Hip Movement Based Authentication

How will imitation affect the results?

Tor Erik Buvarp

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2006

Institutt for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Abstract

This thesis will look at a method within biometric authentication that is quite new within the research topic. This method deals with authentication of a person by means of register the hip movement during ordinary walk. This thesis is a continuation of previous work where good result is achieved. The main goal in this thesis is to see how strong this biometric method is against imitation. If this research gives promising results, a new method to secure portable devices have arose.

An experiment with 22 subjects (132 samples) where a three dimensional accelerometer was attached to the hip during ordinary walk was performed. An equal error rate (EER) of 18% was achieved when the Histogram algorithm was used, and is quite similar to previous results.

In the imitation experiment 20 subjects (80 samples) participated. Two and two visually looked at each other before the experiment, to get better assumption to imitate each others hip movement. An EER of 18% was achieved and this shows that it is difficult to imitate our hip movement.

This is one of the first steps to convince other researchers and end-users that this could be a stronger method to use, compared to existing biometric methods to secure portable devices.

Sammendrag

Denne oppgaven vil se på en metode innen biometrisk autentisering som er ganske ny innen denne type forskning. Metoden tar for seg autentisering av en person ved å registrere hofte bevegelsen i løpet av ordinær gange. Denne oppgaven er en fortsettelse av tidligere arbeid der gode resultater er oppnådd. Hovedmålet med denne oppgaven er å se hvor sterk denne biometriske metoden er mot imitering. Om denne forskningen gir positive resultater, vil en ny metode for å sikre bærbare enheter melde seg.

Et eksperiment med 22 personer (132 datasett) der en tre dimensjonal akselerasjonsmåler var festet til hoften i løpet av vanlig gange ble utført. En equal error rate (EER) på 18% ble oppnådd når Histogram algoritmen ble brukt, noe som er svært likt tidligere arbeid.

I imitasjons eksperimentet deltok 20 personer (80 datasett). To og to så på hverandre visuelt før eksperimentet, for å få bedre forutsetninger for å imitere hverandres hofte bevegelse ved gange. En EER på 18% ble oppnådd og dette viser at det er vanskelig å imitere vår hofte bevegelse.

Dette er en av de første forsøkene på å overbevise andre forskere og slutt brukere om at dette kan være en sterkere metode å bruke, sammenliknet med andre eksisterende biometriske metoder, for å sikre bærbare enheter.

Preface

This thesis you are beginning to read was my last work at Gjøvik University College. After two years of studying, to be an MSc in Information security, I got very interested in the field of biometric authentication and decided to write a thesis about this.

I will bring a big thanks to Davrondzhon Gafurov. He has helped me to modify the software I have been using to evaluate my work, and have given me a lot of good and interesting feedback during this thesis. Einar Snekkenes, my supervisor, has supervised me during this thesis and developed a new device so I could finish my experiments.

My parents have supported me during this period and never doubed me on my work, in spite of the troubles I have experienced.

My last thanks go to all the test persons that voluntary have participated in the experiments. They have walked several times and without them I never could have finished my work.

Contents

List of Figures

List of Tables

1 Introduction

1.1 Topic covered by this thesis

The society is in an increasing need of a safe and easy way to protect sensitive information inside portable devices. Until now a number of different methods have been used. PIN code is the most used method, but recently our biometric features have been used to protect portable devices. Today's scientists are testing out different ways to recognise a person by means of using our biometric characteristics. One of the newest and most successful biometric methods is to use our hip movement, since we often are carrying our portable devices in the hip area. The problem with the other existing biometric methods is that they are weak against cheating. This work will see how strong/weak the hip movement is against imitation. If it is difficult to imitate our hip movement a new and maybe more secure method to secure portable devices have arose.

Keywords: Biometric authentication, accelerometer, hip movement, FAR/FFR, DET curves, Histogram, imitation.

1.2 Problem description

Today's researcher is struggling to find new and more secure ways to authenticate individuals. There are requirement of a high level of security simultaneously as the individuals should not notice that the process is taking place.

In the last few years a new method within biometric authentication have arise. This method examine how an individual is moving (e.g. with video, sensors or accelerometers) and uses this characteristics to identify individuals. The method is easy to use, secure, and has been accepted among the users.

The use of accelerometer attached to the hip area is the newest and most successful way to identify individuals. Individuals bring along portable units such as mobile telephone, PDA, laptop and are often attached in hip area and it is easy to attach a motion capturing device inside them.

The problem with this type of research is to convince other researchers and the end-users that this is an easy and secure technology to use in the future. To achieve such acceptance a total research is needed, both positive and negative results have to be presented. Faking others movement is one of these tasks. If such work gives positive results a new method to secure portable devices have arose and is ready to be used.

1.3 Target group

This report has a number of different target groups.

- Researchers who are working with, and are interested in such type of work.
- Students who are interested in computer security and want to learn about evaluation

theory and biometric authentication.

- People who are interested in protecting sensitive information stored in their own portable devices.

Since such work is related to many types of groups, the report is split into different parts. Reading section 1.6 "Outline of the report" is recommended to quickly find relevant information.

1.4 Research questions

The research question in this thesis is:

- How much research work has been done related to hip movement based authentication?
- Is it possible to use one of the previous research works, use the same distance metric and get similar results?
- How will the results be affected when imitation is performed?
- Can we use our hip movement in a fast and secure way to protect information in portable devices?

1.5 Claimed contributions

The main goal is to come up with an authentication method that can not be imitated or stolen by others. This could then be used to secure PDA's, cell phones or other portable devices, where sensitive information is being stored. Another range of use is to apply this method in access controls of restricted areas. The contribution in this thesis will be to see if the hip movement can be used in such authentication environment, and how temper proof the method are against imitation. This thesis will not come up with new algorithms, but it will see how reliable the previous research that has been done in this area is. If the results in this thesis are good, maybe the traditionally PIN code that is not so secure can be replaced or armoured.

1.6 Outline of the Report

Chapter 2: This chapter will give the reader basic knowledge about the theory used in this thesis.

Chapter 3: This chapter describes previous work related to hip movement based authentication. Other existing methods to secure portable devices and how temper proof they are against cheating is also described here. The chapter ends with a discussion of different ways to present results in biometric researches.

Chapter 4: The choice of methods is presented in this chapter. A mini version of the master thesis is presented later in this chapter where a fictitious experiment is presented. This is done to give the reader a deeper knowledge about the theory used later when the results are presented, and discussed. The chapter ends with a description of the distance metric used in this thesis.

Chapter 5: This chapter contains description of the accelerometer used in this thesis. Problems with the prototype design are also presented here.

Chapter 6: The experimental design is described and discussed in this chapter.

Chapter 7: This chapter describes how the experiment was performed, and how the data was divided and cleaned before it was evaluated.

Chapter 8: The results is presented in this chapter, discussed and compared with previous work.

Chapter 9: A lot of new questions and ideas have aroused during this thesis. This is summarized and discussed in this "Further work" chapter.

Chapter 10: This chapter turns back to the research questions and tries to answer them.

2 Biometric Overview

This chapter will give the reader basic knowledge about the theory used in this thesis.

2.1 What is Authentication?

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be [38]. Generally there are two ways of doing this [17]:

- **Verification:** The easiest way to explain this is to ask the question:"Am I whom I claim I am?". To answer this question the person have to give away his/her biometric features, and this is compared with his/her own biometric template(s) in the system. This is a one-to-one relationship and is used to prevent multiple people from using the same identity [41]. This thesis will look at this part.
- **Identification:** "Who am I?" In this case the system search through the whole database to check if there is a match. This is a one-to-many relationship, and if the person get a match with the template and a given threshold, the person is identified and get access to the given system.

The methods by which a human can authenticate themselves are generally classified into three groups [42]:

- **Something you are:** This is the field of biometrics, including techniques such as fingerprint, retina and gait[1] movement. Some split this category in two parts: "What you are" and "What you do".
- **Something you know:** This is a traditional password system.
- **Something you have:** This includes mechanism such as challenge-response lists, keys, one time pads and smart cards.

Another classification that have been used is:

- **Somewhere you are:** Authenticating a geographical location using GPS.

Sometimes a combination of methods are used, e.g., a bank card and a PIN.

2.2 Biometric Authentication

Biometric refers to the automatic identification of a person based on his/her physiological characteristic. In the article "An introduction to Biometric recognition" [17] they have listed up what measurements that is needed to qualify to be a biometric. They say that any human physiological and/or behaviour characteristic that satisfies these requirements, can be used as a biometric characteristic:

- **Universality:** Each person should have the characteristic.

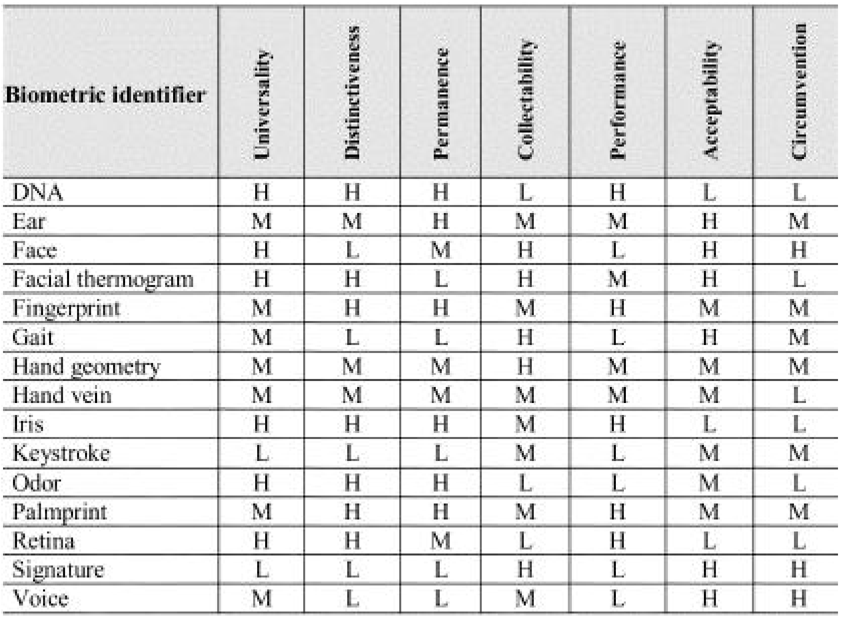
[1] Gait is a person's manner of walking

- **Distinctiveness:** Any two persons should be sufficiently different in terms of the characteristics.
- **Permanence:** The characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time.
- **Collectability:** The characteristic can be measured quantitatively.

Other issues that should be considered is:

- **Performance:** Refers to the achievable recognition accuracy and speed.
- **Acceptability:** Indicates the extent to which people are willing to accept the use of a particular biometric identifier in their daily lives.
- **Circumvention:** Reflects how easily the system can be fooled using fraudulent methods.

Figure 1 shows the most known biometric methods and how well they are to the items mentioned above.



Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Figure 1: Comparison of various biometric technologies taken from [17]. High, Medium, and Low are denoted by H, M, and L, respectively

2.3 Why use the hip movement as an authentication method?

Portable devices contains a lot of financial and private information, and is in most cases protected with a PIN code. A PIN code is difficult to remember and not so secure compared to other authentication methods. To improve security in portable devices, hip movement can be used because most users of portable devices carries them in the hip area. Studies from medicine [28] and psychology [18] present evidence for considering human gait as having distinctive patterns from which individuals can be recognised. Hip movement has also been used in previous research where the results have been very good [27, 2].

When Gait is compared with other biometric methods 1, it is not the best biometric method to use. In chapter 3.4 some biometric methods are described in how to protect portable devices. Some of these methods have got good scores in figure 1, but in chapter 3.5 these biometric methods are not so strong against cheating. If this thesis can prove that our hip movement is difficult to cheat, a better method to protect portable devices have arose.

3 Previous and related Work

The main purpose of this chapter is to answer the first research question. To do this the first section describes the use of accelerometers and sensors to measure peoples gait movement, before the next section describes the use of accelerometers in biometric authentication. Video is the competitive method, and is often compared against accelerometer, so a section where video is used in biometric gait authentication is briefly described.

Figure 1 shows different biometric methods. This thesis will try to convince the reader why the hip movement can be a better method to use than other existing methods. Therefore a section which describes existing methods to secure portable devices is presented, before a section where work related to cheat these methods is described.

In the last few years a lot of new methods to present results in such type of work have been presented. Therefore this chapter will end with a discussion of why the DET curve is the best method to present result in such type of work.

3.1 The use of accelerometers and sensors to measure peoples gait movement

In 1996 Verplaetse started to work with the idea about smart devices [40]. In this work he recommended the use of accelerometers and gyroscopes to measure motion and position of devices. He performed a test where a shoe fitted with an accelerometer was measuring the accelerations of normal gait. The intention of this work was only to measure movement. Four Hungarian students with their supervisor did a research in 2001 where they built a speedometer [14]. They connected three ADXL2002 accelerometers from Analog Devices to a DSP card from Texas Instruments. This could then be used to measure the wearer's speed while walking or running. They could determine the step length and whether the person was walking or running merely on the step frequency derived from the acceleration data. They meant that this type of technology has a variety of potential applications such as health care, sport, fitness, motion capture and robotics. As we have seen, the first researches conducted in this area where not aimed to authenticate people, but see how the human gait was moving. Analysing the daily activity of people was also Quentin Ladetto's goal when he did his research in 2000 [20]. In his work he was able to get more accurate results of a persons step length when he used a combination of acceleration data and GPS[1] data.

The use of sensors is another way to capture gait movement, and is very close to the use of accelerometers. Zhang et al. made a new device in 2003 called Intelligent Device for Energy Expenditure and Activity (IDEEA)[44]. The device consist of a micro computer which can be attached to a belt using medical tape, and can measure duration, frequency and intensity of various types of human physical activity. The main goal was to

[1] Global Positioning System

measure human activity, but they also tried to identify the persons based on their movement. Correct identification rates averaged 98,9% for posture and limb movement type and 98,5% for gait type. These types of activity cannot represent complicated real-life situations. Paradiso and Morris wanted to make a sensor package who is designed to provide continuous and real-time monitoring of gait for clinical biomotion analysis [30]. This work is more related to health care than authentication work, but the interesting part is that their package includes three gyroscopes and three accelerometers, and is designed to continuous monitor a person's gait movement. This device is cheap, small (can fit into a shoe), and can transfer data wireless in real time, and don't need to be used in a motion lab or physician's office.

3.2 The use of accelerometers in biometric authentication

In 2001 work with accelerometer related to biometric authentication was first taking place. It was a Finnish research group with Jani Mäntyjärvi in front [24] which attached two accelerometers to the hip and measured the movement of the hip during normal walk. In this work the best classification results for recognition of different human motions was 83-90%, and they where achieved by utilizing independent component analysis and principal component analysis. This work continued in 2005 where Mäntyjärvi with another group used only one accelerometer attached on the belt, at back [27, 2]. Their goal was to use the movement to protect portable devices. The experiment with 36 test subjects walked with fast, normal and slow walking speed. They used correlation, frequency domain and data distribution statistics to identify the test subjects. The performance of this new method was at the same level or even better than achieved by video based recognition in recent studies. Results between 72% and 88% where the best correct results they got in this experiment. In the end they concluded that changes in walking speed, clothes and ground affected the results.

Gjøvik University college created an MEMS device (Micro-Electro-Mechanical System) in 2005 whom Sønderål used in his thesis [35]. He attached this accelerometer to the leg where it detects the leg's movement in horizontal, vertical and sideway direction as the person walked. Different evaluation methods that can be used in such work, and how all the experiments where performed is described in detail in this report. The chosen method to evaluate the performed experiments in this work was the Fast Fourier Transformation and gave usable results. In 2006 Sønderål and two Phd students used the same data sets, but this time they used Histogram and Cycle length method to evaluate the work [13]. Equal error rates (EER[2]) at 5% and 9% was achieved when these two methods where used. This is better results than Mäntyjärvi et al. got in their work (Respectively 18% and 7%). In their work they conclude that this method is better than video (EER are between 8-24% in such types of work), and the Histogram algorithm is a usable method when such data should be evaluated.

In 2003 did Heinz and a group a research aimed at providing and analyzing standardized, representative sets for typical context recognition tasks [15]. 8 subjects where fitted with three accelerometers and walked the same path that is described in detail in this report. Since this experiment is small there is no final conclusion, but they could see dif-

[2] FAR = FRR, described in 4.1

ferences between all the subjects. The main problem with this, and with other research groups that use multiple accelerometers was to attach the sensors to the test subjects. This work continued in 2005 with K. Kunze et al. where they used 6 test subjects that made 90 walking samples[19]. Their result was in the low nineties for the frame by frame recognition and 100% for the more relevant based case. Another problem which they also in this work conclude with, is how such framework with multiple accelerometers will work in real life settings. The work Kunze et al. did in 2005 was very related to a work Jonathan Lester et al. did in 2003 [22]. This group introduced a method to determine if two devices where carried by the same person. They analysed walking data recorded by low-cost MEMS accelerometers using the coherence function, a measure of linear correlation in the frequency domain. Ling Bao did a similar work in 2003 where he developed algorithms and detected physical activities from five small biaxial accelerometers. [4, 5]. He used decision tree classifier algorithm that is slow to train but quick to use. The best result was when the accelerometers where attached on the thigh and wrist.

3.3 The use of Video in gait movement authentication

Previous section focused on the use of accelerometer. Since video was mentioned to be competitive method, this section will describe some of the related work where video have been used. In fact, video was the first attempt to use the human gait as an authentication method

Lee and Grimson present a study on how gait might be used to identify and classify persons[21]. The gait representation was based on simple features such as moments extracted from orthogonal view video silhouettes. They also wanted to make the experiment realistic so they collected data over different days and times and under varying lightning environments. Their conclusion was that this is a usable method but the clothes affected the person's gait, and they mean face recognition, combined with gait might give better results. When using two types of gait features in this work, one based on average appearance of gait, and one based on spectral components they got promising results. Bobick and Johnson [8] tried in 2001 a gait recognition technique that recovers static body and stride parameters of subjects when they walked. Their experiment contained 18 subjects that walked indoors and 15 of them walked outdoors six months later. There was 6 data points per subject for the angle-view, three data points per subject for the side-view far away, and three data per subject for the side-view close up. Their Equal error rate results where around 16% and they have to tune the experiment under more viewing conditions, so the error over possible views can be characterised.

3.4 Work related to securing portable devices

In 2003 did Sand, Wu and Yang a research on speech recognition to secure portable devices [33]. They consider this method to be one of the cheapest, simplest and convenient methods to use compared to face and fingerprint recognition. Speech from more than 250 persons has been recorded through mobile phones in this work. The equal error rate results where between 7.53-25.89%, when different devices where tested under different conditions. They conclude that this is a very robust system, but the problem with this type of authentication is to find the right way to secure the information.

Fingerprint is probably the most used biometric authentication method. Yoshimitsy Arai wrote a paper in 2005 about the use of fingerprint to secure portable devices [3]. He introduce a fingerprint identification token called FingerQuick[3]. This small device is only 23*85*11 mm^3 and weighs 15 g and has a unique capacitance-type fingerprint sensor that is highly resistant to static electricity and contamination. They are working to make a more competitive chip called LSI (Large-scale integrated circuit) that protects fingerprint data completely, because it does not allow the data to go outside the chip. Fingerprint is a method that gets very good results in such type of work. Qi Su et al. [36, 37] has used a sweep sensor[4] called MBF310[5] , and their EER was 4.23%. The prototype consist an external front-end fingerprint capture sub-system and back-end fingerprint recognition sub-system, and the software includes enrol and match functions. This device can easily be fitted to a mobile phone and it only takes 4.5 seconds to calculate the match time. The further work in this research is to optimise the performance and strengthen the security implementations of the fingerprint authentication mobile phone.

3.5 Work related to cheating within biometric authentication methods

Previous section described more traditional methods to secure portable devices compared using movement data. Some of these methods have in posterity been proven to not be so secure than expected. This section will look at work that is related to cheating of such methods. We have not been able to find any work that present cheating of others movement.

The first article doesn't deal with cheating but rather about weaknesses in the traditional PIN code and password system that is used. Because of the difficulties to remember and choose good enough passwords and PIN codes[43], biometric features is suggested to use.

Fingerprint gets very good score when biometric methods are compared as shown in table 1. In 2004 did Marie Sandstrôm a thesis that faked all fingerprint sensor [32]. She made artificial fingers that she used to fool different sensors. The conclusion in this work is that sensors have to be secured, or the fingerprint has to be used in combination with something else (Smart card or PIN code). When doing this the method will be more complex and more difficult to use. A German group have also cheated fingerprint [31]. They made a video that shows how easy a fingerprint can be taken from a glass and be used to fool a fingerprint sensor.

Jeremy Impson wrote an article in 2005 about securing PDA's [16]. Signature is a method that is very easy to use, and a lot of PDA's solutions offer this method. Jeremy tried a couple of times to fake signatures and didn't have difficulties to write fake signatures. The conclusion is that this is a very easy, but not a secure method to use.

[3] FingerQuick is a registered trademark of NTT Electronics Corporation

[4] The finger sweep across the surface, instead of just put the finger on the sensor

[5] http://www.fujitsu.com/sg/news/pr/fmal_20040708-02.html - Fujitsu 2001-2006 (Last visited June 2006)

3.6 Work related to presenting results

There are many ways to present such results and this section will catch up with previous work that have been studied and discuss them.

The first and maybe most used method is the Receiver operating characteristic curve (ROC) [10]. A ROC curve is a plot of false positive rate against true positive rate as some parameter (Usually the threshold value) is varied. The problem with ROC curves is when multiple curves are used in the same plot. It can be very difficult to distinguish each plot since they are very close to each other. Therefore the Detection error trade-off curve (DET) was suggested to present results [25]. The DET curve is a plot of false positive rate versus false negative rate and thus gives equal emphasis to both types of error. The plot usually has logarithmic scales on both axes, so DET curves tend to be more spread out than ROC curves, making it easier to distinguish individual algorithms results. Figure 2 shows a DET curve that compares the results form the fictitious experiment (The result of this little experiment is described in the next section).

Some researchers mean the ROC and DET curve can give misleading results. Samy Bengio et al. have suggested that a ROC and DET curve can lead to misleading results as it compares performance measures that cannot be reached simultaneously by all systems [6, 7]. They propose a new curve they call "Expected Performance Curves (EPC)". These curves enable the comparison between several systems according to a criterion, decided by the application, which is used to set thresholds according to a separate validation set. Our work does not have such framework so this method will fall outside this type of research.

Sometimes unusual results can occur in an experiment. The DET curve sometimes have the disadvantage that it does not detect such results, so the DET curve looks very good, but this is not the real picture of the result. Adler and Schuckers propose some methods to avoid this by introducing a method that calculate a composite DET curve [1]. The main idea is to calculate a normalized match score, t, as a function of the angle, from a representation of (FMR, FNMR) values in polar coordinates from some center. Then they calculated an average DET curve that will detect such unusual results. Since there have been done research with gate movement with accelerometers, there ROC and DET curve have been used [24, 26, 27, 13], there is no worry that this thesis will get such results.

This section has proposed some methods to present verification performance of biometric systems. The DET curve is the most suitable method to use, since this thesis deals with multiple plots and this is the most commonly used method in researches. However, in general it is up to the researcher to evaluate and make a conclusion of the performed experiment, regardless of the chosen method.

4 Choice of methods

This chapter will explain the underlying theory and the methodology used in this thesis. The method used in this thesis is a mixed approach [11] and contains following steps:

- **Literature study:** This is a qualitative study and was done to get a better understanding of the previous work related to hip movement authentication (Described in chapter 3).
- **Data analysis theory:** This is a quantitative method and a fictitious experiment was made to get a better understanding of the underlying theory. This is described in this chapter, and the algorithm used to analyse the later data is presented in the end of this chapter.
- **Collecting data:** An experiment had to be planned and performed to get data to use on the chosen algorithm. This is a quantitative method and described in chapter 6.
- **Data analysis:** When the data is collected and the algorithm is used, the results can be presented and discussed. This is both quantitative and qualitative methods since the results is compared and discussed related to previous work.

4.1 Data analysis theory

To describe the data analysis theory an fictitious experiment was made, where the weight is used as an authentication method. How an experiment should be planned and performed is described in chapter 6. After the planning is done the experiment can be performed. In this case each test persons have to enrol themselves, in this fictitious case each person has to weigh themselves. This will be registered as "P1, P2,...,Pn", with their corresponding weigh. If this had been a real system these data would be stored and used when the verification process is taking place.

To get this verification process in this little experiment each person has to weigh themselves again after one week. This time the test persons are wearing other clothes, some have put on, or reduced weight. This assumption is made to get realistic results. These data sets will be registered as "A1, A2,...,An". If person "A1" has the same weigh as "P1" this person will be verified as the right person. These data sets are found in table 1 in the "Enrolment" and "Attempt" columns.

The data is now collected and ready to be evaluated, and the next step is to find a way to see the differences between each person. To do this a distance metric is needed where the goal is to find a value that says something about the distance or similarity between the two data sets. There are many distance metrics that can be used on such data sets [35, 9]. In this example a very simple metric will be used to illustrate the theory (The distance metric used in this thesis is described in section 4.3).

Enrolment		Attempt	
Data set A		Data set B	
Person	Weight	Person	Weight
P1	60	A1	63
P2	63	A2	63
P3	70	A3	68
P4	72	A4	72
P5	80	A5	81
P6	84	A5	83
P7	88	A7	93
P8	93	A8	87
P9	64	A9	64
P10	78	A10	80

Table 1: The fictitious data sets

$$D(A,B) = \left(\frac{|A-B|}{A+B}\right) \tag{4.1}$$

Where A and B are two different data set.

These results can now be put into a confusion matrix. In this case values between "0" and "1" will be represented in this matrix, where "0" is a perfect match and "1" is a totally mismatch. Such matrix contains information on the actual and predicted classifications performed by a system. Numbers along the leading diagonal of the table represent digits that have been classified correctly, while off-diagonal values show the number of miss-classifications. From table 2 only A4 and A9 have got perfect score in the verification process. If this had been a perfect system all the values in the diagonal would have been "0". The main idea is to get small values as possible to get perfect results. In this experiment the values is relatively small in the diagonal but there is instances where the values is small outside the diagonal, which gives poorer results. Some researchers also refer such values as "genuine" and "impostor" trials, where the genuine is the correct results, and impostor is the values outside the diagonal. The later result in this thesis will use such values and in this fictitious experiment they can be calculated as follows:

- **Genuine Trials:** These are the values which corresponds with the diagonal in the Confusion Matrix. In this case 10 different attempts are compared with 10 different values, and the value will be 10.
- **Impostor Trials:** These are the values which corresponds with the values outside the diagonal in the Confusion Matrix. The value will be all the values (10*10) minus the diagonal values(10) which is 90

Before the evaluation of these data sets can continue some performance values have to be described;

False accept rate (FAR): The expected proportion of transactions with wrongful claims of identity (in a positive ID system) or non-identity (in a negative ID system) that is incorrectly confirmed. A transaction may consist of one or more wrongful attempts dependent upon the decision policy. A false acceptance is often referred to in the

		A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
		63	63	68	72	81	83	93	87	64	80
P1	60	**0,0244**	0,0244	0,0625	0,0909	0,1489	0,1608	0,2157	0,1837	0,0323	0,1429
P2	63	0	**0**	0,0382	0,0667	0,1250	0,1370	0,1923	0,1600	0,0079	0,1189
P3	70	0,0526	0,0526	**0,0145**	0,0141	0,0728	0,0850	0,1411	0,1083	0,0448	0,0667
P4	72	0,0667	0,0667	0,0286	**0**	0,0588	0,0710	0,1273	0,0943	0,0588	0,0526
P5	80	0,1189	0,1189	0,0811	0,0526	0,**0062**	0,0184	0,0751	0,0419	0,1111	0
P6	84	0,1429	0,1429	0,1053	0,0769	0,0182	0,**0060**	0,0508	0,0175	0,1351	0,0244
P7	88	0,1656	0,1656	0,1282	0,1000	0,0414	0,0292	0,**0276**	0,0057	0,1579	0,0476
P8	93	0,1923	0,1923	0,1553	0,1273	0,0690	0,0568	0	0,**0333**	0,1847	0,0751
P9	64	0,0079	0,0079	0,0303	0,0588	0,1172	0,1293	0,1847	0,1523	**0**	0,1111
P10	78	0,1064	0,1064	0,0685	0,0400	0,0189	0,0311	0,0877	0,0545	0,0986	**0,0127**

Table 2: Fictitious Confusion Matrix

mathematical literature as a "Type II" error. Note that "acceptance" always refers to the claim of the user.

False reject rate (FRR): The expected proportion of transactions with truthful claims of identity (in a positive ID system) or non-identity (in a negative ID system) that is incorrectly denied. A transaction may consist of one or more truthful attempts dependent upon the decision policy. A false rejection is often referred to in the mathematical literature as a "Type I" error. Note that "rejection" always refers to the claim of the user.

Perfect results in biometric systems are almost impossible to get. This means that to get a score "0" in a verification process is difficult. Therefore threshold values (t) have to be defined to decide if the person is verified correctly. The hypothesis will be:

$$A = B \text{ if } D(A, B) > \ t \tag{4.2}$$

$$A \neq B \text{ if } D(A, B) \leq \ t \tag{4.3}$$

To manually calculate the FAR and FRR values some intermediate values have been calculated (In the real experiment this is done automatically), and these are:

All: This column show how many hit that is smaller or equal to the corresponding threshold value compared with the whole data set.

Diag: This column shows how many hit that is smaller or equal to the corresponding threshold value compared only with the diagonal values.

All-Diag: This column shows the differences between the "All" and "Diag" column.

FRR: This column shows the results of false rejections divided by total number of comparisons. In this case this is given by:

$$\frac{\text{"}Diag\text{"} - 10}{10} \tag{4.4}$$

FAR: This column shows the results of false acceptances divided by total number of comparisons. To find this value the whole data set has to be compared with except the diagonal values, so this is given by:

$$\frac{\text{"All} - \text{Diag"}}{90} \tag{4.5}$$

The thresholds values should be all the values between 0 and 1, but in this case only a selected portion of thresholds values have been chosen. The results is described in table 3, where all the calculation that is needed to understand the results is shown.

Thresholds	All	Diag	All-Diag	FRR	FAR
0,1	64	10	54	0	0,6
0,03	25	9	16	0,1	0,178
0,02	19	7	12	0,3	0,133
0,01	12	5	7	0,5	0,078
0,005	6	3	3	0,7	0,033
0,001	6	3	3	0,7	0,033
0,0001	6	3	3	0,7	0,033

Table 3: Calculation results from the fictitious experiment

When the FAR and FRR is calculated with their corresponding threshold values the result can be plotted in a graph. In this example and in this thesis a DET curve will be used (This is discussed in section 3.6). The DET curve can tell us how well the method is in different environments. Systems that deal with sensitive information will have the FAR value small as possible. When this value is small the FRR value will increase, and a lot of users will be faulty rejected. From figure 2 a FAR value that is 1% will give a FRR value like 20%. This means that almost none is faulty accepted but 1/5 of the users have to try several times to get access to the system. The opposite situation is when the system needs a small FRR value. Then the situation will be turned around and a lot of users will be faulty accepted. When researchers evaluate their work they often refer to a value called Equal Error Rate(EER):

- **Equal Error rate:** The error rate occurring when the decision threshold of a system is set so that the proportion of false rejections will be approximately equal to the proportion of false acceptances.

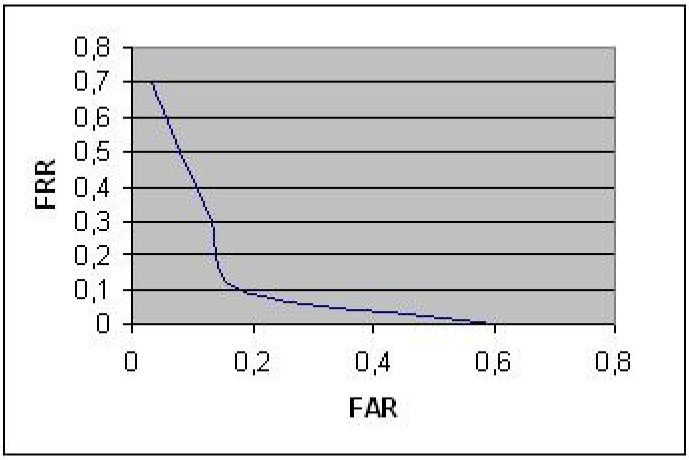


Figure 2: DET curve from the fictitious experiment

4.2 Discussion on how the imitation results will be

This thesis will see how cheating affects the results. The calculation of the results is similar to the fictitious described in previous section. The diagonal from the real experiment is used, and values where the cheating has been performed is re-calculated.

The interesting part is how the final result of the cheating will be. The False rejection rate will not be affected since there is none known users trying to enter the system. If the method is weak against cheating more subjects will be accepted into the system or if it is strong against cheating the results will not affect the system. In biometrics we can list up three cases:

- **The person can cheat the original person:** In this case the person is cheating another subject and succeed to do this. This will result in more people entering the system. The False acceptance rate will increase and the DET curve will be moved more to the right compared with the original one.
- **The person can't cheat the original person:** This is a acceptable result in such type of work. This means that the cheating have no affect on the system. The impostor trials will not be larger or smaller compared to the original data sets. The DET curve will be exact like the original one.
- **There is impossible to cheat the system:** This is a case quite similar to the case above. This means that the cheating persons can't cheat other subjects, and actually they cheat so bad that the impostor trials will increase compared to the original impostor trials. This will result in a DET curve that is better than the original and the DET curve will move a little bit to the left compared with the original results.

4.3 Algorithm Description

This chapter will describe the Histogram algorithm that is used to calculate the result in this thesis. The first idea was to look at and use several algorithms, but because time limit and unexpected troubles (Described in section 5.1.3) with the MR100 device only one algorithm have been chosen to use. If several algorithms is used it is easy to see how temper proof they are against cheating. The only known work that is related and have used this Histogram algorithm is the group from Finland/citeJani2005 so there is something to compare with when the final results is calculated.

To use histogram to evaluate the collected data is one of many ways to do it. This is a simple and easy algorithm to use, and software developed by Davrondzhon Gafurov, a Phd student at Gjøvik university college, was modified and used. This software was first developed to calculate result from an Master thesis that was done in 2005 [35, 13]. This software has been modified so it could be used on these data sets, and it was also possible to modify it to calculate results form the cheating part.

The algorithm works as follows [13]: A n-bin histogram of the combined hip signal is computed. Then, histograms are normalised by the number of recorded samples. The absolute distance was used to calculate the distance between two histograms as described in 4.3

$$dist(x, y) = \sum_{i=1}^{n} |x_i - y_i| \tag{4.6}$$

Where x_i is the probability of a data point falling into bin i of the enrollment's normalised histogram and y_i is the probability of a data point falling into bin i of the verification's normalised histogram.

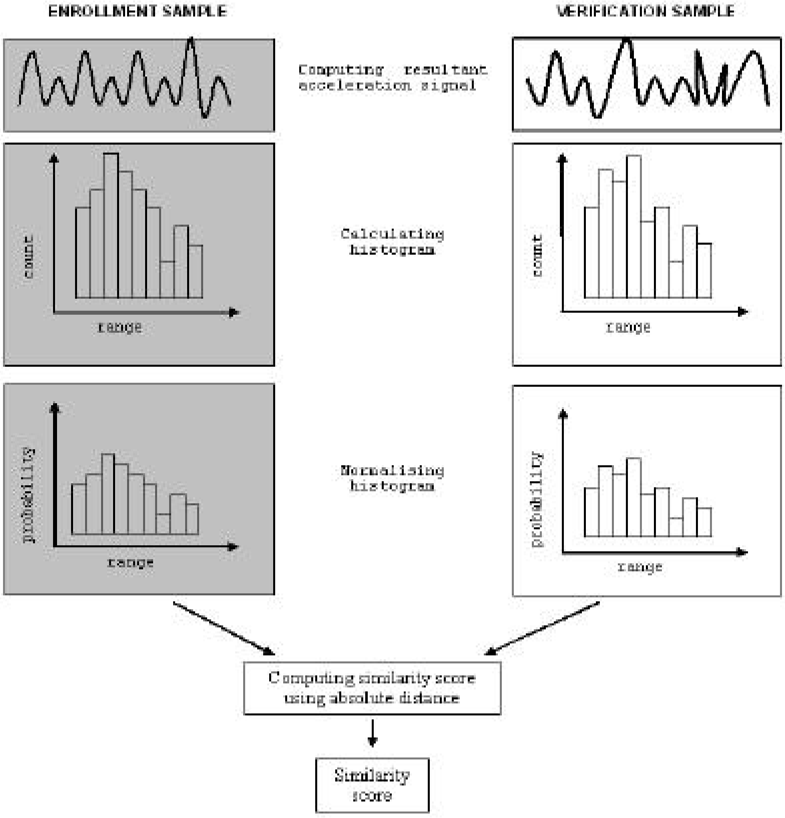
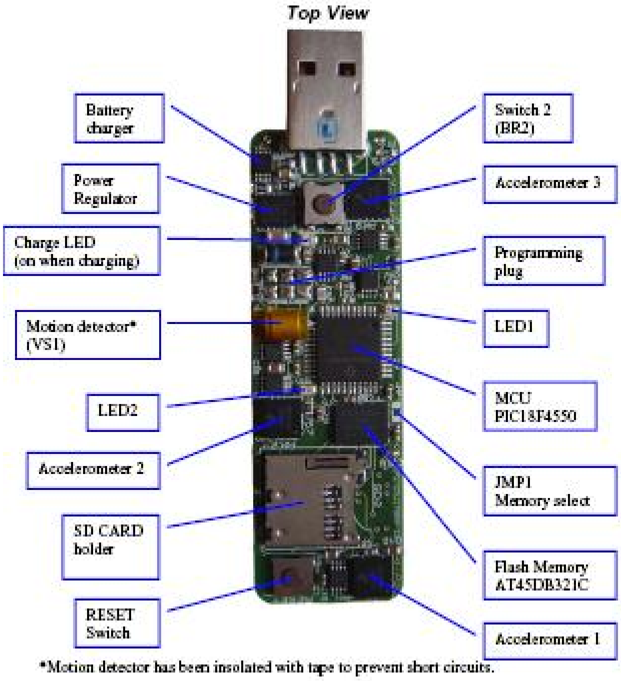


Figure 3: Overview of the Histogram algorithm

5 Technology

5.1 The Accelerometer



*Motion detector has been insolated with tape to prevent short circuits.

Figure 4: The motion recorder (MR 100)

Figure 4 shows the motion recorder (MR 100) that is used in this thesis. This is a MEMS device developed at Gjøvik University college and have different ranges of use, one them is security.

MR 100 is a memory stick like device with the following features [39, 12]:

- High capacity storage (64-256+ MB)
- USB interface
- Wireless bluetooth interface
- Acceleration sensors having 3 axis
  - 100 samples/sec, and a 8 byte timestamp between samples- processor speed 16Mhz
- Rechargeable battery (LiIon)
- Power management features
- Timer/clock

We are going to use the acceleration feature in this device, and the three dimensional directions is shown in figure 5.

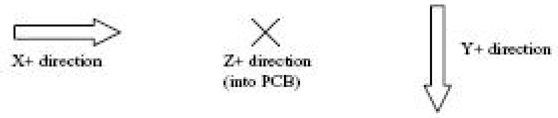


Figure 5: Directions (relative to picture 4 and 7)

When the later experiment is performed the accelerometer will register following characteristics in the hip:

X-axis: This axis will register the back and forward acceleration in the hip when a person walks.

Y-axis: This axis will register the acceleration when a person moves the hip up and down.

Z-axis: This axis register the acceleration when a person moves sideways.

5.1.1 The MMA7260Q accelerometer

This section will give a short technical overview of the MMA7260Q low cost capacitive micromachined accelerometer [34] that is built into the MR100. MMA7260Q is a ± 1.5g - 6g three axis low-g micromachined accelerometer which allows selection among 4 sensitives (1.5g/2g/4g/6g). This device includes a Sleep Mode that makes it ideal for handheld battery powered electronics. A summery of features in MMA7260Q can be listed as follows (taken from the technical data manual):

- Selectable Sensitivity (1.5g/2g/4g/6g)
- Low current Consumption: 500 µA
- Sleep Mode: 3 µA
- Low voltage Operation: 2.2 V - 3.6 V
- 6mm x 6mm x 1.45mm QFN
- High Sensitivity (800 mV/g @ 1.5g)
- Fast Turn on Time
- Integral Signal Conditioning with Low Pass Filter
- Robust Design, High Shocks Survivability
- Pb-Free Terminations
- Environmentally Preferred Package
- Low cost

5.1.2 The sampling of the time value

The intervals between samples are not equal (Should be 10 ms), so the resultant vector should be interpolated in some way. This thesis have not used the time value, since the Hisotgram algorithm looks more on the global characteristics. More advanced algortihms looks at cycle groups and compares each cycle instead of comparing the whole dataset like the algortihm used in this thesis. Such algoritms will have more profit if they use this time value. In the collected data sets in this thesis, the time value have been registered in case someone else would like to use more algortihms on them.

When the MR 100 is registering movement data some noise is also collected. To avoid this, some signal moving average (MA) filter should be applied. Because of troubles with the device like described in the next section, this have been given lower priority in this thesis.

5.1.3 Problems with the MR 100 device

The accelerometer (MR100) is only a prototype and has not been tested on a large scale experiment. Halfway through the experiment the MR100 stopped working. The result of this was lost data (6 persons during ordinary walk and 18 persons that had tried to imitate each other), and most of the experiment had to be repeated. This was a voluntary experiment and two test persons didn't have opportunity to do the last part where imitating was performed (Resulted in 20 subjects in this part).

The solution was to make a totally new device, because the first device had so much mechanical problems that it couldn't be fixed. The new device was similar and worked even better than the first one (The new device didn't make so much noise as the first one). When all the data finally could be collected the whole thesis was behind schedule. The goal in this thesis was not only to look how imitating others movements would affect the result, but also to look how different algorithms were affected when cheating is performed. Because of mechanical problems with the device and time delay in the experiment this part had to be removed and only one algorithm has been used. This will not result in poor results but the final conclusion will be more restricted than first planned.

This section has described the troubles that occurred when a prototype device was used to perform an experiment. It should be a thought-provoking to other researchers and students who want to do a similar work where an untried prototype device is being used. This thesis had to be reduced because of these troubles in order to finish before deadline.

5.2 Software

This section will briefly describe the software used to analyse the data collected from the MR 100 device.

5.2.1 The R Project for statistical Computing

To do the calculation and cleaning of the collected data the R Project for statistical Computing have been used[1]. R is a language and environment for statistical computing and graphics. R is a Free Software and provides a wide variety of statistical and graphical techniques. One of R's strengths is the ease with which well-designed publication-quality plots can be produced, including mathematical symbols and formulae where needed.

[1] http://www.r-project.org - R Project for statistical Computing (Last visited June 2006)

5.2.2 Microsoft Excel

An important part in such type of work is the cleaning of the collected data. The R Project was used to do the raw cleaning, but to ensure that the data was correctly and reliable Microsoft Excel[2] was used. This is a popular computer program that allows creating and editing spreadsheets, which are used to store information in columns and rows that can then be organized and/or processed.

[2] http://www.microsoft.com - Microsoft Corporation (Last visited June 2006)

6 The Experiment methodology

This is a methodology chapter and will describe in detail how the experiment will be performed, and how the data will be collected. This is a very important part if the results in this thesis are so interesting to other researchers, that they will re-examine the results.

6.1 Rules of the experiment

6.1.1 The path

To ensure reliability we must test in an environment identical for every test person. We solve this by instructing each test person to walk a fixed path,like described in figure 6

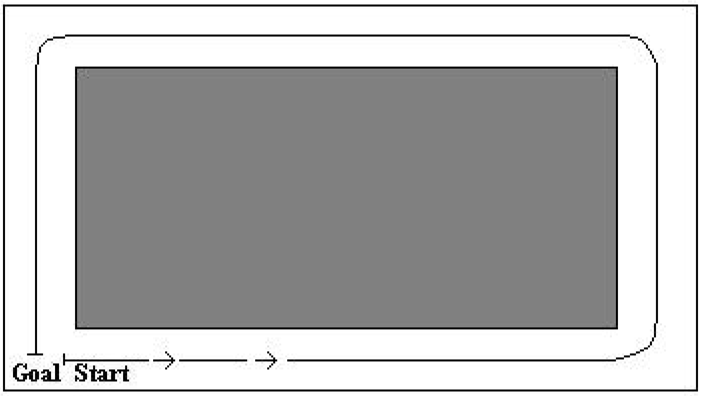


Figure 6: The fixed path every test person will walk during the experiment

This path is about 100 meters long and don't require any sudden turns from the test person.

6.1.2 Test size

The next step is to chose a suitable test size. Biometric Testing Best practice [23] have described how an experiment should be performed to get accurate results. Since this is a thesis with limited resources and time limit a test size of 22 (5 females and 17 males) persons was chosen. To get enough data to compare, every test person has to walk three times. These test persons will be between 20-38 years old and are students at Gjøvik University college.

6.1.3 Planning of the imitation experiment

The imitation of each others movement can be done in two ways. Either by filming every test person or to visually look at each other. This part of the experiment will imply that one test person is faking only one test persons movement and opposite. To create a film of every test person will take long time and it will be difficult to make a film that contain all angles of a persons hip movement. To chose test persons who know each other and spend time together is a better idea. Then these persons visually can look and walk behind each other before the experiment is taking place. Similarity of physical characteristics (weight, height and sex) will not be considered when the pairing will be done, only friendship.

When the imitation experiment will be performed it will be done as follows:

- Only two rounds with imitation will be performed.
- In the first round the target will walk in front, so the imitator (With the accelerometer attached to the hip) can visually look and try to see how the target is moving.
- In the second round the imitator will try to walk alone (With the accelerometer attached to the hip) and try to imitated the targets movement

6.1.4 Motion recorder mounting

How the accelerometer is attached to each test person is very important on how the results will be. The main goal is to get data so realistic as possible. Figure 7 shows the accelerometer attached to a test person. To fit the device in a belt with an elastic band is the best way (Figure 5 shows how the directions are pointed), since the device can follow the movement simultaneously as it is sufficient fasten to the hip. After a test person has walked one round, the possibility to make a realistic environment is possible. This means that the accelerometer can be removed, turned around (Differences in each data sets can be seen), and then attached again before next attempt. If every subjects had walked three times without removing the device, the data sets would have been unfair, and the result will have been more fixed than random.

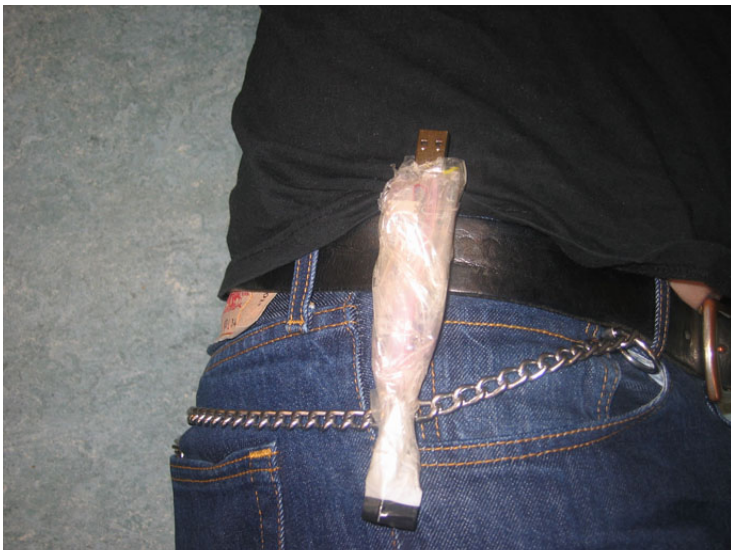


Figure 7: The MR 100 device attached to a test person

6.1.5 Registration of information

In such type of work many factors can have influence on the results. Therefore it is important to register information about each test person. This information together with the data sets can be a totally new research if someone wants to interpret this information in detail. The registered information is (An overview can be found in appendix A):

- Sex
- Age
- Type of shoes

A persons weight is important information, but many of the test persons refused to give away such information, so this was skipped. All this information is stored and completely anonymous. This is because such type of information is sensitive, and Norwegian law [29] has to be followed.

7 The collected data

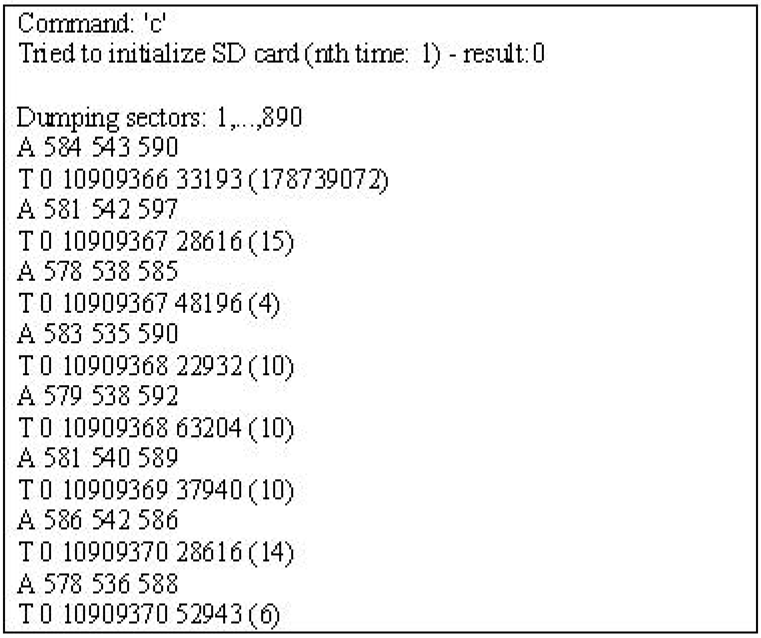
When the experiment was planned like described in chapter 6 the data gathering could take place. This chapter will describe how the raw data looks like and how the transformation was done before these data could be analysed.

7.1 The performed experiment

The final result from the performed experiment was 22 subjects (5 females and 17 males) during ordinary walk, and 20 subjects (5 females and 15 males) that participated in the imitation experiment. Only one pair there male imitated female and opposite, occured, when all the test persons was paired. The rest was male imitated male (7 pairs) and female imitated female (2 pairs). The experiment was performed like described in chapter 6. We experienced some troubles with the attaching of the device but we wanted a realistic environment, and with this removing/re-attaching after each round we was able to collect such realistic data sets

7.2 The raw data format

When the experiment was done the data could be transferred to a computer and stored in a text file. Then it looked like in figure 8. This figure shows the format of the data



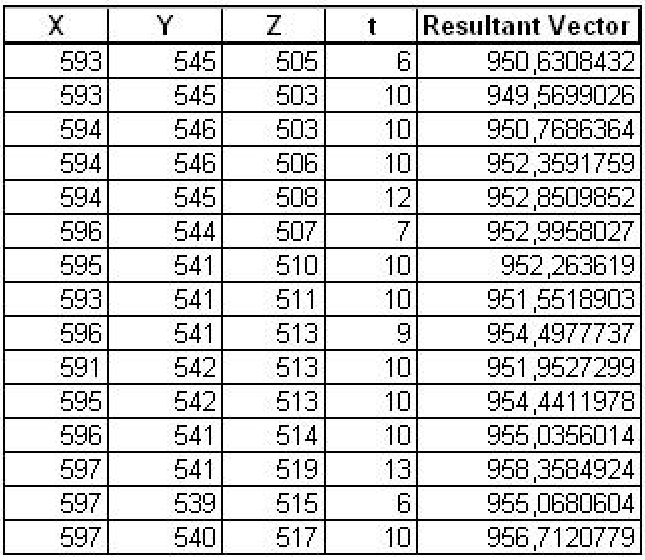
```
Command: 'c'
Tried to initialize SD card (nth time: 1) - result: 0

Dumping sectors: 1,...,890
A 584 543 590
T 0 10909366 33193 (178739072)
A 581 542 597
T 0 10909367 28616 (15)
A 578 538 585
T 0 10909367 48196 (4)
A 583 535 590
T 0 10909368 22932 (10)
A 579 538 592
T 0 10909368 63204 (10)
A 581 540 589
T 0 10909369 37940 (10)
A 586 542 586
T 0 10909370 28616 (14)
A 578 536 588
T 0 10909370 52943 (6)
```

Figure 8: The raw data format from the MR 100 device

which was taken directly from the accelerometer. In the A line the X,Y and Z coordinates are registered, and in the T line the time value is registered. This thesis has not used this time value, but if someone wants to evaluate the data sets with different, and more advanced algorithms this is possible when this value is registered.

7.3 Cleaning of the collected data

After the data was transferred to a computer in different files the cleaning part could be performed. Before this, files only contained X, Y, Z and time value was made as shown in figure 9.



X	Y	Z	t	Resultant Vector
593	545	505	6	950,6308432
593	545	503	10	949,5699026
594	546	503	10	950,7686364
594	546	506	10	952,3591759
594	545	508	12	952,8509852
596	544	507	7	952,9958027
595	541	510	10	952,263619
593	541	511	10	951,5518903
596	541	513	9	954,4977737
591	542	513	10	951,9527299
595	542	513	10	954,4411978
596	541	514	10	955,0356014
597	541	519	13	958,3584924
597	539	515	6	955,0680604
597	540	517	10	956,7120779

Figure 9: Data format with X,Y,Z values, the time value and the resultant vector

Several data files was collected and a R script has been used to split the datafiles in several small files. Then these data could be opened in Excel and a resultant vector was made to make a plot that showed how the relation between the coordinates are. This vector was made by means of the formula described below and figure 9 shows how the data format looks like.

$$\sqrt{(X_1 * X_1) + (Y_1 * Y_1) + (Z_1 * Z_1)} .... \sqrt{(X_n * X_n) + (Y_n * Y_n) + (Z_n * Z_n)} \qquad (7.1)$$

When doing this, the possibility to make a plot that shows how this data looks like in a understandable way. This is shown in figure 10. This figure shows a section of one person who has walked 3 times during the experiment. In point around 10000 and 22000 we easily can see when the accelerometer has been removed and turned around before it had been re-attached. This is not walking data and had to be removed before the data sets could be evaluated. When the cleaning of these data was manually done it resulted in three data sets (Figure 11, left side) from each person during ordinary walk (Two datasets druing imitation walk). To ensure accurate results in this work we decided to split every data set in two, so each person would have 6 data sets each (4 data sets each in imitation walk). How this division is done, is shown in figure 11. The first two data sets in the right corner have been averaged and used as template, and the following 4 data sets have been used to compare with the template. The final result, when this cleaning had been done, was 132 data sets that could be compared during ordinary walk, and 80 data sets in the imitating experiment.

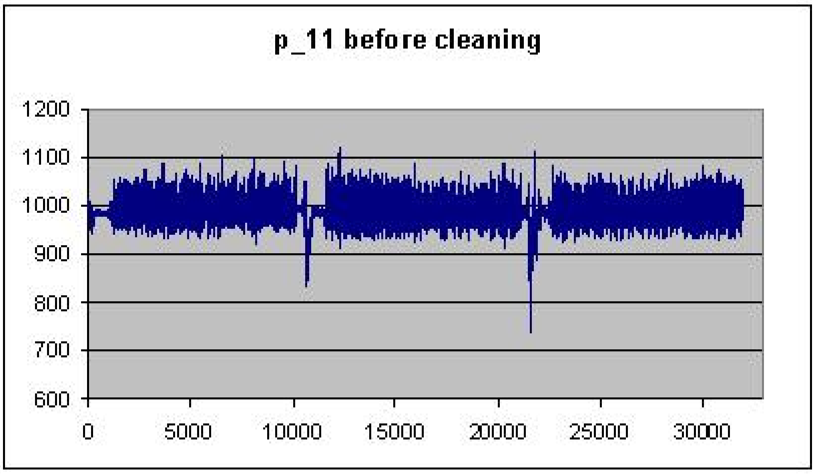


Figure 10: Diagram that shows the raw uncleaned data in an understandable way

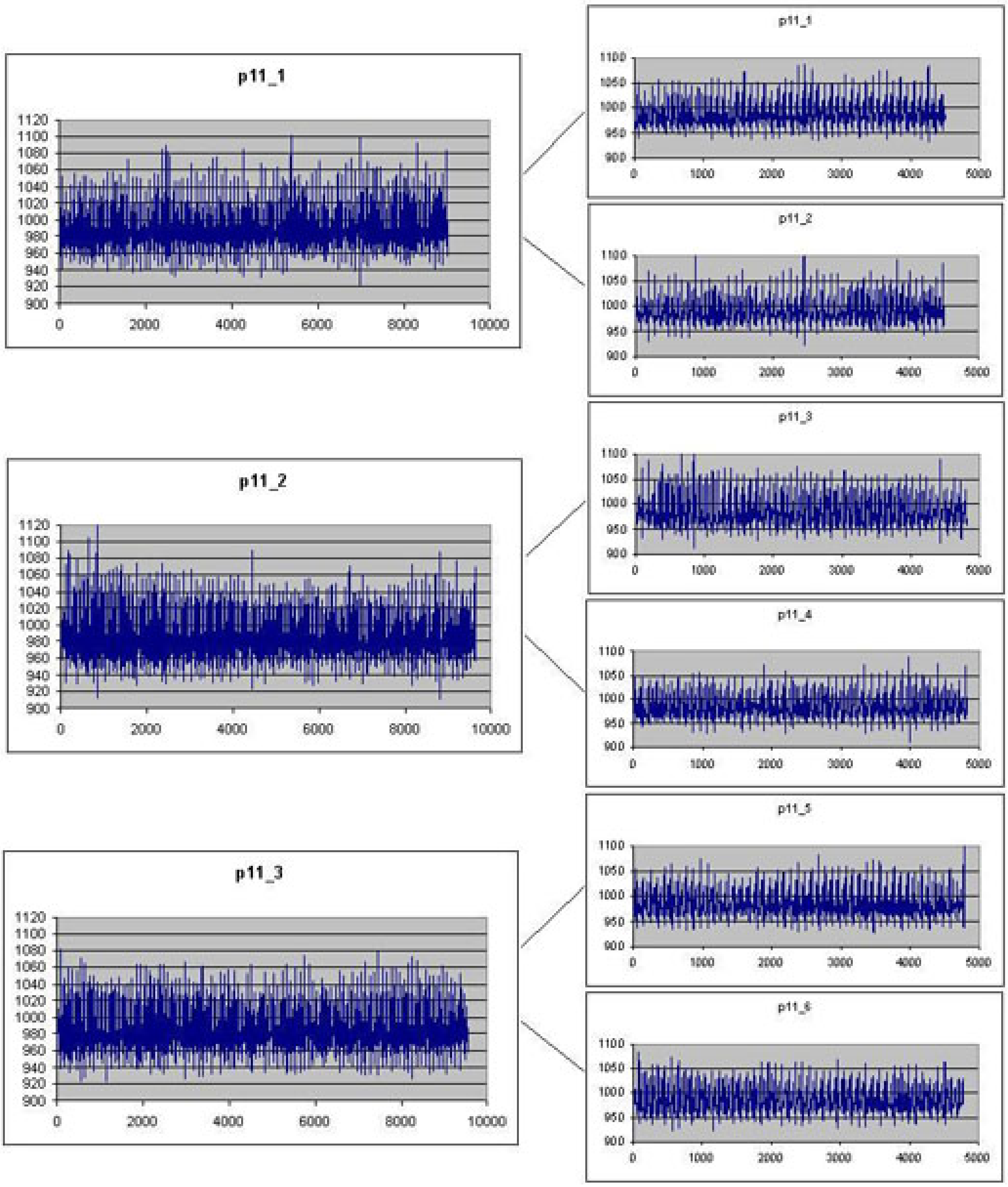


Figure 11: Division of test person P11's dataset ((p11_1+p11_2)/2 = template, and p11_3_4_5_6 is used to compare with the template)

8 Results with discussion

This chapter will present the final results and discuss them in detail. When the data sets was cleaned and the FAR and FRR was calculated a DET curve could be plotted. The most interesting thing in this thesis was to see how the imitation experiment affected the result from ordinary walk.

Figure 12 shows the result from the ordinary walk. This plot contains 22 subjects who have walked 3 times each. 88 genuine and 1848 impostor trials have been used to make this plot. The achieved EER is little bit above 18%, which means that 16 persons are wrongfully rejected and 334 is wrongfully accepted. This is the first attempt to attach only one accelerometer to the hip, but from previous work there are experiments where two accelerometers were attached to the hip[24] and experiments where one accelerometer was attached on the belt, at back[27, 2]. This thesis has been a continuation of this previous work, and we wanted to re-examine the results Mäntyjärvi et al. [27] got in 2005 when they used the Histogram algorithm. It was important to get results from the ordinary walk that related to their results, since this work is the first attempt to investigate how imitation can affect the results. As mentioned above we got an EER at 18% and Mäntyjärvi et al. got 19% (Their device recorded acceleration of 256 samples/sec and they used 108 genuine and 11556 impostor trials to plot their ROC curve). It would have been interesting to evaluate our data sets with the algorithm Ailisto et al.[2] used when they got an EER that was 6.4%, to see if our data was similar to their. As mentioned many times in this thesis, troubles with the device delayed us to test more algorithms on the data sets. It is important to mention that [2, 27] did not use acceleration from the side-way direction, because of too much irregularity in the data sets.

From the previous work we have seen that one of the main range of use is to protect portable devices. Better results have to be achieved before this could be realised, because what happens if he/she is faulty rejected when accessing the portable device? It will be a very bothersome system if persons have to put their portable devices in the pocket and walk several times to get access. Gjøvik University college, Nislab[1] and VTT Electronics[2] in Finland are working to find better algorithms to use on such type of data sets, in order to get more sufficient results. And if such algorithms is developed these have to be tested on larger data sets.

[1] http://www.nislab.no/ - Norwegian Information Security laboratory (Last visited June 2006)

[2] http://www3.vtt.fi/?lang=en - VTT Electronics (Last visited June 2006)

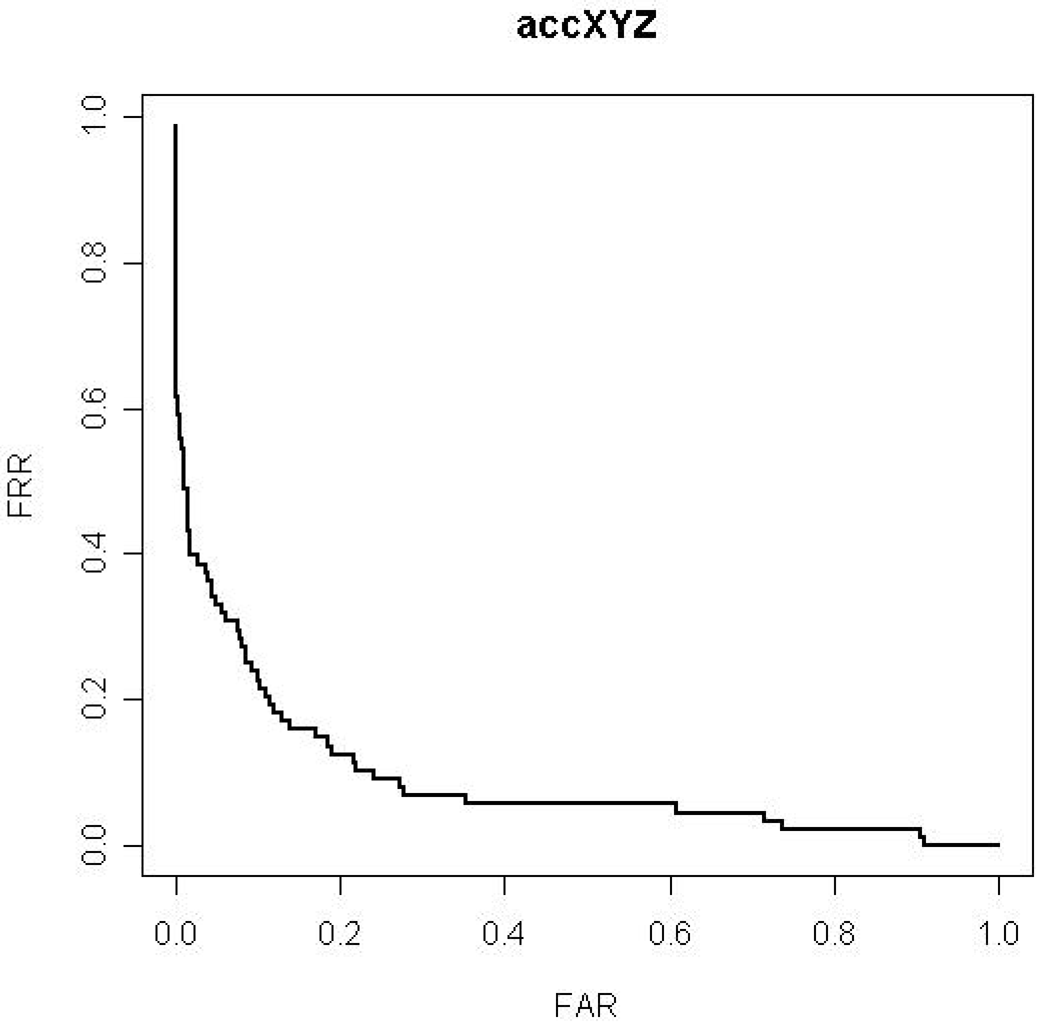


Figure 12: DET curve from ordinary walk

The main goal in this work was to look on how imitation could affect the result. In section 3.4 we presented several existing methods to secure portable devices, and in section 3.5 we presented work where these methods was fooled. The existing methods to secure portable devices are fast and very suitable to use, but they are weak against cheating. This is the reason why we wanted to do this thesis. Using our hip movement is a fast and usable method, but is this method also weak against cheating?

Figure 13 shows the results from the imitation experiment. In this experiment 20 subjects participated and 80 new impostor trials was calculated to plot the new curve. In section 4.2 we had a little discussion about how the cheating plot would be. The EER in the imitation curve is similar to the ordinary curve when the Histogram algorithm is used. This means that it is difficult to cheat others movement, and the imitation don't affect the results. As mentioned in the data analysis chapter it is very important to look on the whole DET curve before a conclusion is made. In our DET curve we have some interesting results. To illustrate this we can make a system where we want a FAR value that is around 3%. If we put this system in a cheating environment like this, we actually can expect a FAR value that increases to around 10%. When we want a low FAR value it is possible to imitate others movement when the Histogram algorithm is used. The other situation is when we want a low FRR value. Then our results shows that it is impossible to cheat others movement. In this thesis we have not managed to find any previous work that is related to cheat on others movement in biometric authentication so we don't have anything to compare with. The experiment is also too small to conclude if this is a reliable result, but it seems like promising results, compared with existing methods to secure portable devices. The test subjects have no assumption to cheat others movement so professional actors/imitators have to be tried and maybe the assumption will be better if the test persons can train more, before they perform the imitation.

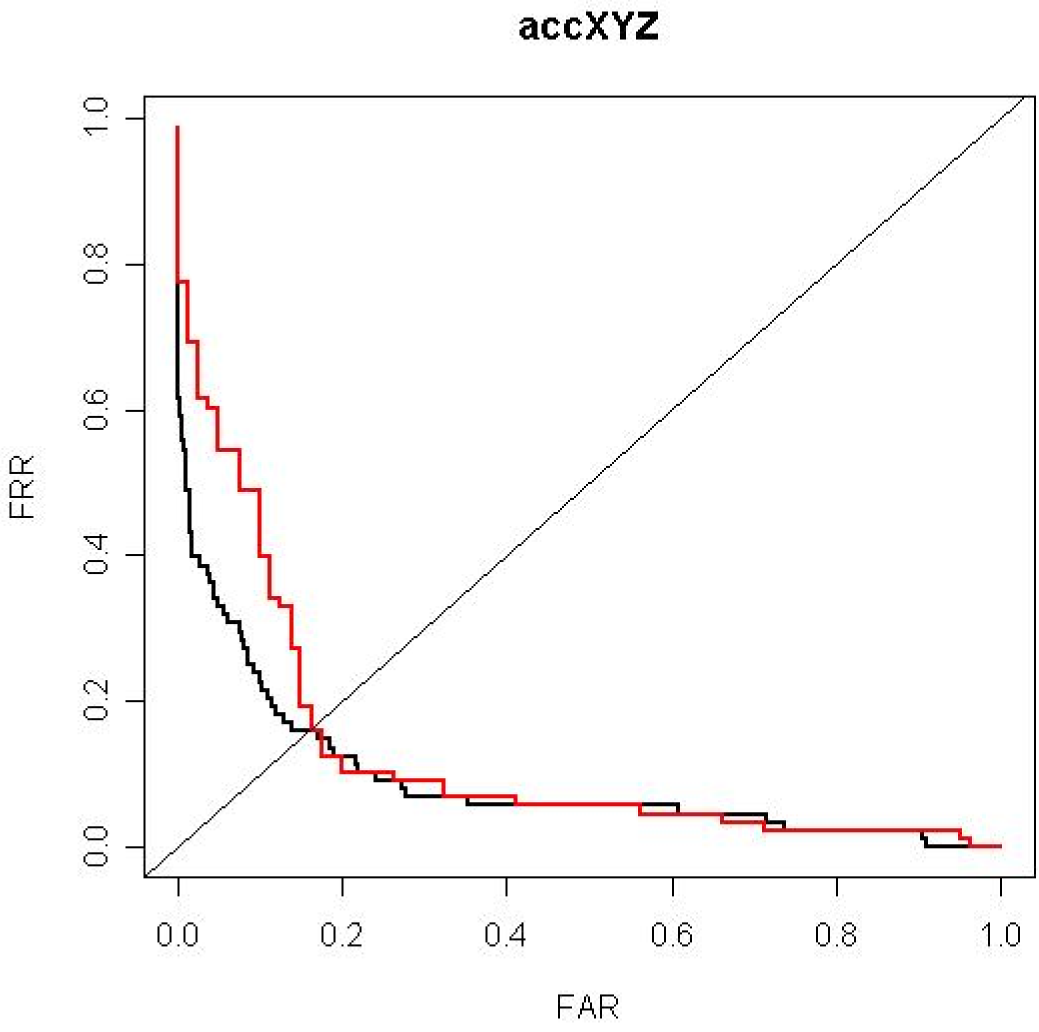


Figure 13: DET curve from ordinary and imitation walk

9 Further Work

A Master thesis like this should contain a scientific work that comes up with some new things. Maybe the most important part in such type of work is to reflect on what have been done, and what could have been done if more time and resources had been available. During work with this thesis a lot of questions have emerged and this chapter will sum up and describe these questions.

- **Test more known algorithms against cheating:**One of the ideas when planning this thesis, was not only to see how cheating can affect the result, but also see how different algorithms perform when cheating is accomplished. Because of mechanical problems with the device, there was no time to test several algorithms because it take some while to understand them. Several impostor and genuine trials should also be calculated to see if this affect the result when the Histogram algorithm is used.

  There exist multiple known algorithms who is suitable to use on such movement data sets. To test different algorithms on such data sets, better results can be achieved and algortimhs that are weak/strong against cheating can be identified.

  The intervals between samples should also have been recalculated so they will become equal. Then the time value can be used in the evaluation process. Some filter to reduce the level of noise should also have been applied before evaluating the movement data.
- **Develop own algorithms:** Better results have to bee achieved before hip movement based authentication can be implemented to secure portable devices. This could be done if better algorithms who is more suitable to use on such type of movement data is developed.
- **Larger and long-term experiment:** If this technology should be used among many end users more experiments have to be done. Biometric features are changing over time, so long-term experiments among others factors like injuries, types of shoes and change of clothes should be studied. Larger experiments should also be performed to see if the results is representative to a larger set of population.
- **Use professional actors/imitators to do the imitation part:** Ordinary people have little assumption to imitate others movement. Experiments there professional actors/imitators are used to do the imitation should be tested to see if this can affect the imitating results. To see if the assumption to imitate others movement becomes better, if training is performed before the experiment should also be tested.
- **Try cheating in all biometric researches to see if it is necessary to perform cheating experiments:** From the previous work we presented work where fast and usable biometric methods is used to secure portable devices. We have seen that these methods are weak against cheating. This should be a thought-provoking thing to consider

when doing such type of research. Many users are interested in securing their sensitive information, rather than have the fastest and most usable method. Try cheating in other exisiting biometric methods and in new arising methods is maybe a good idea when doing such type of research.

- **Secure the data in the MR 100:** Fool biometric methods is not only about cheating others characterisitcs. What happend if someone is abel to steal the prestored template inside the portable device? This could then be used to get access instead of cheating others biometric characterisitcs. Using cryptorgraphic algorithms to secure the prestored information should be done, before such biometric methods is realised. The MR100 device contains a bluetooth function and if the device should be used in the future, the wireless channel should be secured.
- **Use video instead of just look visually on a person while walking:** In the chapter where the experiment was described, the use of video was discussed. Experiments where a video of each person is made should be tried. The assumption to cheat others hip movement might increase.
- **Location Detection:** In the previous work chapter we saw that the first studies with accelerometer was to see how the person was moving and where the persons was located (indoors and outdoors). In this thesis we have made a path that is very restricted compared to real life. Performing experiments where people are walking in normal environments, and try use these data to decide where the person is, or have been is an interseting part. Such results might be used in a sort of access control.
- **Real Time Transmission:** When the data in this thesis have been collected, the device have been removed and the data have been transefred to a computer via an USB interface. The MR 100 device contains a bluetooth function, but this functionality does not work properly enough to use. When this function work, it is possible to collect and analyse the data from a person when he/she walks in real time. Experiments where this is studied is necessary to make a final conclusion if this is a usable method to secure portable devices.
- **Free mounting of the MR 100 device:** In the performed experiment the device have been attached in a similar way on each test person. If a person does not have a wallet that is attached to the belt, they should be able to put the portable device in the pocket without changing the result. This means that more complex algorithm have to calculate the data sets, previously to algorithms like the Histogram algorithm used in this thesis.
- **Cases where the person is faulty rejected:** We mentioned this in the discussion of the reuslt chapter. A backup solution should be implemented if the perosn is faulty rejected. Portable devices are in use all the time and it is too bothersome if the users have to walk over and over to get access to the system. Even if better results are achieved, faulty rejections will occur and a solution of this have to be taken in consideration.

10 Conclusion

The main question in this thesis has been: "**Can we use our hip movement in a fast and secure way to protect data inside portable devices?**

The best way to sum up this work and come up with an conclusion is to go back to section 1.4 and look at the research questions we started with

- **How much research work has been done related to hip movement based authentication?**
  A lot of work has been done related to movement authentication. Accelerometers, video, sensors and gyroscopes have been used to register our movement while we are walking. This thesis has mainly continued the work the group from Finland has done. They have shown that using our hip movement and one accelerometer is a fast and usable method.
- **Is it possible to use one of the previous research work, use the same distance metric and get similar results?**
  The first part of the experiment only registered ordinary walk to see if it was possible to get similar results compared to the previous work. The Histogram algorithm was used and the results showed quite similar results. Compared to the previous work a smaller experiment was performed, but more data from each person was collected and evaluated. A smaller amount of genuine and impostor trials was also calculated compared with the previous work.
- **How will the results be affected when cheating is performed?**
  The second experiment was performed to see if our hip movement is unique enough to determine if this is a secure authentication method. Two and two have looked visually at each other in a while before the experiment was performed. The results showed that it is difficult to cheat when the FRR value is low, and possible to cheat when the FAR value is low, when using the Histogram algorithm. The EER value showed that the imitation didn't have affect on the result, i.e. it is difficult to imitate others movement.

  It is impossible to make a final conclusion because bigger amount of data has to be collected, and more algorithms have to be used. Then a comparison can be done to see if the amount of data collected in this thesis, with the Histogram algorithm is a good method to compare ordinary and imitation walk. Problems with the device and short time limit are the main reason why this hasn't been done in this thesis.
- **Can we use our hip movement in a fast and secure way to protect data inside portable devices?**
  Using hip movement as an authentication method is a fast and usable method. This thesis wanted to see how secure this method was. An experiment with imitation of

others movement have been performed. The results have showed that it is difficult to cheat others movement when the Histogram algorithm is used. Our results shows that it seems like this method is more secure against cheating than other existing biometric methods who are in use securing portable devices

The conclusion of this thesis is that more and bigger experiments has to be performed, more algorithms has to be used on the data sets in order to come up with a final conclusion. If this is done regarding to our promising results, a method to secure portable devices that is stronger against cheating than existing biometric methods can be realised.

Bibliography

[1] Andy Adler and Michael E. Schuckers. Calculation of a composite det curve. In *AVBPA*, pages 860–868, 2005.

[2] H. J. Ailisto, M. Lindholm, J. Mantyjarvi, E. Vildjiounaite, and S.-M. Makela. Identifying people from gait pattern with accelerometers. *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense IV*, 5779:7–14, March 2005.

[3] Yoshimitsu Arai. Recent activities concerning fingerprint identification devices. *NTT Technical Review|*, Vol. 3 No. 5, May 2005.

[4] Ling Bao. Physical activity recognition from acceleration data under semi-naturalistic conditions. Master's thesis, Massachusetts Institute of Technology, 2003.

[5] Ling Bao and Stephen S. Intille. Activity recognition from user-annotated acceleration data. *In Proceedings of Pervasive 2004: the Second International Conference on Pervasive Computing. Springer*, 2004.

[6] S. Bengio and J. Mariéthoz. The expected performance curve: a new assessment measure for person authentication. In *Proceedings of Odyssey 2004: The Speaker and Language Recognition Workshop*, 2004.

[7] S. Bengio, J. Mariéthoz, and M. Keller. The expected performance curve. In *International Conference on Machine Learning, ICML, Workshop on ROC Analysis in Machine Learning*, 2005.

[8] A. Bobick and A. Johnson. Gait recognition using static activity-specific parameters. *In Proceedings of Computer Vision and Pattern Recognition Conference (CVRP 2001)*, Kauai, Hawaii, December 2001.

[9] R.M. Bolle, S. Pankanti, and N.K. Ratha. Evaluation techniques for biometrics-based authentication systems (frr). *Int. Conf. Pattern Recognition (ICPR), Barcelona*, 2, 2000.

[10] Adrian F. Clark and Christine Clark. Performance characterization in computer vision a tutorial. `http://peipa.essex.ac.uk/benchmark/tutorials/essex/tutorial.pdf`, 1999 (Last visited June 2006).

[11] John W. Creswell. *Research Design Ű Quantitative, Qualitative and Mixed Methods Approaches*. SAGE publications, Lincoln, second edition, 2003.

[12] Håvard Feiring. *Hardware overview for the USB AKS device (freescale_v2)*. Nislab, 2005.

[13] Davrondzhon Gafurov, Kirsi Helkala, and Torkjel Søndrol. Gait recognition using acceleration from mems. In *Proceedings of The First International Conference on Availability, Reliability and Security (ARES 2006)*, 2006.

[14] Gábor Guta, Attila Érsek, Norbert Gosztonyi, Sándor Melo, and Dr. István Szabó. Implementing a speedometer for walking and running with the tmss320f243 dsp controller. Application Report, University of Debrecen, April 2000.

[15] E. Heinz, K. Kunze, S. Sulistyo, H. Junker, P. Lukowicz, and G. Tröster. Experimental evaluation of variations in primary features used for accelerometric context recognition. *Lecture Notes in Computer Science, European Symposium on Ambient IntelligenceIssue*, pages 252–263, 2003.

[16] Jeremy Impson. How to protect your mobile device. http://www.microsoft.com/business/executivecircle/content/article.aspx?cid=1766\&subcatid=303, March 07 2005 (Last visited June 2006).

[17] Anil K. Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. *IEEE Trans. Circuits Syst. Video Techn.*, 14(1):4–20, 2004.

[18] G. Johannson. Visual perception of biological motion and a model for its analysis. *Perception and Psychopsysics*, 14:201–211, 1973.

[19] Kai Kunze, Paul Lukowicz, Holger Junker, and Gerhard Tröster. Where am i: Recognizing on-body positions of wearable sensors. *Location- and Context-Awareness: First International Workshop*, 3479:264-270, 2005.

[20] Q. Ladetto. On foot navigation: continuous step calibration using both complementary recursive prediction and adaptive Kalman filtering. In *ION GPS 2000, Salt Lake City, Utah, USA*, 2000.

[21] L. Lee and W. Grimson. Gait analysis for recognition and classification. *Proceedings of the IEEE Conference on Face and Gesture Recognition*, pages 155–161, 2002.

[22] J. Lester, B. Hannaford, and G. Borriello. Ťare you with me?Ť - using accelerometers to determine if two devi ces are carried by the same person. *In A. Ferscha and F. Mattern, editors, Pervasive Computing*, 2004.

[23] A.J. Mansfield and J.L. Wayman. *Best Practices in Testing and Reporting Performance of Biometric Devices*. Teddington, Middlesex, UK, August 2002.

[24] J. Mantyjarvi, J. Himberg, and T. Seppanen. Recognizing human motion with multiple acceleration sensors. *In 2001 IEEE International Conference on Systems, Man and Cybernetics*, 3494:747–752, 2001.

[25] Alvin Martin, George Doddington, Terri Kamm, Mark Ordowski, and Mark Przybocki. The DET curve in assessment of detection task performance. In *Proc. Eurospeech '97*, pages 1895–1898, Rhodes, Greece, 1997.

[26] Jani Mäntyjärvi, Petteri Alahuhta, and Ari Saarinen. Wearable sensing and disease monitoring in home environment. 2004.

[27] Jani Mäntyjärvi, Mikko Lindholm, Elena Vildjiounaite, Satu-Marja Mäkelä, and Heikki Ailisto. Identifying users of portable devices from gait pattern with accelerometers. *Acoustics, Speech, and Signal Processing, 2005. Proceedings. (ICASSP '05). IEEE International Conference on*, 2:ii/973 – ii/976, 2005.

[28] M. Murray. Gait as a total pattern of movement. *American Journal of Physical Medicine*, 46(1):290–332, 1967.

[29] Lov om Behandling av Personopplysninger. http://www.lovdata.no/cgi-wift/wiftldles?doc=/usr/www/lovdata/all/nl-20000414-031.html\&emne=personopplysningsloven\&\&, 2000 (Last visited June 2006).

[30] Joseph A Paradiso and Stacy J. Morris. A compact wearable sensor package for clinical gait monitoring. *Motorola Offspring Journal*, 2002.

[31] Frank Rosengart. Chaos computer club berlin. http://rosengart.de/archives/000031.html, 2004 (Last visited June 2006).

[32] Marie Sandström. Liveness detection in fingerprint recognition systems. Master's thesis, Linkping University, 2004.

[33] Lifeng Sang, Zhaohui Wu, and Yingchun Yang. Speaker recognition system in multichannel environment. *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, 4:3116–3121, 2003.

[34] Freescale Semiconductor. ±1.5g - 6g three axis low-g micromachined accelerometer. http://www.freescale.com/files/sensors/doc/data_sheet/MMA7260Q.pdf, 2006 (Last visited June 2006).

[35] Torkjel Søndrål. Using the human gait for authentication. Master's thesis, Gjøvik University College, Nislab, 2005.

[36] Q. Su, J. Tian, X. Chen, and X. Yang. A fingerprint authentication mobile phone based on sweep sensor. *In Third International Conference on Advances in Pattern Recognition (ICARP)*, Bath, UK, August 2005.

[37] Q. Su, J. Tian, X. Chen, and X. Yang. A fingerprint authentication system based on mobile phone. *In 5th International Conference on Audio- and Video-Based Biometric Person Authentication*, July 2005.

[38] TechTarget. Authentication. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211621,00.html, 2006 (Last visited June 2006).

[39] Tim and Håvard. *YBM-USB Versjon 2F Hardware manual Versjon 1.0*. NISlab, 2005.

[40] C. Verplaetse. Inertial proprioceptive devices: self-motion-sensing toys and tools. *IBM Syst. J.*, vol. 35(3-4):639–650, 1996.

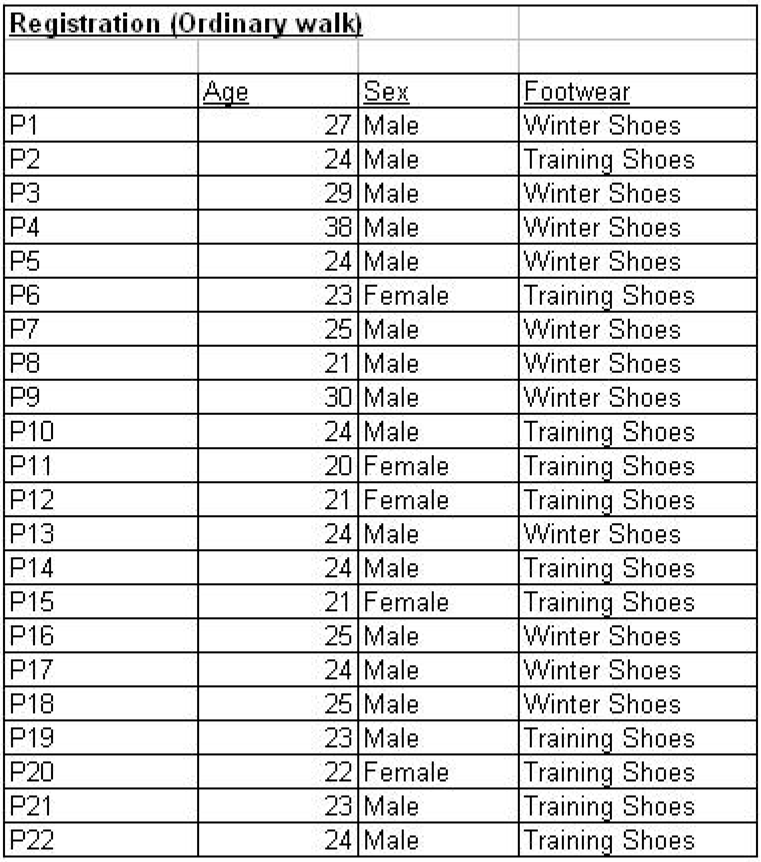
[41] J. L. Wayman. Fudamentals of biometric authentication technologies. *Int. J. Image Graphics*, vol. 1, no 1:93–113, 2001.

[42] Wikipedia. Authentication. http://en.wikipedia.org/wiki/Authentication, 2006 (Last visited June 2006).

[43] Jeff Jianxin Yan, Alan F. Blackwell, Ross J. Anderson, and Alasdair Grant. Password memorability and security: Empirical results. *IEEE Security & Privacy*, 2(5):25–31, 2004.

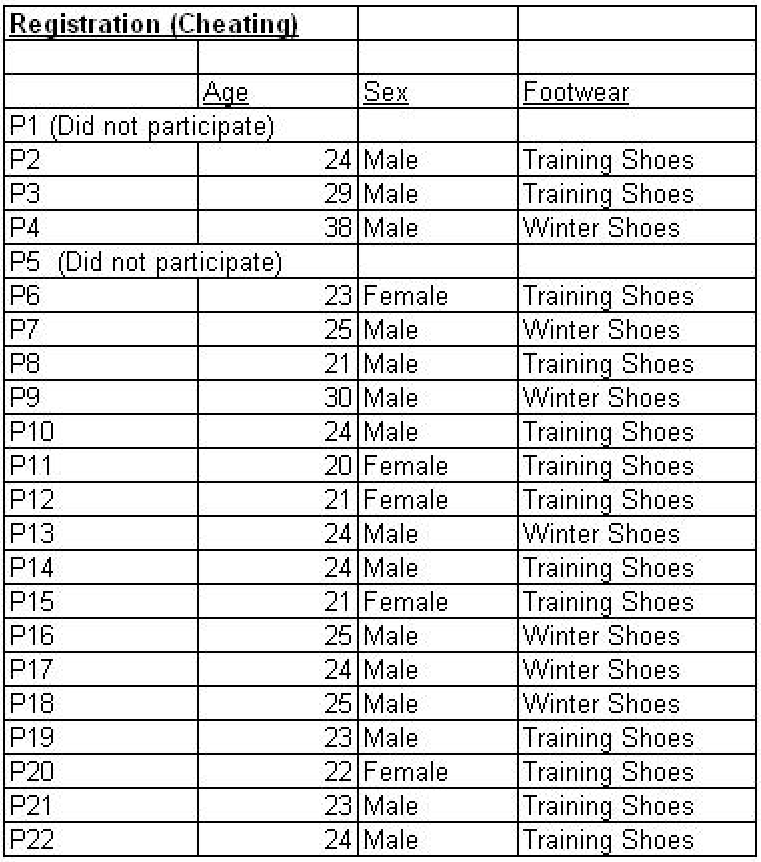
[44] Kuan Zhang, Patricia Werner, Sun Ming, F.Xavier Pi-Sunyen, and Carol N. Boozer. Measurement of human daily physical activity. *Obesity Research*, 11(1), January 2003.

A Registration of information



Registration (Ordinary walk)			
	Age	Sex	Footwear
P1	27	Male	Winter Shoes
P2	24	Male	Training Shoes
P3	29	Male	Winter Shoes
P4	38	Male	Winter Shoes
P5	24	Male	Winter Shoes
P6	23	Female	Training Shoes
P7	25	Male	Winter Shoes
P8	21	Male	Winter Shoes
P9	30	Male	Winter Shoes
P10	24	Male	Training Shoes
P11	20	Female	Training Shoes
P12	21	Female	Training Shoes
P13	24	Male	Winter Shoes
P14	24	Male	Training Shoes
P15	21	Female	Training Shoes
P16	25	Male	Winter Shoes
P17	24	Male	Winter Shoes
P18	25	Male	Winter Shoes
P19	23	Male	Training Shoes
P20	22	Female	Training Shoes
P21	23	Male	Training Shoes
P22	24	Male	Training Shoes

Figure 14: Registration overview (ordinary walk)



Registration (Cheating)			
	Age	Sex	Footwear
P1 (Did not participate)			
P2	24	Male	Training Shoes
P3	29	Male	Training Shoes
P4	38	Male	Winter Shoes
P5 (Did not participate)			
P6	23	Female	Training Shoes
P7	25	Male	Winter Shoes
P8	21	Male	Training Shoes
P9	30	Male	Winter Shoes
P10	24	Male	Training Shoes
P11	20	Female	Training Shoes
P12	21	Female	Training Shoes
P13	24	Male	Winter Shoes
P14	24	Male	Training Shoes
P15	21	Female	Training Shoes
P16	25	Male	Winter Shoes
P17	24	Male	Winter Shoes
P18	25	Male	Winter Shoes
P19	23	Male	Training Shoes
P20	22	Female	Training Shoes
P21	23	Male	Training Shoes
P22	24	Male	Training Shoes

Figure 15: Registration overview (cheating walk)