Performance and Security Analysis of Gait-based User Authentication

Doctoral Dissertation by

Davrondzhon Gafurov

Submitted to the Faculty of Mathematics and Natural Sciences at the University of Oslo in partial fulfillment of the requirements for the degree Philosophiae Doctor (PhD) in Computer Science

2008

Abstract

Verifying the identity of a user, usually referred to as user authentication, before granting access to the services or objects is a very important step in many applications. People pass through some sorts of authentication process in their daily life. For example, to prove having access to the computer the user is required to know a password. Similarly, to be able to activate a mobile phone the owner has to know its PIN code, etc. Some user authentication techniques are based on human physiological or behavioral characteristics such as fingerprints, face, iris and so on. Authentication methods differ in their advantages and disadvantages, e.g. PIN codes and passwords have to be remembered, eye-glasses must be taken off for face authentication, etc. Security and usability are important aspects of user authentication. The usability aspect relates to the unobtrusiveness, convenience and user-friendliness of the authentication technique. Security is related to the robustness of the authentication method against attacks.

Recent advances in electronic chip development offer new opportunities for person authentication based on his gait (walking style) using small, light and cheap sensors. One of the primary advantages of this approach is that it enables unobtrusive user authentication. Although studies on human recognition based on gait indicate encouraging performances, the security per se (i.e. robustness and/or vulnerability) of gait-based recognition systems has received little or no attention.

The overall goal of the work presented in this thesis is on performance and security analysis of gait-based user authentication. The nature of the contributions is not on developing novel algorithms, but rather on enhancing existing approaches in gait-based recognition using small and wearable sensors, and developing new knowledge on security and uniqueness of gait.

The three main research questions addressed in this thesis are: (1) What are the performances of recognition methods that are based on the motion of particular body parts during gait? (2) How robust is the gait-based user authentication? (3) What aspects do influence the uniqueness of human gait?

In respect to the first research question, the thesis identifies several locations on the body of the person, whose motion during gait can provide identity information. These body parts include *hip*, *trouser pockets*, *arm* and *ankle*. Analysis of acceleration signals indicates that movements of these body segments have some discriminative power. This might make these modalities suitable as an additional factor in multi-factor authentica-

tion.

For the research question on security as far as we know, this thesis is the first extensive analysis of gait authentication security (in case of hip motion). A gait-based authentication system is studied under three attack scenarios. These attack scenarios include a minimal effort-mimicry (with restricted time and number of attempts), knowing the closest person in the database (in terms of gait similarity) and knowing the gender of the user in the database. The findings of the thesis reveal that the minimal effort mimicking does not help to improve the acceptance chances of impostors. However, impostors who know their closest person in the database or the genders of the users in the database can be a threat to gait-based authentication systems.

In the third research question, the thesis provides some insights towards understanding the uniqueness of gait in case of ankle/foot motion. In particular, it reveals the following: heavy footwear tends to diminish foot discriminativeness; a sideway motion of the foot provides the most discrimination, compared to an up-down or forward-backward direction of the motion; and different parts of the gait cycle provide different level of discrimination.

In addition, the thesis proposes taxonomy of user recognition methods based on gait.

Acknowledgments

The research resulting in the present thesis has been carried out at Norwegian Information Security Lab (NISLab), Department of Computer Science and Media Technology, Gjøvik University College (GUC), Norway. The support provided by the Research Council of Norway is acknowledged[1]. Retoma AS provided a free copy of their software, which was used for transferring data from some sensors to the computer.

I would like to express my gratitude to the following people for supporting this work with criticism, encouragement and helpful assistance. First of all, I'd like to thank my advisor Professor Einar Snekkenes for accepting me as a PhD student, encouraging me to work hard and being very supportive during our collaboration. My co-advisor Professor Chunming Rong also provided useful comments on the thesis. I am also very grateful to the head of our research group Associate Professor Erik Hjelmås for creating a nice working environment and helping to tackle many administrative problems I came across around the College and Gjøvik town. My gratitude also goes to Associate Professor Patrick Bours and PhD student Kirsi Helkala for interesting discussions and exchange of ideas. In addition, advices and comments provided by Professor Stephen Wolthusen, Professor Slobodan Petrovic, Professor Chik How Tan, Professor Christoph Busch and Associate Professor Katrin Franke are appreciated. I also enjoyed interesting "lunch-talks" during which I got answered to many of my questions regarding life in Gjøvik and Norway from other colleguaes at GUC - Tor Arne, Nils, Geir Olav, Lasse, Hanno, Frode, Knut, Vitaliy, Andrei, Jeremie, Janne and many others. Also, many thanks go to Torkjel Søndrol from Retoma AS for providing assistance with the transfer program. Several persons from Tajikistan also somehow inspired me on working towards my PhD, they are: Abduhafiz Azizov, Professor Muhammadiev E., Professor Usmanoz Z., Dr. Maksudov A., Dr. Maksudov Kh., Dr. Ganiev M. and Professor Pulatov P. I am also grateful to many volunteers who participated in the research experiments carried our during this work. Last but not least, I am very grateful to my family, my parents and my wife, for always supporting me and being patient while I was working on the thesis.

[1]Grant number is NFR158605/V30(431) ("Security of approaches to personnel authentication").

List of papers

The 8 research papers that constitute the main research part of the thesis are:

1. Davrondzhon Gafurov, **A Survey of Biometric Gait Recognition: Approaches, Security and Challenges**, In *Proceedings of Annual Norwegian Computer Science Conference*, Tapir, pp. 119-130, 2007.

2. Davrondzhon Gafurov, Kirsi Helkala and Torkjel Søndrol, **Gait Recognition Using Acceleration from MEMS**, In *Proceedings of IEEE International Conference on Availability, Reliability and Security (ARES)*, pp. 432-437, 2006.

3. Davrondzhon Gafurov, Einar Snekkenes and Patrick Bours, **Gait Authentication and Identification Using Wearable Accelerometer Sensor**, In *Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies (AutoID)*, pp. 220-225, 2007.

4. Davrondzhon Gafurov and Einar Snekkenes, **Arm Swing as a Weak Biometric for Unobtrusive User Authentication**, In *Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Special Session on "Biometrics - From Sensors to Standardization", IEEE Press, 2008 (accepted).

5. Davrondzhon Gafurov, Einar Snekkenes and Tor Erik Buvarp, **Robustness of Biometric Gait Authentication Against Impersonation Attack**, In *Proceedings of International Workshop on Information Security*, Springer LNCS 4277, pp. 479-488, 2006.

6. Davrondzhon Gafurov, Einar Snekkenes and Patrick Bours, **Spoof Attacks on Gait Authentication System**, *IEEE Transactions on Information Forensics and Security*, Special Issue on Human Detection and Recognition, 2(3), pp. 491-502, 2007

7. Davrondzhon Gafurov, **Security Analysis of Impostor Attempts with Respect to Gender in Gait Biometrics**, In *Proceedings of IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, 2007.

8. Davrondzhon Gafurov and Einar Snekkenes, **Towards Understanding the Uniqueness of Gait Biometric**, *to be submitted.*

In addition, the thesis work has also resulted in the follwoing paper which is closely related or overlapping with papers mentioned above.

- Davrondzhon Gafurov, Kirsi Helkala and Torkjel Søndrol, **Biometric Gait Authentication Using Accelerometer Sensor**, *Journal of Computers*, 1(7), pp. 51-59, 2006

Thesis Structure

The thesis consists of two parts. Part I is an introduction to user recognition based on gait and a summary of the thesis contributions. After introduction to user authentication, motivation and biometric system, Chapter 1 presents the current overview of human recognition based on gait. Chapter 2 contains short summaries of each individual paper of the thesis. Chapter 3 presents the overall contributions of the thesis with directions for future work. Part II of the thesis consists of eight articles describing the research work of the thesis. Six of these papers have been published in peer-reviewed journal or conferences, one has been accepted for publication on a conference and one has a status of "to be submitted".

Contents

Part I

Introduction

1 User Authentication Using Gait

This chapter presents an overview of user authentication based on gait. Section 1.1 is a short introduction to user authentication. Next, Section 1.2 contains motivation for the work. A brief description of biometric systems is given in Section 1.3. Section 1.4 presents the current overview of biometric gait recognition with emphasis on approaches using wearable sensors.

1.1 User Authentication

Verifying the identity of a user, usually referred to as user authentication, before granting access to the services, objects, locations etc. is a very important step in almost all kinds of applications such as access control, border control, immigration and so on. Conventionally, user authentication mechanisms are based on something user: knows (knowledge-based), has (token-based) or *is* (biometrics). In a knowledge-based approach, authentication is based on a secret that is shared between a user and a system [1]. An example of such secret can be a password or PIN (Personal Identification Number) code. In token-based authentication, user is authenticated by possessing and presenting a token to the system [2]. An example of the token can be a key or access card used to open a door. Biometric authentication uses physiological and/or behavioural characteristics of the human being [3]. Traditional examples of human characteristics that are used as biometrics include fingerprints [4], face [5], iris [6], voice [7] handwriting [8], etc. Recently, new types of human characteristics like gait [9], typing rhythm [10], mouse usage [11], brain activity signal [12], cardiac sounds [13], foot geometry [14] and so on have been proposed for use as biometrics. The main motivation behind these new biometrics is in being better suited in some application settings compared to the traditional ones. For instance, gait can be captured from a relatively long distance while fingerprint or iris is difficult or impossible to acquire.

Although knowledge-based authentication is relatively easy and cheap to implement, it possesses usability limitations such as memorizing and recalling random passwords/PINs and managing multiple passwords/PINs. In addition, both passwords/PINs and tokens can be lost, forgotten or stolen. Biometric authentication lacks aforementioned drawbacks of the knowledge-based and token-based authentication. The most

important aspect of biometric authentication is establishing a more direct and explicit link to the identity due to its reliance on human features.

1.2 Motivation for the Work

People pass through some sorts of authentication process in their daily life. For example, to prove having access to the computer the user is required to know a password. Similarly, to be able to activate a mobile phone the owner has to know its PIN code, etc. Biometric authentications are also becoming popular in various applications, e.g. commercial [15], border control [16], etc. Authentication methods differ in their advantages and disadvantages, e.g. PIN codes and passwords have to be remembered, fingers must be clean in fingerprint authentication, etc. Security and usability are important aspects of user authentication. The usability aspect relates to the unobtrusiveness, convenience and user-friendliness of the authentication technique. Security is related to the robustness of the authentication method against attacks.

In some applications, increased services may increase the associated risks. For example, thanks to rapid increase of memory space and computational power in mobile phones, their services go beyond mere voice communication; more and more users store their personal and private data (images, videos etc.) in them. Furthermore, mobile phones are being used in high security applications such as mobile banking or commerce [17, 18]. All of these increase the risk of being the target of an attack not only because of the phone value per se but also because of the stored information and provided services.

Protection mechanisms in most mobile phones are based on PIN codes. The user authentication mechanism is static (i.e. single-time) and obtrusive (i.e. requires an explicit action from the user). That is, a user authenticates once by entering a PIN code. Authentication lasts until the device is turned off. In addition, mobile phones are not always under the attention of their owners, e.g. some people tend to forget, leave unattended or even lose them. Surveys of mobile phone users indicate that users do not follow the relevant security guidelines, for example they do not change their PIN codes regularly or use the same code for multiple services [19]. Furthermore, British crime survey for 2005/06 reported that estimated 800000 owners had experienced mobile phone theft and over two-thirds (69%) of the thefts happened when the phones were left unattended [20]. For combating such crimes and improving security in mobile phones, a periodic re-verification of the authenticated user is highly desirable. Periodic re-verification will ensure the correct identity throughout the phone usage. An important aspect of the re-verification procedure is to be *unobtrusive*, such that users will accept it. Apart from usability limitations associated with knowledge-based authentication [21, 22], they are difficult or impossible to adapt for periodic and unobtrusive re-authentication. Indeed, the process of frequently entering a PIN code into a mobile phone is explicit, requires user cooperation and can be very inconvenient and annoy-

ing. Therefore, better mechanisms for unobtrusive and periodic user authentication in mobile phones are desirable.

Recent advances in electronic chip development offers new opportunities for person authentication based on one's gait using small, cheap and light sensors. In such approach, gait is recorded by the sensors, which are attached or carried on various locations on the user's body. The recorded motion is then analysed for person recognition. The motion recording sensors can be integrated within clothes of the user or with mobile phone hardware itself (some phones already have such sensor [23]). One of the primary advantages of this approach is in providing a mechanism for unobtrusive and periodic identity (re-)verification, which makes it a suitable candidate to apply for improving user authentication in mobile phones. For instance, whenever a user makes a few steps his identity is re-verified implicitly in an unobtrusive way. Although many different methods with encouraging performances have been proposed for gait recognition, the security per se (i.e. robustness and/or vulnerability against attack) of a gait-based user authentication has not received much attention.

1.3 Biometric Systems

In biometric systems, registration of a new user is performed in an enrolment stage while verification of the user's identity is carried out in a verification stage. In the enrolment stage, the system acquires biometric data from a user; pre-processes the acquired data (e.g. noise reduction); extracts a set of features from the data (e.g. minutia from a fingerprint image); and stores the extracted feature set as a template in the database. In the verification stage, the same steps as in the enrolment are performed except the last one. In verification, instead of storing the extracted feature set, it is compared against a template feature set in the database to verify the claimed identity. The decision (accept or reject) is made based on a similarity between the acquired and template feature sets using a threshold value. An example of biometric system is presented in Figure 1.1. Depending on the application, a biometric system can operate in identification mode too. In this mode, the system either establishes the identity of an unknown sample or announces no match by comparing the unknown sample to all templates in the database. In other words, the verification searches for the answer to the question "Am I who I claim I am?" (one-to-one comparison), while the identification seeks the answer to the question "Who am I?" (one-to-many comparisons). In the thesis, we will use the term "recognition" when referring to both verification and identification. In addition, a biometric system can function in a negative identification mode, where the system establishes whether the person is who (s)he denies to be [24].

In a verification attempt, if the test (i.e. sample being verified) and template biometric samples are from the same individual, then the attempt is referred to as a genuine attempt. If the test and template biometric samples originate from different individuals

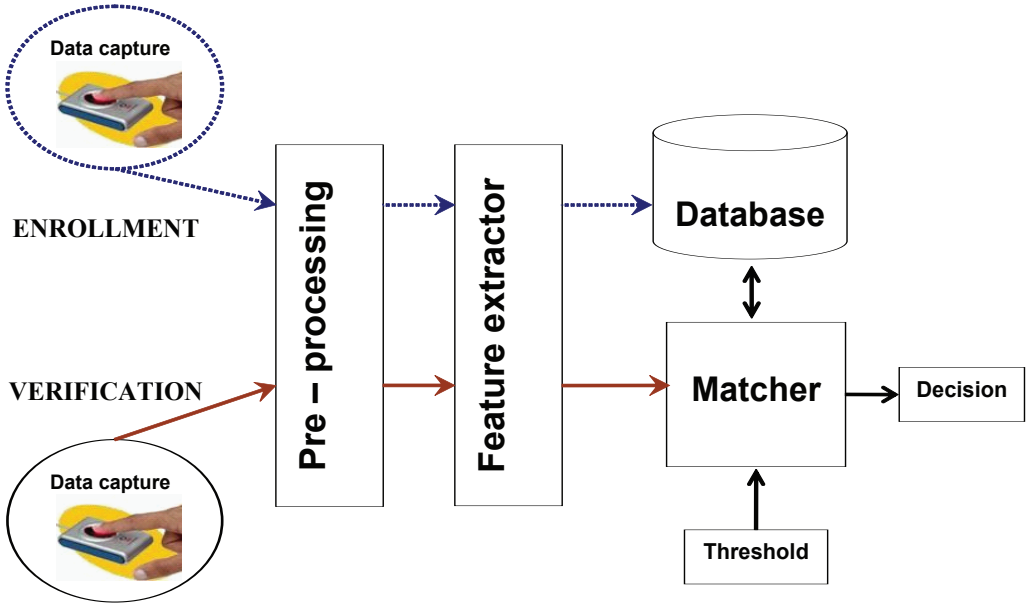

Figure 1.1: An example of biometric system architecture.

then it is referred to as an impostor attempt. Consequently, similarity scores produced by the matcher are referred to as the genuine and impostor scores.

Variability of human biometric signals due to many different types of factors (e.g. dry fingers in fingerprinting, background noise in speaker verification, illuminations in face recognition, etc.) poses challenges to biometric system and makes it non error-free. There are several types of errors associated with biometrics system. The main two of them are FAR (False Accept Rate) and FRR (False Reject Rate)[1]. The FAR value is the probability of wrongfully accepting an impostor, while the FRR represents a probability of wrongfully rejecting a genuine user. The FAR and FRR are estimated using the impostor and genuine scores based on a threshold value. The illustration of the genuine and impostor distributions, FAR, FRR and the threshold is shown in Figure 1.2. Their mathematical relationships are given by Formulas 1.1 and 1.2:

$$FAR = \int_{-\infty}^{t_0} p_{imp}(t)\, dt \tag{1.1}$$

$$FRR = \int_{t_0}^{+\infty} p_{gen}(t)\, dt \tag{1.2}$$

where p_{imp}, p_{gen} and t_0 are the impostor and genuine distribution functions and threshold

[1]For simplicity we do not make a distinction between FAR/FRR and FMR (False Match Rate)/$FNMR$ (False Non-match Rate).

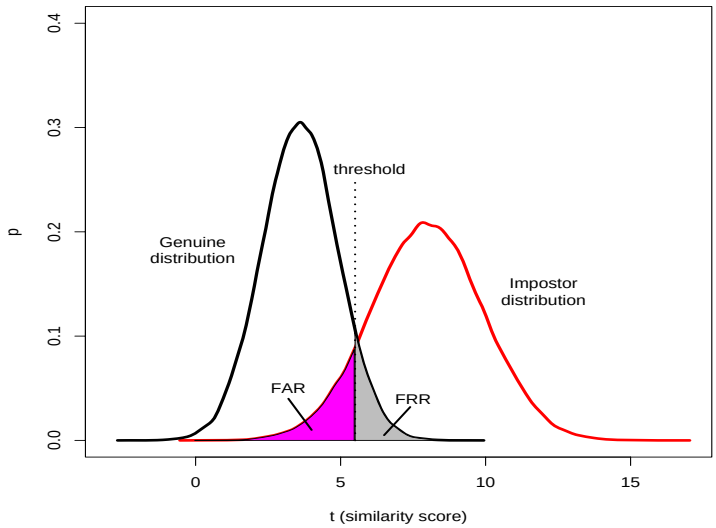

Figure 1.2: An illustration of the genuine and impostor distributions, FAR, FRR and threshold relationships.

value, respectively [2]. Empirically, FAR and FRR can be estimated as follow:

$$FAR = \frac{Number\ of\ accepted\ \ impostor\ attempts}{Total\ number\ of\ impostor\ attempts} \tag{1.3}$$

$$FAR = \frac{Number\ of\ rejected\ \ genuine\ attempts}{Total\ number\ of\ genuine\ attempts} \tag{1.4}$$

It is also useful to know confidence intervals for FAR and FRR. Parametric and non-parametric techniques have been proposed for computing confidence intervals for FAR and FRR [24, 25, 26]. Parametric techniques assume that underlying distribution of the genuine and impostor scores are known, and generated scores are independent [25]. However, such assumptions do not generally hold, e.g. biometric samples from the same person are not independent. Bolle et al. [26] proposed a non-parametric subset bootstrap technique for calculating confidence intervals for FAR and FRR, which makes no assumption about score distributions and also accounts for dependence between biometric samples. The other errors related to the biometric system are a FTE (Failure To Enrol) and a FTA (Failure To Acquire). The FTE is the proportion of the target population for whom a biometric system fails to complete enrolment process [27]. The FTA is the probability of failing to capture/locate image or signal of sufficient quality in verification (or identification) attempts [27].

Often, to report the performance of biometric system in verification mode a DET (Decision Error Trade-off) curve is used [28]. The DET curve is a plot of FAR versus

[2] FAR and FRR are functions of the threshold, i.e. FAR_{t_0} and FRR_{t_0}, but for notational simplicity we omit subscripts.

FRR which shows performance of biometric system under different threshold values. An example of the DET curve is shown in Figure 1.3. The closer the curve is to the origin, the better is the performance of the system. Depending on application requirements (e.g. high, medium or low security), one can select a relevant threshold (i.e. point on the curve), where the biometric system should function. For example, in applications where security is a main concern one is interested in low FAR rather than low FRR, while in the applications where usability is a primary concern one may be interested in low FRR. Usually, to express the performance of a biometric system by a single value, an EER (Equal Error Rate) is used. The EER is a point on the DET curve, where FAR = FRR (see Figure 1.3). Sometimes a TER (Total Error Rate) can also be used as a single value indicator of biometric performance [29]. The TER is a point on the curve where sum of FAR and FRR is minimal. To report the performance of a biometric

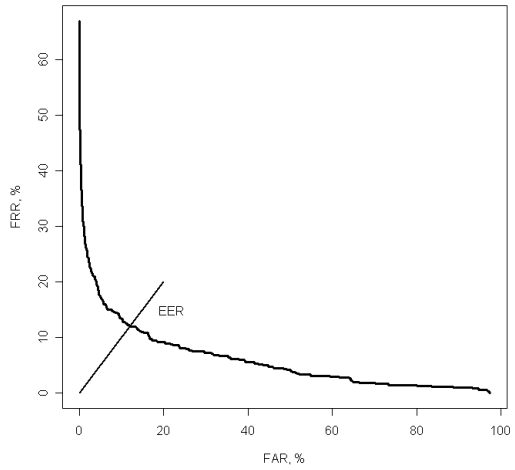

Figure 1.3: An example of a DET curve.

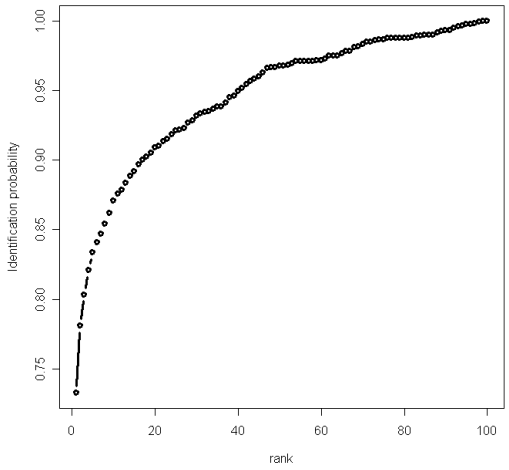

Figure 1.4: An example of a CMC curve.

system in identification mode, a CMC (Cumulative Match Characteristic) curve can be used. The CMC curve is a plot of identification probability versus rank [30] (see Figure 1.4). It indicates a cumulative probability of an unknown sample being within the top closest matches. In this case, to indicate the performance of the system by a single value an identification probability at rank 1 (or recognition rate) can be used.

1.4 Biometric Gait Recognition

Gait is a person's manner of walking [31]. Human gait is a complex biological process that involves nervous and musculo-skeletal systems [32]. Normal human gait is a cyclic process which can be decomposed into several subevents as shown in Figure 1.5.

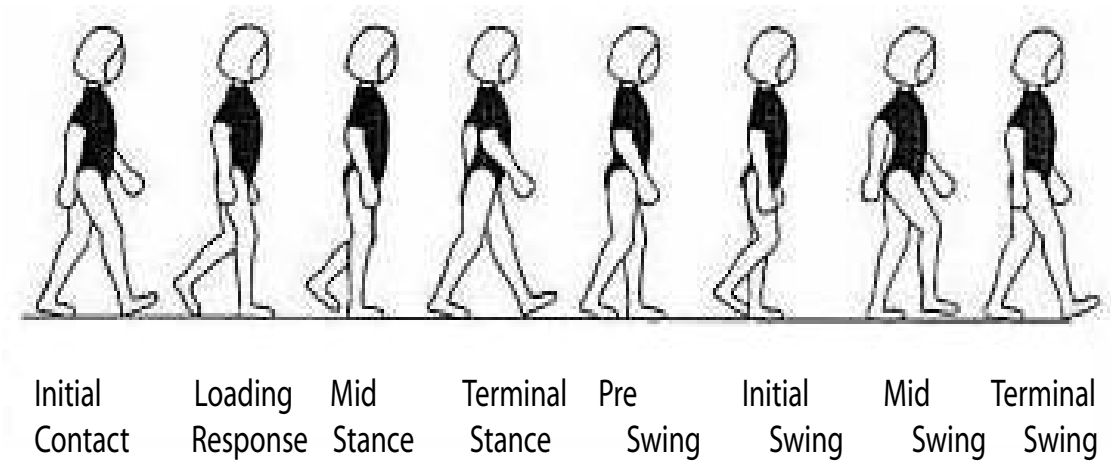

Figure 1.5: Human gait cycle based on the right foot motion from [35].

Early medical studies indicated that gait patterns appeared to be unique to each person [33, 34]. Biometric gait recognition, or simply gait recognition, refers to automatic verification and identification of individuals based on their gait. Recently, gait recognition became an active research direction in biometrics [9, 36]. The primary advantages of gait biometric over other types of biometrics are its unobtrusive way of data collection and that it can be captured from a distance when other types of biometric are inaccessible or obscured [9, 36].

1.4.1 Approaches in Gait Recognition

Techniques in gait recognition can be divided into two groups: model-based and model-free (feature based). Model-based techniques use static and dynamic body parameters and create models of the human body [37, 38, 39]. Model free techniques do not construct a structural model of the human gait, and essentially extract features from the silhouette sequences [40, 41]. From a technological perspective, biometric gait recognition can be categorized into three approaches (which is proposed in Paper 1 [42] of the thesis):

- Machine Vision (MV) based,
- Floor Sensor (FS) based,
- Wearable Sensor (WS) based.

In MV-based approach, gait is captured from a distance using a video-camera and then image/video processing techniques are applied to extract gait related data for recognition (see Figure 1.6) [43, 9, 36]. Earlier works on MV-based gait recognition showed

very promising results, usually with small data sets [44, 45]. For example, Hayfron-Acquah et al. [45] with the database of 16 gait samples from 4 subjects and 42 gait samples from 6 subjects achieved correct classification rates of 100% and 97%, respectively. More recent studies with larger sample sizes including more than 100 persons in the experiments, confirm that gait has distinctive patterns from which individuals can be recognized [40, 46, 47, 9]. For instance, Sarkar et al. [40] with a data set consisting of 1870 gait sequences from 122 subjects obtained 78% identification rate at rank 1 (experiment B). This performance was even improved further to achieve about 90% in other works [48, 49]. Possible application areas for MV-based gait recognition can be in surveillance and forensic applications [50, 51]. A significant amount of research in the area of gait recognition is devoted to the MV-based gait recognition [9, 36, 52, 53, 54]. One reason for much interest in MV-based gait category is availability of large public gait databases, such as the one provided by University of South Florida [40], University of Southampton [55] and Chinese Academy of Sciences [56]. For more information on databases, algorithms and performances in MV-based gait recognition interested readers are referred to [9].

In the FS-based approach, a set of sensors are installed in the floor (see Figure 1.7) and gait related data are measured when people walk on them [57, 58, 59, 60]. The FS-based gait recognition approach enables capture of some gait related data, which are impossible or difficult to collect in MV-based approaches, such as GRF (Ground Reaction Force) [57], heel to toe ratio [59], etc. A brief performance overview of a few FS-based gait recognition works (in terms of recognition rate and number of subjects in the database - last column) is presented in Table 1.1. In this table, although recognition rates are encouraging, the number of subjects used in experiments is very small (except in [60]). Possible application for FS-based gait recognition can be in smart environments where it implements access control to a building/office using a sensor mat in front of the door. Such systems can find deployment as a standalone system or as a part of a multimodal biometric system [59]. In addition to providing identity information, the FS-based gait system can also indicate location information within a building [57].

1.4.2 WS-based Gait Recognition

The WS-based gait recognition is relatively new compared to the other two mentioned approaches. In the WS-based approach, motion recording sensors (MRS) are worn or attached to various locations on the body of the person, such as the waist (see Figure 1.8), pockets (see Figure 1.9), shoes (see Figures 1.10 and 1.11) etc. [64, 29, 65, 66, 67, 68, 69]. The movement recorded by the MRS is then used for recognition purposes. Different types of sensors like accelerometers, gyro sensors, force sensors, etc. can be used for recording motion.

Previously, the WS-based gait analysis has been used successfully in clinical and med-

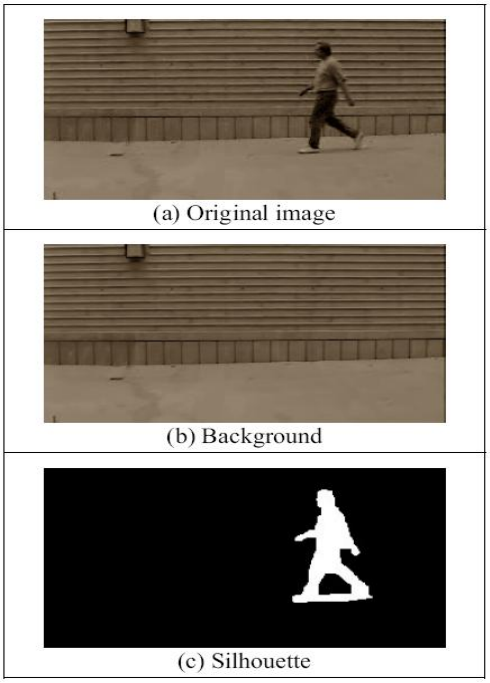

Figure 1.6: An example of silhouette extraction from [43].

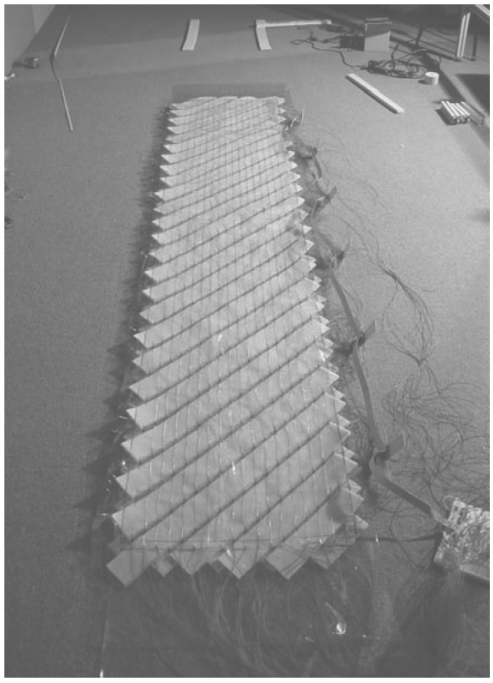

Figure 1.7: A prototype sensor mat from [59].

Figure 1.8: Sensor placement in [29].

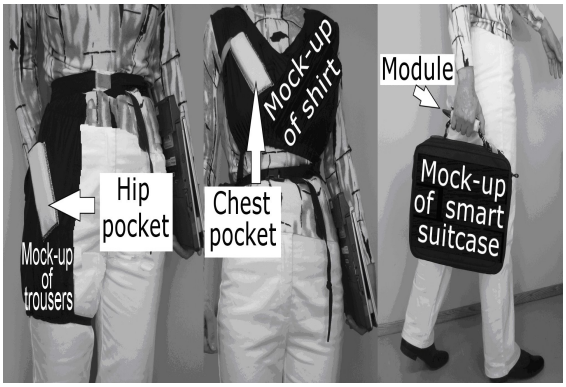

Figure 1.9: Sensor placement in [66].

ical settings to study and monitor patients with different locomotion disorders [70, 71]. In medical settings, the approach is considered to be cheap and portable, compared to the stationary vision based systems [72]. Despite successful application of WS-based gait analysis in clinical settings, only recently the approach has been applied for person recognition. Therefore, so far little has been published in the area of person recognition using WS-based gait analysis. A short summary of the current WS-based gait recognition studies is presented in Table 1.2 [3]. In this table, the last two columns are sampling

[3]In the table, in Vildjiounaite et al. [66] performance of gait recognition is given without fusion.

Study	*Recognition rate, %*	*#S*
Nakajima et al. [61]	85	10
Suutala and Röning [58]	65.8-70.2	11
Suutala and Röning [62]	79.2-98.2	11
Suutala and Röning [63]	92	10
Middleton et al. [59]	80	15
Orr and Abowd [57]	93	15
Jenkins and Ellis [60]	39	62

Table 1.1: A short summary of several FS-based gait recognitions.

Figure 1.10: Shoe with integrated sensors in [64].

Figure 1.11: Shoe with integrated sensors in [67].

frequency of accelerometer sensor (samples per second) and number of subjects used in experiments, respectively. The works listed in this table have been published in the period of 2004-2007. Although the work by Morris [64] was published first in 2004, its primary focus was on clinical aspects of the approach. To our knowledge, the first work on using WS-based gait analysis with the focus on user authentication is the paper by Ailisto et al. [29] published in 2005.

In all studies from the Table 1.2 except Morris [64] and Huang et al. [67], the authors use only accelerometer sensor for collecting motion. Although accelerometers record acceleration of the particular body part in three directions: up-down, forward-backward and sideway; only up-down and forward-backward accelerations are utilized for user verification [29, 65, 69, 68, 66]. Morris [64] and Huang et al. [67] use other types of motion recording sensors including force sensors, bend sensors, gyro sensors etc., in additions to the accelerometer sensor (see Figures 1.10 and 1.11). From the Table 1.2, in [29, 65, 69, 68, 66] performance was evaluated in verification mode, while Morris [64] and Huang et al. [67] evaluated performance in identification mode. It is worth noting that

Study	*Sensor(s) Location*	*Performance, %*		*Samples per second*	*#S*
		EER	Recognition		
Morris [64]	shoe	-	97.4	75	10
Huang et al. [67]	shoe	-	96.93	50	9
Ailisto et al. [29]	waist	6.4	-	256	36
Mäntyjärvi et al. [65]	waist	7-19	-	256	36
Rong et al. [69]	waist	6.7	-	250	35
Rong et al. [68]	waist	5.6, 21.1	-	250	21
Vildjiounaite et al. [66]	hand	17.2, 14.3	-	256	31
Vildjiounaite et al. [66]	hip pocket	14.1, 16.8	-	256	31
Vildjiounaite et al. [66]	breast pocket	14.8, 13.7	-	256	31

Table 1.2: A short summary of the current WS-based gait recognition works.

the direct comparison of the performances from the Table 1.2 (and also from Table 1.1) may not be valid mainly due to the differences among the data sets. In addition, as one can observe from the Table 1.2, although performances are promising, all the works are based on relatively small data sets (less than 37 subjects).

Table 3.1 on page 28 (in Chapter 3) presents an overview of this thesis papers on person recognition using WS-based approach.

An application for the WS-based gait recognition can be in improving authentication in personal electronic devices, e.g. mobile phones. Due to its unobtrusive way of data collection, the WS-based gait biometric can be applied for periodic re-verification of the identity in mobile phones. Whenever the user makes a few steps (walks), his identity will be re-verified to ensure that the user is still the same as authenticated. In WS-based gait biometric, the choice of the sensor placement on the body mainly depends on the application perspective (e.g. mobile phones can be carried in the pocket) and the discriminative power of the particular body segment. The motion recording sensors can be integrated with mobile phone hardware or within clothing of the user and then communicated with the phone via a short range communication protocol (e.g. Bluetooth). In fact, some models of the mobile phones already have integrated accelerometer sensor, e.g. Apple's iPhone [23] has the accelerometer for detecting orientation of the phone. It should be also noted that the mobile phone user still needs a strong authenticator (e.g. fingerprint) for the first time authentication because the accuracy of the WS-based (MV-based and FS-based too) gait recognition is still behind the accuracy of some strong biometrics, see Table 1.3. The WS-based gait recognition can then be used as a supplementary method for increasing security by unobtrusive and periodic re-verification of

Biometric	Study	EER	Data set
Iris	Liu and Xie [73]	1.44	CASIA database [74]
	Monro et al. [75]	0.0259	200 subjects
Fingerprint	Ouyang et al. [76]	3.8	FVC2002 DB1 [77]
	Park et al. [78]	0.99-1.07	FVC2002 DB1 and DB2 [77]
Palmprint	Henning et al. [79]	0.0003	samples from 385 palms
	Wu et al. [80]	0.19	7605 samples from 392 palms

Table 1.3: Performance of some strong biometrics.

the identity.

1.4.3 Challenges in Gait Recognition

There are many factors that influence and pose challenges to gait recognition algorithms, e.g. lighting conditions, viewing angles, walking speed, carrying objects, shoe type, surface condition, foot injuries, aging, etc. Although FS-based and WS-based gait recognitions lack difficulties of MV-based approach such as lighting condition, background noise etc., they share common factors that can alter human gait like walking speed, aging, injuries and so on.

Some works from MV-based category also study the feasibility of gait recognition under challenging conditions, for example at night [81], when running [82], under different viewing angles [83] and so on. Gait data set provided by University of South Florida [40] includes five factors that may influence gait recognition. These factors include change in viewing angle, in shoe type, in walking surface, carrying or not carrying briefcase, and the elapsed time between samples being compared. For example, when the difference between the template and the test samples was in shoe type (A vs. B), view (right camera vs. left camera), briefcase (carrying vs. not carrying) and surface (grass vs. concrete), the recognition rates were 78%, 73%, 61% and 32%, respectively [40].

1.4.4 Security of Gait-based Authentication

In order for human characteristics to be considered as biometrics, they should fulfil at least the following seven requirements [3]: universality, uniqueness, permanence, collectability, performance, acceptability and *security* (i.e. robustness against attacks). Therefore, security of gait is also as important as e.g. its performance.

Gait as a behavioural biometric can be vulnerable to a spoof attack. The spoof attack refers to impersonating another person's biometric by deliberately altering one's biometric with the aim to have a higher chance of being accepted by the system. The

level and success of attacks usually depend on the resources available to the attacker, e.g. time, vulnerability knowledge etc. Impersonation attacks have been studied a lot for other kinds of behavioural biometrics, such as handwriting [84] and voice [85].

In spite of many works devoted to the gait biometric, gait security per se (i.e. robustness or vulnerability against attacks) has not received much attention. In many previous works, impostor scores for estimating FAR were generated by matching the normal gait samples of the impostors against the normal gait samples of the genuine users in the database [29, 65, 86, 87, 39, 88]. However, such an approach might not be valid for expressing the security strength of gait biometric against motivated attackers, who can perform some action (e.g. mimic) or possess some vulnerability knowledge about the system. To our best knowledge, the only research paper (except papers in this thesis) dealing with gait security was published recently by Stang and Snekkenes [89]. Their work belongs to the WS-based category with the accelerometer sensor being placed in the trouser pocket. In their approach, 5 gait templates (1 natural gait and 4 abnormal gaits) were created by one user. Then, 13 volunteers acting as impostors tried to mimic the gait templates (15 attempts on each template). Their gait verification method was based on correlation of acceleration signals. The impostors did not see the actual enrolment of the template gaits. Instead they were given feedback in terms of visual plots and correlation score on their mimicking attempts. In the setting of [89], the results suggest that training can improve the mimicking capabilities of attackers.

Paper 5 [90], Paper 6 [91] and Paper 7 [92] of this thesis are primarily dedicated to the topic of gait security. Stang and Snekkenes [89] paper was published after the papers of the thesis.

1.4.5 Gait in Multimodal Biometric System

Multimodal biometric systems combine evidences from several biometric modalities to establish more reliable and accurate identification [93]. Another important benefit of the multimodal biometric systems is in being more robust against attacks. Indeed, it requires more effort to forge or spoof several biometrics simultaneously compared to a single modality. Several works, which study gait in multimodal biometric systems, indicate improvements of the system both in performance and usability [94, 95, 66, 96, 54]. Shakhnarovich et al. [94] and Zhou et al. [95] combine MV-based gait with face biometric. In [94], a frontal face was captured by one camera and a side-view of the person was captured by another camera. Face-only, gait-only and combined face and gait recognition rates were 80%, 87%, and 91%, respectively [94]. In [95], a single camera was used to capture both face and gait. Recognition rates for face and gait separately were 64.3% and 85.7%, respectively. However, when they were combined, the recognition rate increased up to 100% [95]. Cattin [54] fusing features from MV-based and FS-based gait showed that fusion significantly improves an overall system robustness compared

to the best single feature.

Vildjiounaite et al. [66, 96] combine WS-based gait with voice and fingerprint biometrics. In [66], WS-based gait recognition was combined with speaker verification. Accelerations from the three body locations (hand, hip and chest pockets) were each fused with the voice biometric. Performance proved to be significantly better in a noisy environment, compared to when speaker verification was used alone. Depending on noise level, the EER was in the range of 2%-12%, less than half of the EER of individual modalities [66]. In [96], a cascaded multimodal biometric system based on WS-based gait, voice and fingerprint is presented. The aim of the study was to decrease the effort of the user in authentication, and experiments showed that the system was able to achieve FAR of 1% and FRR of 3% (or less), while requiring explicit effort only in 10-60% of the cases [96].

Although the number of subjects participating in the experiments on the aforementioned works was not large (i.e. 20 in [54], 31 in [66], 12 in [94], 14 in [95], and 32 in [96]), they clearly indicate the potential of using gait in a multimodal biometric system.

2 Summary of Papers

The 8 research papers that constitute the main research part of the thesis are:

1. Davrondzhon Gafurov, **A Survey of Biometric Gait Recognition: Approaches, Security and Challenges**, In *Proceedings of Annual Norwegian Computer Science Conference*, Tapir, pp. 119-130, 2007.

2. Davrondzhon Gafurov, Kirsi Helkala and Torkjel Søndrol, **Gait Recognition Using Acceleration from MEMS**, In *Proceedings of IEEE International Conference on Availability, Reliability and Security (ARES)*, pp. 432-437, 2006.

3. Davrondzhon Gafurov, Einar Snekkenes and Patrick Bours, **Gait Authentication and Identification Using Wearable Accelerometer Sensor**, In *Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies (AutoID)*, pp. 220-225, 2007.

4. Davrondzhon Gafurov and Einar Snekkenes, **Arm Swing as a Weak Biometric for Unobtrusive User Authentication**, In *Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Special Session on "Biometrics - From Sensors to Standardization", IEEE Press, 2008 (accepted).

5. Davrondzhon Gafurov, Einar Snekkenes and Tor Erik Buvarp, **Robustness of Biometric Gait Authentication Against Impersonation Attack**, In *Proceedings of International Workshop on Information Security*, Springer LNCS 4277, pp. 479-488, 2006.

6. Davrondzhon Gafurov, Einar Snekkenes and Patrick Bours, **Spoof Attacks on Gait Authentication System**, *IEEE Transactions on Information Forensics and Security*, Special Issue on Human Detection and Recognition, 2(3), pp. 491-502, 2007

7. Davrondzhon Gafurov, **Security Analysis of Impostor Attempts with Respect to Gender in Gait Biometrics**, In *Proceedings of IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, 2007.

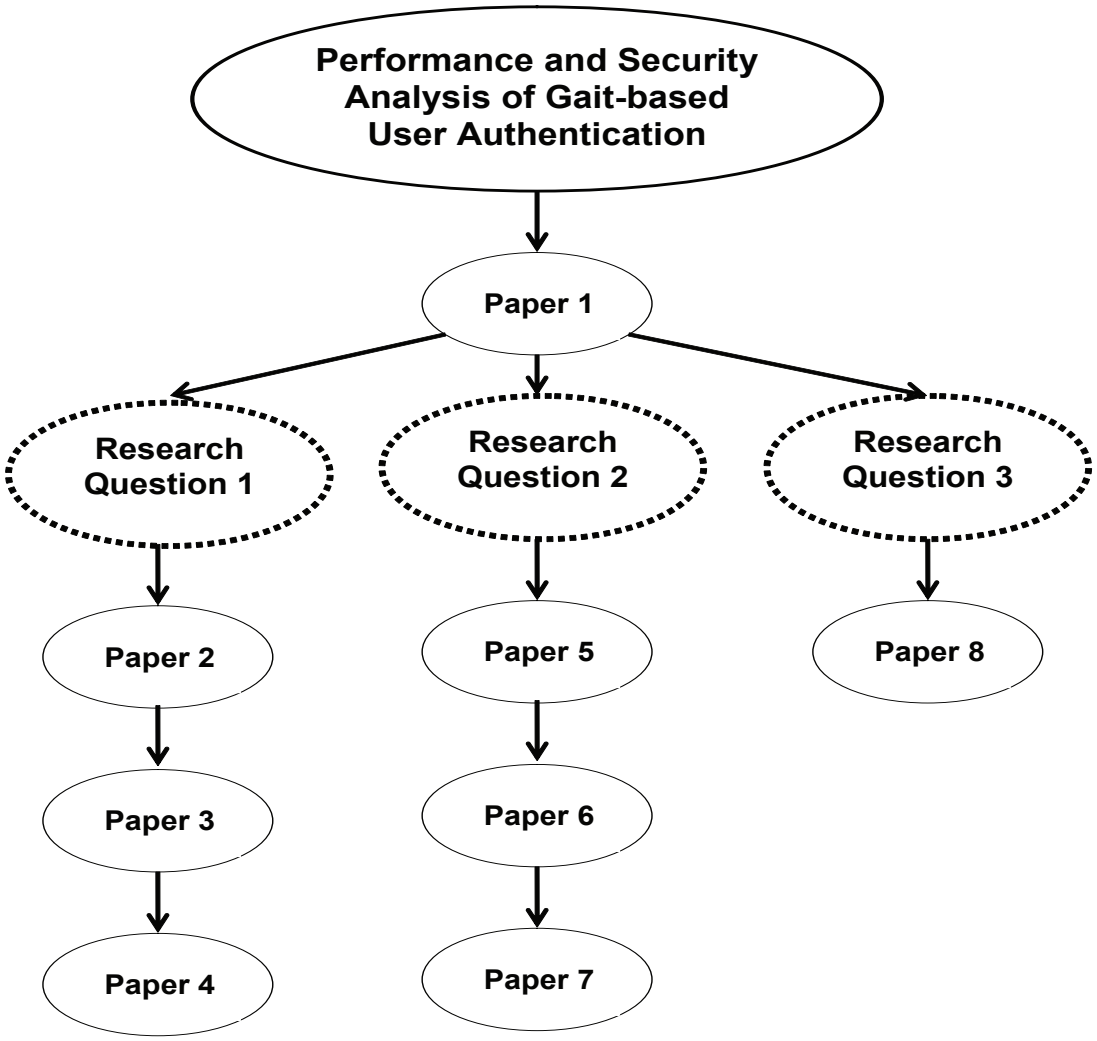

Figure 2.1: An illustration of the relations between the research papers and research questions.

8. Davrondzhon Gafurov and Einar Snekkenes, **Towards Understanding the Uniqueness of Gait Biometric**, *to be submitted.*

The main research questions addressed by these papers are following:

- **Research question 1:** What are the performances of recognition methods that are based on the motion of particular body parts during gait?
- **Research question 2:** How robust is the gait-based user authentication?
- **Research question 3:** What aspects do influence the uniqueness of human gait?

The relations of the papers to the research questions are illustrated in Figure 2.1.

2.1 Summary of Paper 1

A Survey of Biometric Gait Recognition: Approaches, Security and Challenges

The contribution of this paper [42] is on the taxonomy of user recogniton approaches based on gait.

This paper proposes to categorize biometric gait recognition into three groups depending on the way how gait is collected. These categories include Machine Vision (MV) - based, Floor Sensor (FS) - based and Wearable Sensor (WS) - based. In MV-based approach, gait is captured using a video-camera from a distance and then image/video processing techniques are applied to extract gait related data for recognition. In the FS-based approach, a set of sensors are installed in the floor and gait related data (e.g. ground reaction forces) are measured when people walk on a special mat. In the WS-based approach, motion recording sensors are worn or attached to various locations on the body of the person, such as waist, pockets, shoes, etc. The movement recorded by sensors is then used for recognition purposes. An overview of these gait categories are briefly presented and discussed. Such categorization of gait recognition approaches better illustrates potential applications for gait-based recognition system.

There are many factors that can negatively influence the performance of biometric gait recognition. This paper groups such influencing factors into two classes, namely external and internal factors. The external factors are mainly related to the environment and mostly impose challenges to the recognition algorithm per se (e.g. lighting conditions, walking surface conditions, shoe types and so on). The internal factors cause the changes of the natural gait due to sickness (e.g. foot or brain injuries, lower limb disorder etc.) or other physiological changes in body due to aging, drunkenness, pregnancy, gaining or losing weight and so on. The paper reveals that although the influences of some external factors have been studied, the effect caused by the internal factors in gait biometric context have not been investigated yet. The paper also provides some examples, which show that combining gait with other biometric modalities can result in improved performance. In addition, a summary of the security strength of gait biometric under various attack scenarios are also presented (i.e. brief results of Papers 6 and 7).

2.2 Summary of Paper 2

Gait Recognition Using Acceleration From MEMS

The contribution of this paper [97] is on user authentication based on the ankle motion using an accelerometer sensor with a low sampling rate.

The main contributor to the human locomotion is the motion of the feet and legs. From MV-based gait recognition, Liu et al. [98] reported that recognition performance based only on legs is about the same as performance based on the full body. In this

paper, we study the ankle (foot) motion for person verification. Foot motion is collected by an accelerometer sensor, which is attached to the ankle of the person. The sensor measures acceleration in three directions: up-down, forward-backwards and sideways. A combination of these acceleration signals is utilized for authentication. For gait verification two methods, histogram similarity and cycle length, are applied. The first method is based on the distributional statistics of the combined acceleration signal, while the second method is based on the cycle of the combined acceleration. Experimental data set consists of ankle accelerations collected from 21 individuals. The performances of these methods in terms of EERs are 5% (for histogram similarity) and 9% (for cycle length). Another aspect of the paper is that a sampling frequency of the accelerometer sensor used in this paper is 16 Hz, which is the lowest one compared to the accelerometers used in other WS-based gait recognition works [29, 64, 65, 67, 68, 69]. Low sampling also implies that the authentication system requires low resources. A possible application for this approach can be a smart shoe (with integrated accelerometer) that provides identity information based on foot motion to other personal electronics (e.g. mobile phone).

2.3 Summary of Paper 3

Gait Authentication and Identification Using Wearable Accelerometer Sensor

The contribution of this paper [99] is in the area of user recognition using an accelerometer sensor placed in the trouser pocket, and investigating the influence of walking with a backpack on recognition performance.

In case of Paper 2, to provide identity information from the foot to a mobile phone, the sensor must communicate with the device via a short range communication protocol (e.g. Bluetooth). This may require an additional task, e.g. for securing communication between the sensor and the phone. Therefore, a preferable solution would be to integrate the sensor with the mobile phone hardware itself. In such cases motion discriminativeness of the body locations, where phone is carried, must be investigated. One such location is the trouser pockets. This paper investigates the discriminativeness of this body location for person recognition purposes. Although Vildjiounaite et al. [66] also study the acceleration of trouser pocket for user verification, there are significant differences between this paper and their work, mainly in terms of applied methods, performance evaluation modes, data size and experimental setup.

For collecting gait, an accelerometer sensor is used and placed in the trouser pockets. Accelerometer records acceleration in three directions: up-down, forward-backward and sideway. After a pre-processing of the signals (i.e. interpolation and noise reduction), a resultant combination of acceleration vectors is computed and used for recognition. The experimental data set consists of 300 gait sequences collected from 50 subjects. Each subject walked six times, four times without carrying anything and two times

carrying a backpack. In every walking trial, the accelerometer was taken out from the pocket and put back to simulate the realistic settings. The four different methods, namely higher order moments, histogram, correlation and absolute distance, have been applied for recognition. In case of higher order moments, skewness and kurtosis of the resultant acceleration is used as the feature set (as in [65]). The histogram method (same as in Paper 2) is based on distributional statistics of the resultant acceleration. For correlation and absolute distance methods, the averaged cycle of acceleration is computed and used as a feature vector. Performance of the system is studied both in verification and identification modes. In the verification mode, the EERs of 20%, 14%, 9.2% and 7.3% are obtained (using gait samples without carrying backpack). In the identification mode, the identification probabilities at rank 1 of 24.2%, 50.5%, 83.8% and 86.3% are achieved (using gait samples without carrying backpack).

People can walk while carrying something, e.g. backpack. This paper also analyses recognition performance when subjects are carrying a backpack with a load of about 4 kg. In this setting, the difference between test and template gait samples is in carrying or not carrying the backpack. The analysis using the absolute distance method (the best one among the four methods) indicates that performance of the system may decrease (perhaps not significantly) in such setting. In terms of EER it deteriorates from 7.3% to 9.3%, while in terms of identification probability at rank 1 it falls from 86.3% to 86.2%.

2.4 Summary of Paper 4

Arm Swing as a Weak Biometric for Unobtrusive User Authentication

The contribution of this paper is a new user recognition method based on a natural arm swing using an accelerometer sensor.

Like pockets in Paper 3, the arm is another body location, where personal electronics can be attached (e.g. watches). This paper studies an unobtrusive mechanism of user authentication based on a natural arm swing. Arm swing occurring during gait is collected by using an accelerometer, which records arm acceleration in three directions (up-down, forward-backward and sideway). After pre-processing of the acceleration signals, a combination of the accelerations is computed and analysed for recognition. The combined acceleration is analysed in the frequency domain. Using Fourier coefficients of the combined acceleration signal, its amplitude spectrum is computed. The maximum amplitudes in the specified frequency ranges are used as a feature set. Experimental data set consists of 120 arm swing samples from 30 persons. In the verification mode, the EERs of 15%, 13.3% and 10% are achieved using two, four and six features, respectively. In addition, in the verification mode, performances in terms of TER are 29.3%, 24% and 18.7%, respectively. In the identification mode using the same feature sets, identification probabilities at rank 1 of 31.7%, 60% and 71.7% are obtained, respectively.

2.5 Summary of Paper 5

Robustness of Biometric Gait Authentication Against Impersonation Attack

The main contribution of this paper [90] is a new authentication method based on hip motion and a preliminary analysis of its security strength.

Like pockets in Paper 3, the belt (around hip location) is another place, where people usually carry mobile phones. This paper studies hip motion for use in person authentication. The hip accelerations along three orthogonal axes (up-down, forward-backward and sideways) are recorded by an accelerometer sensor, which is attached to the belt of the person around the right hip. The initial pre-processing of the acceleration consists of interpolation and noise reduction by a moving average filter. Then from the three accelerations, a more orientation invariant acceleration is computed and used for authentication. The verification method is based on detecting individual cycles in the signal, normalising them and computing an averaged cycle of the person. Using hip motion data from 22 persons, the EER of about 16% is achieved.

Next, for the first time in gait biometric research, this paper addresses an issue of gait security per se (in case of hip motion). In particular, the robustness of gait biometric against minimal-effort mimicking attacks (i.e. trying to walk as someone else) has been studied. The minimal-effort mimicking refers to the mimicking attempts, where attackers have a restricted time to study the targeted person's gait and a limited number of mimicking attempts. The impostor scores consist of two sets, a friendly impostor set and a hostile impostor set. The friendly impostor set is generated by matching the normal gait samples of the attacker against the normal gait samples of the genuine user (i.e. where 16% EER is achieved). The hostile impostor set consists of the scores generated by matching the mimicked gait samples of the attacker against the normal gait sample of the genuine user. We apply two statistical tests and a D-prime criteria [100] (which shows separability of two distributions) to check the differences among the genuine and two impostor sets. All these tests indicate that the minimal effort mimicry on gait biometric does not help, which means that gait is robust against such types of attack.

2.6 Summary of Paper 6

Spoof Attacks on Gait Authentication System

The primary contributions of this paper [91] are two fold: evaluating the performance of WS-based biometric gait with a large data set and analysing the security strength of gait biometric (in case of hip motion).

This paper significantly extends the Paper 5 by increasing the size of the data set and containing a more extensive analysis on gait security. Gait was collected by an ac-

celerometer sensor, which was attached to the belt of subjects around the hip. The sensor recorded hip acceleration in three orthogonal directions: up-down, forward-backward and sideways. After initial pre-processing of the acceleration signals, the resultant acceleration was computed and utilized for recognition. The gait recognition method consists of detecting cycles in the signal, normalising them and computing the averaged cycle of the hip motion. The experiments consisted of two parts, namely friendly scenario and hostile scenario. In the friendly scenario, subjects walked in their normal walking style. In the hostile scenario, subjects were trying to walk as someone else. Basically, in the hostile scenario attackers are assumed to be active and motivated, while in the friendly scenario attackers are assumed to be passive. In total, we have collected 760 gait sequences from 100 subjects.

Friendly scenario: Although previous studies on WS-based gait recognition reported promising performances, the number of subjects used in the experiments were small or medium (less than 37) [29, 65, 64, 67, 68, 69]. In this paper, we have evaluated the performance of the WS-based gait biometric with the large data set both in verification and identification modes. In the verification mode an EER of 13% was obtained. In the identification mode, an identification rate at rank 1 of 73.2% was achieved.

Hostile scenario: In spite of much research being carried out in gait recognition, the topic of gait vulnerability to attacks has not received enough attention. In nearly all the previous and current studies, the impostor scores for estimating FAR were generated by matching a normal walking sample of the impostor subjects against a normal walking sample of the genuine subjects in the database (i.e. friendly scenario) [29, 65, 86, 87, 39, 88, 40, 48, 101, 88]. However, such an approach might not be valid for evaluating the security strength of gait biometric against deliberate attacks. For example, a motivated attacker may want to mimic the targeted person's gait or use some vulnerability information about the authentication system. Although in Paper 5 of this thesis we showed some encouraging results on gait robustness against mimicking attacks, the size of data set was small and analysis were performed at the score level. Therefore, a larger analysis based on FAR/FRR (which are standard evaluation criteria) were required.

In this paper, an analysis of a minimal-effort impersonation attack and a closest person attack on gait biometrics using a large data set are presented. In the minimal-effort impersonation attacks, impostors tried to study gait of the target person (with limited time) and then attempted to walk like him or her. In the closest person attack, impostor's normal gait samples are matched only to the gait samples of the person who has the most similar gait as the attacker. Analysis based on FAR (and their confidence intervals) indicates that the minimal-effort impersonation attack on gait biometric does not necessarily improve the chances of an impostor of being accepted. However, attackers with knowledge of their closest person in the database can be a serious threat to the gait-based authentication system. In addition, the system is evaluated in the negative

mode by matching mimicked gait samples of the attackers against their own normal gait samples. In this mode not surprisingly, the FRR with their confidence intervals indicate that it is easy to alter one's own gait and not to be recognized by the system.

2.7 Summary of Paper 7

Security Analysis of Impostor Attempts with Respect to Gender in Gait Biometrics

The contribution of this paper [92] is on security analysis of impostor attacks with respect to gender in gait-based authentication system.

Medical studies suggest that there is a significant difference between male and female gait [102, 103]. Likewise, studies from machine vision provide the encouraging results on automatic gender discrimination using gait [104, 105, 106]. Based on these studies and also motivated from Papers 5 and 6, this paper studies the role of gender information in impostors attempts. In this paper, the same experimental data set as in Paper 6 (friendly scenario experiment) is used, where hip motions from 100 persons (70 men and 30 women) were collected. In addition, the same verification method as in Paper 6 is applied in this paper. The assumption made in this paper is that attackers know the genders of users in the database. This is a reasonable assumption, since gender is not considered as secret information and usually the name of the person can reveal one's gender too. In this settings, we investigate how different the impostor scores generated by matching gait samples from persons of the same gender (as attacker) are, compared to the impostor scores generated by matching gait samples from persons of different genders. Analysis based on the FAR with their 95% confidence intervals reveals that for a given threshold value the same gender FAR is significantly higher than the different gender FAR. This suggests that if the attackers know the gender of the users in the database then they can use this information for increasing their acceptance chances.

Some applications might be gender specific, i.e. all users of the system are only men or women. This paper also evaluates performance of the gait-based authentication system when all user are only men or women. FAR curves with their 95% indicate that for a given threshold women's FAR was lower than men's FAR, which may suggest that women's gait (i.e. hip acceleration) is less homogeneous than men's gait.

2.8 Summary of Paper 8

Towards Understanding the Uniqueness of Gait Biometric

The contribution of this paper is in providing some insights towards understanding the uniqueness of gait (in case of ankle motion) by relating the discriminativeness of the gait to the shoe attribute, direction of the motion and the gait cycle.

Paper 2 and previous studies from MV-based studies [107, 108] indicated that foot motion has a discriminating power from which individuals can be recognized. This paper also analyses foot (ankle) motion for authentication with the objective of understanding its discriminativeness. There are many factors that can negatively influence gait recognition and one such factor is shoe type. A study by Enokida et al. [109] shows that when the test and template samples of the person are collected using different shoe types, the performance can decrease significantly. In many previous gait recognition experiments, subjects were walking with their own footwear. In such settings, a system authenticates *person plus shoe* rather than the *person* per se.

Unlike most of the previous gait recognition works, in this paper gait samples are collected when all subjects walked with the same specific types of footwear (only sizes differ), thus eliminating the randomness (noise) introduced by the shoe variability. An accelerometer sensor, which is attached to the ankle of the person, is used for collecting gait. The accelerometer records ankle motion in three directions: up-down, forward-backward and sideway. After interpolation and noise reduction in acceleration signals, gait cycles have been detected, normalized and averaged. The verification method is based on the averaged gait cycle. The gait data set consists of 480 foot motion samples collected from 30 subjects. Each subject walked with the four different types of footwear. Analysis based on DET curves reveals the following: (1) heavy footwear tends to reduce the discrimination, and (2) sideway motion of the foot has the most discriminating power compared to the up-down or forward-backward directions. Although the first finding was expected, the second one is quite interesting, since in previous WS-based works [29, 65, 69, 68] the focus was only on two directions of the motion: up-down and forward-backward acceleration but not the sideway acceleration. This is perhaps due to the fact that their accelerometers were attached to the waist (see Figure 1.8 on page 11) and there is less sideway movements of the waist compared to the foot. Interestingly from biomechanical research, Cavanagh [110] supports our findings by observing that runners express individuality characteristics in medio-lateral (i.e. sideway) shear force.

Based on foot movement, the human gait cycle can be divided into several subevents such as initial contact, loading response, mid swing and so on [32] (see Figure 1.5 on page 9). This paper also introduces a technique for analysing contribution from each acceleration sample in the gait cycle (i.e. gait subevents) to recognition. By applying this technique on the sideway acceleration of the foot motion, the paper reveals that various parts of gait cycle provide different level of discrimination.

The verification performance in terms of EER is in the range of 5%-18.3% mainly depending on the shoe type and the direction of motion. In addition, our analysis confirms that recognition performance can significantly decrease when the test and template samples are obtained using different shoe types.

3 Summary of the thesis contributions

Gait recognition refers to automatic recognition of people by the way they walk. In this thesis, we made original contributions to the area of gait recognition in the following topics: classification of gait recognition methods; gait recognition using wearable sensors; security analysis of gait-based authentication; and understanding the uniqueness of the gait biometric.

3.1 Technical Contributions

Little has been published in terms of classifications of gait data collection. This thesis produced a taxonomy of user recognition methods based on gait. It classifies approaches in gait recognition into three groups, depending on how gait is collected. The three categories in gait recognition are identified. The first category is the approaches that use a video-camera for collecting gait. In the second category, gait is captured using sensors installed on the floor. The third one uses small and wearable sensors, which are placed on the body of the user, for recording motion during gait.

The number of works published on user authentication based on gait using small and wearable sensors is very limited. In addition, existing studies are usually based on relatively small data sets. This thesis presents the analysis of the motion of some body parts during gait for person recognition. Our research identifies some new locations on the body, whose acceleration have discriminative power. These body segments include ankle, belt around hip, trousers pocket and arm. Several methods have been applied on the acceleration signals from these body parts. Performances of some of our methods appear to be better compared to the performance of some previous works, despite the fact that the sampling frequency of our accelerometer sensor is usually lower. In addition, several of our studies include gait samples from larger populations. A short summary of performances of the aforementioned body segments is presented in Table 3.1. In this table, performance is given in terms of the EER and identification rate at rank 1.

Paper number	*Sensor placement on the body*	*Performance, %*		*Number of subjects in experiments*
		EER	P_1 at rank 1	
3	Trousers pocket	7.3	86.3	50
4	Arm	10	71.7	30
6	Hip	13	73.2	100
8	Ankle	5	-	30

Table 3.1: A short summary of performances of some papers in this thesis. The current state of the art on person recognition using motion recording sensors is presented in Table 1.2 on page 13.

Many previous gait recognition studies have limitations in expressing robustness of gait-based user authentication against attacks, because impostor model is assumed to be passive. In real applications, such assumption cannot be valid, e.g. impostors can imitate victim's gait or possess some vulnerability knowledge about authentication system. To our best knowledge, this thesis presents the first extensive security analysis of gait-based authentication in the case of hip motion. In the thesis, we have studied security of the gait-based user authentication under three attack scenarios. These attacks include a minimal effort-mimicry, knowing the closest person in the database (in terms of gait similarity) and knowing the gender of the user in the database. The findings of the thesis reveal that the minimal effort mimicking does not help to improve the acceptance chances of impostors. However, impostors who know their closest person in the database or the gender of the users in the database can be a threat to the gait-based authentication system.

Previously, little has been published on the understanding of human gait's discriminative power with respect e.g. to the different axis of motion, parts of the gait cycle, etc. The thesis also provides some new insights towards understanding the uniqueness of the gait in case of ankle/foot motion with respect to the shoe attributes and axis of the motion. In particular, our analysis shows that heavy footwear tends to diminish gait's discriminative power and the sideway motion of the foot provides the most discrimination compared to the up-down or forward-backward direction of the motion. Based on the foot motion, human gait cycle can be decomposed into several subevent and our research also reveals that various gait cycle parts (i.e. subevents) contribute differently towards recognition performance.

3.2 Ideas for further research

Person recognition based on gait using wearable sensors is a very recent approach compared to the vision based gait approach or other conventional biometric modalities. Therefore, there are still opportunities within this field of research. We would like to outline a few possible directions that could be a natural extension of the work presented in this thesis.

- *Public data set.* Unlike video-based gait biometric, the WS-based gait lacks a large publicly available database. Creating such large WS-based database will further facilitate the development in the direction of WS-based approach and also will allow direct comparisons of various algorithms. Such database should include various external and possibly internal factors that can influence gait recognition.

- *Improving performance.* The accuracy of WS-based (MV- and FS-based too) gait biometric is behind the accuracy of strong biometrics like fingerprint or iris. The following directions for fusing can be investigated to improve accuracy: finding an optimal combination of the motion signals from three directions; fusing motions from different body locations (foot, hip, arm, etc.) and/or different types of sensors (accelerometers, gyroscopes, etc.).

- *More on Gait Security.* Although the thesis showed that the minimal effort mimicry on gait is not helpful, the topic of whether gait of another person can be learned by extensive training still requires further research. In addition, it is also useful to verify whether there are "sheep" (people whose gait is easy to mimic) or "wolves" (people who are good on mimicking other people's gait) population in gait biometric too.

- *Further Gait Potential.* Gait is a complex biological process that involves nervous and musculo-skeletal systems. For further understanding gait's inherit potentials and limitations for security applications, a (long-term) multi-disciplinary approach that combines knowledge from various domains such as medicine, biomechanics, physics, IT, etc. might be necessary.

Bibliography

[1] Art Conklin, Glenn Dietrich, and Diane Walz. Password-based authentication: A system perspective. In *37th Hawaii Int. Conference on System Sciences (HICSS-37 2004)*, 2004. ISBN 0-7695-2056-1.

[2] L. O'Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, Vol. 91, Issue 12:2019–2020, December 2003.

[3] Anil Jain, Ruud Bolle, and Sharath Pankanti, editors. *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Publishers, 1999.

[4] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar. *Handbook of Fingerprint Recognition*. Springer (New York), 2003.

[5] S.Z. Li and A.K. Jain, editors. *Handbook of Face Recognition*. Springer Verlag, 2005.

[6] J. Daugman. How iris recognition works. In *International Conference on Image Processing*, 2002.

[7] B.G.B. Fauve, D. Matrouf, N. Scheffer J.-F. Bonastre, and J.S.D. Mason. State-of-the-art performance in text-independent speaker verification through open-source software. *IEEE Transactions on Audio, Speech, and Language Processing*, 2007.

[8] Alisher Kholmatov and Berrin Yanikoglu. Identity authentication using improved online signature verification method. *Pattern Recognition Letters*, 2005.

[9] Mark S. Nixon, Tieniu N. Tan, and Rama Chellappa. *Human Identification Based on Gait*. Springer, 2006.

[10] N.L. Clarke and S.M. Furnell. Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security*, 2006. ISSN:1615-5262, pp1-14.

[11] A.A.E. Ahmed and I. Traore. A new biometric technology based on mouse dynamics. *IEEE Transactions on Dependable and Secure Computing*, 2007.

[12] Ramaswamy Palaniappan and Danilo P. Mandic. Biometrics from brain electrical activity: A machine learning approach. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2007.

[13] F. Beritelli and S. Serrano. Biometric identification based on frequency analysis of cardiac sounds. *IEEE Transactions on Information Forensics and Security*, 2007.

[14] Andreas Uhl and Peter Wild. Personal identification using eigenfeet, ballprint and foot geometry biometrics. In *IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, 2007.

[15] Fingerprint billing for Germans. http://news.bbc.co.uk/2/hi/europe/4344279.stm. Last visit: 21.04.2008.

[16] Ahmad N. Al-Raisi and Ali M. Al-Khouri. Iris recognition and the challenge of homeland and border control security in UAE. *Telematics and Informatics*, 25(2):117–132, 2008.

[17] Key Pousttchi and Martin Schurig. Assessment of today's mobile banking applications from the view of customer requirements. In *37th Annual Hawaii International Conference on System Sciences (HICSS'04)*, 2004.

[18] B. Dukic and M. Katic. m-order - payment model via SMS within the m-banking. In *27th International Conference on Information Technology Interfaces*, 2005.

[19] N.L. Clarke and S.M. Furnell. Authentication of users on mobile telephones a survey of attitudes and practices. *Computers & Security*, 2005.

[20] Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 british crime survey. http://www.homeoffice.gov.uk/rds/pdfs07/hosb1007.pdf. Last visit: 15.04.2008.

[21] M. A. Sasse, S. Brostoff, and D. Weirich. Transforming the "weakest link" - human/computer interaction approach to usable and effective security. *BT Technology Journal*, 2001.

[22] Roman V. Yampolskiy. Analyzing user password selection behavior for reduction of password space. In *40th Annual IEEE International Carnahan Conferences on Security Technology*, 2006.

[23] Apple's iphone with integrated accelerometer. http://www.apple.com/iphone/features/index.html. Last visit: 09.04.2008.

[24] Ruud Bolle, Jonathan Connell, Sharanthchandra Pankanti, Nalini Ratha, and Andrew Senior. *Guide to Biometrics*. Springer Professional Computing, 2003.

[25] J. L. Wayman. Confidence interval and test size estimation for biometric data. In *IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'99)*, 1999.

[26] R.M. Bolle, N.K. Ratha, and S.Pankati. Error analysis of pattern recognition systems - the subsets bootstrap. *Computer Vision and Image Understanding*, 2004.

[27] ISO/IEC IS 19795-1, information technology, biometric performance testing and reporting, part 1: Principles and framework, 2006.

[28] J. Wayman, A. Jain, D. Maltoni, and D. Maio, editors. *Biometric Systems: Technology, Design and Performance Evaluation*. Springer, 2005.

[29] Heikki J. Ailisto, Mikko Lindholm, Jani Mäntyjärvi, Elena Vildjiounaite, and Satu-Marja Mäkelä. Identifying people from gait pattern with accelerometers. In *Proceedings of SPIE Volume: 5779; Biometric Technology for Human Identification II*, pages 7–14, 2005.

[30] P. Jonathon Phillips, Hyeonjoon Moon, Syed A. Rizvi, and Patrick J. Rauss. The FERET evaluation methodology for face-recognition algorithms. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 22(10):1090–1104, 2000.

[31] *The Oxford English Dictionary: Fourth Edition*. Oxford University Press (Oxford UK), 1951.

[32] Christopher Vaughan, Brian Davis, and Jeremy O'Cononor. *Dynamics of human gait*. Kiboho Publishers, 1999.

[33] M. P. Murray, A. B. Drought, and R. C. Kory. Walking patterns of normal men. *Journal of Bone and Joint Surgery*, 1964.

[34] M.P. Murray. Gait as a total pattern of movement. *American Journal of Physical Medicine*, pages 290–332, 1967.

[35] Stephen Vankoski and Luciano Dias. Clinical motion analysis. http://www.childsdoc.org/99Spring/clinicalmotionanalysis.asp, 1999.

[36] M. S. Nixon and J.N. Carter. Automatic recognition by gait. *Proceedings of the IEEE*, 94(11):2013 – 2024, 2006.

[37] Amos Y. Johnson and Aaron F. Bobick. A multi-view method for gait recognition using static body parameters. In *Third International Conference on Audio- and Video-Based Biometric Person Authentication*, pages 301–311, June 2001.

[38] L. Lee and W. Eric L. Grimson. Gait appearance for recognition. In *International ECCV Workshop on Biometric Authentication*, pages 143–154, June 2002.

[39] Liang Wang, Huazhong Ning, Tieniu Tan, and Weiming Hu. Fusion of static and dynamic body biometrics for gait recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(2), 2004.

[40] Sudeep Sarkar, P. Jonathon Phillips, Zongyi Liu, Isidro Robledo Vega, Patrick Grother, and Kevin W. Bowyer. The humanID gait challenge problem: Data sets, performance, and analysis. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 27(2):162–177, 2005.

[41] 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 Transactions on Image Processing*, 2004.

[42] Davrondzhon Gafurov. A survey of biometric gait recognition: Approaches, security and challenges. In *Annual Norwegian Computer Science Conference*, Oslo, Norway, November 19-21 2007.

[43] Yanmei Chai, Jinchang Ren, Rongchun Zhao, and Jingping Jia. Automatic gait recognition using dynamic variance features. In *International Conference on Automatic Face and Gesture Recognition*, pages 475 – 480, 2006.

[44] C. BenAbdelkader, R. Cutler, H. Nanda, and L. Davis. Eigengait: Motion-based recognition of people using image self-similarity. In *Thrid International Conference on Audio- and Video-Based Biometric Person Authentication*, 2001.

[45] James B. Hayfron-Acquah, Mark S. Nixon, and John N. Carter. Automatic gait recognition by symmetry analysis. In *Audio- and Video-Based Biometric Person Authentication*, pages 272–277, 2001.

[46] Yuan Wang, Shiqi Yu, Yunhong Wang, and Tieniu Tan. Gait recognition based on fusion of multi-view gait sequences. In *International Conference on Biometrics*, pages 605–611, 2006.

[47] Toby H. W. Lam and Raymond S. T. Lee. A new representation for human gait recognition: Motion silhouettes image (MSI). In *International Conference on Biometrics*, pages 612–618, 2006.

[48] Zongyi Liu and Sudeep Sarkar. Improved gait recognition by gait dynamics normalization. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 28(6):863 – 876, 2006.

[49] Ju Han and Bir Bhanu. Individual recognition using gait energy image. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 28(2):316 – 322, 2006.

[50] N. Lynnerup and J. Vedel. Person identification by gait analysis and photogrammetry. *Journal of Forensic Sciences*, 2005.

[51] Peter K. Larsen, Erik B. Simonsen, and Niels Lynnerup. Gait analysis in forensic medicine. In *SPIE Electronic Imaging (Videometrics IX)*, 2007.

[52] Chiraz BenAbdelkader. *Gait as a Biometric for Person Identification in Video.* PhD thesis, University of Maryland, College Park, 2002.

[53] Amos Y. Johnson. *A method for human identification using static, activity-specific parameters.* PhD thesis, Georgia Institute of Technology, 2002.

[54] Philippe Cattin. *Biometric Authentication System Using Human Gait.* PhD thesis, Swiss Federal Institute of Technology, 2002.

[55] J.D. Shutler, M.G. Grant, M.S. Nixon, and J.N. Carter. On a large sequence-based human gait database. In *4th International Conference on Recent Advances in Soft Computing*, pages 66–71, 2002.

[56] Shiqi Yu, Daoliang Tan, and Tieniu Tan. A framework for evaluating the effect of view angle, clothing and carrying condition on gait recognition. In *18th International Conference on Pattern Recognition*, 2006.

[57] R. J. Orr and G. D. Abowd. The smart floor: A mechanism for natural user identification and tracking. In *Proceedings of the Conference on Human Factors in Computing Systems*, 2000.

[58] J. Suutala and J. Röning. Towards the adaptive identification of walkers: Automated feature selection of footsteps using distinction sensitive LVQ. In *Int. Workshop on Processing Sensory Information for Proactive Systems (PSIPS 2004)*, June 14-15 2004.

[59] Lee Middleton, Alex A. Buss, Alex Bazin, and Mark S. Nixon. A floor sensor system for gait recognition. In *Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'05)*, pages 171–176, 2005.

[60] Jam Jenkins and Carla Schlatter Ellis. Using ground reaction forces from gait analysis: Body mass as a weak biometric. In *Pervasive*, 2007.

[61] K. Nakajima, Y. Mizukami, K. Tanaka, and T. Tamura. Footprint-based personal recognition. *IEEE Transactions on Biomedical Engineering*, 47(11), 2000.

[62] J. Suutala and J. Röning. Combining classifiers with different footstep feature sets and multiple samples for person identification. In *IEEE International Conference on Acoustics, Speech, and Signal Processing(ICASSP)*, 2005.

[63] J. Suutala and J. Röning. Methods for person identification on a pressure-sensitive floor: Experiments with multiple classifiers and reject option. *Information Fusion*, 9(1):21–40, 2008.

[64] Stacy J. Morris. *A shoe-integrated sensor system for wireless gait analysis and real-time therapeutic feedback*. PhD thesis, Harvard University–MIT Division of Health Sciences and Technology, 2004. http://hdl.handle.net/1721.1/28601.

[65] Jani Mäntyjärvi, Mikko Lindholm, Elena Vildjiounaite, Satu-Marja Mäkelä, and Heikki J. Ailisto. Identifying users of portable devices from gait pattern with accelerometers. In *IEEE International Conference on Acoustics, Speech, and Signal Processing*, 2005.

[66] Elena Vildjiounaite, Satu-Marja Mäkelä, Mikko Lindholm, Reima Riihimäki, Vesa Kyllönen, Jani Mäntyjärvi, and Heikki Ailisto. Unobtrusive multimodal biometrics for ensuring privacy and information security with personal devices. In *Pervasive*, pages 187–201, May 2006. Springer LNCS.

[67] Huang Bufu, Meng Chen, Panfeng Huang, and Yangsheng Xu. Gait modeling for human identification. In *IEEE International on Conference on Robotics and Automation*, 2007.

[68] Liu Rong, Zhou Jianzhong, Liu Ming, and Hou Xiangfeng. A wearable acceleration sensor system for gait recognition. In *2nd IEEE Conference on Industrial Electronics and Applications (ICIEA)*, 2007.

[69] Liu Rong, Duan Zhiguo, Zhou Jianzhong, and Liu Ming. Identification of individual walking patterns using gait acceleration. In *1st International Conference on Bioinformatics and Biomedical Engineering*, 2007.

[70] 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 *22nd Annual International Conference of the IEEE on Engineering in Medicine and Biology Society*, pages 1879 – 1882, 2000.

[71] 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 *23rd Annual International Conference of the IEEE on Engineering in Medicine and Biology Society*, pages 1153 – 1154, 2001.

[72] D. Alvarez, R.C. Gonzalez, A. Lopez, and J.C. Alvarez. Comparison of step length estimators from weareable accelerometer devices. In *28th Annual International Conference of the IEEE on Engineering in Medicine and Biology Society (EMBS)*, pages 5964 – 5967, Aug. 2006.

[73] Chengqiang Liu and Mei Xie. Iris recognition based on DLDA. In *18th International Conference on Pattern Recognition*, 2006.

[74] Casia iris image database. http://www.cbsr.ia.ac.cn/english/Databases.asp. Last visit: 08.04.2008.

[75] Donald M. Monro, Soumyadip Rakshit, and Dexin Zhang. DCT-Based iris recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4), 2007.

[76] Zhengyu Ouyang, Jianjiang Feng, Fei Su, and Anni Cai. Fingerprint matching with rotation-descriptor texture features. In *18th International Conference on Pattern Recognition*, 2006.

[77] D.Maio, D.Maltoni, R.Cappelli, J.L.Wayman, and A.K. Jain. FVC2002: Second fingerprint verification competition. In *16th International Conference on Pattern Recognition*, 2006.

[78] U. Park, Pankanti, and A. K. Jain. Fingerprint verification using SIFT features. In *SPIE Defense and Security Symposium*, 2008.

[79] P. Hennings, M. Savvides, and B.V.K. Vijaya Kumar. Palmprint recognition with multiple correlation filters using edge detection for class-specific segmentation. In *5th IEEE Workshop on Automatic Identification Advanced Technologies*, 2007.

[80] Xiangqian Wu, Kuanquan Wang, and David Zhang. Palmprint texture analysis using derivative of gaussian filters. In *International Conference on Computational Intelligence and Security*, 2006.

[81] Daoliang Tan, Kaiqi Huang, Shiqi Yu, and Tieniu Tan. Efficient night gait recognition based on template matching. In *18th International Conference on Pattern Recognition*, 2006.

[82] Y. C. Yam, M. S. Nixon, and J. N. Carter. Extended model-based automatic gait recognition of walking and running. In *International Conference on Audio- and Video-Based Biometric Person Authentication*, 2001.

[83] Amit Kale, Amit K. Roy Chowdhury, and Rama Chellappa. Towards a view invariant gait recognition algorithm. In *IEEE Conference on Advanced Video and Signal Based Surveillance*, pages 143–150, July 2003.

[84] Sung-Hyuk Cha and C.C. Tappert. Automatic detection of handwriting forgery. In *Eighth International Workshop on Frontiers in Handwriting Recognition*, pages 264 – 267, August 2002.

[85] Yee Wah Lau, M. Wagner, and D. Tran. Vulnerability of speaker verification to voice mimicking. In *International Symposium on Intelligent Multimedia, Video and Speech Processing*, pages 145 – 148, October 2004.

[86] C. BenAbdelkader, R. Cutler, and L. Davis. Stride and cadence as a biometric in automatic person identification and verification. In *Fifth IEEE International Conference on Automatic Face and Gesture Recognition*, pages 357–362, May 2002.

[87] A.I. Bazin, L. Middleton, and M.S. Nixon. Probabilistic fusion of gait features for biometric verification. In *Eighth International Conference of Information Fusion*, 2005.

[88] Liang Wang, Tieniu Tan, Weiming Hu, and Huazhong Ning;. Automatic gait recognition based on statistical shape analysis. *IEEE Transactions on Image Processing*, 12(9):1120 – 1131, Sept. 2003.

[89] Oyvind Stang and Einar Snekkenes. Experimental security evaluation of correlation based gait authentication. In *The 12th Nordic Workshop on Secure IT Systems*, 2007.

[90] Davrondzhon Gafurov, Einar Snekkenes, and Tor Erik Buvarp. Robustness of biometric gait authentication against impersonation attack. In *First International Workshop on Information Security (IS'06), OnTheMove Federated Conferences (OTM'06)*, pages 479–488, Montpellier, France, Oct 30 - Nov 1 2006. Springer LNCS 4277.

[91] Davrondzhon Gafurov, Einar Snekkenes, and Patrick Bours. Spoof attacks on gait authentication system. *IEEE Transactions on Information Forensics and Security*, 2(3), 2007. Special Issue on Human Detection and Recognition.

[92] Davrondzhon Gafurov. Security analysis of impostor attempts with respect to gender in gait biometrics. In *IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, Washington D.C., USA, September 27-29 2007.

[93] A. Ross and A. K. Jain. Multimodal biometrics: An overview. In *12th European Signal Processing Conference (EUSIPCO)*, 2004.

[94] G. Shakhnarovich, L. Lee, and T. Darrell. Integrated face and gait recognition from multiple views. In *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition.*, 2001.

[95] Xiaoli Zhou, Bir Bhanu, and Ju Han. Human recognition at a distance in video by integrating face profile and gait. In *5th International Conference on Audio- and Video-Based Biometric Person Authentication*, pages 533–543, July 2005.

[96] Elena Vildjiounaite, Satu-Marja Makela, Mikko Lindholm, Vesa Kyllonen, and Heikki Ailisto. Increasing security of mobile devices by decreasing user effort

in verification. In *Second International Conference on Systems and Networks Communications (ICSNC)*, 2007.

[97] Davrondzhon Gafurov, Kirsi Helkala, and Torkjel Sondrol. Gait recognition using acceleration from MEMS. In *1st IEEE International Conference on Availability, Reliability and Security (ARES)*, pages 432–437, Vienna, Austria, April 2006.

[98] Zongyi Liu, Laura Malave, Adebola Osuntogun, Preksha Sudhakar, and Sudeep Sarkar. Toward understanding the limits of gait recognition. In *Proceedings of SPIE – Volume 5404, Biometric Technology for Human Identification*, 2004.

[99] Davrondzhon Gafurov, Einar Snekkenes, and Patrick Bours. Gait authentication and identification using wearable accelerometer sensor. In *5th IEEE Workshop on Automatic Identification Advanced Technologies (AutoID)*, pages 220–225, Alghero, Italy, June 7-8 2007.

[100] R.M. Bolle, S. Pankanti, and N.K. Ratha. Evaluation techniques for biometrics-based authentication systems (FRR). In *15th International Conference on Pattern Recognition*, pages 831 – 837, September 2000.

[101] Nikolaos V. Boulgouris and Zhiwei X. Chi. Gait recognition using radon transform and linear discriminant analysis. *IEEE Transactions on Image Processing*, 16(3):731–740, 2007.

[102] D.C. Kerrigan, M.K. Todd, and U. Della Croce. Gender differences in joint biomechanics during walking: normative study in young adults. *American journal of physical medicine & rehabilitation*, 1998.

[103] S.H. Cho, J.M. Park, and O.Y. Kwon. Gender differences in three dimensional gait analysis data from 98 healthy korean adults. *Clinical Biomechanics (Bristol, Avon)*, 2004.

[104] L. Lee and W.E.L. Grimson. Gait analysis for recognition and classification. In *International Conference on Automatic Face and Gesture Recognition*, pages 148–155, 2002.

[105] J.W. Davis and Hui Gao. Gender recognition from walking movements using adaptive three-mode PCA. In *Conference on Computer Vision and Pattern Recognition Workshop*, 2004.

[106] J. Yoo, D. Hwang, and M. Nixon. Gender classification in human gait using support vector machine. In *Proceedings of Advanced Concepts for Intelligent Vision Systems*, pages 138–145, 2006.

[107] Agus Santoso Lie, Ryo Shimomoto, Shohei Sakaguchi, Toshiyuki Ishimura, Shuichi Enokida, Tomohito Wada, and Toshiaki Ejima. Gait recognition using spectral features of foot motion. In *5th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, 2005.

[108] Agus Santoso Lie, Shuichi Enokida, Tomohito Wada, and Toshiaki Ejima. Magnitude and phase spectra of foot motion for gait recognition. In *11th International Conference on Computer Analysis of Images and Patterns (CAIP)*, 2005.

[109] Shuichi Enokida, Ryo Shimomoto, Tomohito Wada, and Toshiaki Ejima. A predictive model for gait recognition. In *Biometric Consortium Conference*, 2006.

[110] Cavanagh. *The Foot and Leg in Running Sports*, chapter The shoe-ground interface in running, pages 30–44. 1982. (Edited by R. P. Mack).