Chapter 57
Biometric Security

Muzhir Shaban Al-Ani
Anbar University, Iraq

ABSTRACT

The terms biometrics and biometry have been used to refer to the field of development of statistical and mathematical methods applicable to data analysis problems in the biological sciences. Recently biometrics refers to technologies and applications applied for personal identification using physical and behavioral parameters. Biometric security systems ensuring that only the authorized persons are permitted to access a certain data, because it is difficult to copy the biometric features pattern for a specific person. Biometrics is playing an important role in applications that are centric on identification, verification and classification. This chapter focuses on biometric security in their types, specifications, technologies and algorithms. Some algorithms of biometric security are also included in this chapter. Finally latest and future aspects of biometric system and merging technologies are also mentioned, including more details of system structures and specifications and what constitution will shape biometric security of in the future.

INTRODUCTION

Biometrics technology is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze the characteristics of human body, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for identification and authentication purposes.

The oldest effective characteristic that is used for recognition by humans is the face. Since the beginning of civilization, humans have used faces to identify objects and individuals. Other characteristics have also been used for individual recognition such as fingerprint, footprint …etc. True biometric systems began to appear in the latter half of the twentieth century, by the time of the growth of computer systems. This field experienced and explosion of activity in the 1990s and began to surface in everyday applications in the early 2000s.

Information security is concerned with the assurance of confidentiality, integrity and availability of information in all forms. Many tools and techniques can support the management of information security. But biometric authentication system has evolved to support some aspects of information security.

DOI: 10.4018/978-1-5225-0983-7.ch057

Biometric authentication supports the directions of identification, authentication and non-repudiation in information security.

A biometric is a general term used to describe a measurable physiological and/or behavioral characteristic that can be applied for automated recognition. A biometric system provides an automated method of person is recognizing based on the individual's biometric characteristics. Biometric modalities commonly implemented or studied biometrics patterns include fingerprint, face, iris, voice, signature, vein pattern, and hand geometry. Many other modalities are implemented in various stages of development and assessment (Ross et al, 2006).

Now a days the combination of biometrics and security leads to highlighting of a new modern field with huge application in everyday life. This chapter will concentrate on the theory and applications of using biometrics in security that is stronger in the merging of these two fields to generate new more applicable secure systems.

BACKGROUND OF BIOMETRIC SECURITY

Biometrics as a Key of Security

Biometrics technology is not a new concept; it is the oldest form of identification. As early as the 14th century, the Chinese were reportedly using fingerprint-like methods as a method of identifying of their children.

There are three basic, independent but related concepts of security (Jain et al, 1999):

- **Concept of Identification:** Who you are.
- **Concept of Authentication:** Proving whom you are.
- **Concept of Authorization:** What you are allowed to do.

Recently, huge data transfer all over the word every day, therefore identity theft and the loss of data and related intellectual property are growing problems. Now each have multiple accounts and use multiple passwords on an ever-increasing number of computers and Web sites. Maintaining and managing access while protecting both the user's identity and the computer's data and systems has become increasingly difficult. Security is the concept of authentication - verifying that the user is who he claims to be. Biometric based authentication applications refer to three types of authentication (Delac & Grgic, 2004).

- Something you know (most common used is a password or pin)
- Something you have (tokens such as a smart card), and finally
- Something you are (such as biometric).

Requirements for the Biometric Characteristic

In the development of biometric authentication systems, physical and behavioral characteristics for recognition are required many factors (Goswami & Chan, 2011; Scott & Nowak, 2004):