

## Research Article

# Secure and Privacy Enhanced Gait Authentication on Smart Phone

**Thang Hoang and Deokjai Choi**

*Department of Electronics and Computer Engineering, Chonnam National University, Gwangju - , Republic of Korea*

Correspondence should be addressed to Deokjai Choi; dchoi@jnu.ac.kr

Received January ; Accepted February ; Published May

Academic Editors: Y. Pan and J. H. Park

Copyright © 2016 T. Hoang and D. Choi. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Smart environments established by the development of mobile technology have brought vast benefits to human being. However, authentication mechanisms on portable smart devices, particularly conventional biometric based approaches, still remain security and privacy concerns. These traditional systems are mostly based on pattern recognition and machine learning algorithms, wherein original biometric templates or extracted features are stored under unconcealed form for performing matching with a new biometric sample in the authentication phase. In this paper, we propose a novel gait based authentication using biometric cryptosystem to enhance the system security and user privacy on the smart phone. Extracted gait features are merely used to biometrically encrypt a cryptographic key which is acted as the authentication factor. Gait signals are acquired by using an inertial sensor named accelerometer in the mobile device and error correcting codes are adopted to deal with the natural variation of gait measurements. We evaluate our proposed system on a dataset consisting of gait samples of volunteers. We achieved the lowest false acceptance rate (FAR) and false rejection rate (FRR) of 0.01% and 0.02%, respectively, in terms of key length of 128 bits.

## 1. Introduction

Smart environments established by the development of mobile technology have brought vast benefits to human being [1]. Nowadays, mobile devices could be utilized not only for communication and entertainment but also for transaction [2], personal healthcare [3], or even in emergency situations [4]. As a result, more and more personal data are collected and kept in the mobile device for analysis [5], which would lead to increasing system security and user privacy concerns. Basically, security techniques for authentication and identification are commonly based on password (e.g., OTP [6]), token (e.g., ID cards), or biometric recognition (e.g., iris [7], fingerprint [8], face [9], and gait [10] recognition). Biometric based authentication mechanisms are more convenient in terms of end-user usage viewpoint when comparing with the two remaining methods of password and token. However, using biometric authentication on mobile devices should be considered carefully. Due to the fact that biometrics is unique but fuzzy and revocable, most conventional biometric authentication systems are developed based on pattern recognition and machine learning (PR-ML) algorithms to

deal with the natural variations of biometric measurement [11]. Enrollment biometric templates or extracted features are stored under unconcealed form for matching with a new biometric sample to authenticate/identify users. This kind of approaches could leave critical vulnerabilities in terms of system security and user privacy, especially when it is implemented on mobile devices. These devices are easily lost so that an adversary could illegally access the mobile repository to obtain original biometric templates. Since biometrics is tied to unique characteristics of an individual which are hardly changed, the user privacy leak means an adversary could partly or fully determine the user's biometrics. From the viewpoint of system security, a compromise of biometric templates results in everlasting forfeiture. An adversary could utilize compromised templates to thereafter always illegally grant access to sensitive services.

In this paper, we introduce an authentication system based on biometric cryptosystem (BCS) to enhance the system security and user privacy on mobile devices. The biometric modality used in our system is human gait which is collected using an inertial sensor named accelerometer attached to the user's body. This type of sensor has been

















