MSc Project Plan

Face Recognition Software:

Non-zero effort attacks' effect on False Acceptance Rate of face recognition products in a border control environment

Tom Fladsrud
tom@fladsrudsolutions.com
Mobile phone: +47 41 52 84 94
NISlab
Gjøvik University College

version 6.0

December 22, 2004

Abstract

By the end of the year 2006 the Visa Information System (VIS) is to be implemented, and the members of Schengen can start connecting their national VIS systems towards VIS. VIS is the new Europewide visa system operating together with national VIS-systems that includes biometric authentication. Biometrics will be used to implement measures to strengthen the security by making it harder for an adversary to perform identity theft. The intention with the system is to prevent identity fraud and ensure the implementation of the European Union's asylum politics, by exchanging information about the citizens applying for visa [1], [2]. The VIS will consist of a several national VIS's (operational from 2005). When choosing the products for face recognition in a border control environment, such as VIS, it is important that the data on which the evaluation is based is established by using environment similar to that in a border control environment. One of the criteria applied when deciding which product to use will be its False Acceptance Rate (FAR). Literature confirms that biometrics like fingerprints can be easily spoofed using methods like silicon dummy-fingers [3], and it is also possible to spoof face recognition products. This thesis will examine what effect non-zero effort impostors will have on different face recognition products FAR when used in a environment similar to that of a border control environment.

Sammendrag

Innen slutten av år 2006 er Visa Information System (VIS) tenkt implementert, og medlemmer av Schengen kan begynne å koble deres nasjonale VIS- systemer opp mot VIS. VIS er det nye Europeiske visum systemet som opererer sammen med nasjonale VIS systemer som inkluderer biometrisk autentisering. Biometri skal brukes for å implementere tiltak for å styrke sikkerheten ved å gjøre det vanskeligere for en motstander å utføre identitets tyveri. Intensjonen med systemet er å hindre identitetssvindel og sikre innføringen av EU's asyl politikk, ved å utveksle informasjon om innbyggerne som søker visum [1, 2]. VIS vil bestå av flere nasjonale VIS (operative fra 2005). Når man skal velge produkter for ansiktsgjenkjenning i et grensekontroll miljø, slik som VIS, er det viktig at dataene som evalueringer blir basert på er fastslått ved å bruke miljøer som er lignende er grensekontroll miljø. En av kriteriene som blir brukt når man bestemmer hvilket produkt som skal brukes er False Acceptance Rate (FAR). Litteraturen bekrefter at biometri slik som fingeravtrykk lett kan forfalskes ved bruk av silikon fingre [3], og

det er også mulig å lure ansiktsgjenkjenningsprodukter. Denne masteroppgaven vil undersøke hvilken effekt bedragere, som bruker ulike metoder for å lure systemet, har på forskjellige ansiktsgjenkjennings produkters FAR når de brukes i et miljø tilsvarende et grensekontroll miljø.

Contents

1 Introduction

1.1 Topic covered by this thesis

The new visa system involves biometrics such as fingerprint and face recognition. This thesis will focus on the use of face recognition in a border control environment with non-zero effort attackers and the effect these will have on face recognition products False Acceptance Rate (FAR). This thesis will examine the different methods for circumventing face recognition products, involving the resources and skills needed and the potential cost. We will relate these findings to a border-control environment to see what impact this will have on FAR in a border-control environment.

Keywords: False Acceptance Rate, Face recognition, non-zero effort impostors, biometrics, Visa Information System

1.2 Problem description

A growing security issue today is the increased occurrences of identity fraud [4] used in terror related crimes to gain access to resources and locations [5, 6], and illegal immigration with false passport and visa [7, 8]. This is an issue that the new VIS will try to defeat. Applicants trying to get a visa might not give the correct information about their name, place of living and so on, and they might also try to get a visa under several different names. If the authorities checking the information receives applications containing only written data, they have no way of checking if the applicant has tried to apply under a different name. This a problem that VIS will try to defeat by using biometric authentication such as face recognition (mandatory) and fingerprint (optional) [2] as a supplement to manual control. When the applications in addition contain on or more photography's of the applicants face, and this is registered in a central database, the authorities can check the information by searching with given criteria's over registered faces. When deciding which face recognition product to use, one of the criteria's used is the FAR of the product.

Traditional estimation of FAR of face recognition products is usually based on "zero effort" impostors' [9]. In a real border control environment this kind of estimate would not necessarily be representative for the real amount of false acceptances. Potential attackers with plenty of resources could use several technological and physical techniques to circumvent the system. This could involve physiological alteration of their appearances using masks, facial makeup or plastic surgery, or technological techniques to alter information of an applicant for a visa. Also, identical twins is traditionally problematic when using face recognition, although a supplier of 3D face recognition claims to have encountered this problem [10]. It is therefore important to examine how such attacks would influence the FAR and how they are performed and what resources are needed to perform them, so that one is able to estimate how realistic appearances of such attacks are.

1.3 Justification, motivation and benefits

1.3.1 Justification and motivation

There exists little or no publicly available data on face recognition products and how these react to attackers that perform an effort other than simply supplying their own biometric data hoping that they will circumvent the system. How can those employing such systems know which system to use when the evaluation is based sourly on FAR from those that do not make an effort to circumvent the system? This could very well result in the choice of the lesser product. Also, those who employ such system should be aware of the different approaches that exist for circumvention, so that they can make measures to thwart this. This thesis will provide an overview of these attacks and how they are done.

1.3.2 Benefits

Institutions that are employing face-recognition products will undoubtedly benefit from a survey that has demonstrated the effect of non-zero effort impostors on FAR, since this would make them more aware of the potential differences between traditional estimation of FAR and when it is based on non-zero effort attacks. Hopefully this will make for a demand for more realistic evaluations of FAR, more in accordance with the environments it will be employed in. Users may then avoid potentially costly pitfalls. In Norway such stakeholders could be UDI, which heavily involved with the introduction of face-recognition in the new NORVIS (the Norwegian version of VIS) system, and other institutions that decide to use face-recognition products.

1.4 Research question

The following issues will be examined:

1. What efforts does an impostor need to make to deceive a face recognition product in a border control environment?
2. How will the resources of an attacker influence the security of a face recognition product in a border control environment?
3. Does different face recognition products produce different FAR given a type of attack?
4. Could today's procedures for calculating FAR result in a positive evaluation of "insecure" products?
5. What effect will non-zero effort attacks have on the FAR of a face recognition product in a border control environment?

2 Review of state of the art

2.1 What efforts does an impostor need to make to deceive a face recognition product in a border control environment?

Kosmerlj's [9] documents in her thesis the flaws and drawbacks of existing face recognition software, however the technology of face recognition is constantly improved [11], and the need for new studies will emerge along with new technology. Also, face recognition will be used in the new visa system VIS and it is therefore necessary to know which attacks that are possible and how easy it is to perform them. You should also keep in mind that although today's face recognition is far from perfect in automatic authentication systems [9], face recognition in VIS will be supplemented by manual control, something that will make it far harder for an impostor to succeed.

The UK Biometric Working Group [12] deals with possible flaws and possible attacks on biometric products. They also identify drawbacks of using biometrics as authentication like the fact that a biometric feature cannot be replaced when compromised.

However they do not say anything about how the capacity of an adversary will have influence on the strength of a biometric product. From experience with other biometric characteristics used in authentication, such as fingerprint, which adversaries already has circumvented there is reasonable to believe that also face-recognition products could be fooled now or in the future by a skilled adversary. It is therefore necessary to examine if there are known ways of circumventing a face-recognition product, and if the capacity of the adversary must be large for this to be a reality. An idea would be to also look at possible countermeasures regarding this issue.

2.2 How will the resources of an attacker influence the security of a face recognition product in a border control environment?

To evaluate how the resources of an attacker will influence the security of a face recognition product, one has to consider the difficulty of performing a successful attack. Ton van der Putte and Jeroen Keuning demonstrate in their article [3] how easy one can perform attacks on fingerprint system. In the master thesis "Liveness Detection in Fingerprint Recognition Systems" [13] by Marie Sandström she perform a somewhat related study, however this is a study based on fingerprint and it is not related to a border-control environment. Other articles found deal with related issues, but I did not find any articles examining the influence attackers resources would have on face recognition products in a border control environment.

2.3 Does different face recognition products produce different FAR given a type of attack?

False rejection rate (FRR) is the probability that a genuine person is rejected and false acceptance rate (FAR) is the probability that an impostor is accepted as a legitimate person. The point were FRR and FAR are equal is called equal error rate (EER). Face recognition products that shall be used by VIS in a border control environment, where the intension is that as many previously registered candidates as possibly are recognized, shall operate on a small False Rejection Rate when registering a new visa applicant to prevent multiple registrations of visa applicants. Further, the face recognition products must provide as small FAR as possible at the border control when the visa is checked to grant the applicant access to the country, to increase the security.

In the book "Biometrics: Personal Identification in Network Society" [14] there is stated a claim that any human physiological or behavioural characteristic could be a biometrics provided it has the following desirable properties. The authors claim characteristics universability, uniqueness, performanence, collectabillity, performance, acceptability and circumvention make up an ideal biometric.

In the case of information security the uniqueness of characteristic and how easy it is to fool the system may perhaps be the most significant characteristics of a biometric. These characteristics are defined as follows:

- Uniqueness - no to person should have the same characteristics
- Circumvention -how easy is it to fool the system by fraudulent techniques

Although I have found much literature on FAR and Face recognition, none of them addressed if or how different face recognition products will produce different FAR given a type of attack. This calls for a further study on the subject.

2.4 Could today's procedures for calculating FAR result in a positive evaluation of "insecure" products?

If the procedures for estimating FAR that are in use today could lead to a positive evaluation of a so-called "insecure" face-recognition product, it could result in a huge amount of founds going to waste.

There exist studies of calculation of FAR [15], including Kosmerlj's MSc thesis [9]. However none of the literature that I have found deals with FAR calculated in a hostile environment similar to that of a real border environment, and with the impact non-zero effort impostors have on the estimation of the FAR.

This implies a need for further study of the topic that result in an independent and publicly available survey on the subject.

2.5 What effect will non-zero effort attacks have on the FAR of a face recognition product in a border control environment?

Kosmerlj has in her MSc thesis [9] conducted experiments for surveying similarities in faces of persons in a group in computer based biometric recognition. This thesis is however based on persons with 'real' biometrics. That is, they have not done any effort to falsify their biometrics.

Although she survey the impact the size and selection of the test persons have on FAR, she does not examine how FAR will be affected by non-zero effort impostors. She also recognizes the need for a more realistic false acceptance rate in an adversary environment. In that context it is important that the environment in which the test in conducted is similar to that of a real border control environment.

3 Summary of claimed contributions

As we have seen by the literature study, there has been conducted much research in the area of face recognition, and in computing of false acceptance rate with zero effort impostors. But when the new system for visa applications is to be implemented, there is also a use for an examination on how the different face recognition products will work in a border control environment. The overall impression is that experiments conducted does not examine how FAR will be affected by non-zero attacks. Kosmerlj [9] recognizes the need for a more realistic false acceptance rate in an adversary environment. In that context it is important that the environment in which the test in conducted is similar to that of a real border control environment. This is what this thesis will try to do.

The contributions likely to be produced by this thesis are listed bellow:

1. An examination of the existing methods of calculating the FAR

2. An examination of the effort and resources needed by an adversary to perform a successful attack on a face recognition product used in a border control environment, and how the success will depend on the resources of the adversary. Including a definition of what is considered a successful attack.

3. Based on the findings in the literature examination we will try to make an experiment to assist in the qualitative findings.

4. A comparison of FAR obtained by traditional calculations and the result from the experiment with non-zero effort impostors. And a comparison between the products used in the experiment based on the FAR obtained using the different schemes.

5. An analysis to see if today's procedures for calculating FAR could result in a positive evaluation of "insecure" products?

4 Choice of methods

During the selection face of research questions and topic, we used a literature study to find what is the state of the art and what has not yet been answered and what needs further study. Obviously this method must also be applied in during some of the proceeding work with the thesis, among others when establishing the existing methods of calculating false acceptance rate. To establish the impact non-zero effort attacks will have on the FAR of a face recognition product in a border control environment, I will use a mixed methods approach. I intend to start with a thorough examination of both the published and unpublished material related to circumvention of face recognition products. To get hold of the unpublished documents and material I will contact individuals in the face recognition community, to see if they have material that I can use in my thesis. As a supplement to assist in the interpretation of the findings in the qualitative findings of documents, I will try to conduct an experiment based on the findings in the literature and document examination. One suggestion is to perform an experiment based on the results obtained by Kosmerlj [9] in her thesis. These results could be used to examine if face recognition algorithm system compares human faces in a similar way as people do, by using the images of the participants with many look-alikes and testing them on a test panel to see if they have conception of who look alike.

When deciding which research methods to use, I used J.W. Creswell's book "Research design" [16] as a basis.

4.1 What efforts does an impostor need to make to deceive a face recognition product in a border control environment?

There exists little or non available research on this topic, and a natural way of pursuing this is then by conducting an experiment with different methods of circumventing a face recognition product in an environment similar to that of a border control environment. However to be able to do this, I must first examine the different available methods for circumvention of such systems and obtain an understanding of how the face recognition products interpret the human face. Prior to this examination I will make contact with authors of similar research to get hold of published and unpublished material on the subject of circumvention of face recognition products.

4.2 How will the resources of an attacker influence the security of a face recognition product in a border control environment?

From the data that I collect during the literature study I will make an analysis on how the resources of an attacker will influence the security of face recognition products in a border control environment.

Here I will examine data on resources available to known terrorist groups, and to the average illegal immigrant, and compare this to the resources needed for a successful circumvention of the face recognition product. We can then make an assumption on the possibility of attacks.

4.3 Does different face recognition products produce different FAR given a type of attack?

I will here need to examine the ways the face recognition products recognize faces, to see how the different kinds of attacks will affect the face recognition product.

4.4 Could today's procedures for calculating FAR result in a positive evaluation of "insecure" products?

This is more a part of the conclusion of the thesis, and will be based on the data collected in the preceding research questions.

4.5 What effect will non-zero effort attacks have on the FAR of a face recognition product in a border control environment?

The preceding research questions will provide a good basis in the analysis on whether today's procedures for calculating FAR could result in a positive evaluation of "insecure" products or not, and how the resources of an attacker will influence the security of a face recognition product in a border control environment.

4.6 To summarize the research methods used in the different question, table 1 provides an overview of the methods used for each research question

Table 1: Summary chosen research methods

Question	**Research method**
1. What efforts does an impostor need to make to deceive a face recognition product in a border control environment? 4. Could today's procedures for calculating FAR result in a positive evaluation of "insecure" products? 5. What effect will non-zero effort attacks have on the FAR of a face recognition product in a border control environment?	• Literature study • Experiment
2. How will the resources of an attacker influence the security of a face recognition product in a border control environment? 3. Does different face recognition products produce different FAR given a type of attack?	• Literature study

5 Milestones, deliverables and resources

Resources needed to perform the project, besides contact person, will depend upon the form of the experiment. The experiment should be in a form that does not depend on additional equipment to the available face recognition products at NISlab authentication laboratory. If additional equipment is needed, this will be requested as soon as possible.

As there have been no mandatory deadlines for deliverables during the master thesis work, I will present the work conducted at the end of each month to the teaching supervisor and my contact persons. These may then come up with suggestions and directions to guide me in the further work.

5.1 Activities, time schedule and resources

I have chosen to break down the project in the following parts and activities:

- Identifying contact persons within the face recognition community
- Preparing contact with persons within the face recognition community
- Making contact with individuals within the face recognition community to get hold of published and unpublished documents and material
- Study and evaluation of received and collected material
- Preparing an experiment based in the findings from previous findings
- Execute the experiment
- Evaluate the result from the experiment and compare with the result of others on similar experiments
- MCs thesis report writing
- Preparation of presentation of MSc thesis report at Gjøvik University College
- Presenting the final MSc thesis report at Gjøvik University College

These activities is presented in table 2 with an overview of the main activities including an estimation of start and end time, and estimation of the time needed to perform these activities.

The overview in table 2 contains only a rough estimate of the time needed to conduct the thesis. In order to get a better overview of the expected results from each week I have made a time schedule with a plan of each week with the activities and estimated time spent on the thesis. This week schedule is presented in table 3.

Table 2: Activities, deliverables and milestones

Activity	**Hour needed**	**Start time**	**End time**	**Contributors**
Identifying contact persons within the face recognition community. This will be conducted continuously through the thesis work starting with a workload of 10 hours	10	W50		The Internet and information obtained from contact persons at ErgoGroup, Gjøvik University College and UDI
Preparing contact with persons within the face recognition community	10	W52	W2	Teaching supervisor at Gjøvik University College
Contacting individuals within the face recognition community to obtain published and unpublished material	15	W2		
Study and evaluation of received and collected material	280	W2		Teaching supervisor and other contact persons at Gjøvik University College, and contacts at ErgoGroup and UDI
Preparing an experiment based in the findings from previous findings	50	W12	W15	Teaching supervisor and other contact persons at Gjøvik University College
Execute the experiment. The time will depend of the form of experiment	max 80	W15	W18	Contact person at ErgoGroup and Gjøvik University College, and other students at NISlab
Evaluate the result from the experiment and compare with the result of others on similar experiments	90	W19	W22	Teaching supervisor and other contact persons at Gjøvik University College
MCs thesis report writing	200	W1	W26	Teaching supervisor and other contact persons at Gjøvik University College
Preparation and presentation of the final MSc thesis report at Gjøvik University College	41	W21	W23	
Total amount of time neede	776			

5.2 Preliminary table of contents for the MSc thesis report

To provide an overview of the expected outcome of my thesis I present a preliminary table of contents for the MSc thesis report bellow.

Title page

Abstract

Table of contents

1. Introduction
   - 1.1 Need for the study
   - 1.2 Purpose of the study
   - 1.3 Statement of the problem
   - 1.4 Research questions
   - 1.5 Delimitations
2. Theory
   - 2.1 False Acceptance Rate
   - 2.2 Visa Information System and border control environments
   - 2.3 Face recognition
     - 2.3.1 History of face recognition
     - 2.3.2 Face recognition systems evaluation and apprehension of faces
     - 2.3.3 Face recognition circumventions and protection schemes
     - 2.3.4 Definition of a successful attack of a face recognition product in border control environment
3. Experiment
   - 3.1 Description
   - 3.2 Results
4. Discussion and analysis
5. Conclusion
6. Suggestions for future research
7. References
8. Appendixes

Table 3: Schedule of weekly activities

Week	**Hours**	**Activities**
52	20	Identifying contact persons (10) and preparing contact persons within the face recognition community by collecting information on the Internet (10)
2	40	Contact persons within the face recognition community (15), and study and evaluation of received and collected material (25)
3 - 11	279	Gather information, and study and evaluate it (25 per week), and write on the master thesis (6 per week). Delivery 1 and 2 of the master thesis week 6 and 10
12 - 14	75	Gather information and study and evaluate it (5 per week), write on the master thesis (5 per week) and preparing an experiment (15 per week). Delivery 3 of the master thesis week 14
15	30	Preparing the experiment (5), writing on the master thesis (5) and performing the experiment (20)
16-18	90	Writing on the master thesis (10 per week) and performing the experiment (20 per week). Delivery 4 of the master thesis week 18
19-21	90	Evaluate the result from the experiment (30 per week)
22	45	Preparing the master thesis presentation (30) and gather and compare information related to the experiment with the experiment conducted in this thesis (15)
23	32	Preparing the master thesis presentation (10), presenting the master thesis (1) and write on the master thesis (21). Delivery 5 of the master thesis week 23
24 - 26	75	Writing on the master thesis (25 per week)
Total	776	

6 Feasibility study

It is my belief that this thesis will be accomplish within the time frame of 795 hours distributed over 28 weeks (week 52 - 26), and with the resources available at the authentication lab at Gjøvik University College. I will work part time combined with this thesis, and therefore I will also spend most evenings and weekends working with the thesis. With the assistance of my contact persons at Ergo and UDI and contact persons at Gjøvik University College, which has substantial knowledge on the subject of face recognition, I believe this project is feasible within the given time frame. The main part of this project consists of information gathering with literature study analysis of the obtained data. Provided I come in contact with person that have substantial knowledge and material on circumvention of face recognition products, I believe I will succeed. Sandström [13] conducted a similar report in 2004 on fingerprint recognition within the same timeframe, although there exist more material on circumvention of fingerprint recognition products, I believe that this thesis will have about the same amount of workload.

7 Risk analysis

The success of this thesis will to a large degree depend on the success in finding material on circumvention on face recognition products. See table 4 "Risk analysis" for details of potential problems and suggestions on how to solve them.

8 Ethical and legal considerations

If an experiment is carried out the participants will be informed about the purpose of the experiment, and an informed consent will be obtained form these volunteers in accordance with [17]. The data collected from the volunteers will be kept private, and treated in a way to protect the confidentiality. After completion of the project the biometric data will be erased. When finding volunteers it is important that their participation is completely voluntary, and that they can drop out at any time. The volunteers' identity must never be released. These criteria must be followed both because of the ethical issues and legal issues, among others the laws that must be fulfilled in accordance with "Personopplysningsloven" [18].

Table 4: Risk analysis

Problem	**Consequences**	**Problem solutions/reduction**
Illness of the author	The project will be delayed. If I get long-lasting illness, this will lead to postponement of the project.	In the case of long-lasting illness I have to get a delay of the deadline. If the sickness is over a short time, I have to work harder in a period.
I don't find material related to circumvention of face recognition products	The project will not be completed	Resources at ErgoGroup which are heavily involved in the face recognition community could probably help me come in contact with the right contacts.
None of the contact persons within the face recognition community answers to my email	This will make the project less satisfactory.	I have to take contact with potential resources in good time. If they do not respond I shall send a new email or call them in case te email did not get through.
Not enough students wants to participate in the experiment	Unsatisfactory test results	I can include others from outside the NISlab community.
My computer crashes during the writing of the thesis	I will lose important information, and the thesis will be severely delayed	Take backup daily. Weekly backup on an extern hard disk

References

[1] Thor Arne Aass and Bjørn Rygh. Nyhetsbrev om norsk flyktning- og innvandringspolitikk nr. 13. *Kommunal- og regionaldepartementet og Utlendingsdirektoratet*, 11, March 30, 2004. `http://odin.dep.no/krd/norsk/innvandring/nytt/016081-990237/dok-bn.html`.

[2] Eu visa information system gets go-ahead. *eGovernment News*, February 24, 2004. `http://europa.eu.int/ida/en/document/2186/569`.

[3] Ton van der Putte and Jeroen Keuning. Biometrical fingerprint recognition: Don't get your fingers burned. Technical report, September 21 2000.

[4] Justin Madubuko. Identity theft is fastest-growing threat. *Silicon.com*, September 18, 2001. `http://software.silicon.com/applications/0,39024653,11027487,00.htm`.

[5] Norman A. Willox JR. and Thomas M. Regan. Identity fraud: Providing a solution. *LexisNexis*, March 2002. `http://www.lexisnexis.com/about/whitepaper/IdentityFraud.pdf`.

[6] Graeme R. Newman. Identity theft, problem-oriented guides for police. *Problem-Specific Guides Series No. 25, U.S. Department of Justice, Office of Community Oriented Policing Services.* `http://www.cops.usdoj.gov`.

[7] Jennifer Hopkins. Increase in arrests for visa and passport fraud. *U.S. Visa News*, December 29, 2003. `http://www.usvisanews.com/articles/memo2194.shtml`.

[8] Chad Groening. Ins vet warns public about illegal immigration-identity theft link. *Religion News*, November 17, 2003. `http://news.christiansunite.com/Religion_News/religion00070.shtml`.

[9] Marijana Kosmerlj. Passport of the future: Biometrics against identity theft? Msc thesis, Gjøvik University College, NISlab, June 30, 2004. `http://nislab.hig.no/Research/docs/marijanak-2004.pdf`.

[10] Tom Geoghegan. How your face could open doors. *BBC News Magazine*, November 25, 2004. `http://news.bbc.co.uk/1/hi/magazine/4035285.stm`.

[11] Paul Festa. Face recognition gets lift, u.s. says. *CNET News.com*, March 25, 2003. `http://news.zdnet.com/2100-1009_22-994111.html`.

[12] UK Government Biometrics Working Group. Biometric security concerns v1.0. September 2003. www.cesg.gov.uk/site/ast/biometrics/media/BiometricSecurityConcerns.pdf.

[13] Marie Sandström. Liveness detection in fingerprint recognition systems. Msc thesis, Linköpings tekniska högskola, 2004. http://www.ep.liu.se/exjobb/isy/2004/3557/exjobb.pdf.

[14] Ruud Bolle Anil Jain and Sharath Pankanti. *Biometrics: Personal Identification in Network Society.* The Kluwer international series engineering and computer science. Boston: Kluwer, 1999.

[15] Anil K. Jain, S. Prabhakar, and Sharath Pankanti. Can identical twins be discriminated based on fingerprints? Technical Report MSU-CSE-00-23, Department of Computer Science, Michigan State University, East Lansing, Michigan, October 2000.

[16] John W. Creswell. *Research Design Qualitative, Quantitative, and Mixed Methods Approaches, Second Edition.* SAGE Publications, 2003.

[17] A.J. Mansfield and J.L. Wayman. Best practices in testing and reporting performance of biometric devices, version 2.01. August 2002. http://www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf.

[18] Justis og politidepartementet. Personopplysningsloven, 2000, hefte 8. http://www.lovdata.no/cgi-wift/wiftldles?doc=/usr/www/lovdata/all/nl-20000414-031.html&dep=alle&titt=personopplysningsloven&.