biometric

Ayman keshk

March 28, 2017

Contents

Preface

Security and privacy of our personal information and data are? classified as the most important thing

in our life nowadays, that is why we turned to secure our information and data with high level security

using biometrics

Biometrics is concerned with identifying a person based on his or her physiological or behavioral characteristics.

Examples of biometrics systems include fingerprint, hand vein, face, eye (iris or retina), and speech recognition.

The term biometrics is derived from the Greek words bio (life) and metrics (to measure).

Automated biometric systems have only become available over the last few decades,

due to significant advances in the field of computer processing. Many of these new automated techniques,

however, are based on ideas that were originally conceived hundreds, even thousands of years ago.

What are biometric systems used for?

Reliable user authentication is essential. The consequences of insecure authentication in a banking or corporate environment can be catastrophic, with loss of confidential information, money, and compromised data integrity. Many applications in everyday life also require user authentication, including physical access control to offices or buildings, e-commerce, healthcare, immigration and border control, etc.

Currently, the prevailing techniques of user authentication are linked to passwords, user IDs, identification cards and PINs (personal identification numbers). These techniques suffer from several limitations: Passwords and PINs can be guessed, stolen or illicitly acquired by covert observation.

In addition, there is no way to positively link the usage of the system or service to the actual user. A password can be shared, and there is no way for the system to know who the actual user is. A credit card transaction can only validate the credit card number and the PIN, not if the transaction is conducted by the rightful owner of the credit card.

This is where biometrics systems provide a more accurate and reliable user authentication method, as can be summarised in the table underneath:

Why are biometrics secure?

Unique: The various biometrics systems have been developed around unique characteristics of individuals. The probability of 2 people sharing the same biometric data is virtually nil.

Cannot be shared: Because a biometric property is an intrinsic property of an individual, it is extremely difficult to duplicate or share (you cannot give a copy of your face or your hand to someone!).

Cannot be copied: Biometric characteristics are nearly impossible to forge or spoof, especially with new technologies ensuring that the biometric being identified is from a live person.

Cannot be lost: A biometric property of an individual can be lost only in case of serious accident.

Chapter 1

physiological

1.1 Face

1.2 Fingerprint

1.3 Hand

1.4 Iris

1.5 DNA

Chapter 2

behavioral

2.1 keystroke

2.2 signature

2.3 Voice