Int. J. Chem. Sci.: 14(S3), 2016, 805-808
ISSN 0972-768X
www.sadgurupublications.com

MULTIBIOMETRIC SYSTEMS

P. SUBRAMANIAN*, K. NITHIN KRISHNA, RINKU MARYA SEBASTIAN and NAJEEB UR RAHMAN

ECE Department, Aarupadai Veedu Institute of Technology, CHENNAI (T.N.) INDIA

ABSTRACT

Biometrics is the measurement of biological characteristics which are unique to an individual for identifying and verifying the individual. The measurements include fingerprints, retinal scans, iris scans, voice patterns, facial characteristics, palmprints, etc.., Biometric systems have been very much successful in identifying an unknown individual by searching a database of characteristics and by verifying the claim of an individual by comparing his characteristic with that stored in a database. To increase the robustness of the system and to make it more secure, multiple characteristics of the same individual are used. This is referred to as multimodal biometrics. In this paper we review some of the multimodal biometric systems.

Key words: Biometrics, Multimodal biometrics, Biometric fusion.

INTRODUCTION

Identifying and verifying a person is vital in most secure applications. Traditional methods like ID card, passwords can be easily duplicated, lost or stolen[1]. Also these methods are useful for verification only and not for identification. To overcome these problems, biometric features like fingerprints, iris scan, face, gait, palmprint began to be used. These features led to the usage of biometric systems. In these systems any one biometric was used. But these single biometric systems also faced problems like noise in the sensed data, non-universality and susceptibility to circumvention[1]. Hence a new category of using two or more biometric features, called multimodal biometrics has been developed in the recent years.

Biometric systems

A biometric system operates on the basic principle of pattern recognition[2]. Feature vector derived from the specified characteristic of the individual is used[3,4]. Biometric systems using fingerprint recognition, iris recognition, hand geometry recognition, palmprint

*Author for correspondence; E-mail: subramanian@avit.ac.in

recognition, DNA fingerprinting, gait recognition, ear recognition, face recognition, voice recognition have been discussed in the literature. A biometric system involves the stages of enrollment, verification and identification. A good biometric system should possess the qualities like universality, uniqueness, permanence, collectability, acceptability and circumvention. The performance of a biometric system is evaluated by means of parameters including.

(a) False Rejection Rate: the probability of a true user being falsely rejected,

(b) False Acceptance Rate: the probability that a false user is accepted.

A system that uses a single characteristic is called a unimodal biometric system. Every such system has its own drawbacks[5,6] including.

(a) Noise in sensed data – for example smudges in fingerprint during acquisition, user having cold while acquiring voice print, insufficient lighting while acquiring facial images,

(b) Intra class variations – caused by incorrect interaction with the sensors like wrong facial pose,

(c) Inter class similarities – that can occur in a system with large number of users,

(d) Non universality – some characteristics might not be clearly available in certain individuals, and

(e) Spoof attacks.

These drawbacks can be mitigated by combining two or more uni-modal biometrics to get a multi-biometric system[6].

Multibiometrics

Multibiometric systems have been introduced with the aim of reducing the FAR and/or FRR and to avoid spoof attacks[7]. These systems consider inputs from single or multiple sensors. Multi algorithmic biometric systems use two or more algorithms for processing a single sample of a single sensor. Multi-instance biometric systems process use two or more different instances of the same biometric characteristics like multiple fingerprints of the same person. Multisensorial biometric systems use two or more distinctly different sensors to process the same characteristic. Multimodal biometrics process two or more biometric characteristics of the same individual. Different combinations of the biometric characteristics of the same individual can be used.

Biometric fusion

Biometric fusion is the process of combining the classification results of each biometric channel. Fusion can occur at different levels namely matching score level, sensor level, feature level, rank level and decision level[7]. In sensor level fusion biometric traits taken from different sensors are combined to form a single composite trait. In feature level fusion, feature vectors of different biometrics are combined to form a single feature vector. In matching score level fusion, individual matching scores are found and a decision is made of the score to be used for classification or verification. In decision level fusion individual biometrics are used to make individual decisions and then a combined decision is arrived at.

Architecture of a multibiometric system

In a Multibiometric system, the sequence in which the individual biometrics are acquired and processed, determines the architecture of the system. In serial architecture, the result of one modality affects the subsequent modalities[6]. The overall time required for recognition is reduced since the output of first modality determines the subsequent traits to be observed[5]. Since the output of one modality is used to narrow down the number of possible identities before the next modality [15]. In parallel architecture, the individual modalities are processed individually and the results are combined[6].

CONCLUSION

Biometric systems are the mainstay of today's security systems. From unimodal biometric systems we have moved on to Multibiometric systems for improved security. The use of multibiometric systems has led to research in the use of several techniques for fusion of biometric characteristics like fuzzy logic and other soft computing techniques.

REFERENCES

1. Mohit Agarwal, Design Approaches for Multimodal Biometric Systems, Ph.D. Thesis, IIT Kanpur, India (2007).
2. M. Soltane and M. Bakhti, Multi-Modal Biometric Authentications: Concept Issues and Applications Strategies, Int. J. Adv. Sci. Technol., **48** (2012).
3. S. Prabhakar, S. Pankanti and A. K. Jain, Biometric Recognition: Security and Privacy Concerns, IEEE Security & Privacy Magazine, March-April, **1(2)**, 33-42 (2003).

4. A. K. Jain, A. Ross and S. Prabhakar, An Introduction to Biometric Recognition, IEEE Transactions on Circuits and Systems for Video Technology, January, **14(1)** (2004).

5. A. Ross and A. K. Jain, Multimodal Biometrics: An Overview, Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), 1221-1224 (2004).

6. M. Abdolahi et al, Multimodal Biometric System Fusion Using Fingerprint and Iris with Fuzzy Logic, Int. J. Soft Comput. Engg., **2(6)**, 2231-2307 (2013).

7. K. Sasidhar et al., Multimodal Biometric Systems – Study to Improve Accuracy and Performance, Int. J. Comput. Sci. Engg. Survey, **1(2)** (2010).

Accepted : 11.10.2016