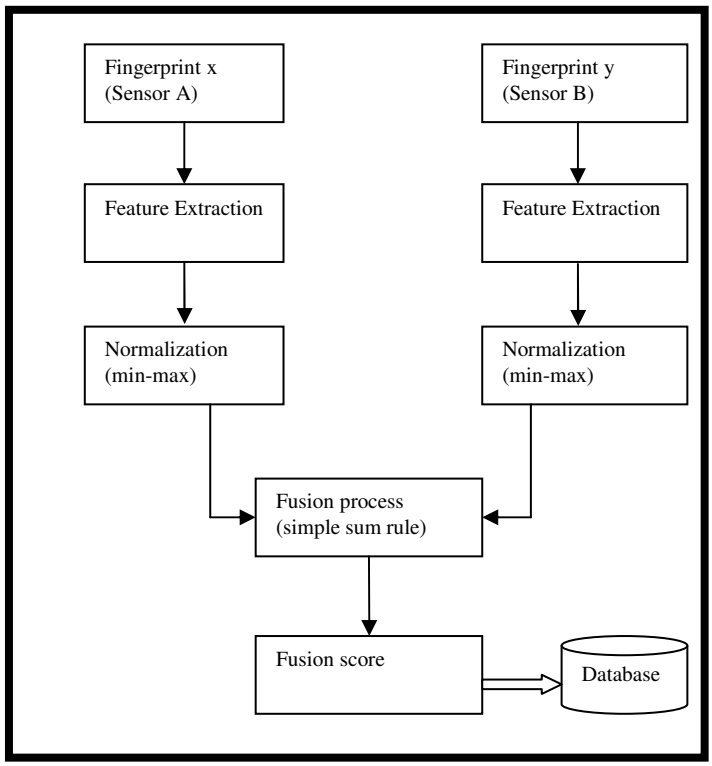

Fig 2: Enrollment process for multiple instances

Authentication phase in a similar way as incase of enrollment phase includes capturing of multiple instance of fingerprints using sensor. Feature extraction is applied to raw data which is available from sensor and feature set is obtained corresponding to each fingerprint instance. After that normalization (min-max) technique is applied to the individual feature set which in result produces the normalized score. Next is to apply the fusion process by using simple sum rule and fusion score is obtained. Now the obtained fusion score is compared with the existing database and correspondingly computes the match score. If the resulting match score is equal to or above the threshold value the user is accepted as genuine otherwise system will reject it and mark the user as fake user.

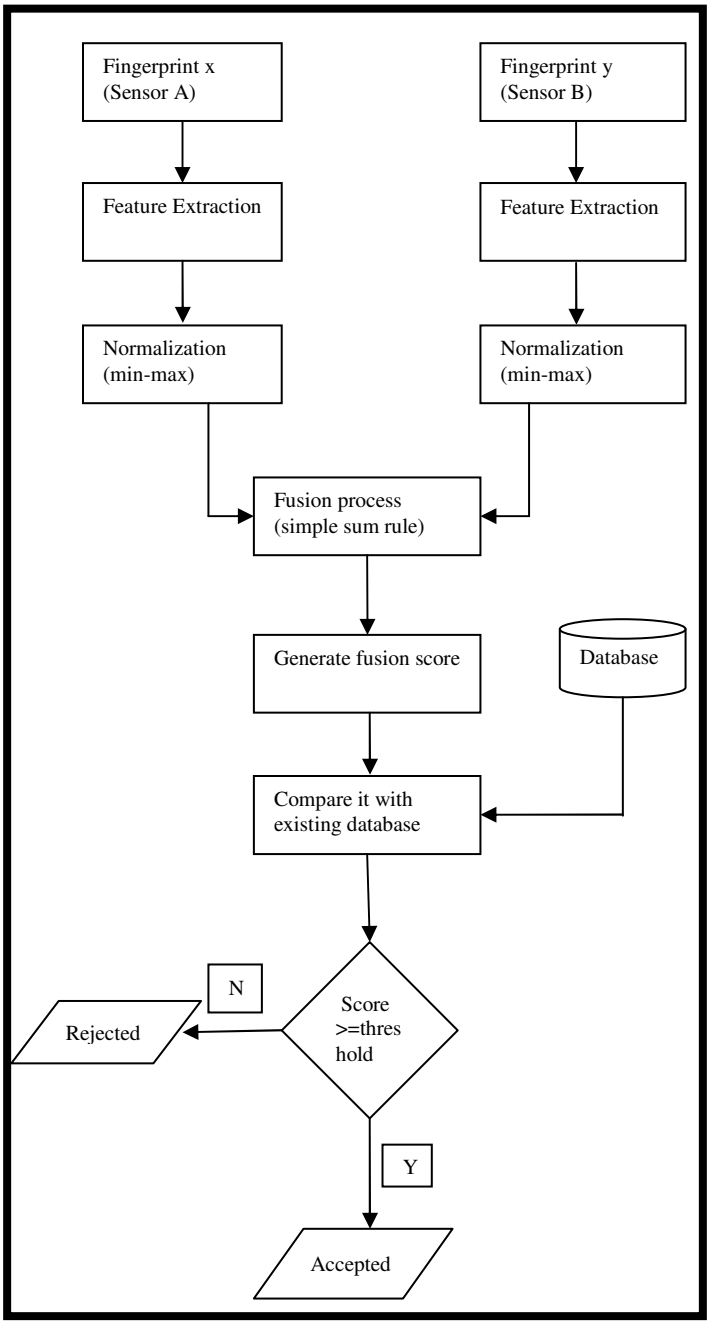

Fig 3: Authentication process for multiple instances

3.1 Algorithm for authentication in proposed scheme:

1. Capture fingerprint x from Sensor A
2. Capture fingerprint y from Sensor B
3. Extract fingerprint x feature set
4. Extract fingerprint y feature set
5. Separately apply normalization (min-max) on fingerprint x and fingerprint y
6. Apply feature level fusion process(simple sum rule) on normalized scores
7. Generate the fusion score
8. Compare the obtained fusion score with the existing database
9. If (score >= threshold)

10. User accepted
11. Else
12. Rejected
13. End

3.2 Advantages of the proposed scheme are:

1. Overall performance of the system is improved.
2. It improves the FAR (false acceptance rate) and FRR (false reject rate).
3. Less storage space is required as there multiple instance of same modality is taken.

4. 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. Fingerprint consists of minutiae points (bifurcation or ending points of ridges) that provide unique information about an individual. These minutiae points are extracted from the available data by applying feature extraction and the available feature set obtained in the form of minutiae points are used for further process.

5. Mathematical Formulas

Here normalization (min-max) technique and fusion process (simple sum rule) are used.

Min-Max normalization method is used to map the raw score in the range of [0, 1]. This method is used where there is lower and upper bound over the values of score.

Let, F denotes set of all scores; f denotes the raw sore from set F and N denotes the normalized score.

Then, the formula used to compute the normalized score using min-max normalization is:

$$N=\frac{f-\min(F)}{\max(F)-\min(F)}$$

For fusion process simple sum rule method is used. This method uses linear transformations for adding the score.

Then,

$$X= (a_1 x_1 - b_1) +\ldots. + (a_n x_n - b_n)$$

Where a_i and b_i are the weight and biased values which can be input as per the need of user.

6. Comparison of Proposed Scheme with Existing Technology

The proposed scheme presents a technique for authentication which uses the concept of multi-biometrics. But traditional method does not use the concept of multi-biometrics using multiple instances. Therefore, this method performs the feature extraction level fusion and hence is more reliable. The main advantage of the proposed scheme is that there is more compatibility between the taken multiple instances due to this less storage space is needed. It reduces the FAR, FRR and GAR and improves the performance of the system.

7. Conclusion & Future Scope

The proposed approach provides a more effective and reliable method of multibiometric authentication using multiple instances like here multiple instances of fingerprint are taken for providing secure authentication. The proposed scheme overcomes the flaws and limitations of traditional unibiometric system. This scheme reduces the FAR (false acceptance rate) and FRR (False reject rate). The use of multibiometric approach improves the overall performance of the system. In future, this approach can be implemented practically to provide high security using multibiometric system.

References

[1] B. Ulery, A. Hicklin, C. Watson, W. Fellner and P., "Hellinan Studies of Biometric Fusion," 2006.

[2] C. Kant, "A Multimodal Approach to Improve the Performance of Biometric System," *BIJIT-BVICAM's International Journal of Information Technology,* 2015.

[3] S. S. Patil, G. S. Chandel and R. Gupta, "Fingerprint Image Enhancement Techniques and Performance Evaluation of the SDG and FFT Fingerprint Enhancement Techniques," *International Journal of Computer Technology and Electronics Engineering(IJCTEE),* pp. 184-190, 2012.

[4] R. Kaur, P. Sandhu and A. Kamra, "A Novel Method for Fingerprint Feature Extraction," in *IEEE Conference 2010 on Networking and Information Technology*, 2010.

[5] P. Verma, Y. Bahendwar, A. Sahu, M. Dubey and P. Verma, "Feature Extraction Algorithm of Fingerprint Recognition," *International Journal of Advanced Research in Computer Science and*

Software Engineering, 2012.

[6] S. A. Sudir and R. T. Yuwono, "Adapatable Fingerprint Minutiae Based Algorithm Based on Crossing Number Method for Hardware Implementation using FGPA Devices," *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT),* 2012.

[7] A. R. a. R. Govindarajan, "Feature Level Fusion using Hand and Face Biometrics," in *Proceeding of SPIE Conference on Biometric Technology for Human Identification*.

[8] A. J. Jacob, N. T. Bhuvan and S. M. Thaampi, "Feature Level Fusion using Multiple Fingerprint," *International Journal on Computer Applications,Special Issue on Computational Science-New Dimensions & Perspectives,* pp. 13-18, 2011.

[9] Y. -F. Yao, X.-Y. Jing and H.-. S. Wong, "Face and Palmprint Feature Level Fusion for Single Sample Biometrics Recognition," *Journal on Neuro Computing,* pp. 1582-1586, 2007.

[10] S. Bhardwaj, "An Algorithm for Feature Level Fusion in Multimodal Biometric System," *International Journal of Advanced Research in Computer Engineering & Technology(IJARCET),* 2014.

[11] S. Inamdar and Y. Dandawate, "Fusion Based Multimodal Biometric Cryptosystem," in *2015 International Conference on Industrial Instrumentation and Control(ICIC)*, 2015.

[12] K. Singh, K. Kaur and A. Sardana, "Fingerprint Feature Extraction," *IJCST,* 2011.