MULTI-BIOMETRIC SYSTEMS: SECURE SECURITY SYSTEMS

Rashmi Singhal *

Payal Jain *

ABSTRACT

Biometrics based user authentication techniques are used for automated recognition of individuals based on their physical or behavioral characteristics. A biometric is a unique and measurable characteristic of an individual like iris, face, signature, hand-geometry and retina. The fusion of multiple biometric characteristics in Multi-biometric systems provides the desired level of security. They combine information from multiple sources like multiple sensors, algorithms or traits and the presence of multiple sources of information makes them more reliable. In addition, they overcome various challenges encountered in mono-biometrics systems like: the problem of noisy data, non-universality, spoof-attacks, inter-class similarities and intra-class variations. Multi-biometric systems may be classified into following categories: multi-sensor systems, multi-algorithm systems, multi-instance systems, multi-sample systems, multi-modal systems and hybrid systems. The heart of any multi-biometric system is the fusion technique applied. There are various levels at which fusion can occur: sensor level, feature level, matching score level, rank level and decision level. In this paper we will present an overview of mono-biometric and multi-biometric systems, various types of multi-biometric systems employed, fusion techniques and their modes of operation.

* Lecturer, Department of Computer Science & Engineering, Maharishi Markandeshwar Engineering College, Maharishi Markandeshwar University, Mullana, Ambala, Haryana.

1. INTRODUCTION

Biometrics based user authentication techniques are used for automated recognition of individuals based on their physical or behavioral traits. A biometric is a unique and measurable characteristic of an individual like iris, face, signature, hand-geometry, and retina. Biometric authentication is more reliable as the physical traits of a human being are difficult to forge as compared to passwords or other security codes. Moreover, these traits do not change over time and need not be remembered for login purpose. A simple biometric system has following modules:

1. Enrollment Module.
   a. Sensor Module.
   b. Feature Extraction Module.
2. Matching Module.
3. Decision Module.

With the increasing need for more secure security systems, biometrics based user authentication is gaining enormous interest by science, industry and society [1]. Biometric systems that cover only a single biometric trait of an individual, known as mono-biometric systems, are generally unable to meet the stringent performance requirements as they suffer from many problems. To overcome these problems Multi-biometric authentication systems (MBAS) are used. Multi-biometric systems perform fusion of two or more mono-biometric systems. Here we present an overview of mono-biometric and multi-biometric systems, types of multi-biometric systems, their fusion techniques and operational modes.

2. MONO-BIOMETRIC versus MULTI-BIOMETRIC SYSTEMS

Mono-biometric systems use only a single biometric characteristic of an individual for verification or identification purpose. For example: fingerprints of a user may be used to allow him access to a secure zone or an iris scanner that scans the iris texture can be deployed at high security places. Similarly other biometric features like face, retina, voice, signatures or hand-geometry can also be used. Biometric systems that cover only a single biometric trait are generally unable to provide the desired performance requirements as they suffer from problems like: noisy-data, spoof attacks, non-universality, insufficient population coverage, and improper sensor adjustment. To overcome these difficulties multi-biometric systems are used.

Multi-biometric systems perform fusion of two or more mono-biometric systems. They perform user identification or authentication based on his/her two or more biometric traits.

Information's obtained from multiple sources like multiple sensors, algorithms or traits are combined to reach at final conclusion and the presence of these multiple sources of information makes them more reliable as compared to mono-biometric systems. Different multi-biometric systems use different combination methods and schemes. Following factors should be considered while selecting a suitable multi-biometric system [9]:

1. Nature of the application.
2. Methodology adopted.
3. The choice and number of biometric traits to be used.
4. The level at which information obtained through multiple traits should be integrated.
5. Cost versus performance trade-off.

C. Lupu and et al. in 2007 [2**]** used fingerprint, voice and iris recognition technologies to identify or verify a person who wants to access a car. Many other researchers proposed several multi-biometric systems that combine multiple different biometric characteristics for ensuring security.

3. ADVANTAGES OF MULTI-BIOMETRIC SYSTEMS OVER MONO-BIOMETRIC

Mono-biometric systems use only a single biometric trait and the unavailability of this trait may result in failure to enrollment. Presence of two or more biometric traits in multi-biometric systems helps overcome the following listed limitations of mono-biometric systems **[3].**

a) *Non-universality (insufficient population coverage)*: Multi-biometric systems follow universal approach by allowing the user to get enrolled with the system by using two or more options. If due to poor quality of a biometric trait, the biometric system is unable to extract some meaningful information from a sample, the user can use some other biometric trait for enrollment process.

b) *Noisy data*: A scar on a finger, voice distortion because of cold or improper illumination on face may result in poor quality of the sample collected. Data thus obtained May not sufficient to authenticate the user. Availability of some other biometric trait makes it possible to determine the identity of the user in such cases.

c) *Spoof-attacks*: Spoof attacks are the direct attacks at sensor level. These types of attacks are prominent while using behavioral traits like signature or voice. If we use iris, hand-geometry or retina as biometric traits (in combination with voice or signatures), it becomes difficult for the imposter to spoof them.

d) *Inter-class similarities*: In a biometric system having multiple users, there is a possibility of inter-class similarities in the feature sets used to represent these traits. The feature set of all the modalities cannot be same for all the users.

e) *Intra-user variation*: Intra-class variations occur when the data acquired during authentication process from an individual is different from the data used to create template earlier. Improper interaction with the sensor or changes made to the characteristics of a sensor may result in these variations.

Multimodal systems may be regarded as fault tolerant systems. They continue to operate even when some source of information gets corrupted.

4. TYPES OF MULTI-BIOMETRIC SYSTEM

The reliability of biometric systems is due to the presence of multiple sources of biometric information. Different multi-biometric systems use different combination methods and schemes in order to create a more precise system. Depending upon the types of sources used, multi-biometric systems may be classified into following categories [4]**:**

a) *Multi-Algorithm Systems*: A single biometric sample captured using a single sensor is processed using multiple different algorithms. The individual results produced are then fused using fusion strategies' to obtain the final recognition result. These systems are more economical as no extra sensor or any other device is required, but they are complex.

b) *Multi-Sensor Systems*: Multiple sensors are used to capture a single biometric trait of an individual. For example: an image of a fingerprint can be captured using an optical scanner as well as a capacitive fingerprint scanner. The information obtained using both the sensors are combined using sensor level fusion techniques. Use of multiple sensors results in the acquisition of complementary information that enhances recognition ability of the system [5**]**.

c) *Multi-Instance Systems:* Multiple instances of a single biometric trait are captured using a single sensor. For example: the left and right irises of an individual are captured, a single algorithm is then applied on them and the results obtained are then fused together.

d) *Multi*-Sample Systems: For example: the frontal profile of a person's profile can be captured along with the left and right profiles. The main issue here is to determine the number of samples to be captured so that a higher degree of variability and typicality is obtained. This approach has both advantages and disadvantages: one advantage is

that it is cost effective as only a single sensor device is required, secondly it can overcome the poor performance in case one of the sample is defected. One disadvantage is that a greater cooperation is required from the user side as multiple copies of the sensor have to be acquired.

e) *Multi-Modal Systems:* Two or more different biometric traits of a person are captured using different sensors. By combining physically uncorrelated biometric traits, the performance of the system is expected to increase. The number of biometric traits to be used is the biggest concern here. R. Zewail and et al. **[6]** in 2004 combined human iris color as a soft biometric with the output of a primary biometric system comprising of fingerprint and iris texture as hard biometrics. In 2006, S. Y. Kung and et al. **[7]** used both voice and facial images for biometric authentication

f) *Hybrid Systems:* The aforementioned different types of systems may be integrated. For example: after capturing both the left and right instances of iris, different algorithms are applied on them individually. The results obtained are then fused together. Such a system will be multi-instance and multi-algorithm system.

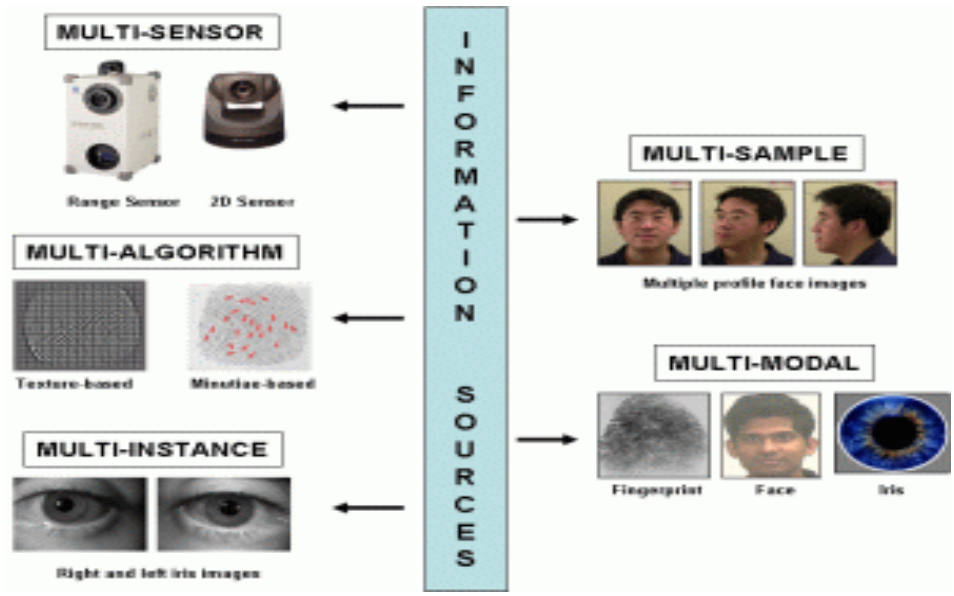

Figure 1: Types of Multi-Biometric System

5. FUSION TECHNIQUE'S

In a multi-biometric system fusion of information obtained through multiple sources is a major issue. Depending on how early the Information obtained using multiple sources is fused together in authentication process, following three types of fusion strategies are used [9]:

1. *Fusion at Feature Extraction level:* Feature sets extracted using multiple individual sensors are combined together to form a joint feature vector which is then passed to matching module. Information integrated at this stage provide better recognition results and is expected to be more effective as the feature set contains maximum information about the input biometric data. However, it does have some drawbacks: firstly, feature sets of different modalities may not be compatible and secondly, it is difficult to have access to different feature sets.
2. *Fusion at Matching Score level:* In first phase of enrollment module feature vectors are extracted from information obtained using independent sensors. In matching module, individual vector sets are compared with the already stored enrollment templates. Depending upon the similarity between these two, a matching score is generated for each subset. These individual matching scores are then integrated and the final integrated score is handed over to the decision module. Fusion at this level is generally preferred as it is easy to access and combine matching scores.
3. *Fusion at Decision Making Level:* In this strategy, separate authentication process is carried out for each biometric sample occupied. At last, the decisions taken by all biometric system are combined to reach at final result. Due to the availability of limited information in decision module this fusion strategy is considered to be rigid.

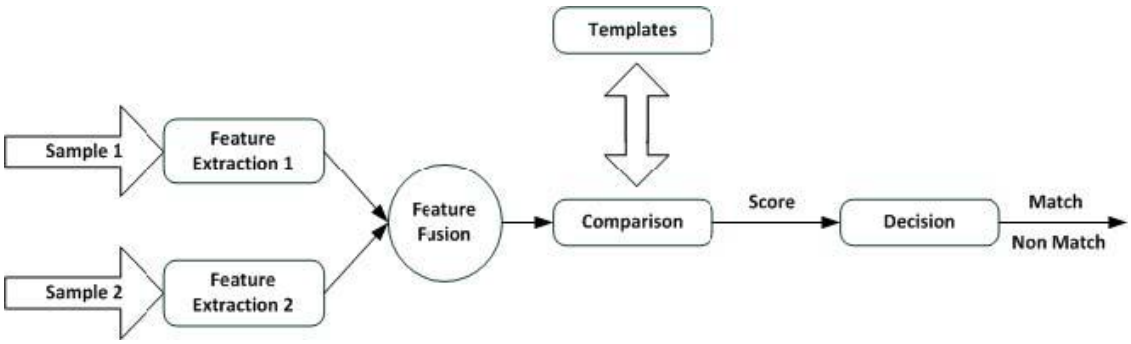

Figure 2: Fusion At Feature Extraction Level

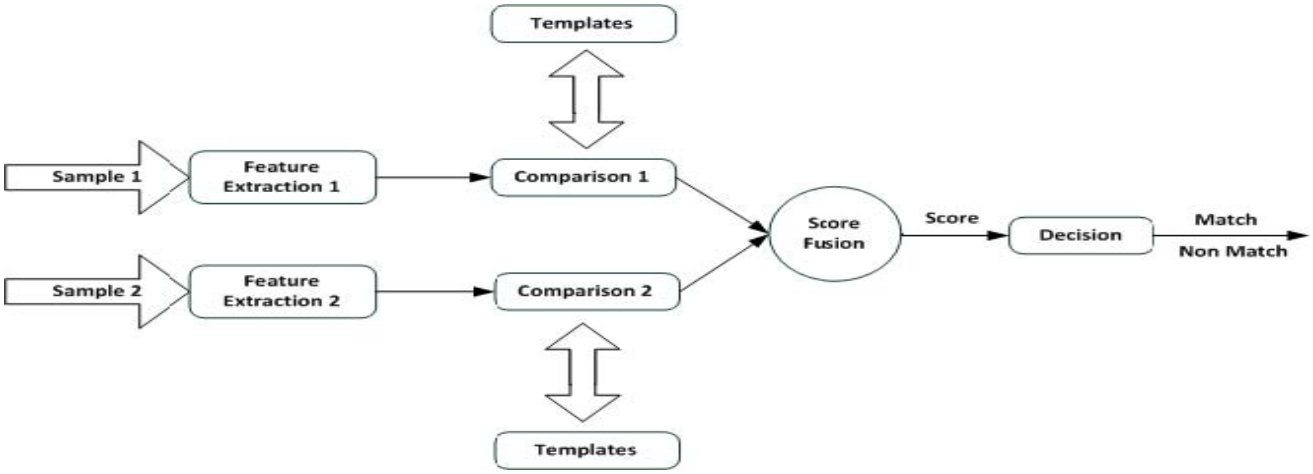

Figure 3: Fusion at Matching Score Level

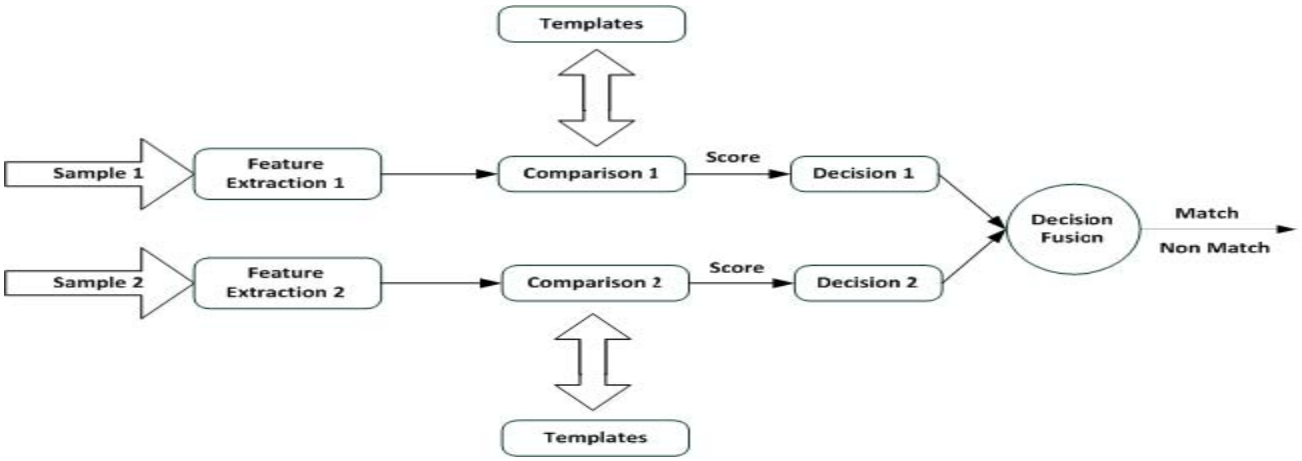

Figure 4: Fusion at Decision Level

6. OPERATIONAL MODES

Biometric system can operate in three modes [3]:

1. *Serial mode*: Multi-biometric systems use more than one biometric trait. If the output of one matching operation on one biometric source is sufficient to authenticate the user, no other biometric samples are processed further. In this mode a decision could be made before acquiring all the samples.
2. *Parallel mode*: Each biometric sample is simultaneously processed. The information's from these multiple modalities are used simultaneously to carry out the authentication process.
3. *Hierarchical mode*: In this mode, individual classifiers are arranged in a hierarchical structure, like a tree.

CONCLUSION

In this paper we presented main issues related to multi-biometric systems. By combining multiple sources of information, these systems address most of the problems encountered in

mono-biometric systems. They cover more population, are fault tolerant, deter spoofing attacks and provide more accurate results. Depending upon the nature of our application, we may choose a suitable multi-biometric system out of the available ones. Further, the performance of the system improves if two or more physically uncorrelated traits are used. Efficiency of a multi-biometric system is highly dependent on the fusion technique employed. Multi-biometrics based user authentication systems are now considered to be more secure security systems.

REFERENCES

1. "*Enhancing Security through a Hybrid Multibiometric System*", Md. Maruf Monwar, Marina L. Gavrilova, 2009 IEEE.
2. "*Multimodal Biometrics for Access Control in an Intelligent Car*", C. Lupu, V. Lupu, 2007 IEEE.
3. "*MULTIMODAL BIOMETRICS: An Overview*", Arun Ross and Anil K. Jain, Proceedings of EUSIPCO, September 2004.
4. "*Trends and Challenges in Mono and Multi biometrics*", Mohamed Deriche, 2008 IEEE.
5. "*An Introduction to Multi-Biometrics".* Arun Ross, EUSIPCO, September 2007.
6. "Soft *and Hard Biometrics Fusion for Improved Identity Verification",* R. Zewail, A. Elsafi, M. Saeb, N. Hamdy, 2004 IEEE.
7. "*On Consistent Fusion Of MultiModal Biometrics",* S.Y. Kung, Man-Wai Mak, 2006 IEEE.
8. "*Multibiometric Authentication, An Overview of Recent Developments",* Uwe M. Bubeck, Term Project, Spring 2003.
9. "*Multibiometric Systems Based Verification Technique",* Farhat Anwar, Md. Arafatur Rahman, European Journal of Scientific Research 2009.