Smartphone-Based Gait Recognition: From Authentication to Imitation

Muhammad Muaaz and René Mayrhofer

Abstract—This work evaluates the security strength of a smartphone-based gait recognition system against zero-effort and live minimal-effort impersonation attacks under realistic scenarios. For this purpose, we developed an Android application, which uses a smartphone-based accelerometer to capture gait data continuously in the background, but only when an individual walks. Later, it analyzes the recorded gait data and establishes the identity of an individual. At first, we tested the performance of this system against zero-effort attacks by using a dataset of 35 participants. Later, live impersonation attacks were performed by five professional actors who are specialized in mimicking body movements and body language. These attackers were paired with their physiologically close victims, and they were given live audio and visual feedback about their latest impersonation attempt during the whole experiment. No false positives under impersonation attacks, indicate that mimicry does not improve chances of attackers being accepted by our gait authentication system. In 29 percent of total impersonation attempts, when attackers walked like their chosen victim, they lost regularity between their steps which makes impersonation even harder for attackers.

Index Terms—Authentication, biometrics, mobile environments, security and privacy protection, sensors, time series analysis

1 Introduction

Smartphones offer a single-point-solution to access a wide variety of services, such as communication, entertainment, social networking, business, finance, travel, and many more. This has led smartphones to not only become an integral part of our daily lives, but also to store a multitude of sensitive information, e.g., bank details, personal or business related emails, pictures, etc. Authentication plays a vital role to protect this growing tide of sensitive information. For a long time knowledge based authentication mechanisms (e.g., PIN, password, and graphical pattern) have been widely employed to protect information in ubiquitous computing environments [2]. However, knowledge based authentication methods suffer from well known usability and security drawbacks [3]. For instance, users typically use their smartphones in frequent sessions of small intervals of time as compared to traditional desktop computers [4], [5], [6]. This not only increases the cognitive load on users in terms of remembering and recalling their login secrets, but also time consuming because users have to enter their secrets again and again. Therefore, a noticeable number of users usually do not activate these authentication methods or tend to use simple secrets [7]. Besides the usability drawbacks, these authentication methods are vulnerable to shoulder surfing [8], [9], smudging [10], [11], and social engineering attacks [12].

Biometrics can bridge the gap between security and usability within mobile environments. In the last couple of years, smartphone manufacturers have started to embed biometric sensors in their flagship smartphones. For instance, Samsung, Apple, Microsoft, Fujitsu and many others have integrated fingerprint sensors and iris scanners in their flagship devices. However, biometric modalities such as face, fingerprint, and iris require an explicit interaction before every authentication attempt, which makes them less convenient when devices are used more often. At the same time, along with the integration of dedicated hardware in smartphones for capturing biometric information, more biometric modalities have also emerged such as gait (automatically identifying or confirming the identity based on the walking style), keystroke dynamics (automatically identifying or confirming the identity based on the typing style on a keyboard), and touchalytics (automatically identifying or confirming the identity based on interaction with the touch screen). These biometric modalities utilize motion sensors, soft keyboards, and touch screens, respectively, to acquire behavioral biometric information and allow users to implicitly authenticate to smartphones or services based on the actions they would perform anyway. Further, fusion techniques like [13] can be designed to integrate authentication scores of different implicit biometrics over time. This would enable smartphones to determine that they are not only being used, but also carried by legitimate users.

Walking is a repeated task, by using accelerometers, human gait can be measured unobtrusively and continuously. This distinguishes gait from other biometric modalities as a more user-friendly authentication mechanism. Nowadays, smartphones have built-in accelerometers to detect changes in screen orientation. In 2009, researchers used smartphone-based accelerometers to identify and verify individuals from their gait. Studies using built-in accelerometers under

- *The authors are with the Josef Ressel Center for Secure Mobile Environments, University of Applied Sciences Upper Austria, Wels 4600, Austria, and the Institute of Networks and Security, Johannes Kepler University Linz, Linz 4040, Austria.*
  E-mail: muhammad.muaaz@fh-hagenberg.at, rene.mayrhofer@jku.at.

Manuscript received 26 Apr. 2016; revised 26 Jan. 2017; accepted 15 Mar. 2017. Date of publication 23 Mar. 2017; date of current version 29 Sept. 2017.
For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TMC.2017.2686855

controlled [14], [15], [16] and uncontrolled experimental setups [1], [17] have shown promising authentication results.

Despite offering a good compromise between security and usability, biometric systems are susceptible to numerous security threats. Attacks on biometric systems are specifically designed to compromise the integrity of an authentication process either by circumventing the security provided by the system or by deterring normal functioning of the system [18]. For biometrics, it is not adequate to only fulfill the property of uniqueness, but they also need to be robust against attacks. Since behavioral biometrics are based on the behavioral traits of an individual, this makes them more vulnerable to impersonation attacks compared to physiological biometrics. Moreover, it is difficult to pre-establish the sophistication level of an attack on the biometric system as it highly depends upon the resources available to the attacker, e.g., time, knowledge of the system and creativity of the attacker. Therefore, it is very important to ensure the robustness of the proposed biometric modality against fraudulent techniques.

This paper evaluates the security of gait against live impersonation attacks in the realm of smartphone-based accelerometers. The contribution of this study is not of algorithmic nature; to the best of our knowledge this is the first work to systematically focus on the security concerns of smartphone-based gait biometrics. There are various reasons why this research work picks up this topic and continues with impersonation attacks. As we know, accelerometers can be attached to different parts of the human body to collect gait data. Different human limbs (when moved while walking) possess different levels of discriminative power [19]. Therefore, it might be possible that gait related information collected from some place on the human body is less or more attack resistant compared to the others. Further, all previous studies [20], [21], [22] focused on impersonation attacks made on gait templates recorded from hip or waist movements. Therefore, those attack scenarios do not provide much help from a realistic point of view as most of the smartphone owners do not attach or place their smartphone to/on the hip or waist.

- We analyze live impersonation attacks on a smartphone-based gait authentication system under strong attack scenarios. For this, we employ sources of live visual and audio feedback and attackers who were trained in copying body motions. This helps attackers to improve their mimicking skills at run time, which is not covered in any previous study [20], [21], [22]. Thus, we argue that findings of our work will advance knowledge in the whole field.
- We implement our gait authentication system on Android and present an evaluation of real time active impersonation attacks against this system.
- With the help of data analysis concepts we attempt to find why gait mimicking is hard, if live feedback can improve impersonation skills of attackers, and estimate the security strength of the smartphone-based gait authentication.

At first, in Section 2, we give an overview of gait authentication approaches, security of biometric systems in general and gait in particular. Then we present our approach to continuous and implicit gait authentication on smartphones in Section 3. Evaluation of zero-effort attacks is given in Section 4. In Section 5 we explain our study design, selection of participants, instructions given to the participants, and the procedure of our experiment to study minimal-effort attacks. Section 6 presents results and discussion on these results. Section 7 concludes our work with future outlook.

2 Related Work

Gait is an individual's walking style. Back in 1967, Murray [26] found similarities in repeated trials of pelvic and thoracic rotations of the same individual and dissimilarities among different users. He concluded that considering movements of all limbs, gait is unique.

2.1 Gait Recognition

Gait recognition is a process of identifying or verifying individuals based on the way they walk. Gait recognition fall into three main categories: Machine Vision (MV) based, Floor Sensor (FS) based, and Wearable Sensor (WS) based [19]. In each category, different sensors are used to acquire gait data. For instance, in MV based approaches, different video recording cameras are used to capture gait. Similarly, Ground Reaction Force (GRF) measuring sensors are placed in or on the ground for FS based approaches, and in WS based approaches motion recording sensors (e.g., accelerometers, gyroscopes) are used. Later, different data processing and classification approaches are applied to identify or verify individuals. However, the first two (MV and FS) categories are not applicable to the scenario of gait authentication on smartphones.

Research on wearable sensor based approaches for gait recognition began in 2005. Researchers have used dedicated wearable sensors, such as accelerometers and gyroscopes to capture gait data [19], [25], [27]. Studies by Gafurov [19] show that different human limbs movements have different levels of uniqueness and universality. For instance, gait data recorded by attaching a dedicated accelerometer to the hip, the back of the waist, and an ankle resulted in Equal Error Rates (EERs) 7.5, 7.7, and 5 percent, respectively. In 2010, Derawi [25] reported an EER of 5.7 percent based on gait data collected from the waist. In 2011, Mjaaland [22] reported 6.2 percent EER based on the gait data acquired from the hip. Zhang et al. [28] reported 2.2 percent EER based on the combined gait data acquired from the left upper arm, right wrist, left thigh, right ankle, and pelvis. Most of the research using wearable sensors is based on the dedicated sensor hardware and its placements do not favor much for smartphone-based gait authentication under realistic scenarios. Nowadays, most of the smartphones have a built-in tri-axes accelerometers. Since 2009, smartphone-based gait authentication is an active research area, and Table 1 outlines studies in this domain. There exist some inherent challenges in wearable sensor based gait recognition such as sensor placement, inter-day performance, clothing, and shoes. In realistic environments such as smartphones placed inside the pockets of the trousers, these challenges even get worst. For instance, every smartphone owner does not place the smartphone in the pockets of their trousers. A survey [7] shows that 70 percent of males and 13 percent of females place their smartphones in one of their trousers front pockets. 1-2 percent of users wear a pouch at their waist to carry their mobile device. 60 percent of

TABLE 1
An Overview of Gait Studies Using Smartphone-Based Accelerometer Data

Study	Smartphone placement	Approach	Participants	Settings	Performance (EER%)	Available on mobile devices
Sprager [23]	waist	PCA & SVM	06	c	92.6% CCR	No
Frank [24]	trouser pocket	time delay embeddings	25	s	100% CCR	No
Kwapisz [16]	trouser pocket	time domain features Neural Nets, J48, KNN	05	s	100% CCR	No
Derawi [25]	waist	gait cycle estimation	60	m	20.1%	No
Nickel [14]	waist	HMM	48	m	FMR 10.29%, FNMR (10.42%)	No
Muaaz [1]	trouser pocket	gait cycle estimation	35	s,c	7.051%, 18.965%	Yes
Yu Zhong [17]	trouser pocket	gait dynamic images & GMM	51	s	3.89%	No

The best performance obtained for the basic settings is reported here. Settings: s = same-day, c = cross-day, and m = mixed-day. CCR indicates that the stated performance measure is the correct classification rate instead of EER. Available on mobile devices indicates if an application is available for mobile devices.

females place their mobile device in their handbags. The rest use their trousers back pockets, jackets pocket, or backpack to carry their smartphones.

Therefore, researchers must not only focus on the collectability of gait data but also on the discriminative power of gait data collected from various positions. Moreover, authentication systems on smartphones should not take a long time to decide if an individual is a genuine or an impostor. Most of the studies outlined in Table 1 used ideal data sets, such as wearing the same shoes and cloths, except [1] where participants were only asked to place the phone inside the pocket of sufficiently tight trousers so to reduce noisy measurements recorded by the smartphone wobbling excessively inside the pockets.

2.2 Attacks on Biometrics

Biometric systems are vulnerable to different types of attacks (e.g., impersonation, replay, spoofing, and hill climbing) [29] that can compromise the security provided by the system, thus resulting in a system failure. These attacks can be grouped in two basic types [30]:

- *Zero-effort or passive attacks*: This means that the biometric template of an attacker may be sufficiently similar to a genuinely enrolled user, resulting in a False Match (FM). The event of FM is directly related to the uniqueness property of a biometric modality. Biometrics modalities such as fingerprints and iris are less vulnerable to zero-effort attacks compared to face, voice, or other behavioral biometric traits.
- *Adversary or active attacks*: This means that an attacker manages to successfully impersonate an enrolled individual. The sophistication level of an adversary attack highly depends upon the resources at an attacker's disposal such as physical or digital artifacts, time, and knowledge about the victim and the biometric system.

To understand threats against a biometric system, it is valuable to look at the possible attack points described in the following section.

2.2.1 Vulnerable Points and Their Consequences in a Generic Biometric System

Bolle et al. [29] identified typical attack points in a generic biometric system as depicted in Fig. 1, which are explained in this section.

At point 1 attackers can perform two different types of attacks, namely: *coercive*, and *imitation* attacks. In a coercive attack, legitimate biometric samples are presented in some unauthorized fashion. Whereas in an imitation attack, an unauthorized individual presents impersonation attempts to the biometric sensor [21], [22], [31]). If point 2 (the channel between sensor and feature extraction module) is

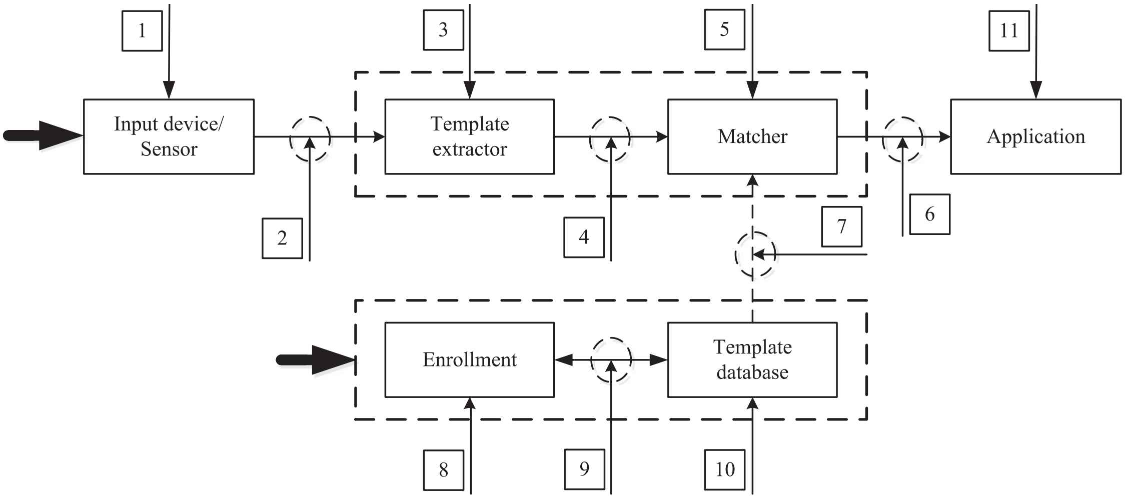


Fig. 1. Possible vulnerable points in a generic biometric authentication system, adapted from [29].

compromised as shown in [32], then attackers can launch a replay attack or alter the submitted biometric sample. Vulnerabilities at point 3 may help attackers to produce predetermined feature sets. Attacks at point 4 could be an attempt to replace legitimate features with synthetic features. Vulnerabilities at point 5 might help attackers to always produce their own-desired results that might lead to denial of service or illegal access to the system. Whereas a compromised channel (point 6) between matcher and application would allow attackers to change authentication results on the fly, thus defying the overall purpose of a biometric system. By attacking the channel between the template database and the matcher at point 7, attackers could intercept and manipulate templates before they reach the matcher. In biometric systems, both enrollment and authentication processes are quite similar, therefore enrollment is also vulnerable at points 1-6 and control over the channel between enrollment and the template database might allow attackers to override biometric templates. A successful attack on the template database may compromise confidentiality, integrity, availability, and privacy of users enrolled in the system. Point 11 indicates that applications could also be attacked, therefore, appropriate security mechanisms must be placed in the application as well.

2.2.2 Impersonation Attacks on Biometric Gait

Attacks on biometric systems can be designed to exploit vulnerabilities that are present in specific modules and in the channels connecting these modules. Most of these communication channels and modules shown in Fig. 1 can be protected by incorporating well-established information and communication security principles, such as using secure channels between different modules of the system. In biometric systems, impersonation attacks are usually more common for multiple reasons. First, input devices or sensors are available to all users (irrespective of genuine or impostors); therefore, attackers might misuse them. Second, attackers do not need to know the architecture or the internals of the system. Therefore, impersonation attacks on gait have been studied in previous works.

For instance, Stang [20] performed an experiment with 13 participants to explore whether it is easy or difficult to learn to walk like someone else. Every participant performed 15 impersonation attempts on pre-recorded walking data, and each attempt lasted for five seconds. A wearable accelerometer was attached to the hip of participants. The impostors were given a short description of the gait they were targeting, and they were given feedback by displaying dynamic graphs of the attacker's walk data overlaid on the victim's walk data. In this study, the author did not create gait templates, but compared complete five seconds raw walk data from a victim and an attacker using *Pearson's product moment correlation coefficient* [33]. Stang employed linear regression to find out how the correlation scores improve over the course of the first to the last attempt. Stang found that improvements were present and concluded that it is easy to copy other's hip movements.

Gafurov et al. [21] conducted two experiments. At first, they recorded gait data by attaching a dedicated accelerometer to the hip of the participants. The focus of the first experiment (named *"friendly scenario"*, involving 100 subjects) was to determine the performance of their system, resulted in 13 percent EER and 73.2 percent recognition rate. They used the results of this experiment as a baseline in their second experiment. In their second experiment they created 45 pairs from 90 participants based on *"friendness" (victim and attacker of every pair know each other)*. Subjects in every pair made four impersonation attempts on each other. They found that the performance of their system (when attackers mimic their victims) was not worse than the baseline results. Based on this observation, they concluded that minimal-effort mimicry of gait may not help to increase chances of impostors being accepted.

Both Stang's [20] and Gafurov's [21] conclusions oppose each other. Their studies are based on completely different data sets, experimental designs, and data analysis methods. Mjalaand et al. [22] have presented a detailed critique on both works. For instance, Stang's work does not present any valid statistical tests made on the data (e.g., confidence intervals or measure of goodness of fit). Correlation is used to determine the strength of association between the victim's and attacker's walk data. Even if an attacker only manages to synchronize steps with the victim, this would result in high correlation. However, Gafurov's work on the other hand suffers from a small number of imitation attempts.

Mjalaand et al. [22] extended Gafurov's work. They conducted an experiment involving 50 participants in three scenarios: *friendly, short-term hostile, and long-term hostile*. The friendly scenario (to determine the baseline performance of their system) resulted in an EER of 6.2 percent. In the short-term hostile scenario, seven participants contributed. These participants were selected based on a small distance between their gait templates. One out of these seven participants was selected as a victim and one-by-one the remaining six participants attempted to imitate the victim. These attackers were trained for two weeks and they were shown videos of victim's walking styles. The Dynamic Time Warping (DTW) distance metric was used to compare victim's and attacker's gait templates. In the long-term hostile scenario only one attacker participated. This attacker was trained for six weeks in the same way as other attackers did in the short-term hostile scenario. The authors concluded that participants did not show any significant improvement in terms of learning the victim's walking behavior. From both hostile scenarios, the authors concluded that long term training of the attackers did not improve their ability of learning victim's walking style.

None of these studies [20], [21], [22] employed live sources of feedback when an attack was really happening. This can additionally inform attackers about their impersonation attempts and give them a live chance to improve their next mimicking attempt. Looking at videos or walk data graphs obscures many details about the target, for instance stride length, real walking pace of the victim, 360 degree view of hip movements, articulation of the target's body, etc. Further, these studies do not mention if the attackers were given time to walk along with their targets to realistically get more familiar about their victims walking styles.

3 Our Approach to Continuous Gait Authentication on Smartphones

Like a conventional biometric system, our approach to gait authentication on smartphones also consists of two parts, namely: enrollment and verification subsystems. These

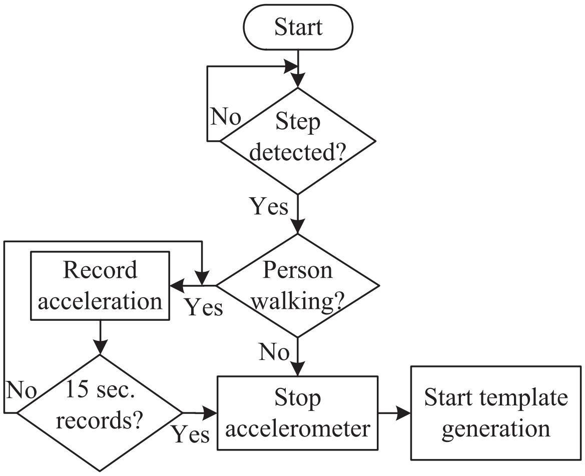


Fig. 2. The data acquisition process in the verification phase based on sensor events.

subsystems employ the same technique to generate gait templates for the enrollment and verification purposes. For enrollment, a user manually starts data recording, then places the smartphone inside the front pocket of the trouser and walks for two to three minutes, and afterwards, takes the device out of the pocket and stops data recording.

Once the enrollment process is successfully finished, a user can start continuous verification. It is important to note that for the verification phase, the smartphone must be placed in the same pocket which was used in enrollment phase—placing the smartphone in a different pocket might worsen authentication performance due to asymmetry in leg muscles strength [34]. Fig. 2 summarizes the data acquisition process during the continuous verification phase. In this phase, two sensors, namely (virtual) pedometer and accelerometer are used. As we know, gait authentication can be performed when a user is walking. Therefore, instead of keeping accelerometer active all the time, we use a pedometer to detect whether a user is walking or not. A (virtual) pedometer is a low powered sensor, allowing to continuously run without draining the battery. On the other hand, collecting data from an accelerometer of an Android device in the background requires a partial wake lock which keeps the central processing unit (CPU) of the device in running state. This significantly affects battery life of the device. Thus, the step detector saves battery life by acting as a trigger for the accelerometer. Upon detecting a step, it triggers the accelerometer to start recording data. It also triggers to stop recording gait data when the user stops walking. This is done by monitoring the timestamps of the pedometer events. A user is assumed to be walking if the time elapsed between two consecutive steps is less than a threshold α (see Table 3), otherwise the user has stopped walking. During our experiments, we found that when users were walking at their normal pace, they take consecutive steps within the range of 0.5-0.8 seconds.

TABLE 2
Average of Three Trials of Battery Consumption at Different Battery Levels (When a User is Continuously Walking)

Time	Battery level				
Initial battery level	100%	80%	60%	40%	20%
After 15 minutes	98%	78%	57%	37%	17%
After 30 minutes	96%	75%	54%	34%	14%

TABLE 3
Thresholds Used in This Approach and Study

Threshold	Description	Value
α	Step detection	800 ms
β	Variance for active segments	$0.8\ (\mathrm{m/s^2})^2$
γ	Outliers removal (DTW dist.)	0.6
ϕ	Gait cycle matching (DTW dist.)	0.4

If a user is continuously walking, then we stop recording gait data after 15 seconds. The gait template generation is started in the background and immediately starts recording gait data. The decision of choosing 15 seconds of gait epochs is inspired of previous studies where 20-30 meters of walks were used for gait recognition [35], [36], and 20 meters can be covered in 15 seconds, at a normal walking speed.

In order to estimate battery consumption, it is important to find out how many steps individuals take on daily bases. A study shows that Americans, Japanese, Western Australians, Belgian, and Swiss people approximately on average accumulate, 5,100, 7,200, 9,600, 9,600, and 9,650 steps/day, respectively [37]. In [38], [39] researchers recommended 10,000 steps/day for cardiovascular health, which is approximately equal to 7.6 kilometers and can be covered approximately in 1 hour and 40 minutes at a normal walking speed. Therefore, we tested battery consumption (at different battery levels (see Table 2), because battery drain is not linear) of our gait authentication application and we estimate that it would approximately consume 13-20 percent of battery for 10,000 steps/day. Moreover, when a smartphone is lying on the table the battery drain of our application is negligible, approximately 1 percent in 45 minutes. A Sony Xperia Z5-Compact smartphone was used to estimate the battery consumption of our smartphone-based gait authentication application. In the following sections we will briefly describe our template generation process.

3.1 Mean Normalization and Active Walk Segment Detection

Accelerometers are very sensitive to noise; even when a smartphone is in a steady state, acceleration measured along any axis is not stable over the time. For instance, when the smartphone is in stable state, the squared sum of acceleration values of all three axis should be equal to the earth gravitational force ($9.81\frac{m}{s^2}$), but in practice this is not the case. Therefore, in the first step, recorded walk data is mean normalized. First, a mean acceleration value is computed for every axis from the acceleration data along that axis. Then, from the acceleration data along every axis its respective mean value μ is subtracted as shown as

$$a'_i(t) = a_i(t) - \mu_i, \qquad i \in (x, y, z) \text{ axis} \tag{1}$$

$$A(t) = \sqrt{a_x^2(t) + a_y^2(t) + a_z^2(t)}, \qquad t = 1, 2, 3, \ldots, k. \tag{2}$$

Then the process of extracting active walk segments begins. We define active segments as those sections of the recorded data when a user was walking. This is done by monitoring

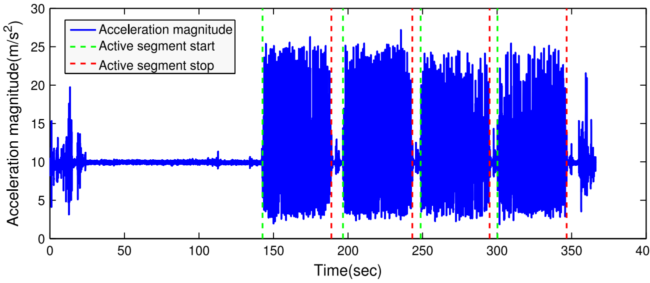


Fig. 3. Detected four walk segments in enrollment phase.

the variance of the acceleration magnitude (see Equation (2)) of the tri-axes accelerometer in a sliding window, as stated in [11]. For our evaluation and implementation, we use a sliding window of two seconds. When the variance of acceleration magnitude rises above or drops below a threshold β (see Table 3) this marks the start and the end of an active walk segment as shown in Fig. 3. A grid search was performed on the recorded gait data to find an appropriate value of β.

3.2 Data Processing

3.2.1 Interpolation

The accelerometer API of Android smartphones does not output acceleration data in equidistant intervals of time. It only outputs data when the onSensorChanged[1] method is triggered. This means the data does not have a fixed sampling rate. A fixed sampling rate is achieved by applying linear interpolation

$$A' = A_0 + \frac{(A_1 - A_0)(t' - t_0)}{t_1 - t_0}. \tag{3}$$

3.2.2 Noise Removal

A Savitzky-Golay smoothing filter [40], also called least-square smoothing filter is used to remove random noise from the data. We preferred this filter over the typical moving average filters, because least-square smoothing not only reduces noise but also maintains the shape and height of waveform peaks. The basic idea behind this filter is to find a least-square fit with a polynomial of high degree for each data point, over an odd sized window centered around that data point.

3.3 Template Extraction

Human gait exhibits a cyclic pattern, and therefore measured acceleration is also periodic. The first step in the gait template generation process is to estimate the gait cycle length.

3.3.1 Gait Cycle Length Estimation

We begin by extracting a small subset of samples (reference, see Fig. 4) from the center of the walk as it is the most stable section of the walk because few cycles in the beginning and ending of the walk may not adequately present the person's gait [41], [42]. Then we compare this reference subset with the other subsets (of similar length) extracted from the same walk by moving one sample forward, towards the end of the walk as shown in Fig. 4. Selecting too few samples for the reference subset will not reflect periodicity in the walk. Similarly, selecting too many samples for the reference subset will reduce the number of comparisons. From our experiments we found that a reference window size equal to the sampling frequency not only reflects periodicity in the data, but also give enough comparisons to estimate the gait cycle length. Comparing the reference subset with subsets extracted from the walk results in a distance vector as shown in Fig. 5. From this vector we find the indices of minima and store them in a minimum index vector. Later, we compute a difference vector which contains the difference of every two adjacent elements of the minimum index vector. Finally, the cycle length is computed by taking the mode of the difference vector.

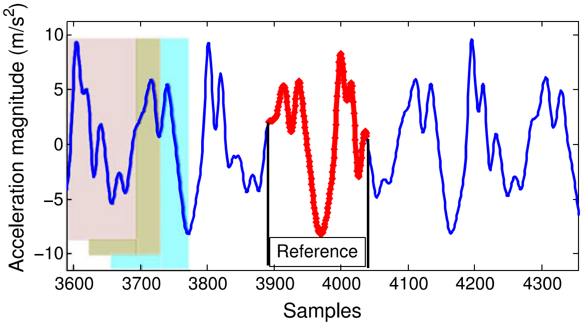


Fig. 4. Estimating the gait cycle length.

In those cases where mode does not exist (which means every step has different length, e.g., if an individual is intentionally changing the walking pace) cycle length is computed by averaging the values of the difference vector.

3.3.2 Gait Cycle Detection

Gait cycle detection starts by extracting a small segment (two times the estimated cycle length) from the center of the walk. Then we detect local minima in this extracted section of the walk. Sometimes interpolation errors could affect this area of the walk and we might detect a wrong minimum. To reduce this risk we use a segment size of double the cycle length. By doing so, we aim to pick two minimum values and we start cycle detection from the index of the most prominent minimum. From the index of this minimum point cycle detection is done in a forward and backward direction by adding and subtracting the cycle length. From our experiments we found that minima in the walk usually do not occur at equal intervals of gait cycle length. Therefore, we add and subtract a small offset value (0.2 times the estimated cycle length) to the index of the newly found end point and search for a local minimum in that region as shown in Fig. 6. Once all minima

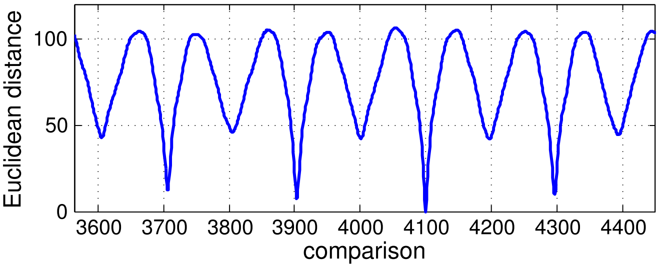


Fig. 5. Estimating gait cycle length from detected minimas.

[1] Androids sensor event listener: goo.gl/XeSMdI

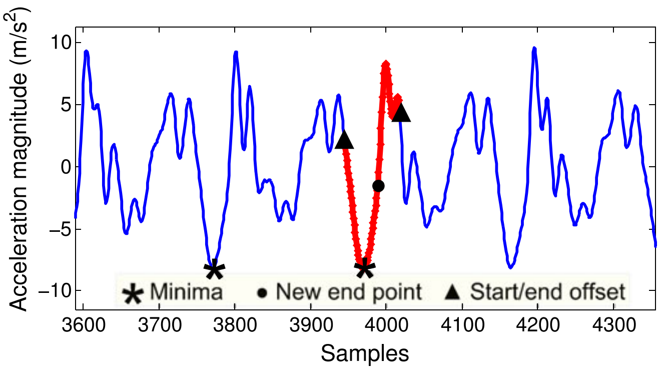


Fig. 6. Estimating the start of a gait cycle.

in both directions are found, the walk is segmented from the indices of these minima. Then all detected gait cycles are normalized to an equal length.

3.3.3 Removing Outliers

Detected cycles are cleaned by deleting unusual cycles. These outliers may occur, e.g., if a person has stumbled while walking. To remove outliers pairwise distances are computed between all detected cycles using DTW. This results in a matrix $D_{n\times n}$, where n is the number of detected cycles. If $A = (a_1, a_2, a_3, \ldots, a_n)$ and $B = (b_1, b_2, b_3, \ldots, b_n)$ are two gait cycles then $DTW(A, A) = 0$ and $DTW(A, B) = DTW(B, A)$

if $D_{n\times n} = (d_{ij})$;

$$d_{ij} = 0, \qquad \text{if } i = j, \qquad 1 \le i, j \le n. \tag{4}$$

$$d_{ij} = d_{ji}, \qquad \text{if } i \ne j, \qquad 1 \le i, j \le n. \tag{5}$$

Here, Equations (4) and (5) imply that only lower or upper triangular elements of the matrix D are computed. Finally, those cycles which have 50 percent of their pairwise distances greater than a threshold γ (see Table 3) are removed. Remaining cycles as shown in Fig. 7 represent the gait template of an individual.

3.3.4 Gait Decision Module

To measure similarity, all gait cycles of a live template (generated in the verification phase) are compared against all gait cycles of an enrolled template, by using DTW. A lower DTW distance between two gait cycles indicates a higher similarity between the compared cycles. Then these pairwise distances are passed to a majority voting module, which returns a confidence score (fraction of pairwise DTW distances below the gait cycle matching threshold ϕ). This value ϕ (see Table 3 is a trade-off between usability and security, and chosen from the distributions of genuine and impostor DTW distances. A positive decision is made if an authentication attempt obtains a 50 percent confidence score.

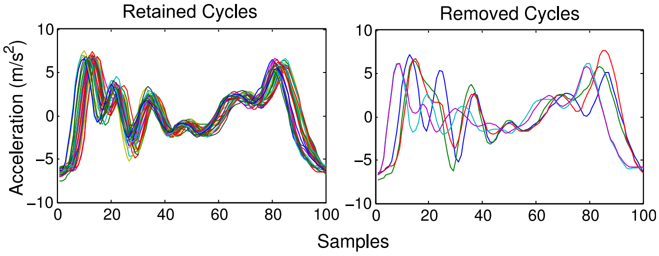


Fig. 7. Example of an extracted gait template.

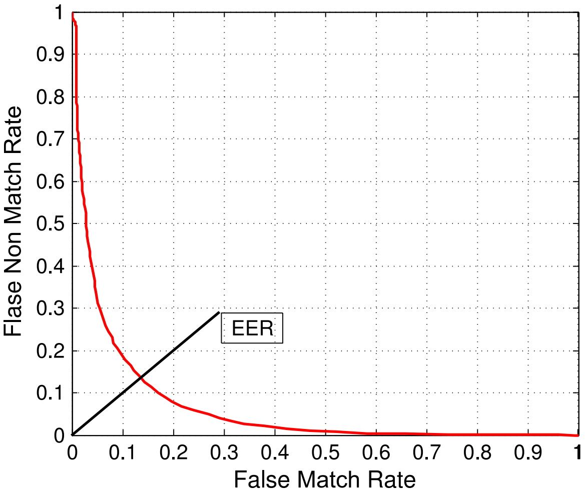


Fig. 8. Performance of our method in terms of DET.

4 Evaluation of Zero-Effort Attack Scenario on Our Authentication System

We have used a gait dataset of 35 participants to evaluate the performance of our gait authentication approach against *zero-effort* attacks. This dataset was recorded by placing the smartphone inside the front left pocket of the trousers and participants were asked to walk (two rounds of a 68 meters long corridor) at their normal walking speed. Details about our data collection process can be found in [1]. The approach given in Section 3 was used for data processing and generating gait templates. The detection error tradeoff (DET) curve (see Fig. 8) shows the performance based on the false match rate (FMR) and false non match rate (FNMR) errors of our system. With this approach, we achieved an EER of 13 percent. The EER is a point where $\text{FMR} = \text{FNMR}$.

5 User Study: Live Impersonation Attacks on Our Authentication System

Gait as a biometric, is an identifier of an individual, but it is not a secret. For instance, an attacker can stalk a victim to learn that victim's walking style. Feeling confident after learning the victim's gait, an attacker may steal the victim's smartphone and try to imitate the victim's gait to get access to the data stored inside the smartphone. To evaluate the resistance of our gait authentication system against this type of attack, we design an active impersonation attack scenario.

5.1 Design

Our impersonation attack scenario consists of two phases: the reenact phase and the coincide phase. A minimal-effort impersonation attack is carried out in the reenact phase. Our definition of a *minimal-effort* attack is where attackers have common knowledge of the system, such as placement of the smartphone in the victim's trouser pocket, clothing of the victim, type of shoes the victim is wearing, limited time (approximately 10 minutes) to observe and rehearse the

TABLE 4
Intra-Pair Absolute Difference and Inter-Pair Mean of the Absolute Difference of Age, Weight, and Other Physical Characteristics, Where U-Leg and L-Leg Indicate Upper and Lower Leg Lengths

Pair	Age (yr)	Weight (kg)	Height (cm)	Shoe size (EU)	U-leg (cm)	L-leg (cm)
1	4	2	4	0	1	2
2	6	3	7	1	4	5
3	5	8	5	2	2	3
4	5	4	3	2	4	4
5	8	3	8	3	2	3
Mean	5.6	4.0	5.4	1.6	2.6	3.4

victims gait by walking next to the victim, and then try to emulate victim's gait.

In the coincide phase, we extend our minimal-effort attack one step further and match victim's and attacker's live templates on the attacker's smartphone in real time while they are walking side by side and give feedback to the attacker about the latest impersonation attempt.

5.1.1 Participants Selection

A total of five attackers (two females and three males) and four victims (two females and two males) participated in this study. Participants who played the role of attackers are acting students at the Anton Bruckner Private University for Music, Drama, and Dance. They are trained as mime artists, specialized in mimicking body motions and body language, whereas participants in the victim group are normal smartphone users. Once attackers were fixed for this study, we started the search for suitable subjects as victims. From the pool of available victims, only four victims were recruited who were close to at least one of the attackers on the basis of their physical characteristics such as age, weight, height, shoe size, upper leg length, and lower leg length. Then each victim was paired with one attacker based on their physical characteristics, except one victim who was a good match for two attackers. We chose five pairs, each of the same gender and none of them knowing each other before the experiment. Further, each pair (victim and attacker) stood in front of an expert mime artist, who observed whether a victim and an attacker were a good match; otherwise the attacker was paired with a new person from the pool of the remaining victims. Table 4 shows the intra-pair absolute difference and inter-pair mean of the absolute difference of age, weight, height, shoe size, upper leg length, and lower leg length between the attacker and the victim who were finally selected for each pair. Upper leg length was measured from the edge of the ilium to the knee joint and lower leg was measured from the knee joint to the floor while the person was sitting in a posture so that the femur bone was parallel to the ground and at 90 degree with the tibia (shin-bone) as shown in Fig. 10.

5.1.2 Instructions to the Participants

Every participant was asked to wear a pair of tight jeans with at least one frontal pocket on the left side and a pair of shoes with flat soles. This type of outfit was chosen to minimize the factors that could influence the study, e.g., variance in cloths and shoes. In this study, victims had a simple role to place a smartphone in their front left trouser pocket and walk at their normal pace as they walk in their routine life. Attackers who were also wearing a similar outfit to the victims were instructed by a mime expert, specialized in mimicking body motions body language. Attackers were asked to focus on the following aspects while observing their victims:

- walking speed and the victim's stride length;
- dynamics of the victim's walking style along with a feeling of the victim's relation to their own weight (lightness or the heaviness of the walk);
- articulation of the victim's body while walking, such as posture, movements of the arms, position of the feet with their relation to the floor, openness or closeness of the feet, how heel strikes the floor and toes leave the floor; and
- movements of the pelvis (e.g., rotation, inclination, translation, and the combination of all), because it is close to the target area where the smartphone is placed inside the pocket.

Further, all participants were informed that in an event of successful match smartphone would vibrate and play a signature sound as a feedback. When our gait authentication application is running in verification mode, it records 15 seconds of acceleration data and produces authentication results in the next three seconds while continuously recording gait data of the following 15 seconds in parallel.

5.2 Procedure

For our experiments we have used one Sony Xperia Z3 and two Sony Xperia Z5-Compact smartphones. Each of these smartphones has a built-in tri-axes accelerometer, which has a range from $-2g$ to $+2g$ and was set to sample acceleration values at 200 Hz. The only reason for using three smartphones was to conduct our study in parallel. Our gait authentication application was installed on all devices and produced two types of logs: event log and data specific log. The event log contains all events of the enrollment and the verification phase with their results and timestamps. The data specific log contains log files of raw data, processed data, and generated gait templates.

5.2.1 Reenact Phase

Before starting with impersonation attacks, we recorded gait templates of our victims. To record a template, victims were asked to place a smartphone inside the front left pocket of their trouser (see Fig. 9a) and complete two rounds of a 16 meters long corridor (see Fig. 9b) at a normal walking speed, while the respective attacker was asked to observe the victim's phone placement and walking style. The template recording session for each victim lasted approximately three to four minutes. Once the enrollment stage was finished, each victim was again given the same smartphone that was used for this victim's template generation. The victim placed that smartphone inside the pocket and walked in the corridor for at least five minutes. This time, the respective attacker was given freedom to apply given instructions (see Section 5.1.2) and own imitation skills to learn the victim's gait as shown in Figs. 9c and 9d. After the rehearsal period was over, the smartphone was

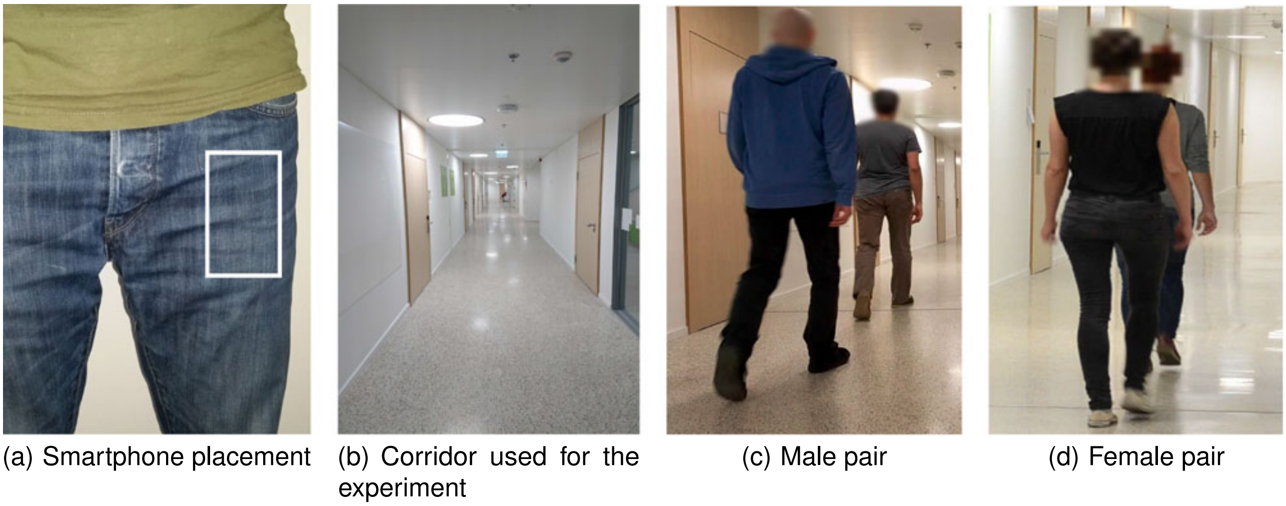

(a) Smartphone placement (b) Corridor used for the experiment (c) Male pair (d) Female pair

Fig. 9. (a) Phone placement inside the trousers pocket, and (b) the venue for experiments. In (c) and (d), the male and the female attacker rehearsing their victim's gait, where attackers are just behind their respective victims.

handed over to the attacker, who then tried to reproduce a walk similar to the respective victim for the next 10 minutes.

5.2.2 *Coincide Phase*

The coincide phase was conducted exactly a week after the reenact phase. This phase was specifically designed to analyze if synchronization of steps and other body movements really help attackers to learn a victim's gait. In this phase, a victim and an attacker walk side by side (see Fig. 11). Victims were asked to walk at their normal pace, ignoring the fact that someone is walking with them. People walking side by side normally tend to adapt each others walking pace, which could significantly change gait cycle lengths and other walk characteristics [43]. For this phase, only two Sony Xperia Z5-Compact smartphones were used for all pairs. These smartphones were connected to each other over a Bluetooth channel. Our gait authentication application was running in verification mode on both smartphones. Victim and attacker placed their smartphones inside the front left pocket of their trousers and walked for 15 minutes. In this phase, live templates from the victim's smartphone were transferred in real time to the attacker's smartphone and compared against the attacker's live template. After comparing the templates, the smartphone inside the attacker's pocket emitted one of the audio feedbacks (given in Table 5 based on the similarity score) about the recently completed 15 seconds walk.

6 Results and Discussion

6.1 Results from the Reenact Phase

Each attacker attempted to emulate their respective victim's gait. Note that each authentication attempt results in a gait template that contains multiple gait cycles based on an individual's natural walking speed. These gait cycles are cross compared against the enrolled gait template using DTW as a distance metric. For a successful authentication attempt, 50 percent of these DTW distances must be below a threshold ϕ (see Table 3). Fig. 12 shows the distributions of DTW distances for all (genuine and impersonation) attempts, without applying the majority voting. Fig. 13 shows the confidence scores of each authentication attempt made by a victim and an attacker. As we can see in Fig. 13, none of the attackers actually managed to achieve a confidence score to mark that attacker as a genuine user. For most of the

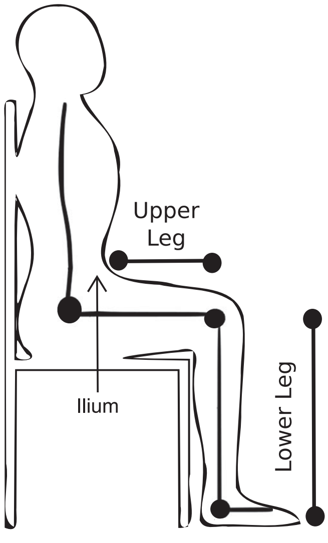


Fig. 10. Posture while measuring upper and lower leg lengths.

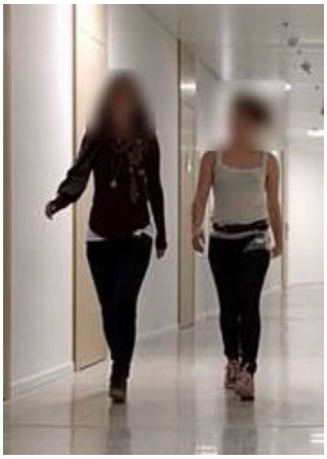


Fig. 11. Victim and attacker walking side by side in coincide phase.

TABLE 5
Confidence-Score-Based Feedback

Confidence score (1-100)	Feedback
$Score \leq 20$	Very bad
$20 < Score \leq 40$	Bad
$40 < Score < 50$	Close
$50 \leq Score \leq 60$	Good
$60 < Score \leq 100$	Very good

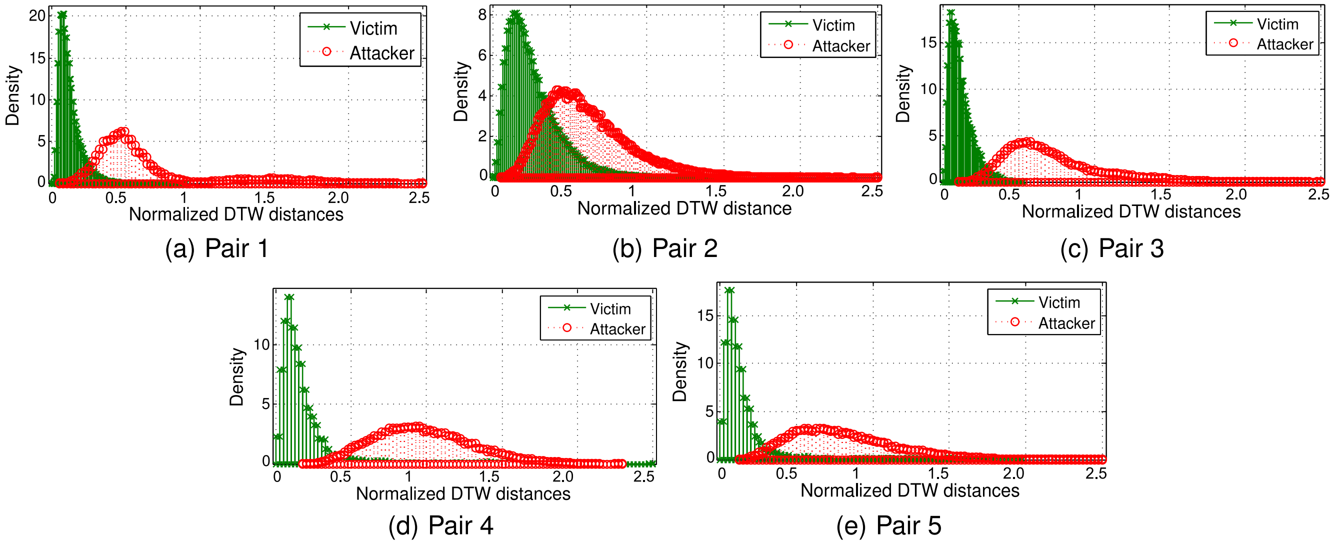
attackers, the confidence score stayed at 0 percent (except the attacker of pair 2 who obtained a maximum confidence score of 25 percent, which is still 50 percent below the threshold line). Surprisingly, the confidence scores of attackers of pair one and three to five stayed at 0 percent. This could only happen in two cases: either all of the gait cycles in an attackers template have DTW distances above the gait cycle matching threshold ϕ or the outliers removal module (see Section 3.3.3) has removed all detected gait cycles. Our event log files reveal that in 73 percent attempts, attackers template failed to match with enrolled templates and in the remaining 27 percent attempts the outliers removal module has removed all gait cycles. This not only indicates resistance of gait as a biometric against active impersonation attempts but also answers why it is hard to imitate someone's gait. Because with every step that an attacker takes, they try to improvise it, making gait cycles irregular enough to be removed by the outliers removal module.

6.2 Results from the Coincide Phase

The coincide phase was particularly designed to study to what extent an attacker can learn a victim's gait by walking side-by-side. Therefore, in this case, an attacker's and a victim's gait cycles are extracted from 15 seconds walk and cross compared using DTW as a distance metric. Then we compute the percentage of pairwise distances below the gait cycle matching threshold ϕ. If an attacker achieves 50 percent as a confidence score, then we cross compare that particular attempt with the victim's enrolled template to verify if in that particular attempt the attacker has managed to mimic the victim's gait. Results indicate three out of five attackers again did not manage to imitate their respective victims. Their scores stay at 0 percent; in 60 percent of the attempts made by these three attackers, templates did not match with their corresponding victim's template and in 40 percent of the attempts, the outliers removal module removed all of the gait cycles due to uneven walking style, as we have discussed in the previous section. Two of the attackers did manage to emulate their victims gait as shown in Figs. 14a and 14b. The attacker in pair 1 (see Fig. 14a) has achieved a maximum confidence score of 40 percent, which is still not good enough to be matched against the enrolled templates (with a set matching threshold of 50 percent). Whereas, attacker two (see Fig. 14b) has achieved a 52.3 percent confidence score in one impersonation attempt. To check if this impersonation attempt could be a threat to our authentication system we cross compared attacker's and victim's templates (produced in coincide phase) with the victims enrolled template. For this particular attempt, the victim and attacker have achieved confidence scores of 79.69 and 29.98 percent, respectively. Fig. 15 indicates that when the victim was achieving high confidence scores, the attacker had no chance to imitate the victim, but with the drop in the victims confidence scores, the attacker was able to mimic the victim to some extent. A possible reason could be that in the beginning the victim was focused; slowly, as the time passed, the victim's gait might have changed because when people walk side by side they tend to deviate from their natural gait. Despite being able to obtain a 52.3 percent confidence score in the 12th impersonation attempt, the attacker was not able to reproduce this high score for the rest of the experiment, which could be compared against the enrolled template of the victim.

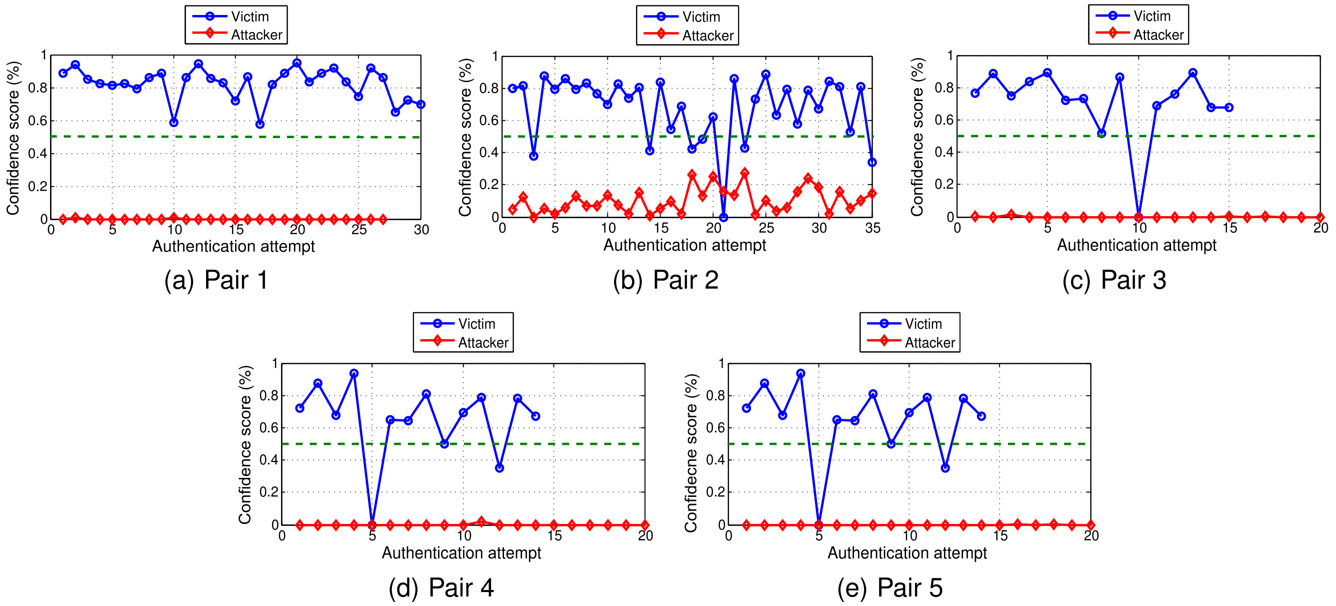
6.3 Security Strength of Gait Authentication

The results of our experiments (reenact and coincide) show that minimal-effort impersonation along with training and feedback does not improve chances of an impostor/attacker being accepted by the system. However, other behavioral



(a) Pair 1 (b) Pair 2 (c) Pair 3 (d) Pair 4 (e) Pair 5

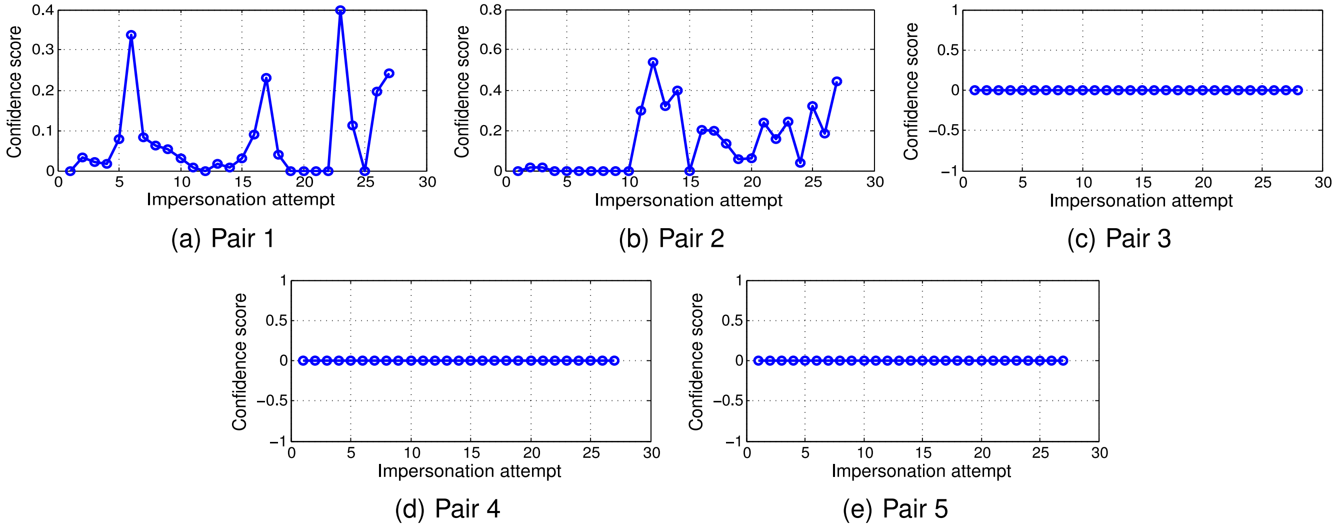
Fig. 12. Pairwise distributions of victim's and attacker's DTW distances to their corresponding enrolled template in all impersonation attempts. Overlapping areas only reflect that some gait cycles from all impersonation attempts have obtained DTW scores closer to the victim's DTW scores.



(a) Pair 1 (b) Pair 2 (c) Pair 3

(d) Pair 4 (e) Pair 5

Fig. 13. Genuine and impostor confidence scores of every pair for each impersonation attempt. The dashed line indicates the majority voting threshold. This means that at least 50 percent of pairwise DTW distances (when gait cycles of live template are compared with the enrolled template) are below the gait cycle matching threshold ϕ. Victims confidence score below the threshold line indicates a false non match such as authentication attempt five in (d).



(a) Pair 1 (b) Pair 2 (c) Pair 3

(d) Pair 4 (e) Pair 5

Fig. 14. Confidence scores of each authentication attempt in coincide phase. Attackers of pairs 3-5 did not show any improvement in mimicking their attackers, whereas the attackers of pair 1 and 2 have shown improvements as compared to the last phase.

traits such as, voice [44] and hand signature [45], [46] are vulnerable to impersonation attacks. Gait is a complex combination of nervous, muscle, and skeletal systems of an individual [47]. Although physical properties of gait such as stride length, pace and openness or closeness of feet might be easier for an attacker to perceive, but still it may be difficult for an attacker to notice the net acceleration accumulated by the accelerometer at the point of contact on the body due to force to mass ratio ($acceleration = \frac{force}{mass}$). When individuals attempt to walk like someone else they lose symmetry in their steps. In 29 percent of impersonation attempts performed in both phases, attackers failed to produce a walk that resembles their victims because of irregular gait cycles. In our experiment we provided feedback to attackers, but it is still not known whether more training of attackers and sophisticated hill-climbing types of attacks would influence the results presented in this study. Therefore, the current results indicate that chances of accepting an impostor under mimicking attacks are not higher than the chances of FMR under zero-effort attack. It is important to note that our results can not be generalized to other approaches to smartphone-based gait recognition because different approaches use different feature sets for gait recognition. However, it is plausible to assume that the general idea of gait attack resistance against impersonation attacks will hold in other cases as well.

7 Conclusion and Future Work

Accelerometer based biometric gait is an unobtrusive way of authenticating individuals to their smartphones. In this work, we evaluated the security strength of smartphone-based

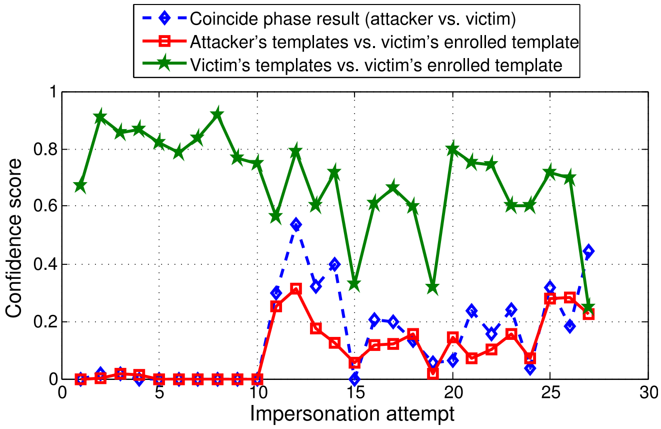


Fig. 15. Templates of the victim's and attacker's of pair 2 from coincide phase are cross compared with the victim's pre-enrolled template.

gait authentication under realistic circumstances by performing zero-effort and minimal-effort impersonation attacks. Initially, an Android application was implemented to record gait data using a smartphone-based accelerometer. We have recorded gait data from 35 participants under a realistic scenario such as placing smartphones inside the front left pocket of their trousers. Under the zero-effort scenario, we achieved an EER of 13 percent. Based on these results, we developed an Android application for continuous gait authentication on smartphones. Like other biometrics, gait can also be vulnerable to impersonation attacks. Therefore, another study was conducted using the same application to investigate attack resistance of our gait authentication system against impersonation attacks. A total of nine subjects participated in this study, four as victims and five as attackers. These attackers are professional actors and trained in mimicking body motions and body language and hand-picked by an expert on mimicking body motions and body language. We have conducted a minimal-effort impersonation attack in two different phases, namely reenact phase and coincide phase. In the reenact phase, attackers were allowed to not only observe but also walk with their targets to closely observe them and later they were asked to emulate their target's gait. In the coincide phase, we analyzed if attackers imitation skills improve when they walk next to their respective victims. Because of the 0 percent FMR in both cases we argue that attackers did not manage to achieve high confidence scores sufficient enough to be accepted by the system. Further, in 29 percent of impersonation attempts, attackers lost regularity in their own steps while imitating the victims. Although the data used for attack scenario includes only few subjects, the results of this study complements previous work [21] and strengthen the argument that it is difficult to mimic gait under stronger attack scenarios. We note that the set of potential attackers trained at the level of our study subjects is small, and that we expect realistic attackers with more limited skills. The results of this study are promising, but in future work we would like to address some open questions. Do "lambs" (people who may be easy to target) and "wolves" (people who may be better attackers) [29] exist in gait biometric as well? What are their physical characteristics? How easily can they be distinguished? Will more training help attackers to impersonate gait biometric? Exploring these questions could be a step forward towards understanding the security limits of gait authentication.

Acknowledgments

This work has been carried out within the scope of *u'smile*, the Josef Ressel Center for User-Friendly Secure Mobile Environments, funded by the Christian Doppler Gesellschaft, A1 Telekom Austria AG, Drei-Banken-EDV GmbH, LG Nexera Business Solutions AG, NXP Semiconductors Austria GmbH, and Österreichische Staatsdruckerei GmbH. Further, the authors would like to thank Mr. Aleksandar Acev for his time and cooperation in attackers selection process. He teaches "movement and physical acting" at the Anton Bruckner Private University for Music, Drama, and Dance. The authors are highly grateful to all participants of this study, especially attackers/actors (Emilie, Janik, Johanna, Lukas, and Simon) for sparing time from their busy schedule. A preliminary version of this work was published in the 12th International Conference on Advances in Mobile Computing and Multimedia [1]. This article extends previous work on gait recognition towards attack resistance of smartphone-based biometric gait and a completely new approach and study for evaluating imitation attacks performed by professional actors.

References

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

[2] D. van Bruggen, S. Liu, M. Kajzer, A. Striegel, C. R. Crowell, and J. D'Arcy, "Modifying smartphone user locking behavior," in *Proc. 9th Symp. Usable Privacy Secur.*, 2013, pp. 10:1–10:14.

[3] L. Cranor and S. Garfinkel, *Security and Usability*. Sebastopol, CA, USA: O'Reilly Media, 2005.

[4] T. Beauvisage, "Computer usage in daily life," in *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, 2009, pp. 575–584.

[5] D. Hintze, R. D. Findling, S. Scholz, and R. Mayrhofer, "Mobile device usage characteristics: The effect of context and form factor on locked and unlocked usage," in *Proc. 12th Int. Conf. Advances Mobile Comput. Multimedia*, 2014, pp. 105–114.

[6] E. Hayashi and J. Hong, "A diary study of password usage in daily life," in *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, 2011, pp. 2627–2630.

[7] F. Breitinger and C. Nickel, "User survey on phone security and usage," in *Proc. Int. Conf. Biometrics Special Interest Group*, 2010, pp. 139–144.

[8] F. Schaub, R. Deyhle, and M. Weber, "Password entry usability and shoulder surfing susceptibility on different smartphone platforms," in *Proc. 11th Int. Conf. Mobile Ubiquitous Multimedia*, 2012, pp. 13:1–13:10.

[9] F. Tari, A. A. Ozok, and S. H. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," in *Proc. 2nd Symp. Usable Privacy Secur.*, 2006, pp. 56–66.

[10] E. von Zezschwitz, A. Koslow, A. De Luca, and H. Hussmann, "Making graphic-based authentication secure against smudge attacks," in *Proc. Int. Conf. Intell. User Interfaces*, 2013, pp. 277–286.

[11] R. Mayrhofer and H. Gellersen, "Shake well before use: Intuitive and secure pairing of mobile devices," *IEEE Trans. Mobile Comput.*, vol. 8, no. 6, pp. 792–806, Jun. 2009.

[12] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *J. Inf. Secur. Appl.*, vol. 22, pp. 113–122, 2015.

[13] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous verification using multimodal biometrics," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 687–700, Apr. 2007.

[14] C. Nickel, "Accelerometer-based biometric gait recognition for authentication on smartphones," Ph.D. dissertation, Fachbereich Informatik, TU Darmstadt, Darmstadt, Germany, Jun. 2012.

[15] M. Muaaz and R. Mayrhofer, "An analysis of different approaches to gait recognition using cell phone based accelerometers," in *Proc. Int. Conf. Advances Mobile Comput. Multimedia*, 2013, pp. 293–300.

[16] J. R. Kwapisz, G. M. Weiss, and S. A. Moore, "Cell phone-based biometric identification," in *Proc. 4th IEEE Int. Conf. Biometrics: Theory Appl. Syst.*, 2010, pp. 1–7.

[17] Y. Zhong, Y. Deng, and G. Meltzner, "Pace independent mobile gait biometrics," in *Proc. IEEE 7th Int. Conf. Biometrics Theory Appl. Syst.*, Sep. 2015, pp. 1–8.

[18] A. Jain, A. Ross, and U. Uludag, "Biometric template security: Challenges and solutions," in *Proc. 13th Eur. Signal Process. Conf.*, Sep. 2005, pp. 1–4.

[19] D. Gafurov, "Performance and security analysis of gait-based user authentication," Ph.D. dissertation, Faculty Math. Natural Sci., Universitas Osloensis, Oslo, Norway, 2004.

[20] Ø. Stang, "Gait analysis: Is it easy to learn to walk like someone else?" Master thesis, Dept. Comput. Sci. Media Technol., Gjøvik Univ. College, Gjøvik, Norway, 2007.

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

[22] B. B. Mjaaland, P. Bours, and D. Gligoroski, *Walk the Walk: Attacking Gait Biometrics by Imitation*. Berlin, Germany: Springer, 2011, pp. 361–380.

[23] S. Sprager and D. Zazula, "A cumulant-based method for gait identification using accelerometer data with principal component analysis and support vector machine," *WSEAS Trans. Signal Process.*, vol. 5, pp. 369–378, 2009.

[24] J. Frank, S. Mannor, and D. Precup, "Activity and gait recognition with time-delay embeddings," in *Proc. 24th AAAI Conf. Artif. Intell.*, 2010, pp. 1581–1586.

[25] M. O. Derawi, "Smartphones and biometrics: Gait and activity recognition," Ph.D. dissertation, Faculty Comput. Sci. Media Technol., Gjøvik Univ. College, Gjøvik, Norway, Nov. 2012.

[26] M. P. Murray, "Gait as a total pattern of movement: Including a bibliography on gait," *Amer. J. Phys. Med. Rehabil.*, vol. 46, no. 1, 1967, Art. no. 290.

[27] H. Ailisto, M. Lindholm, J. Mäntyjärvi, E. Vildjiounaite, and S. Mäkelä, "Identifying people from gait pattern with accelerometers," in *Proc. SPIE*, 2005, Art. no. 5779.

[28] Y. Zhang, G. Pan, K. Jia, M. Lu, Y. Wang, and Z. Wu, "Accelerometer-based gait recognition by sparse representation of signature points with clusters," *IEEE Trans. Cybern.*, vol. 45, no. 9, pp. 1864–1875, Sep. 2015.

[29] R. Bolle, J. Connell, S. Pankanti, N. Ratha, and A. Senior, *Guide to Biometrics*. Berlin, Germany: Springer-Verlag, 2003.

[30] A. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Trans. Inf. Forensics Secur.*, vol. 1, no. 2, pp. 125–143, Jun. 2006.

[31] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial "gummy" fingers on fingerprint systems," in *Proc. SPIE*, 2002, pp. 275–289.

[32] A. Adler, "Sample images can be independently restored from face recognition templates," in *Proc. IEEE Canadian Conf. Elect. Comput. Eng.*, May 2003, vol. 2, pp. 1163–1166.

[33] D. G. Altman, *Practical Statistics for Medical Research*. London, U.K.: Chapman & Hall/CRC, 1991.

[34] M. Muaaz and R. Mayrhofer, "Cross pocket gait authentication using mobile phone based accelerometer sensor," in *Computer Aided Systems Theory*. Cham, Switzerland: Springer, 2015, pp. 731–738.

[35] A. Sam, F. J. Ruiz, N. Agell, C. Prez-Lpez, A. Catal, and J. Cabestany, "Gait identification by means of box approximation geometry of reconstructed attractors in latent space," *Neurocomputing*, vol. 121, pp. 79–88, 2013.

[36] M. Derawi and P. Bours, "Gait and activity recognition using commercial phones," *Comput. Secur.*, vol. 39, pp. 137–144, 2013.

[37] C. Tudor-Locke, C. L. Craig, W. J. Brown, S. A. Clemes, K. De Cocker, B. Giles-Corti, Y. Hatano, S. Inoue, S. M. Matsudo, N. Mutrie, J.-M. Oppert, D. A. Rowe, M. D. Schmidt, G. M. Schofield, J. C. Spence, P. J. Teixeira, M. A. Tully, and S. N. Blair, "How many steps/day are enough? for adults," *Int. J. Behavioral Nutrition Phys. Activity*, vol. 8, no. 1, p. 79, 2011.

[38] B. C. Choi, A. W. Pak, and J. C. Choi, "Daily step goal of 10,000 steps: A literature review," *Clinical Investigative Med.*, vol. 30, no. 3, pp. 146–151, 2007.

[39] Y. Hatano, "Use of the pedometer for promoting daily walking exercise," *Int. Council Health Phys. Educ. Recreation*, vol. 29, no. 4, pp. 4–8, 1993.

[40] W. Gander and U. Matt, "Smoothing filters," in *Solving Problems in Scientific Computing Using Maple and MATLAB*. Berlin, Germany: Springer, 1995, pp. 121–139.

[41] D. Alvarez, R. Gonzalez, A. Lopez, and J. Alvarez, "Comparison of step length estimators from weareable accelerometer devices," in *Proc. 28th Annu. Int. Conf. IEEE Eng. Med. Biology Soc.*, Aug. 2006, pp. 5964–5967.

[42] M. Sekine, et al., "Assessment of gait parameter in hemiplegic patients by accelerometry," in *Proc. 22nd Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, 2000, vol. 3, pp. 1879–1882.

[43] H. Zhang, J. Qian, L. Shen, and Y. Zhang, "Research on healthy subject gait cycle phase at different walking speeds," in *Proc. IEEE Int. Conf. Robot. Biomimetics*, Dec. 2012, pp. 1349–1354.

[44] Y. W. Lau, M. Wagner, and D. Tran, "Vulnerability of speaker verification to voice mimicking," in *Proc. Int. Symp. Intell. Multimedia Video Speech Process.*, Oct. 2004, pp. 145–148.

[45] L. Ballard, D. Lopresti, and F. Monrose, "Evaluating the security of handwriting biometrics," in *Proc. 10th Int. Workshop Found. Handwriting Recognit.*, 2006, pp. 461–466.

[46] S.-H. Cha and C. C. Tappert, "Automatic detection of handwriting forgery," in *Proc. 8th Int. Workshop Frontiers Handwriting Recognit.*, 2002, pp. 264–267.

[47] C. L. Vaughan, B. L. Davis, and J. C. Ó. Connor, *Dynamics of Human Gait*. Champaign, IL, USA: Human Kinetics Publishers, 1992.

Muhammad Muaaz received the bachelor's of engineering degree in computer and information systems from the N.E.D University of Engineering and Technology, Pakistan, and the MSc degree in information and communication systems security from the KTH Royal Institute of Technology, Sweden. Currently, he is researcher with u'smile, the Josef Ressel Centre for User-Friendly Secure Mobile Environments, University of Applied Sciences Upper Austria, and working toward the PhD degree at the Johannes Kepler University Linz, Austria. His research interests include, information security, biometrics, and machine learning.

René Mayrhofer received the Dipl-Ing (MSc) and Dr techn (PhD) degrees from Johannes Kepler University Linz, Austria, and the Venia Docendi for applied computer science from the University of Vienna, Austria. He heads the Institute of Networks and Security (INS), Johannes Kepler University Linz (JKU), Austria, and the Josef Ressel Center on User-friendly Secure Mobile Environments (u'smile). Previously, he held a full professorship for mobile computing with the Upper Austria University of Applied Sciences, Campus Hagenberg, a guest professorship for mobile computing with the University of Vienna, and a Marie Curie Fellowship with Lancaster University, United Kingdom. His research interests include computer security, mobile devices, network communication, and machine learning, which he brings together in his research on securing spontaneous, mobile interaction. He has contributed to more than 60 peer-reviewed publications and is a reviewer for numerous journals and conferences.