International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.2, No.9, September 2013 DOI:10.15693/ijaist/2013.v2i9.1-5

Image Fusion Techniques in Multimodal Biometrics Systems, Applications and Challenges.

Prof. Jitendra B. Jawale
Assistant Professor/Department of E&TC
Army Institute Of Technology,
Dighi, Pune,India

Prof. Mrs. Priti J Jawale
Assistant Professor/Department of E&TC
Dr. D Y Patil Institute Of Engg. & Technology,
Pimpri, Pune, India.

***Abstract*— Automatic identification or verification of individuals based on their anatomical or behavioral characteristics is known as Biometrics. Biometric systems based on a single source of biometric information are unimodal biometrics systems. Most of the unimodal biometric systems fail to be sufficient for recognition due to limitations such as noisy sensor data, non-universality, large intra-user variations, lack of individuality of the chosen biometric trait, susceptibility to spoof attacks and poor error rates. Some of these problems can be alleviated by using multimodal biometrics systems that fuse evidence from multiple biometric sources of the same identity. Ambiguities in one modality like lighting problem can be compensated by another modality like speech features. Hence, multimodal biometric system normally performs better than any of unimodal biometrics. However, integration of evidence obtained from multiple biometric sources is a challenging problem. Fusion can be performed at four different levels of information, namely, sensor, feature, score and decision levels. Fusion at the matching score level is the most common approach as it provides the best trade-off between the information content and the ease in fusion[1,2].**

***Keywords*— multimodal biometrics systems, from multiple biometric sources, Fusion at the matching score level.**

I. INTRODUCTION

Automatic person identification is an important task in our day to day life. The traditional method of establishing a person's identity include knowledge based like password or token based like ID cards, but representation of these identity can easily be lost, stolen or shared. Therefore they are not sufficient for identity verification. Therefore biometric systems are used to overcome the limitations of traditional methods. The survey of biometric and multimodal biometric systems is therefore necessary for high security applications. This paper discusses the biometric system, an overview of multimodal biometrics, challenges in the progress of multimodal biometrics, and its applications to develop the security system. The primary task in an identity management system is determination of individual's identity. This action may necessary for many reasons but in most applications, primary intention is to prevent imposters from accessing protected resources.. Biometric offers natural and reliable solution to the problem of identity determination by recognizing individuals by using certain physiological or behavioral traits associated with the persons. Biometrics is the science of identifying or verifying the identity of person based on physiological or behavioral characteristics [1]. Physiological traits are related to physiology of the body and mainly include fingerprint, face, ear, iris, retina, hand, palm geometry. Behavioral traits related to the person such as signature, voice etc. However, a single biometric characteristic sometimes fails to be accurate enough for the identification because it may suffer a variety of problems. [2-3]. 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. Studies have demonstrated that multimodal biometric systems can achieve better performance compared with unimodal systems [4,5].

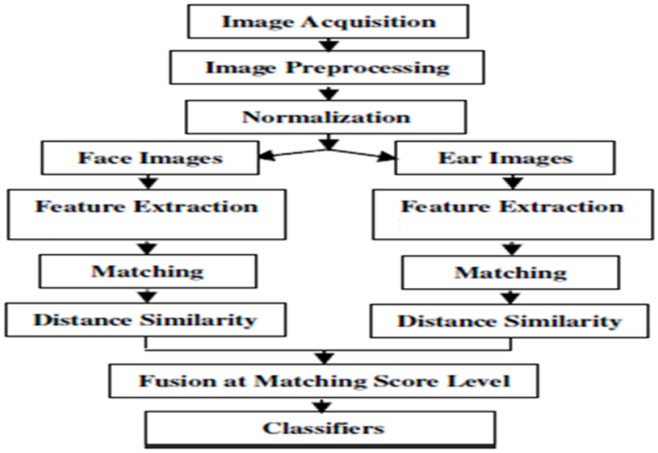

Figure.1. Multimodal System

Biometric system can be operated either in user verification or identification mode. Briefly, in the verification mode, the user claims an identity and the system verifies whether the claim is genuine. For the identification mode, the user does not claim a certain identity but the implicit claim made by the user is that he is one among the persons already enrolled in the system. The user's input is compared with the templates of all the persons trained in the database and the identity of

the person whose template has the highest similarity with user's input is output by the biometric system. In this project, the system compares the user's inputs with the templates of all the persons trained in the database and produces the similarity match scores. If the score is greater than the minimum threshold, the user will be accepted as a genuine user or else considered as an impostor [6].

II. NEED OF MULTIMODAL BIOMETRICS

A multi biometric system uses multiple sensors for data acquisition which allows capturing of multiple samples of a single biometric trait and/or samples of multiple biometric traits. These systems are more reliable due to the presence of multiple, independent biometrics. These systems are able to meet the stringent performance requirements imposed by various applications. They address the problem of non-universality, since multiple traits ensure sufficient population coverage. It would be difficult for an impostor to spoof multiple biometric traits of a genuine user simultaneously. Furthermore, they can facilitate a challenge – response type of mechanism by requesting the user to present a random subset of biometric traits there by ensuring that a 'live' user is indeed present at the point of data acquisition[6].

Table 1. Comparison Of Biometrics System

Biometric Type	Accuracy	Ease of Use	User Acceptance
Fingerprint	High	Medium	Low
Hand Geometry	Medium	High	Medium
Voice	Medium	High	High
Retina	High	Low	Low
Iris	Medium	Medium	Medium
Ear	High	Medium	Medium
Face	Low	High	High

A biometric system is basically a pattern recognition system that acquires biometric data from an individual, extracts a salient feature set from the data, compares this feature set against the feature set stored in the database and executes an action based on the result of the comparison [3]. A generic biometric system can be divided into four main modules: a sensor module; a quality assessment and feature extraction module; a database module; and a matching and decision module.

- Sensor module**:** In order to acquire the raw biometric data of an individual, a suitable biometric reader or scanner is required. A poorly designed interface can result in a high failure-to-acquire rate and consequently low user acceptability.
- Feature extraction module: The quality of the biometric data acquired by the sensor is first assessed in order to determine its suitability for further processing. After quality assessment, the biometric data is then processed and a set of salient discriminatory features extracted to represent the underlying trait. During enrollment, this feature set is stored in the database and is commonly referred to as a template.
- Database module: This module acts as the storage of biometric information. During the enrollment process, the feature set extracted from the raw biometric sample is stored in the database along with some biographic information characterizing the user. The data capture during the enrollment process may or may not be supervised by a human depending on the application.

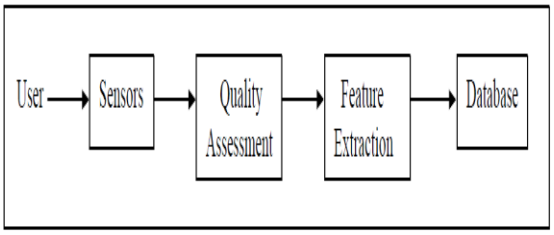

Figure 2. Enrollment processes.

- Matching and decision module: Matching is a process that the extracted features are compared against the stored templates to generate match scores. In a decision process, the match scores are used to either validate a claimed identity or provide a ranking of the enrolled identities in order to identify an individual.

Biometric systems, can be operated either in user verification or identification mode. In the verification mode, the system validates the individual's identity by comparing the captured biometric data with his own biometric template stored in the system database. The system operates a one-to-one comparison to determine whether the claim is true or not. Verification is generally used for positive recognition, where the aim is to prevent multiple people from using the same identity.

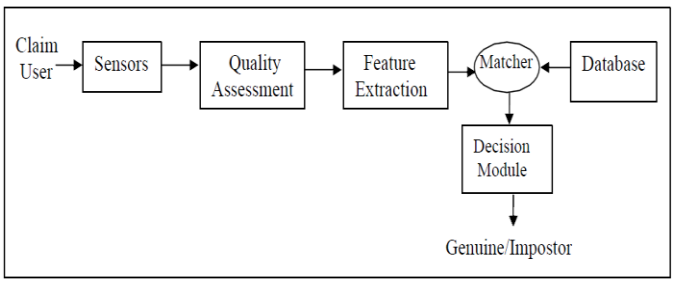

Figure 3. Verification processes.

In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. The system performs a one-to-many comparison to establish an individual's identity without the subject having to claim an identity. If the subject is not enrolled in the system database, the system will not be able to identify the subject's identity. Identification is a critical component in negative recognition applications. The purpose of negative recognition is to prevent a single person from using multiple identities. For the purpose of convenience where the user is not required to claim an identity, identification method may also be used.

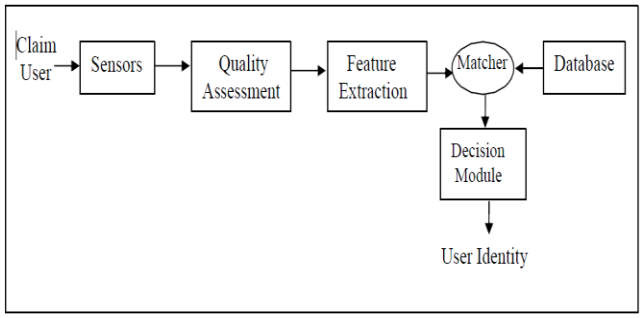

Figure 4. Identification Processes

III. MULTIMODAL BIOMETRICS

The term "multimodal" is used to combine two or more different biometric sources of a person(like face, Ear and finger print) sensed by different sensors. Two different properties of the same biometric can also be combined. In orthogonal multimodal biometrics, different biometrics (like face and Ear) are involved with little or no interaction between the individual biometric whereas independent multimodal biometrics processes individual biometric independently. Orthogonal biometrics are processed independently by necessity but when the biometric source is the same and different properties are sensed, then the processing may be independent, but there is at least the potential for gains in performance through collaborative processing. In collaborative multimodal biometrics the processing of one biometric is influenced by the result of an other biometric. Multimodal biometrics systems that fuse evidence from multiple biometric sources of the same identity. In multimodal biometric system, fusion can be performed at the four different levels:

- at the sensor level
- at the feature-extraction level
- at the matching-score level
- at the decision level

3.1. Fusion At The Sensor Level

Fusion at the sensor level is performed by integrating information from different sensor before feature extraction takes place. For example, information from a 3D shape sensor and a standard camera can be combined to produce 3D textured information of an object. Sensor level fusion is quite rare because fusion at this level requires that the data obtained from the different biometric sensors must be compatible, which is seldom the case with biometric sensors.

3.2. Fusion at the Feature Extraction Level

Feature sets are acquired from each sensor, where each feature set is represented as a vector. Then the vectors are concatenated which results in a new feature vector with higher dimensionality representing a person's identity in a different hyperspace. Fusion at the feature level is also not always possible because the feature sets used by different biometric modalities may either be inaccessible or incompatible.

3.3. Fusion At The Decision Level

The resulting feature vectors from each sensor need to be classified into two classes-reject or accept. Afterwards a majority vote scheme can be used to make a final decision. Fusion at the decision level is too rigid since only a limited amount of information is available.

3.4. Fusion At The Matching Score Level

Each biometric system provides a matching score which indicates the proximity of the feature vector with the template vector. Fusion at this level would mean combining the matching scores in order to verify the claimed identity. In order to combine the matching scores reported by the sensors, techniques such as logistic regression are used. The logistic regression model is simply a non-linear transformation of the linear regression. The logistic distribution is an S-shaped distribution function similar to the standard normal distribution, but it is easier to work with in most applications because the probabilities are easier to calculate. These techniques attempt to minimize the False Rejection Rate (FRR) for a given False Acceptance Rate (FAR). Fusion at the score level is preferred as it offers the best trade-off in terms of the information content and the ease in accessing and combining matching score.

Score fusion techniques can be divided into four categories: combination approach fusion, transformation based score fusion, density based score fusion and classifier based score fusion.

3.4.1. Combination Approach Fusion

This approach combines the individual scores from multiple matchers. It is the easiest method to implement. Generally, score normalization is necessary before combining the raw scores originating from different

matchers can be combined in the fusion stage. Different combination rules are product rule, sum rule, max rule, min rule and median rule.

3.4.2. Density-Based Score Fusion

This approach is based on the likelihood ratio test and it requires explicit estimation of genuine and impostor match score densities. Density estimation can be done either by parametric or non-parametric methods. In parametric density estimation techniques, the form of the density function is assumed to be known and only the parameters of this density function are estimated from the training data. On the other hand, non-parametric techniques do not assume any standard form for the density function and are essentially data driven. After estimating the densities, the probabilities are computed and then decision rules are applied to make a decision. Density based approach has the advantage that it directly achieves optimal performance at any desired operating point (False Acceptance Rate), provided the score densities are estimated accurately.

3.4.3. Transformation-Based Score Fusion

This transformation is known as score normalization and the resulting fusion approach is known as transformation base score fusion. In the transformed domain, the sum, max and min classifier combination rules can be directly applied. The sum of scores fusion method with simple score normalization represents a commonly used transformation based core fusion.

3.4.4. Classifier-Based Score Fusion

In this approach, the vector of match scores is treated as a feature vector which is then classified into one of the two classes: genuine user or impostor. Based on the training set of match scores from the genuine and impostor classes, the classifier learns a decision boundary between the two classes. During verification, any match score vector that falls in the genuine region is classified as genuine. In general, the decision boundary can be quite complex depending on the nature of the classifier.

IV. PERFORMANCE MEASURE OF THE BIOMETRICS SYSTEMS

Generally Performance measure of the biometrics systems is measured by Falls Acceptance Rate (FAR) and False Rejection Rate (FRR) or Genuine Acceptance Rate (GAR). FAR is the case where an impostor, claiming the identity of a client, is rejected FRR is the case where a client, claiming his true identity is rejected. GAR is used as an alternative to FRR. A client score measures the similarity between the trained and test samples of the same person. An impostor score refers to the similarity measure of samples for different persons. In theory, client scores should always be higher than the scores of impostors. If that is the case, a single threshold that separates the two groups of scores could be used to separate between clients and impostors. For example, if a client score is less than the threshold, the verification system will count as a false rejection. If an impostor score is greater than the threshold, it will count as a false acceptance. FRR, FAR, GER and (TER) Total error rate is determine as follows[7].

$$\text{FAR}(\%) = \frac{False\ acceptance\ \ Number}{Number\ \ of\ Imposter} X100\%$$

$$\text{FRR}(\%) = \frac{False\ rejection\ \ number}{number\ \ of\ client\ \ test} X100\%$$

GAR(%)= 100% - FRR(%)

TER(%)=FRR(%) + FAR(%)

IV. APPLICATIONS

Personal information and Business transactions require fraud prevent solutions that increase security and are cost effective and user friendly. The defense and intelligence communities require automated methods capable of rapidly determining an individual's true identity. A homeland. security and law enforcement community require technologies to secure the borders and to identify criminals in the civilian law enforcement environment[8].

V. CHALLENGES TO MULTI-BIOMETRIC SYSTEM

Based on applications and facts presented in the previous sections, followings are the challenges in designing the multi modal systems.

1. The sensor should be fast in collecting quality images from a distance and should have low cost with no failures to enroll.

2. The information obtained from different biometric sources can be combined at five different levels such as sensor level, feature level, score level, rank level and decision level. Therefore selecting the best level of fusion will have the direct impact on performance and cost involved in developing a system.

3. In multimodal biometric systems the information acquired from different sources can be processed either in sequence or parallel. Hence it is challenging to decide about the processing architecture to be used in designing the multi-modal biometric systems[8].

VI. CONCLUSION

Automatic person identification is an important task in our day to- day life. Therefore in this paper multimodal biometric systems and different fusion techniques are discussed. By combining multiple sources of information, the improvement in the performance of biometric system can be achieved. Fusion at the match score level is the most popular due to the ease in accessing and consolidating matching scores. The performance measure, application and challenges faced by multimodal biometric system are also discussed in the paper.

REFERENCES

[1] K. Jain, A. Ross, S. Prabhakar,"An introduction to biometric recognition", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, 2004, pp. 4–20..
[2] D. Zang,"Automated Biometrics: Technologies and Systems", Kluwer Academic Publishers, USA, 2000.
[3] Chander Kant, RajenderNath,"Reducing Process-Time for Finger print Identification System", International Journals of Biometric and Bioinformatics, Vol. 3, Issue 1, 2009, pp.1- 9.
[4] A.K. Jain, A. Ross, "Multibiometric systems", Communications of the ACM, Vol. 47, 2004, pp. 34-40.
[5] R. Frischholz, U. Dieckmann,"BiolD: A multimodal biometric identification system", Computer, Vol. 33, No. 2, 2000, pp. 64-68.
[6] L. I. Kuncheva, C. J. Whitaker, C. A. Shipp, R. P. W. Duin,"Is independence good for combining classifiers?", in Proceedings of International Conference on Pattern Recognition (ICPR), Vol. 2, (Barcelona, Spain), 2000, pp. 168–171.
[7] Md.maruf Monwar, "Enhancing Security through a hybrid Multibiometric System", IEEE Procedding,2009.
[8] Savitri B. Patil, "A Study of Biometric, Multimodal Biometric Systems: Fusion Techniques, Applications and Challenges", IJCST Vol. 3, Issue 1, 2012, pp 524-526.

Authors Profile

Prof. J B Jawale: received the Dip.(Electronics & Communication-1995), BE (Induristial Electronics-1999), M Tech (Electronics-2007) ,PhD (Electronics-Persuing). Presently working as an Asst. Prof. in E &TC Dept. in ARMY INSTITUTE OF TECHNOLOGY, PUNE I had publish four books :1) Digital Image Processing, 2) Power Electronics, 3) Power Devices & Machines, 4) Computer Organization. My area of research is MULTIMODAL BIOMETRICS.

Prof. Priti J Jawale received the Dip.(Electronics & Communication-1995), BE (Induristial Electronics-1999), M Tech (VLSI -2009) , Presently working as an Asst. Prof. in E &TC Dept. in Dr D Y PATIL INSTITUTE OF ENGINEERING & TECHNOLOGY, PIMPRI, PUNE