IJITKM 0973-4414 Volume-10, Number-2 Jan-June 2017 pp. 77-80 available online at www.csjournals.com

Multimodal Biometrics Techniques: A Review

Balwan Singh
balwanbana@gmail.com

Abstract: Multimodal Biometric System is used to enhance the capability of traditional biometric system. Unimodal system is the one where single modality (physiological or behavioral) is used for providing authentication to an individual. Unimodal system includes some limitations like noisy data, non-universality, inter and intra class variations etc. which have worst effect over performance and accuracy of the system. Multimodal system is designed to overcome some of the drawbacks of unimodal system to enhance the performance and accuracy. Multimodal Biometric is one where two or more modalities are fused using different fusion techniques resulting in high performance and accuracy.
Keywords: Authentication, Biometric Trait, Fusion, Multimodal.

I. INTRODUCTION

IN today's world security has become an important issue to deal with, so one of the best solution is use of biometric technologies. Authentication is an important part of security. Biometrics deals in securing data through authentication on the basis of identification and verification. Traditionally, unimodal biometric system was in use which identifies an individual on the basis of single trait (can be physiological or behavioural). Unimodal suffer from following limitations:

A. Noisy data: - susceptibleness of biometric sensors to noise results in inaccurate matching, as noisy knowledge might result in false rejection.

B. Intra class variation: - The biometric knowledge noninheritable throughout verification won't be identical to the information used for generating model throughout enrollment for a personal. This is often best-known as intra-class variation. Giant intra-class variations increase the False Rejection Rate (FRR) of a biometric system.

C. Interclass similarities: - Inter-class similarity refers to the overlap of feature areas corresponding to multiple people. Giant Inter-class similarities increase the False Acceptance Rate (FAR) of a biometric system.

D. Non universality: -Some persons cannot offer the specified standalone biometric, owing to health problem or disabilities [5].

E. Spoofing: - Unimodal biometric is susceptible to spoofing wherever the information will be imitated or forged.

Multimodal biometrics is an enhancement over unimodal system as it overcomes limitation of unimodal system. Multimodal biometrics system provides authentication by combining two or more different traits of an individual providing secure means to protect data [1]. Multimodal biometrics is based upon the fusion techniques which are applied to different levels of multimodal biometric system. As multimodal biometric system provides authentication using two or more modalities of an individual make it difficult for an intruder to spoof it thus provides high reliability and accuracy rates [2].

II. MULTIMODAL BIOMETRIC

Multimodal Biometrics System is one that uses information from multiple modalities (multiple cues) to authenticate an individual. Traditionally, unimodal biometric system is used that provides security using single biometric trait and includes variety of limitations such as noisy data, non-universality, inter class variation and spoof attacks. Multimodal biometrics is one of the advancement over unimodal biometrics in the field of biometrics security. Multimodal Biometrics System has several advantages such as lower error rates and larger population coverage as compared to unimodal biometric system. In addition, a multimodal biometric system is more difficult to spoof attack rather a unimodal biometric system yet it also increases the complexity of system.

Multimodal biometric operates mainly in two phases one is enrollment phase and other is authentication phase which are describe as follows:

A. Enrollment Phase: In enrollment phase biometric characteristics (whether physiological or behavioural) are captured and stored in the retrievable database in the form of a template and further used for identification and verification in the authentication phase.

B. Authentication Phase: Authentication phase deals in verifying or identifying an individual on the basis of captured trait. Identification (one-to-many matching) involves comparing the captured trait with templates corresponding to all users templates in the template database. Verification (one-to-one) involves comparing captured trait corresponding to the template of claimed identity [3].

III. MULTIMODAL BIOMETRIC SYSTEM MODULE

Biometrics is defined as that part of science and technology that deals in identification and verification of an individual on the basis of behavioral and physiological characteristics.

Multimodal Biometric system combines two or more modalities of an individual like fingerprint, iris, palmprint, handgeometry, face, signature etc. and uses fusion techniques for better accuracy and reliability.

Multimodal biometric system consists of four modules which are shown in Figure2 and are as follow:

A. Sensor module: This module is one in which sensor is used to acquire biometric trait of user. For example: fingerprint sensor which is used to capture the fingerprint of an individual.

B. *Feature Extraction Module:* Here important features are extracted from the acquired data. For example: minute points of fingerprint can be extracted.

C. *Fusion Module:* This module fuses two or more biometric traits extracted from different biometric modalities. Fusion can takes place at sensor level, feature extraction level, at matching level or decision level.

D. *Matching and Decision Making Module:* In matching module extracted features are compared with the templates stored in the database based upon which acceptance and rejection is done in case of decision module [4].

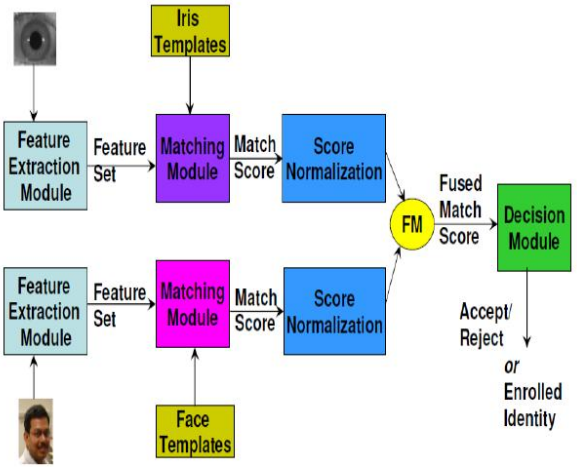

Figure2: Different biometrics system modules [5]

IV. MULTIMODAL BIOMETRICS TECHNOLOGIES

Multimodal biometric offers supplementary data between completely different modalities that will increase recognition performance in term of accuracy and skill to beat the drawbacks of unimodal biometric. Multimodal biometric person authentication systems combine multiple authentication techniques, and area unit necessary for several security applications like government, police investigation etc.

Some existing multimodal biometric technologies are:

A. *Palmprint and Fingerprint:* The independent score of palmprint and fingerprint are combined at feature level. Gabor filtering is used to extract the features. The average verification accuracy obtained is 87% when only 250 features are used which is higher than 76% when only palmprint images are used [6].

B. Face and Fingerprint: Features of face and fingerprint are combined using Neural Network. Principal component Analysis (PCA) and Multilayer perception based face and fingerprint recognition system is used to improve the accuracy and performance [7].

C. Face and Fingervein Biometric Authentication: Multilevel score fusion of face and finger vein is performed to increase the accuracy. Fuzzy fusion is used for combining imposter and genuine score [8].

D. *Palmprint, Handgeometry and Knuckle print:* The individual feature of palmprint, handgeometry and knuckle print are integrated to improve the accuracy of hand based verification. For it there is no need of using two different sensors as the palmprint, handgeometry and knuckle print can be acquired from the same image at same instance of time. Dynamic fusion approach is used to combine the individual match score [9].

E. *Face, Ear and Iris Modalities:* Authentication is provided fusing face, ear and iris modalities features. Principal component analysis based neural network classifier is used to extract the feature from the acquired face and ear image and hamming distance is used for calculating iris templates on fusing all the modalities better result are obtained [10].

F. *Face and Ear Modalities:* Person identification is done using face and ear biometric modalities. PCA based neural network classifier is used to extract the feature from the images. Eigen faces, Eigen ears and their features are used for providing authentication [11].

G. *Fingerprint and iris with fuzzy logic:* The proposed multimodal biometric system uses the two unimodal biometrics modalities (fingerprint and iris) to improve the recognition accuracy. Decision level fusion is performed over the extracted features and fuzzy logic is used for better biometric result combination [12].

V. DIFFERENT TYPES OF FUSION LEVELS IN MULTIMODAL BIOMETRICS

As multimodal biometrics deals in using different biometric modalities the system has to integrate the features of these modalities from acquired data. Its main motive is to enhance the identification and authentication of an individual [13]. Fusion may be a promising approach which will increase the accuracy of systems. Though fusion will increase accuracy, it usually will increase computation prices and template sizes and reduces user acceptance. The fusion can be done at different stages of multimodal biometric system which are classified as sensor level fusion, feature level fusion, matching score level fusion and decision level fusion. In figure2- different fusion levels of multimodal biometrics are shown [2].

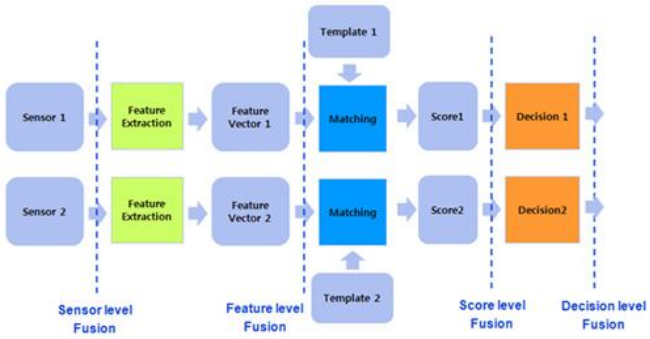

Figure2: Different types of fusion levels in multimodal biometrics

A. *Sensor Level Fusion:* In case of sensor level fusion the combination of different biometric traits takes place which are acquired using different sensors like fingerprint or palmprint scanner, iris or face scanner, video camera etc.

B. *Feature Level Fusion:* Feature level fusion is one where acquired biometric data coming from different sensors are preprocessed and extraction of important feature takes place accordingly particular fusion algorithm is used to form a composite set of features [14].

C. *Matching Score Level Fusion:* At this level the extracted features are compared with the templates stored in the database based upon which different scores are obtained which are combined and used for classification.

D. *Decision Level Fusion:* At this level each acquired traits are separately classified and acceptance or rejection is done based upon the score obtained at the matching score level fusion.

VI. SCORE NORMALIZATION

Score normalization is used to address the problem of incomparable classifier output score. Matching score generated by different matchers are converted into a common domain and can be combined later on [15].

Let X denotes the set of all scores, x denotes a raw matcher score from the set x and N denotes the normalized score.

A. *Min-Max Score Normalization: In* this method raw scores are mapped to the [0, 1] range. Max(x) and Min(x) denotes the end points of the score range.

$$N = \frac{\mathrm{X} - \mathrm{Min(x)}}{\mathrm{Max(x)} - \mathrm{Min(x)}}$$

B. *Z-Score Normalization:* This is a score transformation method which transforms scores to a distribution with mean of 0 and standard deviation of 1.

$$N = \frac{\mathrm{X} - \mathrm{Mean(x)}}{\mathrm{Std(x)}}$$

C. *Tanh-estimators Normalization:* This method also called robust statistical technique. It maps the scores to the range of (0, 1).

$$\mathrm{N}=\frac{1}{2}\left[tanh\left[0.01\left(\frac{X-Mean(x)}{Std(x)}\right)\right]+1\right]$$

D. *Decimal Scaling Normalization:* This method is applied to the scores obtained from different matchers are on logarithmic scale.

$$N = \frac{\mathrm{X}}{10\text{^ n}}$$

VII. MUBITOOL

MUBI is a tool for analyzing biometric system. Only single biometric system can be analyze at a time. Each system consists of number of biometric devices. For adding a device to the project two text files containing genuine and imposter scores are needed. After it devices are added to the project and all information regarding devices is saved in a single binary file. So, MUBITOOL provides an environment for analyzing the results.

VIII. CONCLUSION

Biometrics is a way to provide security to your data based upon the physiological and behavioural characteristics of an individual. To overcome the difficulties arises in case of unimodal biometrics (single trait authentication) idea of multimodal biometric system is adopted to improve authentication process. Multimodal biometric is much efficient and reliable way of securing data as it uses and combine different modalities of an individual to provide reliable authentication or identification. In case of multimodal biometric fusion takes place at different levels results in providing higher accuracy and scalability. Authentication can be enhanced using fusion techniques. It is very important and helpful method for security purpose or controls the criminal offences. Biometric is a stronger method of authentication and verification.

REFERENCES

[1]G.Bhowate, Ms.Priya N.Ghotkar and Prof.Vikas, "Multimodal Biometric System-A Review," *International Engineering Journal for Research and Developement*, vol. 1, no. 1.

[2] N. Aravalli, "Automatic System For Person Authentication by Multimodal Biometrics-A survey," *International Journal of Emerging Technology in Computer Science and Electronics*, vol. 4, no. 2, 2015.

[3] A. Ross and A. Jain, "Information Fusion in Biometrics," *Journal of Pattern Recognition Letters*, vol. 24, pp. 2115-2125, 2003.

[4]K. S. and Y. Bansal, "Concept of Unimodal and Multimodal Biometric System," *International Journal of advanced Research in Computer Science and Software Engineering*, vol. 4, no. 6, 2014.

[5] R.Divya and V.Vijayalakshmi," Analysis of Multimodal Biometric Fusion Based Authentication Techniques for Network Security," *International Journal of Security and Its Applications*,Vol. 9, no. 4 , pp. 239-246,2015.

[6] Mitul D Dhameliya and Jitendra P Chaudhari, " A Multimodal Biometric Recognition System based on Fusion of Palmprint and Fingerprint,"*International Journals of Trend and Technology*,vol. 4,no. 5,2013.

[7] Praveen Kumar Nayak and Devesh Narayan," Multimodal Biometric Face and Fingerprint Recognition Using Neural Network," *International Journal of Engineering Research & Technology (IJERT),* Vol. 1, no.10, 2012.
[8] Muhammad Imran Razzak, Rubiyah Yusof and Marzuki Khalid," Multimodal face and finger veins biometric authentication," *Scientific Research and Essays* Vol. 5(17), pp. 2529-2534, 2010.
[9] Ruth Karunya S and Veluchamy S**.,"** Contactless Hand Based Multimodal Biometrics Identification System,**"** *Research Journal of Engineering Sciences* ,ISSN 2278 – 9472, Vol. 2(3)**,** 6-10, 2013.
[10] Snehlata Barde, A S Zadgaonkar and G R Sinha," Multimodal Biometrics using Face, Ear and Iris modalities," *International Journal of Computer Applications (0975 – 8887)Recent Advances in Information Technology,* 2014.
[11] Snehlata Barde, A.S. Zadgaonkar and G.R. Sinha, "PCA based Multimodal Biometrics using Ear and Face Modalities," *I.J. Information Technology and Computer Science***,** 05, 43-49, 2014.
[12] Mohamad Abdolahi, Majid Mohamadi and Mehdi Jafari,"Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic," *International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307***,** Volume-2, Issue-6, January 2013.
[13]L. Kibona, "Face Recognition as a Biometric Security for Secondary Password for ATM users," *IJSRST*, vol. 1, no. 2, 2015.
[14]N. Geethanjali ,K.Thamaraiselvi et al, "Feature Level Fusion of Multimodal Biometrics and Two Tier Security in ATM System," *International Journal of Computer Applications,* vol. 70, 2013.
[15] Eugen LUPU Petre G. POP," MULTIMODAL BIOMETRIC SYSTEMS OVERVIEW," *ACTA TECHNICA NAPOCENSIS Electronics and Telecommunications*, Vol. 49, no. 3, 2008