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

Davrondzhon Gafurov
Gjøvik University College
davrondzhon.gafurov@hig.no

Abstract

Biometric systems are becoming increasingly important, since they provide more reliable and efficient means of identity verification. Biometric gait recognition (i.e. recognizing people from the way they walk) is one of the recent attractive topics in biometric research. This paper presents biometric user recognition based on gait. Biometric gait recognition is categorized into three groups based on: machine vision, floor sensor and wearable sensor. An overview of each gait recognition category is presented. In addition, factors that may influence gait recognition are outlined. Furthermore, the security evaluations of biometric gait under various attack scenarios are also presented.

1 Introduction

One of the first important steps towards preventing unauthorized access is user authentication. User authentication is the process of verifying claimed identity. Conventionally, user authentication is grouped into three classes:

- Knowledge - based,
- Object (or Token) - based,
- Biometric - based.

The knowledge-based authentication is based on something one knows and is characterized by secrecy. The examples of knowledge-based authenticators are commonly known passwords and PIN codes. The object-based authentication relies on something one has and is characterized by possession. Traditional keys to the doors can be assigned to the object-based category. However, usually the token-based approach is combined with the knowledge-based approach. An example of this combination is a bank-card with PIN code. Biometric authentication is based on something one *is* [1].

In knowledge-based and object-based approaches, passwords and tokens can be forgotten, lost or stolen. There are also usability limitations associated with them. For instance, managing multiple passwords/PINs, and memorizing and recalling strong passwords are not an easy task. According to a survey, the heavy IT user has to

This paper was presented at the NIK-2007 conference; see http://www.nik.no/.

remember on average 21 passwords (some up to 70), 49% of the users write down or store their passwords in a file and 67% never change passwords [2]. Biometric-based person recognition lacks above mentioned difficulties of knowledge-based and object-based approaches. However, one of the most important aspects of biometrics is that they establish more direct and explicit link with humans than passwords or tokens do, since biometrics use measurable physiological and behavioral features of human being. Thanks to this, nowadays the demand for biometrics-based systems is increasing. There are various types of human traits that can be used as biometric, e.g. fingerprint, face, iris, hand geometry, gait and so on.

In this paper, we present a biometric recognition system based on gait. Gait is a person's manner of walking. Biometric gait recognition refers to verifying and/or identifying persons using their walking style. Human recognition based on gait is relatively recent, compared to the traditional approaches such as fingerprint recognition. From a technological perspective, biometric gait recognition can be grouped into three categories, namely machine vision (MV) based, floor sensor (FS) based and wearable sensor (WS) based, see Figure 1. In the rest of the paper, we will refer to these three gait recognition categories as MV-based, FS-based and WS-based, respectively.

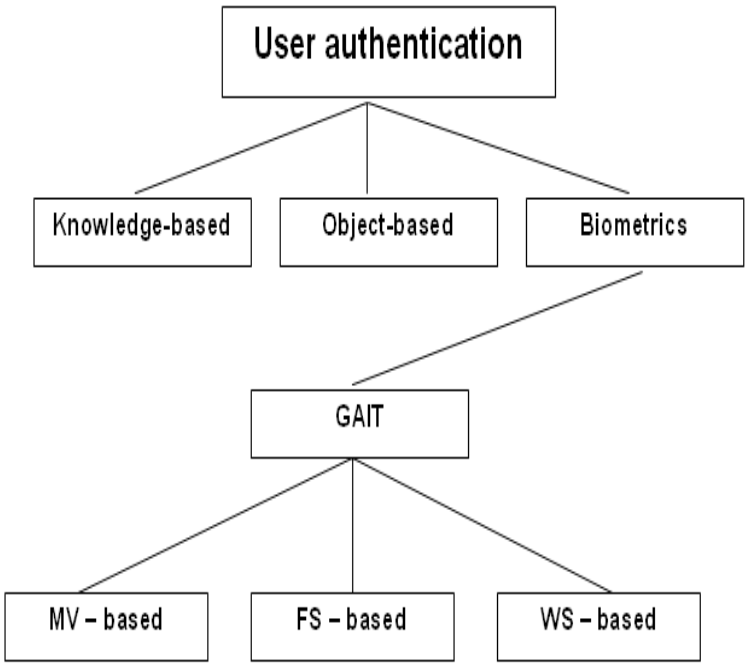

Figure 1: User authentication approaches

The remainder of the paper is structured as follows. Section 2 presents an overview of biometric system's operating modes and errors. Section 3 describes gait recognition approaches, factors that can influence gait recognition and combination of gait with other biometric modalities. Section 4 contains the results of security evaluation of gait biometrics under various attack scenarios. Section 5 concludes the paper.

2 Biometric system

Biometric systems follow the following stages of operation: 1) capture biometric sample of the person, 2) extract set of relevant features from captured sample, 3) and compare the extracted feature set against the template set in the database. Biometric systems operate in

two modes, verification (also called authentication) and identification. In the verification mode, the system performs a one to one comparison and the system's decision is either to accept or to reject a claimed identity. In the identification mode, the system performs one to many comparisons and the system's aim is to assign an identity to one of the user templates or to announce no match. In other words, the verification modes seeks an answer to the question "Am I who I claim I am?", while the identification searches for the question "Who am I?".

Biometric systems are not perfect. There are two important types of errors associated with biometric system, namely a false accept rate (FAR) and a false reject rate (FRR). The FAR is the probability of wrongfully accepting an impostor user, while the FRR is the probability of wrongfully rejecting a genuine user. System decisions (i.e. accept/reject) is based on so-called thresholds. By changing the threshold value, one can produce various pairs of (FAR,FRR). For reporting performance of biometric system in verification mode, researchers often use a decision error trade-off (DET) curve. The DET curve is a plot of FAR versus FRR and shows the performance of the system under different decision thresholds [3], see Figure 2. Using machine learning terminology, FAR and FRR are analogues to False Negative and False Positive, respectively. A modified version of the DET curve is a ROC (Receiver Operating Characteristic) curve, which is widely used in the machine learning community. The difference between DET and ROC curves is in ordinate axis. In the DET curve the ordinate axis is FRR, while in the ROC curve it is 1-FRR (i.e. probability of correct verification). Usually, to indicate the performance of biometric system by a single value in verification mode, an equal error rate (EER) is used. The EER is the point on the DET curve, where FAR=FRR, see Figure 2.

To evaluate the performance of a biometric system in identification mode, a cumulative match characteristics (CMC) curve can be used. The CMC curve is a plot of rank versus identification probability and shows the probability of a sample being in the top closest matches [4], see Figure 3. In identification mode, to indicate performance of the system by a single number, the recognition rate (i.e. identification probability at rank 1) is used. In the next sections, when performance of the method is referred to the recognition rate the system is evaluated in the identification mode, and when it is referred to the EER the system is evaluated in the verification mode. It should be also noted that the given performances (i.e. EER, recognition rates) in next sections are not intended for direct comparisons mainly due to differences in data sets and classification methods. They are intended to give an impression of overall performance of gait biometrics.

3 Biometric gait recognition

MV-based gait recognition

In this category, gait is captured using a video-camera from distance. Video and image processing techniques are employed to extract gait features for recognition purposes. BenAbdelkader et al. [6] used stride and cadence for person identification and verification. Johnson and Bobick [7] extracted static body parameters such as the height, the distance between head and pelvis, the maximum distance between pelvis and feet, and the distance between feet, and used them for recognition. Most of the MV-based gait recognition algorithms are based on the human silhouette [8, 9, 10]. That is the image background is removed and the silhouette of the person is extracted and analyzed for recognition, see Figure 4. For example, Liu and Sarkar [8] computed the average silhouettes over a gait cycle, and used the Euclidean distance between two averaged silhouettes to compute similarity.

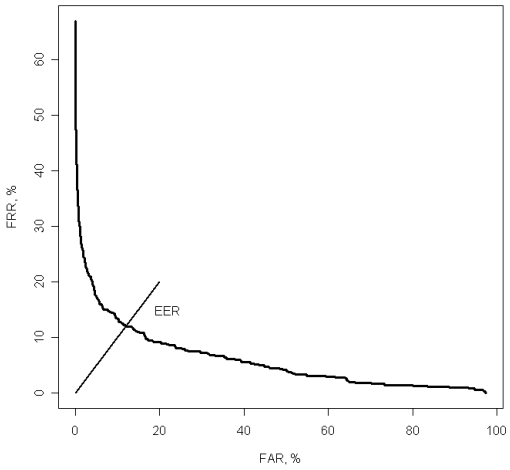

Figure 2: An example of DET curve from [5].

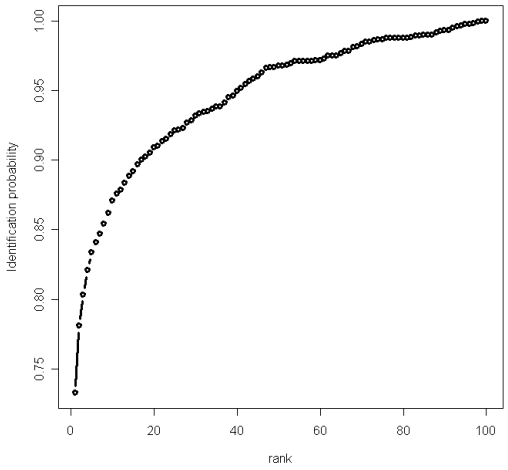

Figure 3: An example of CMC curve from [5].

In terms of performance, earlier MV-based gait recognition studies showed promising results, although the sample sizes were limited [11, 12]. Recent works with larger sample size (more than 100 persons in the database) still indicate the possibility of recognizing people from their gait [13, 14]. For example, Sarkar et al. [13] with a data set consisting of 1870 gait sequences from 122 subjects obtained 78% recognition rate (identification probability at rank 1). This performance has been improved further to achieve 95% by others [15, 16]. Most of the current gait recognition methods are MV-based.

The primary advantage of MV-based gait biometric compared to other modalities is in being captured from the distance when other biometrics are not accessible. Application areas for MV-based gait recognition are usually surveillance and forensics. Although MV-based gait analysis cannot constitute identification in terms of e.g. fingerprints, it can be a useful tool [17, 18]. For example, in a bank robbery case in Denmark, a court found gait analysis from video to be a valuable tool [18]. Usually, in robbery cases, the perpetrator uses a mask to hide his face and puts gloves on his hand, so that no face or fingerprints can be captured or left, but cameras can record the gait of the perpetrator.

FS-based gait recognition

In FS-based approach, a set of sensors or force plates are installed on the floor [19, 20, 21], see Figure 5. Such sensors enable to measure gait related features, when a person walks on them. Orr and Abowd [19] collected 1680 footstep profiles from 15 subjects. Using this data set, they achieved 93% correct recognition rate [19]. Suutala and Roning [20] investigated 31 different features (e.g. max. time value of heel strike, max. amplitude value of the heel strike, etc.) for recognition. By using 200 footsteps from 11 persons, they obtained 70.2% recognition rate [20]. Middleton et al. [21] used three features, stride length, stride cadence and time on toe to time on heel ratio for recognition. These features proved sufficient to achieve an 80% recognition rate based on data set from 15 individuals [21]. It is worth noting that in FS-based gait recognition, the performance was evaluated in the identification mode [19, 20, 21].

One of the main advantages of FS-based gait recognition is in its unobtrusive data

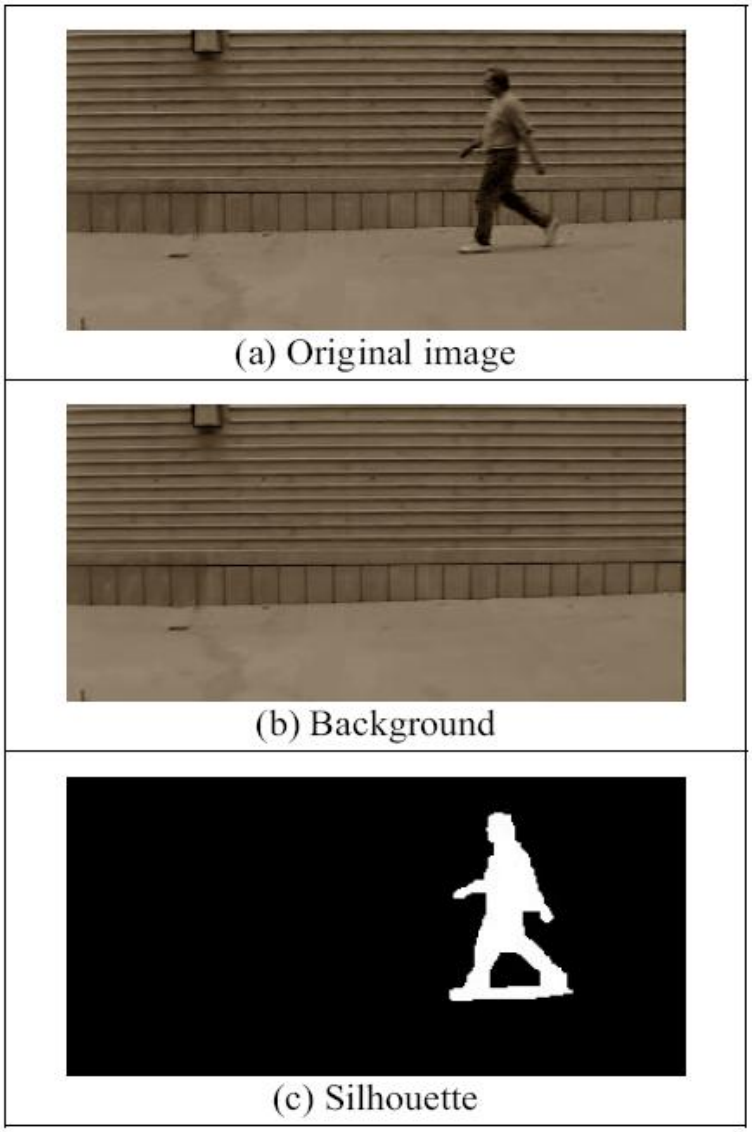

Figure 4: An example of silhouette extraction from [10]

collection. The FS-based gait recognition can be deployed in access control application and is usually installed in front of doors in the building. Such systems can find deployment as a standalone system or as a part of multimodal biometric system [21]. In addition to providing identity information, the FS-based gait system can also indicate location information within a building [19].

WS-based gait recognition

In WS-based gait recognition, gait is collected using body worn motion recording (MR) sensors [22, 23, 24, 25]. The MR sensors can be worn at different locations on the human body. The acceleration of gait, which is recorded by the MR sensor, is utilized for authentication. To our best knowledge, the first WS-based gait recognition was described by Morris [26]. However, the focus of this work was primarily on clinical aspects of the system [26]. Ailisto et al. [22] proposed WS-based gait recognition as a biometric authentication. In their approach, the MR sensor was attached to the waist of the subject. Using waist acceleration from 36 subjects, an EER of 6.4% was achieved [22]. In [23],

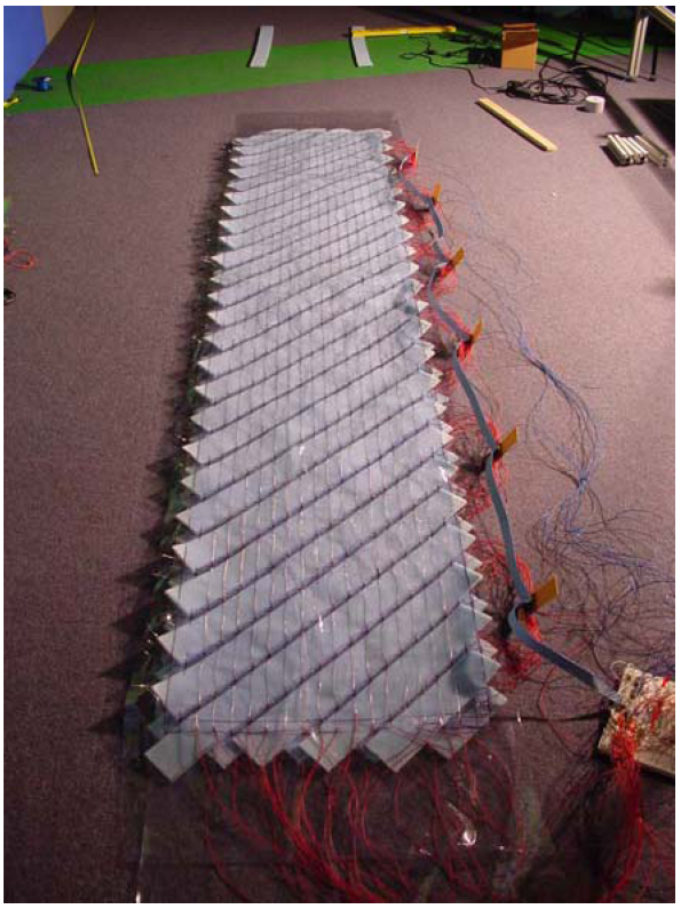

Figure 5: A prototype sensor mat from [21]

the MR sensor was attached to the belt of the subjects, around the right hip as shown in Figure 6. Using the averaged cycle method on a gait data set from 22 subjects, the EER of 16% was achieved [23]. In [24], the MR sensor was attached to the lower part of the leg as shown in Figure 7. Using gait sequences from 21 subjects and applying two methods, histogram similarity and cycle length, the EER of 5% and 9% were obtained [24]. In [25], the MR sensor was carried in the trousers pocket. Four different methods, namely absolute distance, correlation, histogram similarity and higher order moments were applied, and the EER of 7.3%, 9.2%, 14% and 20% were obtained, respectively [25]. In all these mentioned WS-based studies (except in [25]), performance was evaluated only in the verification mode. In [25], performance of WS-based approach was also evaluated in identification mode, and a recognition rate of 86.3% was achieved.

One of the main advantages of the WS-based gait recognition over several other biometric modalities is its unobtrusive data collection. The WS-based approach was proposed for protection and user authentication in mobile and portable electronic devices. With advances in miniaturization techniques it is feasible to integrate the MR sensor as one of the components in personal electronic devices. Mobile phones can be used in applications such as m-commerce [27] and m-banking [28]. This implies that such mobile devices process and store financial and private data. Due to these facts, the risk of being the target of an attack may increase because of not only the device value per se but also because of the information stored in it. Some people tend to leave their mobile phones unattended, forget or even lose. According to the UK statistics, a mobile phone is stolen approximately every three minutes [29]. Therefore, in the future, mobile phones may

Figure 6: The MR sensor attached to the hip [23].

Figure 7: The MR sensor attached to the lower leg [24].

employ constant verification of the user identity (i.e. continuous authentication) [30]. One of the important requirements in continuous authentication is unobtrusiveness. The WS-based method can be a very good candidate to fulfill this requirement, compared to current knowledge-based mechanisms.

Challenges

Although the performance of all three biometric gait recognition approaches are encouraging, there are several factors that may negatively influence the accuracy of such approaches. We can group the factors that influence a biometric gait system into two classes (not necessarily disjoint):

- *External factors*. Such factors mostly impose challenges to the recognition approach (or algorithm). For example, viewing angles (e.g. frontal view, side-view), lighting conditions (e.g. day/night), outdoor/indoor environments (e.g. sunny, rainy days), clothes (e.g. skirts in MV-based category), walking surface conditions (e.g. hard/soft, dry/wet grass/concrete, level/stairs, etc.), shoe types (e.g. mountain boots, sandals), object carrying (e.g. backpack, briefcase) and so on.

- *Internal factors*. Such factors cause changes of the natural gait due to sickness (e.g. foot injury, lower limb disorder, Parkinson disease etc.) or other physiological changes in body due to aging, drunkenness, pregnancy, gaining or losing weight and so on.

One of the public gait data set that was published by Sarkar et al. [13] 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 [13].

Some of the external factors may have various effects on different gait recognition approaches. For example, while carrying an object may influence the dynamics of gait both in WS-based and MV-based categories, it may also create additional difficulties in

MV-based category during human silhouette extraction. The effect of carrying backpack from WS-based perspective is studied in [25]. When carrying backpack the EER increased from 7.3% to 9.3% and recognition rate dropped from 86.3% to 86.2% [25]. Although some of the external factors have been addressed, others are not investigated yet. Moreover, to our knowledge, so far internal factors of the gait have not studied in the context of biometric gait recognition. One needs to cope with such factors in order to develop robust gait recognition systems.

Combining gait with other biometrics

Multi-modal biometric systems combine evidences from several biometric modalities to establish more reliable and accurate identification. In a multi-modal biometric system, gait helps in improving the accuracy of the system when it is integrated with other biometrics [31, 32, 29]. Shakhnarovich et al. [31] combined face and MV-based gait. The frontal face was captured by one camera and the 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 [31]. Zhou et al. [32] used a single camera 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% [32]. In [29], WS-based gait recognition was combined with speaker verification. Performance proved to be significantly better in a noisy environment, compared to when speaker verification was used alone. The EER was in the range of 2%-12%, less than half of the EER of individual modalities [29].

Apart from accuracy improvement, another important benefit of the multi-modal biometric systems is in being more robust against attacks. Indeed, it requires more effort to forge or spoof several biometrics simultaneously compared to only one modality.

4 Security strength of gait biometric

Along with uniqueness characteristics, another important requirement for human physiological or behavioral characteristics to be considered as a biometric is its robustness against attacks. Despite much research in biometric gait recognition, not many works have studied the security of gait biometric per se. In biometric gait recognition, most of the efforts are devoted in the directions of improving recognition accuracy and reducing the effect of influencing factors. The impostors are usually assumed passive and unknowledgeable.

In our previous work, we introduced a two types of impostor attempts, namely *passive impostor attempt* and *active impostor attempt* [5]. In the passive impostor attempts, the attacker walks as himself and this walking sample is matched against targeted gait in the database. This is a traditional approach that was used in many gait recognition systems. In active impostor attempts, the attacker tries the followings: 1) modifies his walking style hoping to better match the targeted person gait and the modified gait of the attacker is matched against the target persons gait sample, or 2) posses some knowledge about the vulnerability of authentication system. For example, such knowledge may include whose gait in the database is the closest to the attacker's gait or what is the gender of the targeted person, etc. Thus, we distinguish between a *friendly evaluation scenario* and a *hostile evaluation scenario*. In the friendly evaluation scenario, all impostor attempts consists of passive impostor. In the hostile evaluation scenario, impostor attempts consists of active impostor attempts. In general, the friendly evaluation scenario is corresponds to

the discriminating power of the system, while the hostile scenario evaluation shows the robustness or vulnerability of the system against various types of attacks.

We have studied different hostile scenarios on WS-based gait authentication system [23, 5, 33]. In [23], a study of minimal effort mimicking on gait biometrics is presented. Minimal effort mimicking refers to the attempts, where impostors have a limited number of mimicking attempts and restricted time to study the target person's gait. The study indicated that trying to walk as someone else is unlikely to improve the chances of impostors to be accepted by the system [23]. Although the results were encouraging, the number of samples were limited. A more elaborate study of spoof attacks with a large data set (100 subjects in experiment) has been carried out in [5]. In particular, two types of attack scenarios are investigated, namely the minimal effort impersonation and a scenario where attackers knew their closest person (in terms of gait similarity) in the database. In the former scenario, impostors were trying to walk as the target person, while in the latter scenario, impostors knew their target person in the database whose gait was the closest to the gait of the attacker. In [33], an attack scenario, where the impostor knows the gender of the person in the database, was studied. In general, it appears that biometric gait is robust against the minimal effort impersonation (or spoof) attacks [23, 5]. However, a gait authentication system can be vulnerable to knowledgeable attackers who, for example, know the person in the database whose gait is close to their gait [5] or know the gender of the persons in the database [33]. Therefore, counter-measures (e.g. combining gait with other modalities) are necessary to defend against these types of attack.

5 Conclusion

In this paper, an overview of biometric gait recognition is given. Depending on the way the gait data is captured, biometric gait verification and identification is categorized into three classes (MV-based, WS-based and FS-based). The primary advantage of MV-based gait biometric is in being captured from the distance. The main advantages of WS-based and FS-based gait biometric is in providing unobtrusive user authentication and identification. It is worth noting that we do not consider gait as a replacement for traditional authentication mechanisms (passwords, fingerprints, etc.) but rather a complementary biometric. In a multi- modal biometric system, gait helps to increase the accuracy of the system too. However, there are many factors that can negatively influence the accuracy of a gait recognition system. An investigation of these factors is very important towards developing robust systems. With respect to gait security, studies also indicated that gait biometric is robust against minimal effort impersonation attacks. However, impostors who know their closest person in the database or the gender of the users in the database can be a threat to a gait authentication system.

References

[1] A. K. Jain, A. Ross, and S. Prabhakar. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics*, 14:4–20, January 2004.

[2] 2002 NTA Monitor password survey. http://www.out-law.com/page-3193, Last visit: 01.06.2007.

[3] A. Martin, G. Doddington, T. Kamm, M. Ordowski, and M. Przybocki. The DET curve in assessment of detection task performance. In *Eurospeech'97*, pages 1895–1898, 1997.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] Zongyi Liu and Sudeep Sarkar. Simplest representation yet for gait recognition: Averaged silhouette. In *International Conference on Pattern Recognition*, pages 211–214, 2004.

[9] Zongyi Liu, Laura Malave, and Sudeep Sarkar. Studies on silhouette quality and gait recognition. In *Computer Vision and Pattern Recognition*, pages 704–711, 2004.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

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

[15] 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.

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

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

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

[19] 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.

[20] J. Suutala and J. Rning. 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] J.J. Wang, Z. Song, P. Lei, and R.E. Sheriff. Design and evaluation of m-commerce applications. In *Asia-Pacific Conference on Communications*, pages 745– 749, 2005.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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.