International Journal of Applied Science and Advance Technology (ISSN: 0973-7405)
January-June 2012, Vol. 1, No. 1, pp. 58-63

MULTIMODAL BIOMETRIC SYSTEM: A SURVEY

Arun Jain[1], Sona Aggarwal[2]
Assistant Professor[1], M.Tech.Student[2]
Department of Computer Sc. & Engineering, H.C.T.M, Kaithal, Haryana (India)
erarunjain@radiff.com, sonaaggarwal56@yahoo.com

Abstract: A biometric system which relies only on a single biometric trait is often not able to meet the desired performance. In Multi-modal system more than one biometric traits are used to identify a person. The study of methods for uniquely recognizing based upon one or more intrinsic physical or behavioral. In this paper we present the use of multimodal biometric system to get the higher degree of security.
Keywords: Multi-modal, Fusion techniques, Applications of Biometric.

1. Introduction

Biometrics system deals with the distinctive physiological or behavioral characteristics of human being. Biometrics system provides different types of techniques that capture a person's identity. Multimodal biometric system provides the technique that combine two or more traits which cannot be easily copied, forgotten or stolen by any intruder. It uses identifiers that capture two or more traits which match with the stored template. And after this process if the person passes all the stages then he/she can continue his/her work.

2. Multimodal Biometric

The Multimodal biometric systems are providing identification and human security over last few decades. Due to this reason multimodal biometrics systems are adapted to 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 measure 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. The biometric identifiers cannot be misplaced. In spite of inherent advantages, unimodal biometric solutions also have limitations in terms of accuracy, enrolment rates, and susceptibility to spoofing. This limitation occurs in several application domains, example is face recognition. The accuracy of face recognition is affected by illumination and facial expressions. The biometric system cannot eliminate spoof attacks. Inspite of using unimodal biometric system that have poor performance and accuracy, we study and propose a new approach to the multimodal biometric system. This new Multimodal biometric systems perform better than unimodal biometric systems and are popular even more complex. Multimodal biometric systems utilize more than one physiological or behavioral characteristic for enrolment, verification or identification. The

reason to combine different modalities is to improve recognition rate.

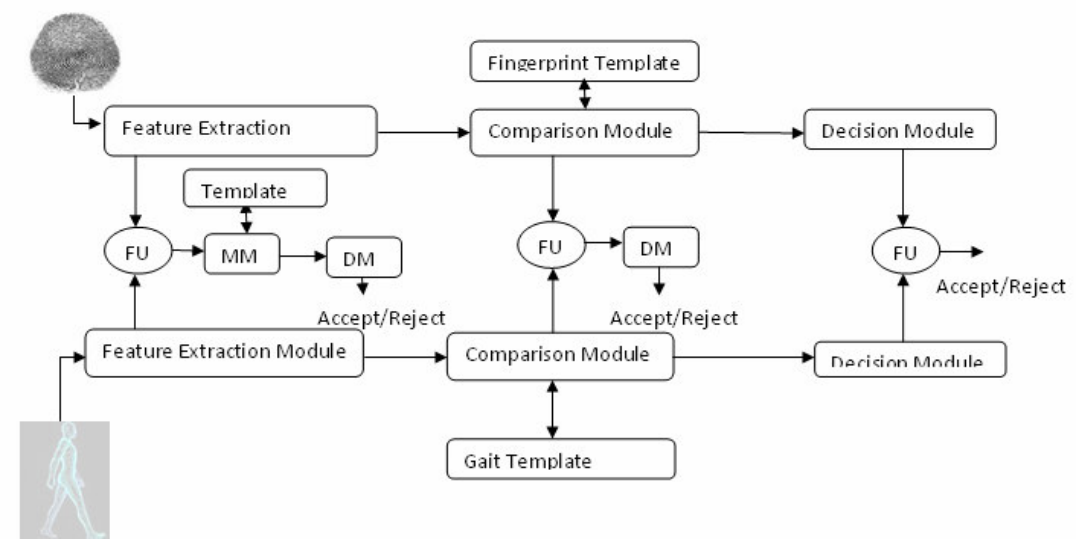

Figure 1: The three levels of fusion in multi-modal biometric system

The aim of multi biometrics is to reduce one or more of the following:

- False accept Rate (FAR)
- False Reject Rate (FRR)
- Failure to Enroll Rate (FTR)
- Susceptibility to Artifacts

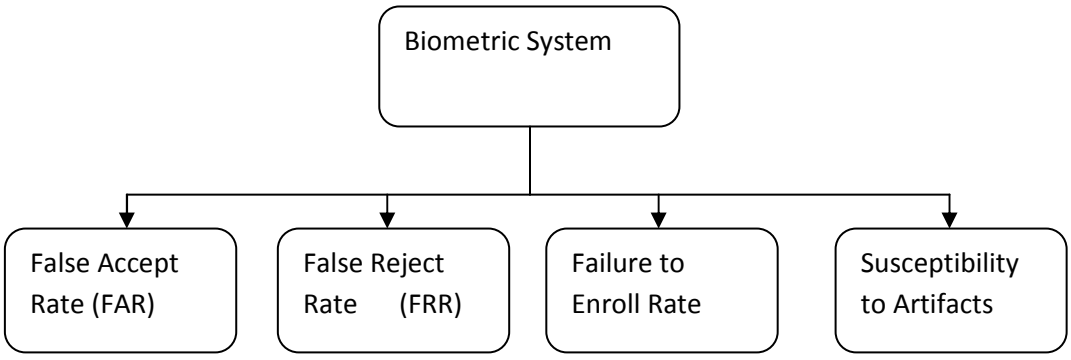

Figure 2: Various rates of biometric system

Multi modal biometric systems take input from single or multiple sensors measuring two or more different modalities of biometric characteristics. For example a system with voice and finger print recognition would be considered "multimodal" even if the "OR" rule was being applied, allowing users to be verified using either of the modalities

3. Application Area of Multimodal Biometrics System

3.1. Law enforcement

An Automated Fingerprint Identification System, or AFIS, is designed to enable a fingerprint to be matched extremely quickly against a large number of records in a criminal database. To do this effectively it will almost always hold encodings of all ten fingers.

Law enforcement agencies have achieved significant success with facial recognition, matching the mug shot (or even composite drawing) of a suspect against a database of offenders. This is particularly useful where the individual has refused to give his name, or has given a false name.

3.2. Airport security

Post 9/11 a real need emerged to identify terrorists trying to board planes. As in many cases the only information available on suspected terrorists was a mug shot or surveillance photo, facial recognition was thrust to center stage as the biometrics which could help identify them before they board the plane. While much work has been done in this area, the practical and logistical issues which have to be overcome have meant that so far, implementation has not been as fast as originally anticipated.

3.3. Smartcards

Smartcards are not a different application, but a particularly secure means of providing an individual with an identity card. They are especially appropriate for biometrics because sufficient memory can be made available to hold the individual's facial image and a number of encoded

arrays. While these will always be held in a central database as well, having them on the card itself enables it to be used in locations where there may be no network access.

The use of Radio Frequency Identification (RFID) enabled Smartcards minimizes the time taken to verify a person's identity, by allowing data on the card to be read without direct contact.

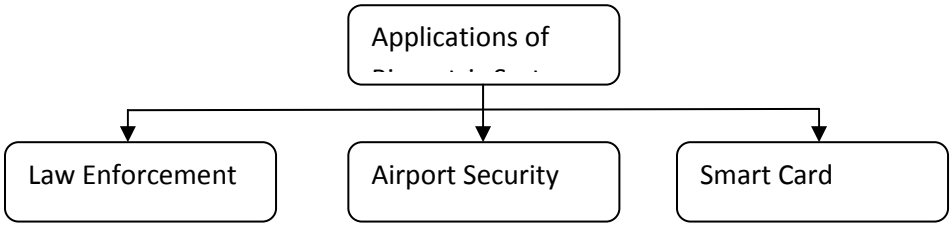

Figure 3: Applications of Biometric System

4. Fusion at various Levels

Based on the type of information available in a certain module, different levels of fusion may be defined.

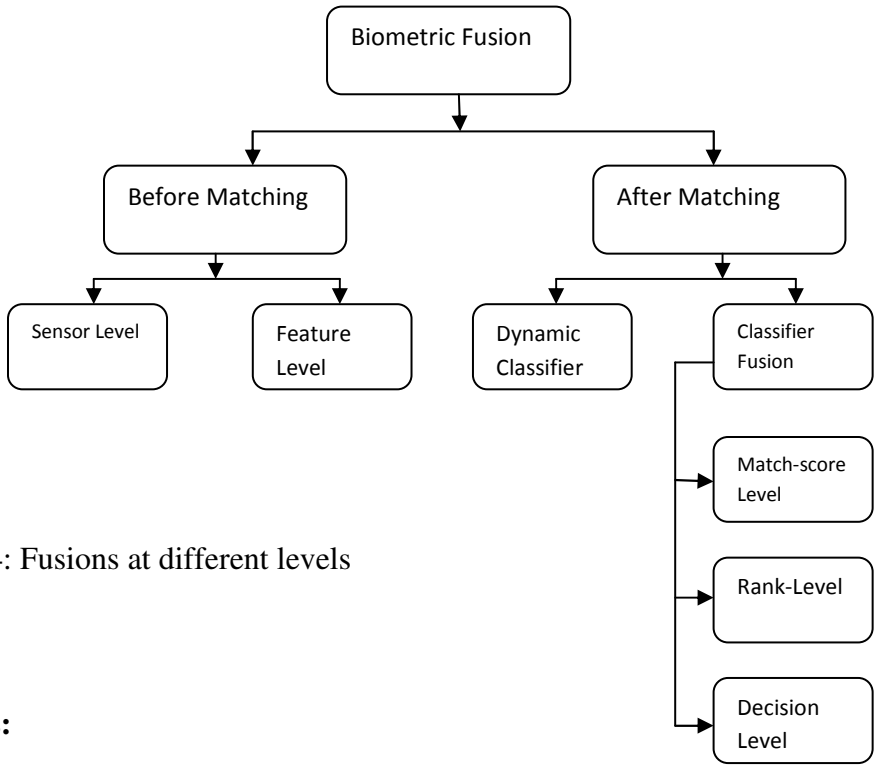

Figure 4: Fusions at different levels

Fusions:

- Sensor Level Fusion
- Feature Level Fusion
- Score Level Fusion
- Rank Level Fusion
- Decision Level Fusion

4.1. Sensor-level fusion: The raw biometric data (e.g., a face image) acquired from an individual represents the richest source of information although it is expected to be contaminated by noise (e.g., non-uniform illumination, background clutter, etc.). Sensor level fusion refers to the consolidation of (a) raw data obtained using multiple sensors, or (b) multiple snapshots of a biometric using a single sensor.

4.2. Feature-level fusion: In feature-level fusion, the feature sets originating from multiple biometric algorithms are consolidated into a single feature set by the application of appropriate feature normalization, transformation and reduction schemes. The primary benefit of feature- level fusion is the detection of correlated feature values generated by different biometric algorithms and, in the process, identifying a salient set of features that can improve recognition accuracy. Eliciting this feature set typically requires the use of dimensionality reduction methods and, therefore, feature-level fusion assumes the availability of a large number of training data. Also, the feature sets being fused are typically expected to reside in commensurate vector space in order to permit the application of a suitable matching technique upon consolidating the feature sets.

4.3. Score-level fusion: In score-level fusion the match scores output by multiple biometric matchers are combined to generate a new match score (a scalar) that can be subsequently used by the verification or identification modules for rendering an identity decision. Fusion at this level is the most commonly discussed approach in the biometric literature primarily due to the ease of accessing and processing match scores (compared to the raw biometric data or the feature set extracted from the data). Fusion methods at this level can be broadly classified into three categories: density-based schemes [6], transformation-based schemes [13] and classifier based schemes.

4.4. Rank-level fusion: When a biometric system operates in the identification mode, the output of the system can be viewed as a ranking of the enrolled identities. In this case, the output indicates the set of possible matching identities sorted in decreasing order of confidence. The goal of rank level fusion schemes is to consolidate the ranks output by the individual biometric subsystems in order to derive a consensus rank for each identity. Ranks provide more insight into the decision- making process of the matcher compared to just the identity of the best match, but they reveal less information than match scores. However, unlike match scores, the rankings output by multiple biometric systems are comparable. As a result, no normalization is needed and this makes rank level fusion schemes simpler to implement compared to the score level fusion techniques [10].

4.5. Decision-level fusion: Many commercial off-the-shelf (COTS) biometric matchers provide access only to the final recognition decision. When such COTS matchers are used to build a multi biometric system, only decision level fusion is feasible. Methods proposed in the literature for decision level fusion include "AND" and "OR" rules [7], majority voting weighted majority voting, Bayesian decision fusion the Dumpster-Shafer theory of evidence and behavior knowledge space [11]

5. Conclusion

In this paper various issues related to multimodal biometrics system have been presented. By combining multiple biometric traits, the performance of biometric system can be improved. Various applications of multimodal biometrics system and different levels of fusion are discussed. The multimodal biometrics is very popular in these days due to its performance and advance level of security. Though some complexity also exists in multimodal system which reduces its acceptability in many areas.

6. References

[1] "Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and interoperability," NIST Report to the United States Congress, Nov.2002.
[2] Biometrics: Personal Identification in networked Society, A.K. Jain, R. Bolle, and S. Pankanti, eds., Kluwer Academic, 1999.
[3] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. Springer, 2003.
[4] M. Indovina, U. Uludag, R. Snelick, A. Mink, and A. Jain, "Multimodal Biometric Authentication Methods: A COTS Approach,"
[5] R. Brunelli and D. Falavigna, "Person Identification Using Multiple Cues," IEEE Trans. Pattern Analysis and

Machine Intelligence, vol. 17, no. 10, pp. 955- 966, Oct. 1995.
[6] J. Kittler, M. Hatef, R.P.W. Duin, and J. Matas, "On Combining Classifiers," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 20, no. 3, pp. 226- 239, Mar. 1998.
[7] L. Hong and A.K. Jain, "Integrating Faces and Fingerprints for Personal Identification," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 20, no. 12, pp. 1295-1307, Dec. 1998.
[8] S. Ben-Yacoub, Y. Abdeljaoued, and E. Mayoraz, "Fusion of Face and Speech Data for Person Identity Verification," IEEE Trans. Neural Networks, vol. 10, no. 5, pp. 1065-1075, 1999.
[9] A. Ross and A.K. Jain, "Information Fusion in Biometrics," Pattern Recognition Letters, vol.24.
[10] P.J. Huber, Robust Statistics. Wiley, 1981.
[11] R. Auckenthaler, M. Carey and H. Lloyd-Thomas, "Score Normalization for Text- Independent Speaker Verification Systems," Digital Signal Processing, vol. 10, pp. 42-54, 2000.
[12] A.K. Jain and A. Ross, "Learning User-Specific Parameters in a Multibiometric System," Proc.IEEE Int'l Conf. Image Processing, pp. 57-60, Sept. 2002
[13] G. Doddington, W. Liggett, A. Martin, M. Przybocki, and D. Reynolds, "Sheeps, Goats, Lambs and Wolves: A Statistical Analysis of Speaker Performance in the NIST 1998 Speaker
Recognition Evaluation," Proc. ICSLD 98, Nov. 1998.