Paper1 Spoof Attacks on Gait Authentication System

DATASET · FEBRUARY 2014

READS
76

3 AUTHORS, INCLUDING:

Davrondzhon Gafurov
Norwegian Directorate of Health
37 PUBLICATIONS **434** CITATIONS
SEE PROFILE

Patrick Bours
Gjøvik University College
71 PUBLICATIONS **522** CITATIONS
SEE PROFILE

Spoof Attacks on Gait Authentication System

Davrondzhon Gafurov, Einar Snekkenes, *Member, IEEE*, and Patrick Bours

***Abstract*—Research in biometric gait recognition has increased. Earlier gait recognition works reported promising results, usually with a small sample size. Recent studies with a larger sample size confirm gait potential as a biometric from which individuals can be identified. Despite much research being carried out in gait recognition, the topic of vulnerability of gait to attacks has not received enough attention. In this paper, an analysis of minimal-effort impersonation attack and the closest person attack on gait biometrics are presented. Unlike most previous gait recognition approaches, where gait is captured using a (video) camera from a distance, in our approach, gait is collected by an accelerometer sensor attached to the hip of subjects. Hip acceleration in three orthogonal directions (up–down, forward–backward, and sideways) is utilized for recognition. We have collected 760 gait sequences from 100 subjects. The experiments consisted of two parts. In the first part, subjects walked in their normal walking style, and using the averaged cycle method, an EER of about 13% was obtained. In the second part, subjects were trying to walk as someone else. Analysis based on FAR errors indicates that a minimal-effort impersonation attack on gait biometric does not necessarily improve the chances of an impostor being accepted. However, attackers with knowledge of their closest person in the database can be a serious threat to the authentication system.**

***Index Terms*—Biometric security, gait mimicking, gait recognition, impersonation attacks, wearable sensor.**

I. Introduction

BIOMETRIC SYSTEMS are increasingly becoming important, as they can offer more reliable and efficient means of authentication than traditional methods. Human biometrics can be classified into two types (not necessarily disjoint sets)—physiological and behavioral. The first type is based on stable physical characteristics, while the second type uses learned, alterable behavioral characteristics. Examples of the physiological type are fingerprints, iris, retina, etc. Voice, keystroke dynamics, handwritten signature, and gait belong to the behavioral group. Gait is a person's manner of walking. Lately, gait as a biometric, has gained much attention. A primary advantage of (vision-based) gait as a biometric is the ability to be captured from the distance while other types of biometrics (e.g., fingerprints) are not available. Earlier studies on gait recognition showed promising results, usually the numbers of subjects in these experiments were limited [1], [2]. For example, BenAbdelkader *et al.* [1] with a data set of 40 walking sequences from six subjects obtained a 93% recognition rate. Hayfron–Acquah *et al.* [2] with a database of 16 gait samples from four subjects and 42 gait samples from six subjects achieved correct classification rates of 100% and 97%, respectively. Furthermore, recent studies with a larger sample size, which include more than 100 people in the experiments, confirm that gait has a distinctive pattern from which individuals can be recognized [3]–[6]. For instance, Sarkar *et al.* [3] with a data set consisting of 1870 gait sequences from 122 subjects, obtained a 78% identification rate (experiment A). This performance was even improved further to achieve 95% in other works [7]–[9].

From a technological point of view, biometric gait recognition systems can be categorized into three classes: 1) machine vision (MV) based, 2) floor sensor (FS) based, and wearable sensor (WS) based. In the rest of this paper, we will refer to these three gait approaches as MV based, FS based, and WS based, respectively. In the MV-based gait recognition system, gait is captured using a (video) camera from a distance, and then video/image processing techniques are employed to extract gait features for recognition. Most of the current gait recognition approaches belong to this category [1]–[9]. In FS-based gait recognition, sensors (e.g., force plates), which are installed in the floor, are used for capturing gait [10], [11]. Such sensors enable measuring gait features, such as ground reaction force (GRF) [10] or heel-to-toe ratio [11], when a person walks on them. In WS-based gait recognition, gait is collected using a set of body-worn sensors [12]–[14]. An accelerometer sensor can be used for collecting gait. For person verification, Ailisto *et al.* [12] and Mäntyjärvi *et al.* [13] collected acceleration data from the waist of the person. In [14], the accelerometer sensor was attached to the lower leg and acceleration of the lower leg was used for authentication.

In this paper, we make use of acceleration data from the hip of the person. The accelerometer sensor records acceleration in three orthogonal directions (forward–backward, up–down, and sideways), and the resulting vector is used for authenticating users. A primary advantage of the WS-based gait over other types of biometrics (except voice perhaps) is enabling unobtrusive user authentication due to this WS-based gait approach having been suggested for protection and user authentication in mobile and portable devices [12], [13]. A list of several proposed biometric authentication modalities alongside with their performance is shown in Table I. Fingerprints, face, keystroke dynamics, and iris recognition require user cooperation and explicit action or input from the user, which are not convenient when devices are often used. In some environments, such as wearable computing, the issues of unobtrusiveness and user's attention are critical [24]. Therefore, WS-based gait recognition can be a better candidate in such environments.

Manuscript received October 31, 2006; revised April 26, 2007. This work was supported by The Research Council of Norway. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Bir Bhanu.

The authors are with the NISLab, Gjøvik University College, Gjøvik, Norway (e-mail: davrondzhon.gafurov@hig.no; einar.snekkenes@hig.no; patrick.bours@hig.no).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2007.902030

TABLE I
BIOMETRIC MODALITIES PROPOSED FOR PROTECTION AND USER AUTHENTICATION FOR PORTABLE, MOBILE AND WEARABLE PERSONAL ELECTRONIC DEVICES

Study	EER %	Biometrics
Chen et al. [15]	4.16	fingerprint
Su et al. [16]	4.23	fingerprint
Lee et al. [17]	4.37	voice
Leung et al. [18]	6.7	voice
Ijiri et al. [19]	-	face
Nagel et al. [20]	6	face
Vildjiounaite et al. [21]	2-12	gait + voice
Ailisto et al. [12]	6.4	gait
Clarke and Furnell [22]	12.8	keystroke dynamics
Lee et al. [23]	0.18	iris

However, for biometrics, it is not enough to be unique; it is also important to be robust against attacks. Behavioral biometrics can be vulnerable to the impersonation or mimicking attacks. Despite much research being carried out in gait recognition, the topic of security per se of gait has not received enough attention. According to a study by Juniper Research [25], mobile biometric solutions will contribute some U.S.$ 268 million worth of revenue of the total mobile identity and access-management market (U.S.$ 1.36 billion) by 2011. Consequently, it is important as a part of risk management to investigate the robustness of proposed biometrics (e.g., gait) against attacks before they can be applied to real applications. The level of attacks that can be applied to a biometric system mainly depend on the resources available to the attackers, such as time, tools (e.g., hardware/software), knowledge of the system (e.g., biometrics vulnerabilities), and so on. Thus, attacks may vary from very sophisticated, where, at the attacker's disposal, all necessary resources are available (i.e., unlimited time, complete knowledge of the system) to low limited ones, where attackers have very limited resources (e.g., limited time and a limited number of attempts).

In the case of the gait authentication system, we define a minimal effort impersonation (mimicking) attacks as those types of attacks where the attacker has no information other than common knowledge of the system (e.g., hip acceleration is used for authentication), limited time to study the target subject's walking style, and a restricted number of mimicking attempts. In [26], a preliminary analysis of the minimal-effort impersonation attack on gait biometrics, which is based on the impostor score distributions, has been reported. Although the results are encouraging, the number of subjects used in the experiment were limited. In addition, a new analysis on the false accept rate (FAR)/false reject rate (FRR) level, which are a more natural way of expressing the performance of biometric systems, are desired.

The contribution of this work is not algorithmic in nature but rather the first work to address the security strength of gait biometrics. More specifically, the main contributions of the paper are:

1) an evaluation of WS-based biometric gait recognition with a large data set (760 gait samples from 100 subjects). Although earlier studies on WS-based gait recognition reported promising performance, the number of subjects used in those studies were moderate [12]–[14];
2) a first feasibility study of attack scenarios on the gait authentication system. Previously, impostor scores for estimating FAR error rates were generated by comparing normal walking of the impostor subjects against normal walking of all other subjects in the database [12]–[14], [27]–[30]. However, such an approach might not be valid for evaluating the security strength of the gait biometric against attacks.

The security performance analysis consists of three parts. The first part includes analysis of normal walking samples. In the second part, the minimal-effort mimicking attack scenario is evaluated. In the third part, an attack scenario with an assumption of attackers knowing their nearest person in the database is conducted. In all three cases, gait samples are compared using the averaged cycle method. The rest of this work is organized as follows. Section II defines performance evaluation scenarios and shows possible attacks on the biometric system. Section III describes the hardware used for collecting gait data and the gait analysis method. Sections IV and V contain descriptions of experiments and results, respectively. Section VI discusses the results and other related works, and Section VII concludes the paper with topics on future work.

II. SECURITY PERFORMANCE EVALUATION SCENARIOS AND ATTACKS ON BIOMETRIC SYSTEM

A. Security Performance Evaluation Scenarios

We distinguish between two types of impostor attempts active impostor attempt and passive impostor attempt. A passive impostor attempt is an attempt when an individual submits his or her own biometric feature as if he or she were attempting successful verification against his or her own template, but in fact is being compared against a nonself template. The passive impostor attack corresponds to the zero-effort attacks defined by Jain *et al.* [31]. An active impostor attempt is an attempt when an attacker performs one or both of the following actions to increase his or her chances to being accepted by the system:

- changes his or her biometric with the aim to match another targeted person and attempts verification against this targeted person's template (e.g., mimicking or impersonation);
- selects a suitable victim with regard to some knowledge (e.g., closest in the database) and attempts verification against this targeted person's template (not necessarily by changing his or her biometric).

Conventionally, the performance of gait biometric systems is evaluated under a friendly scenario, meaning that in previous works, all impostor attempts consist of only passive impostors [12]–[14], [27]–[30]. By a hostile scenario evaluation, we refer to a setting when the biometric system's impostor trials consists of active impostor attempts. In general, friendly scenario evaluation relates to the discriminating power of the biometric, whereas the hostile scenario shows the robustness of the system against attacks.

To illustrate the changes of performance of a biometric system when it is under an attack, there are four hypothetical decision error tradeoff (DET) curves depicted in Fig. 1. The

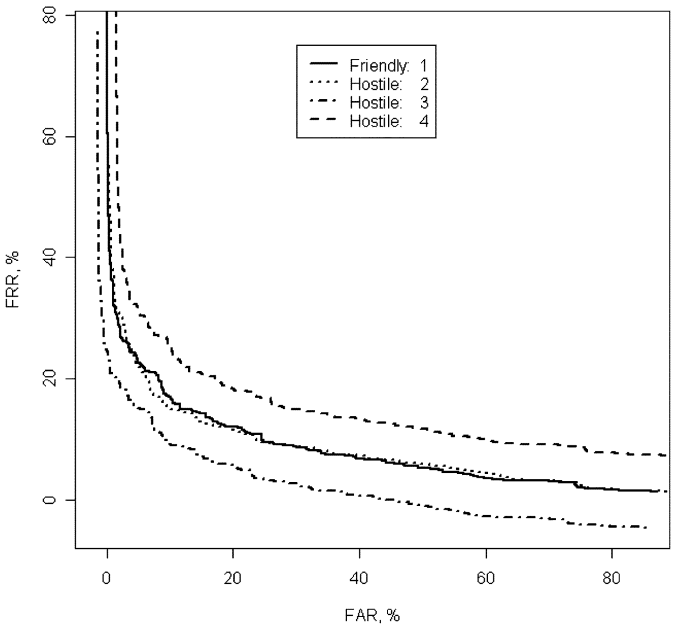

Fig. 1. Examples of performance shift in the biometric system under hostile scenarios.

DET curve is a plot of the FAR versus FRR, which characterizes the performance of the biometric system under different decision thresholds. In other words, by changing the threshold for acceptance, one can produce various combinations of (FAR,FRR) pairs and then based on them, the DET curve can be plotted. In Fig. 1, the first DET curve shows the conventional performance of the system in the friendly scenario. The other three curves represent performance of the system in the hostile scenario. In case of the second curve, the attack does not change performance, and curves (1 and 2) are more or less the same. In case of the third curve, an attack does not succeed at all. In fact, the attack significantly decreases the chances of impostors being accepted by the system (compared to the case 1, friendly scenario). In case of the last DET curve, the attack significantly increases the chances of impostors being accepted by the system. Consequently, in this last case, the particular settings of the biometric system made it vulnerable to the attack.

B. Attacks on Biometric System

Typical points of attack on a biometric authentication system, defined by Ratha *et al.* [32], are depicted in Fig. 2 and are briefly explained below.

1) Presenting fake or imitated biometric to the sensor.
2) Submission of a previously obtained digital biometric sample.
3) The feature extractor is attacked so that it produces feature values dictated by the attacker.
4) Extracted feature values are substituted by the ones selected by the attacker in the fourth type of attack.
5) The score of the matcher is changed to produce a desired high or low matching score.
6) Attack on the database (i.e., modification) of biometric templates.

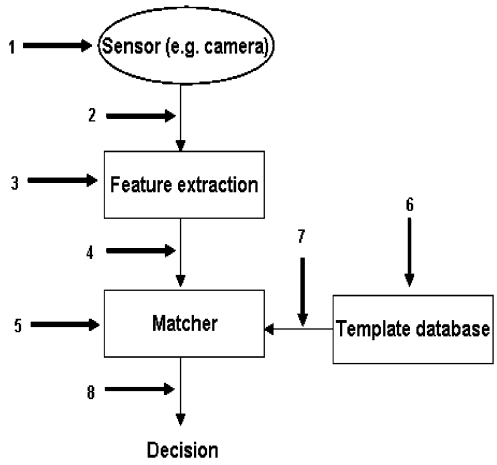

Fig. 2. Eight possible attack points in a biometric authentication system.

7) The transmission channel between the template database and matcher module is attacked (i.e., data in transit are modified).
8) Alternation of decision (reject or accept).

In the biometric system, attacks can be performed both on specific modules of the system and on communication channels between modules. Attacks on the transmission channels are related to the general topic of channel security. They can be defeated using secure channels and data encryption techniques. Usually, for an ordinary attacker, attacks of type 1 or spoof attacks are more accessible than the other types of attacks, since they do not require knowledge of the system architecture or access to internal system components. Besides, other modules of the system are usually behind the walls (inside a physically protected area). In an unattended environment, presenting a fake physiological biometric, or imitating a behavioral biometric could be a serious threat. For example, in fingerprint verification systems, this is referred to as "liveness detection," verifying that the finger presented comes from a living person [33], [34].

In this work, we study the feasibility of imitating or mimicking another person's manner of walking, which is related to an attack of type 1. The primary focus of this paper is on active impostor attacks with minimal effort impersonation. In particular, we exclude extensive adversary training. In the second setting, we test a scenario where impostors select a victim that has the closest gait to their own gait.

III. Gait Authentication Technology

A. Motion-Recording Sensor

The motion-recording (MR) sensor used for collecting gait of the subjects has been developed at Gjøvik University College. It resembles a memory stick device with the following physical characteristics: height $= 90$ mm, width $= 23$ mm, and weight $= 45$ gram, as shown in Fig. 3. The main components of the MR sensor include three accelerometers (2, 3, and 4), 64-MB memory (6) for storing acceleration data, USB (1) and Bluetooth interfaces (8) for data transfer, and a battery (7). The sampling frequency of the MR sensor was about 100 observations per second and its dynamic range was $-6g$ to $+6g$ ($g = 9.8\,\mathrm{m/s^2}$).

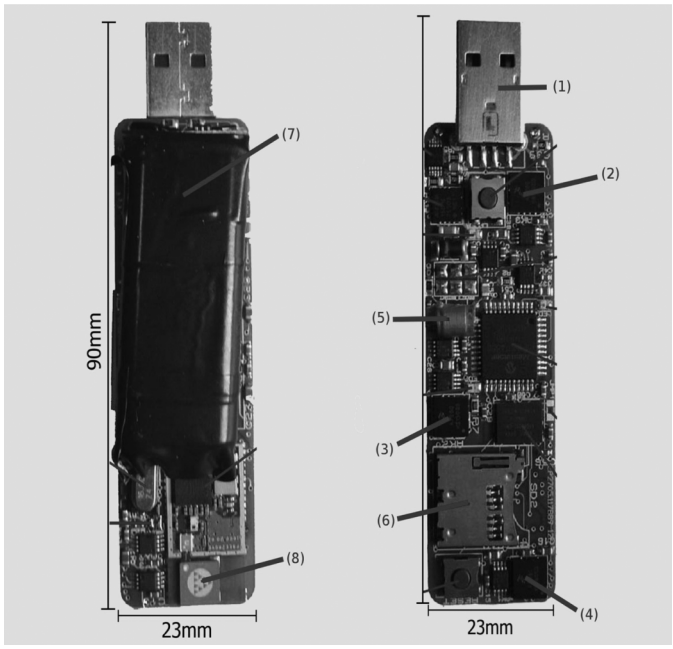

Fig. 3. Internal architecture of the MR sensor.

Fig. 4. MR sensor attached to the belt.

During the experiments, it was attached to the hip of the person as shown in Fig. 4. The hip was chosen as it is a suitable place from a typical application point of view (e.g., people usually carry mobile phones in a similar location).

Output from the MR sensor can be transformed into acceleration (in units of g) in three orthogonal directions: up–down x, forward–backward y, and sideways z. These accelerations are sensitive to the sensor's location and orientation. Therefore, we consider a more invariant combination of them—the magnitude of the resulting acceleration. It is calculated as follows:

$$r_i = \sqrt{x_i^2 + y_i^2 + z_i^2}, \quad i = 1, \ldots, k \tag{1}$$

where r_i, x_i, y_i, and z_i are the magnitudes of resulting, up-down, forward-backward, and sideway acceleration at the observation point i, respectively, and k is the number of recorded observations in the signal.

B. Averaged Cycle Method

Human gait follows a cyclic pattern. Consequently, the resulting acceleration is a periodic signal. From this signal, an averaged walking cycle of the individual is estimated and used as the feature vector. One cycle is equivalent to two steps. The steps involved in comparing the resulting acceleration are as follows.

- Preprocessing: First, the output of the sensor is transformed in order to obtain acceleration in units of g, and then the resulting acceleration is computed. The time intervals between observations in the resulting acceleration signal are not always equal. Therefore, the signal is linearly interpolated before processing. Then, in order to reduce the level of noise, a moving average filter, MA(9), is applied.
- Cycle detection: The natural cadence of the human walking is in the range [90,130] steps/min [27] (i.e., about [45,65] cycles per minute) and the sampling frequency of an accelerometer sensor is about 100 observations/s. With the aid of such clues, we perform cycle detection. Let $R = (r_1, \ldots, r_K)$ be a resulting acceleration signal, and $[r_{m_1}, \ldots, r_{m_L}]$ be the local minima in this signal, which needs to be found. Every cycle contains about 100 observations. A first minimum observation r_{m_1} is found from the first 250 observations in the signal (i.e., $r_{m_1} = \min(r_1, r_2, \ldots, r_{250})$). This minimum observation represents the beginning of the first cycle. Then, the end of the cycle is found as follows $r_{m_2} = \min(r_{m_1+M-d}, \ldots, r_{m_1+M+d})$, where $M = 100$ and $d = 20$. The end of one cycle is considered the start of the next cycle. The procedure is repeated until the last cycle is found.
- Time normalization: Usually, the number of observations in each cycle will not be constant. Therefore, in order to calculate an average cycle of the person, every cycle is normalized in time (by interpolation). Each normalized gait cycle contains exactly 100 observations.
- Averaged cycle: After cycles are found and normalized, an average cycle $A = (a_1, \ldots, a_n)$ is calculated as follows:

$$a_i = \text{median}(w_{ji}) \tag{2}$$

where $i = 1, \ldots, n$, $n = 100$, and w_{ji} is the observation value at observation number i in the normalized cycle $j, i = 1, \ldots, m$, m is the number of detected cycles in the signal. In other words, each observation in the averaged cycle is the median of the corresponding observations in the normalized cycles. The motivation for selecting the median rule for averaging is to reduce the influence of very unusual steps (i.e., cycles). In addition, a few cycles in the beginning and ending of the acceleration signal are

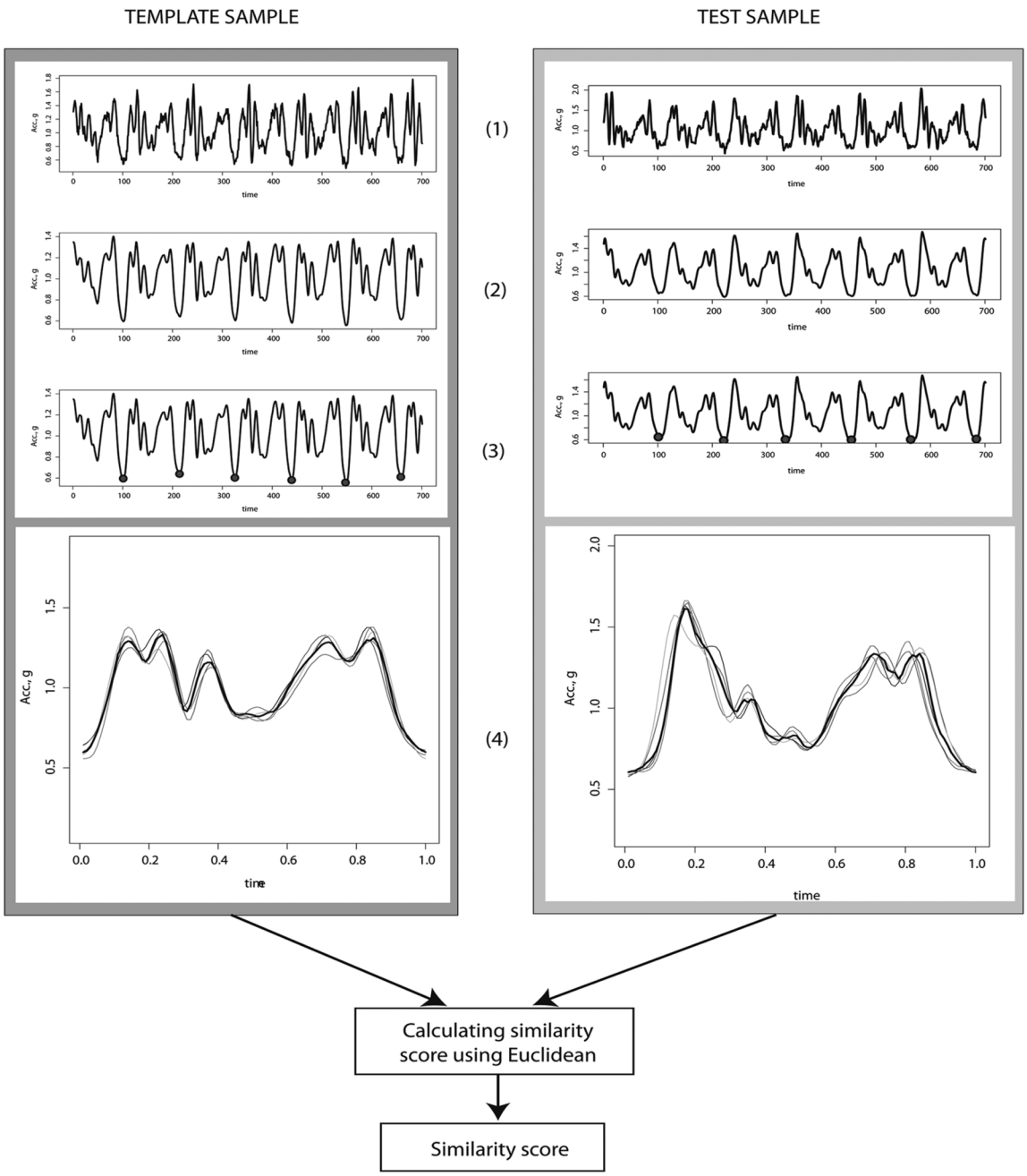

Fig. 5. Steps involved in comparing gait samples. (1) Computing the resulting vector. (2) Interpolation and smoothing. (3) Cycle detection. (4) Calculating the average cycle. In the plots, horizontal and vertical axes are time and acceleration (in units of g), respectively.

omitted, since they may not adequately represent the natural walking rhythm of the person [35], [36].

- Similarity score: As a distance between two averaged gait cycles $B = (b_1, \ldots, b_n)$ and $C = (c_1, \ldots, c_n)$, we use the Euclidean distance

$$\mathrm{dist}(B, C) = \sqrt{\sum_{i=1}^{n} (b_i - c_i)^2} \tag{3}$$

where b_i and c_i are the resulting acceleration values at observation point i, and $n = 100$. This distance value represents the similarity score between two resulting gait signals. For genuine trials, the similarity scores should be smaller than for impostor trials.

The overall process of comparing gait signals by the averaged cycle method is visualized in Fig. 5.

IV. Experiments

No public data set on the WS-based gait is available (perhaps due to the fact that it is a recent approach in gait recognition). Furthermore, due to the specific nature of the experiments (mimicking), we have created a new gait database for the purpose of this study. The experiment consists of two parts—the friendly scenario and hostile scenario. In the former scenario, participants walked using their normal walking style, while in

the latter scenario, subjects tried to walk as someone else (i.e., mimicking). Both experiments were conducted in the same indoors location, and subjects were walking on a level surface for a distance of about 20 m. In both experiments, the MR sensor was attached to the belt of the subjects, around the right hip, as shown in Fig. 4. Data analysis was performed offline (i.e., all collected gait samples were transferred to a PC for later processing).

A. Friendly Scenario Experiment

In the friendly scenario, 100 subjects participated—30 female and 70 male—ranging in age from 19 to 62. Subjects were asked to walk four times in their natural walking style. In each session, the MR sensor was either removed and reattached or subjects were asked to shift their belts a little bit for simulating realistic settings (i.e., the MR sensor is not always exactly in the same position and orientation). In the friendly scenario experiments, we have collected, in total, 400 gait sequences, four samples per subject.

B. Hostile Scenario Experiment

In this scenario, 90 subjects participated—62 male and 28 female. These subjects are a subset of participants from the friendly scenario experiment. Every subject was paired with another one based on "friendness" (45 pairs). Everyone was told to study his or her partner's walking style and try to imitate him or her. One subject from the pair acted as an attacker, the other one as a target, and then the roles were exchanged. We have the following relationships between the attacker and target:

- the gender of the attacker and the target was the same;
- the mean age difference between the attacker and the target was about 4.67 years;
- the pairs knew each other previously, they were friends, classmates, or colleagues (i.e., "friendness");
- for most pairs, the physical characteristics (height and weight) were not significantly different.

The attacker was present during the enrollment time of the target. Both the normal walking and the imitated walking experiment were conducted on the same day. The time interval between normal walking and imitated walking was about 1 h. All attackers were amateurs and did not have special training for the purpose of mimicking. They only studied the target person visually, which can also easily be done in a real-life situation as gait cannot be hidden. The only information about the gait authentication system they knew was that the acceleration of normal walking was used. Except mimicking another main difference between the passive (zero-effort) attack in a friendly scenario and the minimal-effort active attempt in the hostile scenario is that in the minimal-effort active attack, the impostors were explicitly aware that their gait samples would be compared against the targeted person's gait. Every attacker made four mimicking attempts. In the first two attempts, the target person walked in front of the attacker, in the last two attempts, the attacker was mimicking alone. Each gait imitation was conducted without a live feedback of the attempt's result. The feedback procedure was not implemented because in the current version of the MR sensor, there was not a hardware module specifically designed for this purpose (e.g., to produce sound). In the hostile scenario experiments, in total, we have collected 360 gait sequences, four samples per attacker.

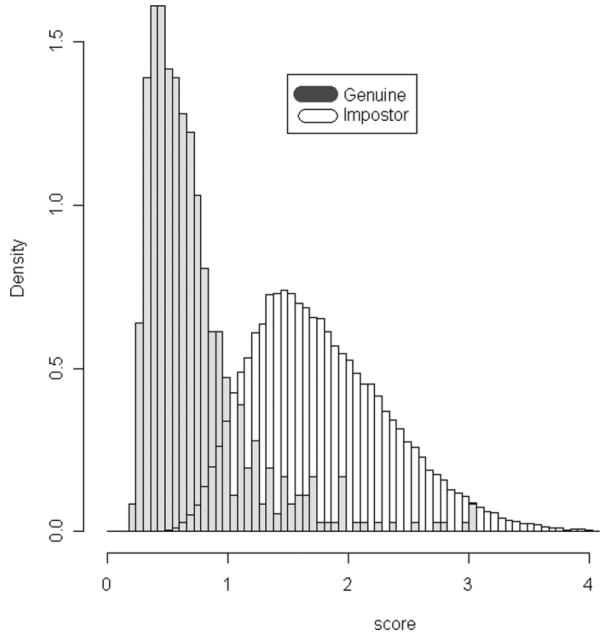

Fig. 6. Distributions of genuine and passive impostor scores.

V. Results

Gait samples were compared using the averaged cycle method, as described previously. In the friendly scenario, the performance of the method was evaluated both in verification and identification modes. In the hostile scenario, two attack scenarios, namely minimal-effort impersonation and closest target attack, were evaluated. In the hostile scenario, our main aim was to see whether FAR can be increased with such types of attack.

A. Results From the Friendly Scenario

We hoped to obtain unbiased estimates of error rates by using the leave-one-out cross comparisons procedure among gait samples [37]. If the number of subjects is n and the number of samples per subject is m, then the number of genuine scores is $n \cdot (m \cdot (m-1)/2)$ and the number of impostor scores is $m^2 \cdot (n \cdot (n-1)/2)$ for a symmetric classifier. In this work, with $n = 100$ subjects and $m = 4$ samples per subject, the numbers of genuine and (passive) impostor scores were 600 and 79200, respectively. We will denote the genuine set as G, which will be used in Sections V-B and V-C. The distributions of the genuine and impostor scores are given in Fig. 6. Based on these two sets of scores, we estimated the FAR and FRR errors. The performance of the method under the friendly scenario in terms of the DET curve is shown in Fig. 7. Usually to indicate performance of the biometric system by a single scalar, an equal error rate (EER) is used. The EER is a point where $\mathrm{FAR} = \mathrm{FRR}$. The EER of the averaged cycle method was about 13%.

For completeness, we also report performance of the method in the identification mode. To evaluate the performance in this mode, a cumulative match characteristic (CMC) curve was chosen [38]. The CMC curve is a plot of the rank versus an

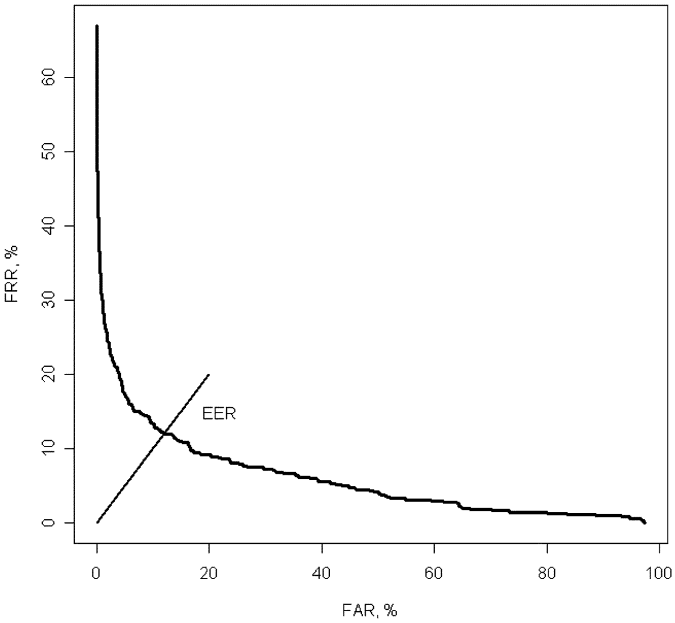

Fig. 7. Performance of the method in terms of the DET curve.

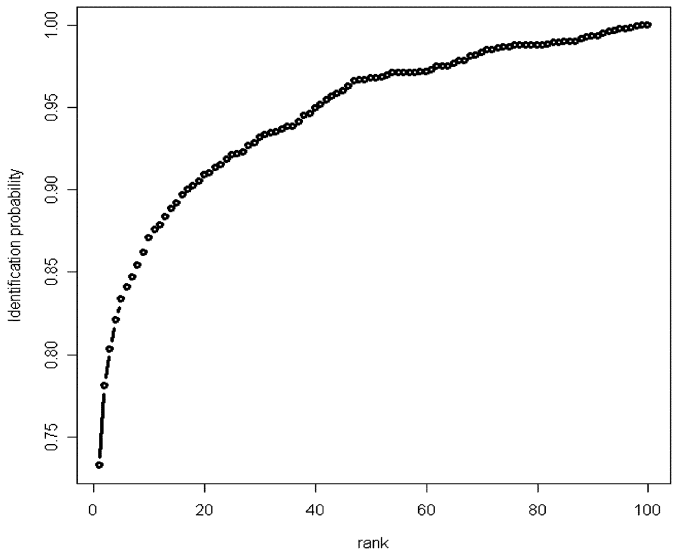

Fig. 8. Performance of the method in terms of the CMC curve.

TABLE II
IDENTIFICATION RATES AT RANKS 1–5

	rank 1	**rank 2**	**rank 3**	**rank 4**	**rank 5**
Identification rate	73.2%	78.1%	80.3%	82.1%	83.3%

identification rate. It indicates the cumulative probability of a match being within the top n closest matches. We define sets S_1, S_2, S_3, and S_4 as the sets of 1st, 2nd, 3rd, and 4th samples of the subjects, respectively. The cardinality of each set S_i is 100 and they are pairwise disjoint (i.e., $S_i \cap S_j = \emptyset, \forall\, i \neq j$; $i, j = 1, 2, 3, 4$). In the parlance of face recognition, the first set S_1 was used as a gallery set (known samples) and the union of the other three sets were used as a probe set (unknown samples) [38]. Every sample from the probe set is compared with each sample in the gallery set. Additionally, our comparisons were conducted under closed universe assumptions, meaning that every sample from the probe set had only one corresponding sample in the gallery set. Then, the second set S_2 was used as a gallery and the remaining sets as a probe set. This was repeated until all four sets had acted as a gallery. Finally, identification rates in every rank were averaged. The resulting CMC curve is shown in Fig. 8. The averaged identification rates on ranks 1–5 are also given in Table II.

B. Results From the Hostile Scenario: Minimal-Effort Mimicry

We obtained two sets of impostor scores X and Y which represent hostile and friendly scenarios impostor scores, respectively. The set X is the set of active impostor scores, while the set Y is the set of passive impostor scores. The first set X was generated by comparing imitated (i.e., mimicked) samples of the attackers against the targets' normal samples. In this case, the number of scores per attacker is 16, since the number of mimicking attempts per attacker is 4 and the number of normal walking per target person is 4 too. Consequently, the cardinality of the set X is 1440 $(= 16 \cdot 90)$. The second set Y was generated by comparing normal walking samples of attackers against normal walking samples of the corresponding targets. The set Y did not include impostor scores which were generated by comparing normal gait sample of an attacker against normal gait sample of a nontarget subject because such nontarget impostor scores might not be valid in security strength evaluation. In the set Y, the number of scores per subject is also 16 $(= 4 \cdot 4)$, and the cardinality of the set Y is again 1440. It should be noted that every score in Y is duplicated, since we use a symmetric matcher. However, this does not affect the estimation of FAR [39]. Based on the active impostor set X and the genuine set G from the previous subsection, the FAR and FRR were estimated. Then, using these estimates, the DET curve in the hostile scenario, was computed. In a similar way, using sets Y and G as impostor and genuine sets, the other pairs of FAR and FRR were estimated. Next, the DET curve in the friendly scenario was computed. The resulting DET curves are shown in Fig. 9.

To get a robust picture of the comparison, we also calculate 95% confidence intervals (CI) for the FARs. For computing a CI, a parametric [37] and a bootstrap technique [40] can be used. However, it has been shown that both the parametric method and the traditional bootstrap method for computing a CI underestimate the confidence regions [39] such methods make the assumption that scores are independent which may not be adequate, since the multiple samples from the same subject are not independent. In our case, the impostor scores are not independent either. To account for this dependency, we computed confidence intervals using the subset bootstrap procedure as described in [39]. Assume $S = \{s_1, \ldots, s_N\}$ is a set of impostor scores, where N is the total number of impostor scores. Then, the 95% confidence interval for the FAR at the threshold point s_k is calculated as follows.

Step 1) $\mathrm{FAR}(s_k)$ is computed from set S.

Step 2) Impostor scores S is divided into T "independent subsets" $P_1, \ldots, P_T$.

Step 3) A bootstrap set S^* is generated by sampling with replacement T subsets from $S = \{P_1, \ldots, P_T\}$.

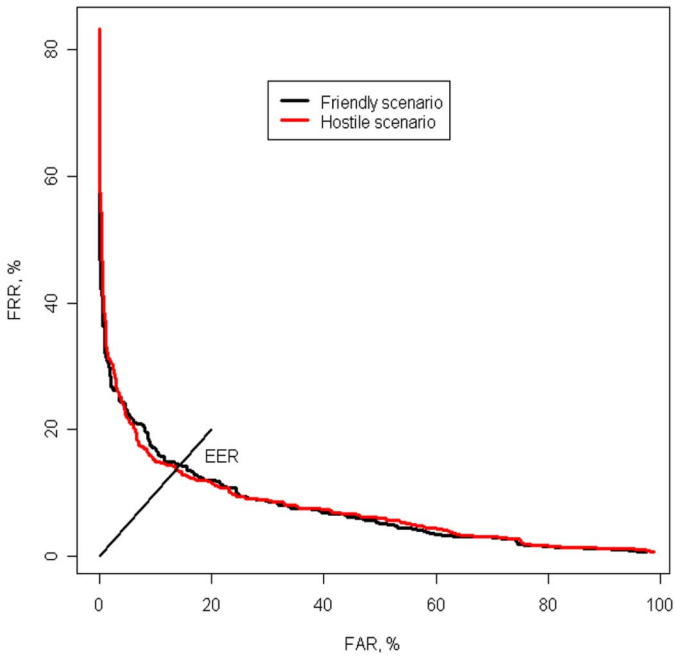

Fig. 9. Performance comparison under friendly scenario and hostile scenarios.

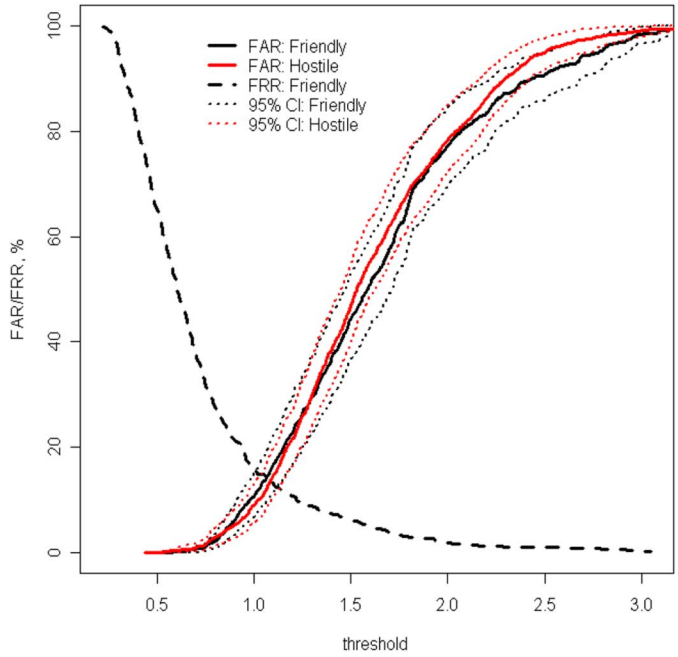

Fig. 10. FAR curves with 95% CI: Friendly scenario versus hostile scenario.

Step 4) $\mathrm{FAR}^*(s_k)$ was computed from set S^*.
Step 5) Steps 3)–4) were repeated $B = 1000$ times.
Step 6) The bootstrap estimates were sorted $\mathrm{FAR}^*_{(1)}(s_k) \leq \mathrm{FAR}^*_{(2)}(s_k) \leq \cdots \leq \mathrm{FAR}^*_{(B)}(s_k)$.
Step 7) The bootstrap confidence interval for $\mathrm{FAR}(s_k)$ is $\left[\mathrm{FAR}^*_{(q_1)}(s_k), \mathrm{FAR}^*_{(q_2)}(s_k)\right]$, where $q_1 = [B * \alpha/2]$, the integral part of $B*\alpha/2$, $q_2 = B - q_1 + 1$, and $\alpha = 0.05$ (for the 95% confidence interval).

In Step 2), for obtaining independent subsets, we divided the impostor scores based on the person [39]. For example for the set X, we divided it into $T = 90$ subsets, each consisting of 16 scores. Every subset represents impostor scores from one attacker. In the same way, the set Y was also divided into independent subsets for computing confidence intervals.

A plot of FAR curves under friendly and hostile scenarios with their 95% confidence bounds is depicted in Fig. 10. The FAR curves cross each other in a few threshold points. In general, the behavior (shape) of both the DET and the FAR curves with their 95% CI indicate that the probability of FAR error in the hostile scenario is not significantly higher than the probability of FAR error in the friendly scenario in case of a minimal effort mimicking attack.

In addition, we compared attackers mimicking samples with their own normal walking samples to verify whether there is a significant difference between genuine attempts in friendly and hostile scenarios. This might be useful in a negative identification scenario (i.e., when users do not want to be recognized by the system). A plot of FRR curves under friendly and hostile scenarios is given in Fig. 11. Confidence intervals for FRR were also computed using the subset bootstrap technique [39]. As one may expect, it shows that FRR significantly increased in the hostile scenario. This implies that in the negative identification scenario, it is easy to fool the system into not recognizing oneself. Another important conclusion one can draw from Fig. 11 is that

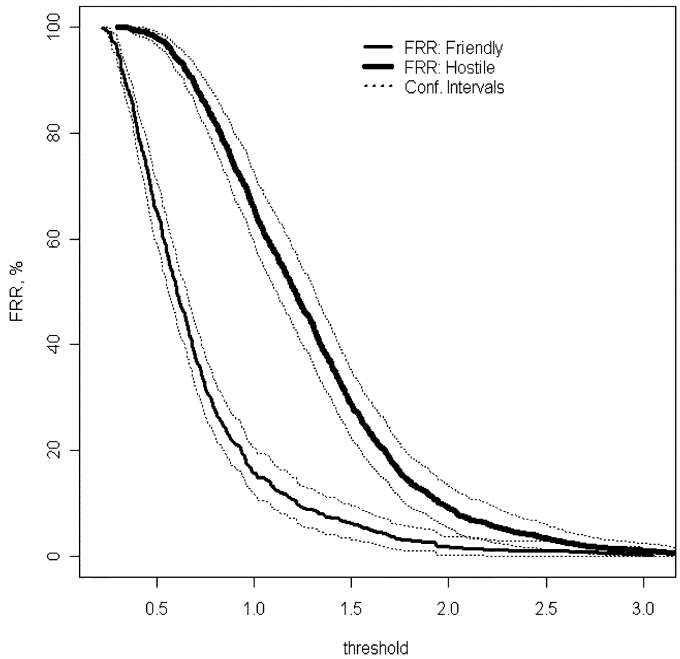

Fig. 11. FRR curves with 95% CI: Friendly scenario versus hostile scenario.

attackers did apparently change their walking style when they were mimicking. However, the impersonation did not help significantly, as can be seen from Figs. 9 and 10.

C. Results From the Hostile Scenario: Closest Target Attack

In addition to the minimal-effort impersonation attack, we studied the active impostor attack with preselecting the closest victim in the database (without mimicry). In other words, in this setting, the attacker had knowledge of his or her closest target in the database. As the database, we used gait data from the friendly scenario and the same attackers from minimal-effort

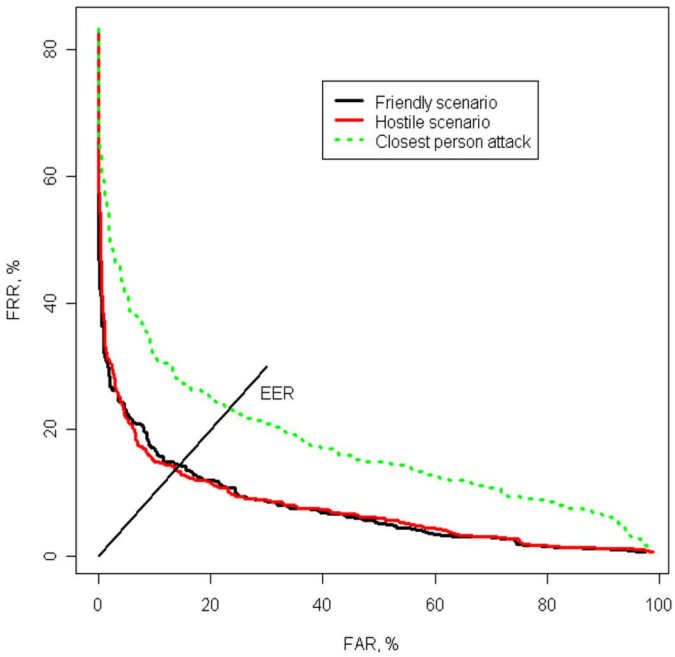

Fig. 12. DET: Attack with the knowledge of the closest person in the database and minimal effort mimicry.

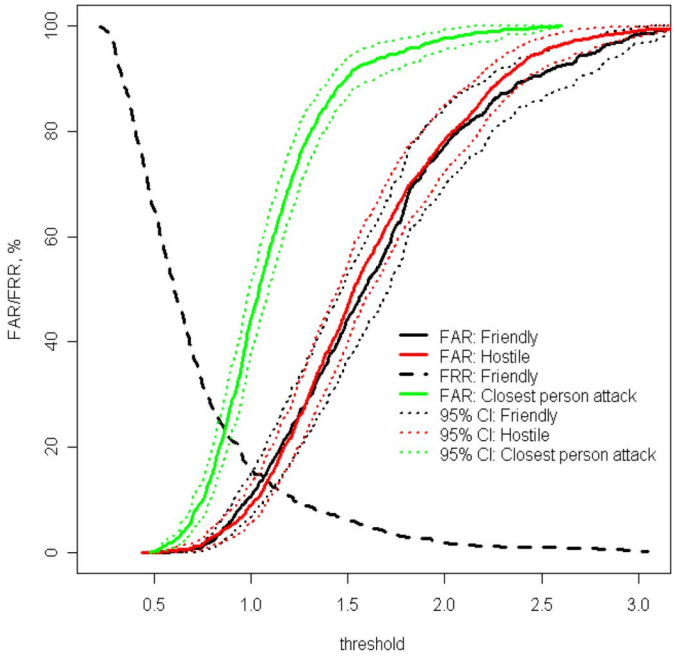

Fig. 13. FAR: Attack with the knowledge of the closest person in the database and minimal effort mimicry.

hostile scenario were used. At first, for every attacker, the closest target in the database (of 99 remaining subjects) was estimated. Then, for generating impostor scores, the natural walking of the attacker was compared to the natural walking of the closest target. For finding the closest target from the database, one of the attacker's walking sample was compared to the four samples of the people in the database, and the averaged score was used as a closeness indicator. The remaining three samples of the attacker were used for generating impostor scores for analysis. In our case, with $n = 90$ attackers and 12 $(= 3{\cdot}4)$ impostor scores per attacker, we obtained an active impostor set Z of cardinality 1080. Comparison plots of the attacks in this setting in terms of DET (computed based on the sets G and Z) and FAR (estimated using the set Z) curves are given in Figs. 12 and 13, respectively. These plots clearly indicate that an attacker with a knowledge of the closest target in the database can have significantly higher chances of being accepted by the system than the attacks with minimal-effort impersonation or passive attacks.

VI. Discussion

A. MV-Based and WS-Based Gait Recognitions

Usually, the performances of MV-based and FS-based gait recognition systems are reported in identification mode (one-to-many comparisons) with the WS-based gait system in authentication mode (one-to-one comparison). A general overview of several WS-based and MV-based gait recognition methods is given in Table III. In the table, columns EER, S#, and Class denote performance of the method in terms of EER, the number of subjects used in the experiment, and gait recognition category to which the approach belongs to, respectively. This table is not a complete list of works in gait recognition, and does not imply a direct comparison of methods (mainly due to differences among the gait data sets). Its primary purpose is to show general authentication performance of methods in biometric gait recognition. More on the current state of the art (available databases, performance accuracies, recognition methods, etc.) on MV-based biometric gait recognition can be found in a recent work by Nixon and Carter [41].

TABLE III
Performances of MV-Based and WS-Based Gait Recognition

Study	EER, %	S#	Class
BenAbdelkader et al. [27]	11	17	MV
Bazin et al. [28](before fusion)	7.3, 15.5, 23.3	115	MV
Wang et al. [29](before fusion)	8.42, 10	20	MV
Wang et al. [30]	8, 12, 14	20	MV
Ailisto et al. [12]	6.4	36	WS
Mäntyjärvi et al. [13]	7, 10, 18, 19	36	WS
Gafurov et al. [14]	5, 9	21	WS
This paper	13	100	WS

Apart from the analysis method and data set, the other technological differences between this work and previous WS-based person recognition approaches from Table III are:

- the sampling frequency of accelerometer sensor (in Hertz): 100 (this paper) versus 256 in [12], [13] and 16 in [14];
- acceleration directions: three directions (this paper) versus two directions in [12] and [13] and three (but different combination) in [14];
- sensor placement: hip (this paper) versus waist in [12] and [13] and lower leg in [14].

In [21], the performance of the recognition system was improved when WS-based gait and speaker recognition were integrated. In general, it might be possible to improve accuracy of the system by using more than one characteristic of gait and then fusing them [28], [29] or by integrating gait with other biometric modalities (e.g., voice [21] or face [42]). On the other hand, integration of gait with other biometrics can also enhance security, as it will be more difficult for an attacker to spoof several

biometrics simultaneously. Although WS-based (and FS-based too) gait recognition methods lack difficulties of MV-based approaches, such as background subtraction, lighting conditions, viewing angle, etc., they share common factors that can alter the gait of the person, for example, foot injury, aging, carrying loads, and so on.

It should be noted that a cycle-detecting procedure in our method depends on the signal (e.g., walking speed) and might not be applicable for other types of signals (e.g., too fast or too slow walking). For coping with these types of signals, more robust cycle detection procedures can be applied.

It is worth mentioning that WS-based gait analysis has been successfully used in clinical and medical settings to study and monitor patients with different locomotion disorders [36], [43]. In medical settings, such an approach is considered cheap and portable, compared to motion capture systems [35].

B. Security Strength Evaluations

To our knowledge, so far in the area of biometric gait recognition, no work has been reported that investigates the vulnerability of gait biometrics (except results reported in [26]). Our results indicate that on gait biometrics, the chances of accepting impostors by minimal effort mimicking the hostile scenario is not higher than the chances of impostors in the friendly scenario. In other words, whether an attacker imitates the target person by minimal effort mimicry or no mimicry at all (i.e., uses his or her natural gait to match), the performance is not influenced significantly. This may seem contrary to the intuition that mimicking should increase the chance of impostors being accepted. However, human gait is a complex process that involves nervous and musculo-skeletal systems [44]. When a person was told to walk as someone else, we believe he or she is given a restriction, since he or she has to walk differently from his or her normal habituated gait. Because of this, he or she may fail to produce natural gait patterns exactly as a target person. In addition, although global properties of gait (e.g., fast versus slow walking, short versus long steps, crippling) can be visually comprehended, it might not be an easy task to do the same with local properties of gait (e.g., net force accumulating acceleration in the hip). Another reason for failure might be due to the dissimilarities on physical characteristics (such as height or weight) between the attacker and target. However, it is worth noting that the role of such physical characteristics in gait recognition per se is not well investigated yet. For example, whether recognition performance is significantly better in a system where users have very dissimilar heights compared to the system where users have very similar heights. Therefore, we hypothesizes that "In general, the probability of false accept in the hostile scenario is not significantly higher than the probability of false accept in the friendly scenario when mimicking dynamic features of gait biometric by minimal effort impersonation attacks."

We emphasize the minimal effort as it is not known whether training can improve the performance of attackers. A system with feedback could be used for training. For instance, every time an attacker performs mimicking, the MR sensor gives an output as to whether the attempt was successful or not. An even better situation could be when the MR sensor periodically informs the attacker on how similar his or her walking is to the stored template rather than a simple "Accept/Reject" response. In this case, the attacker could try to adjust particular parts of his or her walking style. For example, in case of fingerprints, it was shown that with the knowledge of the similarity score returned by the matcher, an attack system was able to generate synthetic fingerprints to obtain a desired score to pass recognition [45].

Unlike gait biometrics, studies of impersonation attacks on voice [46] and handwritten signature [47] have been reported. It has been shown that the speaker verification system might be vulnerable to voice mimicry [46]. In their experiment, Lau *et al.* [46] used only two imitators—a male and a female. Each attacker mimicked voices of three targets from a database, whose voices were the closest, intermediate, and furtherest away from the attacker's voice. Attackers performed mimicking in four sessions. The results showed that an attacker can get a high chance of acceptance if he or she knows the closest speaker in the database, and performance improved at the later sessions [46]. In signature verification, impersonation attacks are usually divided into three categories: random forgery, where the attacker uses his or her own name and style (analogous to the passive attack in our case); simple forgery, where the attacker uses the name of target but own style (analogous to the active attack with minimal effort as in our case); and skilled forgery, where the attacker uses the name and style of the victim (analogous to the active attack with training). Every type of forgery may require a different recognition algorithm. In general, methods based on static features, extracted from the shape of the signature, can easily detect random and simple forgeries, although not skilled forgery. For example, Cha and Tappert [47] observed that subjects could successfully imitate others' handwriting in terms of shape and size, although dynamic features of the handwriting, such as speed and acceleration, were not possible to imitate. However, recent work suggests that even a signature verification system, which uses dynamic features, can be vulnerable to attacks. Ballard *et al.* [48] demonstrated that a generative model for a targeted user's handwriting can be developed which is based on static captured samples of the target and penstroke dynamics learned from general population statistics.

Despite the fact that a minimal effort mimicry does not help in gait authentication, our analysis indicates an attacker with knowledge of the closest person in the database can be a serious threat to the authentication system. Moreover, the attacker does not even have to impersonate his or her nearest target. Such a setting can be in the interest of those attackers who aim to merely pass a system by any account (which implies under the account of the closest user). In case an attacker aims to enter system under the account of a particular person, then impersonation with a training might be necessary (provided that training can help to improve chances of acceptance). It is worth noting that the other types of biometrics (e.g., speaker verification [46]) can be also vulnerable to the closest person attacks. This vulnerability might be related to the fact that difficulties on separating the genuine and impostor distributions. In case of voice or handwritten signature biometrics, for an attacker to estimate his or her closeness to the target in the database, the cooperation of the target might not be necessary (assuming the attacker knows the applied algorithm). For example, a voice recorder can be easily used without the person knowing his or her voice is being

recorded, or the previously recorded voice of the target can be used. It might also not be so difficult to find a piece of paper written by the target. However, in the case of WS-based gait recognition, the attacker should place a motion-recording sensor to the specific body segment of the targeted person, which might not be an easy task without not letting the target know.

VII. Conclusion and Future Work

Biometrics, such as voice, handwritten signature, keystroke dynamics, and gait can be vulnerable to impersonation attacks. This type of attack has already been investigated in the case of speaker and handwritten signature verifications. However, the impersonation attack has not received enough attention for gait and keystroke dynamics biometrics. In this paper, we evaluated the performance of WS-based gait recognition in two different scenarios, namely, friendly and hostile. In the friendly scenario, using gait data set from 100 subjects, we obtained the 13% EER and 73.2% recognition rate (i.e., identification probability at rank 1). In the hostile scenario, we investigated the security strength of gait biometrics against the minimal effort impersonation attack and attacks with the knowledge of the closest person in the database. Our findings indicate that a minimal effort impersonation attack on gait does not significantly increase the chances of impostors being accepted;, in general, the minimal-effort mimicry on gait biometrics may not help. However, an attacker with knowledge of the closest match in the database can be a serious threat to the gait authentication system.

In this work, we studied general robustness of the gait authentication system against attackers rather than evaluating the performance of individual attackers. The DET (likewise FAR/FRR) curves show the general performance of a biometric system, whereas in a real-life application, the biometric system functions only in one (or a few) points on the curve. In regards to attacks, for managers of the biometric system, it is very important to be aware of the systems thresholds (i.e., points in the curves) where the hostile FAR is significantly higher than the friendly FAR. This is essential during the decision-making process in order to decide under which threshold point the system should be operating.

It is still an open question as to whether training can improve attackers mimicking performance. In this paper, a one-to-one scenario—one attacker mimicking one target—was studied. It is also interesting to investigate situations when one attacker impersonates several targets, or one target is mimicked by several attackers. In such settings, it might be possible to identify which attackers mimic relatively better or which targets are relatively easy to attack; otherwise, in Doddington *et al.* [49] terms, whether any "lambs" or "wolves" users exist in gait biometrics. All of these open questions will constitute the basis of our future work.

Acknowledgment

The authors would like to thank H.P. Hornæs and the anonymous reviewers for their useful feedback and suggestions. The authors would also like to thank O.E. Wattne for his help on improving the quality of Fig. 5.

References

[1] C. BenAbdelkader, R. Cutler, H. Nanda, and L. Davis, "Eigengait: Motion-based recognition of people using image self-similarity," presented at the 3rd Int. Conf. Audio- and Video-Based Biometric Person Authentication, 2001.

[2] J. B. Hayfron-Acquah, M. S. Nixon, and J. N. Carter, "Automatic gait recognition by symmetry analysis," in *Audio- and Video-Based Biometric Person Authentication*, 2001, pp. 272–277.

[3] S. Sarkar, P. J. Phillips, Z. Liu, I. R. Vega, P. Grother, and K. W. Bowyer, "The humanID gait challenge problem: Data sets, performance, and analysis," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 27, no. 2, pp. 162–177, Feb. 2005.

[4] Y. Wang, S. Yu, Y. Wang, and T. Tan, "Gait recognition based on fusion of multi-view gait sequences," in *Proc. Int. Conf. Biometrics*, 2006, pp. 605–611.

[5] T. H. W. Lam and R. S. T. Lee, "A new representation for human gait recognition: Motion silhouettes image (MSI)," in *Proc. Int. Conf. Biometrics*, 2006, pp. 612–618.

[6] M. S. Nixon, T. N. Tan, and R. Chellappa, *Human Identification Based on Gait*. Berlin, Germany: Springer, 2006.

[7] A. Kale, A. Sundaresan, A. N. Rajagopalan, N. P. Cuntoor, A. K. Roy-Chowdhury, V. Kruger, and R. Chellappa, "Identification of humans using gait," *IEEE Trans. Image Process.*, vol. 13, no. 9, pp. 1163–1173, Sep. 2004.

[8] Z. Liu and S. Sarkar, "Improved gait recognition by gait dynamics normalization," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 28, no. 6, pp. 863–876, Jun. 2006.

[9] J. Han and B. Bhanu, "Individual recognition using gait energy image," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 2, pp. 316–322, Feb. 2006.

[10] R. J. Orr and G. D. Abowd, "The smart floor: A mechanism for natural user identification and tracking," presented at the Conf. Human Factors in Computing Systems, The Hague, The Netherlands, 2000.

[11] L. Middleton, A. A. Buss, A. Bazin, and M. S. Nixon, "A floor sensor system for gait recognition," in *Proc. 4th IEEE Workshop on Automatic Identification Advanced Technologies*, 2005, pp. 171–176.

[12] H. J. Ailisto, M. Lindholm, J. Mäntyjärvi, E. Vildjiounaite, and S.-M. Mäkelä, "Identifying people from gait pattern with accelerometers," in *Proc. SPIE Volume: 5779; Biometric Technology for Human Identification II*, 2005, pp. 7–14.

[13] J. Mäntyjärvi, M. Lindholm, E. Vildjiounaite, S.-M. Mäkelä, and H. J. Ailisto, "Identifying users of portable devices from gait pattern with accelerometers," presented at the IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Philadelphia, PA, 2005.

[14] D. Gafurov, K. Helkala, and T. Sondrol, "Gait recognition using acceleration from MEMS," in *Proc. 1st IEEE Int. Conf. Availability, Reliability and Security*, Vienna, Austria, Apr. 2006.

[15] X. Chen, J. Tian, Q. Su, X. Yang, and F. Y. Wang, "A secured mobile phone based on embedded fingerprint recognition systems," presented at the IEEE Int. Conf. Intelligence and Security Informatics, Atlanta, GA, May 2005.

[16] Q. Su, J. Tian, X. Chen, and X. Yang, "A fingerprint authentication mobile phone based on sweep sensor," in *Proc. 3rd Int. Conf. Advances in Pattern Recognition*, 2005, pp. 295–301.

[17] Y. Lee, C. Seo, J. Lee, and K. Y. Lee, "Speaker verification system for PDA in mobile-commerce," in *Web Communication Technologies and Internet-Related Social Issues—HSI 2003, Second Int. Conf. Human Society@Internet*, Seoul, Korea, Jun. 2003.

[18] C. C. Leung, Y. S. Moon, and H. Meng, "A pruning approach for gmm-based speaker verification in mobile embedded systems," in *Proc. 1st Int. Conf. Biometric Authentication*, Jul. 2004, pp. 607–613.

[19] Y. Ijiri, M. Sakuragi, and S. Lao, "Security management for mobile devices by face recognition," presented at the Int. Conf. Mobile Data Management, Nara, Japan, 2006.

[20] J.-L. Nagel, P. Stadelmann, M. Ansorge, and F. Pellandini, "Comparison of feature extraction techniques for face verification using elastic graph matching on low-power mobile devices," presented at the IEEE Region 8 EUROCON 2003 the Int. Conf. Computer as a Tool, Ljubljana, Slovenia, 2003.

[21] E. Vildjiounaite, S.-M. Mäkelä, M. Lindholm, R. Riihimäki, V. Kyllönen, J. Mäntyjärvi, and H. Ailisto, "Unobtrusive multimodal biometrics for ensuring privacy and information security with personal devices," in *Pervasive*. Berline, Germany: Springer-Verlag LNCS, 2006, pp. 187–201.

[22] N. L. Clarke and S. M. Furnell, "Authenticating mobile phone users using keystroke analysis," *Int. J. Inf. Security*, pp. 1–14, 2006.

[23] J. J. Lee, S. Noh, K. R. Park, and J. Kim, "Iris recognition in wearable computer," in *Proc. 1st Int. Conf. Biometric Authentication*, Jul. 2004, pp. 475–483.
[24] T. E. Starner, "Attention, memory, and wearable interfaces," *IEEE Pervasive Computing*, vol. 1, no. 4, pp. 88–91, Oct.–Dec. 2002.
[25] Mobile data security: Access, content, identity & threat management 2006–2011 Juniper-Research, 2006 [Online]. Available: http://www.juniperresearch.com.
[26] D. Gafurov, E. Snekkenes, and T. E. Buvarp, "Robustness of biometric gait authentication against impersonation attack," presented at the 1st Int. Workshop on Information Security OnTheMove Federated Conf. Montpellier, France, Oct. 30–Nov. 1, 2006.
[27] C. BenAbdelkader, R. Cutler, and L. Davis, "Stride and cadence as a biometric in automatic person identification and verification," in *Proc. 5h IEEE Int. Conf. Automatic Face and Gesture Recognition*, May 2002, pp. 357–362.
[28] A. I. Bazin, L. Middleton, and M. S. Nixon, "Probabilistic fusion of gait features for biometric verification," presented at the 8th Int. Conf. Information Fusion, Philadelphia, PA, 2005.
[29] L. Wang, H. Ning, T. Tan, and W. Hu, "Fusion of static and dynamic body biometrics for gait recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 2, pp. 149–158, Feb. 2004.
[30] L. Wang, T. Tan, W. Hu, and H. Ning, "Automatic gait recognition based on statistical shape analysis," *IEEE Trans. Image Process.*, vol. 12, no. 9, pp. 1120–1131, Sep. 2003.
[31] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp. 125–143, Jun. 2006.
[32] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *Proc. 3rd Int. Conf. Audio- and Video-Based Biometric Person Authentication*, Jun. 2001, pp. 223–228.
[33] D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, "Fake fingerprint detection by odor analysis," in *Proc. Int. Conf. Biometrics*, 2006, pp. 265–272.
[34] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake finger detection by skin distortion analysis," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 3, pp. 360–373, Sep. 2006.
[35] D. Alvarez, R. C. Gonzalez, A. Lopez, and J. C. Alvarez, "Comparison of step length estimators from weareable accelerometer devices," in *Proc. 28th Annu. Int. Conf. IEEE on Engineering in Medicine and Biology Soc.*, Aug. 2006, pp. 5964–5967.
[36] M. Sekine, Y. Abe, M. Sekimoto, Y. Higashi, T. Fujimoto, T. Tamura, and Y. Fukui, "Assessment of gait parameter in hemiplegic patients by accelerometry," in *Proc. 22nd Annu. Int. Conf. IEEE Engineering in Medicine and Biology Society*, 2000, pp. 1879–1882.
[37] J. L. Wayman, "Confidence interval and test size estimation for biometric data," presented at the IEEE Workshop on Automatic Identification Advanced Technologies, Summit, NJ, 1999.
[38] P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss, "The FERET evaluation methodology for face-recognition algorithms," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 22, no. 10, pp. 1090–1104, Oct. 2000.
[39] R. M. Bolle, N. K. Ratha, and S. Pankati, "Error analysis of pattern recognition systems—The subsets bootstrap," *Comput. Vis. Image Understanding*, 2004.
[40] R. M. Bolle, N. K. Ratha, and S. Pankati, "Evaluating authentication systems using bootstrap confidence intervals," in *Proc. IEEE Workshop on Automatic Identification Advanced Technologies*, Oct. 1999, pp. 9–13.
[41] M. S. Nixon and J. N. Carter, "Automatic recognition by gait," *Proc. IEEE*, vol. 94, no. 11, pp. 2013–2024, Nov. 2006.
[42] X. Zhou and B. Bhanu, "Integrating face and gait for human recognition," presented at the Conf. Computer Vision and Pattern Recognition Workshop, New York, Jun. 2006.
[43] F. Horiuchi, R. Kadoya, Y. Higasi, T. Fujimoto, M. Sekine, and T. Tamura, "Evaluation by accelerometry of walking pattern before falls in hemiplegic patients," in *Proc. IEEE 23rd Annu. Int. Conf. Engineering in Medicine and Biology Soc.*, 2001, pp. 1153–1154.
[44] V. Christopher, D. Brian, and O. Jeremy, *Dynamics of Human Gait*. Cape Town, South Africa: Kiboho, 1999.
[45] U. Uludag and A. K. Jain, "Attacks on biometric systems: A case study in fingerprints," in *Proc. SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents VI*, Jan. 2004, pp. 622–633.
[46] W. L. Yee, M. Wagner, and D. Tran, "Vulnerability of speaker verification to voice mimicking," in *Proc. Int. Symp. Intelligent Multimedia, Video and Speech Processing*, Oct. 2004, pp. 145–148.
[47] C. Sung-Hyuk and C. C. Tappert, "Automatic detection of handwriting forgery," in *Proc. 8th Int. Workshop on Frontiers in Handwriting Recognition*, Aug. 2002, pp. 264–267.
[48] L. Ballard, D. Lopresti, and F. Monrose, "Evaluating the security of handwriting biometrics," presented at the 10th Int. Workshop on Frontiers in Handwriting Recognition, La Baule, France, Oct. 2006.
[49] G. Doddington, W. Liggett, A. Martin, M. Przybocki, and D. Reynolds, "Sheep, goats, lambs and wolves a statistical analysis of speaker performance in the NIST 1998 speaker recognition evaluation," presented at the 5th Int. Conf. Spoken Language Processing, Sydney, Australia, 1998.

Davrondzhon Gafurov received the M.Sc. degree in computer engineering from Technological University of Tajikistan (TUT), Khujand, Tajikistan, in 2000 and is currently pursuing the Ph.D. degree in information security at Norwegian Information Security Lab (NISLab), Gjøvik University College, Gjovik, Norway.

He was an Engineer–Programmer with the Computer Center of Technological University of Tajikistan (CCTUT) and a Part-Time Lecturer with the Department of Programming and Information Technology at TUT from 2000 to 2004. He was also a Fellow with the International Institute for Software Technology, United Nations University (IIST/UNU) in 2001. His research interests include biometrics, security analysis of biometrics, and human movement analysis for security applications.

Einar Snekkenes (M'02) received the B.Sc. (Hons.) degree in computation from the University of Manchester Institute of Science and Technology, Manchester, U.K., in 1986 and the Dr Phil. degree in informatics from Oslo University, Oslo, Norway, in 1995.

Currently, he is Professor of Information Security with the Norwegian Information Security Laboratory, Gjøvik University College, Gjovik, Norway. Previously, he was a Research Scientist with Alcatel and the Norwegian Defense Research Establishment (FFI), Oslo, and Research Director with the Norwegian Computing Center, Oslo. He has published papers on topics, such as the analysis of cryptographic protocols, biometrics, and social engineering. His current research interests include authentication and modeling and analysis relating to information security.

Dr. Snekkenes has served on many committees, including the Norwegian Research Council, ICT security, and vulnerability.

Patrick Bours received the M.Sc. and Ph.D. degrees in mathematics from Eindhoven University of Technology, Eindhoven, The Netherlands, in 1990 and 1994, respectively.

He was a Senior Policy Maker in the area of cryptology with the Netherlands National Communications Security Agency (NLNCSA) for 10 years. During this period, he was involved in various national and international working groups on cryptology. Currently, he is Associate Professor with the Norwegian Information Security Laboratory at Gjøvik University College, Gjovik, Norway. His current interests include biometrics and authentication.