Chapter VIII
Biometrics:
In Search of a Foolproof Solution

BIOMETRIC TECHNOLOGY

Historical Overview

Manual Biometrics

Biometrics is not only considered a more secure way to identify an individual but also a more convenient technique whereby the individual does not necessarily have to carry an additional device, such as an ID card. As defined by the Association for Biometrics (AFB) a biometric is "...a measurable, unique physical characteristic or personal trait to recognize the identity, or verify the claimed identity, of an enrollee." The technique is not a recent discovery. There is evidence to suggest that fingerprinting was used by the ancient Assyrians and Chinese at least since 7000 to 6000 BC (O'Gorman, 1999, p. 44). Over a thousand years ago, potters in East Asia, placed their fingerprints on their wares as an early form of brand identity and in Egypt's Nile Valley, merchants were identified by their physical characteristics (Raina, Woodward & Orlans, 2002, p. 25). The practice of using fingerprints in place of signatures for legal contracts is hundreds of years old (Shen & Khanna, 1997 p. 1364). It is believed that the first scientific studies investigating fingerprints were conducted some time in the late sixteenth century (Lee & Gaensslen, 1994).

In the nineteenth century Alphonse Bertillon in France developed anthropometrics as well as noting peculiar marks on a person such as scars or tattoos. It was as early as 1901 that Scotland Yard introduced the Galton-Henry system of fingerprint classification (Halici, L.C. Jain, Erol, 1999, p. 4; Fuller et al. 1995, p. 14). Since that time fingerprints have traditionally been used in law enforcement. As early as 1960, the FBI Home Office in the UK and the Paris Police Department began auto-ID fingerprint studies (Halici, L.C. Jain, Erol, 1999, p. 5). Until then limitations in computing power and storage had prevented automated biometric checking systems from reaching their potential. Yet it was not until the late 1980s when personal computers and optical scanners became more affordable that automated biometric checking had an opportunity to establish itself as an alternative to smart card or magnetic-stripe auto-ID technology.

Background

According to Parks (1990, p. 99), the personal traits that can be used for identification include: facial features, full face and profile, fingerprints, palmprints, footprints, hand geometry, ear (pinna) shape, retinal blood vessels, striation of the iris, surface blood vessels (e.g., in the wrist), electrocardiac waveforms. Withers (2002), Jain, A. et al. (1999), Lockie (2000), Ferrari et al. (1998, p. 23) and Hawkes (1992, p. 6/4) provide good overviews of various biometric types. Keeping in mind that the aforementioned list is not exhaustive, it is impressive to consider that a human being or animal can be uniquely identified in so many different ways. Unique identification, as Zoreda and Oton (1994, p. 165) point out, is only a matter of measuring a permanent biological trait whose variability exceeds the population size where it will be applied. As a rule however, human physiological or behavioral characteristics must satisfy the following requirements as outlined by Jain et al. (1997, pp. 1365f):

- **Universality:** Every person should possess that characteristic
- **Uniqueness:** No two persons should have the same pattern in terms of that characteristic
- **Permanence:** The characteristics should not change over time (i.e. invariance)
- **Collectability:** The characteristic should be quantifiably measurable.

The four most commonly used physiological biometrics include, face, fingerprint, hand geometry and iris while the two most common behavioral biometrics are signature and voice recognition. Other examples of biometric types include DNA (deoxyribonucleic acid), ear shape, odor, retina, skin reflectance, thermogram, gait, keystroke, and lip motion (Bolle et al., 2007, p. 7; Greening, Kumar, Leedham, 1995, pp. 272-278). Even the Electroencephalogram (EEG) can be used as a biometric as proven by Paranjape et al. (2001, pp. 1363-1366). Most of these techniques satisfy the following practical requirements (Jain et al., 1997, p. 1366):

- **Performance:** Refers to whether or not the identifier is accurate, there are technical resources able to capture and process that identifier, and whether there are environmental factors which impact negatively on the decision policy outcome
- **Acceptability:** Addresses whether or not people are willing to use the system
- **Circumvention:** Refers to how easily a system may be duped.

The Biometric System

Independent of which biometric identifier is under consideration for a given application, they are all viewed as automated pattern recognition systems. Typically a biometric system includes a biometric reader, feature extractor and feature matcher. Biometric readers act as sensors, feature extractors take the input signals and compute those special attributes that are unique, and feature matchers compare biometric features attempting to find a match. Typically a biometric authentication system consists of an enrollment subsystem, an authentication subsystem, and database.