Chapter 15
Real-Time ECG-Based Biometric Authentication System

Jagannath Mohan
VIT Chennai, India

Adalarasu Kanagasabai
SASTRA University (Deemed), India

Vetrivelan Pandu
VIT Chennai, India

ABSTRACT

Security plays an important role in present day situation where identity fraud and terrorism pose a great threat. Recognizing human using computers or any artificial systems not only affords some efficient security outcomes but also facilitates human services, especially in the zone of conflict. In the recent decade, the demand for improvement in security for personal data storage has grown rapidly, and among the potential alternatives, it is one that employs innovative biometric identification techniques. Amongst these behavioral biometric techniques, the electrocardiogram (ECG) is being chosen as a physiological modality due to the uniqueness of its characteristics which integrates liveness detection, significantly preventing spoof attacks. The chapter discusses the overview of existing preprocessing, feature extraction, and classification methods for ECG-based biometric authentication. The proposed system is intended to develop applications for real-time authentication.

DOI: 10.4018/978-1-5225-8241-0.ch015

INTRODUCTION

Biometric advances offer superior security systems over conventional authentication techniques, similar to secret word based ones, given the way that the biometric highlight could be a special physiological characteristic that continuously shows and, contingent upon the strategy utilized, may not be obvious to other individuals. In any case, one concern is that a few biometric strategies have certain equipment and reaction time prerequisites that make them improper for portable gadgets and cards (Boriev et al., 2015).

Finger impression may be a prevalent biometric method and has been utilized for over 100 a long time completely different applications, counting authentication on cell phones. The utilization of cards for monetary exchanges or secure get to has gotten to be irreplaceable within a recent couple of decades. This prominence has to been gone with by security concerns. Conventional cards don't bolster authentication and thus are not unequivocally related to their proprietor. Money related educate have attempted to address this issue through the presentation of PINs (Individual Confirmation Numbers) and incorporated circuits on cards. These highlights stay as it were valuable for contact cards. This has diminished the number of breaches, but detached assaults (Stick burglary or signature producing) are as yet hazardous (Poree et al., 2016).

Portable gadgets such as smartphones and PDAs have turned out to be crucial contraptions for various capacities. Clients are ending up more comfortable with putting away profoundly private data, for example, messages, photographs, and other delicate records on such gadgets. The well-known versatile login strategies depend on numerical or graphical secret codes. These systems are helpless against uninvolved assaults actuated by people observing from a distance to see the gadget screen or the tracking of the fingers with the objective of taking the secret code (Miakotko, 2017).

Conventional authentication has demerits as they can be spoofed by an assailant that captures the personality cleared out by clients on security. This has been illustrated with commercial frameworks that utilize finger impression authentication (Joy et al., 2016). Electrocardiogram (denoted to as ECG or EKG) techniques have the benefits of concealing the biometric highlights during authentication. Electrocardiography records the electrical activity of the heart over a specific timeframe with the help of electrodes placed on the human body (Biel et al., 2001). The electrodes locate the modest electrical changes from the body by heartbeats produced by the heart. There are three fundamental segments to an ECG (Louis et al., 2016). To begin with is the P wave, which acts the depolarization of atria, second is the QRS complex which acts the ventricular depolarization and final is T wave, which appears the