Fusion of Gait and Fingerprint for User Authentication on Mobile Devices

Mohammad O. Derawi*†, Davrondzhon Gafurov*, Rasmus Larsen†, Christoph Busch* and Patrick Bours*
* Norwegian Information Security Lab., Gjøvik Univeristy College, Norway
* Email: {firstname}.{lastname}@hig.no
† Department of Informatics, Technical University of Denmark, Denmark
† Email: rl@imm.dtu.dk

***Abstract*—A new multi-modal biometric authentication approach using gait signals and fingerprint images as biometric traits is proposed. The individual comparison scores derived from the gait and fingers are normalized using four methods (min-max, z-score, median absolute deviation, tangent hyperbolic) and then four fusion approaches (simple sum, user-weighting, maximum score and minimum core) are applied. Gait samples are obtained by using a dedicated accelerometer sensor attached to the hip. The proposed method is evaluated using 7200 fingerprint images and gait samples. Fingerprints are collected by a capacitive line sensor, an optical sensor with total internal reflection and a touchless optical sensor. The fusion results of these two biometrics show an improved performance and a large step closer for user authentication on mobile devices.**

I. Introduction

Mobile devices – particularly mobile phones – are being found in almost everyone's hip pocket these days all over the world. The security issues related to ever-present mobile devices are becoming critical, since the stored information in them (names, addresses, messages, pictures and future plans stored in a user calendar) has a significant personal value. Moreover, the services which can be accessed via mobile devices (e.g., m-banking and m-commerce, e-mails etc.) represent a major value. Therefore, the danger of a mobile device ending up in the wrong hands presents a serious threat to information security and user privacy. Statistics in the UK show that "a mobile phone is stolen approximately every third minute" [1].

Unlike passwords, PINs, tokens etc. biometrics cannot be stolen or forgotten. The main advantage of biometric authentication is that it establishes explicit link to the identity because biometrics use human physiological and behavioral characteristics.

Fingerprint recognition is a broadly researched area with many commercial applications available [2]. Recent publications show that the performance of a baseline system deteriorates from Equal Error Rate (EER) around 0.02 % with very high quality images to EER = 25.785 % due to low qualities images [3] [4]. Thus active research is still going on to improve these numbers.

Video-based gait recognition has been studied for a long time [5][6][7][8] for the use in surveillance systems, e.g. recognizing a unlawful person from a security camera video. Recently accelerometer-based gait recognition has been suggested [9][10].

An individuals gait is known to differ from person to person and to be fairly stable [12], whereas intentional imitation of another person's gait is complicated [13][14]. However, the biometric recognition performance of gait recognition is not as accurate as fingerprint recognition. Researcher are today still improving results when using accelerometers [10][16]. Accelerometer-based gait recognition can today be used for detecting whether a mobile device is being carried by one and the same subject [18], however this has not been applied for embedded accelerometer-based gait recognition in mobile devices. Instead, we see a variety of other biometric modalities that have been planned and used for this idea, such as signature [19], voice [20][21] and fingerprints, which have been employed in a commercial PDA device [22] and newer mobile phones [23]. All of these approaches except gait recognition (and voice) need explicit procedures for user authentication, e.g. writing on a touch screen. And in view of the fact that more and more mobile devices at the present time embed accelerometers (and few fingerprint sensors), people can walk directly to their school, job, friends, family without perceiving gait recognition as a major threat to their privacy. On the other hand, mobile devices are often used under difficult conditions that make the users walk unstable in walking situations when jumping, walking downhill, uphill, etc.

In this paper we present a fusion of fingerprint recognition and accelerometer-based gait recognition as means of verifying the identity of the user of a mobile device. The main purpose of this paper is to study how it is possible to lower down the user effort while keeping the error rates in an acceptable and practical range. However, a fusion between three single modalities in the same time (fingerprint, voice and gait) have already been proposed [24], but our proposal is different since we are only focusing on gait-recognition and fingerprint-recognition as a whole. In contrast to [24], we also have a different setting for both modalities. We are testing out multiple fingerprint scanners with with multiple extractors and comparators for the fingerprint recognition where two of the scanners which are not optical, are more suitable for mobile devices. And finally we are also analyzing gait-recognition

Fig. 1. Left: touchless optical sensor (TST BiRD3), Middle: optical sensor (DP U.4000), Right: capacative line sensor (IDEX SmartFinger® IX 10-4) and a fingerprint image from each database, at the same scale factor.

differently. Therefore, this proposal is a realistic approach to be implemented in mobile devices for user authentication.

II. Multimodal Biometrics

Multi-modal and Multi-biometric fusion is a way of combining two biometric modalities into one single wrapped biometric system to make a unified authentication decision. During the past years of increased use of biometrics to authenticate or identify people, there has also been a similar increase in use of multimodal fusion to overcome the limitations of unimodal biometric system. There are several benefits when combining multiple biometric systems. The cohesive decision leads to a significant improvement in precision and simultaneously reduces the false acceptance rate and false rejection rate. The second benefit is that the more biometric attributes we apply the harder it is to spoof them. The third benefit is the reduction of noisy input data, such as a humid finger or a dipping eye-lid, since if one the input is highly noisy, then the other biometric sample might have a very high quality to make an overall reliable decision. This can also be seen as the fault-tolerance, that is, to continue operating properly in the event of the failure if one system breaks down or compromised then the other might be sufficient to keep the authentication process running. [25][26]

Several of applications in the real world require a higher level of biometric performance than just one single biometric measure to improve security. These kinds of applications will remove the need for national identity cards and security checks with fusion for example air travel, hospitals and et cetera. And for the individual who are not able to present a stable biometric characteristic to an application, then provision is needed.

III. Data Collection

A. Fingerprint Image Data

The fingerprint data used in this paper are captured by two commercial sensors and a prototype sensor as shown in Figure 1. Further detailed information of the sensors is described in Table I. The experiment had 40 participating volunteers for providing fingerprints for database DB1, DB2, and DB3 where 10 were female and 30 males.

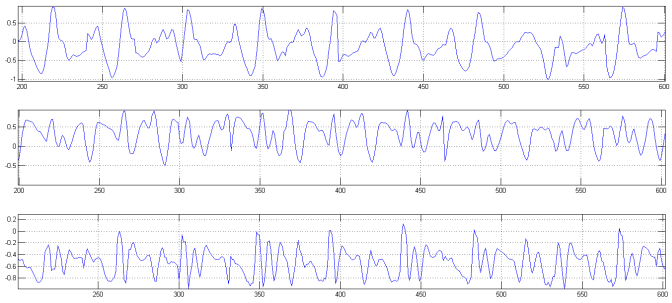

Fig. 2. Acceleration of motion recording in three dimensional axis. Top: x-acceleration, Middle: y-acceleration and Botton: z-acceleration

Database	**DB_1**	**DB_2**	**DB_3**
Sensor Name	**TST**	**Dig. Persona**	**IDEX**
Model	BiRD3	U.4000	SmartFinger® IX 10-4
Resolution	500 DPI	512 DPI	500 DPI
Gray Scale	8-bit	8-bit	8-bit
Acquisition	19x16 [mm]	14.6x18.1[mm]	10x4[mm]
Temperature	5-50 [C]	5-35 [C]	-40-85 [C]
Dimension	160x115x95	79x49x19	10x4x0.8

TABLE I
Sensor Information. [C] = celsius and [mm] = milimeter.

B. Gait Data

In this experiment, 40 subjects participated and walking were recorded. The gender distribution was the same as with the fingerprint experiment. Subjects were told to walk normally for a distance of about 20 meters in a hall on flat ground. At the end of the hall the subjects had to wait 2 seconds, turn around, wait, and then walk back. A so called Motion Recording Sensor (MRS) was used to record the motion. The MRS measures acceleration in three orthogonal directions, namely up-down, forward-backward and sideways as shown in Figure 2. It is also equipped with a storage unit capable of storing 64 megabyte of acceleration data and has both a USB and a Bluetooth-interface, which makes it possible to transfer the data to either a computer, a cellular phone or a PDA. The sampling frequency of the MRS was about 100 samples per second and its dynamic range was between -6g and +6g. During walking trials the MRS was attached to the hip of the persons. Thus, we analyze hip movements for recognition purposes.

C. Multi-biometric Data

The subjects in the fingerprint and gait experiments are different. However, assuming non-correlation of persons fingerprint patterns and gait (walking style) we randomly pick up a gait sample and assign it to fingerprint sample.

IV. Feature Extraction and Comparison

A. Fingerprint Analysis

In order to measure the sensor performance we have applied three different commercial minutia extractor for the feature extraction:

1) Neurotechnology, Verifinger 6.0 Extended SDK
2) TST Biometrics, Basic SDK 2.1
3) NIST, NIST2 SDK (mindtct, bozorth3)

All of the above mentioned SDKs includes functionality to extract a set of minutiae data from an individual fingerprint image and compute a comparison-score by comparing one set of minutiae data with another. The image processing of obtaining the templates can be found in the each SDKs documention report. What can be seen from the description is that NIST and TST are only designed to compare images originating from the same template extractor only. Such extractors or comparators are identified as non-standardized (e.g. proprietary). However, Neurotechnolgy supplier provides ISO and ANSI interoperability due to the standardized template formats they offer.

B. Gait Analysis

The feature extraction for the gait-signals was done by applying different signal processing methods, in contrast to fingerprint. The extraction of features was briefly performed in the following order:

1) *Time interpolation*: Linear time interpolation on the three axis data (x,y,z) since the time intervals between two observation points are not always equal.
2) *Noise reduction*: The weighted moving average filter has been applied since it is fast and implementation is easy.
3) *G-force conversion*: The raw data does not contain g-force values. Therefore it must be converted by using the properties of the sensor in order to achieve values of g.
4) *Resultant Vector*: The resultant vector will be created from the converted values from all three directions.

$$r_t = \sqrt{x_t^2 + y_t^2 + z_t^2}, t = 1, ..., N$$

where r_t, x_t, y_t ,z_t are the magnitudes of resulting, vertical, horizontal and lateral acceleration at time t.

5) *Cycle Detection*: From the resultant vector, steps are being detected meaning that cycles can be extracted.
6) *Feature Vector Creation*: All cycles are being normalized to have equal length and the median cycle will be the representative feature vector.

For the comparison part, the feature vector was compared to a reference feature vector using the dynamic time warping (DTW) since it is able to find the optimal alignment between two time series.

V. Score Level Fusion

A. Representations - Assigning Gait To Finger

Each participant acquired all of his or her 10 fingers in 6 sessions, resulting in 60 templates per scanner. In the gait experiment, we retrieved 12 templates for each person. When combining two biometric against each other, we must ensure that the template ratios from all biometrics are in the same domain. The 10 fingerprints of 6 sessions are not comparable with 12 gait templates of one session. Thus, we must ensure that the domain are within the same range. Two possible opportunities occur:

1) To distribute/copy the 12 templates into 60 templates.
2) To reduce the number of fingerprints (60 templates) to 12 templates.

Second approach would not be a reasonable approach since a lot of data information is lost and performance would change slightly. Therefore we chose the first mentioned approach. This solution had the important fact and awareness of ensuring that duplicates in different sessions for each finger were not assigned. This mean that the solution for assigning was performed as following:

- From the gait templates, we chose 6 random templates out of 12
- These templates were assigned to the first finger
- To avoid duplication for when assigning all 10 fingers for one session, we just choose the next gait template in the list.
- Table II shows how the points mentioned above are distributed into a gait matrix.

$S_{ID} \Downarrow$ / $F_{ID} \Rightarrow$	1 (Rnd)	2	3	4	...	10
1	G_3	G_4	G_5	G_6	...	G_{12}
2	G_5	G_6	G_7	G_8	...	G_2
3	G_{11}	G_{12}	G_1	G_2	...	G_8
4	G_7	G_8	G_9	G_{10}	...	G_4
5	G_1	G_2	G_3	G_4	...	G_{10}
6	G_9	G_{10}	G_{11}	G_{12}	...	G_6

TABLE II
AN EXAMPLE OF RANDOMLY ASSIGNING 12 GAIT TEMPLATES (FROM ONE SUBJECT) TO 10 FINGERS . RND = [RANDOM PICKED], S_{ID} = [SESSION-ID], F_{ID} = [FINGER-ID] AND G_{1-12} = [GAIT TEMPLATE FROM 1-12].

B. Score Normalization

The comparison scores at the output of the individual comparators may not be homogeneous. For example, the dynamic time warping comparator used for gait outputs a distance (dissimilarity) measure while fingerprint comparators output a proximity (similarity) measure. Thus, we simple calculate the multiplicative inverse for the distance score like shown in Equation 1.

$$Score_{similarity} = \frac{1}{Score_{distance}} \cdot factor \qquad (1)$$

Furthermore, the outputs of the individual comparators need not to be on the same numerical scale (range). And finally, the comparison scores at the output of the comparators may follow different statistical distributions [27].

Score normalization is therefore used to map the scores of each simple-biometric into one common domain. Some of

the methods are based on the Neyman-Pearson lemma, with simplifying assumptions. Mapping scores to likelihood ratios, for example, allows them to be combined by multiplying under an independence assumption. The other approaches may be based on modifying other statistical measures of the comparison score distribution.

What is relevant to know is that score normalization is related very close to score-level fusion since it affects how scores are combined and interpreted in terms of biometric performance.

Table IV shows the normalization functions, which are applied in this paper. The relevant abbreviations for the statistical measures are given Table III.

Statistical measures	**Genuine distribution**	**Impostor distribution**	**Both**
Minimum score	S^G_{Min}	S^I_{Min}	S^B_{Min}
Maximum score	S^G_{Max}	S^I_{Max}	S^B_{Max}
Mean	S^G_{Mean}	S^I_{Mean}	S^B_{Mean}
Median score	S^G_{Med}	S^I_{Med}	S^B_{Med}
Score standard deviation	S^G_{SD}	S^I_{SD}	S^B_{SD}

TABLE III
SYMBOLS USED FOR SCORE NORMALIZATION FORMULAS [25].

Method	**Formula**
Min-Max (MM)	S' = $(S - S^B_{Min})$ / $(S^B_{Max}$ - $S^B_{Min})$
Z-Score	S' = $(S - S^I_{Mean})$ / (S^I_{SD})
Median Absolute Deviation	S' = $(S - S^B_{Med})$ / $median(S - S^B_{Med})$
Hyperbolic Tangent	S' = 0.5 (tanh(0.01 (S-S^G_{Mean}) / $S^B_{SD}) + 1)$

TABLE IV
APPLIED SCORE NORMALIZATION APPROACHES [25].

C. Score Fusion

When individual biometric comparators output a set of possible matches along with the quality of each match (comparison score), integration can be done at the comparison score level, see Figure 3. The comparison score output by a comparator contains the richest information about the input biometric sample in the absence of feature-level or sensor-level information. Furthermore, it is relatively easy to access and combine the scores generated by several different comparators. Consequently, integration of information at the comparison score level is the most common approach in multi-modal biometric systems. Table V lists the fusion approaches applied in this paper and outlined from [25].

Method	**Formula**
Simple Sum	$\sum$ (i=1 to N) S'_i
Minimum Score	min (i=1 to N) S'_i
Maximum Score	max (i=1 to N) S'_i
User Weighting	$\sum$ (i=1 to N) $W^*_i \cdot S'_i$

TABLE V
EXAMPLES OF SCORE FUSION METHODS [25].

VI. RESULTS

The results shown below are algorithm performances for biometric verification purposes. Experiments were performed in order to compare the following configuration:

1) Performance of single modalities, i.e. fingerprint recognition and gait recognition separately
2) Performance of multi-modalities, i.e. fingerprint recognition and gait recognition fused

Table VI gives an overview of the single-modality performances. In general, we see that Neurotechnology's extractor and comparator is performing better than NIST's and TST's for all three fingerprint databases with a lowest EER of 1.12 %.

Scanner	**NIST**	**Neurotechnology**	**TST Basic**	**Gait**
DB_1: TST	29.91	1.23	11.08	9.39
DB_2: Digital Persona	19.80	1.12	5.82	9.61
DB_3: IDEX	18.56	2.56	5.50	9.43

TABLE VI
EERS OF FINGERPRINT RECOGNITION (COLUMN 2 - 4) AND GAIT RECOGNITION (LAST COLUMN).

The performances of gait recognition for all three databases using dynamic time warping lies approximately around the same with a lowest EER of 9.43 %.

Table VII takes all of Neurotechnologys fingerprint scores (since the are performing best) and is fused with gait data. Given an EER of 1.23 for fingerprint and an EER of 9.39 we gain an overall fused performance of EER = 0.23 %. However,

Finger	**Gait**	**Finger + Gait**	**Normalization**	**Fusion**
1.23	9.39	0.23	MinMax	Weighted
1.12	9.61	0.39	MAD	Simple Sum
2.56	9.43	0.57	MAD	Simple Sum

TABLE VII
SMALLEST EERS AFTER FUSION. THE TWO LAST COLUMNS SHOWS WHICH NORMALIZATION AND FUSION APPROACHES WERE APPLIED

Table VIII shows how large an improvement can be done

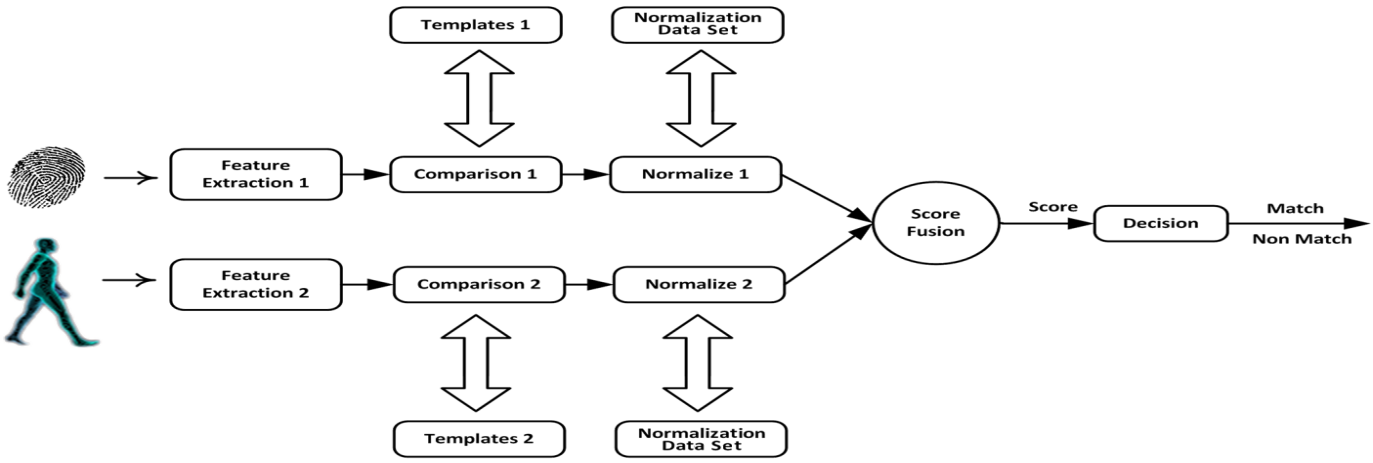

Fig. 3. Overview of the proposed method in the score-level fusion

by having high numbers of EERs. Given that fingerprint has an EER of 19.80 and gait has an EER of 9.61 we gain an improved EER of 1.63.

Finger	Gait	Finger + Gait	Normalization	Fusion
29.91	9.39	3.45	MAD	Max Score
19.80	9.61	1.63	MAD	Simple Sum
18.56	9.43	3.27	MAD	Simple Sum

TABLE VIII
MOST IMPROVED EERS AFTER FUSION. THE TWO LAST COLUMNS SHOWS WHICH NORMALIZATION AND FUSION APPROACHES WERE APPLIED

VII. DISCUSSION

Since personal handhold devices at present time only offer means for explicit user authentication, this authentication usually takes place one time; only when the mobile device has been switched on. After that the device will function for a long time without shielding user privacy. If it is lost or stolen, a lot of private information such as address book, photos, financial data and user calendar may become accessible to a stranger. Even the networking capabilities on the handhold device can be used without restraint until the holder of the device discovers the loss of it and informs this to the network provider. In order to decrease the risks to the owner's security and privacy, mobile devices should verify its user regularly and discreetly who in fact is carrying and using them. Gait recognition is well-suited for this purpose but is difficult under unusual and challenging conditions. In view of the fact that the risk of a handhold device being stolen is high in public area (transport, shopping areas etc), the method for unobtrusive user authentication should work. Since people frequently move about on foot (at short distances) in places where the probability of losing a handhold device are high, a fusion of gait processing with biometrics such as fingerprint recognition is an opportunity to protect personal devices in noisy and normal environments. A possible application scenario of a multi-modal biometric user verification system in a mobile device could be as follows; When a device such as a mobile phone, is first taken into use it would enter a "practicing" learning mode for an appropriate time session, say 24 hours. For this period of time the system would not only form the gait and fingerprint templates, but also investigate the solidity of the behavioral biometrics with respect to the user in question. Password-based or PIN code user authentication would be used during the learning session. If the solidity of the gait and fingerprint biometrics was sufficient enough, the system would go into a biometric authentication "state", a state that will need confirmation from the owner. In this state the system would asynchronously verify the owner's identity every time the owner walked while carrying the phone different places or eventually talked into it. The system would be in a safe state for a certain period of time after verification. If new verification failed, the system would use other means to verify the user, e.g. asking for fingerprint.

Gait biometrics is a behavioral biometrics, and gait can be affected by different factors. Using wearable sensors in gait recognition is a quite new field and therefore a lot of further research would be needed. By looking at topics that are directly connected to this paper it is natural to include more testing conditions, like e.g. walking up- or downhill, injuries, tiredness, heavy load carrying , high-heeled shoes wearing etc. but it would also be interesting to look at several types of environments like the surface, e.g. walking on grass, bad grounds, gravel, sand, etc.

Although the use of gait biometrics alone might be insufficient for user authentication, experiments during this project has shown that its use as a complementary modality to fingerprint recognition improves the performance.

VIII. CONCLUSION

The multi-modal biometric method for frequent authentication of users of mobile devices proposed in this paper was investigated in a technology test. It contained fingerprints and gait data with placement of the accelerometer module in the hip.

Fingerprint-based recognition resulted in different performances of using three different minutia extractors and comparators. The best functioning extractor and comparator pair was Neurotechnologys template extractor and comparator. The algorithm performance resulted in an EER of 1.12 % for DB_2, while DB_1 and DB_3 resulated in EER = 1.23 % and EER = 2.56 %, respectively.

Further, our experimental results show that in all cases that fused algorithm performance (finger + gait) was significantly improved compared to performances of individual modalities. Under the use of NIST extractor and comparator, where EER exceeds 18 %, multi-modal authentication achieved EER of 1.63 % - 3.45 %. In cases, where fingerprint modality alone performed well enough (EER between 1.23 % - 2.56 %), the performance of the combined finger and gait modalities was further improved to EER of 0.23 % - 0.57 % .

The shown results suggest the possibility of using the proposed method for protecting personal devices such as PDAs, smart suitcases, mobile phones etc. In a future of truly pervasive computing, when small and inexpensive hardware can be embedded in various objects, this method could also be used for protecting valuable personal items. Moreover, reliably authenticated mobile devices may also serve as an automated authentication in relation to other systems such as access control system or automated external system logon.

IX. Acknowledgments

We would like to thank IDEX (www.idex.no) for using their prototype sensor for testing. And furthermore thank all of our volunteers participating in the data collection.

References

[1] Biometrics for secure mobile connections. http://www.21stcentury.co.uk/technology/biometrics-for-mobiles.asp. [Online; accessed 08-January-2010].

[2] Nist image group's fingerprint research. http://www.itl.nist.gov/iad/894.03/fing/fing.html. [Online; accessed 25-February-2010].

[3] Fvc2006 the fourth international fingerprint verification competition. http://bias.csr.unibo.it/fvc2006/results/O_res_db2_a.asp. [Online; accessed 25-February-2010].

[4] Fvc2004 the third international fingerprint verification competition. http://bias.csr.unibo.it/fvc2004/results.asp. [Online; accessed 25-February-2010].

[5] S.A. Niyogi and E.H. Adelson. Analyzing and recognizing walking figures in xyt. *CVPR*, 94:469–474.

[6] Chiraz BenAbdelkader, Ross Cutler, Harsh Nanda, Harsh N, and Larry Davis. Eigengait: Motion-based recognition of people using image self-similarity. *Audio and Video-based Person Authentication (AVBPA)*.

[7] Mark S. Nixon, John N. Carter, Jamie D. Shutler, and Michael G. New advances in automatic gait recognition. *Information Security Technical Report*, 7(4):23–35, 2002.

[8] L. Wang, T.N. Tan, W.M. Hu, and H.Z. Ning. Automatic gait recognition based on statistical shape analysis. 12(9):1120–1131, September 2003.

[9] Jani Mantyjarvi Elena Vildjiounaite Satu-Marja Makela Heikki J. Ailisto, Mikko Lindholm. Identifying people from gait pattern with accelerometers. *In Proceedings of the SPIE*, 5779:7–14, 2005.

[10] Davrondzhon Gafurov, Einar Snekkenes, and Patrick Bours. Improved gait recognition performance using cycle matching. In *International Conference on Advanced Information Networking and Applications*, 2010. (to appear).

[11] L. Bianchi, D. Angelini, and F Lacquaniti. Individual characteristics of human walking mechanics. 436:343–358, 1998.

[12] Davrondzhon Gafurov, Einar Snekkenes, and Tor Erik Buvarp. Robustness of biometric gait authentication against impersonation attack. In *OTM Workshops (1)*, pages 479–488, 2006.

[13] Bendik B. Mjaaland. Gait mimicking - attack resistance testing of gait authentication systems. Master's thesis, Norwegian University of Science and Technology, 2009.

[14] Patrick Bours and Raju Shrestha. Eingensteps: A giant leap for gait recognition. *In 2nd International Workshop on Security and Communication Networks (to appear)*, 2010.

[15] Jonathan Lester, Blake Hannaford, and Gaetano Borriello. Are you with me?" – using accelerometers to determine if two devices are carried by the same person. In *Proceedings of Second International Conference on Pervasive Computing (Pervasive 2004*, pages 33–50, 2004.

[16] Luann Rragami, Maurice Gifford, and Nicholas Edwards. Dsv - questions remain... *Biometric Technology Today*, 11(11):7, 2003.

[17] Lifeng Sang, Zhaohui Wu, and Yingchun Yang. Systems, man and cybernetics. *IEEE International Conference on Systems, Man and Cybernetics, System Security and Assurance*, 4:3116 – 3121, 2003.

[18] Heikki Ailisto, Ville Haataja, Vesa Kyllönen, and Mikko Lindholm. Wearable context aware terminal for maintenance personnel. In *EUSAI*, pages 149–159, 2003.

[19] Jean-François Mainguet. Biometrics for large-scale consumer products. In *IC-AI*, pages 310–314, 2003.

[20] Intelligent touch controls, enhanced security and touch control for exceptional mobile devices. http://www.atrua.com/products-wireless.cfm. [Online; accessed 25-February-2010].

[21] Elena Vildjiounaite, Satu-Marja Mäkelä, Mikko Lindholm, Vesa Kyllönen, and Heikki Ailisto. Increasing security of mobile devices by decreasing user effort in verification. In *ICSNC*, page 80. IEEE Computer Society, 2007.

[22] *ISO/IEC TR 24722:2007, Information technology - Biometrics - Multimodal and other multibiometric fusion, 2007.*

[23] Arun A. Ross, Karthik Nandakumar, and Anil K. Jain. *Handbook of Multibiometrics (International Series on Biometrics)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.

[24] A. Jain, K. Nandakumar, and A. Ross. Score normalization in multimodal biometric systems. 38(12):2270–2285, December 2005.