Journal of Network and Computer Applications 34 (2011) 282–293

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Faster person identification using compressed ECG in time critical wireless telecardiology applications

Fahim Sufi *, Ibrahim Khalil

CS & IT, RMIT University, Melbourne, Vic. 3000, Australia

ARTICLE INFO

Article history:
Received 23 December 2009
Accepted 8 July 2010

Keywords:
ECG biometric
ECG compression
Cardiac patient authentication
ECG based human identification

ABSTRACT

Adoption of compression technology is often required for wireless cardiovascular monitoring, due to the enormous size of electrocardiogram (ECG) signal and limited bandwidth of Internet. However, compressed ECG must be decompressed before performing human identification using present research on ECG based biometric techniques. This additional step of decompression creates a significant processing delay for identification task. This becomes an obvious burden on a system if this needs to be done for millions of compressed ECG segments by the hospital. This paper proposes a novel method of ECG biometric directly form compressed ECG harnessing data mining (DM) techniques like attribute selection and clustering. The biometric template created by this new technique is lower in size compared to the existing ECG based biometrics as well as other forms of biometrics like face, finger, retina, etc. The template size (and also the matching time) is up to 8533 times lower than face template, 61 times lower than existing percentage root mean square (PRD) ECG based biometric template and 9 times smaller than polynomial distance measurement (PDM) based ECG biometric. Smaller template size substantially reduces the one to many matching time for biometric recognition, resulting in a faster biometric authentication mechanism and ECG stream verification directly from compressed ECG.

1. Introduction

Person identification from electrocardiogram (ECG) signal was made possible just nine years ago (Biel et al., 2001). Till then there have been a surge of research on ECG based biometric (Sufi et al., 2008b, 2010, in press; Khalil and Sufi, 2008; Sufi and Khalil, 2008a; Biel et al., 2001; Chan et al., 2008; Wubbeler et al., 2007; Poon et al., 2006; Israel et al., 2005; Bui and Hatzinakos, 2008; Irvine et al., 2001). Basically, ECG based biometric can be achieved by comparing the enrollment ECG template and recognition ECG template. These ECG biometric templates are generated utilizing direct time domain methods (e.g. duration and amplitude of P wave, QRS complex, T wave, etc.), signal processing methods (e.g. wavelet distance measurement, WDM, percentage root-mean-square distance, PRD, etc.) or numerous other methods (e.g. polynomial distance measurement, percentage root-mean-square distance, etc.) (Sufi et al., 2010). Irrespective of underlying methods used for the generation of the templates, all the existing ECG biometrics work on plain ECG signal (i.e. uncompressed, not encoded).

However, in a remote telecardiology scenario, ECG packets are often kept in compressed format because of their enormous size. In such a scenario, a patient is attached to a miniature ECG acquisition device that transmits the patient's ECG signals to remote locations using mobile communication devices (Sufi et al., 2009, 2006; Sufi, 2007; Sufi and Khalil, 2008a,b; Lee et al., 2007; Online, 2009a) (Fig. 1). Here, ECG signal acquired by an ECG acquisition device is directed to a patient's mobile phone or personal computer as ECG packets (Via Bluetooth, Wifi, Zigbee or Near Field Communication protocol) which redirects the data to the patient's Internet service provider. Through the public internet infrastructure the compressed ECGs reach the hospital that is remotely monitoring the cardiac patients. If required, the hospital may use public internet to send the compressed ECG to an outside cardiologist for expert opinion. Therefore, it is clearly seen from these tele-cardiology scenarios (Sufi et al., 2009, 2006; Sufi, 2007; Sufi and Khalil, 2008a,b; Lee et al., 2007; Online, 2009a), compressed ECG packets are often preferred for efficient transmission and storage purposes.

Now in these scenarios (remote telecardiology applications), if a patient and his/her ECG data is to be authenticated either by the hospital or the remote cardiologist to guard against malicious distributed denial-of-service (DDOS) attack or spoof attack (Sufi et al., 2008b; Sufi and Khalil, 2008b, 2009b), then the compressed ECG packets are required to be decompressed first before applying existing biometric techniques (Sufi et al., 2008b, 2010, in press; Khalil and Sufi, 2008; Sufi and Khalil, 2008a; Biel et al., 2001; Chan et al., 2008; Wubbeler et al., 2007; Poon et al., 2006; Israel et al., 2005; Bui and Hatzinakos, 2008; Irvine et al., 2001). This added step of decompression before biometric authentication generates slight delay in cardiovascular patient authentication. In wireless body

* Corresponding author.
E-mail address: research@fahimsufi.com (F. Sufi).

1084-8045/$ - see front matter
doi:10.1016/j.jnca.2010.07.004