Chapter XII
From Single Biometrics to Multi-Biometrics

ABSTRACT

In the past decades while biometrics attracts increasing attention of researchers, people also have found that the biometric system using a single biometric trait may not satisfy the demand of some real-world applications. Diversity of biometric traits also means that they may have different performance such as accuracy and reliability. Multi-biometric applications emerging in recent years are a big progress of biometrics. They can overcome some shortcomings of the single biometric system and can perform well in improving the system performance. In this chapter we describe a number of definitions on biometrics, categories and fusion strategies of multi-biometrics as well as the performance evaluation on the biometric system. The first section of this chapter describes some concepts, motivation and justification of multi-biometrics. Section 12.2 provides some definitions and notations of biometric and multi-biometric technologies. Section 12.3 is mainly related to performance evaluation of various types of biometric systems. Section 12.4 briefly presents research and development of multi-biometrics.

12. 1 INTRODUCTION

As mentioned in previous chapters, biometric technologies play an important role in access control and other systems that depend on secure personal authentication.

The fact that biometrics may possess excellent properties such as universality (every person has biometric traits), uniqueness (generally, no two people have identical biometric traits), permanence (most biometric traits do not vary over time), collectability (biometric traits can be measured quantitatively) and good performance (biometric technologies can achieve accurate results under varied environmental circumstances) (Ross & Jain, 2004; Jain, Ross, & Prabhakar, 2004) provides a solid base for these systems. Indeed, biometric technology is a methodology to achieve fast, user-friendly authentication with high accuracy. As mentioned in Chapter I, compared with biometric systems, traditional security systems, such as passwords or tokens-based methods, have some serious disadvantages.

Biometric technologies have many applications (Jain, Bolle, & Pankanti, 1999; Zhang & Jain (Eds.), 2006; Wayman, 2001; Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Herzog & Reithiger, 2006; Jain & Ross, 2004; Jain, 2003). Biometrics can be incorporated in solutions to provide for Homeland Security including applications for improving airport security, strengthening border management control, in visas and in preventing ID theft. Biometrics can be also applied to secure electronic banking, investing and other financial transactions, enterprise-wide network security infrastructures, retail sales, law enforcement, and health and social services. Biometrics can also be integrated with other technologies such as encryption keys or smart cards to produce a hybrid security system. This way of exploiting biometrics is also called two-factor authentication, please refer to web site (http://www.answers.com/topic/two-factor-authentication). As shown in Chapter I, biometric applications can be categorized into several categories.

Varieties of biometric traits can be individually applied for personal authentication (Zhang, Jing, & Yang, 2005; Zhang & Jain (Eds.), 2004; Zhang, 2004); however, the biometric system using a single biometric trait usually suffers from some problems such as unsatisfactory accuracy, spoof attacks, and restricted degrees of freedom (Bubeck, 2003). For example, manual workers with damaged or dirty hands may not be able to provide high-quality fingerprint images. In this case, fingerprint authentication seems not to be a good means for authenticating personal identity. For an iris identification system, the existing registration failure risk would reduce the reliability of the system. For a biometric system using speech, some factors, such as ambient noise, changes in behavioral attributes of the voice, and voice change due to aging, will affect the system's performance. For a biometric system using face images, some challenges, such as variations in facial expression, pose and lighting, will limit the system's performance. One's keystroke trait and signature trait may vary to some extent and also bring side effects into the single biometric system using keystrokes or signature traits. All these examples imply that the single biometric system may not be guaranteed to provide a high accuracy.