Master's Thesis

**Modeling and Discovering Human Behavior from Smartphone Sensing Life-Log Data**

Department of Electronics and Computer Engineering

Graduate School, Chonnam National University

MAFRUR, Rischan

June 2015

**Modeling and Discovering Human Behavior from Smartphone Sensing Life-Log Data**

Department of Electronics and Computer Engineering

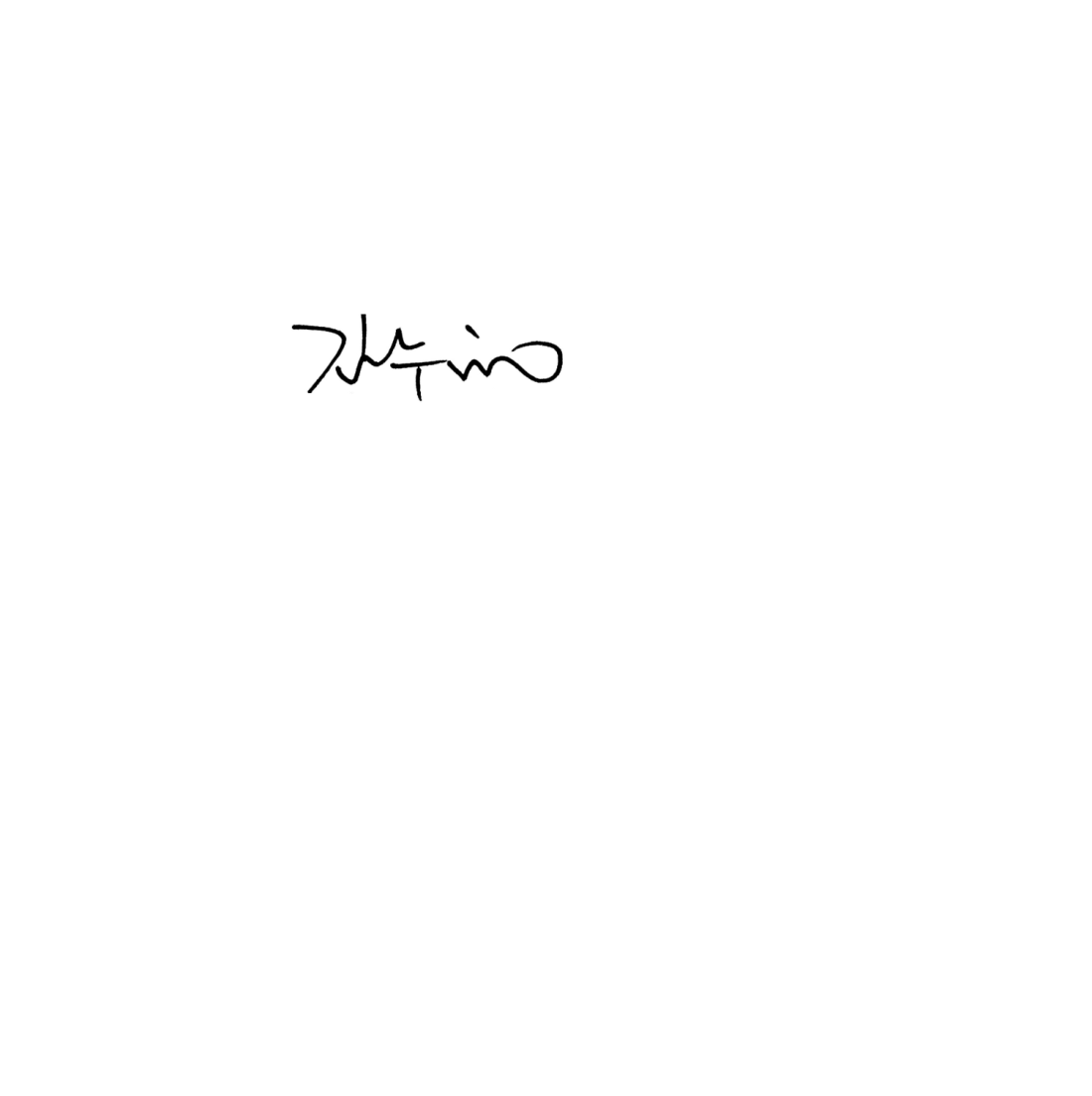
Graduate School, Chonnam National University

MAFRUR, Rischan

Supervised by Professor CHOI, Deok Jai

A dissertation submitted in partial fulfillment of the requirements for the Master of Engineering in Computer Engineering.

Committee in Charge:



|  |  |
| --- | --- |
| KIM, Soo Hyung |  |
| KIM, Kyung Baek | C:\Users\ThangHoang\Desktop\Thesis\kbkim.png |
| CHOI, Deok Jai | C:\Users\ThangHoang\Desktop\Thesis\djchoi.png |

June 2015

Table of Contents

[LIST OF FIGURES iii](#_Toc373313635)

[LIST OF TABLES iv](#_Toc373313636)

[(Abstract) v](#_Toc373313637)

[1. INTRODUCTION 1](#_Toc373313638)

[1.1 Overview 1](#_Toc373313639)

[1.2 Contribution 3](#_Toc373313640)

[2. GAIT AUTHENTICATION USING PATTERN RECOGNITION 6](#_Toc373313641)

[2.1 Data acquisition 6](#_Toc373313642)

[2.2 Data Pre-processing 7](#_Toc373313643)

[2.2.1 Signal Transformation 7](#_Toc373313644)

[2.2.2 Time Interpolation and Noise Elimination 9](#_Toc373313645)

[2.3 Data Segmentation 11](#_Toc373313646)

[2.4 Feature Extraction and Classification 14](#_Toc373313647)

[2.4.1 Time Domain Features 15](#_Toc373313648)

[2.4.2 Frequency Domain Features 16](#_Toc373313649)

[2.4.3 Feature Subset Selection 16](#_Toc373313650)

[3. GAIT BASED BIOMETRIC CRYPTOSYSTEM 19](#_Toc373313651)

[3.1 Background 20](#_Toc373313652)

[3.1.1 Fuzzy commitment scheme 20](#_Toc373313653)

[3.1.2 Binary BCH code 21](#_Toc373313654)

[3.2 Gait Based Biometric Cryptosystem 23](#_Toc373313655)

[3.2.1 Overall architecture 23](#_Toc373313656)

[3.2.2 Real-valued gait template extraction 25](#_Toc373313657)

[3.2.3 Gait template binarization and reliable bits extraction 27](#_Toc373313658)

[3.2.4 Key binding scheme 28](#_Toc373313659)

[4. EXPERIMENTAL RESULTS 30](#_Toc373313660)

[4.1 Data Collection Scenario 30](#_Toc373313661)

[4.2 Gait Authentication using Pattern Recognition and Machine Learning 31](#_Toc373313662)

[4.2.1 Overall Gait Identification Results 31](#_Toc373313663)

[4.2.2 Impacts of Installation Errors 33](#_Toc373313664)

[4.2.3 Authentication Results 34](#_Toc373313665)

[4.3 Gait Based Biometric Cryptosystem 36](#_Toc373313666)

[4.3.1 Intra- and inter- class gait templates variability 36](#_Toc373313667)

[4.3.2 Resampling original gait template length to appropriate values. 38](#_Toc373313668)

[4.3.3 Key binding results 40](#_Toc373313669)

[4.3.4 Security discussion 41](#_Toc373313670)

[4.3.5 Relative comparison with other state of the art biometric cryptosystems 43](#_Toc373313671)

[5. RELATED WORKS 45](#_Toc373313672)

[5.1 Gait authentication using pattern recognition approaches 45](#_Toc373313673)

[5.2 Biometric cryptosystems 47](#_Toc373313674)

[6. CONCLUSIONS 50](#_Toc373313675)

[Bibliography 51](#_Toc373313676)

[References 53](#_Toc373313677)

[(국문초록) 59](#_Toc373313678)

[ACKNOWLEDGEMENT 61](#_Toc373313679)

# LIST OF FIGURES

[**Figure 2.1 (a)** Mobile coordinate system, **(b)** misplacement error, **(c)** disorientation error and **(d)** both cases 6](#_Toc369193731)

[**Figure 2.2** **(a)** Mobile orientation after applying rotation matrix, **(b)** the relative position between the phone and its wearer 9](#_Toc369193732)

[**Figure 2.3** Multi-level wavelet decomposition 10](#_Toc369193733)

[**Figure 2.4** Illustration of a gait cycle 11](#_Toc369193734)

[**Figure 2.5** **(a)** Auto-correlation coefficients, **(b)** detected marking points in Z-signal 13](#_Toc369193735)

[**Figure 3.1** The fuzzy commitment scheme proposed by A. Juels 21](#_Toc369193736)

[**Figure 3.2** The architecture of gait based BCS using fuzzy commitment scheme 24](#_Toc369193737)

[**Figure 3.3** Illustration of extracted real-valued gait templates of 3 users 26](#_Toc369193738)

[**Figure 4.1** **(a)** Confusion matrix of the gait recognition, **(b)** the classification accuracy of feature subsets by applying SFFS and SFS algorithms 32](#_Toc369193739)

[**Figure 4.2** the FRR at zeroFAR before and after applying voting scheme 35](#_Toc369193740)

[**Figure 4.3** The density distribution of real-valued and binary gait templates 37](#_Toc369193741)

[**Figure 4.4** **(a)** The Euclidean distance distribution of real-valued templates, **(b)** The Hamming distance of binary templates 38](#_Toc369193742)

[**Figure 4.5** **(top)** The Hamming distance distribution of binary templates, and **(bottom)** the FAR and FRR of our proposed BCS 41](#_Toc369193743)

# LIST OF TABLES

[**Table 2.1** Feature subset(s) selection using SFS and SFFS algorithms 17](#_Toc373313414)

[**Table 4.1** The performance of reducing feature dimension versus non-reducing 33](#_Toc373313415)

[**Table 4.2** **(a)** Improvements of segmentation based on gait cycles compared with fixed length, **(b)** the influence of disorientation error to the classification results 33](#_Toc373313416)

[**Table 4.3** Optimal length of the real-valued template corresponding with the requisite length of the binary gait template 40](#_Toc373313417)

[**Table 4.4** The FAR and FRR of our gait based BCS with different template length using binary BCH codes 40](#_Toc373313418)

[**Table 4.5** The performance of state of the art BCS using physiological and behaviroal modalities using various scheme such as Fuzzy Commitment scheme (FCS), Fuzzy Extractor, (FE), Feature Transformation (FF) and Password Hardening (PH) 44](#_Toc373313419)

[**Table 5.1** State of the art gait authentication using Standalone (S) and Mobile sensor (M) including Accelerometer (A), Rotation Sensor (R) by approaches: Template Matching (TM), Machine Learning (ML) and Hybrid (H) 46](#_Toc373313420)

**Modeling and Discovering Human Behavior from Smartphone Sensing Life-Log Data**

MAFRUR, Rischan

Department of Electronics and Computer Engineering

Graduate School, Chonnam National University

(Supervised by Professor CHOI, Deok Jai)

# (Abstract)

In this thesis, two novel gait authentication systems using sensor resources on mobile phone are proposed. The first approach focuses on constructing a system based on pattern recognition and machine learning (PR-ML) algorithms, in which the performance is enhanced by executing deep examination at pre- and post- processing steps. The installation errors including misplacement and disorientation, which could badly affect the accuracy of the system, are also overcome completely. A novel and effective segmentation algorithm is also provided to segment signal into separate gait cycles with an optimal accuracy. Subsequently, features are then extracted in both time and frequency domains. We aim to construct a lightweight but high reliable model; hence feature subsets selection algorithms are applied to optimize the dimension of the feature vectors as well as the processing time of classification tasks. Afterward, the optimal feature vector is classified using Support Vector Machine with Radial Basis Function kernel. Nevertheless, PR-ML based biometric authentications remain system security and user privacy issues. In these systems, original biometric templates or extracted features used for authentication are stored insecurely so that a compromise of such data results in everlasting forfeiture. Hence to guarantee system security and user privacy, we propose a second approach of gait authentication based on biometric cryptosystem using fuzzy commitment scheme. Instead of using directly original biometric templates for user verification, the decision is based on a cryptographic key which is biometrically encrypted by gait templates acquired by an integrated mobile accelerometer. The performance of our two approaches is evaluated on the self-constructed dataset consisting of gait signals of 38 volunteers (28 males, 10 females) because of the unavailability of public gait dataset in this area. By implementation on PR-ML approach, we achieved the accuracy approximately 94.93% under identification mode, the zeroFAR, FRR of 3.89% and processing time of less than 4 seconds under authentication mode. In the gait based biometric cryptosystem approach, we achieved the optimal zeroFAR and the FRR of approximately 16.18% and 14.71% corresponding with the key length of 139 and 50 bits respectively. The results also show that mobile sensor-based gait could be utilized as an effective modality to construct a biometric cryptosystem, compared with other factors such as iris, fingerprint, voice, signature, etc.

# INTRODUCTION

## Overview

The explosion of mobility nowadays is setting a new standard for information technology industry. Mobile devices sales skyrocketed over recent years. A survey on the mobile market[[1]](#footnote-1) showed that there were six billion subscriptions by the end of 2011. Technology constantly evolves and creates more intelligent devices. Their abilities are not only limited in calling, or texting, but also cover a variety of utilities, including portable storage and business applications, such as e-commerce or m-banking [2].

However, misconception of mobile devices as being an absolutely safe repository for storing critical information could cause owners to face up to security hassles. Such devices can be easily lost, stolen, or illegally accessed [1], which makes sensitive or/and important information of mobile owners become vulnerable (see more [1]). Consequently, authentication settings have evolved to become a more priority issue. The most widely-used authentication methods in mobile currently are PINs, visual patterns, and pass-words because of their ease in use and implementation. However, these methods are not always effective considering remembrance and security aspects [1]. Implementations on physiological biometric could overcome this issue completely [3, 28]. However, it is hard to deploy them on mobile phone since existing mobile resources would not guarantee to acquire specialized data such as iris, fingerprint, etc. properly. Similar to other active authentications like PIN and password, physiological biometrics also cause time consuming which is one of the main obstacles preventing users from using these techniques. All these forced us to pay attention and perform explicit gestures to be authenticated (e.g. typing passphrases, facing to the front camera, etc.). This causes obtrusiveness and inconvenience in frequent use.

Thus, a friendlier and reliable authentication mechanism which can operate implicitly without users’ awareness is desired to be found and aimed to ameliorate mobile security. Gait has been considered as behavioral biometrics for decades [29]. Previously, gait recognition is mostly implemented by computer vision in which gait signals are recorded by cameras [29, 44, 45]. Recently, novel approaches using wearable sensors to authenticate human gait has been introduced and achieved potential results [11, 13]. Accordingly, sensors are attached to human body in various positions such as pocket, waist and footwear to record physical locomotion. This approach takes advantage of modern mobile devices’ sensing capabilities including GPS, accelerometer, magnetometer, gyroscope sensor, etc. Moreover, devices are usually put in their owners' pockets for most of the day [1], so gaits can be authenticated implicitly and continuously by acquiring walking signals. For this reason, sensor-based gait authentication has a significant advantage in implementation on mobile. It will provide developers with an edge over improving various techniques in authentication.

The above potentialities of wearable sensor authentication motivated us to improve and establish a similar mechanism running on mobile. Since 2009, this study has been initiated on mobile and achieved encouraging results [8, 19]. However, they were still in early stages and methods were tried-out on ideal conditions in which mobiles were always installed at an exact position and orientation by tightening directly to equipment such as suite, footgear, or human body. Processing steps such as segmentation and noise elimination which could directly affect the recognition model were not analyzed in depth. Finally, there was no evaluation of the possibility of running authentication directly on mobile devices. Authentication tasks were assigned to powerful computers rather than mobile resources. An excessively complex model could face up to critical challenges when it is deployed on limited computing devices.

Moreover, biometrics in general and gait in particular are fundamentally unique but, they are also fuzzy and irrevocable [29]. There are slight variations between biometric measurements. Hence most biometric systems have been developed based on pattern recognition and machine learning (PR-ML) algorithms to deal with these variations [3, 5-21, 30-32, 44, 45]. However, such approaches could leave critical vulnerabilities. An attacker could access to the device’s storage to obtain the enrollment biometric templates. This kind of vulnerability cannot be avoided by storing these templates under hash codes as in password based systems. Applying cryptographic hash algorithms on biometrics templates is impractical since hashing algorithms are very sensitive to noise [34]. They do not tolerate a single bit error whereas biometrics is basically noisy especially behavioral biometrics as gait. Loss of enrollment biometric templates could make users confront with security and privacy issues. Since biometrics is tied to unique characteristics of an individual which is hardly to be changed, the user privacy leak means an attacker could partly or fully determine the user’s biometrics. In the system security viewpoint, a compromise of biometric templates results in everlasting forfeiture so that attackers could utilize compromised templates to eternally gain access to authentication services.

## Contribution

We introduce two novel gait authentication systems based on PR-ML algorithms and biometric cryptosystem, respectively. Note that in this thesis, we assumed that users’ gait is not affected by outside conditions in term of human (e.g. emotion, health, disease, etc.) and environmental conditions (e.g. ground material, footwear). We collect gait of volunteers having ordinary state of health under our standard laboratory environment. In the PR-ML approach, we focus on finding solutions to deal with existing matters: (1) the mobile installation issues including misplacement and disorientation errors. To handle them, we introduce a novel lightweight but effective calibration method by taking full advantage of existing sensors including accelerometer and magnetometer on modern mobile phone. (2) Gait preprocessing phases are investigated thoroughly to improve the effectiveness of the authentication mechanism. A novel segmentation algorithm which could segment acquired data into well separated gait cycles is also presented. (3) To make sure the authentication model can run smoothly and independently on limited computational devices like mobile phone, we apply some techniques to reduce the processing time of learning algorithm. A scenario is also designed to construct a particular dataset under more realistic conditions to fairly evaluate our proposed model. We perform our study on both authentication and identification modes. The impacts of mobile installation errors and processing steps to the authentication model are also analyzed. Finally, the authentication is deployed directly on the mobile phone to experiment the possibility of running such model on a limited computational device. With promising results achieved from the experiment, solving installation issues and providing a novel lightweight reliable gait authentication are our main contributions.

In the biometric cryptosystem (BCS) approach, we introduce a first BCS using human gait. The performance of our BCS shows that gait could be used to construct a BCS as effectively as other modalities like fingerprint, face, signature, voice, etc. Our BCS is implemented using mobile sensor-based gait signals and fuzzy commitment scheme which requires not only less storage space but also the low computational complexity. Hence, such system is more applicable – compared with other PR-LM based systems – to be deployed directly on mobile devices with limited computational resources. Finally, mobile devices are more and more equipped various hardware resources such as camera, sensors (e.g. fingerprint sensor, accelerometer, etc.). A multimodal biometric cryptosystem (multiBCS) could be deployed on the mobile devices by fusing biometric modalities such as face, fingerprint, with a new inertial sensor-based gait modality – as supplied by in this thesis – to enhance the performance and security of the devices.

# Dataset

## Data Acquisition

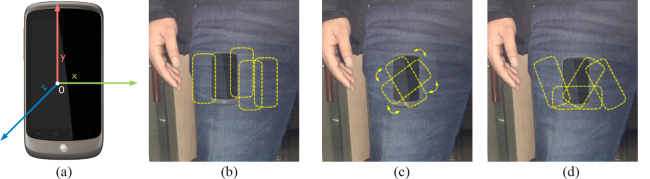
Application Data Collector

About Data Itself

We perform our study on a Google Android HTC Nexus One mobile phone. The authentication mechanism is constructed based on gait signal acquired by a built-in accelerometer. Acceleration forces acting on the phone are measured in three spatial dimensions (, and as illustrated in the figure 2.1(a)) when subjects are walking. Based on the relationships between gravity, acceleration and motion, we present the output of accelerometer as 3-component vectors

|  |  |
| --- | --- |
|  | (2.1) |

where represent the magnitude of the acceleration forces acting on three directions respectively.



**Figure 2.1 (a)** Mobile coordinate system, **(b)** misplacement error, **(c)** disorientation error and **(d)** both cases

Because of the accelerometer’s characteristics, its sensing is very sensitive to mobile installation. Normally in fact, it is impossible to ensure the phone will always be at a fixed orientation and position all the time without additional accessories. Two issues could occur concurrently: (1) misplacement and (2) disorientation errors (Figure 2.1(b-d)). From our observation, the impact of misplacement does not significantly affect accelerometer’s sensing axes once it is put in the trouser pocket. It is easily solved without exploiting more information.

Looking into the case of disorientation error, as accelerometer senses acceleration forces acting on three dimensions of the phone, acquired signals will be contaminated if it is not always fixed correspondingly to its bearer. Acceleration vectors should always be represented in a constantly referred coordination system instead of an unstable one (mobile coordinate system in this case). To do this, an additional built-in magnetometer is used along with the accelerometer. In our study, Earth is considered as the referred context. A rotation matrix is calculated based on the yaw, pitch, and roll angles which represent the angle changes between mobile and Earth coordinate system. These angles are determined by the combination of magnetometer and accelerometer.

In summary, two kinds of information are determined to construct an effective gait authentication model: (1) yaw, pitch and roll angles determined before users start to walk and (2) gait signal of individuals. A scenario to acquire these values is explained meticulously in the Section 4.1

## Data Pre-processing

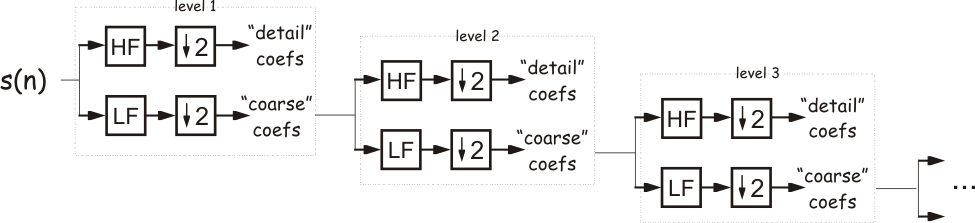
### Data Cleansing

As gait signals of individuals are acquired with arbitrary installations. Thus, the first step is standardizing raw signals to eliminate the impacts of disorientation and misplacement errors.

### Data Transformation

As the mobile accelerometer is power saving designed to be simpler than standalone sensors, its sampling rate is not stable and entirely depends on mobile OS. The time interval between two consecutive returned samples is not a constant. The sensor only outputs value when the forces acting on each dimension have a significant change. The sampling rate of our device is approximately 27 Hz. Therefore, acquired signal is interpolated to 32 Hz using linear interpolation to ensure that the time interval between two sample-points will be fixed.

When accelerometer samples movement data by user walking, some noises will inevitably be collected. These additional noises came from various sources (e.g., idle orientation shifts, screen taps, bumps on the road while walking). Moreover, mobile accelerometer produces numerous noises compared with standalone sensors since its functionality is fully governed by mobile OS layer. A digital filter needs to be designed to eliminate noises and reduce the impact of misplacement error concurrently. Multi-level wavelet decomposition and reconstruction method are adopted to filter the signal.



**Figure 2.3** Multi-level wavelet decomposition

According to the Figure 2.3, original signal is denoted by. High-pass filter and low-pass filter are denoted by and. Within each level, the outputs from high-pass filter are known as detail coefficients. On the other hand, low-pass filter outputs contain most of the information of the input signal. They are known as coarse coefficients. The signal is down-sampled by 2 at each level. Coefficients obtained from the low-pass filter are used as the original signal for the next level, and this process continues until the desired level is achieved.

In contrast, reconstruction is the reverse of decomposition process. To eliminate noises, we assign the detail coefficients to 0. The reconstruction of the signal is computed by concatenating the coefficients of high-frequency with low-frequency. In this study, the Daubechies orthogonal wavelet () with level 2 is adopted for reducing noise and eliminating the impact of misplacement error simultaneously.

## Feature Extraction

In this stage, three phases are investigated to obtain an optimal classification model: First, possible features on both time and frequency domains are extracted on 3 types of acceleration data including -axis signal, magnitude and sum of acceleration forces of axes. As discussed in the Section 2.2.1, signals could not be distinguished with current limited resources on mobile devices. Hence, we consider the sum of forces acting simultaneously on both axes. Second, feature subset selection algorithms are applied for obtaining the best feature set. Feature subsets are selected based on the accuracy criterion of the learning algorithm. Finally, the best feature subsets are classified using Support Vector Machine (SVM) classifier with Radial Basis Function (RBF) kernel.

### Define Human Activity and Behavior

We extract features which can represent characteristics of gait signal in time domain including

|  |  |
| --- | --- |
| * Average maximum acceleration   (2.7)   * Average minimum acceleration   (2.8) | * 10-bin histogram distribution   (2.9) |
| * Average absolute difference   (2.10) | * Standard deviation   (2.11) |
| * Root Mean Square   (2.12) | * Waveform length   (2.13) |

where is the data point in time series of a segment, is the number of gait cycles in the segment, is the total number of data point in the segment.

These features above are extracted on 3 types of signal including , and

|  |  |
| --- | --- |
| * Cadence period   (2.14) | * Cadence frequency   (2.15) |

where is the time length of gait cycle

### Listing Features and Extraction

* 40 first FFT coefficients

|  |  |
| --- | --- |
|  | (2.16) |

* 40 first DCT coefficients

|  |  |
| --- | --- |
|  | (2.17) |

Similar to features on time domains, these coefficients are extracted on , and.

As stated before, the walking speed of users in fact is not absolutely constant. Hence, the length of gait cycles is not stable. Calculating coefficients on frequency domain (e.g. ) requires window frames (or patterns) have the same fixed length. Meanwhile, the length of gait cycles fluctuates slightly around time gap calculated in the Section 2.3. As a result, the number of data points in every gait cycle needs to be normalized by using our proposed algorithm [14] to make sure the frequency coefficients are calculated properly.

# HUMAN BEHAVIORS MODELING

Biometric cryptosystems (BCS) (aka biometric encryption, biometric template protection) have been being developed to enhance both privacy and security of the conventional biometric systems [35-37, 58, 59, 61]. In these systems, biometric templates are bound with a cryptographic key, making it computationally challenging to retrieve either the key or the original template from the biometrically encrypted data. A user would be authenticated / identified if he provided a new template which is sufficiently close to the original which is registered to the system before. The backbone of this system is based on conventional cryptography wherein a cryptographic key is employed as the authentication factor. However unlike conventional password-based system where key management remains security and utilization issues [38, 39], BCS links biometrics with cryptography to overcome such vulnerabilities by biometrically managing such keys with the more secure and more convenient way. In this thesis, we additionally introduce a gait based biometric cryptosystem. Our BCS relies on fuzzy commitment scheme [36] to deal with the natural variations of gait templates. The original gait template is always discarded and is not stored in the system so that the security and privacy are significantly enhanced. Such templates are acquired by an integrated accelerometer in mobile devices and then, are transformed for feasibly binding with cryptographic keys. Helper data supporting authentication are stored in the mobile storage and biometrically encrypted to prevent an attacker from retrieving either the key or original templates. Hence, they are still secure even though mobile devices are lost or compromised.

## Background and Problem Statement

### Smartphone Personal Data

In 1999, A. Juels and M. Wattenberg combined well-known techniques from the areas of error correcting codes and cryptography to achieve a new type of cryptographic primitive referred to a fuzzy commitment scheme [36]. Figure 3.1 illustrates the operation of this scheme in a biometric scenario, wherein codeword c of length represents a secret or a cryptographic key, and witness is the biometric template having the same length with . The -bit can be expressed in terms of the codeword along with an offset such that . The function is to conceal by using a conventional cryptographic hash function while leaving in clear.

|  |  |
| --- | --- |
|  | (3.1) |

Each provides partial information about yet is not saved under archetype and be always concealed by . In the enrollment, a user will provide an original biometrics . The system generates a codeword and computes the fuzzy commitment . The returned values of and are stored locally. In authentication, the user who is supposed to be will provide a fresh biometrics . To decommit using, the system computes , where is an efficient decoding function. will be equal to if is sufficiently close to according to an appropriate distance metric. The differences between and are removed by the error correcting code techniques used in .

C:\Users\ThangHoang\Desktop\res\fuzzy commitment scheme.emf

**Figure 3.1** The fuzzy commitment scheme proposed by A. Juels [36]

### Modeling and Discovering Human Activity and Behaviors

The random error correcting codes used in our system is BCH codes that were discovered independently by Bose and Ray-Chaudhuri [47] and by Hocquenghem [48]. BCH Codes, like many other digital codes, are used to encode a vector information message of length (the cryptographic key in this study) into a codeword vector of length.

BCH codes are the generation of Hamming codes for multiple error correction. It could be defined over any field. However in this work, we only focus on using binary BCH codes over Galois Field with in which, code symbols are represented by bits of.

For any positive integer and, there exists a binay BCH code with length and minimum distance such that

|  |  |
| --- | --- |
|  | (3.2) |

where is the maximum errors which could be corrected. In other word, this binary BCH code could correct up to errors in a block of digits.

Let be a primitive element in Galois Field. The minimal polynomial of over GF(2) is denoted as . The generator polynomial of -error correcting BCH code of length is the Least Common Multiple () of the minimal polynimals of

|  |  |
| --- | --- |
|  | (3.3) |

If is even, could be expressed as where is odd and . Then is a conjugate of . Therefore . (3.3) is equivalent to

|  |  |
| --- | --- |
|  | (3.4) |

The information block length of is determined by

|  |  |
| --- | --- |
|  | (3.5) |

The minimum distance is determined by the weight of the generator polynomial

|  |  |
| --- | --- |
|  | (3.6) |

The encoding process of Binary BCH code could be summarized as follows. Given a information message . We express in term of message polynomial

|  |  |
| --- | --- |
|  | (3.7) |

Parameters including the length of codeword and the -error correcting code are pre-defined. Then, we generate the irreducible primitive polynomial of over with the degree of , and the primitive element of . The minimal polynomials for each element in is determined respectively. Then, the generator polynomial is calculated according to (3.4)

Finally, the encoding process is done by multiplying message polynomial with the generator polynomial yielding a codeword where are coefficients of the codeword

|  |  |
| --- | --- |
|  | (3.8) |

where

|  |  |
| --- | --- |
|  | (3.9) |

Given a codeword , the BCH decoding could be done by a specific algorithm proposed by J. Massey et al. [49]. The outline of BCH decoding includes typical steps as following

* Calculating the syndrome for
* Determining the coefficients of the error polynomial from by using the Berlekamp-Massey Algorithm or Euclidean Algorithm
* Determining the locations of the errors by calculating the inverses of the roots of using Chien search
* Correcting the errors.

A millstone of these steps is described clearly in [43]

## Proposed Methods

### Overall architecture

Figure 3.2 sketches our proposed gait based BCS using fuzzy commitment scheme based on binary BCH codes. The objective of this system is to biometrically encrypt a cryptographic key (i.e. symmetric key) using user’s biometric gait. This key will be successfully replicated if the user provides a fresh template which is sufficiently close to the original which has been registered before according to the Hamming distance metric. The system consists of two phases including enrollment phase and authentication phase which are briefly described as following

In the enrollment phase, gait signal of a user will be firstly acquired and then is pre-processed to eliminate the influence of the acquisition environment. Real-valued gait templates are then extracted and binarized. After that, reliable bits in the binary template are determined via estimating the error probability of each component using statistical analysis. Concurrently, a binary cryptographic key is generated randomly. On the one hand, this key will be encoded using binary BCH codes to mitigate the variations of gait characteristics. The encoded key will be bound with the binary template forming secured. On the other hand, a cryptographic hash function will be applied to keep safely under concealed form. Helper data used for binary template construction along with will also be stored for further use to replicate the key in the authentication phase.

C:\Users\ThangHoang\Desktop\res\biometric cryptosystem model_NO_ATTACK.emf

**Figure 3.2** The overall architecture of our proposed gait based BCS using fuzzy commitment scheme where ⊕ denotes the OR-exclusive operation

In the authentication phase, the user supposed to be will provide a fresh gait template. Such template is also preprocessed and binarized using helper data which is previously stored in the enrollment phase. After that, extracted binary template will be bound with the secured returning a string. This string will be decoded using BCH decoding to obtain a fresh key. Finally, the hash code of will be matched with for authentication decision. The milestones of our system are described in detail as in the following

### Recognizing Human Daily Activity and Behaviors

A gait cycle based segmentation algorithm as discuss in the Section 2.3 is also applied to split the gait signal into separated patterns. A gait template is extracted by concatenating 3 dimensional signals, respectively.

|  |  |
| --- | --- |
|  | (3.10) |

where is the -dimensional signal.

|  |  |
| --- | --- |
|  | (3.11) |

is constructed by concatenating consecutive gait cycles which are separated and normalized by a segmentation algorithm in the Section 2.3. Finally we obtain a gait template with the length of. Figure 3.3 shows extracted gait templates of 3 users. Since samples in the template are real values, we call these templates as real-valued templates in . After that, an interpolation is adopted to resample the gait template to appropriate lengths for possibly binding with the cryptographic key in our system.

Given samples to in an extracted gait template where is the acceleration value sensed at the time of . We apply spline interpolation to simulate the continuity of the template. The spline interpolation such that for is determined by

|  |  |
| --- | --- |
|  | (3.12) |

is a cubic polynomial which is calculated as

|  |  |
| --- | --- |
|  | (3.13) |

where

|  |  |
| --- | --- |
| , , | (3.14) |

Note that *,* is calculated by solving the tridiagonal matrix

|  |  |
| --- | --- |
|  | (3.15) |

where

|  |  |
| --- | --- |
|  | (3.16) |

C:\Users\ThangHoang\Desktop\res\gait_template.emf

**Figure 3.3** Illustration of extracted real-valued gait templates of 3 users

From now, we denote as the length of the gait template after resampling. Resampled templates will be binarized for binding with the BCH codeword which is encoded from a cryptographic key. The binarization is based on statistical analysis and a quantization method which will be described in the next section.

### Human and Machine Time

### Similarity Pattern Detection

We use BCH to denote a binary BCH code, whereis the code length of bits, is the key length of bits and is the error correction capability. The binary cryptographic key of length is generated randomly corresponding to each user and then be encoded into the codeword of length using encoding scheme. After that, we bind the extracted binary gait template with yielding secured. The method used to bind these two binary strings is *exclusive-OR* operation. We summarize all of essential steps both in enrollment phase and verification phase in our system as following

#### *Motif Identitication*

1. Select a by pre-defining parameters including the length of the codeword, the length of secret key.

For each user , biometric template is extracted using the method in Section 3.2.2

1. Determine the mean over all feature vectors and extract binary gait templates using the method in the Section 3.2.3. Then, discard
2. Determine the reliable bit indices and reducing the length of to by only selecting first bits among based on
3. Store as helper data for further use to construct fresh binary templates in the authentication phase
4. Randomly generate a binary secret key with the length of
5. Calculate the hash code of by using a cryptographic hash function (e.g. SHA, MD5, etc.). Then, discard and store .
6. Encode using encoding scheme to obtain the codeword
7. Bind with using *exclusive-OR* operator yielding , and then store

#### *Behavior Profiling*

For each user , a fresh biometric template is extracted using the method in the Section 3.2.2 same as in the enrollment phase

1. Extract binary gait templates with length of using the method in the Section 3.2.3 with the help of and which are previously stored.
2. Bind with using exclusive-OR operator to obtain a corrupted codeword
3. Employ BCH decoding algorithms to obtain the key from
4. Calculating hash code using the equivalent cryptographic hash function as in the enrollment phase
5. Matching with , if , the user is authenticated. Otherwise, it will be rejected.

# EXPERIMENTAL RESULTS

## Training and Testing Dataset

We experimented on data collected from built-in accelerometer and magnetometer in Google Nexus One mobile phone[[2]](#footnote-2). The sampling rate of both sensors is approximately 27Hz by setting to *SENSOR\_DELAY\_FASTED* mode in Android SDK. We would like to construct a more realistic dataset. In reality, two main factors including the effect of footgear and mobile installation often occur that could significantly affect gait of individuals. Hence, a scenario is designed to construct the dataset in which acquired gaits are collected under the influence of such factors. During experiment process, each volunteer will wear all three types of footgear including sleeper, sandal and shoe. The scenario is designed as following:

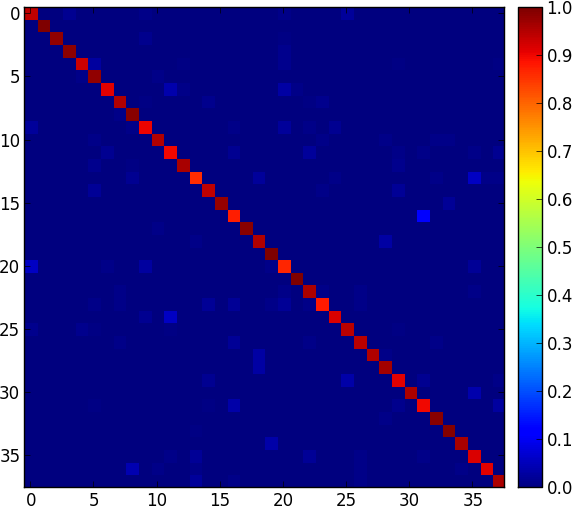
* + *Preparation (1st) phase:* Volunteers wear 1 of 3 footgear types and put the mobile phone in their trouser pocket according to any position and orientation. Subsequently, they will be asked to stand still for few seconds. During this time, the accelerometer and the magnetometer will be activated to collect values for determining yaw, pitch and roll angles. Subsequently, the rotation matrix will be calculated and stored inside mobile storage for acceleration vector transformation later.
  + *Collection (2nd) phase*: After the rotation matrix is stored successfully, volunteers will perform walking activity around 36 seconds on the ground floor. They will be asked to walk as naturally as possible. During this time, accelerometer will be activated to collect gait signals.

A total of 38 volunteers including 28 males and 10 females with the average age from 24 to 28 participated to our dataset construction. Each volunteer will perform around 18 laps. Each lap includes two phases above. Before starting a new lap, they will change the footgear and install the mobile to another orientation and position. Note that since the transformation matrix is always estimated in the preparation phase before volunteers start walking. Hence we have a constraint that when volunteers perform walking, the mobile will not change its position and orientation. To ensure that, we ask volunteers to wear trousers having the narrow pocket (e.g. the jean trouser). Totally, we acquired 24624 seconds walk of 38 volunteers.

## Result and Discussion

### Behavior Identification

Total 8500 patterns are extracted from the dataset by using our segmentation algorithm. Around patterns corresponding to each volunteer are split into two separated parts. The first part is used for training (*T-part*) and the remaining is used for prediction (*P-part*). We used libsvm[[3]](#footnote-3) [26] as the tool to perform SVM with RBF kernel. The performance of RBF kernel fully depends on selecting parameters . In order to construct an optimal SVM model, we perform a strategy to find the good yielding the best classification result. Features described in section 3.4 are extracted on both *T-part* and *P-part*. To deal with over-fitting issue, 10-fold cross validation is applied on T-part with various . The yielding the best cross validation accuracy will be selected. According to [26], we tried exponentially growing sequences of and to identify the ‘coarse’ pair first (e.g. ). Subsequently, a more detailed search is performed to identify a finer () yielding an optimal cross-validation accuracy. The best is identified at the cross-validation accuracy of 98.71%. Then, whole *T-part* is trained again using () to obtain the final SVM model. An overall accuracy rate approximately 94.93% is achieved when using such model to predict *T-part*. Figure 4.1(a) illustrates the confusion matrix of prediction result.

 C:\Users\ThangHoang\Desktop\Authentication\Paper\unknown\image\SFFS_SFS_alg.emf

(a) (b)

**Figure 4.1** **(a)** Confusion matrix of the gait recognition using SVM and RBF kernel, **(b)** the classification accuracy of feature subsets by applying SFFS and SFS algorithms

Additionally, by applying the SFS and SFFS algorithm, the dimension of feature vectors is reduced and the classification accuracy is slightly increased as well. The processing time is also ameliorated significantly (Table 4.1 and Figure 4.1(b)). By applying SFFS, the prediction time only costs 411 milliseconds per sample using mobile resources. In authentication mode, a task requires to predict on 9 consecutive samples (as discussed in the Section 4.2.3). It costs less than 4 seconds to make a decision. This is an acceptable level compared to original case (≈ 20 seconds). Note that processing time is very important in mobile applications since we aim to deploy a lightweight authentication model running directly on mobile phone. Nowadays, it is likely to be optimized by its weight, power and size rather than computational power (e.g. CPU, memory). Hence reducing feature dimension will help the mobile device to perform classification task more quickly so that the interaction between the phone and its user is also improved.

**Table 4.1** The performance of reducing feature dimension versus non-reducing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Scheme** | **No. of Subsets** | **Accuracy** | **Loading Time** | **Prediction Time** |
| **Original** | 29 | 94.34 % | 205897 ms | 2280 ms |
| **SFS** | 12 | 94.90 % | 86799 ms | 398 ms |
| **SFFS** | 13 | 94.93 % | 84223 ms | 411 ms |

### Validity of The Results

Before discussing the impact of mobile installation, we first compare the performance of segmentation based on gait cycles against previous studies used fixed size segmentation [15-17]. Since walking is a regularly cyclic activity, it is relatively easy to perceive that segmentation based on gait cycle always yields a better classification result compared with based on a fixed length (Table 4.2(a)).

**Table 4.2** **(a)** Improvements of segmentation based on gait cycles compared with fixed length, **(b)** the influence of disorientation error to the classification results

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| (a) | | |  | (b) | | |
| **Segmentation method** | | **Accuracy** |  | **Segmentation method** | **Fixing dis-orientation** | **Accuracy** |
| Fixed length | 3000 ms | 87.88 % |  | Fixed length | No | 79.53 % |
| 6000 ms | 87.78 % |  | Our algorithm | No | 84.03 % |
| 9000 ms | 84.73 % |  | Yes | 94.93 % |
| Gait cycle | 2 GCs | 92.26 % |  |  |  |  |
| 4 GCs | 94.93 % |  |  |  |  |
| 8 GCs | 90.94 % |  |  |  |  |

Second, we analyze the impacts of installation errors to segmentation algorithm and the classification accuracy. Note that a perfect accuracy rate of segmentation is achieved when using our algorithm with the transformed -signal. All gait cycles are detected and segmented correctly. Table 4.2(b) illustrates the performance of the segmentation task with/without fixing disorientation error. As discussed above, the periodicity of walking is only represented well in transformed -signal. Without rectifying such issues, the segmentation algorithm could not determine precisely the regularity of gait cycles caused by -signal’s instability. Therefore, each segmented pattern could not only represent a sequence of consecutive gait cycles well. That leads features extracted from these patterns could not represent the characteristics of walking style of individuals as well. As a result, the classification accuracy rate is contaminated. Even with using segmentation based on fixed length, the best achieved classification rate at length of 3000 ms is also worse (79.53%).

## Experimental Evaluation

The variation of biometric gait could be influenced by acquisition conditions. Since this is the early approach of gait based BCS not using PR-ML algorithms to handle natural variations of biometric gait, we only consider gait signals not to be influenced by many environmental conditions such as the influence of footgear, the installation errors, etc. Hence, we exclude gait signals which are significantly influenced by these conditions. Only signals acquired when the phone is placed vertically inside the trouser pocket with a fixed orientation and position are selected. Totally, we obtained 34 out of 38 users satisfying our conditions above and having at least 16 gait templates extracted by our proposed segmentation and template extraction method. Each extracted template consists of consecutive gait cycles and each gait cycle is normalized to samples of length. Therefore, templates will have the equal length of samples where 3 is the number of dimensions in the acquired signal including as described in the Section 3.2.2. After that these real-valued gait templates are resampled using interpolation to appropriate lengths for binarization and key binding scheme. Finally, such resampled gait templates will be equally divided into two parts used for training and testing.

### Time Execution and Performance

Figure 4.3 illustrates the normalized Euclidean distance distribution of real-valued gait templates and the Hamming distance distribution of binary template based on reliable bits selection. The Euclidean distance of two real-valued templates of length is calculated by

|  |  |
| --- | --- |
|  | (4.1) |

The Hamming distance of two binary templates of length is calculated by

|  |  |
| --- | --- |
|  | (4.2) |

C:\Users\ThangHoang\Desktop\fig1.emf

**Figure 4.3** The density distribution of real-valued and binary gait templates

Looking at the case of the Euclidean distance distribution of real-valued templates, the discrimination is likely to be low. In a more details, the distribution areas of same and different users mostly distribute from 0 to 0.2. That means gait templates between users are likely to be similar. Therefore, applying a threshold-based classification on such templates will result in a high error rate. From our experiment, we observe that extracting binary templates using the quantization method not only makes such templates be applicable to binding with binary BCH codewords but also increase the discrimination property. This is because binary templates only contains bits having high reliable. As shown in the Figure 4.3, the Hamming distances of intra- and inter- class templates are more discriminant and distribute mostly around 0.2 and 0.5 respectively. Templates between users are more dissimilar so that determining an appropriate threshold to classify such templates is more straightforward to achieve an acceptable error rate.

### **Limitation**

Spline interpolation is necessarily adopted to resample gait templates from the original length of to appropriate values of for extracting binary templates having sufficient length to bind with a binary BCH codeword (e.g. ). Hence, we analyze the impacts of resampling process on the gait template similarity. Figure 4.4(a) shows that the variation of real-valued templates is not influenced by the resampling process. The similarity of such templates does not changed significantly when they are resampled to various lengths.

C:\Users\ThangHoang\Desktop\res\euc_dist\63to4158interp.emf C:\Users\ThangHoang\Desktop\res\ham_dist\511bits_variousn.emf

**Figure 4.4** **(a)** The Euclidean distance distribution of real-valued templates when they are resampled to various length of , **(b)** The Hamming distance of binary templates of length extracted from when is resampled to be times of

However, although resampling process does not modify the similarity of real-valued templates, it adversely affects the reliable bits selection process which determines reliable bits out of to extract binary templates. If is much larger than, determining reliable bits based on their error function may be instable because of existing a large number of bits having a same error probability. Such bits could be selected arbitrarily. As a result, the extracted binary templates are more sensitive to error. Figure 4.4(b) illustrates the changes of distribution area when is resampled to a value of times of in term of . The distance of intra class templates are getting decreased and towards to 0. In other words, binary templates of the same user are getting more similar. That makes the number of errors need to be corrected in a template of the same user will be reduced. However, the distribution area of inter-class templates not only reduces to 0 but also be getting wider and mixes with the distribution of intra class templates. This phenomenon also happens in different cases of (e.g. ). Hence, an appropriate value of should be selected according to the requirement of to trade off the similarity of intra- and inter- templates.

In BCH codes, the length of information is inversely proportional to the number of correcting errors. The larger theis, the lower the information would be. For example, suppose the BCH codeword of length is 511 bits, if is up to 25 bits approximately 5% of , the length of key will be 157 bits. If is up to 121 bits ≈ 24% of , will be reduced significantly to 10. Applying cryptographic hash functions to conceal the cryptographic key at this length is insecure. Hence, in our system, we set to be approximately 12% for to be large enough.

As discussed above, the FAR and FRR reflect the security and friendliness of a BCS, respectively. In our system, we prioritize the security so that our objective is to make the FAR always equal to 0% and the FRR is as low as possible. To do that, the appropriate value of is selected based on analyzing the distance distribution of intra- and inter- class binary templates as already illustrated in the Figure 4.4(b). Table 4.3 specifically shows our selected values of. At such values, the normalized Hamming distance of extracted binary templates between users is always larger than 12% so that the expected FAR of 0% could be achieved, whereas the normalized Hamming distance of gait templates of the same users would be mostly lower than 12%, hence a low FRR could be achieved

**Table 4.3** Optimal length of the real-valued template corresponding with the requisite length of the binary gait template

|  |  |
| --- | --- |
|  |  |
| 127 | 317 |
| 255 | 586 |
| 511 | 126 |

# RELATED WORKS

## Smartphone Personal Data

State of the art BCSs which were previously proposed mostly focus on using physiological modalities such as iris [54, 57], face [50, 52, 46] and fingerprint [53, 55]. There are some studies that use behavioral biometrics such as signature [51], voice [40, 42] and keystroke [41]. Generally, BCSs could be classified into 2 subsystems including key binding and key-generation systems [60]. In key-binding systems – like our approach, a random key string is generated and then, bound with a biometric template yielding helper data. Such data is stored for further utilization to retrieve the key in the authentication phase. Several key binding techniques are fuzzy commitment scheme [36], helper data scheme [59] and fuzzy vault [37]. The key is revocable so that helper data containing a partial of biometric template is also revocable. A new helper data could be recreated by binding a fresh biometric template with a new key which is generated randomly, if the old data is compromised. Some key-binding based systems were implemented using various biometric modalities such as iris [57], face [50, 52, 46], fingerprint [53, 55], hand written signature [51], voice [42], keystroke [41] and authors achieved promising results. For example, F.Hao et al [57] proposed an iris based BCS using fuzzy commitment scheme. They used 2048 bits of iris code combined with the concatenated codes and achieved the FAR and FRR of 0% and 0.47% respectively, the key length and the security of their system is the key length are 140 and 44 bits respectively. In contrast to key-binding systems – the key generation scheme – helper data is created directly only from the biometric template. Such helper data will associate with a presented query which is close to the original template [56] to generate either the unique key string or the original template. Typical techniques of such scheme are fuzzy extractor [35, 58], secure sketches [61]. Applications of key-generated have already been implemented on iris [54] and voice [40]

All studies above are uni-modal BCSs wherein authors attempted to achieve the optimal performance in terms of FAR, FRR, key length and the security strength against to masquerade attacks. Hence, some other authors introduced multi-modal BCS by fusing several biometric modalities to enhance the performance of the system [28, 33, 60, 62, 63] (e.g. increases the key length and the security level of the system, reduces the rate of FAR and FRR, etc.) In [33], A. Nagar et al. combine fingerprint, iris and face together to construct a multimodal BCS. At the security level of 53 bits equivalent to , the Genuine Acceptance Rate () of 99% are achieved, compared with using individual modality such as . Nandakumar and Jain [62] used two biometric modalities of fingerprint and iris to construct a key-binding based multiBCS using fuzzy vault. The combination of two modalities results in the and of approximately 1.8% and ~0.01%, wherein the is significantly reduced compared with the of 12% and 21.2% when individually using single fingerprint and iris respectively.

## Modeling and Discovering Human Behaviors

Human gait has been considered as a particular style and manner of moving human feet and hence contains the information of identity authentication. In a more detailed level view, the mechanism of human gait involves synchronization between the skeletal, neurological and muscular system of human body [4]. In 2005, H. Ailisto et al. were the first to propose the gait authentication using wearable sensor [13] and this area was further expanded by Gafurov et al. [10]. In general, sensors are attached to various positions on human body to record locomotion signal. Various sensors are experimented including gyroscope, rotation sensor but acceleration sensor (or accelerometer) is the most commonly used. In this field, there are two typical approaches: (1) Template Matching (TM) and (2) Machine Learning (ML). In (1), acquired signal is preprocessed and then split into patterns. Best patterns which represent the most characteristics of the subject are considered as representative gait templates. They are then stored as referred templates corresponding to individual. Various distance metrics such as Dynamic Time Warping (DTW) [9, 19, 14], Euclidean distance [8, 9], auto-correlation [13], nearest neighbors [11] are used for calculating the similarity score between a given pattern and referred templates.

Second method is the most popular approach used in pattern recognition areas. In this approach, gait signal is segmented into patterns. On each pattern, features are extracted in time domain, frequency domain, and wavelet domain or by special techniques such as time delay embedding [18]. Extracted feature vectors are then classified using supervised classifiers like HMM [16], SVM [17, 15, 20, 14, 18], ANN [5], LDA [5]. Some other works propose hybrid approaches in which either distance metrics such as DTW [7], Euclidean [10, 12], are used to measure the similarity scores of features extracted in time and frequency domains, or similarity scores of gait templates can be considered as features which are used for classification [6].

**Table 5.1** State of the art gait authentication using Standalone (S) and Mobile sensor (M) including Accelerometer (A), Rotation Sensor (R) by approaches: Template Matching (TM), Machine Learning (ML) and Hybrid (H)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Study** | **Sensor /**  **Sampling rate** | **Location** | **Methods** | **No. of Subjects** | **Results** |
| [14]  [6] | M–A / 27Hz  S–A / 50Hz | T Pocket  Ankle | TM, ML  H | 11  22 (16M 6F) | 79.1%, 92.7% RR  3.03% EER |
| [5] | 9 S–R | Body | ML (LDA) | 30 (25M 5F) | ~ 100% RR |
| [15] | M–A | T Pocket | ML (SVM) | 36 | HTER: 10.1% |
| [7] | S–A / 40Hz | Ankle | H | 22 | 3.27% EER |
| [16-17] | M–A / 120Hz  M–A / 45Hz | Hip | ML (HMM)  ML (SVM) | 48 (30M 18F) | 6.15% EER, 5.9% FAR, 6.3% FRR |
| [8]  [18] | S–A / 100Hz  M–A / 25 Hz | Ankle  T Pocket | TM (Euclidean)  ML (SVM) | 10  25 | 20% EER  100% RR |
| [9] | S–A / 100Hz | Hip | TM (PCA) | 60(43M 17F) | 1.6% EER |
| [19] | M–A / 45Hz | Hip | TM (DTW) | 51 (41M 10F) | 20% EER |
| [20] | M–A / 37Hz | Hip | ML ( SVM) | 6 | 90.3 ± 3.2% RR |
| [10] | S–A / 16Hz,  100Hz | Ankle Pocket Arm Hip | H (Euclidean)  H (Manhattan) | 21 (12M 9F)  100 (70M 30F) 50(33M 17F) 30 (23M 7 F) | 5% EER  7% EER  10% EER  13% EER |
| [11] | S–A / 100Hz | Body | TM(NN) | 30 | 96.7% RR |
| [12] [13] | S–A / 256Hz | Waist | TM(cross-corr.), H (FFT, histogram) | 36 (19M 17F) | 6.4 %, 10%, 19% EER |

In early stages, most of works used standalone sensors (SSs) have been implemented with a variety of success rate, they still have some restrictions. For example, SSs is relatively expensive and the interface of some special sensors needs to be developed separately. Thus, there is an increasing need to develop an easy-to-operate gait monitoring system within pervasive and ubiquitous environment. Recently, the developing of micro electromechanical (MEMs) technology helped such sensors to be miniaturized and integrated inside mobile devices (known as mobile sensors - MS). Gait authentication has been initially experimented on MS during recent years. In 2009, S. Sprager et al. used built-in accelerometer in Nokia cellphone positioned at the hip to collect and analyze gait signal [20]. Feature vectors for classification were built based on collected data using dimension reduction on cumulants by Principal Com-ponent Analysis (PCA). The classification in this module was accomplished by Support Vector Machines (SVM). They achieved about 90.3% accuracy. However, the number of experimental participants is rather small (6 persons). In comparison to SSs, MSs are designed to be cheaper, simpler and as a result the quality is not guaranteed as SSs. For example, the sampling rate is low and unstable (<50Hz vs.>100Hz), the noise is rather high. Derawi et al. [19] pointed up that impact by redid Holien’s work [21] using MS instead of SS and achieved EER of 20.1% compared to 12.9%. Table 5.1 summarized gait authentication approaches and their performances with various evaluation metrics such as Equal Error Rate – EER, Recognition Rate – RR, etc. on both SS and MS.

# CONCLUSIONS

In this thesis, we proposed two approaches of gait authentication using PR-ML algorithms and biometric cryptosystem, respectively. In the PR-ML based authentication system, although the quality of built-in sensors is low (the sampling rate is only 27Hz), the achieved results are very considerable. It reflects high potentials to deploy our mechanism to support current active mobile authentications such as PIN or password in reality. Since there is currently no public dataset in this field, the comparison between related works is only relative. Therefore, a more realistic dataset is also constructed to evaluate our mechanism fairly. Nevertheless, many environment factors such as human emotion, time effect, disease and ground materials which could be affected to the human gait is not explored yet. Hence, such issues will be considered deeper in future.

Looking at the case of the biometric cryptosystem, we introduce a novel system using gait combined with fuzzy commitment scheme. The achieved performance in terms of FAR, FRR as well as the key length and the security level are relatively comparative with other state of the art BCSs. The results show the potentials to construct an effective BCS especially on mobile devices since we use mobile sensors to acquire biometric gait and a lightweight model which only require low storage capability and computational complexity. Moreover, gait could be considered as a new modality for multi-modal BCSs. The drawbacks of our work are that the FRR is still rather high which could causes inconvenient for users. Hence, our further work will focus on reducing the rate of FRR by constructing higher discriminant templates as well as finding an optimal quantization scheme for binarization.

# Bibliography

[1] **Hoang Minh Thang**, Vo Quang Viet and Deokjai Choi, “Step Detection Using Accelerometer Sensor on Mobile Phone”, in 2012 Spring conference of *Korea* Multimedia Society (KMMS), 2012.

[2] **Hoang Minh Thang**, Vo Quang Viet and Deokjai Choi, “Acceleration-Based Adaptive Authentication Scheme on Mobile Phone”, in International Conference on Smart Media and Applications (SMA 2012), 2012.

[3] **Hoang Minh Thang**, Vo Quang Viet and Nguyen Dinh Thuc, Deokjai Choi, “Gait Identification Using Accelerometer on Mobile Phone”, in International Conference on Control, Automation and Information Science (ICCAIS 2012), 2012.

[4] Vo Quang Viet, **Hoang Minh Thang** and Lee Changmoo, Deokjai Choi, “Fall Detection for Mobile Phone based on Movement Pattern”, in Journal of Korean Society for Internet Information Vol. 13, No. 4, August, 2012.

[5] Vo Quang Viet, **Hoang Minh Thang** and Deokjai Choi, “Adaptive Energy-Saving Strategy for Activity Recognition on Mobile Phone”, in 12th IEEE Symposium on Signal Processing and Information Technology (ISSPIT), 2012.

[6] Vo Quang Viet, **Hoang Minh Thang** and Deokjai Choi, “Balancing Precision and Battery Drain in Activity Recognition on Mobile Phone”, in 18th IEEE International Conference on Parallel and Distributed Systems (ICPADS), 2012.

[7] Vo Quang Viet, **Hoang Minh Thang** and Deokjai Choi, “Energy Saving in Forward Fall Detection using Mobile Accelerometer”, in International Journal of Distributed Systems and Technologies, January, 2013.

[8] **Thang Hoang**, Chuyen Luong, Son Do, Deokjai Choi, “Improving Cell Phone Based Gait Identification with Optimal Response Time Using Cloudlet Infrastructure”, in International Conference on Future Information & Communication Engineering (ICFICE 2013), 2013.

[9] Vo Quang Viet, **Hoang Minh Thang** and Deokjai Choi, “Personalization in Mobile Activity Recognition System using K-medoids Clustering Algorithm”, in International Journal of Distributed Sensor Networks (IJDSN), Vol 2013, 2013.

[10] Chuyen Luong, Son Do, **Thang Hoang** and Deokjai Choi, "A mobility prediction algorithm for the seamless handoff.", in 5th IEEE International Conference on Ubiquitous and Future Networks (ICUFN), 2013.

[11] **Thang Hoang**, Viet Vo, Anh Nguyen, Deokjai Choi and Thuc Nguyen, “A Lightweight Gait Authentication on Mobile Phone Regardless of Installation Error”, in 28th IFIP TC-11 International Information Security and Privacy Conference (SEC 2013), 2013.

[12] **Thang Hoang**, Chuyen Luong, Son Do and Deokjai Choi, “Adaptive Cross-Device Gait Recognition Using Mobile Accelerometer”, in Journal of Information Processing System (JIPS) 2013, Vol. 9, No. 2, 2013.

[13] **Thang Hoang** and Deokjai Choi, “A Biometric Cryptosystem Using Gait Captured from Mobile Accelerometer”, in FTRA 2013 International Symposium on Ubiquitous Computing and Embedded Systems (UCES), 2013.

# References

[1] F. Breitinger and C. Nickel, “User Survey on Phone Security and Usage”, in *BIOSIG, Vol. 164GI*, 2010.

[2] K. Pousttchi and M. Schurig, “Assessment of today’s mobile banking applications, from the view of customer requirements”, in *37th HICSS’04*, 2004.

[3] A. K. Jain, A. Ross and S. Prabhakar, “An Introduction to Biometric Recognition”, in *IEEE Transaction on Circuits and System for Video Technology, Vol. 14, No. 1*,2004.

[4] D.J. Fish and J. Nielsen, “Clinical assessment of human gait”, in *Journal of Prosthetics and Orthotics 2*, 1993.

[5] S. Mondal, A. Nandy, P. Chakraborty and G.C Nandi, "Gait Based Personal Identification System Using Rotation Sensor", in *CIS Journal, Vol. 3, No. 3*, 2012.

[6] H. Sun and T. Yuao,"Curve Aligning approach for gait authentication based on a wearable sensor", in *Physiological Measurement, Vol. 33, No. 6,* 2012.

[7] L. Yuexiang, W. Xiabo, Q. Feng, "Gait Authentication Based on Acceleration Signals of Ankle", in *Chinese Journal of Electronics, Vol. 20, No. 3*, 2011.

[8] S. Terada, Y. Enomoto, D. Hanawa and K. Oguchi, “Performance of gait authentication using an acceleration sensor”, in *34th ICTSP,* 2011

[9] P. Bours and R. Shrestha, "Eigensteps: A giant leap for gait recognition", in *IWSCN*, 2010.

[10] D. Gafurov and E. Snekkenes, "Gait Recognition Using Wearable Motion Recording Sensors", in *EURASIP Journal on Advances in Signal Processing, Vol 2009*, 2009.

[11] G. Pan, Y. Zhang and Z. Wu, "Accelerometer-based gait recognition via voting by signature points", in *IET Electronic Letters Vol. 45, No. 22*, 2009.

[12] J. Mäntyjärvi, M. Lindholm, E. Vildjiounaite, S. M. Mäkelä, and H. Ailisto, “Identifying Users of Portable Devices From Gait Pattern With Accelerometers”, in *ICASSP*, 2005.

[13] H. Ailisto, M. Lindholm, J. Mantyjarvi, E. Vildjounaite and S.M. Makela, "Identifying People from Gait Pattern with Accelerometers", in *Proceeding of SPIE 5779, Biometric Technology for Human Identification II*, 2005.

[14] H.M. Thang, V.Q. Viet, N. D. Thuc and D. Choi, “Gait Identification Using Accelerometer on Mobile Phone”, in *ICCAIS,* 2012.

[15] M.R. Hestbek, C. Nickel and C. Busch, "Biometric Gait Recognition For Mobile Devices Using Wavelet Transform And Support Vector Machines", in *IWSSIP 2012*, 2012.

[16] C. Nickel and C. Busch,"Classifying Accelerometer Data via Hidden Markov Models to Authenticate People by the Way they Walk", in *2011 IEEE ICCST,* 2011.

[17] C.Nickel, H. Brandt and C.Busch, "Classificatoin of Acceleration Data for Biometric Gait Recognition on Mobile Devices", in *BIOSIG 2011*, 2011.

[18] F. Frank, S. Mannor and D. Precup, “Activity and Gait Recognition with Time-Delay Embeddings”, in *24th AAAI,* 2010.

[19] M. O. Derawi, C. Nickel, P. Bours, and C. Busch, “Unobtrusive User-Authentication on Mobile Phones using Biometric Gait Recoginition”, in *6th IIH-MSP,* 2010.

[20] S. Sprager and D. Zazula, “A cumulant-based method for gait identification using accelerometer data with Principal Component Analysis and Support Vector Machine”, in *Journal WSEAS Transactions on Signal Processing,* 2009.

[21] K. Holien, “Gait Recoginition under non-standard circumstances”, Master thesis, Gjøvik University College, 2008.

[22] N. Kern, H. Junker, P. Lukowicz, B. Schiele and G. Troster, “Wearable Sensing to Annotate Meeting Recordings”, in *Journal Personal and Ubiquitous Computing, Vol. 7, Issue 5, October 2003,* 2003.

[23] M. W. Whittle, “Gait analysis an introduction 4th edition”, 2007.

[24] P. Pudil, J. Novovicova and J. Kittler, “Float search methods in feature selection”, in *Patter Recognition Letters 15,* 1994.

[25] A.W. Whitney, “A Direct Method of Nonparametric Measurement Selection”, in *IEEE Transactions on Computers, Vol. C-20, Issue 9*, 1971.

[26] C. Chang and C.J. Lin, “LIBSVM: a library for support vector machines” in *ACM Transactions on Intelligent Systems and Technology,* 2011.

[27] G. M. Weiss and F. Provost, “Learning when training data are costly: The effect of class distribution on tree induction, in *Journal of Artificial Intelligence Research,* 2003.

[28] Kanade, Sanjay, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi. "Obtaining cryptographic keys using feature level fusion of iris and face biometrics for secure user authentication.", in *Computer Vision and Pattern Recognition Workshops (CVPRW), 2010 IEEE Computer Society Conference on. IEEE*, 2010.

[29] Jain, Anil K., Patrick Joseph Flynn, and Arun Abraham Ross, eds. “Handbook of biometrics”. Springer, 2008.

[30] Uz, Tamer, et al. "Minutiae-based template synthesis and matching for fingerprint authentication.", in *Computer Vision and Image Understanding 113.9: 979-992*, 2009

[31] Zhang, Yan-Ning, et al. "2D representation of facial surfaces for multi-pose 3D face recognition.", in *Pattern Recognition Letters 33.5(2012): 530-536*, 2012.

[32] Kim, Dong-Ju, Kwang-Woo Chung, and Kwang-Seok Hong. "Person authentication using face, teeth and voice modalities for mobile device security.", in *Consumer Electronics, IEEE Transactions on 56.4(2010): 2678-2685*, 2010.

[33] Nagar, Abhishek, Karthik Nandakumar, and Anil K. Jain. "Multibiometric cryptosystems based on feature-level fusion.", in *Information Forensics and Security, IEEE Transactions on 7.1 (2012): 255-268*, 2012.

[34] Preneel, Bart. “Analysis and design of cryptographic hash functions.”, Diss. Katholieke Universiteit te Leuven, 1993.

[35] Dodis, Yevgeniy, Leonid Reyzin, and Adam Smith. "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data." In, *Advances in cryptology-Eurocrypt 2004. Springer Berlin Heidelberg, 2004. 523-540,* 2004.

[36] Juels, Ari, and Martin Wattenberg. "A fuzzy commitment scheme". In *Proceedings of the 6th ACM conference on Computer and communications security. 28-36*, 1999.

[37] Juels, Ari, and Madhu Sudan. "A fuzzy vault scheme.", in *Information Theory, IEEE International Symposium on (2002)*, 2002.

[38] Tam, L., Myron Glassman, and Mark Vandenwauver. "The psychology of password management: a tradeoff between security and convenience.", in *Behaviour & Information Technology 29.3 (2010): 233-244*, 2010.

[39] Gaw, Shirley, and Edward W. Felten. "Password management strategies for online accounts." In *Proceedings of the second symposium on Usable privacy and security. ACM*, 2006.

[40] Carrara, Brent, and Carlisle Adams. "You are the key: generating cryptographic keys from voice biometrics." In *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on. IEEE*, 2010.

[41] Monrose, Fabian, Michael K. Reiter, and Susanne Wetzel. "Password hardening based on keystroke dynamics." In *International Journal of Information Security 1.2 (2002): 69-83*, 2002.

[42] Inthavisas, K., and D. Lopresti. "Secure speech biometric templates for user authentication.", in *Biometrics, IET 1.1 (2012): 46-54*, 2012.

[43] R. H. Morelos-Zaragoza, “The Art of Error Correcting Coding”, John Wiley & Sons Ltd. Baffins Lane, Chichester, West Sussex, England, 2002.

[44] Boulgouris, Nikolaos V., Dimitrios Hatzinakos, and Konstantinos N. Plataniotis. "Gait recognition: a challenging signal processing technology for biometric identification.", in *signal processing magazine, IEEE 22.6 (2005): 78-90*, 2005.

[45] Chen, Changhong, et al. "Frame difference energy image for gait recognition with incomplete silhouettes.", in *Pattern Recognition Letters 30.11 (2009): 977-984*, 2009.

[46] Feng, Yi Cheng, and Pong C. Yuen. "Binary discriminant analysis for generating binary face template.", in *Information Forensics and Security, IEEE Transactions on 7.2 (2012): 613-624*, 2012.

[47] Ray C. Bose and Dwijendra K. Ray-Chaudhuri. “On a class of error correcting binary group codes”, in *Information and Control, 3(1):68–79*, 1960.

[48] Alexis Hocquenghem. “Codes correcteurs d’erreurs. Chiffres”, 2:147–156, 1959.

[49] Massey, James. "Shift-register synthesis and BCH decoding.", in *Information Theory, IEEE Transactions on 15.1 (1969): 122-127,* 1969.

[50] Van Der Veen, Michiel, et al. "Face biometrics with renewable templates.", in *Electronic Imaging 2006. International Society for Optics and Photonics*, 2006.

[51] Maiorana, Emanuele. "Biometric cryptosystem using function based on-line signature recognition.", in *Expert Systems with Applications 37.4 (2010): 3454-3461*, 2010.

[52] Feng, Yi Cheng, Pong C. Yuen, and Anil K. Jain. "A hybrid approach for generating secure and discriminating face template.", in *Information Forensics and Security, IEEE Transactions on 5.1 (2010): 103-117*, 2010.

[53] Li, Peng, et al. "An effective biometric cryptosystem combining fingerprints with error correction codes.", in *Expert Systems with Applications 39.7 (2012): 6562-6574*, 2012.

[54] Álvarez Mariño, R., Fernando Hernández Álvarez, and Luis Hernández Encinas. "A crypto-biometric scheme based on iris-templates with fuzzy extractors.", in *Information Sciences 195 (2012): 91-102*, 2012.

[55] Kelkboom, Emile JC, et al. "Maximum Key Size and Classification Performance of Fuzzy Commitment for Gaussian Modeled Biometric Sources.", in *Information Forensics and Security, IEEE Transactions on 7.4 (2012): 1225-1241*, 2012.

[56] Jain, Anil K., Karthik Nandakumar, and Abhishek Nagar. "Biometric template security.", in *EURASIP Journal on Advances in Signal Processing 2008: 113*, 2008.

[57] Hao, Feng, Ross Anderson, and John Daugman. "Combining crypto with biometrics effectively.", in *Computers, IEEE Transactions on 55.9 (2006): 1081-1088*, 2006.

[58] Verbitskiy, Evgeny A., et al. "Key extraction from general nondiscrete signals.", in *Information Forensics and Security, IEEE Transactions on 5.2 (2010): 269-279*, 2010.

[59] Linnartz, Jean-Paul, and Pim Tuyls. "New shielding functions to enhance privacy and prevent misuse of biometric templates.", in *Audio-and Video-Based Biometric Person Authentication. Springer Berlin Heidelberg*, 2003.

[60] Rathgeb, Christian, and Andreas Uhl. "A survey on biometric cryptosystems and cancelable biometrics.", in *EURASIP Journal on Information Security 2011.1 (2011): 1-25*, 2011.

[61] Li, Qiming, Yagiz Sutcu, and Nasir Memon. "Secure sketch for biometric templates.", in *ASIACRYPT. Springer Berlin Heidelberg, 2006. 99-113*, 2006.

[62] Nandakumar, Karthik, and Anil K. Jain. "Multibiometric template security using fuzzy vault.", in *Biometrics: Theory, Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference on. IEEE*, 2008.

[63] Chin, Y. J., et al. "Integrated Biometrics Template Protection Technique Based on Fingerprint and Palmprint Feature-level Fusion.", in *Information Fusion (2013)*, 2013.

**패턴 인식 및 생체인식 암호화 시스템을 이용한 모바일 폰에서의 보행 인증**

MAFRUR, Rischan

전남대학교 대학원 전자컴퓨터공학과

(지도교수: 최덕재)

# (국문초록)

본 논문에서는 휴대 전화에 내장된 센서 자원을 활용하여 두 가지의 새로운 보행 인증 시스템을 제안하였다.

첫 번째 방법으로 전처리 단계에서 정밀한 검토를 실행함으로써 성능을 향상 시킨 패턴 인식 및 기계 학습(PR-ML) 알고리즘을 기반으로 하는 시스템 구축에 초점을 맞추었다. 효과적이며 새로운 분할 알고리즘은 분할 신호를 완벽한 정확성을 갖는 분리된 보행 주기로 제공한다. 그 다음으로, 특징은 시간 및 주파수 영역으로부터 추출된다. 이 시스템은 간단하면서 신뢰성이 높은 모델의 구축을 목표로 하기 때문에 특징 부분 집합 선택 알고리즘은 특징 벡터의 크기뿐만 분류 아니라 분류 태스크의 처리 시간을 최적화하기 위해 적용되고, 최적의 특징 벡터는 SVM 및 RBF 커널을 이용하여 분류된다.

이러한 최적화 방안에도 불구하고 PR-ML 기반의 생체 인식 인증은 여전히 시스템 보안 및 사용자의 개인정보 보호 문제가 남아있다.

본 시스템에서, 인증에 사용되는 본래의 생체 인식 템플릿이나 추출된 특징은 끊임없는 손실을 갖는 데이터 결과를 절충하기 위해서 안전하지 않게 저장된다.

두 번째 방법으로는 사용자의 개인정보 보호와 더불어 시스템의 보안을 보장하기 위해서 Fuzzy Commitment Scheme 방식을 이용한 생체 인식 암호화 시스템을 기반의 보행 인증을 연구하였다. 사용자 확인을 위한 본래의 생체 인식 템플릿의 사용을 대신에 생체 측정 통합 모바일 가속도 센서에 의해 취득한 보행 템플릿을 사용하여 암호화 된 암호 키를 기반으로 한다.

관련 분야의 연구에서 모바일 가속도 센서에 의해 취득한 공용 보행 데이터 집합이 없기 때문에, 자체적으로 38명의 피험자(남 10, 여 28)로부터 보행 신호를 취득하여 성능을 평가하였다.

PR-ML 방식을 구현함으로써 식별 모드에서 94.93%, zeroFAR, FRR 3.89%에 가까운 정확도를 달성하였으며, 인증 모드에서 4초 미만의 처리 시간을 달성했다.

또한 보행 기반의 생체 인식 암호화 방식에서, 139 및 50 비트의 키 길이를 갖을 때, 거의 16.18%과 14.71%에 해당하는 최적의 zeroFAR 및 FRR를 달성하였다.

따라서 본 연구의 결과는 모바일 센서 기반의 보행은 홍채, 지문, 음성 등의 생체 요인과 비교했을 때, 생체 암호 시스템을 구축하는 효과적인 요소로 활용 할 수 있음을 보여준다.

# ACKNOWLEDGEMENT

Foremost, I would like to express my sincere gratitude to my supervisor and advisor Professor Deokjai Choi for his useful comments, remarks and engagement through the studying process of this master thesis. His kind guidance supported me a lot in all the time of research and writing this thesis. I would also be grateful to him not only for enlightening me the first glance of research but also for his valuable advice about the future of my life. I also would like to thanks also go to my thesis committee, including Professor Soohyung Kim, and Professor Kyungbaek Kim from whom I got much knowledge during studying their classes and in thesis review process. I also would like to thank members of Advanced Network Lab mates: Ki Hyun Bang, Dokyeong Lee, Muhammad Fiqri Muthohar, Gde Dharma Nugeraha, Priagung Khusumanegara, Alvin Prayuda Juniarta who shared their idea and supported me throughout my master course.

I also deeply appreciate the generous support from BK21(+), NRF, ITRC and NIPA in two years for bringing me a great financial support and academic opportunities.

Finally I would like to thank to Allah Almighty God, my beloved prophet Muhammad SAW who is the inspiration of my life, my dear parents, my beloved Indonesian community and Muslim community for their endless love and care during my period away from home. Without them, this work could not be done.

June 2015

Rischan Mafrur

1. Report of the Wireless Intelligence Company [J. Gillet, "Wireless Intelligence: Global mobile connections surpass 6 billion by year-end", 2011] [↑](#footnote-ref-1)
2. Access http://www.gsmarena.com/htc\_google\_nexus\_one-3069.php for its specification [↑](#footnote-ref-2)
3. Software available at http://www.csie.ntu.edu.tw/~cjlin/libsvm [↑](#footnote-ref-3)