International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 11 • Issue 1 pp. 78-82 Jan 2019-June 2019 www.csjournals.com

A Multi-Biometric System for Secure Fingerprint Recognition

[1]Dr. Anoop Sharma, [2]Rahul kaushal
Deptt. Of Computer Science, Sighania University, Rajasthan

Abstract: Biometric cryptosystems fuses the advantages of cryptography for example higher adaptable security levels and biometric for example disposal of dull errand of retaining the passwords or conveying the tokens. Notwithstanding validation, this framework is utilized for the assignment of encryption/decoding or information stowing away. The biometric key is produced from a biometric build utilizing cryptographic key extraction calculations. Single biometric cryptosystems are truly influenced by different assaults like Intrusion assault, work creep, and so forth and consequently numerous biometric characteristics are bound together to shape a Multi-biometric Cryptosystem. The risk of rupturing the security of the private information persuades the advancement of the information concealing methods in this paper. The proposed multi-biometric cryptosystem for the most part centers around two stage: 1) multi-biometric combination and 2) private layout security strategy. In this paper secure multibiometric framework for secure unique mark acknowledgment has been proposed.

Keywords: Authentication, Biometric Cryptosystem, Cryptographic key, Encryption/Decryption.

I. Introduction

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[1]. 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[2]. The main purpose of the purposed scheme is to reduce the FAR (false acceptance rate), FRR (false reject rate) and total response time.

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[3]. To overcome some of the limitations of traditional unibiometric system a multi-biometric system is designed.

II. Fingerprints Recognition:

Fingerprints are basically a texture patterns that consist of ridges and valleys that are present on the tip of finger. Mainly there are three basic patterns of fingerprint ridges that are arch, loop, and whorl on the basis of these pattern we can easily differentiate the identity and these are shown in Figure 1. with example as well[4-5].

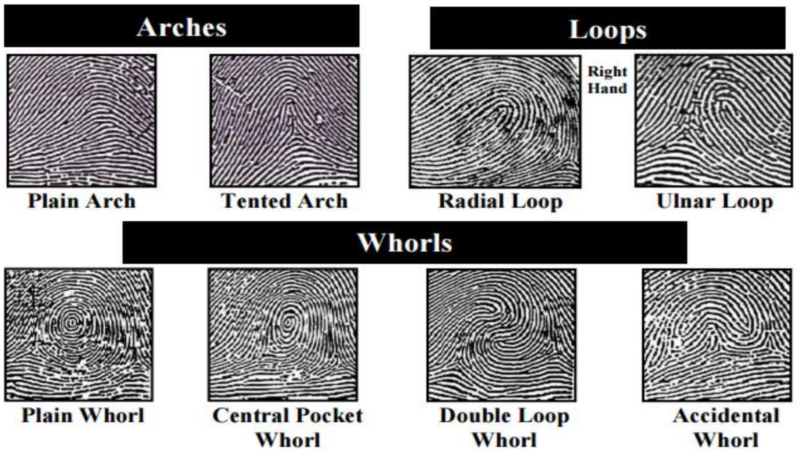

Figure .1 (a) Arch (b) Loop (c) Whorl

- Arch: In this pattern the ridge that runs along the fingertip and curves up in the middle. Where as in tented arches they have sharp spiked effect.
- Loop: Basically in a loop they have a stronger curve rather than arches and they enter and exist on the same side. Whereas Radial loops slant toward the thumb & ulnar loops loop away from the thumb impression.
- Whorl: an oval arrangement of ridge lines, often making a spiral pattern around a central point. Principal types are a plain whorl and a central pocket loop whorl, double loop whorl & finally Accidental whorl[6].

III. Architecture of 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[7-9].

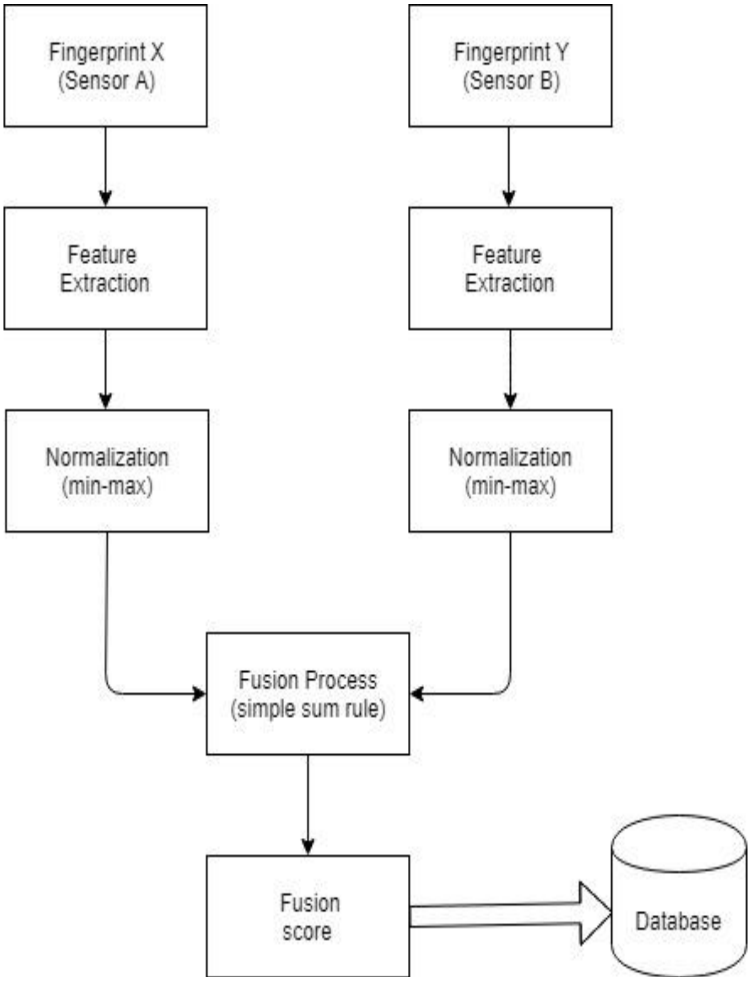

Figure .2 Enrollment process for multiple instances

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.

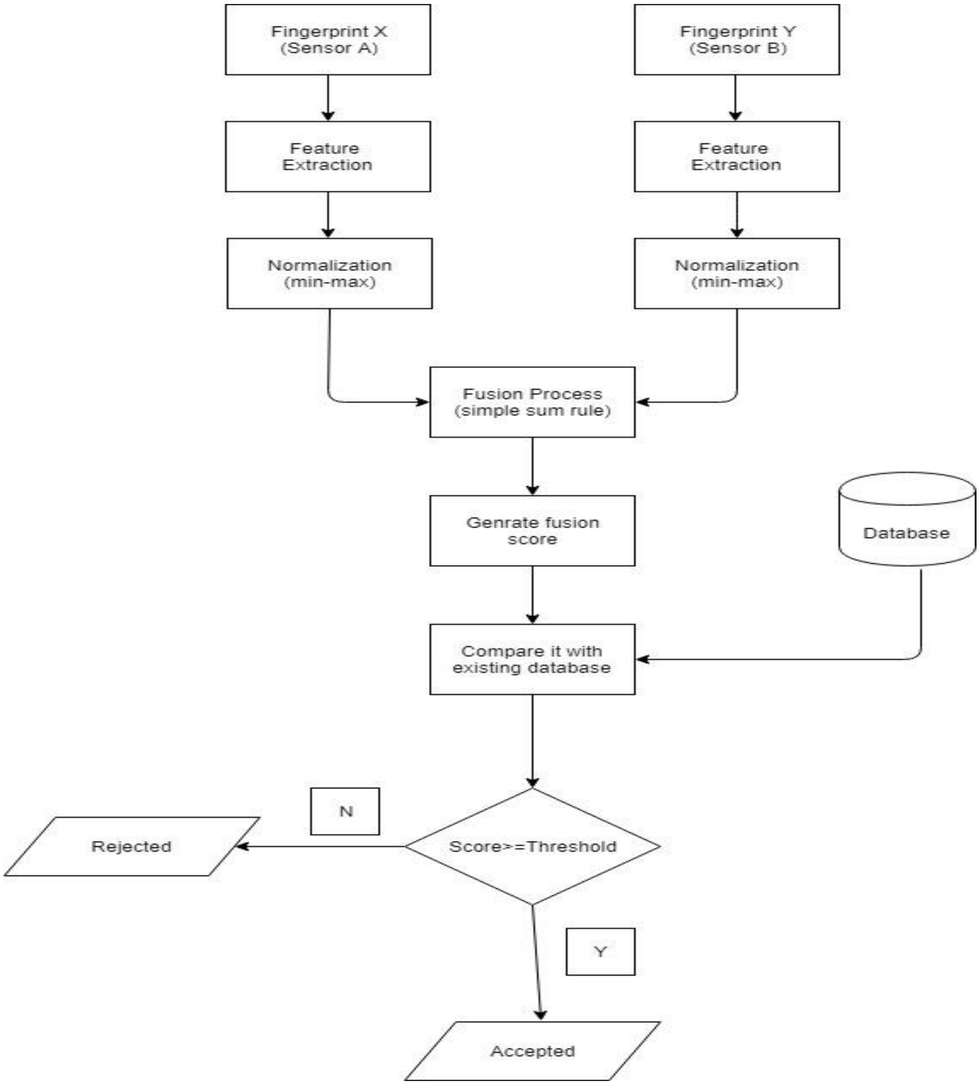

Figure 3 Authentication process for multiple instances

IV. Proposed scheme Algorithm:

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

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.

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[10].

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,

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

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

V. 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[11-12].

VI. Conclusion

Multiple instances of fingerprint have been used to overcome the problem of traditional biometric system. The main purpose of the purposed scheme is to reduce the FAR (false acceptance rate), FRR (false reject rate) and total response time. The next chapter discuss about enhancing security using feature level fusion of face and iris.

References

[1] A. Jain and K. Nandakumar, "Biometric Authentication: System Security and User Privacy," IEEE computer society, vol. 45, no. 11, Nov. 2012.

[2] W. Deffie, M. E. Hellman, "New direction in cryptography," IEEE transcation on information theory, vol. 22, no. 6, Nov. 1976.

[3] Uludag, U.; Pankanti, S.; Prabhakar, S.; Jain, A.K., "Biometric cryptosystems: issues and challenges," in Proceedings of the IEEE, vol. 92, no. 6, June 2004.

[4] Christina-Angeliki Toli,Bart Preneel, "A Survey on Multimodal Biometrics and the protection of their templates," Privacy and Identity Management for the Future Internet in the Age of Globalisation, Springer, Sep. 2014.

[5] Devi, T.R., "Importance of Cryptography in Network Security," International Conference on Communication Systems and Network Technologies (CSNT), Apr. 2013.

[6] Y.J. Chin, T.S. Ong, A.B.J. Teoh, K.O.M. Goh, " Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion," Journal on Information Fusion, Elsevier, vol. 18, July. 2014.

[7] Christian Rathgeb,Andreas Uhl, "A survey on biometric cryptosystems and cancelable biometrics," Journal on Information Security ,Springer International Publishing, Jan 2011.

[8] Bo Fu; Yang, Simon X.; Jianping Li; Dekun Hu, "Multibiometric Cryptosystem: Model Structure and Performance Analysis," IEEE Transactions on Information Forensics and Security, vol. 4, no. 4, Dec. 2009.

[9] Nagar, A.; Nandakumar, K.; Jain, A.K., "Multibiometric Cryptosystems Based on Feature-Level Fusion," IEEE Transactions on Information Forensics and Security, vol. 7, no. 1, Feb. 2012.

[10] Cai Li; Jiankun Hu; Pieprzyk, J.; Susilo, W., "A New BiocryptosystemOriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion," IEEE Transactions on Information Forensics and Security, 2015.

[11] P. Wild, P. Radu, L. Chen and J. Ferryman, "Towards anomaly detection for increased security in multibiometric systems: Spoofing-resistant 1median fusion eliminating outliers," IEEE International Joint Conference on Biometrics (IJCB), Sep. 2014.

[12] Ning Wang; Qiong Li; El-Latif, A.A.A.; Xuehu Yan; Xiamu Niu,, "A Novel Hybrid Multibiometrics Based on the Fusion of Dual Iris, Visible and Thermal Face Images," International Symposium on Biometrics and Security Technologies (ISBAST), July 2013.