Gait-based authentication using a wrist-worn device

Guglielmo Cola
Dipartimento di Ingegneria dell'Informazione
University of Pisa
guglielmo.cola@iet.unipi.it

Marco Avvenuti
Dipartimento di Ingegneria dell'Informazione
University of Pisa
marco.avvenuti@unipi.it

Fabio Musso
University of Pisa
f.musso@studenti.unipi.it

Alessio Vecchio
Dipartimento di Ingegneria dell'Informazione
University of Pisa
alessio.vecchio@unipi.it

ABSTRACT

Every individual has a distinctive way of walking. For this reason gait can be a key element of biometric techniques aimed at authenticating and/or identifying the user of a wearable device. This paper presents a lightweight method that uses the acceleration collected at the user's wrist for authentication purposes. The user's typical gait pattern is learned during the first period of use, then detection of anomalies in a set of acceleration-based features is used to understand if a new user, a possible impostor or a thief, is wearing the device. The method has been successfully evaluated with 15 volunteers, showing an Equal Error Rate of 2.9%. These results suggest that gait-based authentication with a wrist-worn device can be carried out with high accuracy levels. A comparison with a similar method executed on a pocket-worn device is also included.

CCS Concepts

•**Security and privacy** → **Biometrics;** Usability in security and privacy; •**Human-centered computing** → **Mobile devices;** *Gestural input;* •**Computer systems organization** → **Sensors and actuators;**

Keywords

Accelerometer; Anomaly detection; Biometrics; Gait analysis; Gait-based authentication; Gait-based identification; Smartwatch; Walking detection; Wearable sensor; Wrist-worn device

1. INTRODUCTION

Smartphones are nowadays a key element of our lives, as they are used to perform a large number of common activities, such as paying in shops, tracking the user during sport sessions, or suggesting navigation directions. Smartphones are increasingly used in combination with other wearable devices, in particular smartwatches. The latter ones can be worn continuously throughout the day and, besides being a convenient tool for interacting with smartphones in simple operations, they also provide the opportunity to gather information about their users with unprecedented levels. In particular, since smartwatches are directly worn over the skin and thanks to additional sensors with respect to smartphones (e.g., heart rate sensor), they are particularly suitable for fitness monitoring and medical applications.

These capabilities are inevitably paired with significant concerns from the point of view of privacy and security. In fact, information collected through these devices is strictly personal and it can be used to infer user's habits and lifestyle. Unfortunately, access to these devices is generally granted using simple authentication methods like passwords and PINs. In addition, these mechanisms are frequently disabled by users: interaction with smartphones is characterized by a large number of short sessions, thus introducing a PIN at the beginning of each session is cumbersome.

The effort required from the user in authenticating himself/herself can be drastically reduced using biometric techniques. Many biometric methods are based on the fact that every user has a very specific way of performing some activities. Thus, the acceleration produced when these activities are carried out can be compared against a template acquired during the setup phase. The activity usually considered for authentication purposes is walking, as it is frequently executed. Also, gait is very user-specific [4], and this is clearly important in a recognition method based on biometrics.

Besides smartphones and smartwatches, biometric recognition methods are relevant for the whole class of wearable devices, in particular those used for personal healthcare [22]. In telemedicine applications, patients are remotely monitored by means of wearable systems. It has been observed that in some situations, patients are tempted to give their own device to someone else, e.g. to reach the prescribed amount of activity [15]. In this context, gait-based authentication can be useful to recognize possible misbehaving users.

Biometric methods based on gait can be divided in two

MOBIQUITOUS '16, November 28-December 01, 2016, Hiroshima, Japan

DOI: http://dx.doi.org/10.1145/2994374.2994393

categories, those used for *authentication* and those used for *identification* [16]. In authentication, the system is aimed at understanding if the user who is currently wearing the device is the usual one (the owner of the device) or a new user. The latter is not known in advance. This means that the system knows the typical gait pattern of the owner, but it has no knowledge about possible other users. Authentication can be useful, for instance, to lock the device if the current user does not behave like the owner. In identification, the system is aimed at understanding who is the current user within a set of possible users. The set of possible users is known in advance, i.e. a template of gait is available for every user. Identification is useful whenever a single device is shared by a group of people, as operations can be automatically customized to match the user's needs and preferences.

This paper presents a gait-based authentication method that relies on accelerometric information collected at the user's wrist, e.g. by using a smartwatch. Performing detection and analysis of gait with an accelerometer placed near the wrist is much more challenging than using a sensor close to the user's center of mass, because hands are subject to a significantly larger amount of accelerations throughout the day. The proposed method is able to distinguish the genuine user (i.e. the owner) from unauthorized users. The typical gait pattern of the genuine user is learned during an initial period of use; subsequently, anomalies in gait are automatically detected and used to infer if the current user is an impostor. An experimental evaluation of the method has been carried out with the help of 15 volunteers. Results show that the method is able to achieve an Equal Error Rate (EER) as low as 2.9%.

2. RELATED WORK

Some pioneering work about gait-based authentication using accelerometric information has been presented in [2]. The method relies on cross-correlation for comparing gait instances collected at runtime against a template of the user's typical step. The technique, in an experimental evaluation carried out using a waist-mounted accelerometer on a pool of 36 users, showed a correct authentication rate equal to 88%.

The effectiveness of different metrics, in the context of gait-based authentication, has been explored in [11]. In particular, correlation, histogram, high-order moments, and absolute distance have been compared on a set of 50 users. For each user six gait instances have been collected using an accelerometer placed in their trouser pockets. Best results were obtained using absolute distance, which achieved an EER of $\sim$ 7%. The effects caused by disturbing factors were also preliminarily studied (in particular, carrying a backpack).

A method for gait-based verification on smartphones is discussed in [18]. Acceleration samples were collected at 100 Hz and processed in blocks of 512 samples. Features both in the frequency and time domain are extracted and provided as input to a classification system. The adopted classification method relies on a Gaussian Mixture Model trained according to the user's typical gait pattern. Another model, the Universal Background Model, is used to represent the different walking pattern exhibited by a population of individuals. Verification of the user is based on the output of the two models. The method has been evaluated both in controlled and uncontrolled conditions. In controlled experiments, a set of 47 subjects performed a number of activities, such as standing, sitting, walking, biking, etc, while carrying their smartphone (different positions were allowed). In such scenario the obtained EER was approximately 14%. The uncontrolled experiments comprised eight subjects, who were monitored for two/three weeks.

A comparison of some gait-based authentication methods is presented in [21]. In particular, a novel technique is compared with some existing ones ([12, 24, 9]) on a common dataset of gait traces. The size of the dataset is very large, as it comprises traces collected from $\sim$ 740 users. Nevertheless, the number of gait-instances for each user is rather small: only two instances, one used for training and the other for evaluation (this obviously poses a limit on the degree of diversity in the set of gait instances produced by a single user).

Gait-based authentication is also used to detect user spoofing in mobile healthcare systems [23]. Accelerometer readings were collected at 50 Hz using a common smartphone. Only the vertical component of acceleration is used to perform authentication. Extraction of gait cycles is based on the Pearson's correlation coefficient. Then, to cope with the possible different walking speeds, collected gait cycles are aligned to a reference step cycle via interpolation. The proposed framework is able to compute user verification either on the mobile device or on an external server. If executed on the mobile device, authentication is carried out using weighted Pearson correlation coefficients; if executed on the server-side, authentication is achieved by means of a Support Vector Machine classifier. An experimental evaluation was carried out involving a set of 26 subjects for six months. Over 3000 traces were collected (each trace included ten minutes of walking). An 80% detection rate and 10% false positive rate were obtained when classification occurred on the mobile device. The server-based approach showed a better detection rate (90%) and similar false positive rate.

Another system related to mobile healthcare is the one discussed in [3]. From previous studies, the same authors observed that a number of users involved in medical treatment tried to cheat (e.g. by giving the monitoring device to a friend, or simulating prescribed activities). Thus, they propose a method for user authentication based on a Random Forest classifier. An experimental evaluation was carried out with the help of six volunteers in controlled conditions.

A gait-based identification and authentication method, which relies on a smartwatch as a means for collecting accelerometric information, is discussed in [14]. Approximately five minutes of walk in a set of 59 users were collected using commercial smartwatches. Sampling frequency was set at 20 Hz. More than 40 features were extracted from raw data and used as input to a set of classifiers (Random Forest, Rotation Forest, Naive Bayes, and Multi-Layer Perceptron). Using ten seconds of data, the best performing method, in terms of identification, was Rotation Forest, which achieved an accuracy equal to 84%. As far as authentication is concerned, the best performing classifiers were Random Forest and Rotation Forest, with an accuracy approximately equal to 98%. In particular, results about authentication were obtained creating an impostor model. Such model was created using the traces of four users extracted randomly from the set of 59 users. Then evaluation was carried out using a different set of four users (again extracted randomly form the set of all users).

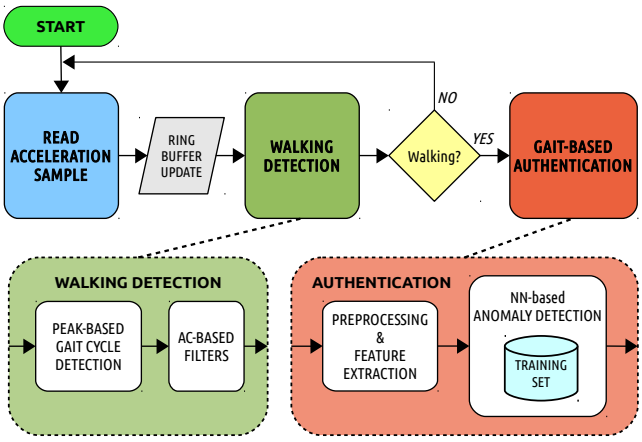


Figure 1: Flowchart representation of the proposed method.

With the exception of the last study, all previous methods rely on embedded devices and smartphones attached to the user's waist, or placed in one of the user's pockets. Thus, the possibilities of gait-based authentication using acceleration collected at the user's wrist are little explored. Besides providing a deeper understanding of such solution, this paper also includes a comparison with a smartphone-based solution.

3. METHOD

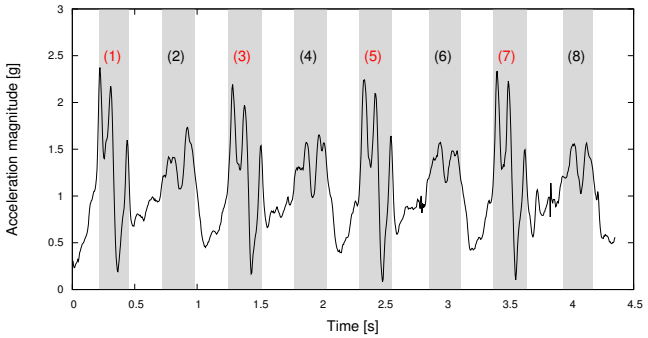
The gait-based authentication method is described by the flowchart in Figure 1. A wrist-worn device – equipped with a tri-axial accelerometer – continuously collects acceleration samples. Acceleration samples are used as inputs to a *walking detection* algorithm. Walking detection enables the extraction of *gait segments* from raw acceleration data. Each gait segment is a vector of acceleration samples collected during a predefined number of gait cycles. *Feature-extraction* is applied to each gait segment to extract a vector with the most relevant features. Hereafter, we use the term *gait instance* to refer to such feature vector. Gait instances are finally used to feed an *anomaly detection* technique – exploiting anomaly detection, the system recognizes whether a gait instance has been produced by the authorized user.

Each subtask of the authentication method is described in detail in the following sections.

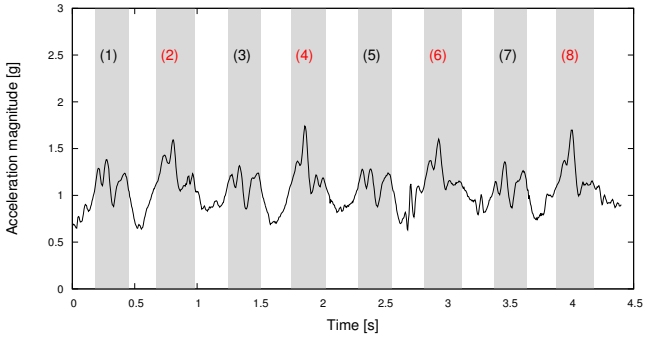
3.1 Walking detection algorithm

The walking detection technique is mainly based on the peak-detection algorithm described in [8]. The acceleration magnitude signal is analyzed so as to identify the group of peaks produced at each step. A gait segment is detected when 8 consecutive steps are found. It is a lightweight technique that can be executed in real time on miniaturized devices and that proved able to achieve high detection accuracy when the sensor is placed in near-waist position (e.g., in a trouser pocket, or fixed at the waist using a belt). The technique has been adapted to work with acceleration signals coming from a wrist-worn device (e.g., a smartwatch).

An example of the peculiarities of gait acceleration patterns is shown in Figure 2, which shows two acceleration magnitude (Euclidean norm) signals produced simultaneously by the same user. In this experiment the user walked



(a) Front trouser pocket (thigh) trace.



(b) Wrist trace.

Figure 2: Gait acceleration pattern example.

carrying one sensor in a front trouser pocket (Figure 2a) and another sensor attached to his wrist like a watch (Figure 2b). In both conditions, the algorithm can exploit the group of peaks in the acceleration signal that are produced by each foot contact. It is interesting to observe that the same groups of peaks are clearly visible even in the wrist trace – the foot impact is actually transmitted to the accelerometer using the body as a medium [17]. Inevitably, since the accelerometer is farther from the feet, the signal is less intense when collected at the wrist. To manage this difference, the threshold used to detect peaks in the acceleration magnitude was lowered for wrist traces.

Each step is numbered and highlighted with a gray vertical band. In both traces, it is possible to observe the asymmetry in the signal between consecutive steps/groups. This is due to the fact that both sensors are on a specific side of the body (left or right) – the step involving the leg closer to the sensor produces the highest acceleration peaks, even when the sensor is wrist-worn. Such steps are highlighted in Figure 2 with red numbers. In Figure 2a it is clearly visible that the odd steps were produced by the leg that is carrying the sensor. Conversely, the even steps in Figure 2b were produced by the leg on the same side as the hand carrying the watch. As previously mentioned, in this particular experiment the sensors were placed at opposite sides of the user's body (right thigh and left arm).

The walking detection technique was further refined adding a filter based on autocorrelation to reduce the detection of gait segments characterized by an irregular pattern between consecutive gait cycles (a gait cycle includes 2 steps, and it is expected to be regular regardless of the asymmetry in the position of the sensor).

Table 1: List of features.

AAV	AC_C1	AC_C2
AC_DP1	AC_DP2	duration
IQR	kurtosis	max
median	mean	MCR
MAD	min	P2P
RMS	skewness	st.dev.

The aim of this filtering technique was twofold: first, irregular gait patterns are less suitable for gait analysis; second, the regularity check can be exploited to filter out "fake" gait segments, which may be detected when the user is simply moving the hand that is carrying the device.

3.2 Preprocessing and Feature extraction

An acceleration sample consists of three components, one per each of the three axes of the accelerometer. In turn, a gait segment, being a vector of samples, is actually formed by three acceleration vectors: **x**, **y**, and **z**. The acceleration measured on these vectors is affected by the orientation of the device with respect to the user's body.

To reduce the effect of noise, each acceleration vector is low-pass filtered using a second-order Butterworth filter with 20 Hz cut-off frequency. Then, an additional vector **m** (*magnitude*) is computed by finding the Euclidean norm (acceleration magnitude) of each sample in the gait segment:

$$acceleration\ magnitude = \sqrt{x^2 + y^2 + z^2}. \quad (1)$$

Acceleration magnitude is insensitive to changes in the orientation of the device.

Two additional vectors can be estimated by projecting the acceleration vectors on the direction of gravity (*vertical acceleration*, **v**) and on the horizontal plane (*horizontal acceleration magnitude*, **h**). The technique to compute these projections is indicated in [19]. These vectors are relative to the direction of gravity, and are thus insensitive to changes in the orientation of the device with respect to the user's body.

In sum, there are six vectors that can be used to feed feature extraction algorithms: **x**, **y**, **z**, **m**, **v**, and **h**. Hereafter, we use a suffix to describe on which specific vector a feature-extraction algorithm is computed. For example, $mean_x$ indicates that the mean is found on the acceleration vector **x**.

The feature-extraction algorithms considered in this paper are listed in Table 1. The list includes widely-used statistical features, such as *mean*, *median*, *skewness*, *kurtosis*, Peak-to-Peak amplitude (*P2P*), standard deviation (*stDev*), and Median Absolute Deviation (*MAD)*.

The Average Absolute Variation (AAV) has been successfully used in fall detection and gait analysis systems [1, 6, 7]. It is found as:

$$AAV = \sum_{i=1}^{N-1} \frac{|x_{i+1} - x_i|}{N}, \quad (2)$$

where N is the number of samples in the gait segment, and x_i is the i-th sample in the segment.

Autocorrelation-based features are used to evaluate regularity among gait cycles [20]. Unbiased autocorrelation coefficients are found 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 mean of the samples in the gait segment. Coefficients are also normalized to one at zero lag ($AC_0 = 1$). Finally, the dominant periods in the autocorrelation signal are found by means of a peak detection algorithm. Features AC_DP1 and AC_DP2 describe the lag of the first and second dominant period, respectively. In turn, AC_C1 and AC_C2 are the normalized coefficients at the first and second dominant period.

The procedure used to select a subset of these features is described in Section 4.3. The result of feature extraction is a *gait instance*, which consists in a vector of features.

3.3 Anomaly detection

The approach used in this paper to distinguish genuine instances from unauthorized users' data is based on *semi-supervised* anomaly detection [5]. It is supposed that a set with genuine user's instances is available to form a training set. Differently from systems that use *supervised* classifiers, this method does not require the availability of other users' data.

Euclidean distance and Nearest-Neighbor (NN) analysis is used to assign an *anomaly score* to each gait instance. This anomaly score, in turn, is compared against a threshold to classify a gait instance as *normal* (genuine user) or *abnormal* (unauthorized user).

Let $T = \{t_1, ..., t_M\}$ be the set of gait instances of the genuine user collected during the training phase, and let $dist(a, b)$ be the Euclidean distance between gait instances a and b. The first step in finding the anomaly score for a given gait instance g consists in computing

$$dist_{min}(g) = dist(g, n_g),$$

where n_g is the nearest-neighbor of g in the training set T. More formally

$$n_g = \arg\min_{i \in T} dist(g, i).$$

Distance $dist_{min}(g)$ is then normalized using the standard deviation of the distances between nearest-neighbors in the training set:

$$sd_T = \sqrt{\frac{1}{M} \sum_{i=1}^{M} (dist_{min}(t_i) - \overline{dist}_T)^2},$$

where

$$\overline{dist}_T = \frac{1}{M} \sum_{i=1}^{M} dist_{min}(t_i).$$

In particular, normalization exploits the average and standard deviation of the NN distances among instances in the training set to produce the anomaly score (AS) as follows:

$$AS_g = \frac{dist_{min}(g) - \overline{dist}_T}{sd_T}. \quad (3)$$

For example, if the average distance in the training set is 0.8 and standard deviation is 0.2, then a gait instance with NN distance equal to 1.2 will have $AS = 2$. Higher anomaly score values indicate that the instance is more distant from the user's training data, and it is thus more likely to belong to an unauthorized user.

The threshold used to distinguish normal and abnormal instance (AS_{th}) is selected by evaluating the trade-off between detecting anomalies and generating false positives. This trade-off is described in Section 5.2 by means of ROC curve analysis.

4. EXPERIMENTAL SETTING AND PREPROCESSING

This section describes the experiments performed to gather gait data, as well as the procedure used to evaluate the performance of gait-based authentication. As previously mentioned, besides illustrating a method suitable for wrist-worn devices, we aim to compare such method with one based on a device carried in a pocket (near the user's thigh).

4.1 Wearable device

The device used in the experiments is a Shimmer 3, embedding a TI MSP430 microcontroller (up to 24 MHz clock, 16 KB RAM, 256 KB flash) and an ST Micro LSM303DLHC accelerometer [25]. Such accelerometer is similar to the ones found in common smartwatches and activity trackers.

During the experiments, acceleration was sampled with $\sim$ 50 Hz frequency. Samples were saved to the Shimmer's SD memory, to ensure repeatable evaluation of collected data. However, we also verified that the device is capable of executing the proposed method in real time.

4.2 Experiments

Fifteen volunteers (4 females, 11 males , age 28.2 $\pm$ 2.5, height 174.2 $\pm$ 9.6 cm, weight 68.7 $\pm$ 14.9 kg) were involved in experiments to gather gait data. Each user carried two Shimmer 3 devices during the experiment: one in a front trouser pocket (*pocket trace*), and another worn like a watch (*wrist trace*). Thus, two simultaneous traces were collected by each volunteer, enabling direct comparison of the same technique with a pocket and wrist-worn device.

Volunteers were asked to walk 6 times a corridor: 2 times at preferred pace, 2 times at fast pace, and finally 2 times keeping the hand inside their pocket. In that way, we were able to collect (at least) 3 different gait patterns from each user. In addition, at the end of the experiment the volunteers were asked to perform random movements with their hands, aiming at producing fake gait detections (movements included, for example, drawing an 8 in the air several times).

Collected gait data were processed with the walking detection algorithm to obtain gait segments.

4.3 Feature selection

As discussed in Section 3, the preprocessing module of the method produces 6 acceleration vectors. Except for autocorrelation-based features, which were found only on acceleration magnitude, and the duration feature, which is simply the duration of a gait segment, all of the other features can be computed on each of the 6 vectors. In sum, there are 83 possible features.

A first reduction of the features can be performed considering the particular scenario – pocket vs. wrist. When the device is worn in a pocket (e.g., a smartphone) it is not reliable to assume that the orientation of the device does not vary over time. Thus, it is key to rely only on acceleration vectors that are insensitive to changes in the orientation of the device, namely the acceleration magnitude ($\mathbf{m}$), vertical acceleration ($\mathbf{v}$), and horizontal acceleration magnitude ($\mathbf{h}$).

A wrist-worn device (e.g., a smartwatch) can be reasonably expected to be always worn with the same orientation with respect to user's arm. Thus, wrist-based gait analysis can exploit the acceleration vectors based on the local coordinate system of the accelerometer ($\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$). On the other hand, the estimation of vertical and horizontal acceleration, which refers to the direction of gravity with respect to the reference frame of the accelerometer, is unlikely to provide useful information. Indeed, the direction of gravity with respect to the device may change significantly within a gait segment, due to the possible pendulum-like swing of the arm.

In sum, the following three approaches were considered regarding the initial set of features:

1. pocket-worn device with features based on orientation-independent acceleration vectors ($\mathbf{m}$, $\mathbf{v}$, $\mathbf{h}$);
2. wrist-worn device with the same approach as for the pocket-worn case;
3. wrist-worn device with features based on $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$, and $\mathbf{m}$ (estimation of vertical and horizontal acceleration is not used).

For each approach, feature selection was performed using the Correlation-based Feature Subset Selection method with greedy hill climbing search [13]. The result of feature selection for each approach is shown in Table 2. Hereafter, we refer to the three approaches as $POCKET_{mhv}$, $WRIST_{mhv}$, and $WRIST_{xyzm}$.

4.4 Evaluation procedure of the anomaly detection technique

This paper studies a one-versus-all authentication problem, where the system is trained only on the genuine user's data and is expected to recognize unauthorized attempts to use the device. Consequently, for each volunteer in the dataset, the method is tested by using that volunteer as the genuine user and the others as the possible impersonators. The evaluation procedure consists of the following steps:

- a volunteer x is set as the genuine user;
- each instance of x is used to estimate the *False Rejection Rate* (FRR) of an anomaly detection classifier trained on the remaining instances (leave-one-instance-out cross-validation);
- the *False Match Rate* (FMR) of the same classifier is estimated with all the data belonging to the other volunteers;
- results related to FRR and FMR are averaged over cross-validation iterations.

FRR and *FMR* are metrics that are typically used to describe the performance of authentication systems. FRR is

Table 2: Evaluated approaches and selected features.

Approach name	Position	Input	Selected features
POCKET_{mhv}	Trouser pocket	**m**, **h**, **v**	AC_C1, AC_DP2, kurtosis_h, kurtosis_m, kurtosis_v, MAD_m, $\max_h$, MCR_m, MCR_v, mean_h, median_h, median_v, $\min_m$, $\min_v$, st.dev_h, skewness_h, skewness_m, skewness_v
WRIST_{mhv}	Wrist	**m**, **h**, **v**	AC_C1, AAV_m, AC_DP1, AC_DP2, duration, IQR_m, kurtosis_m, MCR_h, MCR_m, median_m, median_v, RMS_m, st.dev._h, skewness_h, skewness_m
WRIST_{xyzm}	Wrist	**x**, **y**, **z**, **m**	AC_C1, AAV_y, AC_DP2, kurtosis_x, $\max_x$, $\max_z$, MCR_m, MCR_y, MCR_z, mean_x, mean_y, mean_z, median_m, median_x, median_z, $\min_x$, RMS_z, skewness_y, skewness_m

the proportion of genuine user's instances that are not authorized by the system. FMR is the proportion of unauthorized gait instances that are authorized by the system (inverse of the *true positive rate*).

By choosing a specific threshold on the anomaly score, it is possible to apply the procedure described above and obtain the result in terms of FRR and FMR for each user. However, to better evaluate the performance of the system, it is interesting to evaluate the performance as the threshold is varied. The result of this evaluation is a *ROC curve*, that depicts the trade-off between the true positive rate and the false positive rate [10]. In this biometric application based on anomaly detection, let us define a *positive* as the detection of an unauthorized user, and a *negative* as the detection of the genuine user. According to this definition, it follows that the true positive rate corresponds to the inverse of FMR (1-FMR), while the false positive rate corresponds to the FRR. The ROC curve thus plots 1-FMR versus FRR.

The overall performance of a ROC curve is typically measured, in the context of biometrics systems, in terms of *Equal Error Rate* (EER), which is the point of the curve having the same FMR and FRR value. The *Area Under the Curve* (AUC) is another performance indicator that is commonly used.

5. RESULTS AND DISCUSSION

In the following we first describe and discuss the results of walking detection, both in pocket and wrist position. Then, we present and discuss the results of gait-based authentication with the three different approaches introduced in Table 2. In addition, results related to gait-based identification are shown as a corollary contribution.

5.1 Walking detection results

The histograms in Figure 3 show detailed results of walking detection on both acceleration traces (pocket and wrist). In particular, Figure 3a shows the number of gait segments detected, while Figure 3b describes the average time interval required to detect a gait segment. Both results – detected segments and time interval – are shown per each user and on average.

In terms of detection rate, it can be observed that the algorithm performed fairly well even at the wrist. Indeed, in most cases the difference between pocket and wrist was minimal ($\pm$ 2 detected segments). On average, when the user is walking, a gait segment is provided every 4.9 s in the pocket and every 5.5 s at wrist position. In the worst case, which occurred at the wrist for user 15, a gait segment is detected every 7.4 s. This detection rate reasonably meets the requirements of a gait-based authentication method, where detecting all the steps with high sensitivity is not strictly necessary.

Table 3: Average results of the three approaches.

Metric	POCKET_{mhv}	WRIST_{mhv}	WRIST_{xyzm}
AUC (%)	99.6	97.3	99.6
EER (%)	2.5	8.0	2.9

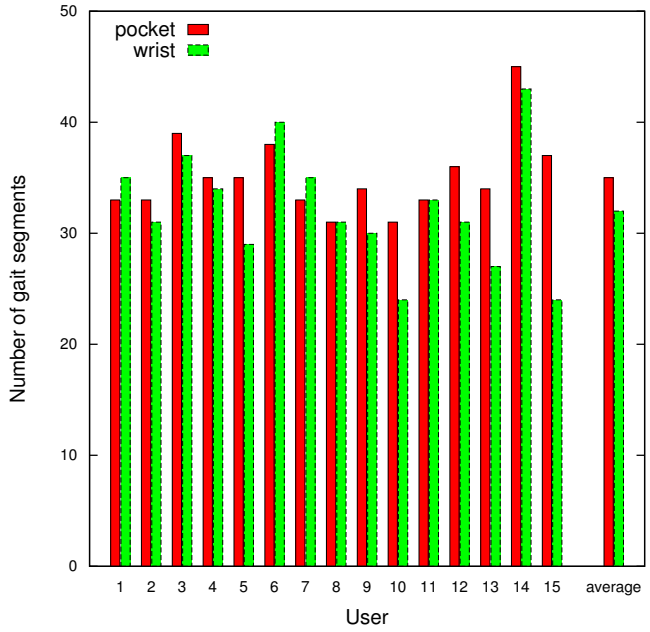
It was also verified that the autocorrelation-based filter successfully filtered out all the random hand movements made by volunteers at the end of their experiments. As it is shown in the next section, filtering out irregular patterns is key to preserve authentication accuracy.

5.2 Gait-based authentication results

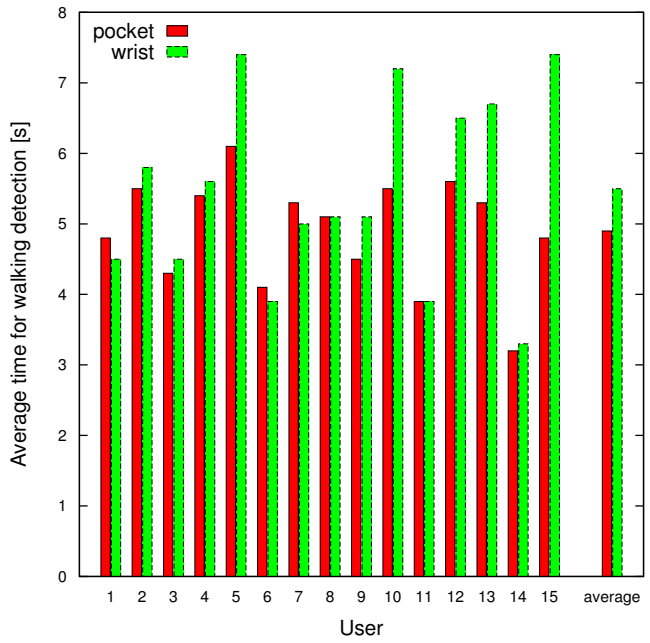
Figure 4 shows the results of ROC analysis applied to the three evaluated approaches. WRIST_{mhv} clearly shows a reduced performance with respect to POCKET_{mhv}, confirming that the estimated vertical and horizontal vectors – when the device is on the arm – provide information that is of little use for gait analysis. That was highly expected, since the acceleration-based technique used for these estimations – described in [19] – is based on the assumption that gravity has a constant orientation with respect to the local reference frame of the accelerometer. While this assumption is reasonable in a front trouser pocket, it is likely to be false with a wrist-worn device, where the device is constantly rotated due to the arm swing during gait. More advanced techniques for estimating gravity direction would require the use of a gyroscope, which we have intentionally excluded to reduce power consumption and ensure lightweight computational requirements.

However, the wrist-worn device can successfully exploit the fact that the local reference frame of the sensor is expected to remain in consistent position, with respect to the user's body, throughout device use (the watch is always worn the same way). As shown in Figure 4, the WRIST_{xyzm} approach is actually capable of achieving results very close to the ones achieved with data collected from the user's pocket.

Average results in terms of AUC and EER are shown in Table 3. WRIST_{xyzm} achieved excellent accuracy, with EER as low as 2.9% and AUC as high as 99.6%. These results are in line with the best performing gait-based authentication works in the literature, which are typically based on waist-



(a) Number of gait segments detected



(b) Time to detect a gait segment in seconds

Figure 3: Walking detection results, per user and on average.

worn or pocket-worn sensors. Also, they are in line with the results achieved by the POCKET$_{mhv}$ approach, which showed the same AUC (99.6%) and a similar EER (2.5%).

These results suggest that – taking advantage of their peculiar placement on the user's body – wrist-worn devices may represent an effective tool for the collection and analysis of gait patterns, including gait-based authentication.

5.3 The impact of autocorrelation-based filtering on EER

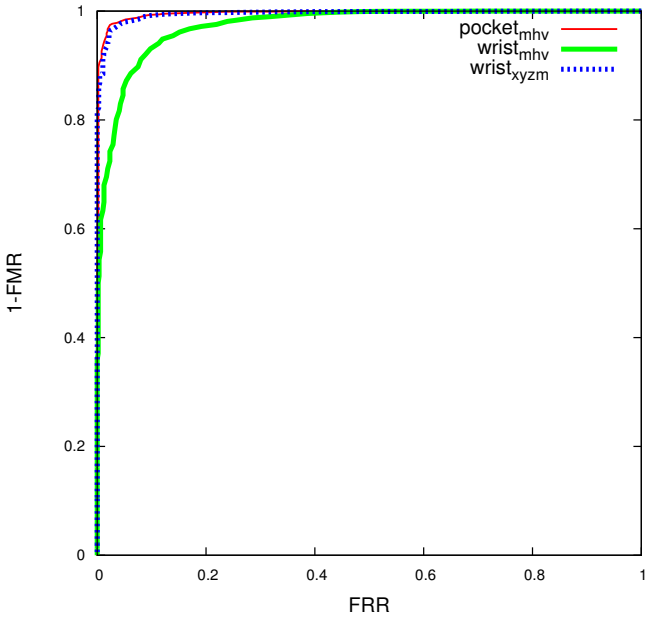


Figure 4: ROC curve analysis of the three approaches.

Table 4: Effect of autocorrelation-based filtering on EER and AUC

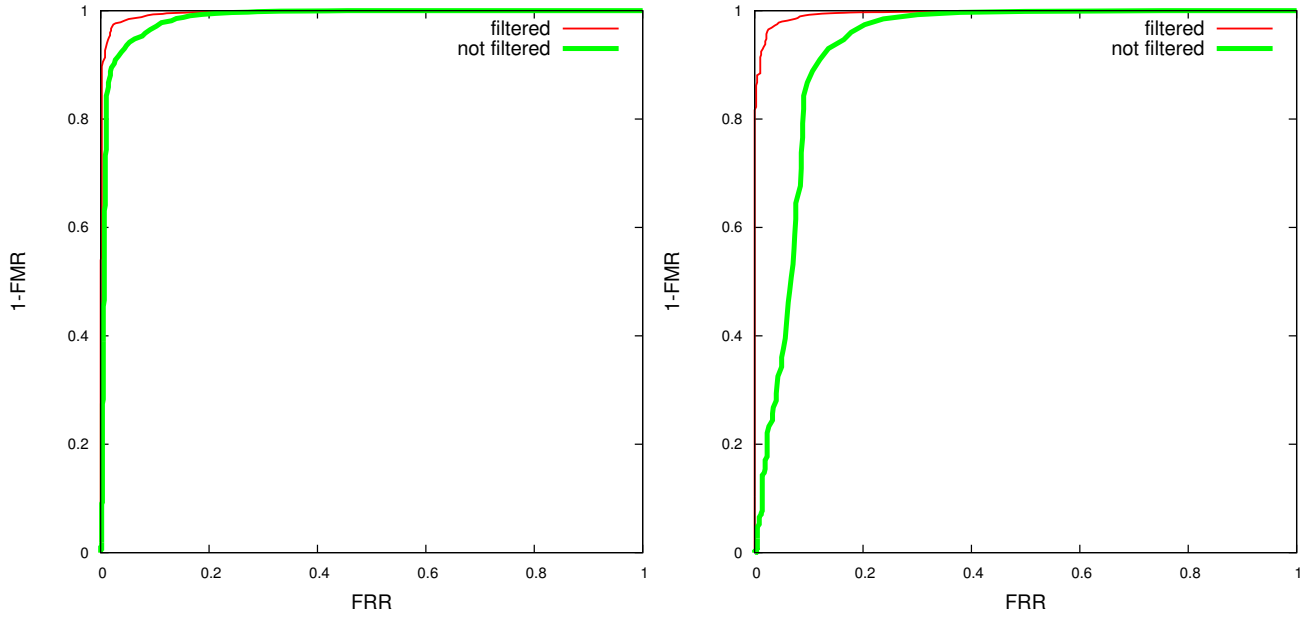
Metric	POCKET$_{mhv}$	WRIST$_{xyzm}$
AUC variation (%)	+1.2	+6.3
EER variation (%)	−3.7	−7.8

As previously stated, autocorrelation analysis is used to discard highly irregular gait segments that could potentially "confuse" the classifier. In terms of gait segments detected, the effect of the filter was negligible for the pocket traces (−5.2%), and more relevant for the wrist traces (−18%). However, in the latter case, most of the filtered gait segments were produced with repetitive hand movements and did not contain gait information.

The ROC analysis shown in Figure 5 clearly demonstrates that the effect of autocorrelation-based filtering was key to improve authentication performance. The first ROC curve, in Figure 5a, is related to the POCKET$_{mhv}$ approach, while the one in Figure 5b is related to the WRIST$_{xyzm}$ approach. In both cases, the AUC and EER metrics are significantly improved – numerical details are given in Table 4. However, the effect is much more visible in the wrist-based experiments. The reason is that, when the device is wrist-worn, spurious hand movements – like those produced by our volunteers at the end of their experiment – may mislead the walking detection technique.

5.4 Gait-based identification

As a corollary contribution, we here present the results related to identification. Differently from authentication, gait-based identification systems attempt to identify gait instances considering a predefined set of users who time-share the same device. Supervised classification can be used instead of anomaly detection, since a complete training set is



(a) POCKET$_{mhv}$ experiment. (b) WRIST$_{xyzm}$ experiment.

Figure 5: Effect of autocorrelation-based filtering on the ROC curve.

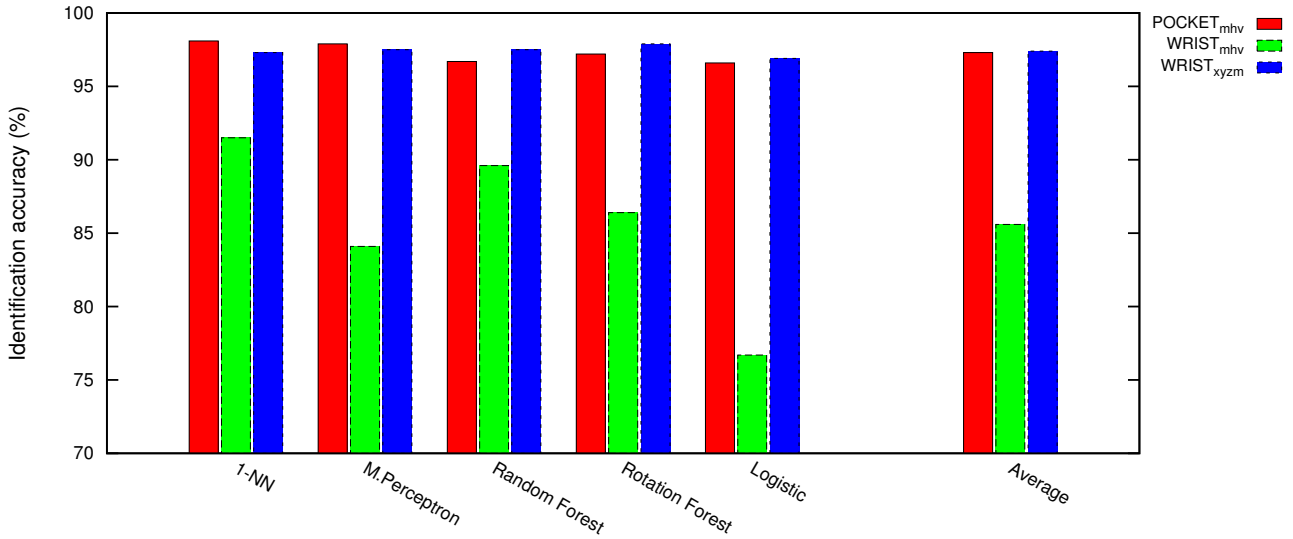


Figure 6: Identification accuracy (%) with different supervised classifiers.

available, with examples for all the users to be recognized. The histogram in Figure 6 shows the overall identification accuracy obtained by each approach with widely-used classification schemes and ten-fold cross-validation. Accuracy is defined as the ratio between the number of correctly identified gait instances and the total number of instances in the dataset.

The evaluated classifiers were Nearest-Neighbor, Multilayer Perceptron, Random Forest, Rotation Forest, and Multinomial Logistic. The average result among the different classifiers is also shown. The red, green, and blue bars show the performance of the POCKET$_{mhv}$, WRIST$_{mhv}$, and WRIST$_{xyz}$ approach, respectively. These results further confirm that – when the local reference frame is used – the wrist-worn device is capable of achieving similar results with respect to a pocket-worn device. Indeed, the average result obtained by POCKET$_{mhv}$ (97.3%) and WRIST$_{xyz}$ (97.4%) is almost identical.

6. CONCLUSIONS AND FUTURE WORK

Wrist-worn devices, like smartwatches and activity trackers, are increasingly adopted by the general public. We have presented an authentication method that uses a wrist-worn accelerometer to understand if the legitimate user, or someone else, is carrying the device. Performance evaluation on a set of volunteers demonstrated that authentication can be

performed with an Equal Error Rate as low as 2.9%.

Existing methods for gait-based authentication were designed for being executed on smartphones. As discussed in previous sections, a direct transposition of such methods on wrist-worn devices could be inadequate. With smartphones, assuming that the position and orientation of the device is always the same with respect to user's body is not possible. This implies that features have to be computed on a global reference system, so that the typical acceleration pattern is preserved if the user changes the position of the device or its orientation. Since smartwatches are always worn the same way, there is no need to compute selected features on a global reference system. In practice, the reference system of the device can be directly used, thus making implementation simpler.

Another major difference with respect to smartphones is the presence of spurious movements, which make detection and analysis of gait more complex. Hands are subject to a much larger amount of accelerations, if compared to parts of the body that are in proximity of the center of mass. Thus, a smartphone carried in a user's pocket is generally exposed to significantly less movements than a smartwatch. We found that the problems introduced by spurious movements can be greatly reduced by adopting autocorrelation-based filters in the walking detection technique. In particular, we found out that such filters reduce the EER by 7.8%.

The presented method deliberately uses information produced by a single sensor, the accelerometer. We decided not to use other sensors commonly available on smartwatches, such as gyroscopes or magnetic sensors, because the power consumption of the latter ones is significantly larger than the power consumption of an accelerometer (in some cases by an order of magnitude). An energy-demanding method would be of little practical use on the considered devices, which are operated through batteries with reduced capacity.

Future work will concern an evaluation of the method in uncontrolled environment. Another factor that deserves attention is the possibility of continuously training the system without increasing indefinitely the size of the training set. As new gait instances are collected, the system has to decide if they have to be included in the user's template, and if so which elements have to be removed.

Acknowledgments

This research was supported by the PRA 2016 project "Analisi di dati sensoriali: dai sensori tradizionali ai sensori sociali" ("Analysis of sensory data: from traditional sensors to social sensors"), funded by the University of Pisa.

7. REFERENCES

[1] S. Abbate, M. Avvenuti, F. Bonatesta, G. Cola, P. Corsini, and A. Vecchio. A smartphone-based fall detection system. *Pervasive and Mobile Computing*, 8(6):883 – 899, 2012.

[2] H. J. Ailisto, M. Lindholm, J. Mantyjarvi, E. Vildjiounaite, and S.-M. Makela. Identifying people from gait pattern with accelerometers. In *Proceedings of SPIE*, volume 5779, pages 7–14, 2005.

[3] 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 *Proceedings of the 11th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, pages 92–97, June 2014.

[4] L. Bianchi, D. Angelini, and F. Lacquaniti. Individual characteristics of human walking mechanics. *Pflügers Archiv*, 436(3):343–356, 1998.

[5] V. Chandola, A. Banerjee, and V. Kumar. Anomaly detection: A survey. *ACM computing surveys (CSUR)*, 41(3):15, 2009.

[6] G. Cola, M. Avvenuti, A. Vecchio, G. Z. Yang, and B. Lo. An on-node processing approach for anomaly detection in gait. *IEEE Sensors Journal*, 15(11):6640–6649, Nov 2015.

[7] G. Cola, M. Avvenuti, A. Vecchio, G.-Z. Yang, and B. Lo. An unsupervised approach for gait-based authentication. In *Proceedings of the 12th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, pages 1–6. IEEE, June 2015.

[8] G. Cola, A. Vecchio, and M. Avvenuti. Improving the performance of fall detection systems through walk recognition. *Journal of Ambient Intelligence and Humanized Computing*, 5(6):843–855, 2014.

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

[10] T. Fawcett. An introduction to ROC analysis. *Pattern recognition letters*, 27(8):861–874, 2006.

[11] D. Gafurov, E. Snekkenes, and P. Bours. Gait authentication and identification using wearable accelerometer sensor. In *Proceedings of the IEEE Workshop on Automatic Identification Advanced Technologies*, pages 220–225, June 2007.

[12] D. Gafurov, E. Snekkenes, and P. Bours. Improved gait recognition performance using cycle matching. In *Proceedings of the IEEE 24th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pages 836–841, April 2010.

[13] M. A. Hall and G. Holmes. Benchmarking attribute selection techniques for discrete class data mining. *IEEE Transactions on Knowledge and Data Engineering*, 15(6):1437–1447, 2003.

[14] A. H. Johnston and G. M. Weiss. Smartwatch-based biometric gait recognition. In *Proceedings of the IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–6, Sept 2015.

[15] 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*, 2012, 2012.

[16] J. Kwapisz, G. Weiss, and S. Moore. Cell phone-based biometric identification. In *Proceedings of the Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS)*, pages 1–7. IEEE, Sept 2010.

[17] B. Lo, S. Thiemjarus, A. Panousopoulou, and G.-Z.

Yang. Bioinspired design for body sensor networks [life sciences]. *IEEE Signal Processing Magazine*, 30(1):165–170, 2013.

[18] H. Lu, J. Huang, T. Saha, and L. Nachman. Unobtrusive gait verification for mobile phones. In *Proceedings of the 2014 ACM International Symposium on Wearable Computers*, pages 91–98, New York, NY, USA, 2014.

[19] D. Mizell. Using gravity to estimate accelerometer orientation. In *Proceedings of the IEEE International Symposium on Wearable Computing*, pages 252–253, 2003.

[20] R. Moe-Nilssen and J. L. Helbostad. Estimation of gait cycle characteristics by trunk accelerometry. *Journal of Biomechanics*, 37(1):121 – 126, 2004.

[21] 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*, 47(1):228 – 237, 2014.

[22] 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*, 9(1), 2012.

[23] Y. Ren, Y. Chen, M. C. Chuah, and J. Yang. User verification leveraging gait recognition for smartphone enabled mobile healthcare systems. *IEEE Transactions on Mobile Computing*, 14(9):1961–1974, Sept 2015.

[24] L. Rong, Z. Jianzhong, L. Ming, and H. Xiangfeng. A wearable acceleration sensor system for gait recognition. In *Proceedings of the 2nd IEEE Conference on Industrial Electronics and Applications*, pages 2654–2659, May 2007.

[25] Shimmer. http://www.shimmersensing.com, 2016.