Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme

Thang Hoang, Deokjai Choi & Thuc Nguyen

International Journal of Information Security

ISSN 1615-5262
Volume 14
Number 6

Int. J. Inf. Secur. (2015) 14:549-560
DOI 10.1007/s10207-015-0273-1

Springer

Int. J. Inf. Secur. (2015) 14:549–560
DOI 10.1007/s10207-015-0273-1

REGULAR CONTRIBUTION

Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme

Thang Hoang · Deokjai Choi · Thuc Nguyen

Published online: 30 January 2015

Abstract Authentication systems using gait captured from inertial sensors have been recently developed to enhance the limitation of existing mechanisms on mobile devices and achieved promising results. However, most these systems employed pattern recognition and machine learning techniques in which biometric templates are stored insecurely, which could leave critical security and user privacy issues. Specifically, a compromise of original gait templates could result in everlasting forfeiture. In this paper, two main results will be presented. Firstly, we propose a novel gait authentication system on mobile devices in which the security and privacy are preserved by employing a fuzzy commitment scheme. Instead of storing original gait templates for user verification like in conventional approaches, we verify the user via a stored key which is biometrically encrypted by gait templates collected from a mobile accelerometer. Secondly, the discriminability of sensor-based gait templates are investigated to determine appropriate parameter values to construct an effective gait-based biometric cryptosystem. The performance of our proposed system is evaluated on the dataset including gait signals of 34 volunteers. We achieved the zero-FAR and the False Rejection Rate of approximately 16.18 % corresponding to the key length, as well as the system security level of 139 bits. The results from our experiment show that accelerometer-based gait could be further investigated to construct a biometric cryptosystem, as effective as other biometric traits such as iris, fingerprint, voice, and signature.

Keywords Fuzzy commitment scheme · Biometric cryptosystem · Gait recognition · Accelerometer · Error correcting

T. Hoang · D. Choi (✉)
Department of Electronics and Computer Engineering, Chonnam National University, Gwangju, South Korea
e-mail: dchoi@jnu.ac.kr

Present address:
T. Hoang
Faculty of Information Technology, Saigon Technology University, Ho Chi Minh City, Vietnam
e-mail: hmthang@ejnu.net; thang.hoangminh@stu.edu.vn

T. Nguyen
Faculty of Information Technology, University of Science VNU-HCMC, Ho Chi Minh City, Vietnam
e-mail: ndthuc@fit.hcmus.edu.vn

1 Introduction

Security techniques for identification, authorization, or authentication are commonly based on knowledge (e.g., passwords), token (e.g., ID cards), or biometrics (e.g., iris, fingerprint, gait). Biometrics has been widely accepted as the ultimate proof of identity via recognizing individuals based on their behavioral or physiological characteristics [1]. It has significant advantages considering end-user usage when compared with the two methods of knowledge and token. Users do not need to remember complicated passwords or preserve their ID cards from stealing or counterfeiting. Human gait has been considered as behavioral biometrics for several decades [2] with implementations based on computer vision [2] and wearable sensor technologies [3,4]. From 2010, implicit sensor-based gait recognitions are initially proposed to support existing authentication mechanisms that are obtrusive and inconvenient in frequent use on mobile phones [5] and achieved promising results [6–9]. Gait-based authentication has significant advantages in terms of user friendliness and security aspects, compared with using other biometric modalities [9,10]. Specifically, gait could be collected implicitly without the user awareness. It is difficult to mimic gait data [10], whereas a copy of a fingerprint or

face could be easily obtained, and the system security fully depends on the resistance of the sensor [2].

However, even though human gait is a new biometric trait which is unique, irrevocable but it is less discriminant and much more noisy than other modalities such as iris, fingerprint, face, etc. [1]. Hence, inertial sensor-based gait recognition approaches focus on developing pattern recognition and machine learning (PR-ML) algorithms to deal with high variations between gait measurements [3,4,6–9]. Enrollment gait templates or extracted features are stored in unconcealed forms for matching with new templates to recognize individuals. However, such approaches could leave a critical vulnerability, especially when they are deployed on portable devices. When the device is stolen or malware infected, an attacker could illegally access the repository to obtain or reconstruct original gait templates. Applying cryptographic hash algorithms to protect biometric templates as in password-based systems is enormously impractical because they do not tolerate any single bit error. Loss of enrollment templates means users are confronted with security and privacy issues. Since biometrics is extremely difficult to change, the privacy leak means an attacker could partly or fully determine the user's biometrics. From the viewpoint of system security, a compromise of biometric templates results in everlasting forfeiture. The attacker could utilize compromised templates to thereafter always illegally grant access to sensitive services.

In this paper, we propose a novel gait authentication by using the biometric cryptosystem (BCS) approach to maintain the security and privacy of the system. Instead of storing original gait templates for user verification like other systems, we verify the user via a stored cryptographic key which is biometrically encrypted by gait templates collected from a mobile accelerometer before. These templates are employed merely to encrypt/ or retrieve the key and then are always discarded so that the security and privacy are maintained. Moreover, we employ a fuzzy commitment scheme [11] so that the system has significant advantages in terms of small storage space and low computational complexity, compared with other gait authentication systems using PR-ML techniques [6,7,9] when it is directly deployed on portable devices with limited computational resources.

Our main contribution in this paper is threefold

- We propose a first approach of inertial sensor-based gait authentication on mobile phone in which the security and privacy are preserved. To the best of our knowledge, security and privacy issues have not been taken into account in smartphone-based gait authentication systems in the literatures
- We analyze the discriminability of gait templates collected from an inertial mobile sensor named accelerometer. Based on the analyzed result, we suggest a method to determine appropriate parameters to construct an effective gait-based biometric cryptosystem
- We analyze the security strength of our authentication system resistant to different attacks.

The remainder of this paper is organized as follows. The overview of our system architecture and proposed method are described in detail in Sect. 2. Our experimental evaluations and a security discussion are presented in Sect. 3. Section 4 describes some state-of-the-art studies related to our work. Finally, a conclusion is presented in Sect. 5.

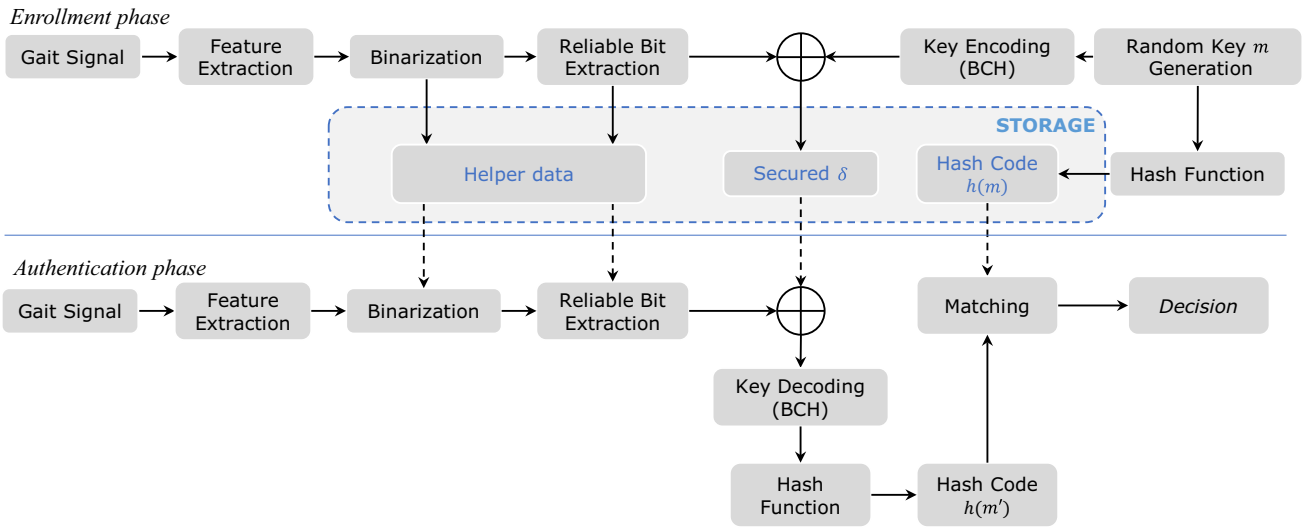

Fig. 1 The overall architecture of our gait authentication system based on BCS using a fuzzy commitment scheme, where *circled plus* denotes the exclusive-OR operation

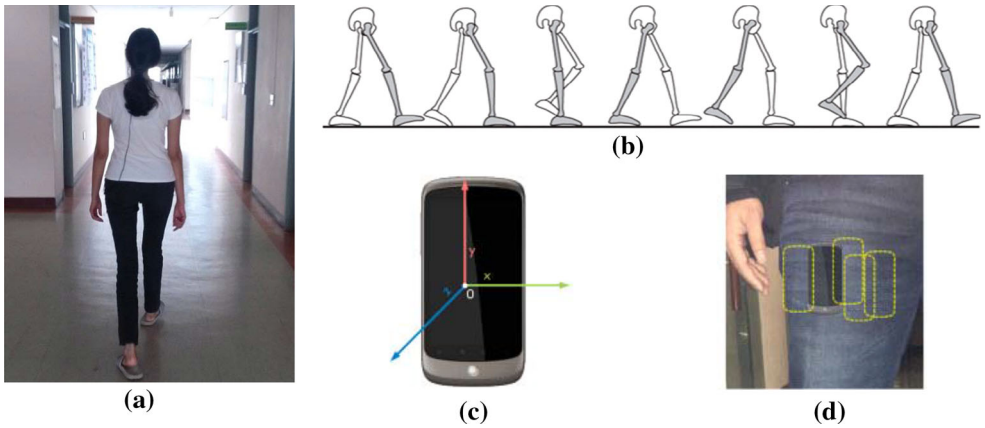

Fig. 2 Illustrations of **a** human gait and **b** a gait cycle, **c** data collection device—the Google Nexus One mobile phone with an integrated three-dimensional accelerometer, **d** the position of the phone (pocket) on user's body during gait capture process

2 Gait-based biometric cryptosystem

Figure 1 sketches the specification of our gait-based biometric cryptosystem following the fuzzy commitment scheme [11]. In this system, we used binary BCH code as the error correcting code to handle the differences between biometric measurements. In the enrollment phase, gait signals of a user will be acquired and preprocessed to eliminate the influence of the acquisition environment. Real-valued gait templates are then extracted and binarized. Then, reliable binary templates w are extracted based on determining reliable components. Concurrently, a cryptographic key m, which is generated randomly, is encoded to a codeword c by using the binary BCH encoding scheme. The fuzzy commitment scheme computes the hash code of m and a secured δ using a cryptographic hash function h and a binding function, respectively. Values of $h(m)$, δ along with helper data used for extracting binary templates is stored for further authentication.

In the authentication phase, the user suggested to be authentic will provide a fresh gait template. Such template is also preprocessed, and a binary template w' is extracted by using helper data which is previously stored in the enrollment phase. The decoding function computes the corrupted codeword c' by binding w' with δ. Then, a cryptographic key m' is retrieved from c' by using the BCH decoding algorithm. Finally, the hash code of m' will be calculated and matched with $h(m)$ for an authentication decision. The milestones of our system are described in detail the following sections.

2.1 Gait biometrics acquisition

Human gait is a pattern of movement of the limbs which has been recognized as a distinguishable characteristic of the individual (Fig. 2a). The gait recognition has been analyzed for decades as a behavioral biometrics similar to a signature, voice, etc. [1]. In summary, the gait of an individual could be examined using three common techniques including Machine Vision Technology (MVT) [1], Floor Sensor Technology (FST) [4], and Wearable Sensor Technology (WST) [3,6–9]. In this study, we use gait signals based on WST since this is not only the latest approach but also appropriate for personal usage. Gait data could be collected by simply attaching wearable sensors directly to the user's body (Fig. 2d). A Google Nexus One mobile phone placed inside the pocket is employed to collect the gait signal (Fig. 2c, d). This discrete time signal is a sequence of combined acceleration values of gravity acceleration, ground reaction force, and inertial acceleration which are sensed by a built-in three-dimensional (X, Y, Z) accelerometer during walking. Based on the relationship between gravity, acceleration, and motion, we present an acceleration sample returned by the accelerometer as a three-component vector

$$\mathbf{a} = (a_X, a_Y, a_Z) \in \mathbb{R}^{1\times 3} \tag{1}$$

where a_X, a_Y, a_Z represent the acceleration values of X, Y, Z dimensions, respectively. Figure 3 illustrates acquired gait signals of a user.

2.2 Gait signal preprocessing and gait cycle extraction

We utilize a part of the dataset in [7] for this study. The dataset is filtered to be appropriate for our objective in this work (see Sect. 3.1 for a detail description). In this dataset, raw gait signals, which are acquired by a low-quality accelerometer, are irregular due to the influence of environment acquisition. In particular, the sampling rate of the mobile sensor is irregular and the raw signals contain a great deal of noise. Hence, we apply preprocessing steps as in [7] to improve the quality of the signals. These include linear interpolation to obtain precise samples at the corrected sampling rate of 32Hz, a multi-level wavelet decomposition (Db6), in which the detail coefficients of levels 1 and 2 are set to 0, is adopted to eliminate noise.

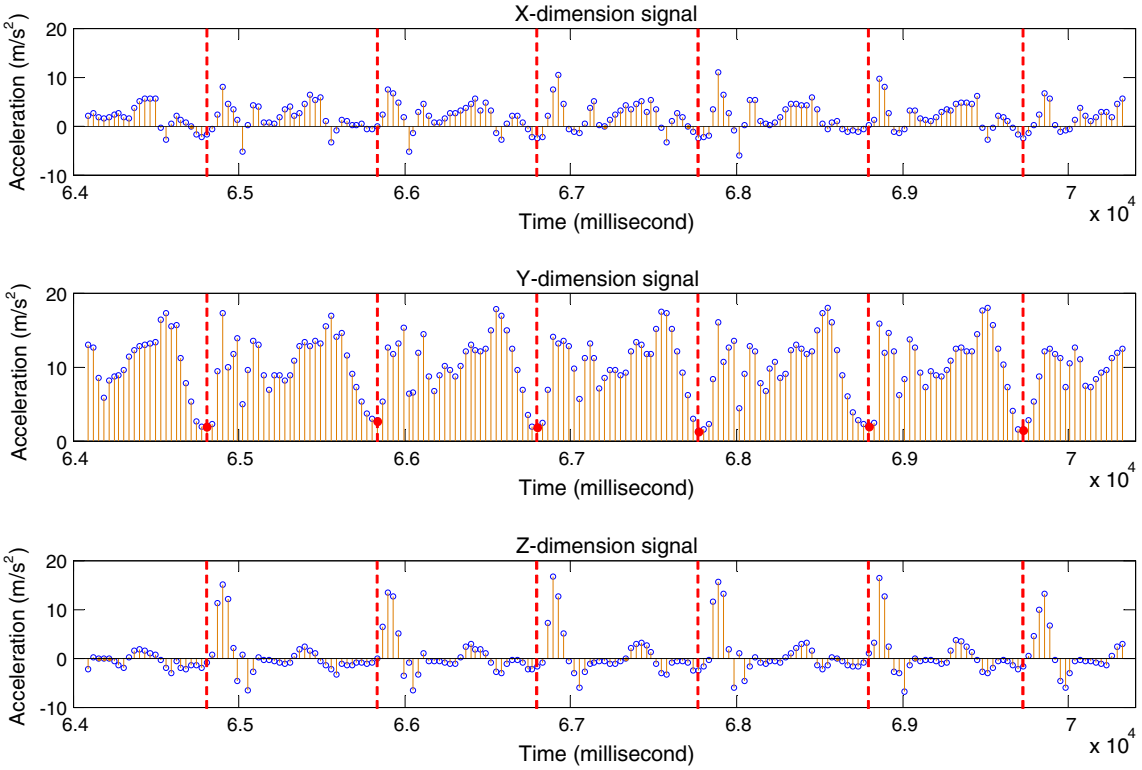

Fig. 3 A sequence of discrete gait samples sensed by a three-dimensional (X, Y, Z) mobile accelerometer

Moreover, separate gait cycles are extracted by using a gait cycle-[1] based segmentation algorithm. In this section, we only present the modification of the segmentation algorithm and refer the reader to the original work proposed in [7] for more detail. First, the algorithm determines the beginning and ending signs of a gait cycle occurred in the signal. Then, a separate gait cycle is extracted based on such signs. These signs could occur in one of three dimensions of signals which represent the vertical acceleration during walking. This acceleration is represented by the Z dimension signal in [7] since the authors utilized an additional magnetometer, along with an accelerometer to calibrate the original signal which is influenced by the disorientation. We modified the algorithm to work on the Y dimension signal without calibration since in this study, the mobile phone is considered to be placed vertically inside the user pocket as illustrated in Fig. 2d. As a result, the vertical acceleration will be represented by the Y dimension of the mobile, instead of its Z dimension. Figure 3 illustrates the detected signs (red points) of gait cycles in the Y dimension signal.

[1] Gait cycle is defined as the time interval between two successive occurrences of one of the repetitive events during walking, as illustrated in Fig. 2b

2.3 Real-valued gait template extraction

Because the walking speed is always inconstancy, making the number of samples in each gait cycle not identical, we first normalize the length of each gait cycle to a fixed value of n_s. That means there are n_s acceleration samples in each gait cycle

Let $\mathbf{S}_u = \left[\mathbf{a}_{u1} \ldots \mathbf{a}_{uv} \ldots \mathbf{a}_{un_s}\right]^\top$ be a normalized gait cycle

We form a gait template $\mathbf{T}$ by concatenating m consecutive gait cycles.

$$\mathbf{T} = \left[\mathbf{S}_1 \ldots \mathbf{S}_u \ldots \mathbf{S}_m\right]^\top = \left[\mathbf{a}_{11} \ldots \mathbf{a}_{uv} \ldots \mathbf{a}_{mn_s}\right]^\top$$

Let $n_t = mn_s$. So,

$$\mathbf{T} = \begin{bmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_i \\ \vdots \\ \mathbf{a}_{n_t} \end{bmatrix} = \begin{bmatrix} (a_X)_1 & (a_Y)_1 & (a_Z)_1 \\ \vdots & \vdots & \vdots \\ (a_X)_i & (a_Y)_i & (a_Z)_i \\ \vdots & \vdots & \vdots \\ (a_X)_{n_t} & (a_Y)_{n_t} & (a_Z)_{n_t} \end{bmatrix} \in \mathbb{R}^{n_t \times 3} \quad (2)$$

An interpolation method is adopted to resample $\mathbf{T}$ to an appropriate size for binding with a cryptographic key. Let y be the timestamp of the acceleration sample generated by the accelerometer. There are n_t pairs of acceleration sample with corresponding timestamp $\{(\mathbf{a}_i, y_i)\}_{i=1}^{n_t} =$

$\{(a_X)_i, (a_Y)_i, (a_Z)_i, y_i)\}_{i=1}^{n_t}$ in each $\mathbf{T}$. We simultaneously apply a spline interpolation to each component $((a_X)_i, y_i)$, $((a_Y)_i, y_i)$, $((a_Z)_i, y_i)$ to simulate the continuity of $\mathbf{T}$. The spline interpolation $f(y)$ such that $f(y_i) = \mathbf{a}_i$ for $1 \le i \le n_t$ is $f(y) = f_i(y)$, $y_i \le y \le y_{i+1}$ in which $f_i(y)$ is a cubic polynomial which is defined by

$$f_i(y) = \frac{1}{6h_i}\mathbf{z}_{i+1}(y - y_i)^3 + \frac{1}{6h_i}\mathbf{z}_i(y_{i+1} - y)^3 + \mathbf{c}_i(y - y_i) + \mathbf{d}_i(y_{i+1} - y) \quad (3)$$

where

$$h_i = y_{i+1} - y_i,\ \mathbf{c}_i = \frac{1}{h_i}\mathbf{a}_{i+1} - \frac{h_i}{6}\mathbf{z}_{i+1},$$
$$\mathbf{d}_i = \frac{1}{h_i}\mathbf{a}_i - \frac{h_i}{6}\mathbf{z}_i$$

Note that $\mathbf{z}_1 = \mathbf{z}_{n_t} = (0, 0, 0)$, and the remaining $\mathbf{z}_i$ ($i = 2 \ldots n_t - 1$) are calculated by solving the tridiagonal linear system of equations

$$h_{i-1}\mathbf{z}_{i-1} + 2(h_{i-1} + h_i)\mathbf{z}_i + h_i\mathbf{z}_{i+1} = 6(\mathbf{b}_i - \mathbf{b}_{i-1}) \quad (4)$$

where

$$\mathbf{b}_i = \frac{1}{h_i}(\mathbf{a}_{i+1} - \mathbf{a}_i)$$

Assume that the size of the gait template $\mathbf{T}$ is $n' \times 3$ after interpolation. We represent $\mathbf{T}$ in the form of single vector of $(1 \times 3n')$ by concatenating three dimensions of the gait template following the X, Y, Z orders, respectively.

$$\mathbf{T} = \begin{bmatrix} (a_X)_1 & (a_Y)_1 & (a_Z)_1 \\ \vdots & \vdots & \vdots \\ (a_X)_{n'} & (a_Y)_{n'} & (a_Z)_{n'} \end{bmatrix} \Rightarrow$$
$$\boldsymbol{\tau} = \left((a_X)_1, \ldots, (a_X)_{n'}, (a_Y)_1, \ldots, (a_Y)_{n'}, (a_Z)_1, \ldots, (a_Z)_{n'}\right)$$
$$= (\tau_1, \ldots, \tau_i, \ldots, \tau_{n_r}) \in \mathbb{R}^{1 \times n_r} \quad (5)$$

where $n_r = 3n'$.
Since components in $\boldsymbol{\tau}$ are real values, we refer to $\boldsymbol{\tau}$ as real-valued templates. These templates will then be used to extract binary gait templates.

2.4 Gait template binarization and reliable bits extraction

We use a quantization scheme in [12] which was previously applied for face template binarization. Assume the number of users is denoted as N. The number of resampled real-valued gait templates extracted from each user is M. Denote $\boldsymbol{\tau}_j^{(u)} (u = 1 \ldots N, j = 1 \ldots M)$ as the jth real-valued template of length n_r of the user u extracted by (5)

$$\boldsymbol{\tau}_j^{(u)} = \left((\tau_j^{(u)})_1, \ldots, (\tau_j^{(u)})_i, \ldots, (\tau_j^{(u)})_{n_r}\right)$$

The mean over intra-class variability of the user u is calculated as $\boldsymbol{\mu}^{(u)} = \frac{1}{M}\sum_{j=1}^{M}\boldsymbol{\tau}_j^{(u)}$ and the mean over all gait templates $\boldsymbol{\mu}$ is calculated by all templates of users in the enrollment phase $\boldsymbol{\mu} = \frac{1}{N}\sum_{u=1}^{N}\boldsymbol{\mu}^{(u)}$. The quantization scheme transforms the ith component in $\boldsymbol{\tau}_j^{(u)}$ to $\{0, 1\}$ by comparing the ith component of $\boldsymbol{\mu}^{(u)}$ with a specific threshold defined by the corresponding ith component of $\boldsymbol{\mu}$. For each user u, the binary template $\boldsymbol{\omega}^{(u)}$ is determined by

$$\boldsymbol{\omega}^{(u)} = \left(\omega_1^{(u)}, \ldots, \omega_i^{(u)}, \ldots, \omega_{n_r}^{(u)}\right) \quad (6)$$

with

$$\omega_i^{(u)} = \begin{cases} 0 & \text{if } \mu_i^{(u)} \le \mu_i \\ 1 & \text{if } \mu_i^{(u)} > \mu_i \end{cases}$$

A reliable bit extraction method in [12] is also applied to determine the index of reliable bits in $\boldsymbol{\omega}^{(u)}$. The reliability $r_i^{(u)}$ of the component $\omega_i{}^{(u)}$ in $\boldsymbol{\omega}^{(u)}$ is estimated based on the Gaussian error function.

$$r_i^{(u)} = \frac{1}{2}\left(1 + \text{erf}\left(\frac{\left|\mu_i^{(u)} - \mu_i\right|}{\sqrt{2\sigma_i^{2(u)}}}\right)\right) \quad (7)$$

where $\sigma_i^{2(u)}$ is the variance of the ith component of gait template of the user u

$$\sigma_i^{2(u)} = \frac{1}{M-1}\sum_{j=1}^{M}\left((\tau_j^{(u)})_i - \mu_i^{(u)}\right)^2$$

Denote $\mathbf{i}^{(u)} = (i_1^{(u)}, \ldots, i_j^{(u)}, \ldots, i_{n_r}^{(u)})$, where $r_{i_j}^{(u)} > r_{i_{j+1}}^{(u)}$ as the index vector of components following the descending order of reliability values. First $n_c (n_c < n_r)$ components of $\mathbf{i}^{(u)}$ will be used to extract the final binary template string w of length n_c.

$$w^{(u)} = \omega_{i_1}^{(u)} \ldots \omega_{i_j}^{(u)} \ldots \omega_{i_{n_c}}^{(u)} \in \Sigma^{n_c} \quad (8)$$

where $\Sigma = \{0, 1\}$.
The value of n_c is selected to be equal to the length of the BCH codeword which will be presented in the following section.

2.5 Cryptographic key encoding and key-binding scheme

2.5.1 BCH encoding scheme

We adopt the error correcting codes to handle the natural variations of gait biometrics. We use the BCH code discovered independently by Bose and Ray-Chaudhuri and by Hocquenghem [13]. Let Σ be a finite and non-empty set. Basically, the BCH code is used to encode an information message $m = m_0 \ldots m_{k-1} \in \Sigma^k$ into a codeword $c = c_0 \ldots c_{n_c-1} \in \Sigma^{n_c}$. We focus on using the binary BCH code over the Galois field GF(2) in which code symbols are

represented by bits of {0, 1}. Therefore, $\Sigma = \{0, 1\}$. For any positive integer v ($v \geq 3$) and t ($t < 2^{v-1}$), there always exists a binary BCH code with length n_c and minimum distance $d_{\min}$ which satisfies

$$n_c = 2^v - 1 \quad \text{and} \quad d_{\min} \geq 2t + 1 \tag{9}$$

(t is the maximum number of errors which could be corrected). Let α be a primitive element in the GF(2^v), and $\Phi_i(x)$ is the minimal polynomial of α^i over GF(2). The generator polynomial $g(x)$ of t-error correcting BCH code of length n_c is the least common multiple (LCM) of the minimal polynomials of $\left\{\alpha^i\right\}_{i=1}^{2t}$.

$$g(x) = \text{LCM}\left(\Phi_1(x), \Phi_2(x), \ldots, \Phi_{2t}(x)\right) \tag{10}$$

The key length is determined by

$$k = n_c - \deg(g(x)) \tag{11}$$

where $\deg(\cdot)$ denotes the degree of the argument.
Denote $\text{BCH}_2(n_c, k, t)$ as a binary BCH code, the encoding process could be summarized as follows. Given a binary cryptographic key $m = m_0 \ldots m_{k-1} \in \Sigma^k$, we express m in terms of message polynomial $m(x)$

$$m(x) = m_{k-1}x^{k-1} + m_{k-2}x^{k-2} + \cdots + m_0 \tag{12}$$

Parameters including $n_c = 2^v - 1$ and t are pre-defined. Then, we generate the irreducible primitive polynomial over GF(2) with the degree of v, and the primitive element α of GF(2^v). The minimal polynomials for each element in GF(2^v) are determined, respectively. Then, the generator polynomial $g(x)$ is calculated according to (10).

Finally, $m(x)$ is multiplied by $g(x)$ yielding a codeword $c(x) = c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_0$, where $c_0 \cdots c_{n-1}$ are coefficients of the codeword

$$c(x) = m(x)g(x) = x^{n-k}m(x) + r(x) \tag{13}$$

where

$$r(x) = x^{n-k}m(x) \mod g(x)$$

Given a codeword c, the key information could be retrieved using BCH decoding algorithms which are described clearly in [13].

2.5.2 Key-binding scheme

A binary cryptographic key m of length k is generated randomly and encoded into the codeword c of length n_c using $\text{BCH}_2(n_c, k, t)$. Then, we bind the reliable binary gait template string w extracted in the Sect. 2.4 with c yielding a secured δ which is then kept in the storage. The method used to bind these two binary strings is $\oplus$ operation. The hash code $h(m)$ of m is calculated and stored for further use for user authentication. Helper data including $\mathbf{i}$, $\boldsymbol{\mu}$ extracted in the Sect. 2.4 are also stored to extract reliable binary gait template strings in the authentication phase. Note that in the enrollment phase, after we obtain δ, $\mathbf{i}$, $\boldsymbol{\mu}$ and $h(m)$, all other data as well as the original gait template will always be immediately discarded to preserve the security and user privacy.

3 Experimental results

3.1 Dataset description

We used the dataset previously employed in [7] for evaluating this system. The original dataset consists of gait signals of 38 users including 28 males and 10 females captured by an integrated accelerometer in Google Nexus One regardless of installation errors. In this study, we do not consider the disorientation problem. Hence, we only select gait signals captured when the phone is placed vertically inside the trouser pocket with a fixed orientation, as illustrated in Fig. 2d, wherein the Z-axis of the mobile is fixed. We accumulated the gait signals of 34 users, each having at least 16 gait templates. Each user will have an equal number of extracted gait templates so that we randomly select 16 templates for users having more than 16 templates. According to Sect. 2.3, we create gait templates, each consisting of $m = 4$ consecutive gait cycles. Each separate gait cycle length is normalized to $n_s = 32$. Therefore, these templates will have an identical length of $3 \times 4 \times 32 = 384$, where 3 is the number of dimensions including X, Y, Z. Figure 4 shows the extracted real-valued templates of three different users. Then, such templates are resampled using spline interpolation. The 16 resampled templates of each user will be divided equally for training and testing. In the training phase, eight random templates are used to calculate helper data $\boldsymbol{\mu}$, $\mathbf{i}$, and a binary template w is extracted. In the testing phase, the remaining eight templates are divided into two equal parts. Each part is employed to extract a binary template w'. The performance evaluation is based on the results achieved from these two parts.

3.2 The discriminability of intra- and inter-class gait templates

Figure 5 illustrates the normalized Euclidean distance distribution of real-valued gait templates and the Hamming distance distribution of the binary template based on reliable bits selection. The Euclidean distance of any two real-valued templates $\boldsymbol{\tau}_1$, $\boldsymbol{\tau}_2$ of length n_r is calculated as $d_E(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2) = \sqrt{\sum_{i=1}^{n_r}(\tau_{1i} - \tau_{2i})^2}$ and the Hamming dis-

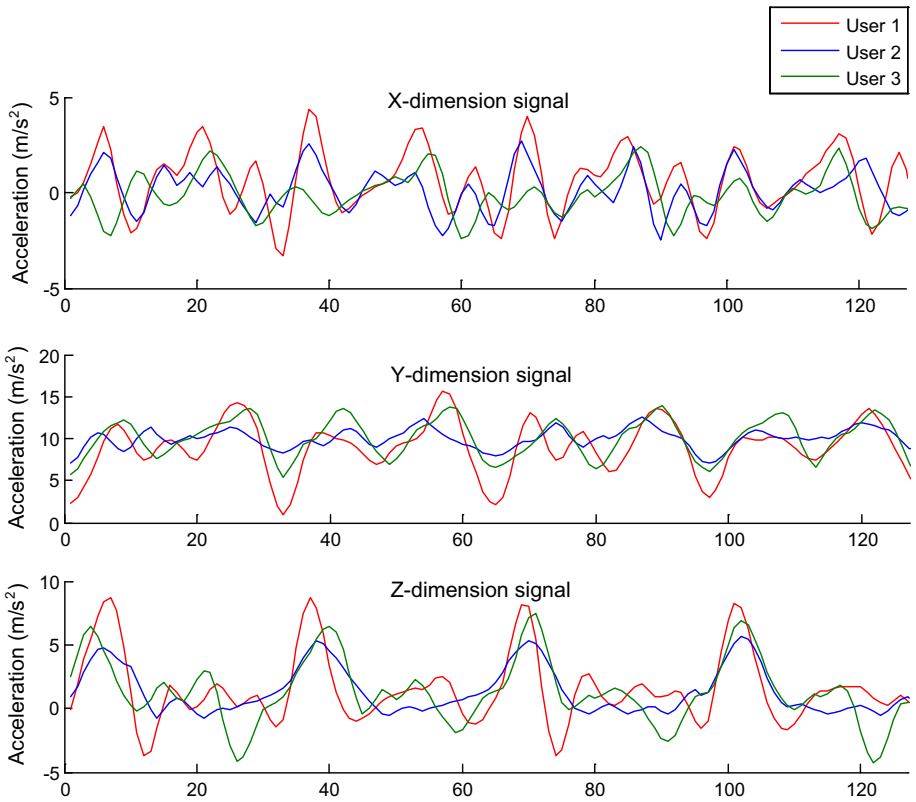

Fig. 4 An illustration of extracted real-valued gait templates of three different users

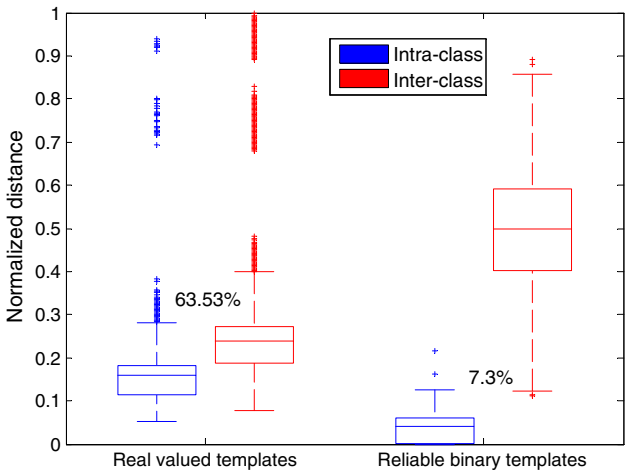

Fig. 5 The distance distribution of real-valued gait templates and binary gait templates

tance of any two binary templates w, w' of length n_c is calculated as $d_H(w, w') = \frac{1}{n_c} \sum_{i=1}^{n_c} (\omega_i \oplus \omega'_i)$. Looking at the cases of real-valued templates, the Euclidean distance of intra- and inter-class templates is low and their distribution areas are considerably overlapped. Therefore, it is also a challenge to recognize individuals based on real-valued templates by using a proper threshold. After binarization, the discriminability of reliable binary templates extracted using the quantization scheme along with reliable bits extraction is enhanced, in comparison with real-valued templates.

As shown in Fig. 5, the Hamming distances of intra- and inter-class reliable binary templates are more discriminant and distribute mostly around 0.04 and 0.5, respectively. The overlapped area reduces from 63.53 %, in cases of real-valued templates, to 7.3 %. Note that, as the size of the overlapped area is reduced, the discriminability increases further. Inter-class templates are more dissimilar so that determining an appropriate threshold to recognize individuals is more straightforward to achieve an acceptable recognition rate.

3.3 The impact of resampling on the discriminability of binary templates

For experimental analysis, we employ BCH codewords of three different lengths, $n_c = 511, 255$, and 127, respectively. As already stated, in order to extract reliable binary templates having equivalent length with the codeword, spline interpolation is necessarily adopted to resample gait templates from the original length of $n_0 = 384$ to an appropriate value of n_r. In this section, we analyze the influence of resampling to the discriminability of binary templates, whereby we determine the proper system parameter of n_r to achieve the optimal performance. Since the resampling is applied to the real-valued templates, we first analyze the impact of the resampling. Figure 6a shows that the similarity as well as overlapped area of intra- and inter-class templates does not change significantly when these templates are resampled to various lengths. Therefore, it can be concluded that

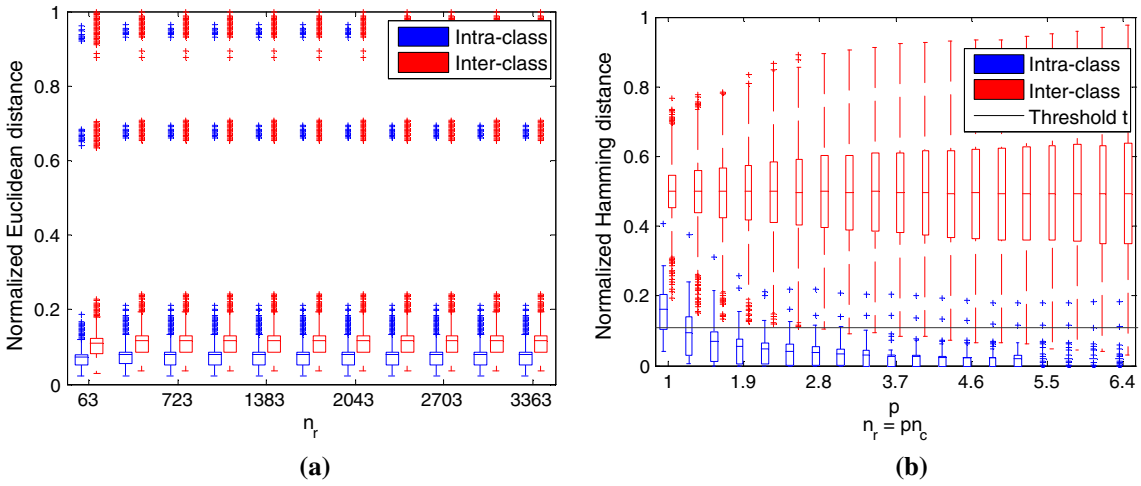

Fig. 6 **a** The Euclidean distance distribution of resampled real-valued templates $\boldsymbol{\tau}$ of different lengths n_r, **b** the Hamming distance distribution of binary templates w of length $n_c = 511$ extracted from $\boldsymbol{\tau}$ with different lengths $n_r = pn_c$

resampling does not affect the discriminability of real-valued templates. However, the discriminability of binary templates varies proportionally according to the length of the resampled real-valued templates. Figure 6b illustrates the trend of Hamming distance distribution of binary templates of length $n_c = 511$, extracted from real-valued templates with different lengths of $n_r = pn_c$, where $p > 0$. When p is increased, the intra-class and inter-class binary gait templates become more similar so that the discriminability will be decreased. This is due to only n_r reliable components out of n_c components in the original real-valued gait template which are selected to form the final binary gait template. As described in the Sect. 2.3, the term 'reliability' reflects the stability of bits extracted according to the bit extraction method. Binary templates containing many high reliable bits will result in a low Hamming distance and vice versa, binary templates containing many low reliable bits will result in a high Hamming distance. So, we can see that if n_r is too close to n_c (when p is small), which means that the pool size is small, the extracted reliable binary template could include even low reliable bits. When the pool size is getting increased (when p is increased), the extracted reliable binary template could include more highly reliable bits. As a result, the Hamming distance between distinct pairs of binary templates both in intra-class and inter-class cases will be decreased.

As BCH_2 (n_c, k, t) is adopted to handle the variability of the gait templates, the normalized Hamming distance is equivalent to t. A larger t coincides with a shorter key. For example, if t is up to 121 bits 24 % of $n_c = 511$, then $k = 10$. This length is insecure because an attacker can use brute force to guess the key. Hence, we set t to be approximately 12 % of n_c for k to be sufficiently long in all three cases of $n_c = 511, 255$, and 127. Note that the False Acceptance Rate (FAR) and False Rejection Rate (FRR) reflect the security and friendliness of the system, respectively. The security is more important so that we would like to achieve the FAR of 0 % and the FRR is as low as possible. Consequently, we analyze the Hamming distance distribution of intra- and inter-class binary templates under the threshold of 12 % to select an appropriate value of n_r. Looking to the area under the threshold in the Fig. 6b, we can see that if n_r is approximate to n_c, the population of intra-class templates will be small, resulting in a high FRR. If n_r is much larger than n_c, the population of inter-class templates will be slightly increased, making FAR > 0 %. Hence, we select the optimal parameters of p in range [2.2, 2.6] to ensure the concurrent achievement of zeroFAR, low FRR, and long enough authentication key of the system. Table 1 shows the specific values of n_r according to three different values of n_c.

Table 1 Selected values of length n_r after interpolation and concatenation of the real-valued templates corresponding to the requisite length of the binary template

n_c	n_r
127	321
255	579
511	1,221

3.4 Results

Figures 7 and 8 illustrate the Hamming distance distribution of extracted binary templates and the error rates of FAR and FRR of our system according to different key lengths, respectively. When the key length increases, the FAR decreases exponentially to 0 and the FRR increases exponentially. As already stated, the FAR of 0 % could be achieved when

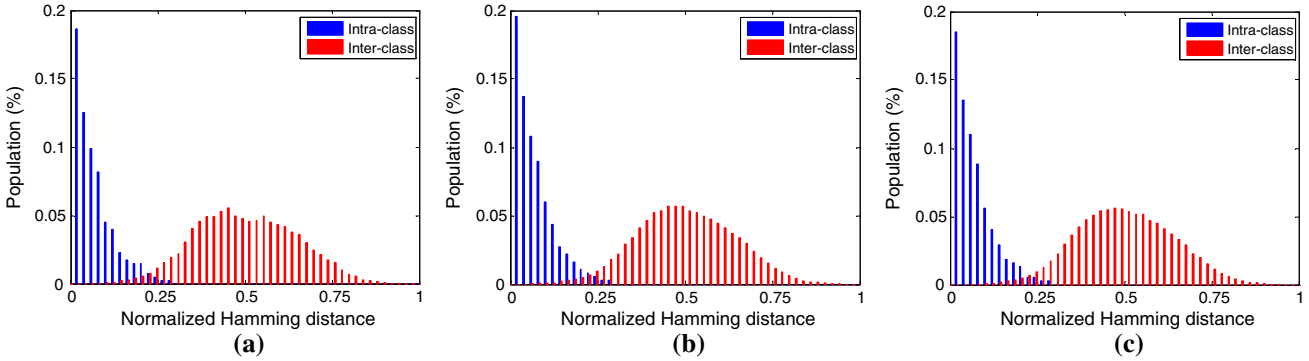

Fig. 7 The Hamming distance distribution of binary templates of length n_c. **a** $n_c = 127$, **b** $n_c = 255$, **c** $n_c = 511$

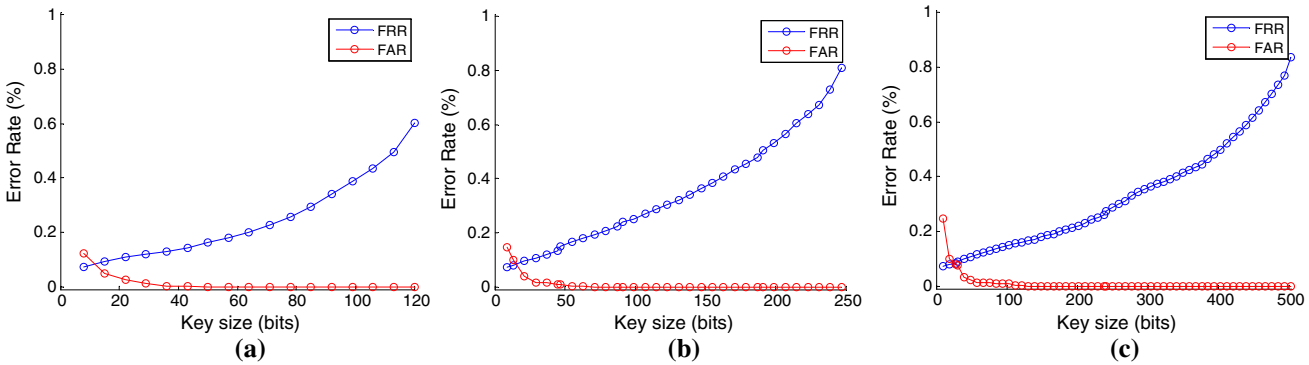

Fig. 8 The error rates of our system when binding binary templates with cryptographic keys of different lengths. **a** $n_c = 127$, **b** $n_c = 255$, **c** $n_c = 511$

Table 2 The error rates of our system according to three different codeword lengths (n_c) and key lengths (k)

n_c (bit)	k (bit)	FAR (%)	FRR (%)
511	121	0.08	16.18
511	**139**	**0**	**16.18**
511	148	0	17.65
255	63	0.27	19.12
255	**71**	**0**	**20.59**
255	79	0	22.59
127	36	0.18	14.71
127	43	0.13	14.71
127	**50**	**0**	**14.71**

The bold lines illustrate the best results

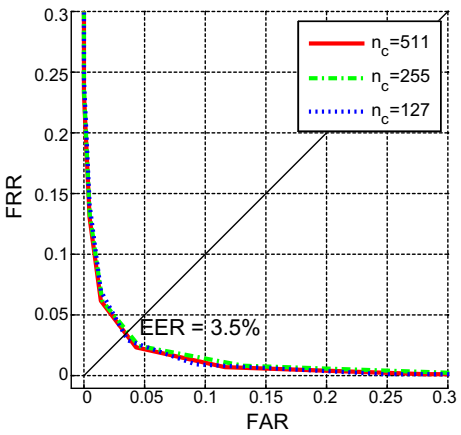

Fig. 9 The ROC curves of our gait authentication system

$t \leq 0.12n_c$. The best performances of our system corresponding to three different lengths of the binary template are considered at the zeroFAR and the lowest FRRs, as shown in the Table 2. The overall error rates of our system is also represented by a receiver operating characteristic (ROC) curve which illustrates the full relationship between the FAR and the FRR (Fig. 9). It can be seen that the equal error rate (EER) of the gait authentication system is approximately 3.5 % if we use a flexible threshold, instead of error correcting codes.

Furthermore, we analyze the memory requirement of the system. We consider the longest length $n_c = 511$ of the codeword as well as the binary template used in this study. The helper data that need to be stored include $\boldsymbol{\mu}$, $\mathbf{i}$, δ, $h(m)$. To generate binary templates of length $n_c = 511$, the essential length of real-valued templates is about 1,221. Therefore, the length of $\boldsymbol{\mu}$ is also 1,221. Each component in $\boldsymbol{\mu}$ is a real value which requires 8 bytes for representation so that $\boldsymbol{\mu}$

requires 9768 bytes. **i** contains the index of 511 highest reliable components. The maximum index value is 1,221 so that it requires 11 bits to represent an index. Therefore, whole **i** requires $511 \times 11 \div 8 \approx 703$ bytes. δ is formed by XOR-ing the codeword with the binary template, hence the length of δ is 511 bits $\approx$ 64 bytes. We use SHA-256 to calculate the hash code of the cryptographic key so that the length of $h(m)$ is 256 bits = 32 bytes. In total, our system requires approximately $703 + 9768 + 64 + 32 = 10{,}567$ bytes $\approx$ 11 KB to store all necessary data. Moreover, our system has a low computational complexity. Most operations are performed on bits (e.g., generate δ using $\oplus$ operation, calculate $h(m)$ using SHA-256, and encode and decode BCH codewords). Hence, the system has significant advantages when deployed on portable devices with limited computational resources.

3.5 Security discussion

In this section, we discuss the security of our system. First, we assume that the attacker cannot access to the mobile storage to obtain the stored data. The cryptographic key m in our system is generated randomly with the length of k bits. Thus, the attacker will attempt all possible m to be authenticated by executing a brute force attack, which requires the attacker to calculate 2^k hash codes to match with the $h(m)$ stored in the storage. Therefore, the strength of our system in this situation is k bits. Particularly, $k = 139$, 71, and 51 corresponding to n_c of 511, 255, and 127, respectively, as shown in the Table 2. Second, we assume that the attacker can access the mobile storage and obtain stored data generated in the enrollment phase including the helper data, the secured δ along with the hash code $h(m)$ of the cryptographic key m.

Once $h(m)$ is lost, it is extremely difficult to recover m from $h(m)$. The attacker's probability of success rate is 2^{-n}, where n is the length of $h(m)$ [22] (e.g., in SHA-256, $n = 256$). This is considerably more expensive than executing a brute force attack on m. Additionally, δ does not reveal any information about the binary template w or m. To retrieve w from δ, the attacker needs to guess the exact m by trying to calculate 2^k hash codes, as discussed above. To retrieve m from δ, the attacker could attempt to masquerade a template w' which is sufficiently close to w. The probability of success depends on the uncertainty of binary templates. Here, we measure the uncertainty of the binary template by calculating its entropy. The entropy ε of the whole binary template is calculated by summing the entropy of each bit in the template together.

$$\varepsilon = \sum_{i=1}^{n_c} H(q_i) \tag{14}$$

The entropy of each bit b_i is calculated by the binary entropy function $H(q_i) = -(q_i log_2(q_i) + (1-q_i) log_2(1-q_i))$ where $q_i = Pr(b_i = 1)$. According to n_c = 511, 255, and 127, we achieved the corresponding entropy ε of approximately 500.720, 250.456, and 124.508, respectively. We used binary BCH codes which allows up to 12 % incorrect bits. Hence, the attacker could attempt to find ε bits within the Hamming distance of κ bits, where $\kappa = 0.12\varepsilon$. The security s_T of our system against brute force attacks on the binary template can be estimated using the sphere-packing bound [13]

$$s_T \geq \frac{2^{\varepsilon}}{\sum_{i=0}^{\kappa} \binom{\varepsilon}{\kappa}} \approx \frac{2^{\varepsilon}}{\binom{\varepsilon}{\kappa}} \tag{15}$$

According to (15), s_T will be approximately 239, 121, and 61 bits corresponding three values of ε above. The achieved values of k and s_T are large enough as discussed in [11]; hence, the disclosure of δ is as difficult as finding collision in SHA-1 or factoring RSA-1024. In summary, the strength S of our system against brute force attacks when the portable storage is compromised is between k and s_T. Since $k < s_T$ in all three different binary template lengths, so $k \leq S \leq s_T$. Therefore, the final security strength of our system is equivalent to the length of the key. In particular, $S = k = 139$ (or 71 or 50) bits.

3.6 Relative comparison with other state-of-the-art biometric cryptosystems

Table 3 shows the relative comparison of our system with recent state-of-the-art BCSs using other physiological or behavioral biometric factors such as face, iris, fingerprint, voice, signature, and gait. Camera-based gait has been used to generate strong keys by [21]. The authors achieved the FAR and FRR of approximately 6 and 13.3 %, respectively, corresponding to the generated key length of 280 bits. They evaluate their system on a gait dataset regardless of footgear, which is relatively similar to our context. However, the approach is different from ours so that the comparison is just relative. First, a secure sketch scheme is used to generate a random key, instead of binding with the key. Second, the gait used in the system is captured from the camera, instead of from the inertial sensors. To the best of our knowledge, no BCS using inertial sensor-based gait biometrics is currently available. There are limitations when using gait biometrics captured by an inertial sensor. The mobile device is attached on a specific position in the body during walking so that the acquired gait signal only represents the movement of a part of the body (e.g., users thigh in this work). Hopefully, it can be seen that our proposed method can fulfill the current security mechanism. It outperforms other behavioral biometrics (signature, voice, and keystroke) in terms of key length and relatively competitive with other physiological biometrics in terms of zeroFAR and the security strength. The FRR

Table 3 The performance of state-of-the-art BCSs using physiological and behavioral modalities with various schemes such as fuzzy commitment scheme (FCS), fuzzy extractor (FE), secure sketch (SS), and password hardening (PH)

Study	Modality	Scheme	Key length (bits)	Security (bits)	FAR (%)	FRR (%)
Physiological modality						
[14]	Face	FCS	75	75	1	3.62
[15]	Fingerprint	FCS	50	48	0	4.85
[16]	Iris	FE	192	–	4.42	9.67
[17]	Iris	FCS	140	44	0	0.47
Behavioral modality						
[18]	Signature	FCS	29	–	6.95	6.95
[19]	Voice	FE	30–51	–	<10	<10
[20]	Voice	PH	139	18–30	8.24 ± 1.13	8.24 ± 1.13
[21]	Gait (camera based)	SS	60	60	10	9.3
			280	280	6	13.3
This study	Gait (wearable sensor based)	FCS	139	139	0	16.18
			71	71	0	20.59
			50	50	0	14.71

of 16.18 % is still rather high compared with other systems. However, this is not a critical issue. Unlike other biometric modalities such as fingerprint, iris, or signature which require the users to pay attention and performs a particular action to collect the data, the human gait could be captured continuously and implicitly without making user annoyed. Moreover, we utilized two binary template samples, each constructed from eight gait templates for testing. We found that the authentication always has at least one success out of two trials. Hence, if we apply a voting scheme to a sequence of testing samples for final authentication decision, the FRR will be reduced significantly.

4 Related works

State-of-the-art BCS which were previously proposed mostly focus on using physiological modalities such as iris [16,17], face [12,14], and fingerprint [15]. In some other studies, behavioral biometrics such as signature [18], voice [19,20] have been used. Generally, BCSs could be classified into two main subsystems including key-binding and key-generation systems [23]. In key-binding systems, as our system, a random key string is generated and is then bound with a biometric template, yielding secured data. Such data are stored for further utilization to retrieve the key in the authentication phase. Several key-binding techniques are the fuzzy commitment scheme [11] and fuzzy vault [24]. The key is revocable so that the stored data is also revocable. A new data could be recreated by binding another biometric template with a new key which is generated randomly, if the old key is compromised. Some key-binding-based systems have been implemented using various biometric modalities such as iris [17], face [12,14], fingerprint [15], hand written signature [18], and voice [20] with promising results achieved. For example, F. Hao et al. [17] proposed an iris-based BCS using the 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 are 140 and 44 bits, respectively. In contrast with key-binding systems, the key-generation scheme, helper data, is created directly only from the biometric template. Such data will be associated with a presented query which is sufficiently close to the original template to retrieve either a unique key string or the original template. Typical techniques of this scheme are the fuzzy extractor [25] and secure sketches [26]. Particular applications of a key-generated scheme have already been implemented on iris [16], camera-based gait [21], and voice [19]. Besides, multimodal BCSs fusing several biometric modalities to enhance the performance of uni-modal system, in terms of FAR, FRR, key length, and the security strength to withstand masquerade attacks, have been introduced [23,27,28]. For example, A. Nagar et al. [28] combined fingerprint, iris, and face together to construct a three-factor BCS. At the security level of 53 bits equivalent to FAR $\approx 2^{-53}$, the Genuine Acceptance Rate ($GAR = 1 - FRR$) of 99 % was achieved, compared with using an individually single modality as $\mathrm{GAR}_{\mathrm{fingerprint}} \approx 2\,\%$, $\mathrm{GAR}_{\mathrm{iris}} \approx 91\,\%$, $\mathrm{GAR}_{\mathrm{face}} \approx 12\,\%$.

5 Conclusion

In this paper, we proposed a security and privacy preserved gait authentication system on mobile phone by employing

a fuzzy commitment scheme. The achieved performances in terms of FAR, FRR, and the security level are relatively promising for further investigation to construct a well secure gait authentication on portable devices. However, since we use a simple quantization scheme, the achieved error rate of FRR is still rather high which could affect the friendliness of the system. Hence, the next work will focus on enhancing the performance, especially in term of the authentication rate of the system by analyzing the discrimination of gait templates and determining a more effective quantization scheme for gait template transformation. Besides, multimodal biometric cryptosystems that fuse some biometric modalities have been proposed recently to adapt with applications requiring high security levels. Opportunely, portable devices are becoming increasingly more equipped with many sensors which could be utilized to capture various users' biometric traits (e.g., face, fingerprint, signature, and voice). Therefore, investigating on a multimodal biometric cryptosystem using existing available sensors on mobile phone will also be our main further work.

Acknowledgments This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2012R1A1A2007014). This research was also supported by 2012-18-02TD VNU-HCMC Project.

References

1. Jain, A.K., Flynn, P.J., Ross, A.A. (eds.): Handbook of Biometrics. Springer, Berlin (2008). doi:10.1007/978-0-387-71041-9
2. Galbally, J., Cappelli, R., Lumini, A., Gonzalez-de-Rivera, G., Maltoni, D., Fierrez, J., Ortega-Garcia, J., Maio, D.: An evaluation of direct attacks using fake fingers generated from ISO templates. Pattern Recognit. Lett. **31**(8), 725–732 (2010). doi:10.1016/j.patrec.2009.09.032
3. Ngo, T.T., Makihara, Y., Nagahara, H., Mukaigawa, Y., Yagi, Y.: The largest inertial sensor-based gait database and performance evaluation of gait-based personal authentication. Pattern Recognit. **47**(1), 228–237 (2014). doi:10.1016/j.patcog.2013.06.028
4. Yun, J.: User identification using gait patterns on UbiFloorII. Sensors **11**(3), 2611–2639 (2011). doi:10.1007/11596448_141
5. Tam, L., Glassman, M., Vandenwauver, M.: The psychology of password management: a tradeoff between security and convenience. Behav. Inf. Technol. **29**(3), 233–244 (2010). doi:10.1080/01449290903121386
6. Frank, J., Mannor, S., Precup, D.: Activity and gait recognition with time-delay embeddings. In: AAAI, pp 1581–1586 (2010)
7. Hoang, T., Choi, D., Vo, V., Nguyen, A., Nguyen, T.: A lightweight gait authentication on mobile phone regardless of installation error. In: Security and Privacy Protection in Information Processing Systems, pp. 83–101. Springer, Berlin (2013). doi:10.1007/978-3-642-39218-4_7
8. Lu, H., Huang, J., Saha, T., Nachman, L.: Unobtrusive gait verification for mobile phones. In: Proceedings of the 2014 ACM International Symposium on Wearable Computers, pp. 91–98. ACM (2014). doi:10.1145/2634317.2642868
9. Derawi, M., Bours, P.: Gait and activity recognition using commercial phones. Comput. Secur. **39**, 137–144 (2013). doi:10.1016/j.cose.2013.07.004
10. Mjaaland, B. B., Bours, P., Gligoroski, D.: Walk the walk: attacking gait biometrics by imitation. In: Information Security (pp. 361–380). Springer, Berlin, Heidelberg (2011). doi:10.1007/978-3-642-18178-8_31
11. Juels, A., Wattenberg, M.: A fuzzy commitment scheme. In: Proceedings of the 6th ACM Conference on Computer and Communications Security, pp. 28–36. ACM (1999). doi:10.1145/319709.319714
12. Van Der Veen, M., Kevenaar, T., Schrijen, G. J., Akkermans, T. H., Zuo, F.: Face biometrics with renewable templates. In: Proceedings of SPIE (vol. 6072, No. 1, p. 60720J) (2006). doi:10.1117/12.643176
13. Morelos-Zaragoza, R.H.: The Art of Error Correcting Coding. Wiley, New York (2006)
14. Feng, Y.C., Yuen, P.C.: Binary discriminant analysis for generating binary face template. IEEE Trans. Inf. Forensics Secur. **7**(2), 613–624 (2012). doi:10.1109/TIFS.2011.2170422
15. Li, P., Yang, X., Qiao, H., Cao, K., Liu, E., Tian, J.: An effective biometric cryptosystem combining fingerprints with error correction codes. Expert Syst. Appl. **39**(7), 6562–6574 (2012). doi:10.1016/j.eswa.2011.12.048
16. lvarez Mario, R., Hernndez lvarez, F., Hernndez Encinas, L.: A crypto-biometric scheme based on iris-templates with fuzzy extractors. Inf. Sci. **195**, 91–102 (2012). doi:10.1016/j.ins.2012.01.042
17. Hao, F., Anderson, R., Daugman, J.: Combining crypto with biometrics effectively. IEEE Trans. Comput. **55**(9), 1081–1088 (2006). doi:10.1109/TC.2006.138
18. Maiorana, E.: Biometric cryptosystem using function based online signature recognition. Expert Syst. Appl. **37**(4), 3454–3461 (2010). doi:10.1016/j.eswa.2009.10.043
19. Carrara, B., Adams, C.: You are the key: generating cryptographic keys from voice biometrics. In: 2010 Eighth Annual International Conference on Privacy Security and Trust (PST) (pp. 213–222). IEEE (2010). doi:10.1109/PST.2010.5593251
20. Inthavisas, K., Lopresti, D.: Secure speech biometric templates for user authentication. IET Biom. **1**(1), 46–54 (2012). doi:10.1049/iet-bmt.2011.0008
21. Argyropoulos, S., Tzovaras, D., Ioannidis, D., Strintzis, M.G.: A channel coding approach for human authentication from gait sequences. IEEE Trans. Inf. Forensics Secur. **4**(3), 428–440 (2009). doi:10.1109/TIFS.2009.2025858
22. Menezes, A.J., Van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press, Washington (2010)
23. Rathgeb, C., Uhl, A.: A survey on biometric cryptosystems and cancelable biometrics. EURASIP J. Inf. Secur. **2011**(1), 1–25 (2011). doi:10.1186/1687-417X-2011-3
24. Juels, A., Sudan, M.: A fuzzy vault scheme. Des. Codes Crypt. **38**(2), 237–257 (2006). doi:10.1007/s10623-005-6343-z
25. Dodis, Y., Reyzin, L., Smith, A.: Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. In: Advances in Cryptology-Eurocrypt 2004, pp. 523–540. Springer, Berlin, Heidelberg (2004). doi:10.1007/978-3-540-24676-3_31
26. Li, Q., Sutcu, Y., Memon, N.: Secure sketch for biometric templates. In: Advances in Cryptology ASIACRYPT 2006, pp. 99–113. Springer, Berlin, Heidelberg (2006). doi:10.1007/11935230_7
27. Chin, Y.J., Ong, T.S., Teoh, A.B.J., Goh, K.O.M.: Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion. Inf. Fusion **18**, 161–174 (2014). doi:10.1016/j.inffus.2013.09.001
28. Nagar, A., Nandakumar, K., Jain, A.K.: Multibiometric cryptosystems based on feature-level fusion. IEEE Trans. Inf. Forensics Secur. **7**(1), 255–268 (2012). doi:10.1109/TIFS.2011.2166545