Chapter 3
ECG-Based Biometrics

Swanirbhar Majumder
NERIST (Deemed University), India

Saurabh Pal
University of Calcutta, India

ABSTRACT

Like all human beings have different fingerprints, they have differently shaped hearts. The ECG, or the electrocardiogram, is the signature of the movements by the human heart, and thus, all ECGs are different. ECG biometrics is an area of biometric identification by the usage of the ECG features in time or frequency/transform domain. Along with these, if the present-day cloud servers also come to play, one has an efficient and cost-effective ECG-based biometric system using cloud computing to provide real-time identification via a secure connection. This chapter focuses on ECG-based biometrics with an overview at the end about how cloud-based big databases of stored ECG signatures and cloud servers can play a part in it.

INTRODUCTION

In recent years, advancement in computing and digital signal processing technologies are achieved that enable automatic identification of individual based on their biological, physiological or behavioural traits. The technologies have also increased the number of traits that can be collected and used to identify people and to control access to resources. Systems that use any biological, physiological or behavioural trait to grant access to resources are called biometric systems.

Biometrics has recently become a popular research area because of the critical validation of the identity in several aspects such as financial transactions, access control, travelling and other. Biometrics is defined as the automatic identification of a person based on the physiological/behavioural characteristics of the individual. The word biometrics originates from two Greek words ‘bios’ and ‘metron’. The meaning of bios is life and the meaning of metron is measure i.e. biometrics is the measure of trait i.e. a distinguishing feature or characteristics of living beings. A biometrics is also called as biometrics authentication and this is so called because an authentication system is based on three measures:

DOI: 10.4018/978-1-5225-0983-7.ch003

- What you know-i.e. a password;
- What you have-i.e. a token or credit card, debit card, pass card;
- What you are-i.e. biometrics.

This method of identification is preferred for various reasons; the person to be identified is required to be physically present at the point of identification; identification based on biometric techniques obviates the need to remember a password or carry a token. With the increased use of computers or vehicles of information technology, it is necessary to restrict access to sensitive or personal data. By replacing PINs, biometric techniques can potentially prevent unauthorized access to fraudulent use of ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. PINs and passwords may be forgotten, and token based methods of identification like passports and driver's licenses may be forged, stolen, or lost.Thus biometric systems of identification are enjoying a renewed interest.

Biometrics is rapidly evolving technology, which is being used in forensics such as criminal identification and prison security, and has the potential to be used in a large range of civilian application areas. Biometrics can be used transactions conducted via telephone and Internet (electronic commerce and electronic banking). In automobiles, biometrics can replace keys with key -less entry devices.

Biometrics dates back to the ancient Egyptians, who measured people to identity them. But automated devices appeared within living memory. One of the first commercial devices introduced less than 30 years ago. The system is called the indentimat. The machine measured finger length and installed in a time keeping system. Biometrics is also catching on computer and communication system as well as automated teller machines (ATM's).

Biometrics devices have three primary components. One is an automated mechanism that scans and captures a digital / analog image of living personal characteristics. Another handles compression, processing, storage and comparison of image with the stored data. The third interfaces with application systems. These pieces may be configured to suit different situations. A common issue is where the stored image resides: on a card, presented by the person being verified or at a host computer.

Recognition occurs when an individual's image is matched with one of a group of stored images. This is the way the human brain performs most day to day identifications. For the brain this is a relatively quick and efficient process, where as for computers to recognise that a living image matches one of many it has stored, the job can be time consuming and costly.

There are different types biometrics modalities such as fingerprint recognition, voice recognition, speech recognition, ECG biometrics etc. The ECG biometrics is an advance and more recent biometric technology. ECG biometric can be defined as the identification of human by using the characteristics of ECG signal. Since ECG is only present in a living object, it represents the liveliness detection and therefore according to paper (Odinaka, 2010), it can be said as that ECG signals cannot be copied i.e. mimic is not possible in case of ECG signal.

The unique property in case of an ECG biometrics is that it can be used as a multi-biometrics approach. In this approach, the role of ECG is interesting either as a security enhancement layer in hard biometrics system, or as a standalone soft biometrics for low security and low user throughput applications.

The ECG signal is composed of P wave, QRS complex and T wave. This ECG signal has some fiducial features as well some non fiducial features. Characteristic points to be the actual points located on an ECG trace and fiducial features to be the features that are derived from these characteristic points.

Since ECG biometric is used for identification purpose, the primary work is to extract the features from an ECG signal. There are various techniques have been proposed by scholars for the extraction of