Multimodal Biometrics Security: A Review

[1]Ms. Pooja Saini, [2]Prof. Priyanka Rao

[1]Research Scholar, [2]Assistant Professor
G H Raisoni College of Engineering & Management, Pune

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 system's accuracy. Multimodal biometric 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[1]

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: -Biometric sensors are used to match noise feature as it results in inaccurate matching then it outputs false rejection.

B. Intra class variation: -In verification phase, the biometric knowledge of noninheritable won't be indistinguishable to the information that is secondhand for producing model during matriculation phase. This is often best identified as intra class dissimilarity. Giant intra class dissimilarities upsurge False Rebuff Rate of a biometric organization.

C. Inter class comparisons: - If the topographies of numerous persons intersection then it denotes to Inter class comparison. Giant Inter-class comparisons growths the False Reception Rate of a biometric organization.

D. Non universality: -The individual taking health problematic and infirmities [5] incapable to offer the quantified impartial biometric arrangement.

E. Spoofing: - Unimodal biometric is susceptible to spoofing wherever the information will be 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 data having noise disturbance, 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 merits like low error rates and covers huge population as compared to unimodal biometric system.It is more difficult to spoof attack in a multimodal biometric rather a unimodal biometric yet complexity of system increases.

Multimodal biometric operates mainly two phases which are defined as shadows:

A. Enrollment Stage: In this stage 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 biometric traits with the biometric templates that are stored in record. Corroboration (one-to-one) involves associating apprehended trait with the master of requested uniqueness [3] or being.

III. MULTIMODAL BIOMETRIC SYSTEM MODULE

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

Two or more modalities of an individual like fingerprint, iris, palmprint, handgeometry, face, signature etc. combines in multimodal biometric system.It also 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 Abstraction Component:* Here imperative landscapes are mined from the learned data. For example: tiny points of impression 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 Conclusion Making Unit:* In matching component removed landscapes are associated with the masters stored in the record grounded upon which taking and denial is done in case of conclusion element [4].

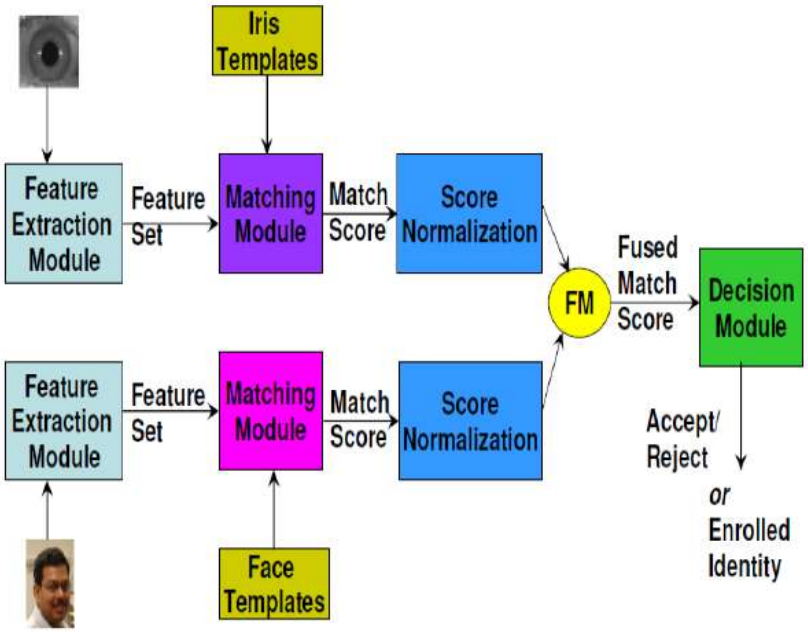

Figure2: Different biometrics system modules [5]

IV. MULTIMODAL BIOMETRICS TECHNOLOGIES

Some existing multimodal biometric technologies are:

Palmprint and Impression: The independent score of palm print and impression are pooled at mouth level. Gabor cleaning 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].

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

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

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].

Face, Ear and Iris Modalities: In this authentication is provided by using appearance, ear, and iris modalities landscapes. Principal module analysis (PCA) based neural system classifier is used to cutting the mouth from the acquired face and ear image.The hamming distance technique is used for calculating iris templates by fusing all the modalitiesand we obtained the better result [10].

Face and Ear Modalities: Person identification can be done by using expression and earlobe biometric modalities. We can practice PCA grounded neural system classifier to quotation the nose from the descriptions. Eigen faces and ears features are used for providing authentication [11].

A. *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 for the 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 increases prices of computation, sizes of template and reduces user acceptance. The fusion can be done at different stages of multimodal biometric system which are as follows as instrument smooth combination, mouth smooth combination, and corresponding score adjacent combination and conclusion level combination. In figure2- dissimilar combination levels of multimodal biometrics are shown [2].

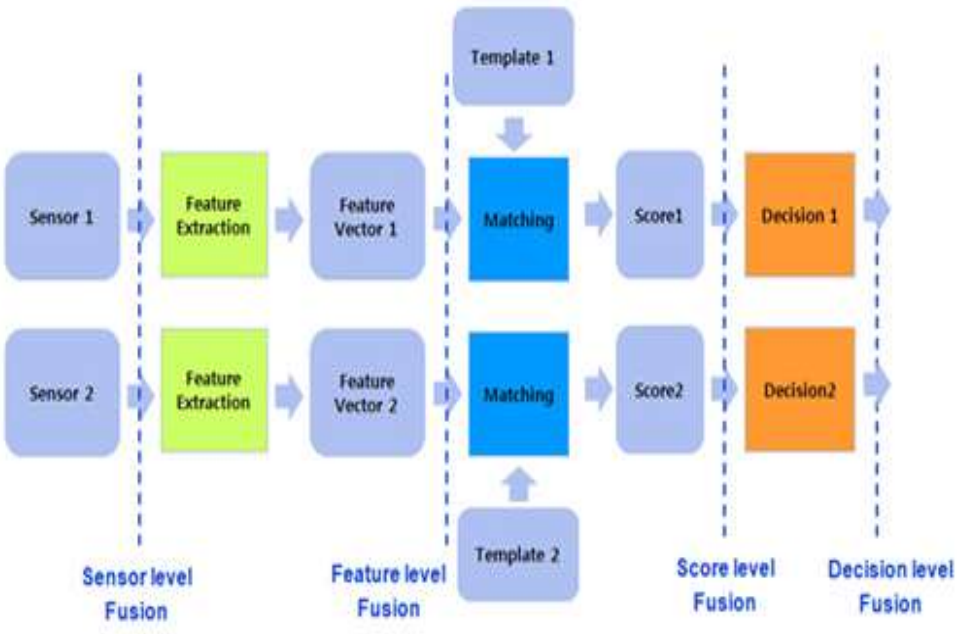

Figure2: Different types of fusion levels in multimodal biometrics

A. *Sensor Glassy Combination:* In case of sensor glassy combination the combination of different personalities of biometric takes place which are acquired using different sensors like fingerprint or palm print scanner, iris or face scanner, video camera etc.
B. *Feature Level Fusion:*This is the one where acquired biometric data arises from different type of sensors are processed early 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 we compared the templates that stored in database with the extracted features.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] assortment. Max(x) & Min(x) signifies the end opinions of the groove variety.

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

B. *Z-Score Regularization:* This is a score conversion process which transmutes scores to a circulation with unkind of 0 and average unconventionality of 1.

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

C. *Tanh-estimators Normalization:* This method is known as Robust Statistical technique. The score maps to the range of (0, 1) with this method.

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

D. *Decimal Mounting Regularization:* This technique is functional to the scores gotten from diverse matchers are on logarithmic gauge.

$$N=\frac{\mathrm{X}}{10\hat{}\ \mathrm{n}}$$

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 unimodal biometrics (single trait authentication), the idea of multimodal biometric approach is adopted to improve authentication process. It 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. Pramila, Reena, Collective Bargaining: A Concept, International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences (IJIRMPS), Volume 6, Issue 4, July-August 2018, ISSN: 2349-7300 (Available at http://www.ijirmps.org/research-paper.php?id=168)
4. A. Ross and A. Jain, "Information Fusion in Biometrics," *Journal of Pattern Recognition Letters,* vol. 24, pp. 2115-2125, 2003.
5. 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.
6. Rohit kumar, Sorab kumar, Hybrid Approach for Image security by the use of DWT and SLT, International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences (IJIRMPS), Volume 6, Issue 4, July-August 2018, ISSN: 2349-7300 (Available at http://www.ijirmps.org/research-paper.php?id=191)
7. 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.
8. 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.
9. S.KANNADHASAN, M.SARAVANAPANDI, C.GURUNATHAN, Switching Strategies Based Cascaded Multilevel Inverters Using Modulation Techniques, International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences (IJIRMPS), Volume 6, Issue 4, July-August 2018, ISSN: 2349-7300 (Available at http://www.ijirmps.org/research-paper.php?id=186)
10. 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.
11. 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.
12. 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.
13. BHARGAV S, Dr. H. N. Jagannatha Reddy, STRENGTHENING OF TWO WAY RC SLAB USING POLYPROPYLENE FABRIC, International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences (IJIRMPS), Volume 6, Issue 4, July-August 2018, ISSN: 2349-7300 (Available at http://www.ijirmps.org/research-paper.php?id=158)
14. 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.

15. 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.
16. 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.
17. Neeraj Agarwal, Nikhil Garg, A RESEARCH ON GREEN CONCRETE, International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences (IJIRMPS), Volume 6, Issue 4, July-August 2018, ISSN: 2349-7300 (Available at http://www.ijirmps.org/research-paper.php?id=172)
18. L. Kibona, "Face Recognition as a Biometric Security for Secondary Password for ATM users," *IJSRST*, vol. 1, no. 2, 2015.
19. 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.
20. Eugen LUPU Petre G. POP," MULTIMODAL BIOMETRIC SYSTEMS OVERVIEW," *ACTA TECHNICA NAPOCENSIS Electronics and Telecommunications*, Vol. 49, no. 3, 2008