A SURVEY ON MULTIMODAL BIOMETRICS

1. Nabila Kazmi
M.Tech Student, Department of CSE, Integral University, Lucknow, India
2. Dr. Faiyaz Ahmad
Assistant Professor, Department of CSE, Integral University, Lucknow, India

Abstract
A biometric system based entirely on one biometric trait is often not able to meet the desired performance requirements. Identification based on multiple biometric traits represents an emerging trend.Physical traits like fingerprints, face, iris and so on depend on physical characteristics which are by and large inborn and stable. Behavioral traits like voice, gait, signature or keystroke and so then again is a quantifiable characteristic. Unimodal (simple) biometric systems created for each of these biometric features may not generally meet the required performance and security measures. The current research uncovers that multimodal biometric system is more viable in authentication as compared to unimodal biometric. The goal of this paper is to glance at the significance of the utilization of multimodal biometrics in the area of secure individual confirmation. This paper gives an alternate acumen to utilize biometrics as a largest amount of system security with the fusion of numerous biometrics modalities.

1. **Introduction:** The procedure by which a person's identity can be authenticated by applying the biological trait i.e. physical and behavioral traits is called Biometric. A biometric system measures at least one physical or behavioral attributes including unique fingerprint, palm print, face, iris, retina, ear, voice, signature, gait, hand-vein data of an individual to decide or check his identity[1]. These qualities are hinted by various terms, for example, traits, indicators, identifiers, or modalities.

2. Multimodal Biometric

Multimodal biometric is a system that merges the obtained result from more than one biometric traits for the purpose of individual identification. Multimodal biometric systems are more reliable than unimodal biometric system because many independent biometric modalities are used in it. The use of multimodal biometric system may result highly accurate and secure biometric identification system, as unimodal (simple) biometric system may not provide high accurate identification due to non-universality. Such as, a few proportions of individuals can have cut, worn or unrecognizable prints, fingerprint biometric may produce improper results. The failure in multimodal biometric systems of any one trait may not affect seriously the individual identification as different technologies as well as different traits can be successfully employed. Hence the spoofing can extremely be minimized; thus improving the efficiency of the overall system. The four common modules in any biometric system - sensor module, feature extraction module, matching module and decision making module are described below.

2.1 Sensor Module

In this module, the raw data of the user is measured by using the biometric sensor or scanner. This raw biometric data is converted into a permanent form for later use and then it is sent to the next module for feature extraction. The various factors like size and cost are impacted by the design of the sensor module of the biometric system.

2.2 Feature Extraction Module

In this module, the raw data transferred from the sensor module and accordingly generation of a synoptic but indicative digital representation of the underlying traits or modalities took place. After extracting the biometric features it is given as an input to the matching module for further comparison.

2.3 Matching Module

In this module, the extracted features are compared with the existing templates in the database and generate a match score. This match score can be controlled by the quality of the given biometric data. The matching module also summarized a decision making module in which the generated match score is used for validating the claimed identity.

2.4 Decision Making Module

Decision making module identifies whether the user is a genuine user or an impostor based on the match scores. These are used to either validate the identity of an individual or provides a ranking of the enrolled identities for identifying an individual[2]. A simple block diagram for multimodal biometric system is shown in fig 1.

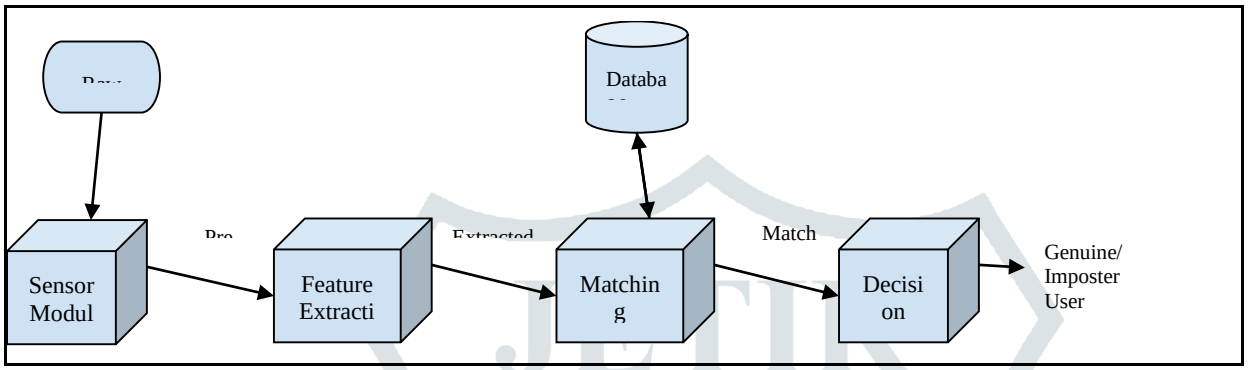

Fig 1. Block Diagram of Modules in Biometrics

3. Types of Multimodal Biometric:

Based on the traits, sensors and feature sets many different types of multimodal systems are there:

3.1 Single biometric trait, multiple sensors: Multiple sensors are used to record the same biometric characteristic. The raw data taken from different sensors can then be combined at the feature level or matcher score level to improve the performance of the system.

3.2 Multiple biometrics: Multiple biometric traits such as fingerprints and face can be combined. Different sensors are used for each biometric characteristic. The interdependency of the traits ensures a significant improvement in the performance of the system. A commercial product BioID [3] uses voice, lip motion and face of a user to verify identity.

3.3 Multiple units, single biometric traits: Two or more fingers of a single user can be used as a biometric trait. It is an inexpensive way of improving system performance, as it doesn't require multiple sensors or incorporating additional feature extraction or matching modules. Iris can also be included in this category.

3.4 Multiple snapshots of single biometric: In this, more than one instance of the same biometric is used for the recognition. For e.g. multiple impressions of the same finger or multiple samples of the voice[4]. Multiple matching algorithms for the same biometric: In it different methods can be applied to feature extraction and matching of the biometric characteristic.

4. Level Of Fusion:

The information of the multimodal system can be fused at any of the four modules:

4.1 Fusion at the sensor level: In this level, the raw data from different sensors are fused. In this fusion, we can either use samples of the same biometric trait obtained from multiple compatible sensors or multiple data of the same biometric trait obtained using a single sensor. In it, the data is fused at a very early stage so it has all information as compared to other fusion levels. In this fusion very less work has been done in this area till now.

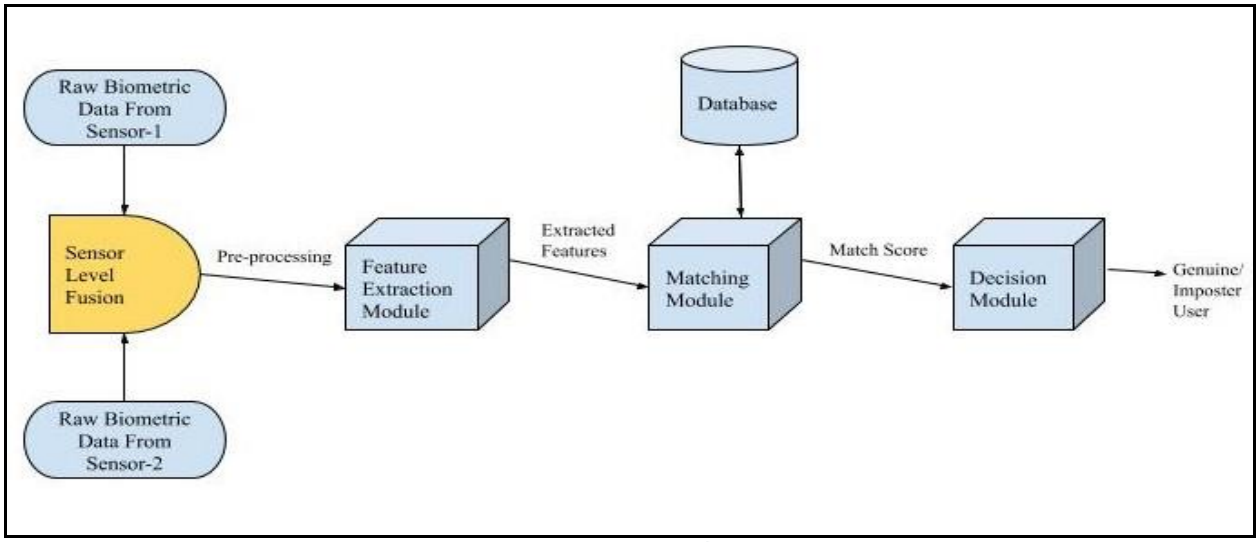

Fig 2. Sensor level Fusion

4.2 Fusion at the Feature Extraction Level: The data or the feature set originating from multiple sensors or sources are fused together. Features extracted from each sensor form a feature vector. These feature vectors are then concatenated to form a single new vector[5][6]. In feature level fusion, the same feature extraction algorithm or different feature extraction algorithm on multiple modalities can be used. This level of fusion is challenging because relationship between features is unknown and structurally incompatible features are common in the curse of dimensionality. Because of these difficulties, limited work is reported on feature level fusion of multimodal biometric system.

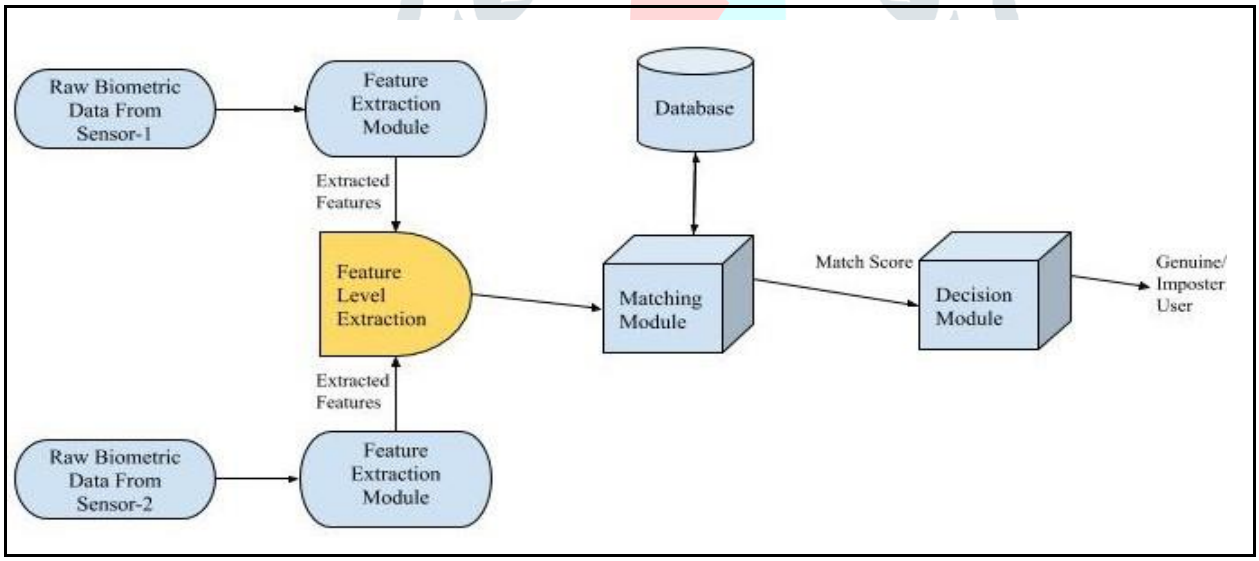

Fig 3. Feature Level Fusion

4.3 Fusion at Matcher Score Level: Each system provides a matching score indicating the proximity of the feature vector with the template vector. These scores can be combined to assert the veracity of the claimed identity[7]. The scores that are obtained from different matchers are not identical, score normalization technique is adapted to map the scores obtained from different matchers on to a same range. These scores contain the wealthy information about the input. Also it is quite easy to combine the scores of different biometrics so lot of work has been done in this field.

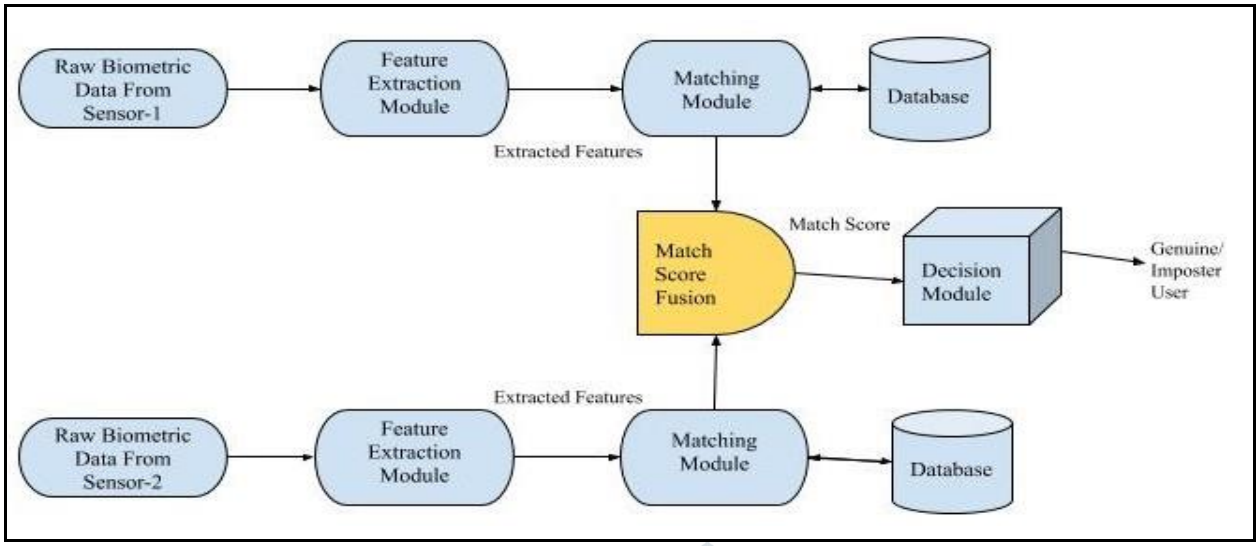

Fig 4. Matching Score Level Fusion

4.4 Fusion at the Decision Level: The last output of the multiple classifiers are combined. A scheme based on majority vote can be used to make the final decision. Decision level fusion includes very conceptual level of information so they are preferred least in designing multimodal biometric systems. Biometric systems that fuse information at the early stages are more effective than those in which integration is done in the later stages. So fusion at the feature level is assumed to give better recognition results but it is difficult to fuse at this level because feature sets of the various systems may not be compatible. More over all commercial Biometric systems don't provide access to the feature sets, which they use in their products. Fusion at the matcher score level is usually preferred because it is relatively easy to access and combine the scores presented by different modalities.

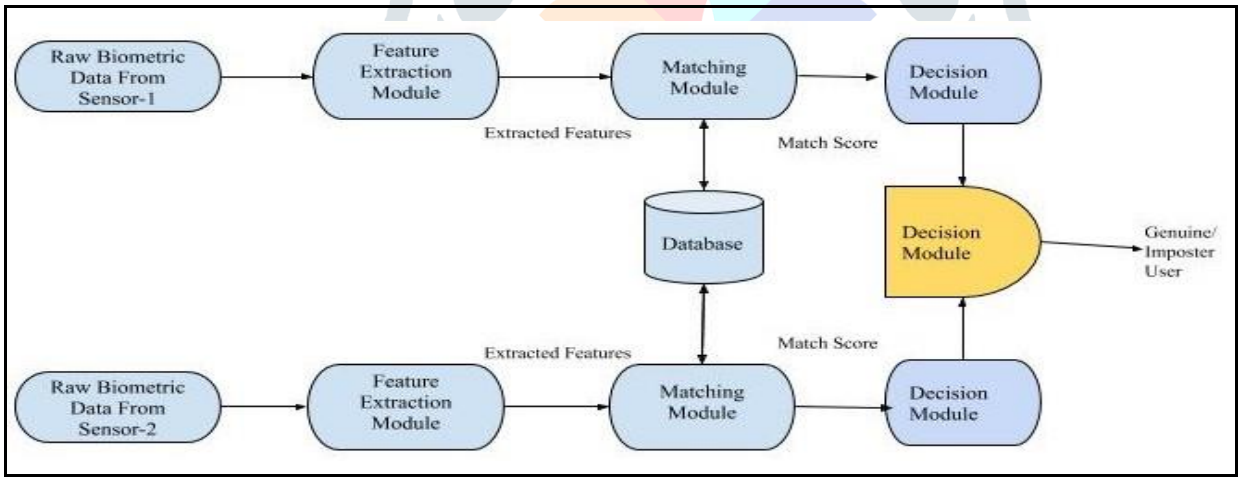

Fig 5. Decision Level Fusion

5. Related Work

Sheena S and Sheena Mathew [2], mention the importance of the use of multimodal biometrics over unimodal biometric. Robert W. Frischholz and Ulrich Dieckmann [4] proposed a multimodal biometric identification system named as BioID and fused face, voice and lip movement at sensor level fusion. Sanjay Kumar, Surjit Paul and Dilip Kumar Shaw [8] proposed a multimodal biometric authentication system for secured access to different web applications via WLAN using UML diagrams to design so. V. D. Mhaske and A. J. Patankar [9] fused fingerprint and palmprint by using modified Gabor filter to extract the features, Short Time Fourier transformation for better quality images and then Euclidean distance method to match the result. Ms. Shraddha S. Giradkar and Dr. N. K. Choudhari [10] presented a software and hardware based fake detection method to detect different fraudulent access attempts in multimodal biometrics. R. Parkavi, K.R. Chandeesh Babu, J.Ajeeth Kumar [11] fused fingerprint and iris at matching score level by using Minutiae matching and Edge detection. L.Nisha Evangelin and Dr. A.Lenin Fred [12] fused fingerprint, palmprint and finger-knuckle-print at feature level extraction by using Grey Level Co Occurrence Matrix. Arun Ross and Rohin Govindarajan [13] proposed

a novel technique to perform fusion of face and hand geometry at feature level. Souheil Ben-Yacoub, Yousri Abdeljaoued, and Eddy Mayoraz [14] evaluated different binary classification schemes i.e. support vector machine, multilayer perceptron, C4.5 decision tree, Fisher's linear discriminant, Bayesian classifier to carry on the fusion. Arun Ross, Anil Jain and Jian-Zhong Qian [15] addresses the problem of information fusion in verification systems by fusing face, fingerprint and hand geometry. Lin Hong and Anil K. Jain [16] introduce a decision level fusion framework which integrates faces and fingerprints which complement each other in terms of identification accuracy and identification speed.

6. Design Issues in Biometric Systems:

- Choice and number of biometric indicators
- Fusion Level: Representation (incompatibility & unavailability of features)
- Matching score (preferred; normalize matching scores)
- Fusion methodology
- Learning weights of individual biometric for each user
- Decision (too rigid; majority vote)
- Verification vs. Identification system
- Cost vs. Performance Trade-Off

7. Applications of Multimodal Biometrics

The defense and the intelligence communities require high level security systems. Border management, interface for criminal and civil applications, and first responder verification are the major areas which uses the Multimodal Biometrics. Personal or private information and Business transactions require fraud arrest solutions that increase security and are cost effective and user friendly. Multimodal biometrics can provide the best solutions to all the areas where high level security systems are needed.

8. Conclusion

There are many multimodal biometric systems in practice for authentication of an individual, choice of appropriate modal, selection of optimal fusion level and redundancy in the extracted features are still some of the limitations faced in the design of multimodal biometric system that needs to be addressed.

9. References

[1] Waleed Dahea, HS Fadewar, "Multimodal biometric system: A review", International Journal of Research in Advanced Engineering and Technology ISSN: 2455-0876, 2018

[2] Sheena S, Sheena Mathew, "A Study Of Multimodal System", IJRET eISSN: 2319-1163 | pISSN:2321-7308.

[3] Anil K. Jain, Salil Prabhakar and Arun Ross, "An introduction to biometric system", IEEE-2004

[4] Frischholz R, Dieckmann U. BiolD: A multimodal biometric identification system, Computer. 2000; 33(2):64-68.

[5] Sakshi Kalra, Anil Lamba, "Improving Performance by combining Fingerprint and Iris in Multimodal Biometric", International Journal of Computer Science and Information Technologies, 2014

[6] Mohammad Basheer K. P, Dr. T. Abdul Razak, "Improved Security Through Multimodal Biometric Using Fingerprint and Iris", International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869 (O) 2454-4698 (P), Volume-7, Issue-1, January 2017

[7] Hanaa S. Ali and Mahmoud I. Abdalla, "Score-Level Fusion for Efficient Multimodal Person Identification using Face and Speech", IJCSIS, 2011

[8] Sanjay Kumar, Surjit Paul and Dilip Kumar Shaw, "Design and Modeling of Real Time Multimodal Biometric Authentication System", 10.3844/JCSSP/2017

[9] V. D. Mhaske and A.J. Patankar, "Multimodal biometrics by integrating fingerprint and palmprint for security", IEEE, 2013

[10] Ms. Shraddha S. Giradkar and Dr. N. K. Choudhari, "a survey paper on various biometric security system methods", IRJET, 2016
[11] R. Parkavi, K.R. Chandeesh Babu, J.Ajeeth Kumar, "Multimodal Biometrics for User Authentication", IEEE, 2017
[12] L. Nisha Evangelin and Dr. A. Lenin Fred, "Feature Level Fusion Approach For Personal Authentication In Multimodal Biometrics", IEEE, 2017
[13] Arun Ross and Rohin Govindarajan, "Feature Level Fusion in Biometric Systems", 2000
[14] Souheil Ben-Yacoub, Yousri Abdeljaoued, and Eddy Mayoraz, "Fusion of Face and Speech Data for Person Identity Verification", IEEE 2000
[15] Arun Ross, Anil Jain and Jian-Zhong Qian, "Information Fusion in Biometrics", 2001
[16] Lin Hong and Anil K. Jain, "MULTIMODAL BIOMETRICS", 2001
[17] H. K. Ekenel, S. Y. Bilgin, . Eden, M. Kiriçi, H. Erdogan and A. Erçil, "Multimodal Person Verification from Video Sequences "
[18] K. Vamsi, Dr. Raman Chadha, Salony Tuli, "Templates Fusion With ROI Using Watermarking Technology" International Journal of Engineering Sciences & Research Technology, 2017
[19] Anu, Madhwendra Nath and Dr. Harvir, "A Review On Biometric Fusion", International Journal of Advance Research in Computer Science and Management Studies, 2014
[20] T. Sreenivasa Rao, E. Sreenivasa Reddy, "Multimodal Biometric Authentication Based on Score Normalization Technique", Springer-Verlag Berlin Heidelberg 2013
[21] Mini Singh Ahuja, Sumit Chabbra, "Biometric Encryption: Combining Fingerprints and Cryptography" HPAGC 2011, CCIS 169, pp. 505–514, 2011. © Springer-Verlag Berlin Heidelberg 2011
[22] Suvarnsing Bhable, Sangramsing Kayte , Jaypalsing Kayte RajuMaher, Dr.K.V. Kale, "A Multimodal Biometrics System: Review Paper" IOSR Journal of Computer Engineering, 2015
[23] A K Jain, Arun A Ross, Karthik Nandakumar, "Introduction to Biometrics", Foreword by James Wayman, Springer, ISBN 978- 0-387-77325-4
[24] Prof. Vijay M. Mane, Prof. (Dr.) Dattatray V. Jadhav, "Review of Multimodal Biometrics: Applications, challenges and Research Areas", International Journal of Biometrics and Bioinformatics, 2009
[25] Snehlata Barde, Sujata Khobragade, Rasmiprava Singh, "Authentication Progression through Multimodal Biometric System", International Journal of Engineering and Innovative Technology, 2012
[26] M. Y. Shams, S. H. Sarhan and A. S. Tolba, "Adaptive Deep Learning Vector Quantisation for Multimodal Authentication", Journal of Information Hiding and Multimedia Signal Processing, 2017
[27] B. Shanthini, S. Swamynathan, "A Novel Multimodal Biometric Fusion Technique for Security", International Conference on Information and Knowledge Management, 2012
[28] Sumit Chabbra, Nirmaljit Singh, "Applications of Swarm Intelligence in Biometrics systems " International Journal of Innovative Research in Computer and Communication Engineering, 2014