IDEA GROUP PUBLISHING **ITB12296**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This paper appears in the publication, *Biometric Image Discrimination Technologies*
by David Zhang, Xiaoyuan Jing, and Jian Yang © 2006, Idea Group Inc.

Chapter I

An Introduction to Biometrics Image Discrimination (BID)

ABSTRACT

In this chapter, we briefly introduce biometrics image discrimination (BID) technologies. First, we define and describe types of biometrics and biometrics technologies. Then, some applications of biometrics are given. The next section discusses biometrics systems and discrimination technologies, followed by a definition of BID technologies. The history and development of BID technologies is offered, and an overview and taxonomy of appearance-based BID technologies, respectively, is provided. Finally, the last section highlights each chapter of this book.

DEFINITION OF BIOMETRICS TECHNOLOGIES

Biometrics image discrimination (BID) is a field of biometrics, the statistical analysis of biological characteristics. A common interest in biometrics is technologies that automatically recognize or verify individual identities using a measurable physiological or behavioral characteristic (Jain, Bolle, & Pankanti, 1999; Zhang, 2000a, 2000b). Physiological characteristics might include facial features, thermal emissions, features of the eye (e.g., retina and iris), fingerprints, palmprints, hand geometry, skin pores or veins in the wrists or hand. Behavioral characteristics include activities and their artefacts, such as handwritten signatures, keystrokes or typing, voiceprints, gaits and gestures.

Biometrics lays the foundation for an extensive array of highly secure authentication and reliable personal verification (or identification) solutions. The first commercial biometrics system, Identimat, was developed in the 1970s as part of an employee time clock at Shearson Hamill, a Wall Street investment firm (Miller, 1994). It measured the shape of the hand and the lengths of the fingers. At the same time, fingerprint-based automatic checking systems were widely used in law enforcement by the FBI and by United States (U.S.) government departments. Advances in hardware, such as faster processing power and greater memory capacity, made biometrics more viable. Since the 1990s, iris, retina, face, voice, palmprint, signature and DNA technologies have joined the biometrics family (Jain, Bolle, & Pankanti, 1999; Zhang, 2000b).

Rapid progress in electronics and Internet commerce has made more urgent need for secure transaction processing using biometrics technology. After the September 11, 2001 (9/11) terrorist attacks, the interest in biometrics-based security solutions and applications increased dramatically, especially in the need to identify individuals in crowds. Some airlines have implemented iris recognition technology in airplane control rooms to prevent entry by unauthorized persons. In 2004, all Australian international airports will implement passports using face recognition technology for airline crews, and this will eventually become available to all Australian passport holders (Zhang, 2004). As the costs, opportunities and threats of security breaches and transaction fraud increase, so does the need for highly secure identification and personal verification technologies.

The major biometrics technologies involve finger scan, voice scan, facial scan, palm scan, iris scan and signature scan, as well as integrated authentication technologies (Zhang, 2002a).

Finger-Scan Technology

Finger-scan biometrics is based on the distinctive characteristics of a human fingerprint. A fingerprint image is read from a capture device, the features are extracted from the image and a template is created. If appropriate precautions are followed, the result is a very accurate means of authentication. Fingerprint matching techniques can be placed into two categories: minutiae-based and correlation-based. Minutiae-based techniques first find minutiae points and then map their relative placements on the finger. However, there are some difficulties with this approach when the fingerprint image is of a low quality, because accurate extraction of minutiae points is difficult. Nor does this method take into account the global pattern of ridges and furrows. Correlation-based methods are able to overcome the problems of a minutiae-based approach. However, correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation. Fingerprint verification may be a good choice for in-house systems that operate in a controlled environment, where users can be given adequate training. It is not surprising that the workstation access application area seems to be based almost exclusively on fingerprints, due to the relatively low cost, small size and ease of integration of fingerprint authentication devices.

Voice-Scan Technology

Of all the human traits used in biometrics, the one that humans learn to recognize first is the voice. Speech recognition systems can be divided into two categories: text-