MULTIMODAL BIOMETRICS - SOURCES , ARCHITECTURE & FUSION TECHNIQUES: AN OVERVIEW

1. MADHAVI GUDAVALLI
Associate Professor, Department of CSE,
Vignan's Nirula Institute Of Technology & science for Women , Guntur, INDIA
E-mail: madhavik4u@gmail.com

2.Dr.S.VISWANADHA RAJU
Professor in CSE,
School of Information Technology,
Jawaharlal Nehru Technological University (JNTUH)
Kukatpally, Hyderabad, INDIA
E-mail: viswanadha_raju2004@yahoo.co.in

3. DR. A. VINAYA BABU
Professor & Principal, Department of CSE,
JNTUH College of Engineering, JNTUniversity Hyderabad, Kukatpally, Hyderabad,INDIA
E-mail: dravinayababu@jntuh.ac.in

4.Dr.D.SRINIVASA KUMAR
Professor & Principal, Department of CSE,
Nalanda Institute of Engineering & Technology,
Guntur, INDIA
E-mail: srinivaskumar_d@yahoo.com

ABSTRACT

Biometrics is the science and technology of measuring and analyzing biological data of human body, extracting a feature set from the acquired data, and comparing this set against to the template set in the database. The increasing demand of enhanced security systems has led to an unprecedented interest in biometric based person authentication system. Biometric systems based on single source of information are called Unimodal systems. Although some Unimodal systems have got considerable improvement in reliability and accuracy, they often suffer from enrollment problems due to non-universal biometrics traits, susceptibility to biometric spoofing or insufficient accuracy caused by noisy data . Hence, single biometric may not be able to achieve the desired performance requirement in real world applications. One of the methods to overcome these problems is to make use of multimodal biometric authentication systems, which combine information from multiple modalities to arrive at a decision. Multimodal biometric systems are those which utilize, or capability of utilizing, more than one physiological or behavioral characteristic for enrollment, verification, or identification. Studies have demonstrated that multimodal biometric systems can achieve better performance compared with Unimodal systems. We discuss here different multimodal sources, multimodal architectures & different fusion techniques used in multimodal biometric systems.

KEYWORDS

Architecture, Biometrics, Feature Vector, FRR, FAR, Fusion, Multimodal, Sources, Unimodal.

I. INTRODUCTION

The security of a system[5] has three primary components - authentication, authorization, and accountability. Authentication is the most fundamental of these three elements because it comes first. In the information technology domain, authentication means either the process of verifying the identities of communicating equipment, or verifying the identities of the equipment's users which are primarily humans.

Biometric systems[1] are becoming popular as a measure to identify human being by measuring one's physiological or behavioral characteristics. Biometrics identifies the person by what the person is rather than what the person carries, unlike the conventional authorization systems like smart cards. Unlike the possession-based and knowledge-based personal identification schemes, the biometric identifiers cannot be misplaced, forgotten, guessed, or easily forged.

The Multimodal biometric systems are providing identification and human security over last few decades. Due to this reason Multimodal biometric systems are adapted to

978-0-7695-4696-4/12 $26.00 © 2012 IEEE
DOI 10.1109/ISBAST.2012.24

many fields of applications. Some of these multimodal systems are human computer dialog interaction based systems where the user interacts with the PC through voice or vision or any other pointing device in order to complete a specific task. Multimodal biometric systems are those which utilize, or are capability of utilizing, more than one physiological or behavioral characteristic for enrollment, verification, or identification. A biometric system is essentially a pattern recognition system. This system measures and analyzes human body physiological characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements for authentication purposes or behavioral characteristics.

II.MULTI MODAL BIOMETRIC SYSTEM

Multimodal biometrics refers to the use of a combination of two or more biometric modalities in a verification / identification system. Identification based on multiple biometrics represents an emerging trend. The most compelling reason to combine different modalities is to improve the recognition rate. This can be done when biometric features of different biometrics are statistically independent. There are other reasons to combine two or more biometrics. One is that different biometric modalities might be more appropriate for the different applications. Another reason is simply customer preference.

The aim of multi-biometrics[2] is to reduce one or more of the following:

- False accept rate (FAR)
- False reject rate (FRR)
- Failure to enroll rate (FTE)
- Susceptibility to artifacts or mimics

The accuracy of a multimodal biometric system is usually measured in terms of matching errors and image acquisition errors. Matching errors consist of false match rate (FMR) where an impostor is accepted and false non-match rate (FNMR) where a genuine user is denied access. Image acquisition errors comprise of failure-to-enrol (FTE) and failure-to-acquire (FTA). A summary of the different biometric errors is provided in Table I.

Table I Biometric errors

	Sometimes referred as	*Refers to*
1)Matching Errors		
False Match Rate (FMR)	False Positive Rate (FPR)	An impostor's Sample matches a legitimate user's template
False Non Match Rate (FNMR)	False Negative Rate (FNR)	A legitimate user's Sample does not match his/her own template
2)Image Acquisition Errors		
Failure to Enroll (FTE)	Failure to Enroll Rate (FER)	A user that is unable to successfully enroll in a biometric system
Failure to Acquire (FTA)		A user that is unable to provide a good quality biometric trait at Verification

III. MULTIMODAL SOURCES

Multimodal biometrics does not only refer to the use of two or more separate biometric sensors. Instead the multiple inputs can come from a variety of sources[3].

1.Single Trait / Multiple Sensors

The same biometric trait is measured by two different sensors. These sensors could provide very different inputs.

2.Single Trait / Multiple Classifiers

A single trait is used, but different classifiers are input into the system. For example: The minutiae points and texture could be retrieved from a single finger.

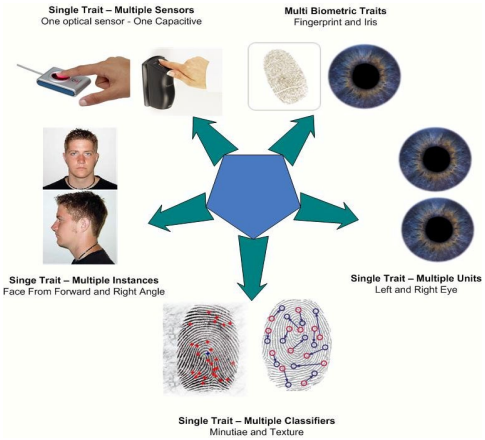

Figure 1. Multimodal Biometric Sources

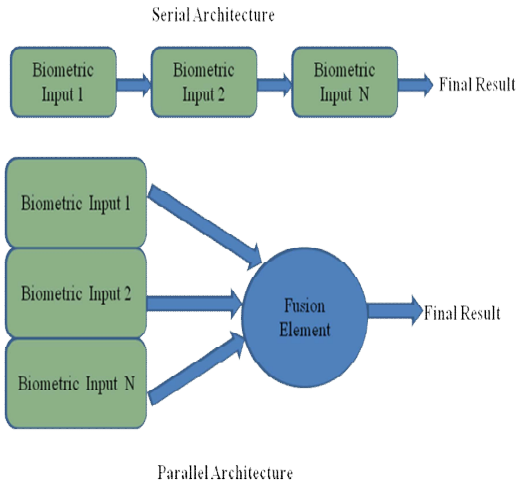

Figure 2. Two Main Architecture Designs for Multimodal Systems

3.Single Trait / Multiple Instances

Again, a single trait is used, but similar inputs that are slightly different to one another are used. For example: A person's face could be scanned from a head on angle, or from a side angle.

4.Single Trait / Multiple Units

A single trait is used, but different examples of it are input. For example: A persons left eye and right eye are both input into the system.

5. Multiple Biometric Traits

Two different biometric traits are combined to verify or identify a user. For example: A fingerprint and face are both input .

IV. MULTIMODAL BIOMETRIC SYSTEMS ARCHITECTURES

Once it has been determined which different biometric sources are to be integrated, the system architecture is selected. It is generally accepted that there are two main types of system designs[6] when it comes to multimodal biometric systems – namely '**serial**' and **parallel**'.

Serial

In serial architecture[6], also known as cascade architecture, the processing of the different inputs are done in sequence. Therefore, the output from the first biometric trait, will affect the processing of the 2nd biometric trait, and so forth.

Parallel

In parallel architecture, the processing of different biometric inputs[6] are done independently from each other. Once both have been separately processed, their results are combined.

V. MODES OF OPERATION

A multimodal system can operate in one of three different modes: serial mode, parallel mode, or hierarchical mode. In the serial mode of operation, the output of one modality is typically used to narrow down the number of possible identities before the next modality is used . Therefore, multiple sources of information (e.g., multiple traits) do *not* have to be acquired simultaneously. Further, a decision could be made before acquiring *all* the traits. This can reduce the overall recognition time. In the parallel mode of operation, the information from multiple modalities are used simultaneously in order to perform recognition. In the hierarchical scheme, individual classifiers are combined in

a treelike structure. This mode is relevant when the number of classifiers is large.

VI. FUSION IN MULTIMODAL BIOMETRIC SYSTEMS

In multimodal biometrics we use more than one biometric modality; we have more than one decision channels. We need to design a mechanism that can combine the classification results from each biometric channel; this is called as biometric fusion. Multimodal biometric fusion combines measurements from different biometric traits to enhance the strengths and diminish the weaknesses of the individual measurements.

Fusion at matching score, rank and decision levels have been extensively studied in the literature [7,8]. Multimodal Biometrics with various levels of fusion: sensor level, feature level, matching score level and decision level[5].

The sensor level and the feature level are referred to as **pre-mapping fusion** while the matching score level and the decision level are referred to as **post-mapping fusion** [11]. In pre-mapping fusion, the data is integrated before any use of classifiers, while in post-mapping fusion, the data is integrated after mapping into matching score/ decision space.

A. Pre-mapping fusion I : Sensor level Fusion

In sensor Fusion[5] we combine the biometric traits coming from sensors like Thumbprint scanner, Video Camera, Iris Scanner etc, to form a composite biometric trait and process. An example of the sensor fusion level is sensing a speech signal simultaneously with two different microphones. Although fusion at such a level is expected to enhance the biometric recognition accuracy [10, 12], it can not be used for multimodal biometrics because of the incompatibility of data from different modalities [10].

B. Pre-mapping fusion II : Feature Level Fusion

In feature level fusion signal coming from different biometric channels are first preprocessed, and feature vectors are extracted separately, using specific fusion algorithm we combine these feature vectors to form a composite feature vector. This composite feature vector is then used for classification process. Concatenating the feature vectors extracted from face and fingerprint modalities is an example of a multimodal system. It is stated in [10, 12] that fusion at the feature level is expected to perform better in comparison with fusion at the score level and decision level. The main reason is that the feature level contains richer information about the raw biometric data. However, such a fusion type is not always feasible [10, 12]. For example, in many cases the given features might not be compatible due to differences in the nature of modalities. Also such concatenation may lead to a feature vector with a very high dimensionality. This increases the computational load. It is reported that a significantly more complex classifier design might be needed to operate on the concatenated data set at the feature level space[10].

C. Post-mapping fusion I : Matching Score Level

Here, rather than combining the feature vector, we process them separately and individual matching score is found, then depending on the accuracy of each biometric channel we can fuse the matching level to find composite matching score which is then sent to the decision module [9]. Currently, this appears to be the most useful fusion level because of its good performance and simplicity [13, 14] This fusion level can be divided into two categories: combination and classification. In the former approach, a scalar fused score is obtained by normalising the input matching scores into the same range and then combining such normalised scores. In the latter approach, the input matching scores are considered as input features for a second level pattern classification problem between the two classes of client and the Impostor [15].

D. Post-mapping fusion II : Decision level Fusion

Each modality is first pre-classified[5] independently. The final classification is based on the fusion of the outputs of the different modalities. In this approach, a separate

decision is taken for each biometric type at a very late stage. This seriously limits the basis for enhancing the system accuracy through the fusion process. Thus, fusion at such a level is the least powerful[16].

Table II. Multimodal Biometric Fusion Techniques

Fusion Level	Sometimes referred as	Refers to
Sensor Level		The raw data of the sensors are Combined.
Feature Level	Representation Level Fusion	The features extracted from the different sensors are concatenated to create a joint feature vector.
Confidence Level	Score Level Integration Measurement Level Integration Opinion Fusion Soft Decision Fusion	The matching scores of each subsystem are combined using techniques such as Weighted Sum rule, Weighted Product, linear discriminant, decision tree and the Bayesian Rule.
Abstract Level	Decision Fusion	The decision of the subsystems are combined using techniques such as an AND rule, OR rule and Majority Voting.

Multimodal biometric system can implement any of these fusion strategies or combination of them to improve the performance of the system; the different levels of fusion are shown in Fig.3[5] as follows. The effectiveness of the fusion scheme greatly influences the accuracy of a multimodal biometric system.

Fusion at the sensor level[5] is very complex and fusion at the feature level may not always be feasible. It is difficult to combine the minutia feature of a fingerprint image with the eigen-coefficients of a face image. There is currently very little published about those fusion techniques.

Fusion at the confidence level is often the preferred fusion technique since it is relatively easy to combine the opinions of the different subsystems. Fusion at the confidence level can adjust the weight assigned to each subsystem to arrive at a more accurate decision. This can be achieved using a non adaptive approach or an adaptive approach. In a non-adaptive approach, the weight of each subsystem is based on the subsystem's bias. In a multimodal biometric system with a fingerprint and voice subsystems, the initial accuracy of the fingerprint subsystem could be higher than the voice subsystem. Therefore, a higher weight can be assigned to the fingerprint subsystem.

An adaptive approach[4] is where the contribution of at least one subsystem varies on the user's identity claim or the environment. Research clearly demonstrates the benefits of assigning weight to subsystems depending on user-specific parameters as opposed to parameters common to all. By computing a matching threshold for each user using cumulative histograms of impostor's scores for each biometric trait, an increase in accuracy was observed when using a user specific threshold versus a common threshold. Also, by learning user-specific weight for each trait, a low weight could be assign to a less reliable trait and a higher weight to a more reliable one. It was demonstrated that the error rates were reduced for that particular individual. The weight of each subsystem can also be assigned depending on the environment. For a multimodal biometric system combing fingerprint and speech information, the system can lower the weight associated to the speech subsystem when the signal to noise ratio is low.

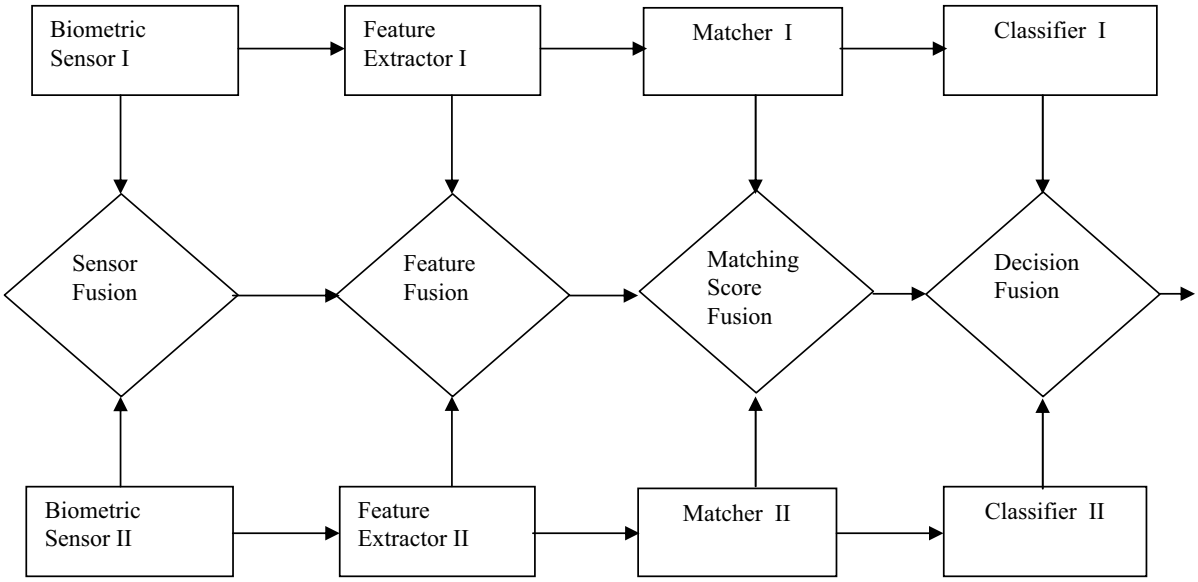

Figure 3. Fusion levels in Multimodal Biometric Systems

VII. NORMALIZATION

Fusion techniques have been limited to small populations (~100 individuals), while employing low performance non-commercial biometric systems. A normalization step is generally necessary before the raw scores originating from different matchers can be combined in the fusion stage. For example, if one matcher yields scores in the range [100, 1000] and another matcher in the range [0, 1], fusing the scores without any normalization effectively eliminates the contribution of the second matcher. Normalization addresses the problem of incomparable classifier output scores in different combination classification systems.

We present three well-known normalization methods. We denote a raw matcher score as s from the set S of all scores for that matcher, and the corresponding normalized score as n . Different sets are used for different matchers.

*A. Min-Max (MM):*This method maps the raw scores to the [0, 1] range. max(S) and min(S) specify the end points of the score range (vendors generally provide these values)

$$n = (s - \min(S)) / (\max(S) - \min(S))$$

B. Z-score (ZS): This method transforms the scores to a distribution with mean of 0 and standard deviation of 1. mean() and standard() denote the deviation operators

$$n = (s - \text{mean}(S)) / (\text{std}(S))$$

C. Tanh (TH) : This method is among the so-called *robust* statistical techniques . It maps the scores to the (0, 1) range

$$n = 0.5[\tanh(0.01(s - \text{mean}(S)) / (\text{std}(S))) + 1]$$

VIII. APPLICATIONS

The defense and intelligence communities require automated methods capable of rapidly determining an individual's true identity as well as any previously used identities and past activities, over a geospatial continuum from set of acquired data. A homeland security and law enforcement community require technologies to secure the borders and to identify criminals in the civilian law enforcement environment. Key applications include border management, interface for criminal and civil applications, and first responder verification.

Enterprise solutions require the oversight of people, processes and technologies. Network infrastructure has

become essential to functions of business, government, and web based business models. Consequently securing access to these systems and ensuring one's identity is essential. Personal information and Business transactions require fraud prevent solutions that increase security and are cost effective and user friendly. Key application areas include customer verification at physical point of sale, online customer verification etc.

IX .CONCLUSION

Multimodal biometric systems elegantly address several of the problems present in unimodal systems. By combining multiple sources of information, Multimodal biometric systems improve matching performance, increase population coverage, deter spoofing, and facilitate indexing. This paper has discussed the various sources and architectures related to multimodal biometric systems. By combining multiple sources of information, the improvement in the performance of biometric system is attained. Various fusion levels of multimodal systems are discussed. Fusion at the match score level is the most popular due to the ease in accessing and consolidating matching scores. Performance gain is pronounced when uncorrelated traits are used in a multimodal system.

Designing biometric sensors, which automatically recognize the operating environment (outdoor / indoor / lighting etc) and communicate with other system components to automatically adjust settings to deliver optimal data, is the challenging area. The sensor should be fast in collecting quality images from a distance and should have low cost with no failures to enroll.

REFERENCES

[1] A. K. Jain, A. Ross and S. Prabhakar, "*An introduction to biometric recognition*". IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, pp. 4–20, Jan 2004.

[2] Chander Kant, Rajender Nath, "Reducing *Process-Time for Fingerprint Identification System*", International Journals of Biometric and Bioinformatics, Vol. 3, Issue 1, pp.1- 9, 2009.

[3] A.K.Jain, A.Ross, " *Multibiometric systems*". Communications of the ACM, vol. 47, pp. 34-40, 2004.

[4] K.Sasidhar, VijayaLKakulapati, Kolikipogu Ramakrishna & K.KailasaRao, **"**Mutimodal Biometric Systems –study to improve accuracy and performance", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010.

[5] Ashish Mishra ,"Multimodal Biometrics it is: Need for Future Systems**",** International Journal of Computer Applications (0975 – 8887) Volume 3 – No.4, June 2010

[6]http://ujdigispace.uj.ac.za/bitstream/handle/10210/2538/Chapter3.pdf , " Introduction To MultiModal Biometrics".

[7] J. Fierrez-Aguilar, J. Ortega-Garcia and J. Gonzalez-Rodriguez,"Fusion strategies in Biometric Multimodal Verification",Proceedings of International Conference on Multimedia and Expo,ICME 2003.

[8] "Multimodal Biometrics: Issues in Design and Testing," in Proceedings of Fifth International Conference on Multimodal Interfaces, R. Snelick, M. Indovina, J. Yen, and A. Mink, (Vancouver, 2003), pp. 68–72.

[9] A. Ross and A. Jain, "Information Fusion in Biometrics," *Pattern Recognition Letters, Special Issue on Multimodal Biometrics*, vol. 24, pp. 2115-2125, 2003.

[10] M. Faundez-Zanuy, "Data fusion in biometrics," IEEE Aerospace and Electronic Systems Magazine, vol. 20, pp. 34-38, 2005.

[11] C. Sanderson and K. K. Paliwal, "Information Fusion and Person Verification Using Speech and Face Information," IDIAP-RR 02-33, 2003.

[12] A. K. Jain and A. Ross, "Multibiometric Systems," Interagency Information Exchange on Biometrics, 2003.

[13] A. K. Jain, K. Nandakumar, and A. Ross, "Score normalisation in multimodal biometric systems" *Pattern Recognition*, vol. 38, pp. 2270–2285, 2005.

[14] M. Indovina, U. Uludag, R. Snelick, A. Mink, and A. Jain, "Multimodal Biometric Authentication Methods: A COTS Approach," *Proceedings of Multi - Modal User Authentication (MMUA)*, pp. 99-106, 2003.

[15] J. Fierrez-Aguilar, "Adapted Fusion Schemes for Multimodal Biometric Authentication ", PhD Thesis: University of Madrid 2006.

[16] A. Ross and A. Jain, "Multimodal biometrics: an overview," *Proceedings of the 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria)*, pp. 1221-1224, 2004.