An Unsupervised Approach for Gait-based Authentication

Guglielmo Cola, Marco Avvenuti, and Alessio Vecchio
Dip. di Ingegneria dell'Informazione
University of Pisa, Pisa, Italy
Email: {g.cola, m.avvenuti, a.vecchio}@iet.unipi.it

Guang-Zhong Yang, and Benny Lo
Hamlyn Centre
Imperial College London, London, UK
Email: {g.z.yang, benny.lo}@imperial.ac.uk

***Abstract*—Similar to fingerprint and iris pattern, everyone's gait is unique, and gait has been proposed as a biometric feature for security applications. This paper presents a *lightweight* accelerometer-based technique for user authentication on smart wearable devices. Designed as an unsupervised classification approach, the proposed authentication technique can learn the user's gait pattern automatically when the user first starts wearing the device. Anomaly detection is then used to verify the device owner. The technique has been evaluated both in controlled and uncontrolled environments, with 20 and 6 healthy volunteers respectively. The Equal Error Rate (EER) in the controlled environments ranged from 5.7% (waist-mounted sensor) to 8.0% (trouser pocket). In the uncontrolled experiment, the device was put in the subject's trouser pocket, and the results were similar to the respective supervised experiment (EER=9.7%).**

***Index Terms*—Gait Analysis, Gait-Based Authentication, Anomaly Detection, Wearable sensors.**

I. Introduction

In recent years, mobile phones have evolved from simple communication devices to almost universal tools for daily activities, such as navigation, on-line payment, and social networking. As a consequence, smartphones provide access to a large amount of personal and confidential information. Security is generally enforced through authentication methods, like passwords and PINs, that require explicit users' actions. To reduce the burden, novel mechanisms based on biometry have been proposed for user authentication.

Similarly, user authentication and identification are major challenges for miniaturized smart wearable devices, especially those used for remote health monitoring and rehabilitation [1], [2]. Besides the concerns related to unauthorized access to personal health information, it is essential for the device to authenticate and identify the user in order to ensure reliability of the health information captured. For instance, in telemedicine applications, where patients' activities are monitored to assess their health status, users could be tempted to give their monitoring device to other people, in order to reach the activity levels prescribed by caregivers [3].

To address these needs, some motion based biometric techniques have been proposed for device owner identification and authentication. Every individual has his/her own way of performing everyday activities, and thus by comparing acceleration data to pre-acquired templates it is possible, with reasonable accuracy, to passively recognize or authenticate the user. In particular, almost all the techniques devised so far are based on the analysis of walking segments for two main reasons: i) gait is highly specific [4]; ii) walking is a common activity, and thus it provides numerous opportunities to collect user-specific information.

The aim of gait-based *identification* is to recognize the person who wears the device among a set of possible users. In more detail: the set S of users is known and the gait identification technique recognizes the current wearer s of the device, with $s \in S$. Such techniques are particularly useful, for example, when a single monitoring device is time-shared among a set of patients or athletes, as the device can be reconfigured according to the identity of the user under monitoring without any manual intervention.

Gait-based *authentication* (or verification), on the other hand, is the problem of detecting if a new, and previously unseen user, starts using the device. This problem is somehow more challenging because no information about the new users is available in advance. A system that provides timely detection of new users can be used to detect if a patient is cheating (by giving the device to another person) or if the device is stolen.

This paper focuses on the latter scenario: the wearable device is used by a single user (the *genuine user*) and the proposed method detects if a different and unexpected user (the *unauthorized user*) starts using the device. The proposed method automatically learns the user's gait pattern during the first few days of use, and then any unauthorized use of the device will be recognized by the anomaly detection techniques. The method has been evaluated in different conditions, both in controlled and uncontrolled environments.

II. Related work

The first acceleration-based method for user authentication was proposed by Ailisto et al. [5]. Acceleration data was collected at the user's waist at 256 Hz frequency. Then, after isolating individual steps, the cross-correlation value was calculated between current steps and a template signal. From the 36 subject experiments, it has been shown that the proposed technique has an error rate of 12%.

Gafurov et al. studied different metrics for gait-based authentication: absolute distance, correlation, histogram, and

high order moments [6]. They also studied the effects of carrying a backpack on the authentication process. The proposed metrics were evaluated on a data set with 300 gait sequences, collected from 50 subjects in a controlled environment using an accelerometer placed in the pocket of user's trousers. The absolute distance metric achieved the best performance (with equal error rate of 7.3%).

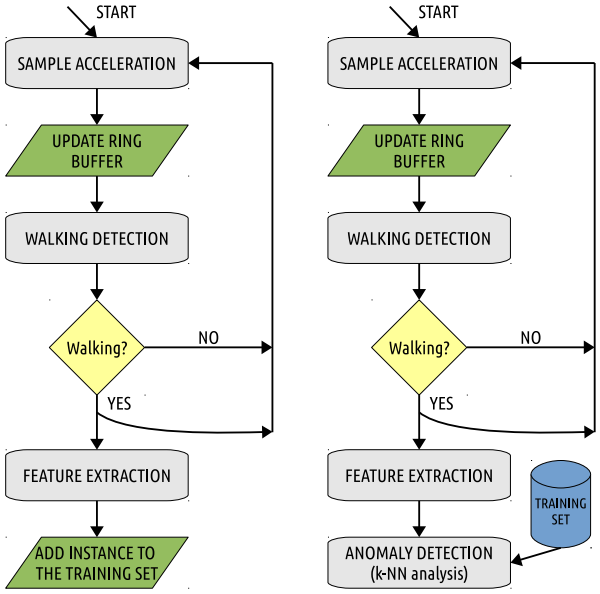
In [7] the authors presented a large database containing gait traces collected using accelerometers and gyroscopes. The database was also used to evaluate the performance of some gait-based authentication techniques [8]–[11]. However, the small number (two) of traces for each subject in the database has hindered its validity in evaluating gait authentication techniques, as such limited data cannot take into the account the slight variation in one's own walking pattern. In fact, there is only one trace, besides the one used for training, for evaluating the accuracy of an authentication technique. In addition, such trace was collected during the same session and under the same scenario, thus it is reasonable to assume that it is highly similar to the one used for training.

In [12], a method is proposed to assess authenticity of information produced by a remote health monitoring system. The aim of the method is to detect both fake data produced by patients who shake the device to simulate the prescribed activities and the use of the monitoring device by another person, e.g. a friend who performs the patient's activities on his/her behalf. The work in [12] was motivated by previous experience of the authors, who observed that in a study which comprises 90 cardiac patients (45 in the intervention group and 45 in the control group), some participants were found cheating during the study. To detect an impostor, the authors compared walking and running patterns using a Random Forest classifier. The evaluation, carried out on a set of six subjects, showed that the proposed approach has accuracy of 90%. The testing dataset was collected in a supervised environment, where the six subjects were asked to wear the device at their waist and to walk and run for five minutes meanwhile the acceleration data was collected.

Unobtrusive gait verification for mobile phones is discussed in [13], where the authors proposed a technique based on Gaussian Mixture Model - Universal Background Model (previously adopted for speaker verification [14]). The equal error rate was approximately of 14% on a dataset collected in a controlled environment, where subjects were told to carry the device in at least two placements (such as pant front pocket, belt clip, jacket, or bag). An evaluation was also performed in real-world settings, with eight users monitored for two/three weeks.

III. Method

The proposed method exploits an *unsupervised* training phase to automatically learn the typical gait pattern of the genuine user. A flowchart representation of the unsupervised training process is shown in Figure 1a. Raw acceleration samples are used as inputs to a walking detection algorithm. The acceleration segments containing walking pattern (*gait segments*), are then processed by a feature extraction algorithm. The result of feature extraction is a vector with thirteen acceleration-based features (*gait instance*). During the training phase each detected gait instance is added to the training set.



(a) Training phase (b) Authentication

Fig. 1. Flowchart representation of the proposed method.

When the training phase ends, the system starts performing gait-based authentication as soon as the user walks (Figure 1b). The anomaly detection algorithm, trained on the previously generated training set, classifies gait instances as genuine or abnormal.

Details of the proposed technique will be described in the following sections.

A. Walking detection

The walking detection technique is based on the algorithm described in [15]. The algorithm first detects the peaks in the acceleration magnitude signal produced by each step. When eight consecutive steps are detected, a test based on standard deviation is performed on the duration of the steps. If standard deviation is below a predefined threshold, the acceleration segment will then be recognized as a gait pattern. Since the signal may be highly asymmetric when the sensor is in a trouser pocket, left and right steps are evaluated separately. The algorithm, despite its simplicity, showed high accuracy in detecting walking activity when the sensor was placed in a pocket or near the waist. The parameters of the algorithm are user-independent.

In this work, the algorithm was further refined in order to ensure that only segments showing a consistent pattern are considered. More precisely, a filter based on autocorrelation was added to verify the similarity among consecutive strides. In addition, the first and the last steps in a walk were discarded.

TABLE I
SELECTED FEATURES

AC1	AAV	IQR	Kurtosis	Mean
Median	MAD	RMS	Skewness	St.Dev.

B. Preprocessing

To reduce noise in the acceleration signal, each gait segment is low-pass filtered at 20 Hz using a second-order Butterworth filter. After, the system automatically estimates three acceleration values: (i) the Euclidean norm of the acceleration vector (acceleration magnitude), (ii) the acceleration along the direction of gravity (vertical acceleration), (iii) the Euclidean norm of the acceleration vector on the horizontal plane (horizontal acceleration magnitude). Vertical acceleration and horizontal acceleration magnitude are calculated as indicated in [16].

These three acceleration values are independent from the orientation of the device with respect to the user's body. Thus, users can wear the device without caring about its orientation.

C. Feature extraction

The features used in this work are listed in Table I. Feature selection was performed starting from a set of 37 features and a greedy heuristic feature selection technique based on the wrapper method was used. Mean, median, Inter-Quartile Range (IQR), Root Mean Square (RMS), kurtosis, standard deviation and skewness are statistical measurements which are widely used in activity recognition systems [17]. The Median Absolute Deviation (MAD) is a robust measure of statistical dispersion [18].

The Average Absolute Variation (AAV) has been previously used to recognize the activities of daily living in fall detection systems [2], [19]. It is found as:

$$AAV = \sum_{i=1}^{N-1} \frac{|x_{i+1} - x_i|}{N},$$

where N is the number of samples in the segment; x_i is the i-th sample in the segment.

AC1 is the autocorrelation coefficient at the first dominant period. As suggested in [20], this coefficient indicates the regularity among consecutive steps. Unbiased autocorrelation coefficients are calculated as follows:

$$AC_k = \frac{1}{N-k} \sum_{i=1}^{N-k} x_i * x_{i+k},$$

where AC_k is the k_{th} unbiased autocorrelation coefficient; N is the number of acceleration samples in the gait segment; x_i is the i-th sample minus the average of the samples in the gait segment.

AC1, MAD, kurtosis, standard deviation, and skewness are calculated on the acceleration magnitude of the gait segment samples. AAV and mean are calculated on the horizontal acceleration. Finally, median, IQR, and RMS are calculated on both the vertical and horizontal acceleration. In total, a *gait instance* is a vector with thirteen features.

D. Anomaly detection

The anomaly detection technique is based on k-NN sum analysis. The *Anomaly Score* (AS) of a gait instance is determined by the sum of the distances with the k-nearest neighbors in the training set:

$$AS_i = \sum_{j=1}^{k} distance\ (g_i, n_j),$$

where n_j is the j-th nearest neighbor of g_i in the training set. The distance between gait instances is found using the Euclidean distance. A prior normalization step is performed to ensure that the features contribute to the distance with equal importance.

The algorithm determines a threshold to discriminate genuine and abnormal gait instances on the basis of their anomaly score. A gait instance g_{new} is classified as abnormal if and only if:

$$AS_{new} > TH,$$

where AS_{new} is the anomaly score of g_{new}, and TH is the threshold selected by the algorithm.

The threshold TH is selected using a parameter $c \geq 0$ as follows:

- if $c \in$ [0,1], TH is found such that the proportion of instances in the training set having an anomaly score smaller than TH is equal to c;
- if $c > 1$, TH is equal to c times the greatest anomaly score in the training set.

For example, if c = 0.5, the threshold is set as the median among the AS values of the training set instances. If c = 1, instead, the highest AS among training instances is used as the threshold. A higher choice for c is likely to produce less false rejections, meaning that genuine gait segments are correctly authorized. On the other hand, this may hinder the performance in terms of false matches, where a significant proportion of gait instances produced by unauthorized users could be authenticated as genuine.

It is important to highlight that the training set contains only the genuine user's instances, which are used to model the authorized gait pattern. Conversely, unauthorized gait patterns are totally unknown to the system. This aspect enables training instances to be collected in a totally unsupervised fashion when the user starts using the gait-based authentication application.

IV. EXPERIMENTAL SETTING AND PREPROCESSING

This section describes the experiments carried out to evaluate the performance of the proposed method.

A. Wearable device

The device used in our experiments is a Shimmer 2r [21], which embeds a TI MSP430 microcontroller (up to 8 MHz clock, 10 KB RAM) and a Freescale MMA7361 tri-axial accelerometer with $\pm$6 g range per axis. Acceleration samples were stored on the Shimmer SD memory during the experiments, in order to enable repeatable analysis on collected data.

TABLE II
MAIN CHARACTERISTICS OF THE DATASETS

Dataset	Users	Sensor position	Environment
D1	20	Waist (lower back)	Corridor (supervised)
D2	20	Front trouser pocket	Corridor (supervised)
D3	6	Front trouser pocket	Unsupervised

TABLE III
VOLUNTEERS' CHARACTERISTICS

Dataset	Gender		Age	Height [cm]	Weight [kg]
	M	F	(mean±SD)	(mean±SD)	(mean±SD)
D1	12	8	27.8 ± 3.8	171.7 ± 10.6	68.6 ± 16.1
D2	15	5	34.6 ± 12.9	175.3 ± 8.7	70.4 ± 12.3
D3	3	3	37.8 ± 19.5	168.3 ± 5.8	64.3 ± 16.0

However, it was verified that the device is capable of executing the walking detection algorithm and gait-based authentication in real-time.

B. Datasets

Three different datasets were used: the main characteristics are shown in Table II and Table III.

The first two datasets, D1 and D2, were both collected in a supervised condition: the volunteers were asked to walk four times in a corridor. In D1, the Shimmer device was placed on the waist with a belt, while in D2, the users placed the device inside their trouser pocket. In the latter case, the device was encapsulated into a small box (95x60x12 mm) to mimic the form factor of a smartphone.

The traces of D3, instead, were collected without any supervision. Some information about these experiments are shown in Table IV, including duration, activities performed, and gait segments detected. The users were asked to keep the sensor in their trouser pocket during their normal activities, for about ten hours on average. To reduce the burden, the volunteers were asked to roughly annotate the current activity or location. More precisely, the following labels were used: home, office, transport, city, and countryside. *Home* includes activities such as housekeeping, watching TV, resting; *office* is for time spent at work, and generally consists in short walks and long periods sitting in front of a desk; *transport* refers to using private or public transportation; *city* is used for periods spent visiting shops, bars, and walking outdoors; finally, *countryside*, refers to periods spent walking on uneven terrains in the countryside.

C. Evaluation procedure

At first, the walking detection algorithm was applied to the datasets in order to automatically extract gait segments. These segments were then processed with the feature extraction to extract gait instances. As previously mentioned, a gait instance is a vector with thirteen acceleration-based features.

The supervised datasets D1 and D2 were used for a first evaluation of the authentication method in supervised environments. Due to the reduced amount of training data, leave-one-instance-out cross validation was used. For each user x the *False Rejection Rate* (FRR) and the *False Match Rate* (FMR) were estimated as follows:

- the gait instances belonging to x formed the training set;
- one instance i belonging to x was left out from the training set, and the anomaly detection classifier was trained on the remaining ones;
- FRR was estimated on i, while FMR was estimated on the instances produced by the other users in the dataset;
- this procedure was repeated for each instance in the training set, and the classification results were averaged.

In D3, where the data was collected in uncontrolled scenarios, much more gait segments were available to train and validate the classifier. For each user, we evaluated the classification accuracy using a different percentage of the available data for training. More precisely we evaluated the results obtained by using 50%, 75%, and 90% of the genuine user's gait instances for training. The remaining gait instances belonging to the genuine user were used to evaluate FRR, while all the gait instances produced by the other users were used to estimate FMR.

The results of the evaluations described above depend on the parameters selected for the anomaly detection algorithm: the number of neighbors k used in k-NN analysis, and the parameter c used to find the threshold to discriminate between genuine and unauthorized user. ROC and EER analysis, using c as the varying parameter, was used to select k in the range [1,10]. For D1 and D2 the choice was to set k = 2, while for D3 k = 3 was used. After selecting a value for k, the performance achieved by the classifier was measured in terms of the *Equal Error Rate* (EER).

As a corollary contribution, the discrimination of the selected feature set for gait identification was also evaluated. As mentioned, the main objective of identification is to recognize the current user among a predefined set of known users. Standard supervised classifiers were used for this evaluation.

V. RESULTS AND DISCUSSION

In the following subsections, we will present and discuss the results related to the supervised as well as the unsupervised experiments. Then, as a corollary contribution, we will show the results of gait identification based on the same feature set.

A. Supervised authentication experiments

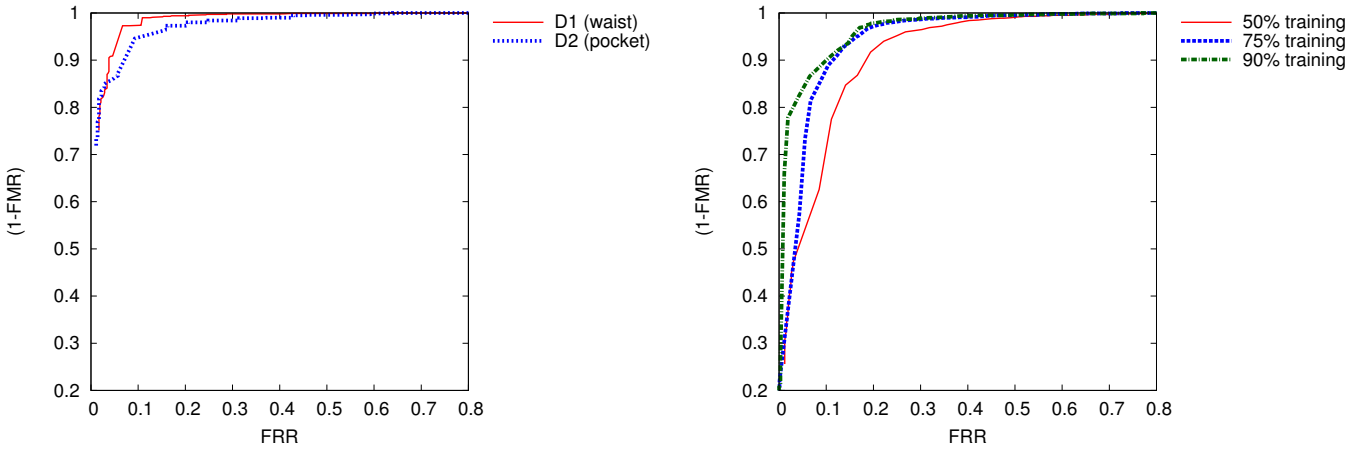
The ROC plot obtained setting k = 2 in the supervised scenarios is depicted in Figure 2a. The average EER is 5.7% for D1, and 9.0% for D2.

In D1, the sensor was firmly placed on the user's waist using a belt. The waist is the most common body position in accelerometer-based gait analysis systems, being an approximation of the center of mass [22]. On the other hand, in D2 the user placed the device in his/her trouser pocket. This position is likely to be more convenient for the user, but inevitably leads to an asymmetric gait pattern. Also, the acceleration signal is noisier due to the possible movements inside the pocket.

Hence, it is interesting to note that, despite a slightly reduced performance in the trouser pocket experiment, the

TABLE IV
STATISTICS ABOUT THE UNSUPERVISED DATASET D3

User	Experiment Duration [h]	Activities (%)					Gait segments detected
		Home	Office	Transport.	City	Countryside	
1	8.2	0.0	76.6	4.1	19.3	0.0	562
2	11.9	0.0	82.9	0.0	17.1	0.0	721
3	9.2	94.7	0.0	2.2	3.2	0.0	326
4	10.6	0.0	82.4	0.0	17.6	0.0	595
5	12.3	54.3	36.7	9.0	0.0	0.0	479
6	8.6	18.9	0.0	43.6	9.5	28.1	259
Total	60.8	28.0	48.3	8.9	10.8	4.0	2942



(a) Supervised experiments, D1 and D2.

(b) Unsupervised experiment, D3.

Fig. 2. ROC analysis of authentication in both controlled and uncontrolled environments.

proposed method proved to be robust enough to achieve high accuracy in both cases.

B. Unsupervised authentication experiments

In the unsupervised experiments, we evaluated the average performance achieved by using different portions of the genuine user's data as the training set. The ROC plot in Figure 2b shows the results of this analysis.

When using 50% of the available genuine user's data for training, the EER is 14.8%. Classification results improve when more training instances are provided to the anomaly detection algorithm: the EER decreases to 10.8% and 9.7% when the portion of training data is 75% and 90%, respectively.

Taking into account the relatively higher variability of gait during everyday activities in uncontrolled environments, the results achieved by the proposed method are promising. In these unsupervised experiments, despite the limited duration, the users produced gait segments in different contexts, as reported in Table IV. For example, one user spent the final part of the experiment in the countryside, thus walking on a completely different terrain. Nevertheless, the classifier showed high accuracy when enough gait examples were provided for training the anomaly detection algorithm. Indeed, with 90% of the genuine user's data to form the training set, the EER result is close to the one achieved in the respective supervised experiment (D2).

In this evaluation, during the training phase, all the gait instances were added to the training set. While the results show that the performance improves with more training data, it would be important to prevent possible outliers from being included into the training set. This task was partially performed by the proposed walking detection algorithm, which uses standard deviation and autocorrelation to ensure that only consistent gait segments are used for authentication.

After the unsupervised training phase, reinforcement learning can be easily implemented with the proposed approach. When a false rejection occurs, the genuine user can be authenticated relying on a different method (e.g. a PIN). Then, the system can automatically add the rejected gait instance to the training set, in order to reduce the probability of similar errors in the future.

C. Gait identification

Figure 3 shows the results of gait-based identification in D3, achieved by using the same walking detection algorithm and feature set combined with supervised classifiers. More precisely, it shows the accuracy achieved by four classifiers with training data of different sizes, which in this case contains examples from all the users in the dataset. Remarkably, using neural network, random forest, or k-NN classification the

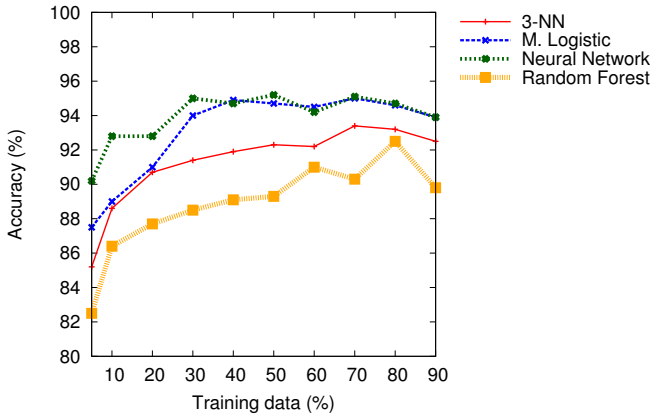


Fig. 3. Identification accuracy in the uncontrolled experiments.

accuracy is consistently above 90% when at least 20% of data is used for training.

As previously explained, supervised classification cannot be used for gait-based authentication, since unauthorized gait instances are not available in advance to train the classifier. This approach could only be used to identify the current user among a predefined set of known users. However, this result confirms the efficacy of the selected feature set in capturing the most relevant characteristics of gait patterns.

VI. Conclusions and Future Work

A new gait analysis method for user authentication on wearable devices has been presented. By automatically learning the user's gait pattern during the initialization phase, the proposed method can authenticate the user from the walking pattern captured by an embedded accelerometer. The lightweight k-NN based anomaly detection algorithm used for the authentication process can be implemented in a wearable node with very limited resources. Extensive experiments were conducted to evaluate the performance of the proposed approach. The results obtained from both controlled and uncontrolled experiments have shown the robustness and high classification accuracy of the method.

In future work, we plan to extend the duration of the unsupervised experiments and to increase the number of subjects involved. With more data, it will be possible to evaluate the training phase extensively. In addition, techniques for the detection of outliers could be used to limit the growth of the training set and improve the classification rate.

References

[1] S. Patel, H. Park, P. Bonato, L. Chan, and M. Rodgers, "A review of wearable sensors and systems with application in rehabilitation," *Journal of NeuroEngineering and Rehabilitation*, vol. 9, no. 1, 2012.

[2] S. Abbate, M. Avvenuti, F. Bonatesta, G. Cola, P. Corsini, and A. Vecchio, "A smartphone-based fall detection system," *Pervasive and Mobile Computing*, vol. 8, no. 6, pp. 883 – 899, 2012.

[3] J. Kirby, C. Tibbins, C. Callens, B. Lang, M. Thorogood, W. Tigbe, and W. Robertson, "Young people's views on accelerometer use in physical activity research: Findings from a user involvement investigation," *ISRN Obesity*, vol. 2012.

[4] L. Bianchi, D. Angelini, and F. Lacquaniti, "Individual characteristics of human walking mechanics," *Pflügers Archiv*, vol. 436, no. 3, pp. 343–356, 1998.

[5] H. J. Ailisto, M. Lindholm, J. Mantyjarvi, E. Vildjiounaite, and S.-M. Makela, "Identifying people from gait pattern with accelerometers," in *Proc SPIE*, vol. 5779, 2005, pp. 7–14.

[6] D. Gafurov, E. Snekkenes, and P. Bours, "Gait authentication and identification using wearable accelerometer sensor," in *Automatic Identification Advanced Technologies, 2007 IEEE Workshop on*, June 2007, pp. 220–225.

[7] 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 Recognition*, vol. 47, no. 1, pp. 228 – 237, 2014.

[8] D. Gafurov, E. Snekkenes, and P. Bours, "Improved gait recognition performance using cycle matching," in *Advanced Information Networking and Applications Workshops (WAINA), 2010 IEEE 24th International Conference on*, April 2010, pp. 836–841.

[9] L. Rong, Z. Jianzhong, L. Ming, and H. Xiangfeng, "A wearable acceleration sensor system for gait recognition," in *Industrial Electronics and Applications, 2007. ICIEA 2007. 2nd IEEE Conference on*, May 2007, pp. 2654–2659.

[10] M. Derawi, P. Bours, and K. Holien, "Improved cycle detection for accelerometer based gait authentication," in *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on*, Oct 2010, pp. 312–317.

[11] N. T. Trung, Y. Makihara, H. Nagahara, R. Sagawa, Y. Mukaigawa, and Y. Yagi, "Phase registration in a gallery improving gait authentication," in *Biometrics (IJCB), 2011 International Joint Conference on*, Oct 2011, pp. 1–7.

[12] N. Alshurafa, J.-A. Eastwood, M. Pourhomayoun, S. Nyamathi, L. Bao, B. Mortazavi, and M. Sarrafzadeh, "Anti-cheating: Detecting self-inflicted and impersonator cheaters for remote health monitoring systems with wearable sensors," in *Wearable and Implantable Body Sensor Networks (BSN), 2014 11th International Conference on*, June 2014, pp. 92–97.

[13] H. Lu, J. Huang, T. Saha, and L. Nachman, "Unobtrusive gait verification for mobile phones," in *Proc of the 2014 ACM Int Symposium on Wearable Computers*, New York, NY, USA, 2014, pp. 91–98.

[14] D. A. Reynolds, T. F. Quatieri, and R. B. Dunn, "Speaker verification using adapted gaussian mixture models," *Digital Signal Processing*, vol. 10, no. 13, pp. 19 – 41, 2000.

[15] G. Cola, A. Vecchio, and M. Avvenuti, "Improving the performance of fall detection systems through walk recognition," *Journal of Ambient Intelligence and Humanized Computing*, vol. 5, no. 6, pp. 843–855, 2014.

[16] D. Mizell, "Using gravity to estimate accelerometer orientation," in *Proc IEEE Int Symp Wearable Comput*, 2003, pp. 252–253.

[17] M. Zhang and A. A. Sawchuk, "A feature selection-based framework for human activity recognition using wearable multimodal sensors," in *Proceedings of the 6th International Conference on Body Area Networks*, ser. BodyNets '11. ICST, Brussels, Belgium, Belgium: ICST, 2011, pp. 92–98.

[18] C. Leys, C. Ley, O. Klein, P. Bernard, and L. Licata, "Detecting outliers: Do not use standard deviation around the mean, use absolute deviation around the median," *Journal of Experimental Social Psychology*, vol. 49, no. 4, pp. 764 – 766, 2013.

[19] S. Abbate, M. Avvenuti, G. Cola, P. Corsini, J. V. Light, and A. Vecchio, "Recognition of false alarms in fall detection systems," in *Proc IEEE Int Workshop Consum eHealth Platf Serv Appl*, Las Vegas, NV, USA, Jan. 2011, pp. 538–543.

[20] R. Moe-Nilssen and J. L. Helbostad, "Estimation of gait cycle characteristics by trunk accelerometry," *Journal of Biomechanics*, vol. 37, no. 1, pp. 121 – 126, 2004.

[21] Shimmer, "http://www.shimmersensing.com," 2015.

[22] D. Giansanti, S. Morelli, G. Maccioni, and G. Constantini, "Toward the design of a wearable system for fall-risk detection in telerehabilitation," *Telemed e-Health*, vol. 15, pp. 296–299, 2009.