Chapter 4
Multimodal Biometric System and Information Fusion

ABSTRACT
Integrating different information originating from different sources, known as information fusion, is one of the main factors of designing a biometric system involving more than one biometric source. In this chapter, various information fusion techniques in the context of multimodal biometric systems are discussed. Usually, the information in a multimodal biometric system can be combined in sensor level, feature extraction level, match score level, rank level, and decision level. There is also another emerging fusion method, which is becoming popular—the fuzzy fusion. Fuzzy fusion deals with the quality of the inputs or with the quality of any system components. This chapter discusses the associated challenges related to making the choice of appropriate fusion method for the application domain, to balance between fully automated versus user defined operational parameters of the system and to take the decision on governing rules and weight assignment for fuzzy fusion.

1. INTRODUCTION
The optimal biometric system is one having the properties of distinctiveness, universality, permanence, acceptability, collectability, and security. As we saw in the introductory chapters, no existing biometric security system simultaneously meets all of these requirements. Despite tremendous progress in the field, over the last decades researchers noticed that while a single biometric trait might not always satisfy secure system requirements, the combination of traits from different biometrics will do the job. The key is in aggregation of data and intelligent decision making based on responses received from individual (unimodal) biometric systems.
Thus, Multimodal biometrics emerged as a new and highly promising approach to biometric knowledge representation, which strives to overcome problems of individual biometric matchers by consolidating the evidence presented by multiple biometric traits (Ross, Nandukamar, & Jain, 2006). As an example, a multimodal system may use both face recognition and signature to authenticate a person. Due to reliable and efficient security solutions in the security critical applications, multimodal biometric systems have evolved over last decade as a viable alternative to the traditional unimodal security systems.

2. ADVANTAGES OF MULTIMODAL BIOMETRIC SYSTEM

The advantages of multimodal biometric systems over unimodal systems are mainly due to utilization of more than one information source. Figure 1 shows a sample multimodal biometric system. The most prominent implications of this are increased and reliable recognition performance, fewer enrolment problems, and enhanced security (Ross & Jain, 2004).

2.1. Increased and Reliable Recognition Performance

A multimodal system allows for a greater level of assurance of a proper match in verification and identification modes (Hong & Jain, 1998). As multimodal biometric systems use more than one biometric trait, each of those traits can offer additional evidence about the authenticity of any identity claim. For example, the gaits (the patterns of movements) of two persons of the same family (or coincidentally of two different persons) can be similar. In this scenario, a unimodal biometric system based only on gait pattern analysis may results in false recognition. If the same biometric system also includes fingerprint matching, the system would results in increased recognition rate, as it is very unlikely that two different persons have same gait and fingerprint patterns.

Another example of increased and reliable recognition performance of multimodal biometric systems is ability to effectively handle the noisy or poor quality data. When the biometric information acquired from a single trait is not reliable due to noise, the availability of other trait allows the system to still perform in a secure manner. For example, in a face and voice-based multimodal biometric system, due to noise, if the individual’s voice signals cannot be accurately measured, the facial characteristics may be used for authentication.

2.2. Fewer Enrolment Problems

Multimodal biometric systems address the problem of non-universality or the insufficient population coverage, where a portion of a population has a biometric characteristic that is missing or not suitable for recognition, and thus reduce the failure to enroll rate significantly (Frischholz & Dieckmann, 2000). Depending on the system design, many multimodal biometric systems can perform matching even in the absence of one of the biometric samples. For example, in a fingerprint and face based multimodal system, a person (who is a carpenter) cannot enroll his fingerprint information to the system due to the scars in his fingerprints. In this case, the multimodal system can still perform authentication using the facial characteristics of that person. Moreover, if certain features can be extracted from fingerprint (but not all due to damage to the finger), then these features still can be sued to increase accuracy rate or confidence level of the final decision.

2.3. Enhanced Security

Multimodal biometric systems make it more difficult for an impostor to spoof biometric traits of