Accelerometer-Based Speed-Adaptive Gait Authentication Method for Wearable IoT Devices

Fangmin Sun, Chenfei Mao, Xiaomao Fan, and Ye Li, *Member, IEEE*

***Abstract*—With the rapid development of wearable Internet of Things (WIoT) devices, a significant amount of sensitive/private information collected by them poses a considerable challenge to the security of the WIoT devices. The accelerometer-based gait recognition is considered as an emerging and fast-evolving technology in security and access control fields and has achieved outstanding performance at certain fixed walking speeds. However, the gait recognition performance of the above technology deteriorates dramatically when the walking speed varies. To address this issue, both the speed-adaptive gait cycle segmentation method and individualized matching threshold generation method were proposed in this paper. Furthermore, the contrast experiments were conducted on the ZJU-GaitAcc public dataset sampled from five different body locations and the self-collected dataset sampled at various walking speeds. The experimental results indicated the average gait recognition and user authentication rates of 96.9% and 91.75%, respectively. As compared to the available state-of-the-art methods based on the fixed walking speeds and constant thresholds, the proposed method improved the gait recognition by 25.8% and user authentication by 21.5%.**

***Index Terms*—Device security, gait recognition, sensor signal processing, user authentication, wearable Internet of Things (WIoT) devices.**

Fig. 1. Typical architecture of the WIoT devices.

I. Introduction

RECENT years witness the rapid development and the aggressive incorporation of wearable Internet of Things (WIoT) devices into multiple application fields [1]. Unlike other types of Internet of Things (IoT) devices, the wearable ones embedded in or worn on the human body are mostly used in human-centered applications. The typical architecture of the WIoT network is shown in Fig. 1. The integration of various kinds of sensors into WIoT devices has dramatically enhanced their functionality [2]. Taking smart watches (e.g., Apple watch, Android wear, etc.) as an example, these can be used not only for social networking, entertainment, localization, and payment but also for health and daily activity monitoring. The robust functionality and massive of private information stored in the WIoT devices necessitate the user authentication and access control.

Passwords have been the most popular method for user authentication of the WIoT devices for a long time. The preset passwords (a string consisting of numbers and/or characters) need to be input into these devices to prove the user's identity or gain an approval to the private resource access. However, some wearable devices have no input interface, which excludes the use of passwords. Besides, passwords should not be too simple to meet with the security demand or too complicated to keep them in one's memory. The above limitations combined with the growing demand for the quality of experience of WIoT devices make the password-based identification techniques obsolete and require more lucrative alternatives, including biometrics.

Biometrics refers to any automatically measurable, robust, and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual [3]. Unlike passwords, biometric identifiers are intrinsic human features, which make them more

Manuscript received June 5, 2018; revised July 16, 2018; accepted July 23, 2018. Date of publication July 27, 2018; date of current version February 25, 2019. This work was supported in part by the National Natural Science Foundation of China under Grant 61702497, in part by the Shenzhen Science and Technology Projects under Grant JCYJ20170412110753954 and Grant JCYJ20170413161515911, in part by the Special Fund Project for Overseas High-Level Talents Innovation and Entrepreneurship under Grant KQJSCX20170731165939298, in part by the Special Support Plan for Technological Innovation Leading Talents of Guangdong Province under Grant 2014TX01X060, and in part by the Major Projects of Guangdong Province under Grant 2017B030308007 and Grant 2015B010129012. *(Corresponding author: Ye Li.)*

F. Sun, X. Fan, and Y. Li are with the Joint Engineering Research Center for Health Big Data Intelligent Analysis Technology, Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen 518055, China (e-mail: ye.li@siat.ac.cn).

C. Mao is with the Institute of Electronic and Information Engineering, Shenzhen University, Shenzhen 518067, China.

Digital Object Identifier 10.1109/JIOT.2018.2860592

reliable and efficient means of authentication than traditional password-based methods.

Biometric identifiers are often categorized as physiological and behavioral characteristics [3]. Examples of physical features include fingerprints, palm veins, face recognition, palm print, iris recognition, retina, etc. Behavioral characteristics are related to the pattern of behavior of a person, e.g., typing rhythm, gait, signature, etc.

Physical biometrics identifies people by their exclusive intrinsic features (e.g., fingerprints, face, retina), which usually needs particular modules or facilities (cameras or scanners) to acquire the respective data. However, the authentication procedures strongly rely on the user cooperation such as fingerprint scanning and might, therefore, be annoying and obtrusive in frequent use [4]. Moreover, physical biometrics can also be cracked/stolen and copied, e.g., fingerprint replicas are usually used by imposters to access the WIoT devices illegally.

Behavioral biometrics is an emerging security technology that identifies people by their behavioral patterns, which turned out to be more laborious to imitate/fraud than physical features [5]. Multiple data points are used to capture an array of human activities, such as walking style, typing speed and style, finger movements on the touchscreen or keyboard, etc. [6].

A human gait (walking style) was found to have a number of advantages over other behavioral biometric parameters, namely a more secure data collection procedure, no need for the explicit user's interaction, and high fraud resistance. With the incorporation of accelerometers into various kinds of IoT devices, the gait signal can be readily extracted from the acceleration (ACC) signal, with no additional equipment being required. This makes the accelerometer-based gait authentication procedure more cost-effective and adaptable WIoT devices, as compared to the machine vision- and floor sensor-based gait authentication methods [7]. Given the above advantages of the gait biometric, the gait-based long-term and continuous identity authentication is very lucrative.

Despite the above advantages, the available accelerometer-based gait authentication methods have their limitations. First, they are prone to the user authentication performance deterioration in case of the gate speed variation. In the majority of studies on the gait-based biometric authentication, the gait cycles were analyzed only at constant values of users' walking speed. However, in practical applications, the walking speed is shown to be affected by the particular time of the day, physical or emotional conditions of the users, etc. Such variations make the gait cycle segmentation via available techniques quite problematic. Moreover, most of the above studies adopted fixed matching thresholds, which usually violated the balance between the false negative (reject) rates and false positive (accept) ones. Therefore, an adjustment of the matching threshold is expedient for the authentication performance improvement.

Based on the above brief background, we propose a speed-adaptive gait authentication method for the WIoT devices, which improves the gait recognition and user authentication rates in cases, where the users are walking at different speeds. The proposed procedure comprises two innovative components: 1) speed-adaptive gait extraction method and 2) individualized threshold generation method.

The aims of this paper were as follows.

1) Elaboration of a walking speed-adaptive gait recognition method, which would automatically compute the step frequency and estimate the gait cycle length.
2) Development and verification of an adaptive threshold generation method for the Pearson correlation coefficient (PCC)-based gait template matching method, in order to reduce the equal error rate (EER).
3) Experimental study of the effect of IoT device location relative to the user's body parts on the user recognition rate.

The rest of this paper is organized as follows. The related recent works on the gait-based authentication are described and compared in Section II. The methodology overview proposed in this paper is given in Section III. The detailed adaptive gait cycle segmentation and user authentication methods are described in Sections IV and V, respectively. The performance of the proposed methods is validated in Section VI. Finally, this paper is concluded in Section VII.

II. Related Works

The accelerometer-based gait recognition is considered as a newly emerging technology with high prospects of yielding the breakthrough solution to robust user authentication. In this section, related works on accelerometer-based gait authentication are briefly discussed and analyzed.

With the incorporation of acceleration sensors into wearable and mobile devices, the WS-based gait recognition and authentication became very topical. Nickel used the WS-based gait authentication method as the doctorate research topic [8] and provided a comprehensive analysis of gait biometric and authentication in joint efforts with other researchers, including Nickel and Busch [9] and Derawi *et al.* [10]. Gafurov *et al.* [11], [12] used the combination of sampled three-axial acceleration values (*x*-, *y*-, and *z*-axis) for the authentication, and achieved the EERs of 5% and 9% via the histogram similarity and cycle length methods, respectively [13].

As mobile/cell phones have gained a "must-have" status worldwide, the gait biometric authentication using the acceleration signals sampled by mobile phones has been intensively studied. Ren *et al.* proposed a user verification system leveraging unique gait patterns derived from acceleration readings to detect possible user spoofing in mobile healthcare systems [14]: readily available accelerometers embedded in smartphones were applied for the user verification, and the experimental results confirmed the feasibility and accuracy of this method. De Marsico and Mecca [15] proposed a smartphone built-in sensor-based gait recognition method, which made it possible not only to verify the identity of the device owner but also provided an efficient identification among a set of enrolled subjects. The applicability of mobile phones with low-grade accelerometers for the user authentication was studied by Derawi [16], [17].

The security performance of the WS-based gait recognition when facing mimicking (spoof) attacks was addressed by Gafurov *et al.* [12]. The security strength of a smartphone-based gait recognition system against zero-effort and live minimal-effort impersonation attacks under realistic scenarios were evaluated in works of Muaaz *et al.* [18]–[21]. The above findings proved that the gait, as an authentication biometric, is not vulnerable to impersonation attacks.

Given the popularity of gait authentication studies, several public inertial sensor datasets for gait-based authentication have been constructed, such as the ZJU-GaitAcc acceleration dataset proposed by Zhang *et al.* [22], the OU-ISIR inertial sensor dataset introduced by Ngo *et al.* [23]–[25], while numerous studies have been performed based on the public datasets [26], [27].

Noteworthy is that the gait segmentation can be based on the fixed length and gait cycle. In the former case, the data are split into segments of a fixed time length without considering the periodicity of the gait signal, while the latter case implies the segmentation is performed according to the human gait cycle. Multiple publications on the cycle-based gait segmentation adopted the local minima to identify the gait start and end points. However, due to peculiarities of walking patterns of different people, the end point does not always coincide with the next local minimum after the start point: sometimes it may be the second or even third local minimum after the start point. To solve this problem, Ren *et al.* [14] proposed a gait segmentation method revealing the endpoint within a fixed range after the start point. This method exhibited a good performance at stable walking speeds but, in case of walking speed variation, the gait cycle recognition failed.

The above studies were based on the assumption of constant walking speed, while in the practical application scenarios, the user walking speed is subject to permanent variations. The problem is that the error in the cycle identification for one period will affect the detection of the following periods as well, so the detection error is accumulated throughout the total identification cycle. For these reasons, it is expedient to take advantage of the fact that the same user's gait patterns are unique and the consecutive step cycles should present a high correlation of the collected walking data. Thus, a person's gait pattern can be used as a template by identifying the first distinguishable step cycle. Then, the correlation relationship inherent to the same user's walking trace can be utilized to search for the maximum correlation between the first distinguishable cycle and the rest of trace to derive the step cycle sequence.

To cope with the above challenges, a speed-adaptive gait cycle segmentation method and an individualized threshold generation method are proposed in this paper. First, the fast Fourier transform (FFT)-based gait cycle estimation method was adopted to improve the gait segmentation accuracy, and then the autocorrelation-based individualized threshold was applied to determine the legitimacy of the claimed identity. The gait and user recognition rate under various walking speeds were improved, as compared to the available method with fixed speed and threshold, which is referred to as fixed method. The procedures and algorithms of the proposed method are presented and discussed in the following sections.

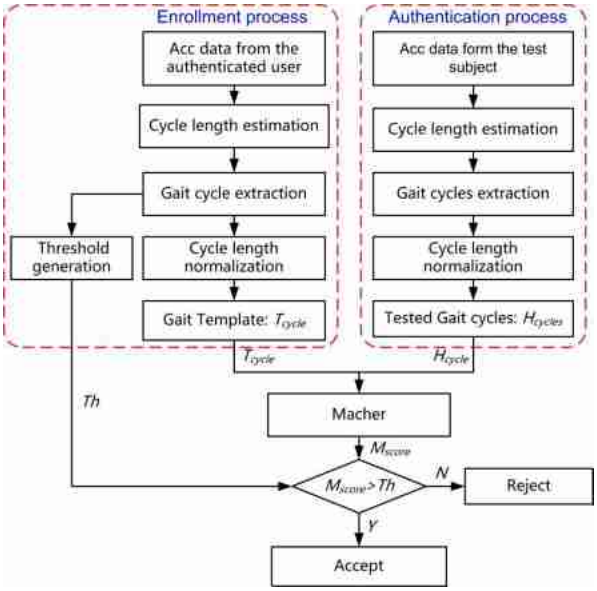

Fig. 2. Signal processing via the accelerometer-based gait recognition (enrollment) and user authentication methods.

III. Methodology Overview

The general framework of the proposed gait-based user authentication method is shown in Fig. 2. The authentication process can be reduced to the following two steps: 1) registration and 2) authentication. For the user registration step, 1-min walking acceleration data of the authenticated user were collected and logged to the computing module, subjected to the FFT, and the obtained FFT results were then used to estimate the step cycle length. Based on the step cycle length, the gait cycle was detected and then normalized to construct the gait template. For the authentication step, the walking acceleration data of the probe user are first segmented into pieces of eight seconds' length with an overlap of four seconds. Then each data segment is subjected to FFT to get the estimated step cycle length, and then all gait cycles are detected and normalized using the method, which will be described in Section IV. Finally, the PCC-based template matching method is used to determine whether to accept or reject the probe user eventually.

In this paper, two different datasets were used for the model validation. The first one is ZJU-GaitAcc public dataset [25], [26] provided by Zhejiang University, which consists of acceleration signals sampled from five different locations on the human body. It is used to estimate the impact of the sensor nodes' placement on the authentication performance. The second dataset contains the data collected via the self-designed H-shirt [28] from users walking at different speeds and is used to study the effect of walking speed variation on the authentication performance. In compliance with state-of-the-art approaches, only the vertical acceleration signal is used for the user authentication.

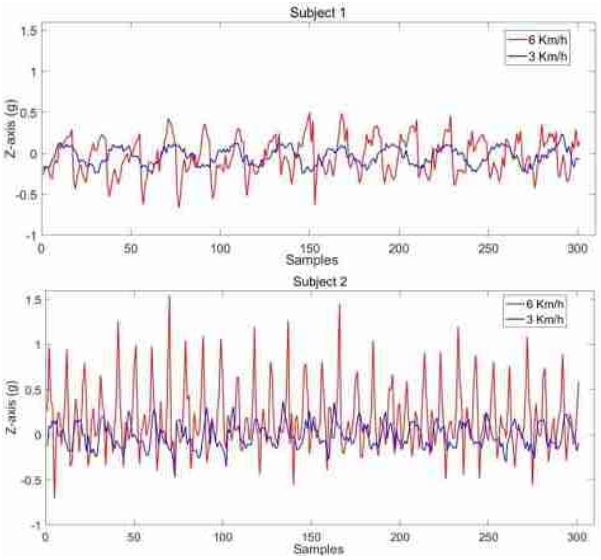

Fig. 3. ACC signals corresponding to different walking speeds and users.

In the following sections, the proposed speed-adaptive gait segmentation and individualized authentication methods are discussed in detail.

IV. Adaptive Gait Cycle Extraction

The gait segmentation is the key feature of the gait-based authentication, which can be implemented in various ways. Gait signals obtained from an individual are composed of periodic segments called gait cycles. Each gait cycle starts when one foot touches the ground and ends when the same foot touches the ground again [4]. These cycles physically correspond to two consecutive steps of the individual. To split the signal into gait cycles, a determination of the gait cycle period is required. In this section, the proposed speed-adaptive gait cycle detection method, which allows one to detect the gait accurately, is described, as the critical procedure for the gait-based user authentication.

A. Acceleration Signal Versus Walking Speed

To detect the gait cycle, the conventional method usually extracts the gait cycles by finding the first two consecutive local minima points as the start (*sp*) and end (*ep*) points in the accelerometer readings. These are treated as the start and end points of the first extracted step cycle, respectively. However, the two consecutive local minima points are not corresponding to the actual step cycle theoretically. This is attributed to the fact that when the walking speed is changed, the end point of the gait cycle would not be revealed in the predetermined range of $[\tau_1 + M - d, \tau_1 + M + d]$, where τ_1 is the position of the start point of the gait cycle, and M and d are constant values [14].

The acceleration signals acquired at different walking speeds from various users are shown in Fig. 3. Since M is a constant value, the gait cycles would not be accurately detected in the M-centered window when the step frequency changes.

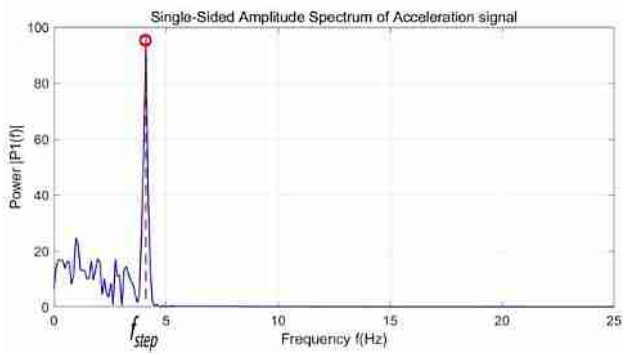

Fig. 4. FFT results on the acceleration signal and the estimated step frequency.

The correct segmentation of gait cycle is critical for the user authentication. To solve the above problem, an adaptive gait cycle extracting method is proposed in the following section, which can accurately extract the gait cycle for arbitrary walking speeds.

B. Adaptive Gait Cycle Extracting Method

The sampled acceleration signal was first processed by the FFT, and the main peak points of the FFT results were used to determine the step frequency. The step cycle length was then calculated, according to the step frequency f_{step} (Fig. 4). The estimated gait cycle length L_e can be estimated as

$$L_e = \frac{f_s}{f_{\text{step}}} \tag{1}$$

where f_s is the sampling rate of the acceleration signal.

Then the gait cycle can be recognized via the estimated gait cycle length. After the first local minimum point is selected as the gait start point (*sp*), the end point (*ep*) of the gait cycle is derived in the following range:

$$sp + L_e - d < ep < sp + L_e + d \tag{2}$$

where d is the gait cycle length deviation, which determines the search scope of the gait cycle endpoint. The value of d depends on the gait cycle length L_e and can be derived as follows:

$$d = \beta \quad L_e = 0.3 \times L_e \tag{3}$$

where β is a regulating factor, which is set at 0.3 in this paper, insofar as the experimental experience shows that one's step length variation does not exceed 1/3 of the step length.

The recognized gait cycle is used to construct the gait cycle template, as is shown in Fig. 5. The proposed speed-adaptive method can accurately extract the gait cycles for arbitrary walking speeds.

As the PCC can be applied only to vectors of the same length, whereas the gait template and probe gait cycles may have different lengths, the detected gait cycles need to be normalized to an equal length before the template-matching process. As the three-spline interpolation algorithm has a low computational complexity and can yield smooth curves, it was used in this paper to normalize/unify the gait cycle length. The

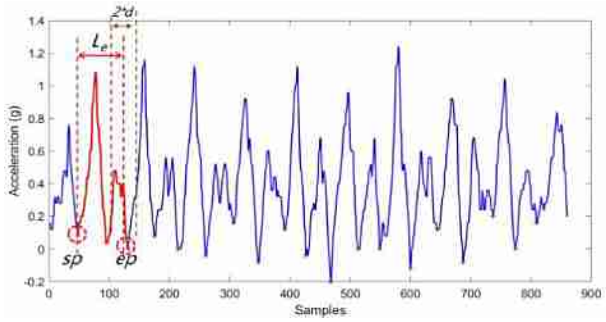

Fig. 5. Gait cycle recognition process.

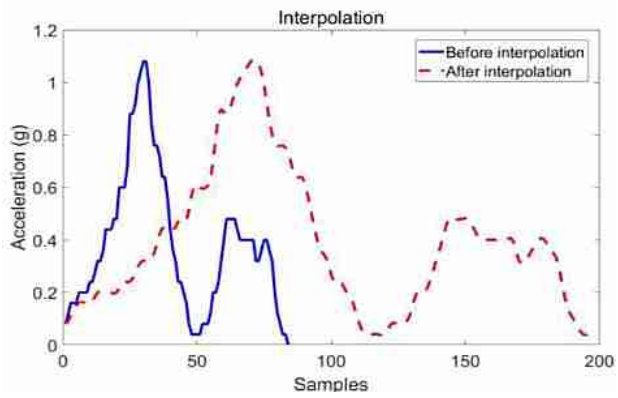

Fig. 6. Interpolation of the gait template.

interpolation results of the recognized gait cycle are shown in Fig. 6, where the gait cycle length is normalized by 200 samples. The speed-adaptive gait extracting procedure is shown in Algorithm 1.

Algorithm 1 Speed-Adaptive Gait Extraction Process

Input:
Acceleration date: $Acc = \{x_i, i = 1, 2, \ldots L\}$
Sample frequency: f_s
Procedure:
1. $[min, min\_index] = findmin(Acc)$*; //find the local minimum points of the Acc*
2. $sp = Acc(min\_indenx(1))$*; // the start point is the first local minimum point*
3. $freq = fft(Acc)$*;*
4. $f_{step} = max(freq)$*; //estimate the step frequency*
5. $L_e = f_s/f_{step}$*; //the estimated step length*
6. $d = \beta \times L_e = 0.3 \times L_e$*;*
7. $searchRange = [sp + L_e\text{-}d, sp + L_e + d]$*; //to define the searching range for the end point ep*
8. $ep =$ *the local minimum point lacate in the searchRange;*
9. $gaitCycle = \{x_k, k = sp, sp+1, \ldots, ep\}$*; // the extracted gait cycle*
10. $T_{cycle} = spline(gaitCycle, 200)$*; //length normalization*
11. $D_{rest} = \{x_j, j = ep + 1; ep+2, \ldots, L\}$*;*
Output:
The extracted templated gait cycle: T_{cycle}
The residual data in Acc : D_{rest}

V. User Authentication Algorithm

In this section, the proposed user authentication method with the individualized threshold is discussed, wherein PCC is adopted for the template comparison. Then, the authentication decision was made, according to the PCC between the gait cycle template and the tested gait cycles. The detailed authentication method is described as follows.

A. Pearson Correlation Coefficient

To decide whether the user's identity is true or false, the distance or metric function-based methods are usually applied. There are many template-matching algorithms, including the cross-correlation [29], Manhattan (absolute) distance [30], Euclidean distance [31], dynamic time warping [32], PCC [33], etc. However, among these methods, the PCC is considered to be the optimal one for measuring the correlation between variables of interest, since it is based on the method of covariance, which provides the information not only on the correlation/fit but also on the direction of the relationship [34].

PCC is also referred to as Pearson product moment correlation, which shows the linear relationship between two sets of data. Its value is ranged between -1 and $+1$, where -1 implies the total negative linear correlation, 0 corresponds to no linear correlation, and $+1$ is the total positive linear correlation. The following equation is used to derive PCC:

$$\rho_{x,y} = \frac{\mathrm{cov}(x, y)}{\sigma_x \sigma_y} = \frac{E\big((x - \mu_x)\big(y - \mu_y\big)\big)}{\sigma_x \sigma_y} \tag{4}$$

where cov is the covariance between x and y, σ_x and σ_y are the standard deviations of x and y, respectively, μ_x and μ_y are the mean values of x and y, respectively, while E is the expectation.

The correlation between data sets is a measure of their relation closeness. The PCC between the gait cycle template and the user's gait cycles is instrumental in determining the user validity.

B. Threshold Generation

The threshold used to accept or reject the user authentication is a key factor in the recognition performance. If a too high threshold is set, the false accept rate (FAR) will be lower, while the false reject rate (FRR) will be higher, and vice versa. Besides, the gait consistency of people varies.

Many researchers use the threshold ($\mathrm{Th_{optimal}}$) corresponding to the balance (FAR=FFR). However, since $\mathrm{Th_{optimal}}$ varies for different users, the fixed threshold-based method may have a poor universality. To tackle this problem, the individualized threshold generation method is introduced in this section.

To construct the gait template, a certain period of acceleration data (e.g., equal to 1 min) should be collected and saved. Moreover, these data are applied to the generation of individualized thresholds.

The collected data can be presented as $T = \{x_i, i = 1, 2, \ldots, L\}$, while the gait template established in the previous section has the form of $T_{\mathrm{cycle}} = \{x_i, i = sp, sp + 1, \ldots, ep\}$. The length S of the gait template T_{cycle} is equal to $ep - sp + 1$, as is shown in Fig. 5, while the residual data, which remain after the template in T is extracted, can be described as $D_{\mathrm{rest}} = \{x_j, j = ep + 1, ep + 2, \ldots, L\}$. Then, PCC of the

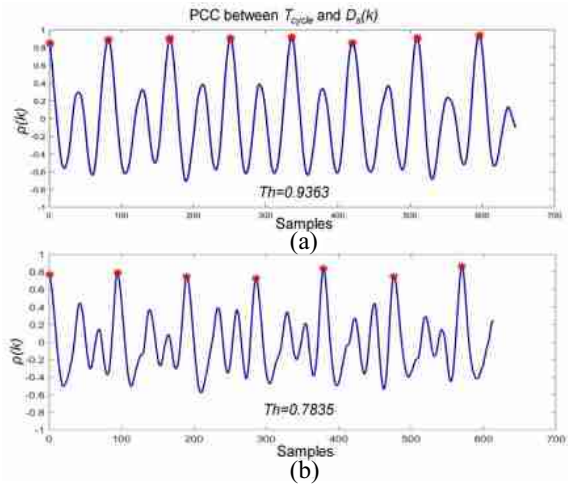

Fig. 7. Individualized Th values for different users. (a) Th = 0.9363 and (b) Th = 0.7835.

gait cycle template T_{cycle} with the rest of the gait cycle in D_{rest} can be calculated, while the average value of PCC can be used as the decision-making threshold.

To achieve this goal, the sliding window method was used to calculate PCC between T_{cycle} and D_{rest}. The value of PCC between the template T_{cycle} and the consecutive $R = L-S-ep$ samples in the recorded accelerometer readings are calculated. First, a window with the size equal to the template length S is used to segment D_{rest} into data segments D_s as follows:

$$D_s(k) = [D_{\text{rest}}(k), \ldots, D_{\text{rest}}(k+s)],\ \ k = 1, 2, \ldots, R. \quad (5)$$

Next, PCC between T_{cycle} and D_s is calculated by the following formula:

$$\rho(k) = \text{PCC}\big(T_{\text{cycle}},\ D_s(k)\big), \quad k = 1, 2, \ldots, R. \quad (6)$$

According to [10], the local maximum point of $\rho(k)$ is PCC between the gait template and the remaining gait cycle. To find the true PCC of the gait cycle, only the local maximum points, which exceed 0.5, are selected. The individual correlation threshold Th can be derived

$$\text{Th} = \frac{1}{M}\sum \text{local max}(\rho(k)),\ \ k = 1, 2, \ldots, R \quad (7)$$

where M is the number of detected local maximum points. The value of Th is then saved to decide whether the user identity is true or false. If PCC of the user gait with the gait template is less than Th, the user identity will be considered false. The computing procedure of the individualized threshold is shown in Algorithm 2. Fig. 7 illustrates an example of the generated individualized correlation thresholds of two subjects whose gait consistency is different.

The advantage of using the individualized threshold for the user authentication is that it takes into consideration the gait pattern deviation of different people. If the gait of an individual has a poor consistency, then Th will be smaller, while in the opposite case, it will be larger. So the individualized discrimination threshold can effectively reduce FAR and FRR values.

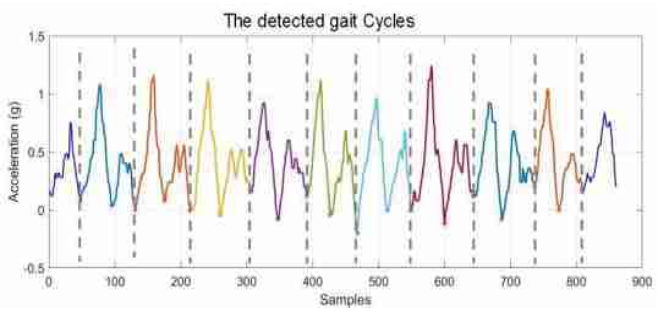

Fig. 8. Segmented gait cycle of a tested user.

Algorithm 2 Individualized Threshold Generation Process

Input:
The extracted template gait cycle: T_{cycle},
The residual data in Acc: D_{rest}
Procedure:
1. $S = length(T_{cycle})$;
2. $R = L - S - ep$;
3. ***For*** $k = 1{:}R$
4. $D_s(k) = [D_{rest}(k), D_{rest}(k+1), \ldots, D_{rest}(k+S)]$;
5. $pcc(k) = PCC(T_{cycle}, D_s(k))$;
6. ***End for***
7. $peak = findpeak(pcc)$; //find the local maximum point of pcc
8. $M = length(peak)$;
9. $Th = \frac{1}{M}\sum_{i=1}^{M} peak(i)$;

Output:
The individualized Threshold: Th

C. Gait-Based Identity Authentication

To authenticate the user's identity, the collected acceleration data have to be first segmented into cycles, as shown in Fig. 8. The gait cycle-extracting method proposed in this paper is also used to split the test data collected from different users.

When the first gait cycle is detected, the end point of the first gait cycle is used as the start point of the next gait cycle, and the same gait cycle detection method is applied until all complete gait cycles are identified. To unify the gait cycle length, all detected gait cycles are normalized by the cubic spline interpolation, and the gait cycle length is extended to 200 samples.

Assume that N gait cycles were detected and stored in the matrix H_{cycle}, and each gait cycle is stored as a row of the following matrix:

$$H_{\text{cycles}} = \begin{bmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,199} & x_{1,200} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,199} & x_{2,200} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ x_{N,1} & x_{N,2} & \cdots & x_{N,199} & x_{N,200} \end{bmatrix}. \quad (8)$$

PCC values of the gait template T_{cycle}, with each gait cycle in H_{cycles}, are calculated via (6). The score used to evaluate the matching level is given by (7), where M is the set of n values, which corresponds to $\mathcal{M}(n) > \text{Th}, n = 1, 2, \ldots, N$

$$\mathcal{M}(n) = \text{PCC}\big(T_{\text{cycle}}, H_{\text{cycles}}(n, :)\big),\ \ n = 1, 2, \ldots, N \quad (9)$$

$$M_{\text{score}} = \frac{1}{N}\sum_{n=1}^{N} \mathcal{M}(n). \quad (10)$$

(a) (b)

Fig. 9. Placement of the acceleration sensor nodes. (a) Placement of sensors in ZTU-GaitAcc dataset. (b) Placement of the designed sensor note in the H-shirt.

The decision on accepting or rejecting the test object as the legal user will be made based on the assessed value of M_{score}.

The proposed authentication procedure uses the number of gait cycles N to reduce the gait recognition error caused by the gait deviation. Thus, an increase in the applied gait number N results in the user authentication rate improvement.

VI. Performance Evaluation

In this section, the performance of the proposed authentication methods is tested on both the collected acceleration data and the public dataset. The impacts exerted on the recognition performance by placing sensors in different locations of the human body and varying walking speeds are identified and discussed in detail.

A. Experimental Methodology

1) Data Sources: The ZJU-GaitAcc public dataset was used to study the impact of the sensor placement on the user recognition rate. The ZJU-GaitAcc dataset, which is described in detail elsewhere [25], is composed of accelerometer signals from five sensor nodes positioned at different body locations, namely the right wrist, left upper arm, right side of the pelvis, left thigh, and right ankle. The sensors' placement and the corresponding numbers of the ZJU-GaitAcc dataset are shown in Fig. 9(a). The records were taken on the flat floor of 20 m length and contained the gait acceleration series of 175 volunteers. Of these, 153 subjects participated in two sessions (Sessions 1 & 2), while the remaining 22 persons were covered by a single session (Session 0). The age of participants ranged from 16 to 40 years, their body height varied from 1.5 m to 1.9 m, about 2/3 and 1/3 of them were of male or female gender, respectively. For each subject, six records per session were obtained, where each record contained five gait acceleration series, which were simultaneously measured at five body locations. The data for Sessions 1 and 2 with acceleration signals of 153 subjects were used in this paper. However, according to the agreements with the volunteers, the ZJU-GaitAcc provided no specific personal information other than the gait acceleration, so that only general statistics of the datasets are listed in Table I.

TABLE I
Statistical Breakdown of Subjects Included in the Dataset

Gender ratio	Age (years)	Height (m)	Weight (kg)
Male : Female=2:1	16~40	1.5~1.9	unknown

TABLE II
Physical Parameters of Test Subjects

Subject No.	Gender	Age (years)	Height (m)	Weight (kg)
1	F	30	1.6	52
2	M	31	1.71	63
3	F	24	1.6	48
4	M	27	1.76	68
5	M	24	1.69	65
6	M	26	1.8	76
7	F	23	1.63	51
8	F	24	1.62	50
9	M	29	1.72	72
10	F	26	1.6	49

Besides, to estimate the walking speed effect on the gait detection rate and the user authentication rate, the H-shirt depicted in Fig. 9(b) and integrated with three-axial acceleration sensor was used to sample the acceleration signal when the user was walking on the treadmill at different speeds. Ten users were asked to walk at speeds varying from 2 to 6 km/h with a speed increment of 0.5 km/h. For the consistency of these test data with those of the ZJU-GaitAcc database, two tests with three months intervals were carried out, with each test involving six records made at different walking speeds. In each record, the subjects were asked to walk 500 gait cycles. In this experiment, ten young adults were enrolled to participate in the data collection. The physical parameters of test subjects are shown in Table II.

The sampling rate of the ZJU-GaitAcc public dataset was set as 100 sps. To be consistent with the public dataset, the data collected using the self-designed H-shirt had the identical sampling rate of 100 sps.

2) Evaluation Procedure: First, the performance of the adaptive gait cycle extracting method was tested using the collected and ZJU-GaitAcc data. Then the impact of walking speed and sensor nodes' placement on the gait detection rate was analyzed.

Next, the user authentication rate was evaluated using the metrics of false reject and accept rates (FRR and FAR, respectively). In earlier studies, the sensor was placed in the fixed position of the body, while both the data used as a template and those used as a probe were collected from the same body locations [35]–[37]. Therefore, the scenarios envisaging that template and probe data could be collected from different body locations were not considered. In this paper, the acceleration data from different body locations were used as templates and probes for the cross-validation. Moreover, the acceleration

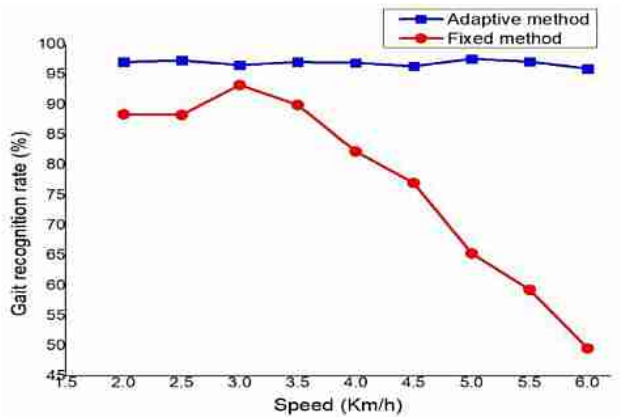

Fig. 10. Gait recognition rate versus walking speed curves obtained via the proposed adaptive and conventional fixed methods.

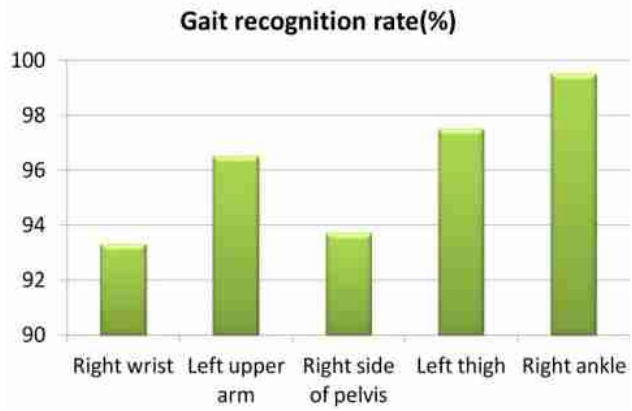

Fig. 11. Gait recognition rate for different placements of the sensor nodes.

data corresponding to different walking speeds were also tested using the acceleration data collected via the H-shirt.

The traditional authentication performance of the method was evaluated via the receiver operating characteristic (ROC) curve. The ROC curve shows a tradeoff between FRR and FAR when a receiver changes the threshold in personal authentication scenarios [38]. However, in this paper, the individualized threshold was automatically generated, whereas FAR and FRR values were calculated and compared with the available results.

To check whether the gait recognition and user authentication rates can be improved by the proposed speed-adaptive gait extraction and individualized threshold generation methods, we also implemented the so-called "fixed method" as a reference. The latter refers to the gait authentication method based on the fixed walking speed gait template extraction and the constant template matching thresholds.

B. Gait Detection Performance Evaluation

The gait detection rate is defined as the ratio of the accurately detected number of gait cycles and their actual total number. In this section, the gait detection rate provided by the proposed method was evaluated for different scenarios. First, the recognition rate was tested for the case where the users walked at different speeds. Then, the impact of the sensor nodes' placement in different parts of the body on the recognition rate was assessed.

1) Gait Detection Rate for Different Walking Speeds: Insofar as the ZJU-GaitAcc dataset contained no information on the user walking speed, the ACC data collected via the H-shirt were used in this paper to correlate the gait cycle detection rate with the walking speed. For the actual gait cycle of each record, N_{cycles} is equal to 500, so the gait cycle detection rate G_r can be derived as follows:

$$G_r = 1 - \frac{1}{R}\sum_{i=1}^{R}\frac{\left|\mathrm{N}_{\text{cycles}} - N_{\text{detected}}\right|}{N_{\text{cycles}}} \tag{11}$$

where R is the number of records, N_{cycles} is the number of gait cycles provided by the ZJU-GaitAcc dataset, and N_{detected} is the number of detected gait cycles. In this paper, $R = 12$.

The test results depicted in Fig. 10 strongly indicate that the proposed method has superior performance, as compared to the fixed method, when the users walked at different speeds. The fixed method exhibited a good performance when users' walking speeds were less than 3.5 km/s, but it rapidly deteriorated at walking speeds exceeding 3.5 km/s. In contrast to this, the adaptive method exhibited superior performance and was only slightly affected by variations in walking speed values. The average gait recognition rate of the speed-adaptive method was 96.9%, in the case where the enrolled subjects were walking at different speeds, which implied an improvement of 25.8%, as compared to that obtained by the fixed method (i.e., based on the fixed walking speeds and constant thresholds).

2) Gait Recognition Rate for Sensor Nodes' Placement at Different Body Locations: The impact of the sensor nodes placement was studied, and the recognition performance was evaluated using the ZJU-GaitAcc dataset. The number of gait cycles and the limits of the gait cycles were preset in the dataset. So the number of gait cycles detected via the proposed speed-adaptive method was compared with the gait cycle information provided in the dataset, while the gait detection rate was derived via (11).

The analysis of gait recognition rates for the five locations under study (Fig. 11) implies that the highest gait recognition rates are attained when the sensor nodes are placed on the user ankle, thigh, and the upper arm (in the decreasing order). This finding can be ascribed to the fact that the acceleration signals at these locations are less susceptible to the interference from other small-scale movements of other body parts, as compared to pelvis or wrist.

C. User Authentication Performance Evaluation

In this section, the user authentication performance of the proposed method is evaluated and discussed in detail. FAR and FRR values were counted when the gait template ACC signal and the probe ACC signal were sampled from different body sensor placements. The template ACC signal is the acceleration signal used for the template construction, while the term "probe ACC signal" specifies that the acceleration signal is

TABLE III
FARs FOR DIFFERENT TEMPLATE AND TEST SENSOR DATA OF THE SAME PERSON

No.	1	2	3	4	5
1	1.02%	5.19%	6.21%	9.90%	10.01%
2	7.09%	3.92%	4.98%	8.09%	10.01%
3	8.21%	5.02%	3.87%	11.31%	9.98%
4	11.90%	8.09%	11.31%	2.62%	5.10%
5	12.01%	10.01%	9.81%	5.97%	1.92%

TABLE IV
FRRs FOR DIFFERENT TEMPLATES AND TEST SENSOR DATA

NO.	1	2	3	4	5
1	2.13%	7.16%	7.34%	13.39%	14.81%
2	6.86%	3.23%	8.56%	12.89%	13.96%
3	9.07%	9.69%	4.37%	12.97%	13.86%
4	12.98%	12.93%	13.11%	2.80%	6.91%
5	15.15%	12.79%	14.24%	5.78%	3.87%

used as a test point. Eventually, the identity recognition rates for different walking speeds were evaluated and analyzed.

1) Impact of the Sensor Nodes' Placement on the Identity Recognition Rate: First, FAR and FRR parameters were tested when the sensor nodes were placed in different body locations. The test results obtained are shown in Tables III and IV. The number in the first row/first column of the table corresponds to the number of the body locations, where the template/probe ACC data were sampled, respectively. The ZJU-GaitAcc data were used in this experiment. The experimental results on FAR and FRR are shown in Tables III and IV, respectively. When the adaptive threshold was used to determine whether the user identity should be accepted or rejected, both FAR and FRR values were reduced, yielding a smaller EER, as compared to the conventional methods.

As the correlation coefficients for the sequences sampled from two body locations are approximately consistent, the test results shown in Tables III and IV exhibit a certain symmetry, this means that the FAR/FRR ratio obtained when sensor No. 1 sensor was used as a template and sensor No. 2 as a test sensor is similar to the one obtained when these are switched. Besides, the test results listed in the diagonal of Tables III and IV are lower than those in the same row and column, insofar as the correlation between the acceleration signals collected from the same body sensor locations is much stronger than that between the acceleration signals obtained from different ones.

However, when the adaptive threshold is generated by PCC of the template, where the remaining data are located in the same sampling dataset, the similarity between the data from the same sampling is higher than that between different samplings. Therefore, the FRR is higher than the FAR. Meanwhile, an increase in the number of probe cycles would reduce the FRR values, which is discussed in more detail in the next section.

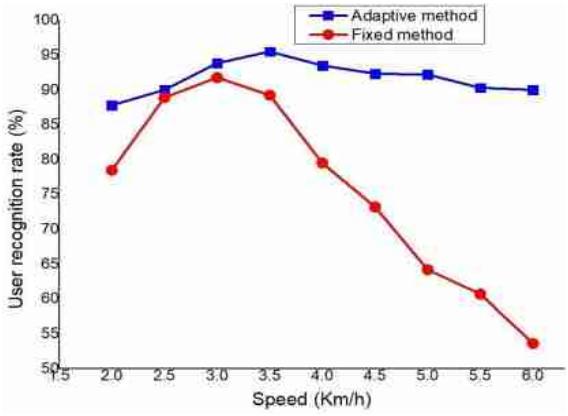

Fig. 12. User recognition rate versus walking speed curves obtained via the proposed adaptive and conventional fixed methods.

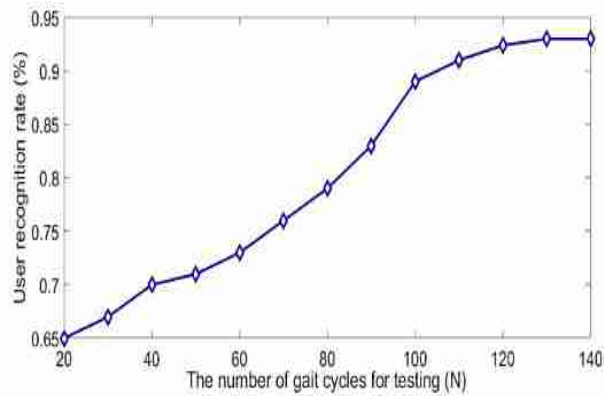

Fig. 13. User recognition rate versus the number of gait cycles used for testing.

2) Impact of the Walking Speed on the Identity Recognition Rate: In this section, the user authentication performance is assessed for the case where users walk at different speeds. The data collected using the H-shirt was used in this paper, and the test results were compared with those obtained by the fixed threshold method. The comparative analysis results are shown in Fig. 12. The results obtained strongly suggest that the adaptive threshold method outperforms the fixed threshold one when the users walk at varying speeds. The average user recognition rate of the speed-adaptive method is 91.75%, in the case where the enrolled subjects were walking at different speeds, which was by 21.5% higher than that provided by the reference fixed method based on the fixed walking speeds and constant thresholds.

3) Impact of the Number of Gait Cycles Used for Testing: We also studied the effect of the used number of probe gait cycles N in matrix H_{cycle} on the authentication performance. In this experiment, ten users wearing the H-shirt were asked to walk at a fixed speed of 4 km/h for 1 min. At least 156 cycles were included in the sampled data of each subject. Tests were performed using different numbers of gait cycles ranging from 20 to 140, with the increment/interval equal to 20.

The test results plotted in Fig. 13 imply that an increase in the number of probe gait cycles improves the user recognition rate. Moreover, the FRR can be reduced with an increase in the number of gait cycles in the probe dataset.

VII. Conclusion

The speed-adaptive gait cycle segmentation and individualized matching threshold generation techniques are proposed in this paper. They were implemented by a speed-adaptive gait recognition method for user verification using available accelerometers embedded into WIoT devices. The effect of the node placement on the gait cycle segmentation and the user authentication was analyzed. The contrast experiments on gait and user recognition performance were conducted using the public dataset ZJU-GaitAcc sampled from five different body locations and the self-collected dataset sampled under different walking speeds. The contrast experiments on gait and user recognition performance were conducted using the public dataset ZJU-GaitAcc sampled from five different body locations and the self-collected dataset sampled under different walking speeds. The experimental results showed that the average gait recognition rate and user verification rate were 96.9% and 91.75%, respectively. As compared to state-of-the-art methods based on the fixed walking speed and constant thresholds, the performance of the proposed method was improved by 25.8% for gait recognition and 21.5% for user recognition. The individualized decision-making model and the speed-adaptive ability of the proposed method would promote the practical application of the accelerometer-based gait authentication technology.

The main results obtained in this paper make it possible to draw the following conclusion.

1) A walking speed-adaptive gait recognition method, which can automatically compute the step frequency and estimate the gait cycle length, was proposed and experimentally corroborated.
2) An adaptive threshold generation method was developed for the PCC-based gait template matching method, which reduces the EER.
3) The effect of mobile device location relative to the user's body parts on the user recognition rate was studied, and the results obtained are discussed in detail.

In the further research on the gait-based user authentication, it is expedient to test new algorithms such as neural networks for the gait cycle segmentation and template matching, in order to improve the authentication performance. The fusion of different kinds of biometrics, such as ECG, for user authentication is also envisaged in the follow-up studies to enhance the security of the WIoT devices. Furthermore, the impact of users' clothing and footwear, as well as their physical conditions (e.g., tiredness, idling, illness, etc.) on the gait biometric-based authentication will also be studied in our future work. Finally, the gait authentication methods for older adults (over 50 years of age) and young children (under ten years of age) will be further studied. The intrabody gait fluctuations of these age groups are more substantial than those of users of the age range between 10 and 50 years, due to the immaturity of young children's walking skills and physical strength declination of older adults. Therefore, a gait authentication model that can be used by the above age groups is the focus of our further research efforts.

References

[1] G. Fortino, R. Gravina, A. Guerrieri, and G. Di Fatta, "Engineering large-scale body area networks applications," in *Proc. 8th Int. Conf. Body Area Netw. (ICST)*, 2013, pp. 363–369.

[2] S. Sprager and M. B. Juric, "Inertial sensor-based gait recognition: A review," *Sensors*, vol. 15, no. 9, pp. 22089–22127, 2015.

[3] A. K. Jain, A. A. Ross, and K. Nandakumar, *Introduction to Biometrics*. New York, NY, USA: Springer, 2011.

[4] T. Hoang, D. Choi, and T. Nguyen, "On the instability of sensor orientation in gait verification on mobile phone," in *Proc. 12th IEEE Int. Joint Conf. E-Bus. Telecommun.*, vol. 4, Jul. 2015, pp. 148–159.

[5] F. Miao, S.-D. Bao, and Y. Li, "Biometric key distribution solution with energy distribution information of physiological signals for body sensor network security," *IET Inf. Security*, vol. 7, no. 2, pp. 87–96, Jun. 2013.

[6] A. Turgeman, "System, device, and method of detecting identity of a user of a mobile electronic device," U.S. Patent 8 938 787, 2015.

[7] N. M. Bora, G. V. Molke, and H. R. Munot, "Understanding human gait: A survey of traits for biometrics and biomedical applications," in *Proc. IEEE Int. Conf. Energy Syst. Appl.*, 2015, pp. 723–728.

[8] C. Nickel, "Accelerometer-based biometric gait recognition for authentication on smartphones," Ph.D. dissertation, Dept. Comput. Sci., Tech. Univ. Berlin, Berlin, Germany, 2012.

[9] C. Nickel and C. Busch, "Does a cycle-based segmentation improve accelerometer-based biometric gait recognition?" in *Proc. 11th Int. Conf. IEEE Inf. Sci. Signal Process. Appl. (ISSPA)*, 2012, pp. 746–751.

[10] M. O. Derawi, C. Nickel, P. Bours, and C. Busch, "Unobtrusive user-authentication on mobile phones using biometric gait recognition," in *Proc. IEEE 6th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP)*, 2010, pp. 306–311.

[11] D. Gafurov, K. Helkala, and T. Søndrol, "Biometric gait authentication using accelerometer sensor," *J. Comput.*, vol. 1, no. 7, pp. 51–59, 2006.

[12] D. Gafurov, E. Snekkenes, and P. Bours, "Spoof attacks on gait authentication system," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 491–502, Sep. 2007.

[13] D. Gafurov, E. Snekkenes, and P. Bours, "Improved gait recognition performance using cycle matching," in *Proc. IEEE 24th Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, 2010, pp. 836–841.

[14] Y. Z. Ren, Y. Y. Chen, M. C. Chuah, and J. E. Yang, "User verification leveraging gait recognition for smartphone enabled mobile healthcare systems," *IEEE Trans. Mobile Comput.*, vol. 14, no. 9, pp. 1961–1974, Sep. 2015.

[15] M. De Marsico and A. Mecca, "Biometric walk recognizer," *Multimedia Tools Appl.*, vol. 76, no. 4, pp. 4713–4745, 2017.

[16] M. O. Derawi, "Accelerometer-based gait analysis, a survey," in *Norwegian Infor. Security Conf. (NISK)*, 2010, pp. 1–12.

[17] M. O. Derawi, "Biometric options for mobile phone authentication," *Biometric Technol. Today*, vol. 2011, no. 9, pp. 5–7, 2011.

[18] M. Muaaz and C. Nickel, "Influence of different walking speeds and surfaces on accelerometer-based biometric gait recognition," in *Proc. 35th IEEE Int. Conf. Telecommun. Signal Process. (TSP)*, 2012, pp. 508–512.

[19] M. Muaaz and R. Mayrhofer, "An analysis of different approaches to gait recognition using cell phone based accelerometers," in *Proc. ACM Int. Conf. Adv. Mobile Comput. Multimedia*, 2013, p. 293.

[20] M. Muaaz and R. Mayrhofer, "Orientation-independent cell phone based gait authentication," in *Proc. 12th Int. Conf. Adv. Mobile Comput. Multimedia*, 2014, pp. 161–164.

[21] M. Muaaz and R. Mayrhofer, "Smartphone-based gait recognition: From authentication to imitation," *IEEE Trans. Mobile Comput.*, vol. 16, no. 11, pp. 3209–3221, Nov. 2017.

[22] Y. Zhang *et al.*, "Accelerometer-based gait recognition by sparse representation of signature points with clusters," *IEEE Trans. Cybern.*, vol. 45, no. 9, pp. 1864–1875, Sep. 2015.

[23] T. T. Ngo *et al.*, "Phase registration in a gallery improving gait authentication," in *Proc. IEEE Int. Joint Conf. Biometrics*, 2011, pp. 1–7.

[24] T. T. Ngo, Y. Makihara, H. Nagahara, Y. Mukaigawa, and Y. Yagi, "Performance evaluation of gait recognition using the largest inertial sensor-based gait database," in *Proc. 5th IEEE IAPR Int. Conf. Biometrics (ICB)*, 2012, pp. 360–366.

[25] T. T. Ngo, Y. Makihara, H. Nagahara, Y. Mukaigawa, and Y. Yagi, "The largest inertial sensor-based gait database and performance evaluation of gait-based personal authentication," *Pattern Recognit.*, vol. 47, no. 1, pp. 228–237, 2014.
[26] (2015). *ZJU-GaitAcc Dataset*. [Online]. Available: http://www.ytzhang.net/datasets/zju-gaitacc/
[27] (2013). *OU-ISIR Biometric Database*. [Online]. Available: http://www.am.sanken.osaka-u.ac.jp/BiometricDB/InertialGait.html
[28] F. Sun, C. Yi, W. Li, and Y. Li, "A wearable H-shirt for exercise ECG monitoring and individual lactate threshold computing," *Comput. Ind.*, vols. 92–93, pp. 1–11, Nov. 2017.
[29] X. Y. Qian *et al.*, "Detrended partial cross-correlation analysis of two nonstationary time series influenced by common external forces," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 91, no. 6, 2015, Art. no. 062816.
[30] W.-Y. Chiu, G.-G. Yen, and T.-K. Juan, "Minimum Manhattan distance approach to multiple criteria decision making in multiobjective optimization problems," *IEEE Trans. Evol. Comput.*, vol. 20, no. 6, pp. 972–985, Dec. 2016.
[31] I. Dokmanic, R. Parhizkar, J. Ranieri, and M. Vetterli, "Euclidean distance matrices: Essential theory, algorithms, and applications," *IEEE Signal Process. Mag.*, vol. 32, no. 6, pp. 12–30, Nov. 2015.
[32] A. Mueen and E. Keogh, "Extracting optimal performance from dynamic time warping," in *Proc. ACM 22nd ACM SIGKDD Int. Conf. Knowl. Disc. Data Min.*, Aug. 2016, pp. 2129–2130.
[33] W. Wiedermann and M. Hagmann, "Asymmetric properties of the Pearson correlation coefficient: Correlation as the negative association between linear regression residuals," *Commun. Stat. Theory Methods*, vol. 45, no. 21, pp. 6263–6283, 2016.
[34] S. Huang, A. Elgammal, J. Lu, and D. Yang, "Cross-speed gait recognition using speed-invariant gait templates and globality–locality preserving projections," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 10, pp. 2071–2083, Oct. 2015.
[35] A. H. Johnston and G. M. Weiss, "Smartwatch-based biometric gait recognition," in *Proc. IEEE 7th Int. Conf. Biometrics Theory Appl. Syst. (BTAS)*, 2015, pp. 1–6.
[36] W. Tao, T. Liu, R. Zheng, and H. Feng, "Gait analysis using wearable sensors," *Sensors*, vol. 12, no. 2, pp. 2255–2283, 2012.
[37] J. Hannink *et al.*, "Sensor-based gait parameter extraction with deep convolutional neural networks," *IEEE J. Biomed. Health Inform.*, vol. 21, no. 1, pp. 85–93, Jan. 2017.
[38] Y. Liu, Z. Yang, C. Y. Suen, and L. Yang, "A study on performance improvement due to linear fusion in biometric authentication tasks," *IEEE Trans. Syst., Cybern. Man, Syst.*, vol. 46, no. 9, pp. 1252–1264, Sep. 2016.

Fangmin Sun received the B.S. degree in measurement and control technology and instruments from Xian Electronic Technology University, Xi'an, China, in 2010 and the Doctoral degree from the State Key Laboratory of Transducer Technology Institute of Electronics, Chinese Academy of Sciences, Beijing, China, in 2015.

She is currently an Assistant Professor with the Shenzhen Institute of Advanced Technology, Shenzhen, China. Her current research interests include wireless body sensor networks, low-power communication technology, biomedical signal processing, and wearable health-monitoring devices.

Chenfei Mao received the B.S. degree in electronic and communication engineering from Lanzhou City University, Lanzhou, China, in 2016. He is currently pursuing the graduation degree at Shenzhen University, Shenzhen, China.

His current research interests include biomedical signal processing and biometric authentication for wearable devices.

Xiaomao Fan received the B.S. degree in chemistry from Nanchang University, Nanchang, China, in 2003, and the M.S. degree in system engineering from the Shanghai University of Science and Technology, Shanghai, China, in 2011. He is currently pursuing the Ph.D. degree in computer application technology at the University of Chinese Academy of Sciences, Beijing, China.

His current research interests include machine learning and high-performance computing.

Ye Li (M'09) received the B.S. and M.S. degrees in electrical engineering from the University of Electronic Science and Technology of China, Chengdu, China, in 1999 and 2002, respectively, and the Ph.D. degree in electrical engineering from Arizona State University, Tempe, AZ, USA, in 2006.

He is a Professor with the Shenzhen Institute of Advanced Technology (SIAT), Chinese Academy of Sciences, Shenzhen, China. In 2007, he was with Cadence Design Systems, Inc., San Jose, CA, USA. Since 2008, he has been the Director of the Research Center for Biomedical Information Technology, SIAT. His current research interests include body sensor networks, wearable computing, and health data mining.