Gesellschaft für Informatik (GI)

publishes this series in order to make available to a broad public recent findings in informatics (i.e. computer science and information systems), to document conferences that are organized in cooperation with GI and to publish the annual GI Award dissertation.

Broken down into the fields of
• Seminar
• Proceedings
• Dissertations
• Thematics
current topics are dealt with from the fields of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure the high level of the contributions.

The volumes are published in German or English.

Information: http://www.gi-ev.de/service/publikationen/lni/

ISSN 1617-5468
ISBN 978-3-88579-249-1

The proceedings of the BIOSIG 2009 include scientific contributions of the annual conference of the Special Interest Group on Biometrics and Electronic Signatures (BIOSIG) of the Gesellschaft für Informatik (GI). The conference took place in Darmstadt, 17.-18. September 2009. Within two days mainly the advances of biometrics research and updates in the application field of electronic signatures have been presented and discussed by professionals.

Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.):
BIOSIG 2009: Biometrics and Electronic Signatures

155

GI-Edition

Lecture Notes in Informatics

Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.)

BIOSIG 2009: Biometrics and Electronic Signatures

Proceedings of the Special Interest Group on Biometrics and Electronic Signatures

17.–18. September 2009, Darmstadt, Germany

Proceedings

Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.)

BIOSIG 2009

Proceedings of the Special Interest Group on Biometrics and Electronic Signatures

17.-18. September 2009 in Darmstadt, Germany

Gesellschaft für Informatik e.V. (GI)

Lecture Notes in Informatics (LNI) - Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-155

ISBN 978-3-88579-249-1
ISSN 1617-5468

Volume Editors
Arslan Brömme
InterComponentWare AG
Industriestraße 41, D-69190 Walldorf
Email: arslan.broemme@aviomatik.de
Christoph Busch
Hochschule Darmstadt
Fachbereich Media
Haardtring 100, D-64295 Darmstadt
Detlef Hühnlein
secunet Security Networks AG
Sudetenstraße 16, D-96247 Michelau
Email: detlef.huehnlein@secunet.com

printed by Köllen Druck+Verlag GmbH, Bonn

Chairs' Message

Welcome to the annual international conference of the Special Interest Group on Biometrics & Electronic Signatures (SIG BIOSIG) of the Gesellschaft für Informatik (GI) e.V.

The SIG BIOSIG was founded as an experts' group for the topics of biometric person identification/authentication and electronic signatures and its applications. Over the last eight years the annual conference in strong partnership with the Competence Center for Applied Security Technology (CAST) established a well known forum for experts from industry, science, and representatives of the national governmental bodies working in these areas.

The BIOSIG 2009 international conference is jointly organized by SIG BIOSIG, CAST, the German Federal Office for Information Security (BSI), the European Commission Joint Research Centre (JRC), the European Biometrics Forum (EBF), and the Center for Advanced Security Research Darmstadt (CASED).

The international program committee accepted full scientific papers strongly along the LNI guidelines within a scientific review process of about four reviews per paper in average. This year's acceptance rate for scientific contributions (regular research papers) is about 40%.

Furthermore, the program committee has created a very interesting program including selected contributions of strong interest (invited and further conference contributions) for the outlined scope of this conference.

Darmstadt, 17th September 2009

Arslan Brömme
InterComponentWare AG

Christoph Busch
Hochschule Darmstadt

Detlef Hühnlein
secunet Security Networks AG

Chairs

Arslan Brömme
InterComponentWare AG, Walldorf, Germany

Christoph Busch
Hochschule Darmstadt, Germany

Detlef Hühnlein
secunet Security Networks AG, Michelau, Germany

Program Committee

Ignacio Alamillo, Harald Baier, Andre Braunmandl, Björn Brecht, Arslan Brömme, Patrick Bours, Bud Bruegger, Christoph Busch, Victor-Philipp Busch, Henning Daum, Nicolas Delvaux, Farzin Deravi, Martin Drahanský, Simone Fischer-Hübner, Marc Fischlin, Lothar Fritsch, Rüdiger Grimm, Olaf Henniger, Detlef Hühnlein, Bart Jacobs, Holger Junker, Sokratis K. Katsikas, Klaus Keus, Ulrike Korte, Bernd Kowalski, Michael Kreutzer, Andreas Kühne, Herbert Leitold, Luigi Lo Iacono, Jan Löschner, Stefan Lucks, Tarvi Martens, Fabio Martinelli, Gisela Meister, Johannes Merkle, Alexander Nouak, Reinhard Posch, Kai Rannenberg, Heiko Roßnagel, Raul Sanchez-Reillo, Günter-Egon Schumacher, Jörg Schwenk, Max Snijder, Till Teichmann, Raymond Veldhuis, Guilin Wang, Alexander Wiesmaier, Christopher Wolf, Xuebing Zhou, single reviews by Daniel Hartung, Matthias Herbst, Alexander Opel

Hosts

Special Interest Group on Biometrics and Electronic Signatures (**BIOSIG**)
of the Gesellschaft für Informatik (GI) e.V.
http://www.biosig.org

Competence Center for Applied Security Technology (**CAST**) e.V.
http://www.cast-forum.de

Bundesamt für Sicherheit in der Informationstechnik (**BSI**)
http://www.bsi.bund.de

European Commission Joint Research Centre (**JRC**)
http://ec.europa.eu/dgs/jrc/index.cfm

European Biometrics Forum (**EBF**)
http://www.eubiometricsforum.com

Center for Advanced Security Research Darmstadt (**CASED**)
http://www.cased.de/

BIOSIG 2009 – Biometrics and Electronic Signatures

"**Biometrics and Electronic Signatures – Research and Applications**" –
17th -18th September 2009

Biometrics and electronic signatures are central technological components within the present landscape of authentication and identification of entities, the integrity of biometric templates and signatures, and electronically signed entity information as well as in multiple sceanrios of emerging future identity management. Recent developments in the confidentiality domain show also additionally a strong interest in integrating biometric information in cryptographic keys.

Years of research and development in biometrics and electronic signatures elapsed and still three main scientific questions based on biometric measurement data, knowledge, possession, time, and place are in need to be answered:

1. "who can it be?" - based on partially available data
2. "who is it for sure?" - based on fully available data
3. "can it be misused?" - based on any available data

Challenges are given in sufficient number in going to answer all three questions like you will see in this year's program.

Single different competing modalities and factors have been approached and fine tuned to find the best identity determining method. Multimodal approaches have been tested to compensate the deficiencies of single modalities and to find again a best multimodal authentication and identification method.

Identity management applications and broad public used applications with the inherent legal considerations regarding non-repudiation are still in strong need of reliable authentication and identification technology. Users are expecting this anyway before they are willing to accept the proposed technology in their daily life.

Now, multifactor multimodal biometric authentication and identification technology with biometric multitemplates of different types is a promising method candidate in place to find a balance between the need for scalable convenience and sensitivity in clear dependence of the intended application.

BIOSIG 2009 offers you again a platform for experts' discussions and focuses this year on **Research and Applications** in the area of **Biometrics and Electronic Signatures.**

Table of Contents

BIOSIG 2009 – Regular Research Papers 11

Minutiae Interoperability
Elham Tabassi, Patrick Grother, Wayne Salamon, Craig Watson 13

Semantic Conformance Testing Methodology for Finger Minutiae Data
Dana Lodrová, Christoph Busch, Elham Tabassi, Wolfgang Krodel, Martin Drahanský 31

The Fuzzy Vault for Fingerprints is Vulnerable to Brute Force Attack
Preda Mihăilescu, Axel Munk, Benjamin Tams 43

Multi-Sample Fusion with Template Protection
Emile J.C. Kelkboom, Jeroen Breebaart, Raymond N.J. Veldhuis, Xuebing Zhou, Christoph Busch 55

Challenges for the Implementation and Revision of International Biometric Standards Demonstrated by the Example of Face Image Data
Peter Ebinger, Margarida Castro Neves, René Salamon, Oliver Bausinger 69

Spectral Selection for a Biometric Recognition System Based on Hand Veins Detection Through Image Spectrometry
Franciso Cortés, José M. Aranda, Raul Sanchez–Reillo, Juan Meléndez, Fernando López 81

The Extended Access Control for Machine Readable Travel Documents
Rafik Chaabouni, Serge Vaudenay 93

SAMLizing the European Citizen Card
Jan Eichholz, Detlef Hühnlein, Jörg Schwenk 105

Sanitizable Signatures: How to Partially Delegate Control for Authenticated Data
Christina Brzuska, Marc Fischlin, Anja Lehmann, Dominique Schröder 117

A Survey of Distributed Biometric Authentication Systems
Neyire Deniz Sarier 129

BIOSIG 2009 – Invited Conference Contributions 141

Quantitative Standardization of Iris Image Formats
Patrick Grother 143

Reverse Public Key Encryption
David Naccache, Rainer Steinwandt, Moti Yung 155

BIOSIG 2009 – Further Conference Contributions 171

Classification of Skin Diseases and Their Impact on Fingerprint Recognition
Martin Drahanský, Eva Březinová, Filip Orság, Dana Lodrová 173

Supplemental Biometric User Authentication for Digital-Signature Smart Cards
Olaf Henniger, Ulrich Waldmann 177

Tamper-proof and privacy-protected fingerprint identification systems
Michael Schwaiger 181

On-line Signature Biometrics using Support Vector Machine
Aitor Mendaza-Ormaza, Oscar Miguel-Hurtado, Ivan Rubio-Polo, Raul Alonso-Moreno 185

A Note on the Protection Level of Biometric Data in Electronic Passports
Harald Baier, Tobias Straub 189

Biometrie – Beschleuniger oder Bremser von Identitätsdiebstahl
Christoph Busch 193

BIOSIG 2009

Regular Research Papers

Minutiae Interoperability

Elham Tabassi, Patrick Grother, Wayne Salamon, and Craig Watson

{tabassi,pgrother,wsalamon,cwatson}@nist.gov

Abstract: Many large scale identity management applications require storage and exchange of standardized minutiae templates. Minutia templates offer a more space-efficient, less resource intensive, and more cost effective alternative to raw images. Recent minutiae interoperability tests (ILO, MTIT, MINEX) all reported variation in minutia selection and placement as the major factor affecting interoperability. This paper quantifies their effects and investigates how variation in selection and placement of minutia from different suppliers relates to loss of performance compared with proprietary templates. We concur with MTIT findings that conformance testing methodologies for evaluating the semantic content of minutia templates is essential and interoperability can be improved by closer adherence to the minutia placement requirement defined in a standard.

1 Introduction

Use of fingerprint templates is increasingly favored over the use of conventional fingerprint images mostly due to its compact representation, and also for privacy concerns. A fingerprint image requires a considerable amount of memory for storage (about 200 Kbytes uncompressed and 15 Kbytes compressed), as opposed to fingerprint templates that are only a fraction of that size (about 300 bytes). Also, the use of fingerprint templates are believed to be more secure allowing privacy sensitive solutions. Addressing size and privacy concerns, a more compact representation of fingerprint images, or templates, has gain acceptance as an alternative to the use and exchange of images for fingerprint matching in dissimilar applications.

A template is a list of specific friction ridge characteristics from a fingerprint image. Minutiae points are local ridge characteristics where a friction skin ridge begins, terminates, or splits into two or more ridges. A minutia point is generally described by its position and orientation in a fingerprint. For many applications, minutiae templates offer a more space-efficient, less resource intensive, and more cost effective alternative to raw images.

For open systems use of minutiae templates as the medium for fingerprint interchange may adversely affect the interoperability and hence performance. Different vendors use different coordinate systems, location and angle definitions to describe the same minutia. These differences could result in lower accuracy of fingerprint matching systems that exchange minutiae extracted using different methods rather than exchange of finger images. Consequently, to improve interoperability, standards have been developed to specify the location and formatting of minutiae data, (i.e. minutiae template), for matching purposes

[JTC08, Ame08, MN07]. These standards create the possibility of a fully interoperable multivendor marketplace for applications involving fast, economic, and accurate interchange of compact biometric templates. To assess the sufficiency and performance of these standards, several evaluations [G+06, Int05, UK 06] have been organized to quantify interoperability and performance degradation of fingerprint matching systems using standard templates compared with proprietary templates.

This paper reviews the problem of interoperability identified in the recent tests and focuses on the factors associated with degraded interoperability when minutiae templates are exchanged. Section 2 gives an overview of the existing minutiae standards. Section 3 reviews federated applications that require interoperable subsystems. The objective of interoperability tests is listed in Section 4 which is followed by overview of NIST Minutia Exchange Interoperability Test and its findings in Section 5. That gives context for our examining of causes of loss in performance when using standard minutia templates vs. proprietary image-based templates in Section 6 which is the main focus of this paper, followed by conclusions and way forward in Section 7.

2 Minutiae standard templates

The first minutiae standard was established in 1986 when the Federal Bureau of Investigation and National Institute of Standards and Technology (formerly the National Bureau of Standards) developed the minutiae-based ANSI/NBS-ICST 1-1986 Data format for fingerprint information interchange standard [McC04]. The standard has been revised three times since, but its latest version; ANSI/NIST-ITL 1-2007 Type-9 Record [MN07]; includes many of the requirements from its original standard. ANSI/NIST Type-9 minutiae information may be extracted and encoded in any of several different manners depending on the system that is used to scan an image, extract minutiae, and encode the minutiae template. The "standard format" defines a common block of tagged fields including mandatory minutia location, angle, type (ridge ending, bifurcation, compound, and undetermined), quality, finger position, finger pattern classification that produced minutia information, and optional data such as ridge count data and core or delta information. Additional reserved blocks are registered and allocated for use by specific vendors allowing them to encode minutiae data and any additional required characteristic or feature data in accordance with their own systems specific hardware and software configuration.

Developed in 2004 and currently under revision, the INCITS 378-2004 Fingerprint minutia format for data interchange [Ame08] is driven by commercial verification rather than law-enforcement identication needs. This standard was based on the ANSI/NIST-ITL1-2000 standard and the FBIs electronic fingerprint transmission specication (EFTS 7.0). The standard specifies how to compute minutia location and angle. Minutia type and quality are also recorded. Unlike ANSI/NIST-ITL1-2007 that uses lower left of an image as the origin, this format uses the upper left corner of the image. A minutia's angle is stated in increments of two degrees. The standard also has provision for an open format defined for the optional inclusion of common extended data fields. These include core and delta information, ridge count information for either four-neighbor quadrants or eight-neighbor

octants, and vendor-defined information. The INCITS 378-2004 also contains provision for formatting data from several presentations or views of the same finger thus accommodating systems that rely on several readings of the same finger to construct a good average template.

International standard ISO/IEC 19794-2 Information technology-Biometric data interchange formats-Part 2: Finger minutia data [JTC08] was developed in 2005 and is currently under revision. Its structure is quite similar to the INCITS 378-2004 standard. The most significant difference between the ISO standard and the INCITS 378-2004 is the representation of minutiae angle which is 2 degrees increments in INCITS 378-2004 as opposed to 1.40625 degrees in the ISO version. As different vendors quantize to different values before mapping to 2 degree increments, this change in representation may not be signicant. ISO/IEC 19794-2 also defines compact representation of minutiae data for storage on smart cards.

3 Interoperable federated applications

Interoperability is not always a requirement for biometric systems, but only when the sources of its different subsystems are different suppliers. Generally speaking, a biometric system is a combination of several subsystems: data acquisition subsystem; transmission and data storage subsystem; template generation (or feature extraction) subsystem for subsequent comparison against stored templates; and finally decision making (or matching) subsystem based on comparison scores, thresholds and possibly other information like biographical or fusion information.

For closed systems, when the supplier of the different subsystems is the same, there is no interoperability issue. Otherwise, high performance would be achieved only if the various subsystems could successfully interoperate. Large-scale identity management applications such as personal identity verification (PIV)[Com], transportation security agency transportation worker identification credential (TWIC) program, and registered travelers (RT)[tsa08] in the U.S. as well as European citizen card are example of large-scale biometric systems that interoperability of its subsystems is essential. In the context of minutia interoperability, that means that minutia extractor algorithm and minutia comparison algorithm of a biometric system should be interoperable. Figure 1 shows the most general scenario for minutia interoperability. Fingerprint images are acquired using capture device A at the enrollment where enrolled templates are generated using algorithm X. Capture device B and template generator Y are used for authentication. Finally minutia comparison algorithm Z, compares minutia templates generated by algorithms X and Y. This is three-way interoperability because algorithms X, Y, and Z need to interoperate. However, often the minutia extractor and matcher of authentication phase (i.e. algorithms Y and Z of Figure 1) are from the same supplier, which makes it a two-way interoperability problem instead of three-way.

If template data rather than fingerprint image could be used with sufficient accuracy in a multi-vendor system, then bandwidth, storage space, and number of template extractions

would all be substantially reduced.

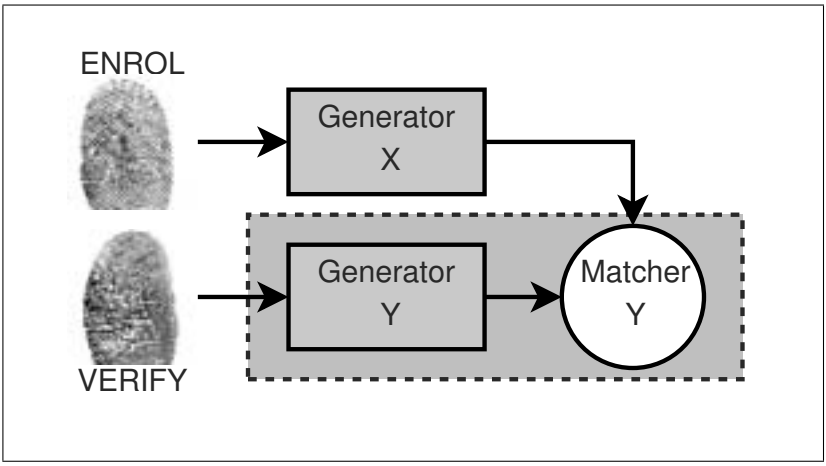


Figure 1: Three-way interoperability: Fingerprint images are acquired using capture device A at the enrollment where enrolled templates are generated using algorithm X. Capture device B and template generator Y are used for authentication. Finally minutia comparison algorithm Z, compares minutia templates generated by algorithms X and Y.

4 Interoperability tests

With increasing number of applications built on standardized templates questions arise regarding interoperability and sufficiency (performance) of the data interchange standard. A data interchnage format is sufficient when information coded in a standrad template is sufficient to enable successful recognition. In other words, error rates when comparing standardized templates are comparable with that of image-based proprietry templates of a leading minutiae extractor algorithm. This is distinct from the issue of interoperability, which mainly considers whether the comparison subsystem is able to process templates generated by different minutia extraction algorithms. Therefore, there is two layers to any interoperability test; interoprability and sufficiency. Minutiae template interoperability testing (MTIT) [UK 06] and the international standard on biometric performance testing and reporting (ISO/IEC 19795-1) [JTC05] refers to these as basic-interoperability and perfomance-based interoperability.

There have been several fingerprint recognition evalutions; fingerprint vendor technology evaluation (FpVTE)[WH$^+$04], fingerprint verification competition (FVC)[oBUUdM06], ongoing NIST proprietary fingerprint templates evaluations (PFT)[W$^+$08] to name a few, but there have been very few interoperability evaluations. The first interoperability test was performed in 2003 by the international labour organization (ILO)[Int05]. NIST initiated minutia exchange interoperability test (MINEX)[G$^+$06] in 2004 which currently is

an on-going evaluation. Minutia template interoperability testing (MTIT) was performed by UK national physics laboratory in 2005. These tests were designed to determine and improve the feasibility of using standard minutiae templates as the interchange medium for fingerprint information between dissimilar fingerprint matching systems. These tests unanimously reported minutia selection and placement as main factors affecting interoperability, without quantifying their effect. This paper aims to investigate how variation in selection and placement of minutia from different suppliers relates to loss of performance compared with proprietary templates using MINEX data. An overview of MINEX follows.

5 The minutia exchange interoperability (MINEX) test

In 2004, national institute of standard and technology performed a large scale minutiae interoperability test to evaluate a) interoperability of the two minutiae extraction subsystems that generate standardized INCITS 378-2004 templates with respect to a comparison subsystem; and b) whether use of standardized minutiae templates instead of image data would result in successful match, i.e. if use of INCITS 378-2004 minutae template as opposed to image results in comparable error rates. The former evaluates feasibility of INCITS 378-2004 minutia templates and the latter its sufficiency. [JTC05] regards these two as basic interoperability and performance-based interoperability.

MINEX is by some measures the largest biometric test ever conducted. It involved testing the core template handling competency of fourteen fingerprint vendors using fingerprint images from a quarter of a million people, and executing in excess of 4.4 billion comparisons, in the production of more than 23,000 detection error tradeoff (DET) characteristics from 493418 mate (same-person) and 975890 non-mate (different person) comparisons.

5.1 Test design

MINEX test design is explained in [G$^+$04]. Each vendor participant provided NIST with their SDK that contained binary C libraries to:

1. create an INCITS 378-2004 MIN:A template from an image, coding minutia location (x, y), angle (θ), and type,
2. create an INCITS 378-2004 MIN:B template from an image, MIN:B is MIN:A with additional ridge count, core and delta information (this was optional),
3. create a proprietary template from an image,
4. produce a comparison score from two MIN:A templates,
5. produce a comparison score from two MIN:B templates (optional), and
6. produce a comparison score from two proprietary templates.

The minutiae quality field required by INCITS 378-2004 was set to zero in all cases, as no universally accepted denition for it exists. Creation of MIN:B templates were optional and only six out of fourteen vendors supplied MIN:B .

To establish a baseline set of performance statistics, MINEX participants were required to generate and compare the proprietary minutiae templates using their propriery minutia extraction and comparison algorithms.

In addition to the proprietary template generation and comparison functions, each MINEX vendors SDK was required to encode and compare MIN:A templates. In these "native" comparions, minutae template representation is constrained by the INCITS 378-2004 specifications while there is no constrain on "proprietary" comparisons. Therefore, the "properiety" comparisons are expected to give better performance than using MIN:A or MIN:B templates. Sufficiency of INCITS 378-2004 was quantified by the performance loss of properietry vs native comparions.

MINEX considered the two-way and three-way interoperability scenraios. Specifically four scenaroios were examined:

1. Enrollment template is generated with supplier X and compared with a template generated with supplier Y in verification transation using comparison algorithm of supplier Y. This is a two-way interoperability and reflects the typical access control situation in which supplier Y's generator and comparison algorithm are bundled together.

2. Compariosn algorithm Z compares templates generated by supplier X and supplier Y. This three-way interoperability scenario (as shown in Figure 1) is the most general case.

3. Comparison algorithm Z compares templates generated by the same supplier (X). This is commercially atypical but was included to examine whether comparison algorithm's dealing with the same-kind templates could result in any performance gain.

4. Comparison algorithm Z compares templates generated by supplier X and supplier Y from the same image. This examines the core of interoperability failure when effect of any difference in image due to re-capture are isolated.

MINEX used the false-non-match-rate (FNMR) at a fixed false-match-rate (FMR) as the figure of merit. The FNMR is the fraction of same-person comparisons that result in a comparison score less than or equal to the operating threshold of the comparison subsystem. FNMR is a measure of inconvenience i.e. the fraction of genuine transactions that result in failure. Likewise the FMR is the fraction of non-mate comparisons that result in a comparison score greater than the operating threshold. FMR is regarded as a measure of security, i.e. the fraction of illegitmate matching attempts that result in success. As is typical in offline testing [JTC05], MINEX did not fix an operating threshold but instead uses all the scores from a comparison algorithm as thresholds that could be used in actual operation. This contrasts with scenario testing which often uses a device configured

with one fixed operating threshold. The output is then a decision and not a score, and this precludes investigation of performance at other thresholds.

5.2 Goals

MINEX objectives, as stated in [G+06], were to assess the viability of the INCITS 378-2004 [Ame08] templates as the interchange medium for fingerprint data. Three specific objectives were

1. To determine whether standardized minutiae enrollment templates can be subsequently matched against an authentication template from another vendor,
2. To estimate the verication accuracy when INCITS 378-2004 templates are compared relative to existing proprietary formats, and
3. To compare the INCITS 378-2004 template enhanced with ridge count "extended" data (MIN:B) with the standards base template (MIN:A).

The first item is the interoperability test and measures core capability of comparison algorithms to process INCITS 378-2004 tempaltes generated by different minutia extraction algorithms. The second item is the sufficiency test and measures performance loss of using INCITS 378-2004 templates instead of image-based proprietry templates. The last item examines the utility of additional ridge count, core and delta information in the extended data fields of INCITS 378-2004 and if it could improve performance.

5.3 Datasets

Four datasets were used in MINEX testing that represented a range of operational image qualities. All of these are operational data sets gathered in on-going US Government operations, and have been sequestered at NIST for testing. MINEX uses randomly selected extracts of those databases. The integrity of the ground truth of the datasets was assured by human inspection. The quality composition of the datasets is tabulated using the NIST fingerprint image quality (NFIQ [TWW04, TW05]) method in Table 1. NFIQ summarization is performed according to recommendations in [TG04].

All datasets used were left and right index fingers only using live-scan plain impressions. The original images were given to NIST already WSQ compressed at approximately 15:1. The images were given to the template extraction algorithms as decompressed (using NISTs WSQ decoder) "raw" pixel data. The original target sample sizes were 62,000 mates and 122,000 non-mates. These totals were reduced after consolidations and a few WSQ decompression failures were taken into account. The testing was performed by using the second instance of the mates as the enrollment image and the first instance as the authentication image. So for each dataset there were a little under 62,000 mate scores. The

Table 1: Summary of NIST fingerprint Image Quality values for the four MINEX data sets

Dataset	finger	1 Best	2	3	4	5 Worst	Summary
1	R	0.424	0.314	0.206	0.026	0.031	92.652
	L	0.442	0.268	0.212	0.034	0.044	91.089
2	R	0.437	0.338	0.157	0.007	0.061	90.912
	L	0.467	0.316	0.157	0.006	0.053	91.812
3	R	0.315	0.374	0.255	0.025	0.031	91.967
	L	0.348	0.3267	0.253	0.028	0.045	90.594
4	R	0.459	0.404	0.105	0.016	0.017	95.386
	L	0.432	0.375	0.143	0.021	0.029	95.386

non-mate scores were generated by comparing the non-mate authentication samples to the same enrollment images used with the mates, so for non-mate scores most enrollment images were used twice. This generated a little under 122,000 non-mate scores for a total of just under 184,000 scores per finger/dataset.

5.4 MINEX **findings**

As mentioned earlier, MINEX measured fingerprint matching error rates when multiple vendors generate and verify the interoperable templates standardized in INCITS 378-2004 . Specifically, MINEX evaluated a tripartite application paradigm in which the enrollment template, the verification template and the comparison algorithm could potentially be provided by different vendors. The study also compared performance available from standard templates with proprietary templates on the same datasets. Two- and three-way interoperability tests result in interoperability matrices of Table 2. The proprietary column shows performance figures (single finger false non-match rate at false match rate of 0.01) when both enrollment and verification templates are generated and compared using proprietary algorithms of a supplier. The native column shows performance numbers when INCITS 378-2004 templates are generated and compared with algorithms from the same supplier. Columns 4, 5, and 6 of Table 2 show, respectively, performance numbers when verification template generator and comparison algorithm are from the same supplier and different from the enrollment template generator, template generator and comparison algorithm are from different suppliers, and when template generator are from the same suppliers but different from the comparison algorithm supplier. Detail interoperability matrices are provided in [G+06]. Qualitatively, the headline findings are that error rates

- are lowest when proprietary templates are used,
- increase when both templates and the matcher are from the supplier (native comparisons),

- increase further when both templates are generated by the same supplier but different from the comparison algorithm supplier, and
- are highest when template and matchers all come from different suppliers.

The loss in performance of proprietary systems compared with native comparisons is somehow expected since standard templates almost always contain less information than proprietary templates. The cost to achieve interoperability is that standard templates do not encode sufficient information needed to achieve performance level comparable with proprietary templates. The fact that using minutia template generators and comparison algorithms from different suppliers result in further performance loss points out the variations in selection and placement of minutiae by different extraction algorithms; either some minutiae are found by one algorithm and missed by the other one, or their encoding makes them look mismatch by the comparison algorithm. That suggests minutia extraction algorithms may systematically interpret a common input differently. The respective algorithmic difficulties are as follows:

- *Selection* - Different implementations will embed different approaches to detection of true minutiae and rejection of false minutiae. This may include regional biases such as ignoring minutiae in the periphery.
- *Placement* - Different implementations will generally report different values for (x, y, θ) despite the qualitative requirements on placement given in INCITS 378-2004 , clause 5.

Examples of these are depicted in Figure 2. Only the two out of six shown minutia are detected and placed similarly by the two minutia extraction algorithms. Note that different colors denote different minutia type. The overall (negative) effect on error rates is shown in Figure 3. Performance of native comparisons (i.e. the same supplier generated and compared standard templates) is always superior to the interoperable comparisons (i.e. comparison of standard templates generated by different suppliers), and in most cases rather significantly.

Further examination of why and how these factors affect interoperability is discussed in the following section.

6 Causes of interoperability degradation

The two major recent interoperability tests, MINEX [G$^+$06] and MTIT [UK 06], identified detection of false minutia and inconsistency in placement of true minutia as two major issues impacting interoperability. This section aims to quantify the effect of selection and placement of minutiae on performance, which is the main contribution of this paper. Detailed discussion follow.

Table 2: Interoperability Matrix: False non-match rate at false match rate of 0.01 for single finger verification. The two-way interoperability values are average over 8 minutia extractor algorithms. The three-way interoperability values are averages over 64 minutia extractor algorithms.

	Proprietary	Native	2 way-interoperability (mean FNMR)	3 way-Interoperablility (mean FNMR)	2 way-Interoperablility (mean FNMR)
Matcher		Enrollment = X Verification=X Matcher = X	Enrollment = X Verification=Y Matcher = Y	Enrollment = X Verification=Y Matcher = Z	Enrollment = X Verification=X Matcher = Z
Vendor 1	0.0089	0.0136	0.0273	0.0268	0.018
Vendor 2	0.0189	0.0251	0.0388	0.0413	0.0260
Vendor 3	0.0225	0.0225	0.0351	0.0373	0.0247
Vendor 4	0.089	0.0140	0.0209	0.0315	0.0225
Vendor 5	0.0047	0.0129	0.0303	0.0283	0.0191

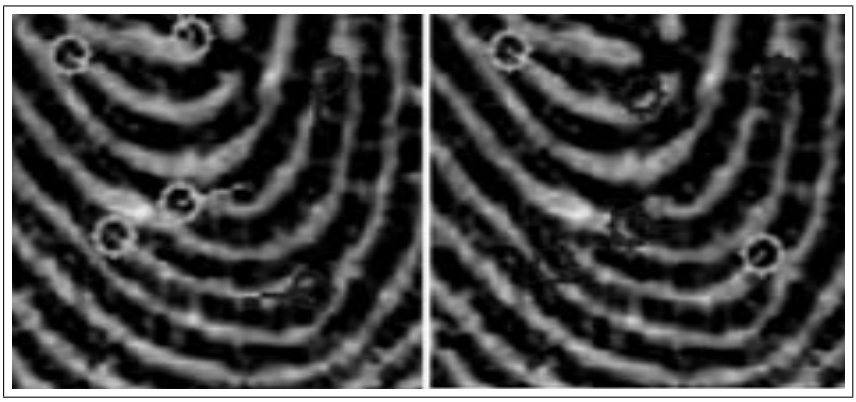


Figure 2: The results of alternative minutiae selection and placement algorithms: Note the angle differnce at top right, and the type, angle, and location differences at bottom right.

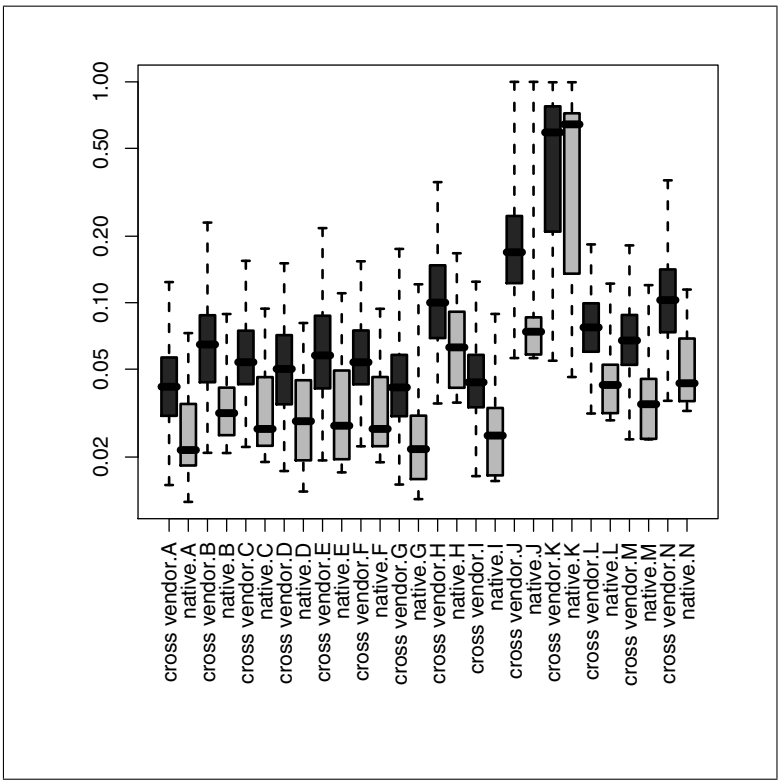


Figure 3: False non-match rate of native (standard minutia templates generated and compared with algorithms from the same supplier) and interoperable (standard minutia templates generation and comparison are performed using algorithms from different suppliers) at a false match rate of 0.01.

6.1 Effect of minutia placement on performance

The objective is to quantify the effect of variation in (x, y, θ) encoding by different minutia extractor algorithms on performance. To do so, we first calculated the number of minutia that are found to be the same within two finger minutia templates of the *same* image created by two different extractors. The criteria for overlapping minutiae is that the (x, y) coordinate of one minutia falls within radius R of an imaginary circle drawn about the second minutia's coordinate (We used $R = 5$ pixels). The fraction of overlapped minutiae is the size of the intersection set divided by the size of the smaller of the number of minutiae in the two input templates. Further, we calculated the mean displacement of those minutiae that are found to be paired as well as the difference in their angle.

Suppose M_i^n is the set of minutiae templates created by algorithm i from the n^{th} image ($n = 1 \dots N$). That is,

$$M_i^n = \{(x_k, y_k, \theta_k) \mid k = 1 \dots K_i\} \tag{1}$$

For each image $n = 1 \dots N$, the set of minutiae in common between extractors i and j is given by

$$R_{ij}^n = \{(k, l) \mid d_{ij}^n(k, l) \leq 5 \; and \; i \neq j\} \tag{2}$$

where

$$d_{ij}^n(k, l) = \sqrt{(x_k^n - x_l^n)^2 + (y_k^n - y_l^n)^2} \tag{3}$$

is the distance between the k^{th} minutia of extractor i and the l^{th} minutia of extractor j from the n^{th} image.

We picked the seven better performers of MINEX participants which result in $C(7, 3) = 210$ different combinations of minutia generators and matcher. To estimate variation in minutiae placement by different suppliers, we selected a random subset of $N = 20,000$ right index images of MINEX Dataset 1 (see Table 1). For each $n = 1 \dots N$ image, we computed the fraction of overlapped minutiae for algorithms i and j

$$m_{ij}^n = \frac{|R_{ij}^n|}{min(|R_i^n|, \; |R_j^n|)} \tag{4}$$

mean misplacement over all of overlapped minutia

$$d_{ij}^n = \frac{\sum_{(k,l)} d_{ij}^n(k, l)}{|R_{ij}^n|} \tag{5}$$

and mean angular difference of overlapped minutiae

$$A_{ij}^n = \frac{\sum_{(k,l)} |(\theta_k^n - \theta_l^n)|}{|R_{ij}^n|} \tag{6}$$

To get a summary statistic of the above three quantities for each (enrollment, verification) minutiae generator pair, we computed their 1-percentile value over all $20,000$ images.

$$\begin{aligned} \text{angleDifference} &= \{\text{CDF}^{-1}_{A_{ij}}(0.01) \mid \forall i \neq j \text{ extractors}\} \\ \text{fractionInCommon} &= \{\text{CDF}^{-1}_{R_{ij}}(0.01) \mid \forall i \neq j \text{ extractors}\} \\ \text{misplacement} &= \{\text{CDF}^{-1}_{d_{ij}}(0.01) \mid \forall i \neq j \text{ extractors}\} \end{aligned} \tag{7}$$

We used a model that is additive in fraction of overlapped minutia, misplacement of overlapped minutiae, and difference in angle of overlapped minutia (eq. 7) to describe the performance loss of native comparisons (template generators and comparison algorithm from same supplier) compared with interoperable comparisons (template generators and comparison algorithm from different supplier). Performance loss is expressed as the delta between false nonmatch rate of native comparisons (F_{kkk}) and false non-match rate of interoperable comparisons (F_{ijk}) when threshold was set at native comparisons' false match rate of 0.01.

$$\begin{aligned} F^t_{ijk} - F^t_{kkk} &= \alpha + \beta_1 \text{ratio} + \beta_2 \text{misplacement} \\ &\quad + \beta_3 \text{angleDifference} + \epsilon \end{aligned} \tag{8}$$

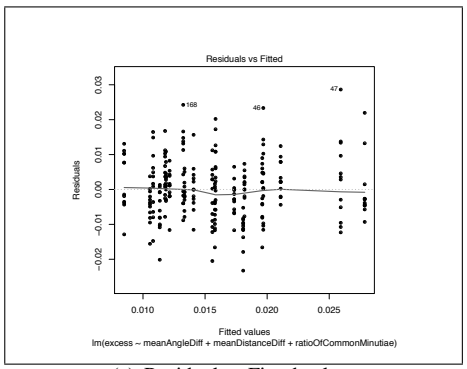
The result are shown in Table 3 and Figure 4. The residual error have an almost normal distribution which along with very small p-values suggest that all three factors are quite significant.

Table 3: Linear fit parameter of equation 8

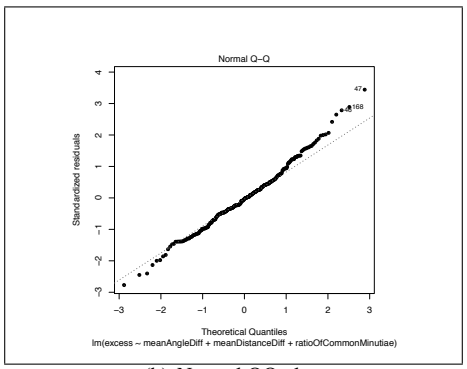
Coefficients	Estimate	Std. Error	t value	$Pr(>\|t\|)$
Intercept α	5.481968	0.600207	9.133	$< 2e-16$
mean angular difference β_3	-5.441200	0.597892	-9.101	$< 2e-16$
mean misplacement β_2	-0.013793	0.002778	-4.966	$1.28e-06$
fraction of overlapped minutia β_1	-0.033737	0.006147	-5.488	$1.00e-07$

6.2 Effect of minutia selection (or detection strategy) occurrence densities

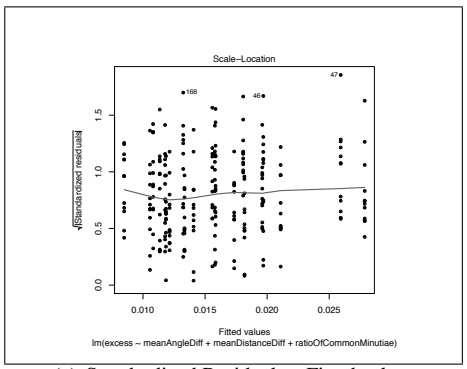
Consider a corpus of N single finger images collected in an operational scenario in which the right index finger of N subjects is stored as a greylevel raster of a fixed size. Suppose further that we apply a minutiae detection algorithm to each of those images and save the result as an INCITS 378 minutiae record. We then compute a two-dimensional histogram



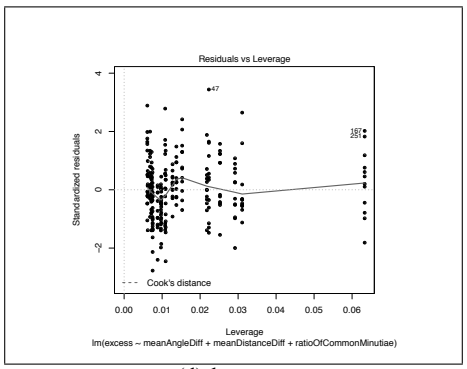
(a) Residual vs Fitted value



(b) Normal QQ plot

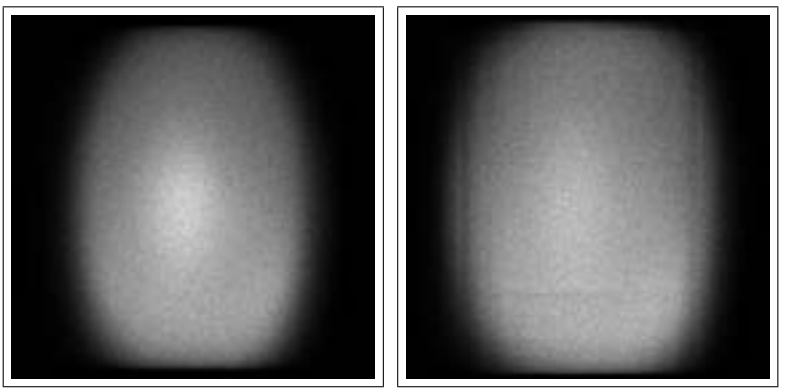


(c) Standardized Residual vs Fitted value



(d) leverage

Figure 4: Diagnosis plots of the linear fit of eq. 8. The almost normal distribution of residual error indicates that the loss of performance could mostly be explained by the three factors: fraction of overlapped minutiae, mean minutiae misplacement and mean angular difference of overlapped minutiae.



(a) Narrow (b) Wide

Figure 5: Examples of two-dimensional Minutiae Placement Density Functions.

of (x, y) location of minutia

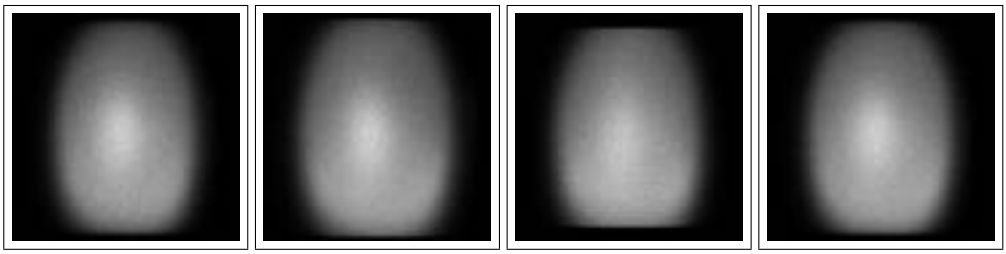
$$P(x, y) = \sum_{i=1}^{N} \sum_{k=1}^{K_i} \delta(x - x_{ik}, y - y_{ik}) \tag{9}$$

where the function $\delta_{ik}(x, y) = 1$ if and only if the k-th minutia of the i-th template is placed at position (x, y), and is zero otherwise.

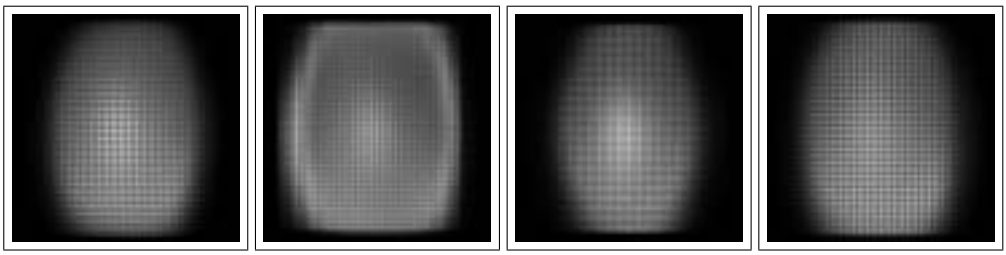
We computed such functions for the minutia extraction algorithms submitted to the MINEX evaluation, using a database of 368 by 368 optically acquired right index finger images from N = 183525 subject. We observed a median of $K = 38$ minutiae per record. Note that the input templates were not transformed in any way (by registration of the core, for example). The image population was not sampled by any factor (such as sex, quality, or image class), and the angle and type information for each minutiae was ignored.

The intent of this analysis was to discern whether some implementations exhibit regional preferences in how they find minutiae, for example whether some template generators center-weight while others weight in the periphery. Indeed such diversity is apparent in the images of Figure 5 which are min-max linearly scaled versions of the $P(x, y)$ estimates (eq. 9). Note that the template generator of Fig. 5(a) finds minutiae in a narrower region than that in Fig. 5(b). One notable caveat here is that these are systemic aggregated results and that for any given image (including perhaps the difficult-to-match ones) the behaviour of the two minutiae extractors may be very similar.

A second, unexpected, finding of this computation is that almost half of the MINEX minutiae extractors exhibit a periodic structure in their respective $P(x, y)$. Some of these are shown in the second row of Figure 6. Why this occurs is not known, except perhaps to the algorithm developers. One possible explanation would be the periodicity arises as an artifact of a Fourier transform operation applied to tiles across the image. Such an



(a) Smooth PDF



(b) Periodic structure in PDF

Figure 6: Examples of 2D Minutiae Placement Density Functions. In the top row the figures show more or less expected form; In the second row the minutiae densities exhibit a variety of periodic patterns. The order of appearance here does not correspond to the alphabetic ordering used in the MINEX report.

approach would not necessarily have to be incorrectly implemented because the periodicity would be a natural, and unintended, consequence of the operation.

The presence of fine grained periodic structure in a two-dimensional histogram such as Figure 6 is inconsistent with the expected smoothly varying form. Indeed it indicates that minutiae are not being placed in the natural locations. Obviously, this minutia misplacement adversly affects interoperability because higher performing template generators of the MINEX test do not exhibit such pattern. Furthermore, minutia extractor algorithms that exhibit such behavior are *probably* not conformant to the INCITS 378-2004 standard. We say probably and not definitely because in principle, a generator could chose to either preferentially include minutiae that actually fall on the grid, or preferentially exclude those that don't. In both cases, the result would be as shown in Figure 6. If such a strategy was implemented correctly then a conclusion of non-conformance with INCITS 378-2004 is incorrect. Note, however, there seems to be no good reason to implement such schemes as this would naturally reduce the number of minutiae.

7 Conclusion

The variation in minutiae selection and placement by different vendors is correlated with degraded interoperability. The 2D minutiae occurrence density functions (Figure 6) suggest that INCITS 378-2004 minutiae template generation is idiosyncratic. Specifically the periodic grid patterns indicate that the encoder is tending to quantize minutiae location, and so departing from the requirements of the standard. The exact behavior is different for each encoder, and is absent completely in some others. Such interoperability issues could be resolved by semantic conformance test which tests how faithful reported minutiae are to the underlying ground truth. Future studies include applying other methods such as generalized linear mixed model to quantify the effect of minutia placement and selection as well as advancing semantic testing methodologies.

References

[Ame08] American National Standard. ANSI-INCITS 378 Fingerprint Minutia Format for Data Interchange, August 2008.

[Com] Computer Security Division - NIST. Federal Information Processing Standards Publication 201 Personal Identity Verification for Federal Employees and Contractors.

[G+04] Patrick Grother et al. Minutiae Interoperability Exchange Test 2004 (MINEX04) API Specification, December 2004.

[G+06] Patrick Grother et al. MINEX Performance and Interoperability of the INCITS 378 Fingerprint Template, NISTIR 7296, April 2006.

[Int05] Geneva International Labour Organization. Seafarers' Identity Documents Biometric Testing Campaign Report, 2005.

[JTC05] JTC1 SC37 Working Group 5. ISO/IEC 19795 Biometric Performance Testing and Reporting: Part 1 - Principles and Framework, August 2005.

[JTC08] JTC1 SC37 Working Group 3. International Standard ISO/IEC 19794-2 Information Technology - Biometric Data Interchange Formats - Part 2: Finger minutia data, August 2008.

[McC04] R. Michael McCabe. *Automatic Fingerprint Recognition Systems*. Springer, New York, 2004.

[MN07] R Michael McCabe and Elaine M Newton. Data format for the interchange of fingerprint, facial and other biometric information - part 1, April 2007.

[oBUUdM06] Biometric System Laboratory (University of Bologna), Pattern Recognition Image Processing Laboratory (Michigan State University), Biometric Test Center (San Jose State University), and Biometrics Research Lab ATVS (Universidad Autonoma de Madrid). Fingerprint Vendor Competition, March 2006.

[TG04] Elham Tabassi and Patrick Grother. Quality Summarization - Recommendations on Biometric Quality Summarization across the Application Domain NISTIR 7422, August 2004.

[tsa08] TSA Registered Traveler Security, Privacy and Compliance Standard for Sponsoring Entities and Service Providers, January 2008.

[TW05] Elham Tabassi and Charles Wilson. A Novel Approach to Fingerprint Image Quality. In *Proc. IEEE ICIP'05*, volume 2, pages 37–40, Genova, Italy, September 2005.

[TWW04] Elham Tabassi, Charlse L. Wilson, and Craig I. Watson. NIST Fingerprint Image Quality NISTIR 7151, August 2004.

[UK 06] UK National Physics Laboratory. Minutia Template Interoperability Testing, June 2006.

[W+08] Craig I Watson et al. NIST Proprietary fingerprint template (PFT) Testing, May 2008.

[WH+04] Charles L. Wilson, Austin Hicklin, et al. Fingerprint Vendor Technology Evaluation NISTIR 7123, June 2004.

Semantic Conformance Testing Methodology for Finger Minutiae Data

Dana Lodrova[1], Christoph Busch[2,3], Elham Tabassi[4],
Wolfgang Krodel[5], Martin Drahansky[1]

1 - Brno University of Technology - Faculty of Information Technology, CZ
2 - Hochschule Darmstadt - CASED, DE
3 - Gjøvik University College - NISlab, NO
4 - National Institute of Standards and Technology, US
5 – Bundeskriminalamt - ZD23/AFIS, DE

email: ilodrova@fit.vutbr.cz

Abstract: This paper proposes a methodology to measure the semantic conformance rate of standardized biometric minutia interchange records. The paper proposes a fingerprint modality specific assertion test. A conformance test based on this methodology can attest for a given algorithm or software under test that the generated minutiae templates are a faithful representation of the input signal (i.e. fingerprint image). The test methodology is based on ground truth data that has been composed by dactyloscopic experts. As individual experts assessment yields slightly diverging coordinates a clustering algorithm is proposed that merges a set of manually placed minutia into one ground truth data set. The methodology is evaluated on ten-print fingerprint images and the NIST baseline minutia extraction algorithm.

1 Introduction

Many large scale biometric systems require compact storage of biometric references. The reference should represent a biometric characteristic and be compliant to an interoperable standardized format. The reference should be a faithful representation of a biometric characteristic (e.g. fingerprint). Also since for enrolment and verification different feature extraction algorithms could be used, it is necessary that a biometric reference is an interoperable representation of the biometric characteristic and therefore compliant to an interoperable standardized format. For fingerprint recognition systems the compact coding of minutia data provides interoperability among systems, where the reference is stored in tokens with limited storage capacity [iso05]. Examples for such systems are the European Citizen Card [ecc07] or the U.S. PIV Card [nist07]. The essential features of a fingerprint minutia template are locations, type (ridge endings and ridge bifurcations) and directions. This data is the relevant information for almost every fingerprint comparison subsystem.

As different vendors apply different concepts and algorithms to identify minutiae locations, directions and types, automatically generated minutiae are scattered around the truth (real) minutiae data. That means, in order to achieve sufficient interoperability and acceptable overall performance among different implementations, conformance testing is an essential process. ISO/IEC FDIS 29109-1 has categorized conformance testing into three levels [iso09a]. Level 1 focuses on basic data field testing. Level 2 is a syntactic test and inspects whether the data fields are filled with meaningful values [iso09b]. Level 3, however, is a semantic test, which inspects whether a generated interchange record is a faithful representation of the initial biometric data (e.g. fingerprint image) [bus09]. Level 3 conformance test is important because without accurate representation of biometric data, desirable interoperability and performance could not be achieved.
In this paper we focus on Level 3 conformance testing for finger minutia data. The basic idea of our method was presented in [bus09]. This paper contains an extension of the proposed method and augments new methodology for clustering of minutiae, which is required for the computation of conformance rates. Furthermore we describe an implementation and present preliminary results.
This paper is organized as follows. The second section describes challenges associated with minutiae detection. In section 3 we propose a methodology for computation of semantic conformance rates. The fourth section describes a clustering algorithm needed to merge ground truth data provided by multiple experts. Conclusion remarks and future work are in section 6.

2 Challenges associated with minutia detection

When minutia extractors are applied to a fingerprint images the following three situations can occur that may cause a challenge for the comparison subsystem:

Imprecisely placed minutiae
Imprecise detection of a minutia may be associated with:

- inaccurate minutia position
  (some distance can be tolerated),
- false minutia type,
- inaccurate minutia direction
  (some delta angle can be tolerated),
- wrong (different) minutia quality [1]

Probably the most frequent defect is the wrong minutia type (see Fig. 1). Ridge ending is detected as ridge bifurcation or vice versa, mostly because of noise around this minutia or due variations of the papillary line grey value. On the other side, some vendors intentionally do not set the type of minutiae properly.

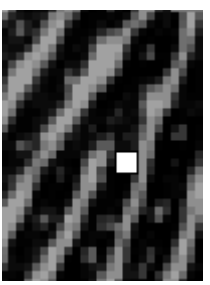


Fig. 1: Wrong minutia type: ridge bifurcation detected as ridge ending (square).

Problematic minutia detection inside the fingerprint area
Automatically detected minutiae can be in a number of problematic locations:

[1] In the absence of a standardized quality algorithm – investigation of minutia quality is not considered in this work.

- scars,
- “papillary dots”,
- dirt or hair glued on finger,
- skin diseases (for example eczema or tubercle),
- bent skin,
- written text or drawings inside the fingerprint area.

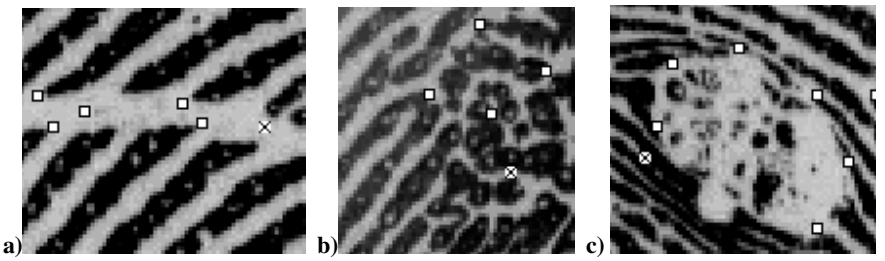


Fig. 2: Minutiae detected in problematic locations in the fingerprint area: a) bent skin, b) papillary dots, c) tubercle, (square: ridge ending, cross: ridge bifurcation, extractor: NIST mindtct).

Problematic minutiae detection outside the fingerprint area or at the borders

Some minutiae extraction algorithms detect minutiae at the border of the fingerprint area or even outside. This is a consequence of improper foreground/background masking and can be caused by dirt and drawings or characters in the background. Fig. 3a shows one false minutia (ridge ending) in the background noise and a further false minutia (ridge bifurcation) in some background drawing (present in the scanned ten-print card)

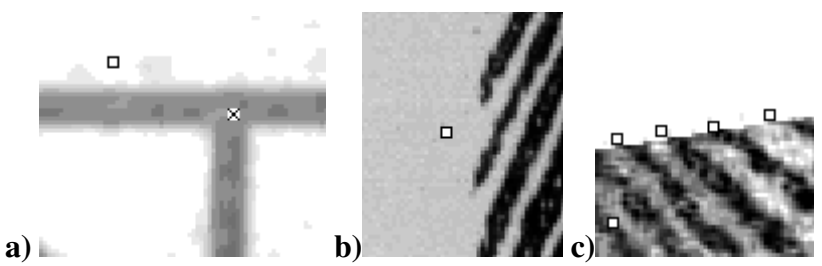


Fig. 3: Minutiae detected: a) outside the fingerprint area or b), c) at the borders.

3 Semantic conformance testing methodology

In order to determine whether or not a minutia extractor is conformant to some ground truth, we propose three conformance rates[2]. The ground-truth minutiae (GTM) placements, as explained in section 4, are the cluster center of various manual expert minutiae placements.

[2] Conformance can be stated, if the conformance test yields a conformance rate above a defined threshold.

The first rate cr_{gtm} indicates to which extent automatically placed minutia are located in the vicinity of the ground truth. If no automatically generated minutia (AGM) is found within the tolerance limits of a ground truth minutia (GTM), the minutia conformance score is valued 0. Otherwise the *i*-th minutia specific score mcs_i yields some value in the range [0, …, 1], where a cost-factor (punishment) *p* represent other defects. The conformance rate is given by

$$cr_{gtm} = \frac{\sum_{i=1}^{ngtm} mcs_i}{ngtm} \tag{3.1}$$

where *ngtm* is the number of minutiae (GTM) in the ground truth database. The minutia conformance score is given by:

$$mcs = \begin{cases} 0 & if\ d \geq tol_d \\ 1-p & otherwise \end{cases}, \quad tol_d = \frac{W}{4} \tag{3.2}$$

where *d* is the Euclidean distance between a GTM and the nearest AGM. *W* is the space between parallel skeletonized ridges. We intentionally chose tol_d to be W/4, since this is the maximal possible radius around a GTM, such that two neighbored GTM areas will not overlap each other. This situation is illustrated in Fig. 4.

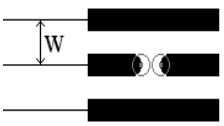


Fig. 4: Ridge space *W* and minutia tolerance

A punishment *p* reduces the *mcs* due to differences in the orientation or due to a different minutia type.

$$p = p_{\Delta\theta} + p_{\Delta t} \tag{3.3}$$

$$p_{\Delta\theta} = \frac{\left|\theta_{gtm} - \theta_{agm}\right| * 0{,}5}{\pi} \tag{3.4}$$

$$p_{\Delta t} = \begin{cases} 0{,}25 & if\ t_{gtm} \neq t_{agm} \\ 0 & otherwise \end{cases} \tag{3.5}$$

We intentionally chose different punishments for different deficiencies, as the impact on the observed biometric interoperability performance is strongest for the inaccuracies in minutia location, less relevant for the inaccuracies in minutia angle determination and least relevant for a diverting minutia type.

Frequently minutia extractors mislabel the minutia type, i.e. a ridge bifurcation is detected as ridge ending and vice versa. In this case not only the type is different, but also the delta $\Delta\Theta$ between angles might be close to π. We assume that it is not justified to punish one defect twice. Thus if we detect that one minutia is labeled as ridge ending and the other as ridge bifurcation, we automatically increase the angle of *agm* by π.

The second conformance rate is cr_{agm}, which describes the proportion of false minutiae wrongly placed outside or at the borders of the fingerprint area.

$$cr_{agm} = \frac{\sum_{i=1}^{nagm} mps_i}{nagm} \tag{3.6}$$

$$mps = \begin{cases} 0 & if\ agm\ is\ outside\ the\ fingerprint\ area \\ 0{,}5 & if\ agm\ is\ at\ the\ borderline \\ 1 & otherwise \end{cases} \tag{3.7}$$

where *nagm* is the number of AGMs.

The third conformance rate is cr_{amf}, which represents the automated extracted minutiae focus with respect to the fingerprint area. This can be understood as the proportion of minutiae inside the fingerprint area for which no mate was found in the set of GTMs:

$$cr_{amf} = 1 - \frac{niagm}{nagm} \tag{3.8}$$

In Eq. (3.8) *niagm* is the number of focused AGMs inside the fingerprint area, which does not correspond to any GTM.

4 Ground truth minutia data

Conformance testing based on the proposed methodology requires a ground truth database with a large set of minutiae.

4.1 Collecting of ground truth data

Fig. 5: GUI for dactyloscopic experts.

To collect the GTM database, we provide a graphical user interface for dactyloscopic experts (see screenshot in Fig. 5), which supports measuring of location, type, angle and quality in an image. Further information, e.g. on cores and deltas, pattern type and signal quality, is determined for future use.

Information set by experts is stored in an internal *.gtm file format. Its encoding scheme follows the ISO 19794-2 standard, where possible.

Example of *.gtm file format:

```
Width                    : 832 px
Height                   : 768 px
Fingerprint type         : R
Fingerprint quality      : 2
Fingerprint completeness: 1
```

```
Number of minutiae: 3
-------------------------------------------------------------
 id:  type,   x  ,   y  , angle, quality of minutiae
-------------------------------------------------------------
  0:     2,   527,   234,    81,   90
  1:     1,   452,   358,   104,   70
  2:     0,   360,   170,   187,   10

Number of cores    : 1
-------------------------------------------------------------------
 id:   x  ,   y  , quality of position, angle, quality of angle
-------------------------------------------------------------------
  0:   388,   165,                  90,   213,   70

Number of deltas   : 1
-----------------------------------------------------------
 id:   x  ,   y  , angle, angle, angle, quality of delta
-----------------------------------------------------------
  0:   342,   341,    66,   231,    66,   70
```

4.2 Clustering scattered data from experts

The minutia measurements by experts can be expected to be similar in many cases but will be scattered. Thus it is required to cluster the scattered data (individual *.gtm files from *n* contributing experts) and to compose the ground truth data as an input to our process, which generates conformance rates (see Fig. 6).

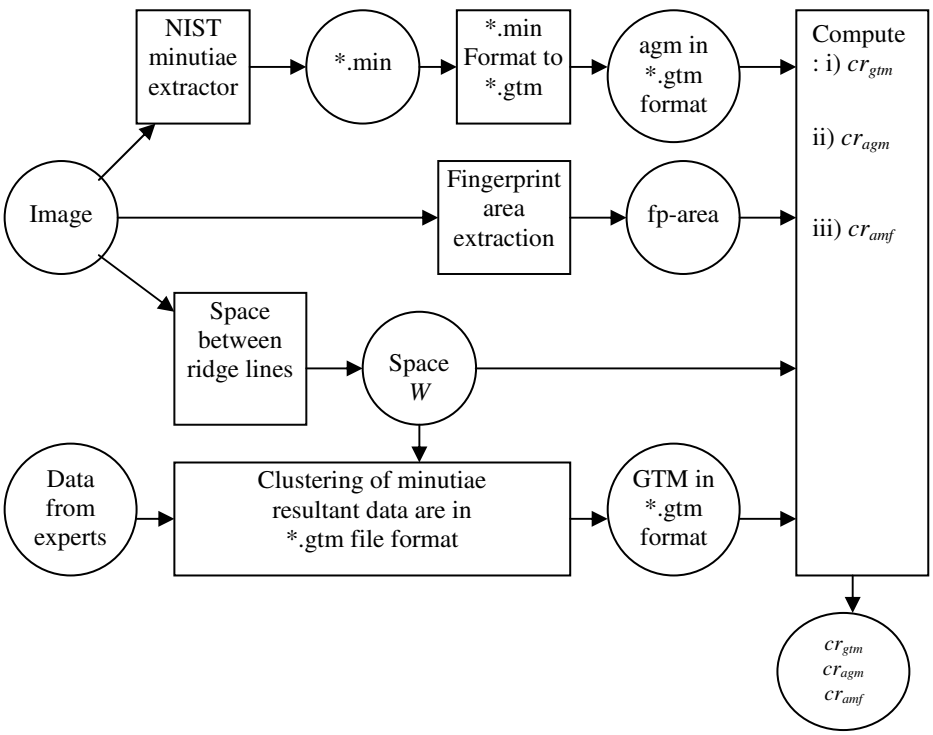


Fig. 6: Process workflow to determine conformance rates. For a sample evaluation the NIST mindtct minutiae extraction algorithm has been submitted to the conformance testing methodology. Circles represent files/values and squares represent software components.

The first processing step is to analyze cluster of minutiae *gtms* in an image where *gtms* are marked by different experts. Then we mark the fingerprint area of the image and compute space between ridges (*W*). The same image is also processed by the minutiae extraction algorithm under the test, in our case, the NIST mindtct algorithm [nbis] was used for illustration purposes. These information sources influence the resulting conformance rates.

The clustering algorithm that analyzes the minutia measurements from various experts and computes a ground truth minutia (GTM) as cluster center is a non-trivial task, as the target number of clusters is not known. To solve this task we propose a new algorithm, which is inspired by the Apriori algorithm [wk09] and by hierarchical clustering generally. At first, the *gtmi* data sets from *n* experts are stored into an array of minutiae (in this case a `struct` with values regarding position, angle, type, quality, expert ID and a Boolean marker "processed"/"not used"). Next we create an array of minutiae pairs. We create a pair from each two minutiae, if the following conditions are satisfied:

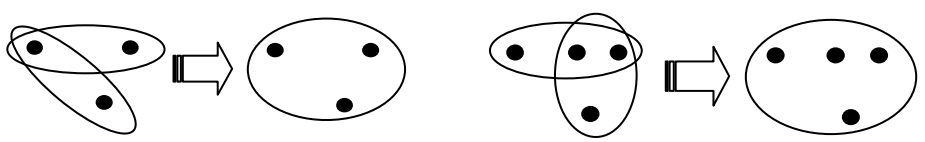
- Each minutia has been placed by a different expert
- The distance between minutiae is less or equal than *W*/2 (all minutiae will be inside a circle with radius *W*/4)

When we are creating a pair of two minutiae, we mark both minutiae as processed and then insert a newly created pair to the array of pairs only if such pair is not already included in the set.

Then we similarly create an array of triplets. We create a triplet from all pairs of minutiae pairs (created in the previous step), which satisfy the following conditions:

- Minutiae pairs have **one** identical (joint) minutiae
- Each minutia in a new **triplet** candidate has been placed by a different expert
- The distance of all minutiae pairs from new **triplet** candidate is less or equal than *W*/2 (all minutiae will be inside a circle with radius *W*/4)

Thus we have added the first condition and require that the minutia pairs have one identical minutia that will establish the link for the triplet creation (see Fig. 7a).



a) **b)**

Fig. 7: Minutiae clustering: a) creation of triplet from two pairs, b) creation of quadruples.

The process step for creation of quadruples is almost identical:

- Minutiae triplets have **two** identical (joint) minutiae (see Fig. 7b)
- Each minutia in a new **quadruple** candidate has been placed by a different expert.
- The distance of all minutiae triplets from the new **quadruple** candidate is less or equal than *W*/2 (all minutiae will be inside a circle with radius *W*/4).

Then we continue the creation of *n*-tuples until *n* is equal to the number of experts (*nexp)*.

In order to determine each cluster center it is necessary to compute an average minutiae position in the cluster, as well and an average angle and type. There are two possible methods to derive the average minutia positions, which implement a straightforward sum

$$X_{GTM} = \frac{\sum_{i=1}^{ngtm} x_i}{ngtm},\ Y_{GTM} = \frac{\sum_{i=1}^{ngtm} y_i}{ngtm} \tag{4.1}$$

and a minimum / maximum approach, as given in Eq. (4.2).

$$X_{GTM} = \frac{\min(x) + \max(x)}{2},\ Y_{GTM} = \frac{\min(y) + \max(y)}{2} \tag{4.2}$$

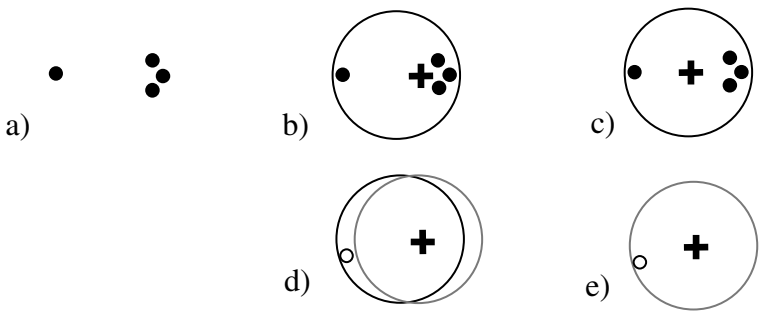


Fig. 8: Comparison of two methods for computation of the cluster center. Eq. 4.1 is in parts b) and d), eq. 4.2 in parts c) and e). Black dots are minutiae from experts; crosses are computed centers of cluster and white dots are tested agm.

The impact of the two methods is illustrated in Fig.8. As one can see, the first method shows stronger robustness w.r.t. outliers. As only one expert measured the minutia to be on the left side and the other three experts opted for the right side, the cluster center will tentatively be located on the right hand side. The advantage of this choice is that the ground truth data will show stronger robustness and reliability, while at the same time the risk that an automated generated minutia will be rejected corresponds to the likelihood that the minority opinion eventually represents the ultimate truth. However we have chosen the first averaging method since experts are only human beings, their hands can shake or they might be distracted while measuring the minutia position.

In the same line it is necessary to compute the average minutia type. We assign a ground truth minutia type if more than 2/3 of the experts vote for one type and we can state consensus[3]. Otherwise the minutia type is set to UNKNOWN and punishment for wrong minutia type can not be used.

[3] According to ISO directives a majority of 2/3 in a ballot manifests consensus.

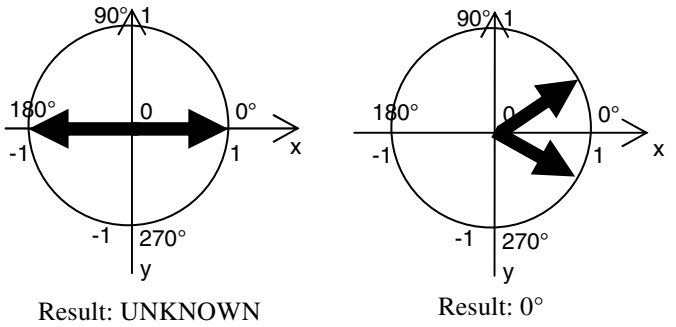


Fig. 9: Computation of average angle.

The computation of the mean direction requires an additional consideration. It might happen that one expert measures a specific minutia direction to be 180° while a second expert measures the same direction with 0°. Furthermore there might be a situation, in which three experts conclude in three completely different opinions (e.g. 0°, 120° and 240°). In such a case it is appropriate to set the ground truth direction to UNKNOWN. We compute an average direction by first converting all angles to directional vectors with length 1. Thus each endpoint (x_m and y_m coordinates) is located on the unit circle. Next we compute the mean $\underline{x}$ and $\underline{y}$ coordinate and take them as endpoint of the resultant direction vector, which might have a length smaller 1. If the resultant vector's length is less than 1/3, then the resultant direction will be UNKNOWN, otherwise we just convert resultant vector into a ground truth direction. We also set the direction to UNKNOWN in such cases, where the minutia type is UNKNOWN, as we consider a consensus regarding the minutia type to be a precondition for a reliable ground truth minutia direction.

4.3 Reliability of clusters

For the computation of the conformance rates of equations (3.1) – (3.8) it is essential to consider the reliability of each GTM. Such GTM reliability in turn depends on the quality of a cluster that created the GTM. The quality of a cluster is impacted by two factors. On one hand the number of experts that detected the minutia. If an image has been processed by 20 experts and only two of them have found this concrete minutia (and maybe those attributed a low minutia quality), then we cannot consider the mean minutia to be reliable. On the other hand if the concrete minutia is detected by 18 experts (and maybe all of them attributed a good minutia quality) then we can consider cluster center to be a reliable GTM. In order to distinguish unreliable minutia from reliable minutia we consider the quality of a cluster as defined in equation (4.3):

$$quality\ of\ \ cluster = \frac{\sum_{i=1}^{ncl} q_i}{nexp},\ quality\ of\ \ cluster \in \langle 0-100 \rangle \tag{4.3}$$

where q_i is the minutia quality of the i-th minutia in the cluster, *ncl* is the number of minutia in that cluster and *nexp* is number of experts processing this image. For example if all experts detected this minutia with minutia quality 50, then the quality of this cluster is 50. This is the same result as if this concrete minutia would be detected only by half of the experts but with minutia quality 100.

5 Methodology evaluation

For evaluation purposes, we used 17 images from NIST SD14, SD29 database, which were processed by 11 experts from the German Federal Criminal Police Office (BKA). The average space between parallel ridge lines and the fingerprint area were computed manually.

In Fig. 10 you can see the example of measured minutiae from experts mapped into the original image. Squares are ridge endings and triangles are minutiae of type "other". As you can see, the experts are quite consistent in their measurement (minutia placement and types), but there are still some problematic cases (e.g. two minutiae of "other" type in the top/left corner of the image).

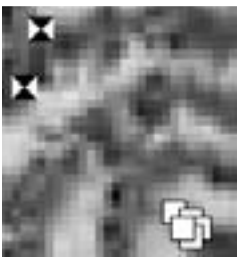


Fig. 10: Minutiae positions and types (8 experts; squares are ridge endings, symbol of two bl;ack triangles indicate minutia of "other" type).

One possible problems is e.g. a very short ridge line (dot). Some experts mark the beginning and end (two ridge endings) of this short ridge line and other experts mark the center of the dot specified the minutia type "other". Other problem can be e.g. minutiae, where experts cannot decide if there are ridge endings or bifurcations.

Finally we can see in Fig. 11 the results of the clustering algorithm – the cluster centers. The shape of minutiae has the same meaning as in the figures. The clustering method is very reliable in cases where experts' opinions are consistent.

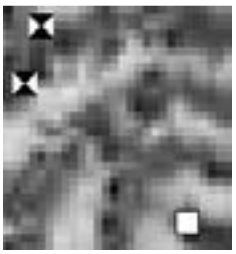


Fig. 11: Location and minutia type of cluster centers (squares are ridge endings, symbol of two bl;ack triangles indicate minutia of "other" type).

If experts are not consistent in their opinions and measured minutia locations are spread more widely, then it happens that instead of one cluster center there are two or even more of them. In order to limit the ground truth database to just the most reliable minutiae it was necessary to decide, which threshold value should be used for the "quality of cluster". On the one hand it is not reasonable to keep a cluster that has been created from only one expert's opinion if we have a large number of experts. On the other hand, the threshold value should not be too high, such that there will be too few clusters and eventually the conformance rate would be computed on very few GTMs.

In order to identify a suitable threshold for the quality of clusters, we compute all conformance rates for all images for threshold values between 0 and 50. Next we compute average values and their standard deviations (see Fig. 12). As a threshold value we choose the value, where both conformance rates (cr_{gtm} and cr_{amf}) have the same value. Thus for this sample data set the threshold value was chosen as 37. All computed conformance rates can be found in Tab. 1.

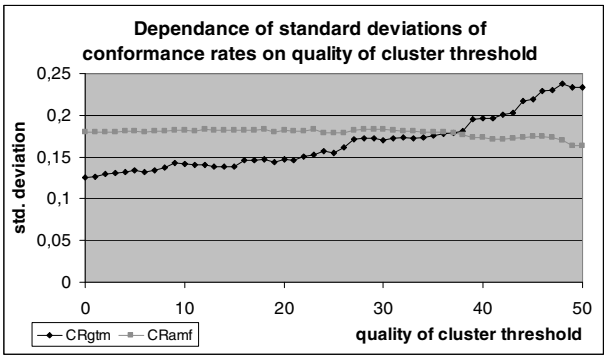


Fig. 12: Standard deviation of conformance rates vs. quality of cluster threshold.

Tab. 1: Results for the chosen threshold of cluster quality (37) .

	cr_{gtm}	cr_{agm}	cr_{amf}	*ngtm*	*nagm*
average	0,353	0,885	0,662	59	100
std. deviation	0,179	0,066	0,178		

Fig. 13 shows cluster centers, i.e. ground truth minutiae (*gtms*) that pass the quality threshold of 37. Previously figured problems have been resolved, because the problematic cluster centers, which caused these problems, are not included because they did not pass the cluster quality of 37.

One possibly problematic situation remains. For some minutiae there is more than one cluster center. In this case the AGM can belong to one of such clusters or all of them and this can have an influence on the cr_{gtm} conformance rate. Theoretically it can happen that also two ridge endings will be vis-à-vis and the minutiae from experts will be set so that the resultant clusters will partly overlap each other. If the AGM will be placed so that it can belong to both of them, this would be a greater problem than the previous situation.

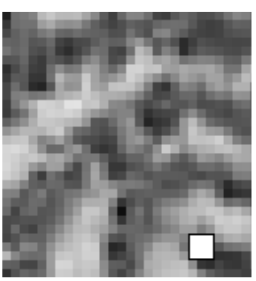


Fig. 13: Positions and types of cluster centers, which pass the quality threshold 37.

As a solution of this problem we propose to try clustering of clusters and then set the rule that one AGM can belong to one cluster only. This will of course be the cluster where AGM has the lower punishment.

6 Conclusion and future work

In this paper we have proposed a methodology for Level 3 Conformance Testing for finger minutiae data. We have also implemented the proposed method and the preliminary evaluation is yielding promising results. For illustrative purposes we have conducted a conformance test for the NIST mindtct algorithm. The preliminary tests show that this methodology works well; nevertheless more extensive tests with several 100 images will be conducted in the near future. However there are still a number of open issues, which need to be addressed in future research: i) inclusion of a conformance rate for cores and deltas in the methodology, ii) quality controlled semi-automated definition of the fingerprint area, iii) quality controlled semi-automated definition of the average space between the ridge lines in an the image, iv) determination and validation of thresholds for every conformance rate such that minutiae extractor will be conformant only if the extractor exceeds all thresholds and v) validation of the clustering of clusters or clustering approach in accordance with the minutiae type.

7 Acknowledgement

We thank all the forensic experts at BKA that devoted their time to generate the ground truth database and thus make this work possible.

References

[bus09] C. Busch, D. Lodrova, E. Tabassi, W. Krodel: Semantic Conformance Testing for Finger Minutiae Data, Proceedings of IEEE IWSCN 2009, Trondheim, pp. 17-23, ISBN 978-82-997105-1-0, May 2009.

[ecc07] CEN TC 224 WG15 Identification card systems: European Citizen Card, 2007.

[iso05] International Standards ISO/IEC IS 19794-2: Information technology – Biometric data interchange formats – Part 2: Finger minutiae data, 2005.

[iso09a] International Standards ISO/IEC FDIS 29109-1 Information Technology - Conformance Testing Methodology for Biometric Interchange Formats defined in ISO/IEC 19794 – Part 1: Generalized Conformance Testing Methodology, Feb. 2009.

[iso09b] International Standards ISO/IEC FCD 29109-1 Information Technology - Conformance Testing Methodology for Biometric Interchange Formats defined in ISO/IEC 19794 – Part 2: Finger minutiae data, Feb. 2009.

[nist07] National Institute of Standards and Technology: Biometric Data Specification for Personal Identity Verification, NIST Special Publication 800-76-1, 2007, http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf.

[wk09] http://en.wikipedia.org/wiki/Apriori_algorithm. Last visited July 2009.

[nbis] NIST Biometric Image Software http://fingerprint.nist.gov/NBIS/index.html.

The Fuzzy Vault for Fingerprints is Vulnerable to Brute Force Attack

Preda Mihăilescu, Axel Munk, and Benjamin Tams*
University of Göttingen
preda@uni-math.gwdg.de, munk@math.uni-goettingen.de,
btams@math.uni-goettingen.de

Abstract: The *fuzzy vault* approach is one of the best studied and well accepted ideas for binding cryptographic security into biometric authentication. We present in this paper a brute force attack which improves on the one described by T. Charles Clancy et. al. in 2003 in an implementation of the vault for fingerprints. Based on this attack, we show that three implementations of the fingerprint vault are vulnerable and show that the vulnerability cannot be avoided by mere parameter selection in the actual frame of the protocol. We will report about our experiences with an implementation of such an attack. We also give several suggestions which can improve the fingerprint vault to become a cryptographically secure algorithm. In particular, we introduce the idea of *fuzzy vault with quiz* which draws upon information resources unused by the current version of the vault. This may bring important security improvements and can be adapted to the other biometric applications of the vault.

1 Introduction

Secure communication relies on trustable authentication. The most wide spread authentication methods still use passwords and pass-phrases as a first step towards identity proving. Secure pass-phrases are hard to remember, and the modern user needs a large amount of dynamic passwords for her security. This limitation has been known for a long time and it can in part be compensated by the use of chip cards as universal access tokens.

Biometrical identification, on the other hand, is based on the physical identity of a person, rather then by their control of a token. Reliable biometric authentication would thus put an end to password insecurity, various repudiation disputes and many more shortcomings of phrase or token based identities. Unlike the deterministic keys which are common for cryptography, biometric data are only reproducible within vaguely controlled error bounds, they are prone to various physical distortions and have quite a low entropy.

Overcoming the disadvantages of the two worlds by using their mutual advantages is an important concern. We look back over almost a decade in which the biometrics community developed an increasing concern for the security and privacy of biometrical systems. It is not the purpose of this technical note to clarify the interesting notions and attempts which

*corresponding author, supported by Graduiertenkolleg 1023 *Identification in mathematical models* of **DFG**

were developed in this context. For this purpose, we refer to the survey [UMP+04] of Uludag et. al. on biometric cryptosystems.

Researchers from cryptography and coding theory attempted to develop new concepts allowing to model and evaluate, from an information theoretical point of view, algorithms which deal with the specific restraints of biometrics: non-uniformly distributed data with incomplete reproducibility and low, hard to estimate, entropy. Both communities are motivated by the wish to handle biometrics like a classical password, thus protecting it by some variant of one-time functions and performing the verification in the image space. Unlike passwords, the biometrics are not deterministic. This generates substantial challenges for the verification after one-time function transforms. Juels and Wattenberg [JW99] and then Juels and Sudan [JS02] have developed, namely the *fuzzy commitments* and *fuzzy vault*, two related approaches with a strong impact on biometric security. The papers of Dodis et. al. [DORS08, BDK+05] can be consulted for further theoretic developments of the concepts of Juels et. al. and their formalisation in an information theoretic framework. It is inherent to the problem that core concepts of the theory, such as the entropy of a biometric template, are hard even to estimate. Thus the security proofs provided by the theory do not translate directly in practical estimates or indications.

In 2003, Clancy, Kiyavash and Lin gave [CKL03] a statistically supported analysis for a realistic implementation of the vault for fingerprints. The authors observe from the start that the possible parameter choices in this context are quite narrow in order to allow sufficient security; they succeed to define a set of parameters which they claim provides the cryptographically acceptable security of $O(2^{69})$ operations for an attack. Our analysis shows that faster attacks are possible in the given frame, thus making brute force possible. The analyses in [CKL03] are outstanding and have been used directly or indirectly in subsequent papers; the good security was obtained at the price of quite a high error probability ($20\% - 30\%$). In [UPJ05, Ulu06], Uludag, Pakanti and Jain provided an implementation of the fuzzy vault for fingerprints which uses alignment help-data and was applied to the fingerprints from the FVC2002 database [MMC+02]. This improves the identification rate; however some of the simplifications they make with respect to [CKL03] reduce security quite dramatically, and the ideas of these authors could very well be combined with the more conservative security approach of Clancy et. al.. Yang and Verbauwhede [YV05] describe an implementation of the vault, with no alignment help, which follows closely the concepts of [CKL03] and focusses upon adapting to various template qualities and numbers of minutiae recognised in these templates.

This paper is not to be understood as a proof of weakness of the fuzzy vault scheme, in its abstract setting. At the contrary, one needs not to change biometrics or go to more costly multibiometrics to make the current version of fuzzy vault secure. We argue that multi-finger biometrics are more than sufficient in this respect.

In this paper, which extends an earlier unpublished one [Mih07], we describe the original fuzzy vault in Section 2 and argue that the security proofs and remarks given in [JS02] are not useful for fingerprint applications. In Section 3, we discuss the various implementations mentioned above and show that essentially brute force attacks can be performed in feasible time in all instances. In Section 4, we will report about our experiences with an implementation of an attack based on these considerations. Afterwards, in Section 5 we

discuss possible variants and alternatives and suggest some additional sources of information which might render the fuzzy vault secure in connection with fingerprint application.

The ideas of fuzzy vaults and commitments are of great importance in biometric security. While their information theoretic foundation [JW99, JS02, DORS08, BDK+05] is well set and understood, the core problem of estimating entropies brings their biometric application at the borderline between skills and science. A *minima moralia* in this case requires a realistic evaluation of simple attacks, like a well conceived brute force attack. The estimate of a brute force attack to a system is an irrefutable *upper bound* for the security of that system; if that bound shows to be too low, concerns and improvements are called for. Moreover, using only some statistics of minutiae locations in various images of the same fingerprint, it proves that pushing parameters to the extremes cannot suffice for gaining secure fuzzy vaults for single fingerprints, without bringing some new ideas in play. In this respect, we do not claim novelty to this result. Therefore, we present also a new idea, which we call *fuzzy vault with quiz*, that is likely to highly increase security, even in the case of one finger identification. The idea is very simple and will be presented in the specific context of fingerprints; conceivably, it may also be regarded as a generalization of the general concepts in fuzzy schemes and commitments. In this paper, we simply give an example of quiz and support its validity by an implementation.

This paper concentrates on fingerprints, for two reasons: first, there is a considerable amount of research concerning the application of fuzzy vaults or fuzzy-vault-inspired hash variants to fingerprint security. Second, the patterns of vulnerability and possible improvements can be discussed more accurately on a single biometrics. The interested reader may find observations which can be applied to other biometrics and also to multibiometrics.

2 The Fuzzy Vault

The *fuzzy vault* is an algorithm for hiding a secret string S in such that a user who is in possession of some additional information T can easily recover S, but an intruder should face computationally infeasible problems in order to achieve this goal. The information T can be fuzzy, in the sense that the secret S is locked by some related, but not identical data T'. Juels and Sudan define the vault in quite general terms and allow multiple applications. Biometry is one of them and we shall restrict our description directly to the setting of fingerprints. Generalizations can be found in [JS02, DORS08, BDK+05].

The string is prepared for the transmission in the vault as follows. Let $S \in \{0,1\}^*$ be a secret string of l bits length. The user (Alice, say) that wishes to be identified by the string S has her finger scanned and a *locking set* $\mathcal{L}$ comprising the carthesian coordinates of t minutiae in the finger scan is selected from this finger template T'; the couples of coordinates are concatenated to single numbers $X_i = (x_i||y_i) \in \mathcal{L}$. One selects a finite field $\mathbb{F}_q$ attached to the vault and lets $k' + 1 = \lceil \frac{l}{\log_2(q)} \rceil$ be the number of elements in $\mathbb{F}_q$ necessary to encode S. One assumes that $0 < \max_{X \in \mathcal{L}} X < q$ and maps $X \hookrightarrow \mathbb{F}_q$ by some convention. Selecting $f(X) \in \mathbb{F}_q[X]$ to be a polynomial of degree $k \geq k'$ with coefficients which encode S in some predetermined way, one builds the *genuine* set $\mathcal{G} =$

$\mathcal{G}(\mathbb{F}_q, S, t, k, \mathcal{L}) = \{(X_i, Y_i) \ : \ X_i \in \mathcal{L}; Y_i = f(X_i)\}$, which encodes the information on S. The genuine verifier Bob has an original template T of Alice's finger and should use this information in order to recover $f(X)$ and then S. In order to make an intruder's (Victor's, say) attempt to recover S computationally hard, the genuine set is mixed with a large set of *chaff* points $\mathcal{C} = \{ \ (U_j, W_j) \ : \ j = 1, 2, \ldots, r - t\}$, with $U_j \notin \mathcal{L}$ and $W_j \neq f(U_j)$; the chaff points should be random uniformly distributed. chaff points and genuine lists are shuffled to a common vault with parameters $\mathcal{V} = \mathcal{V}(k, t, r, \mathbb{F}_q) = \mathcal{G} \cup \mathcal{C}$.

Upon reception, Bob will generate an *unlocking* set $\mathcal{U}$ containing those X_i coordinates of vault points, which well approximate coordinates of minutiae in T. This templates must have negligible nonlinear distortions and be aligned modulo affine transforms. The second condition is addressed in [Ulu06]. The unlocking set may be erronated either by allowing some chaff points which are closer to T' than locking points, or by simple coordinate imprecision. Both problems can be dealt within given limits of error correcting codes. Thus Juels and Sudan suggest using Reed Solomon codes for decoding $f(X)$.

The security argumentation in [JS02] is based upon the expectation that the chaff points will build an important amount of subsets of t elements, whose coordinates are interpolated by polynomials of degree k, thus hiding $f(X)$ from Victor among these random polynomials. The argument is backed up by the following lemma, a proof of which can be found in [JS02, CKL03].

Lemma 1. *For every $\mu, \ 0 < \mu < 1$ and every vault $\mathcal{V}(k, t, r, \mathbb{F}_q)$, there are at least $\frac{\mu}{3} \cdot q^{k-t} \cdot (r/t)^t$ random polynomials $g \in \mathbb{F}_q[X]$ such that $\mathcal{V}$ contains t couples $(U_j, g(U_j))$.*

2.1 A brute force attack

If Victor intercepts a vault $\mathcal{V} = \mathcal{V}(k, t, r, \mathbb{F}_q)$, but has no additional information about the location of minutiae or some of their statistics, he may still try to recover S by brute force trials. For this, he needs to find by random trials $k + 1$ points in the genuine list $\mathcal{G}$. The chances that $k + 1$ points of the vault are also in the genuine list are:

$$1/\mathbf{P} = \frac{\binom{r}{k+1}}{\binom{t}{k+1}} \sim (r/t)^{k+1} < 1.1 \cdot (r/t)^{k+1}, \quad \text{for} \quad r > t > 5. \tag{1}$$

This, together with the fact that the odds for a point $(X, Y) \in \mathbb{F}_q^2$ to lay on the graph of a given polynomial $f \in \mathbb{F}_q[X]$ are equal to the probability $P[Y = f(X)] = 1/q$ yield the ground for the proof of Lemma 1. Lagrange interpolation of a polynomial of degree k can be done in $O(k \log^2(k))$ operations [JvzG03]; checking whether an additional point (U, W) lays on the graph of $f(X)$ (so $W = f(U)$) requires $O(k)$ steps, so $K = O(\log^2(k))$ such verifications can be done at the cost of one interpolation.

We assume now with Clancy et. al., that there is a degree $k < D < t$ which is minimal with the property that among all polynomials $g \in \mathbb{F}_q[X]$ of degree k which interpolate vault points, $f(X)$ is the only one interpolating at least D points. This yields a criterion for identifying f.

Lemma 2. *Let $\mathcal{V} = \mathcal{V}(k, t, r, \mathbb{F}_q)$ be a fuzzy fingerprint vault and $k < D < t$ be chosen as above. Then an intruder having intercepted $\mathcal{V}$ can recover the secret S in $R = C \cdot (r/t)^{k+1}$ operations, where $C < 8rk$.*

Proof. We have shown that in less then $< 1.1 \cdot (r/t)^{k+1}$ trials, Victor can find a set of $k+1$ points from the locking set $\mathcal{L}$. In order to find such a set and then S, for each $(k+1)$-tuple $\mathcal{T} = (X_i, Y_i)_{i=0}^{k} \subset \mathcal{V}$ Victor has to

1. Compute the interpolating polynomial $g_{\mathcal{T}}(X)$. It is proved in [JvzG03] that the implicit constant for Lagrange interpolation is 6.5; let $K = 6.5 \cdot \log^2(k)$. Thus all interpolation polynomials require $< 7.2 \cdot k \log^2(k) \cdot (r/t)^{k+1}$ operations.

2. Search a point $(U, W) \in \mathcal{V} \setminus \mathcal{T}$ such that $g(U) = W$. This requires the equivalent of r/K Lagrange interpolations. If no point is found, then discard $\mathcal{T}$.

3. If $\mathcal{T}$ was not discarded, search for a further point verifying $g(U) = W$. This step is met with probability $1/q$. If a point is found, add it to $\mathcal{T}$; otherwise discard $\mathcal{T}$.

4. Proceed until a break condition is encountered (no more points on the graph of $g(X)$) or D points have been found in $\mathcal{T}$.

Adding up the numbers of operations required by the steps 1-4., with weights given by the probabilities of occurrence, one finds:

$$R < 7.2 \cdot (r/t)^{k+1} \cdot k \cdot K \cdot \frac{rq}{K(q-1)} < 8.0 \cdot (rk) \cdot (r/t)^{k+1},$$

as claimed. Note in particular that the bound does not depend on D, since this value is absorbed in the sum of the series $\sum(1/q)^i$, of probabilities to successfully add i point to $\mathcal{T}$. □

Here are some remarks on factors that influence the complexity of the brute force attack.

Restricting the region of interest from which Victor chooses points is irrelevant, if minutiae are assumed to be uniformly distributed over the template. In this case, r and t are scaled by the same factor and thus r/t and the complexity of brute force remain unchanged.

The complexity grows with the degree k of the polynomial $f(X)$. However, high degrees k require large unlocking sets, which may not be possible for average quality fingerprints and scanners. Thus one can only augment the degree to an extent to which it is not (too much) increase the work required for unlocking by Bob.

The complexity grows with the number of chaff points. There is a bound to this number, given by the size of the image on the one side and the variance in the minutiae location between various data capturings and extractions [CKL03]. Clancy and his co-authors find empirically the lower bound $d \geq 10$ for the distance between chaff points, and this distance was essentially respected also by the subsequent works.

The complexity grows while reducing t. This is however also detrimental for genuine unlocking, since it may reduce the size of the unlocking set below the required minimum.

What can be inferred about the security of fingerprint vaults from the seminal paper [JS02]? First, one observes that Juels and Sudan suggest to use error correcting codes, thus avoiding explicit indications to whether an interpolation polynomial is the correct $f(X)$. Uludag and Jain suggest on the other hand in [Ulu06] the use of CRC codes: thus S is padded by a CRC code, adding 1 to the degree k' needed to encode S. Upon decoding, Bob can check the CRC and ascertain that he found the correct secret. This simplifies the unlocking procedure. Does it bring advantages to Victor? If the degree $k > k'$ and thus the CRC does not increase additionally the polynomial degree, Victor has a gain of $O(8 \cdot r/\log^2(k))$, as follows from Lemma 2. Otherwise, there is no gain.

It is made clear in the Chapters 4 and 5 of [JS02] that the amount of chaff points is essential for security. The suggested minimum lays about $r \sim 10^4$. For fingerprints, a large amount of chaff points decreases the average distance between these (and also genuine points) in the list. The value $r = 10^4$ leads to an average distance of $2 - 5$ pixels between the point coordinates, depending on the resolution of the original image. This is below realistic limits as mentioned above. At this distance, even in presence of a perfect alignment, the genuine verifier Bob should need some additional information (like CRC or other) providing the confirmation of the correct secret. Such a confirmation is contrary to the security lines on which Juels and Sudan make there evaluation. There is an apparent conflict between the general security proofs in [JS02] and realistic applications of the fuzzy vault to fingerprints. In [JS02] the authors explicitly warn that *applications involving privacy-protected matching* cannot achieve sufficient security. It is not clear, whether fingerprint matching is considered in [JS02] as belonging to this category.

3 Implementations Of The Fingerprint Vault

We start with the most in depth analysis of security parameters for the fingerprint vault, which was done by Clancy and co-authors in [CKL03]. The paper focusses on applications to key release on smart cards. They suggest using multiple scans in order to obtain, by correlation, more reliable locking sets. As mentioned above, the variance of minutiae locations which they observed in the process leads to defining a minimum distance between chaff (and genuine) points, which is necessary for correct unlocking. This minimal distance $d \sim 11$ implies an upper bound for the size r of the vault and thus the number of chaff points!

The authors use very interesting arguments on packing densities and argue that in order to preserve the randomness of chaff points, these cannot have maximal packing density. On the other hand, assuming that the intruder has access to a sequence of vaults associated to the same fingerprint and he can align the data of these vaults, then the randomness of chaff points allows a correlation attack for finding the genuine minutiae. This argument suggests rather using perfectly regular high density chaff point packing. These are hexagonal grids with mutual distance d between the points. The genuine minutiae can be rounded to grid points, and Victor will have no inference point for distinguishing these from the chaff points. We shall comment below on this point.

The implementation documented in this paper suggests the following parameters for optimal security: $k = 14, D = 17, t = 38, r = 313$. The brute force attack in Lemma 2 is more efficient then the one of Theorem 1 of [CKL03], on which they base their security estimates. Using the above parameters and Lemma 2, we find an attack complexity of $\sim 2^{55}$; comparing this to the complexity of genuine unlocking yields a security factor $F \sim 2^{49}$ which is below cryptographic security, unlike the 2^{69} deduced in [CKL03]. By the very balanced arguments used in the parameter choice, the security bounds obtained on base of this paper are an indication of the vulnerability of the fingerprint vault in general.

Yang and Verbauwhede describe in [YV05] an implementation of the vault, in which the degree of the polynomials $f(X)$ varies in dependence of the size t of the genuine list, which itself depends directly on template quality. From the point of view of security, the paper can be considered as a follow up of [CKL03], which addresses the problem of poor image quality with its consequences for the size of the locking set. Secret sizes and polynomial degrees are adapted to the size of locking sets. The proposal is consistent, its vulnerability to attacks is comparable to [CKL03] in general, and higher, when adapting to poor image quality.

The major contributions of Uludag and Jain in [Ulu06] is to provide a useful set of *helper data* for easing image alignment. This has an important impact on the identification rate. As mentioned above, they bring the elegant and simple proposal of adding a CRC to the secret, thus easying the unlocking work. We discussed above the issue of the security risk increasment: this is arguably small, below a factor of 2^8. On the other hand, the degree of $k = 8$ for the polynomial $f(X)$ and vault size $r = 224$, whilst $t = 24$, makes their system more vulnerable, with an absolute attack complexity of $\sim 2^{37}$.

4 Attacking Fuzzy Fingerprint Vaults

In this section, we will report about our experiences with attacks on fingerprint vaults. Before coming to data we describe how we proceeded in implementing our attack.

4.1 Implementation of our attack

Before we implemented the attack a working en- and decryption should have been available for us. Its implementations essentially requires operations in a finite field. Therefore we worked with Victor Shoups *Number Theory Library* (`NTL`) [Sho09]. Furthermore, we strictly used finite fields of characteristic 2 for this gives canonical conventions for identifying finite field elements with positive integers (bitwise).

Our encryption implementation requires the degree k of the polynomial f, the number t of points to be extracted from a fingerprint template, the fingerprint template, and the size r the vault will have. In this first version, the template simply is taken from a list of minutiae locations. For a minutia location (x, y) the concatenation $(x\|y) = x + 2^{16} \cdot y$ is computed where we implicitly assume that x and y fit into 2 byte length integers. As

already mentioned in section 2 the size $q = 2^m$ is chosen so that for all minutia locations of the template (x, y) the inequality $(x\|y) < q$ holds. Similar, given the secret $S \in \{0,1\}^*$ of l bits length the size q fulfils $k > \left\lceil \frac{l}{\log_2(q)} \right\rceil$. Using NTLs functionalities a defining polynomial $P(X) \in \mathbb{F}_2[X]$ of a finite field $\mathbb{F}_q$, $q = 2^m$, is built and then the secret S is identified with its corresponding polynomial $f \in \mathbb{F}_q[X]$ of degree k. If α is a root of P and $(x\|y) = \sum_{i=0}^{m-1} x_i 2^i$ is given in its binary representation the vault point (X, Y) is obtained from this by setting $X = \sum_{i=0}^{m-1} x_i \alpha^i$ and $Y = f(X)$. In this way the locking set is constructed. The chaff points are generated by generating locations (x, y) having a reasonable distances to genuine minutiae locations and then, as above, X is computed but $Y \in \mathbb{F}_q$ is generated at random such that (X, Y) does not lie on the polynomial graph. In such a way the vault $\mathcal{V}$ is obtained. If $(X, Y) \in \mathcal{V}$ is a point of the vault then, as above, there are unique integers x, y corresponding to X and Y, respectively. By this, a partial order is given on the vault points. Thus, in its representation the array of vault points is sorted w.r.t. this order such that no one is able to distinguish genuine points from chaff points just using knowledge about how genuine points are dispersed in the vault (e.g. appended or pushed in front).

Next, the implementation of the decryption was done ignoring the alignment modulo affine transform for this does not affect the attack. Given a list of minutiae locations our implementation simply extracts those vault points (after deconcatiations of their X-coordinate into (x, y)) which well approximate template locations. Using the Peterson-Berlekamp-Massey algorithm as suggested in [JS02] one succeeds in recovering the polynomial $f \in \mathbb{F}_q[X]$ if at least $\frac{k+t}{2}$ of extracted vault points are also genuine points.

In such a way we implemented a working protocol of fuzzy vault for fingerprints.

Thereafter, the implementation of the attack as in subsection 2.1 was done analogue. The attack requires the vault data and a process id number giving a seed such that parallel running processes will interpolate different polynomials from a randomly chosen sequence of $(k + 1)$-tuple of vault points.

4.2 Running brute force attacks

Each attack against our fingerprint vaults were done on a 4 multiprocessor `Quad-Core AMD Opteron(tm) Processor 8347 HE` with 1.9 GHz and 32GB RAM using 8 processes in parallel.

A first attack we ran was against a vault consisting of $r = 224$ points hiding a polynomial of degree $k = 8$ interpolating $t = 24$ vault points. Thus, for the probability $\mathbf{P}$ for a single trial to lead to the desired polynomial fulfilled $\lfloor 1/\mathbf{P} \rfloor = 2\,542\,897\,440$. These are the same security parameters as in [Ulu06]. Due to our implementation of the protocol the size of the finite field in which our operations took place was 2^{25} contrary to 2^{16} in [Ulu06]. We started 8 processes in parallel. All processes together interpolated and tested 11347 polynomials per second of CPU time whether they interpolate t vault points. Hence, we expected the whole attack to succeed in discovering the polynomial after 1 day 7 hours 7

minutes and 33 seconds of CPU time. Lucky as we were it in fact succeeded after 1 hour and 58 seconds of CPU time.

Another vault with same security parameters as before but a finite field of size 2^{108} this time (due to a larger bit length of the encrypted secret) was attacked. This time the attack interpolated and tested 17123 polynomials a second of CPU time. This let us expect to succeed in discovering the polynomial after 20 hours 37 minutes and 34 seconds of CPU time. The attack was successful after 10 hours 55 minutes and 8 seconds of CPU time. One may wonder why in this larger field relatively more operations can be performed. This may be due to tuning details of `NTL`.

We also started a brute force attack against a vault having optimal security parameter as suggested by this paper. Thus, $r = 313$, $t = 38$ and $k = 14$. In fact we did not succeed in breaking such a vault but do a few calculations out of our experiences. The probability **P** that a randomly selected $(k+1)$-tuple leads to the hidden polynomial fulfils $\lfloor 1/\mathbf{P} \rfloor = 953\ 116\ 315\ 773\ 448$. We interpolated and tested 8124 polynomials a second of CPU time. Thus, we expect to succeed in discovering the polynomial after more than 1860 years. Modern supercomputers thus are able to break such a vault within a feasible amount of time.

5 Security Discussion

We discuss in this section several variants for improving security of the fingerprint vault.

5.1 Using more fingers

We have shown that the parameters r, t, k, allowing to control the security factor, are naturally bounded by image size, variance of minutiae location and average number of reliable minutiae. They cannot thus be modified beyond certain bounds and it is likely that this bounds have been very well derived in [CKL03]. It lays thus at hand to propose using for instance the imprints of two fingers rather then only one, for creating the vault. This way the parameters can be virtually doubled, yielding to a literal squaring of the security factor.

5.2 Non - random chaff points

As mentioned above, it is argued in [CKL03] that chaff points should have random distribution; this leads to halving the packing density. However, one can embrace the opposite attitude, consisting in laying a hexagonal grid of size $d = 11$, proposed by the authors. Each grid point will be attached to some vault point - chaff or genuine. Thus Victor will have no means for distinguishing between chaff points and genuine ones, despite of the regularity of the grid. Thanks to the error correcting codes, the genuine points can always

be displaced by a distance at most $d/2$ to a grid point. It is the packing density which, according to the results in [CKL03] doubles, thus doubling the vault size r. It is thus conceivable that this strategy may also improve the security of the vault. Nevertheless, the consequences need still be analysed.

5.3 Quizes using additional minutiae information

There is more information in a minutia than its mere coordinates. Such are for instance the orientation, lengths and curvatures of incoming lines, neighbouring data, etc.. We propose to attach to each minutia a quiz which can be solved in robust manner by Bob, but which introduces for Victor several (say b) bits of incertainty per minutia. Thus for polynomial degree k, the security may be increased by a factor of 2^{kb}.

We give in the case of the orientation a simple example of how a quiz functions. This, in fact, was added by us to the implementation we reported in Section 4. Let X be the concatenated coordinates of a fixed minutia and let α be its orientation, in a granularity of π/n, for some small integer n. Then, along with $(X, f(X))$, the vault will also contain a random value β instead of α: thus the minutia is represented by (X, Y, β). Upon reception, Bob computes the integer $0 \leq j < n$ such that $j\frac{\pi}{n} = \alpha - \beta \bmod \pi$. The value of j will then encode a certain transformation $Y' = T(Y)$ of the received value Y and in fact the interpolating value will be set to be $Y' = f(X)$. Note that the vault creator has control on the generation of β and it may be chosen such that the value of j can be safely recovered (thus $\alpha - \beta$ is bounded away from a multiple of π/n). For chaff points, β is random.

In our implementation, the transformation given by j was chosen as a kind of shift of Y. If θ is a root of a defining polynomial of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ then any $Y \in \mathbb{F}_{2^m}$ can be written as $Y = \sum_{i=0}^{m-1} y_i\theta^i$. The value j then defines $T(Y) = \sum_{i=0}^{m-1} y_{r(i,j)}\theta^i$, where $r(i,j) = i + j \bmod n$. Its inverse is then given by $T^{-1}(Y) = \sum_{i=0}^{m-1} y_{r(i,-j)}\theta^i$.

Several robust additional informations may as well increase the security of the fingerprint vault to a cryptographically acceptable level.

5.4 The alternative of cryptographic security

These observations lead to the question: is the use of one-way functions and template hiding an intrinsic security constraint, or just one in many conceivable approaches to securing biometric authentication? The second is the case, and it is perfectly feasible to construct a secure biometric authentication system based on the mechanisms used by state of the art certification authorities. Basically, the scanners of the biometric system need to:

1. Have enclosed, temper proof, cryptographic units.
2. Encrypt templates immediately after the image generation.
3. Build up secure channels to the matching servers, using challenge response mecha-

nisms.

4. Create distinguished templates e.g. by endowing them with time stamps, scanner credentials and signature.

On the server side, template databases should be encrypted and the matching be performed in secure, temper proof environments. These requirements are quite general and must be fulfilled in cryptographically secure environments, so adding them to a biometric system is possible. Note that the template is transmitted in encrypted form *and* is event-bound. Only upon verification of signature, credentials and time stamps will the verification proceed with the template matching. If the cryptographic verification fails, no subsequent action is taken: in particular, *a compromised template is not sufficient to break the system* . At the contrary, in order to use a fake template, one needs to gain control upon the scanner and force its credentials and signatures upon a stolen template: this is assumed to be hard. This eliminates the stringent and possibly unachievable condition to protect the templates as if their revelation would compromise their usage in any system at any ulterior time.

6 Conclusions

It has been attempted to achieve security in biometric application either by using one-way functions adapted to the specifics of biometric data, or by direct application of strong cryptographic techniques. We showed that one of the leading methods of the first category, the fuzzy vault, allows a simple attack to its instantiation for fingerprint data [CKL03, UPJ05, Ulu06, YV05].

The attack described and implemented is a brute force attack, the *worst case* for the attacker, and thus the best case for the genuine user. It is an indication of the security limitation of the current applications of the fuzzy vault to fingerprints. The attack can definitely be improved. E.g., by using some meet in the middle strategy in the combinatorial search. More important, the upper bound in Lemma 2 was estimated on the assumption that the attacker does not distinguish the chaff points in his search. This is not realistic, since an intruder should use some statistics on the minutiae locations in a fingerprint to derive probabilities for points to be genuine ones. This would lead to a useful order of priorities in the brute force search described above; the result would be conceivably comparable to a reduction of the number of chaff points to less than a half! Note that the *helper data* proposed in [Ulu06] are in this case also a major help for the attacker.

It would be interesting to conduct such attacks in the future. However, considering that the upper bound found in this paper, together with these natural improvement strategies clearly show that security is insufficient, one may argue that the development and investigation of more secure alternatives to the present fuzzy vault implementation should have higher research priority. We have brought some suggestions which may help raising the security level of the fingerprint vault to cryptographically acceptable values.

One may argue that similar attacks could be possible to other related methods and thus cryptographic security is preferable, whenever it can be achieved or afforded. Subsequent work should consider variants of the one-way function ideas which could have higher secu-

rity, even if they do not meet the standards of cryptographic security. Also, cryptographic security can be achieved by in a wide scale of variants; analysing pros and cons of such variants is an open topic.

References

[BDK+05] Xavier Boyen, Yevgeniy Dodis, Jonathan Katz, Rafail Ostrovsky, and Adam Smith. Secure Remote Authentication Using Biometric Data. In *Advances in Cryptology—EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 147–163. Berlin: Springer-Verlag, 2005.

[CKL03] T. Charles Clancy, Negar Kiyavash, and Dennis J. Lin. Secure smartcard-based fingerprint authentication. In *WBMA '03: Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*, pages 45–52, New York, NY, USA, 2003. ACM Press.

[DORS08] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM J. Comput.*, 38(1):97–139, 2008.

[JS02] Ari Juels and Sudan. A Fuzzy Vault Scheme. In A. Lapidoth and E. Teletar, editors, *Proc. IEEE Int'l Symp. Information Theory*, page 408, 2002.

[JvzG03] Jürgen Gerhard Joachim von zur Gathen. *Modern Computer Algebra*. Cambridge University Press, Cambridge (UK), second edition, 2003.

[JW99] Ari Juels and Martin Wattenberg. A fuzzy commitment scheme. In *CCS '99: Proceedings of the 6th ACM conference on Computer and communications security*, pages 28–36, New York, NY, USA, 1999. ACM.

[Mih07] Preda Mihăilescu. The Fuzzy Vault for fingerprints is Vulnerable to Brute Force Attack. *CoRR*, abs/0708.2974, 2007.

[MMC+02] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, and A. K. Jain. FVC2002: Second Fingerprint Verification Competition. In *Proceedings of 16th International Conference on Pattern Recognition (ICPR2002), Quebec City*, pages 811–814, 2002.

[Sho09] Victor Shoup. NTL: A library for doing number theory, version `5.5.1`, 2009. available from `http://www.shoup.net/ntl/`.

[Ulu06] Umut Uludag. Securing fingerprint template: fuzzy vault with helper data. In *Proceedings of CVPR Workshop on Privacy Research In Vision*, page 163, 2006.

[UMP+04] Umut Uludag, Student Member, Sharath Pankanti, Anil K. Jain, Senior Member, Salil Prabhakar, Anil, and K. Jain. Biometric Cryptosystems: Issues and Challenges. In *Proceedings of the IEEE **Vol. 92, No. 6***, pages 948–960, 2004.

[UPJ05] Umut Uludag, Sharath Pankanti, and Anil K. Jain. Fuzzy vault for fingerprints. In *Proc. AVBPA, Lecture Notes in Computer Science 3546*, pages 310–319. Springer, 2005.

[YV05] S. Yang and I. Verbauwhede. Automatic secure fingerprint verification system based on fuzzy vault scheme. In *Proc. IEEE Int. Conference on Acoustics, Speech and Signal Processing*, pages 609–612, 2005.

Multi-Sample Fusion with Template Protection

E.J.C. Kelkboom and J. Breebaart
Philips Research, The Netherlands
{Emile.Kelkboom, Jeroen.Breebaart}@philips.com

R.N.J. Veldhuis
University of Twente, Fac. EEMCS, The Netherlands
R.N.J.Veldhuis@utwente.nl

X. Zhou and C. Busch
Fraunhofer Institute for Computer Graphics Research IGD, Germany
{Xuebing.Zhou, Christoph.Busch}@igd.fraunhofer.de

Abstract: The widespread use of biometrics and its increased popularity introduces privacy risks. In order to mitigate these risks, solutions such as the helper-data system, fuzzy vault, fuzzy extractors, and cancelable biometrics were introduced, also known as the field of template protection. Besides these developments, fusion of multiple sources of biometric information have shown to improve the verification performance of the biometric system. Our work consists of analyzing feature-level fusion in the context of the template protection framework using the helper-data system. We verify the results using the FRGC v2 database and two feature extraction algorithms.

1 Introduction

More applications are using biometrics ranging from simple home or business applications with a small and limited group of enrolled people (for example access control to buildings or rooms) to large-scale systems used by an entire nation or even the entire world (for example identity cards with biometrics or the electronic passport e-Passport). Unfortunately, its widespread use increases the related privacy risks such as identity theft or activity monitoring by cross-matching between biometric databases of different applications. However, the field of template protection provides the technology that enables the mitigation of these privacy risks by transforming the biometric template with a one-way operation in order to guarantee the irreversibility property and by randomizing the biometric template that guarantees that multiple protected templates from the same biometric sample cannot be linked to each other. In the literature, different types of technologies have been presented, for example the *Helper-Data Systems* (HDS) [KGK+07, KSA+05, TAK+05], *Fuzzy Vaults* [JS02, NJP07], *Fuzzy Extractors* [CR07, DRS04], and *Cancelable Biometrics* [RCCB07].

Besides the template protection developments, fusion of multiple sources of biometric information has shown to improve the verification performance of the biometric system. As

described in [RNJ06], the basic principle of fusion is the reconciliation of evidence presented by multiple sources of biometric information in order to enhance the classification performance. Furthermore, different sources of biometric information can be extracted from the same biometric modality by: (i) capturing a sample of multiple instances (left and right index fingerprint or iris) with the same sensor, (ii) using different types of sensors to acquire a different biometric sample from the same instance, (iii) capturing several samples using the same sensor and instance, and (iv) extracting dissimilar feature representations of the same biometric sample using different algorithms. These cases are referred to as the multi-instance, multi-sensor, multi-sample, and multi-algorithm systems, respectively. Furthermore, the fifth type is the multi-modal system, which is the fusion of sources of biometric information from multiple modalities, for example fingerprint, face, iris, voice, palm or retina. To complete the summary from [RNJ06], the sixth type is referred to as the hybrid system, which consists of a combination of the aforementioned fusion types. The most common implementations of multi-biometric systems address fusion at the feature-level, score-level or decision-level.

In the work of [NJ08], the Fuzzy Vault template protection system is used for applying multi-sample, multi-instance, and multi-modal fusion. In case of multi-sample fusion, they create a single mosaiced template from multiple fingerprint impressions from which they construct the vault. For multi-instance fusion they take the union of the minutiae sets of the left and right index fingers for constructing the vault. For multi-modal fusion, a fingerprint and a iris sample are combined by concatenating the unordered minutiae set with the transformed iriscode extracted from the fingerprint and iris samples, respectively. The vault is constructed using the concatenated unordered set. The verification performance has improved for all three cases as well as the claimed security.

Furthermore, the works of [KGK+07, KSA+05, LT03] based on the HDS template protection system inherently apply multi-sample fusion at feature-level by averaging the multiple enrolment samples. However, no arguments are provided for applying feature-level fusion instead of either score-level or decision-level.

Our work also consists of applying multi-sample fusion using the HDS, but we analyze the performance improvements of fusion at feature-, score-, and decision-level fusion. We use 3D face range images of the FRGC v2 dataset [PFS+05] and verify the performance improvement on two recognition algorithms.

The outline of this paper is as follows. In Section 2 we briefly discuss the HDS system, while in Section 3 we discuss the application of multi-sample fusion at feature-, score-, and decision-level using the HDS system together with the experimental setup and results. We finish with the conclusions in Section 4.

2 Template Protection Scheme

In the literature, many presented template protection schemes are based on the capability of generating a robust binary vector or key from biometric measurements of the same subject. This also holds for the HDS system we consider and is depicted in Figure 1. For the sake of

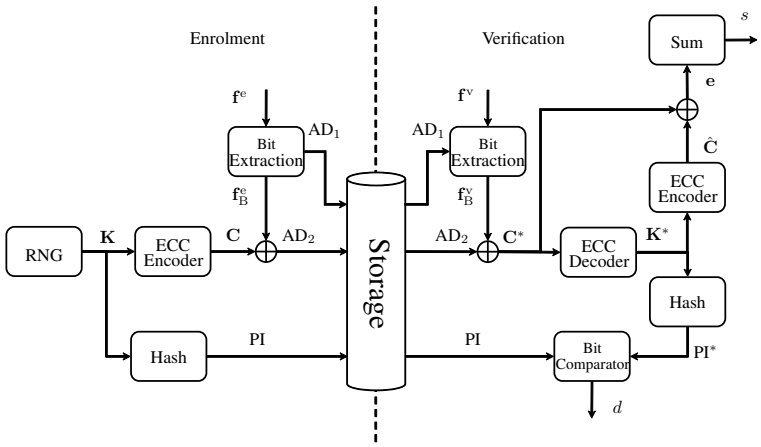


Figure 1: The HDS template protection scheme.

coherence we use the terminology *auxiliary data* (AD) and *pseudo identity* (PI) proposed in [BBGK08], which is in line with standardization activities in ISO [ISO09]. Within the *Bit Extraction* module, a binary vector $\mathbf{f}_{\mathrm{B}} \in \{0,1\}^{N_{\mathrm{B}}}$ is extracted from the real-valued representation of the biometric sample, $\mathbf{f} \in \mathbb{R}^{N_{\mathrm{F}}}$. We use a single bit quantization scheme based on thresholding and the *reliable component selection* (RCS) algorithm. We select the N_{B} most reliable components based on the estimated z-score of each component. With use of the multiple (N_{e}) enrolment samples, the z-score is estimated as the ratio between the distance of the estimated mean with respect to the quantization threshold and the estimated standard deviation, see [KGK$^+$07] for a more detailed description of the z-score estimation and the quantization scheme. The index information of the selected reliable components is stored as auxiliary data AD$_1$.

The binary vector $\mathbf{f}_{\mathrm{B}}^{\mathrm{e}}$ could be used as a key for any encryption purposes, however it is not considered as being practical because of the high probability that it is not exactly the same in both the enrolment and verification phase ($\mathbf{f}_{\mathrm{B}}^{\mathrm{e}} \neq \mathbf{f}_{\mathrm{B}}^{\mathrm{v}}$), due to measurement noise and biometric variability that lead to *bit errors*. The number of bit errors is also referred to as the Hamming distance $d_{\mathrm{H}}(\mathbf{f}_{\mathrm{B}}^{\mathrm{e}}, \mathbf{f}_{\mathrm{B}}^{\mathrm{v}})$. To deal with the bit errors, we use error-correcting codes (ECC). The combination of the ECC with a cryptographic hash function forms the scheme also known as the Fuzzy Commitment scheme [JW99]. In the enrolment phase, a binary secret or message vector $\mathbf{K} \in \{0,1\}^{k_{\mathrm{c}}}$ is randomly generated by the *Random-Number-Generator* (*RNG*) module. A codeword $\mathbf{C}$ of an error-correcting code is obtained by encoding $\mathbf{K}$ in the *ECC-Encoder* module. As the ECC we use the linear block type code "Bose, Ray-Chaudhuri, Hocquenghem" (BCH) [BRC60], which is specified by the codeword length (n_{c}), secret length (k_{c}), and the corresponding number of bits that can be corrected (t_{c}), in short $[n_{\mathrm{c}}, k_{\mathrm{c}}, t_{\mathrm{c}}]$. Some practical BCH settings are provided in Table 1, where the bit error rate (BER) is the ratio $t_{\mathrm{c}}/n_{\mathrm{c}}$. The codeword is XOR-ed with $\mathbf{f}_{\mathrm{B}}^{\mathrm{e}}$ in order to obtain auxiliary data AD$_2$. Hence, $\mathbf{f}_{\mathrm{B}}^{\mathrm{e}}$ should have the same dimension as $\mathbf{C}$, implying $N_{\mathrm{B}} = n_{\mathrm{c}}$. Furthermore, the hash of $\mathbf{K}$ is taken in order to obtain the pseudo identity PI. Under the assumption that the bits of $\mathbf{f}_{\mathrm{B}}$ are independent, from [TG] we can use the secret

size k_c as a measurement of the difficulty of guessing the enrollment binary vector $\mathbf{f}_B^e$ from the protected template $\{AD_1, AD_2, PI\}$, hence safeguarding the privacy. The larger the secret size the more difficult it is to either guess $\mathbf{f}_B^e$ or $\mathbf{K}$ from PI.

In the verification phase, a new biometric sample is taken and transformed into its binary representation within the *Bit Extraction* module with help of auxiliary data AD_1. The new word $\mathbf{C}^*$ is computed by XOR-ing $\mathbf{f}_B^v$ with AD_2, and for a genuine case it is expected that $\mathbf{C}^*$ is close to $\mathbf{C}$. The candidate secret $\mathbf{K}^*$ is obtained by decoding $\mathbf{C}^*$ in the *ECC-Decoder* module. Subsequently, the candidate pseudo identity PI^* is computed by hashing $\mathbf{K}^*$. The decision in the *Bit-Comparator* module is based on whether PI and PI^* are bitwise identical.

The *Bit-Comparator* module outputs a match as its decision d only if PI and PI^* are identical, which occurs when the number of bit errors between the binary vectors $\mathbf{f}_B^e$ and $\mathbf{f}_B^v$ is smaller or equal to the error-correcting capability t_c of the ECC. Thus, there is a match when the Hamming distance is smaller than t_c, $d_H(\mathbf{f}_B^e, \mathbf{f}_B^v) = ||\mathbf{f}_B^e \oplus \mathbf{f}_B^v||_1 \leq t_c$. Therefore, the fuzzy commitment scheme can be considered as a Hamming distance classifier with threshold t_c. Note, that the maximum number of bits that the BCH can correct t_c^* is close to 25% of the codeword length. In the remainder of the text, we indicate this limitation as the *ECC-limitation*.

As a distance score s we use the number of bits that had to be corrected by the ECC decoder. The candidate secret $\mathbf{K}^*$ is encoded to its corresponding codeword $\hat{\mathbf{C}}$ and is XOR-ed with $\mathbf{C}^*$ in order to obtain the error pattern $\mathbf{e}$. The error pattern is equal to the bit differences between the enrolment and verification binary feature vectors ($\mathbf{f}_B^e \oplus \mathbf{f}_B^v$) as follows

$$\begin{aligned} \mathbf{e} &= \hat{\mathbf{C}} \oplus \mathbf{C}^* \\ &= \hat{\mathbf{C}} \oplus (\mathbf{f}_B^v \oplus AD_2) \\ &= \hat{\mathbf{C}} \oplus (\mathbf{f}_B^v \oplus (\mathbf{f}_B^e \oplus \mathbf{C})) \\ &= (\hat{\mathbf{C}} \oplus \mathbf{C}) \oplus (\mathbf{f}_B^e \oplus \mathbf{f}_B^v) \\ &= (\mathbf{f}_B^e \oplus \mathbf{f}_B^v) \text{ if } \hat{\mathbf{C}} = \mathbf{C}, \end{aligned} \tag{1}$$

where $\hat{\mathbf{C}}$ is equal to $\mathbf{C}$ when there is a match, i.e. $\mathbf{K}$ and $\mathbf{K}^*$ are equal. The distance score s is thus the sum of the error pattern, hence equal to $d_H(\mathbf{f}_B^e, \mathbf{f}_B^v)$ and only a valid score when there is a match, i.e. $d_H(\mathbf{f}_B^e, \mathbf{f}_B^v) \leq t_c$. If the score is not valid we only know that $d_H(\mathbf{f}_B^e, \mathbf{f}_B^v) > t_c$.

Table 1: Some examples of the BCH code given by the codeword (n_c) and secret (k_c) length, the corresponding number of correctable bits (t_c), and the bit error rate (BER) t_c/n_c.

n_c	k_c	t_c	BER $= t_c/n_c$
127	8	31	24.4%
	15	27	21.3%
255	9	63	24.7%
	21	55	21.6%
511	10	127	24.9%
	31	109	21.3%

3 Experiments

In this section we present the methods for multi-sample fusion at feature-, score-, and decision-level and empirically validate the best performance achieved at each level by means of a biometric database and two feature extraction algorithms.

3.1 Experiment Setup

3.1.1 Biometric Databases

All the results in this work are obtained using the FRGC v2 dataset [PFS+05] containing a total of 4007 3D shape samples from 465 subjects.

However, one of the two 3D shape recognizers we used could not successfully extract a feature vector out of each sample, hence reducing the dataset to 3507 samples from 454 subjects. As the template protection algorithm works best at multiple enrolment samples, the subset of subjects with at least 6 (5 as enrolment samples with at least one for the verification) samples or more is created. This resulted into a subset of 261 subjects with in total 2970 samples.

3.1.2 Feature Extraction Algorithms

The first algorithm is the shape-based 3D face recognizer from [GIA06] and is referred to as Algo1. It has two main steps: 1) the alignment of faces, and 2) the extraction of surface features from 3D facial data. In the alignment step, each face is registered to a generic face model (GFM) and the central facial region is cropped. The GFM is computed by averaging correctly aligned images from a training set. After the alignment step, we can assume that all faces are transformed in such a way that they best fit the GFM, and have the same position in the common coordinate system.

After alignment, the facial surface is divided into 174 local regions. For each region, the maximum and minimum principal curvature direction are computed. Each of the two directions is presented by the azimuthal and the polar angle in the spherical coordinate system. Combining all the regions leads to a feature vector dimension $N_{\mathrm{F}} = 174 \times 2 \times 2 = 696$.

The second algorithm, Algo2, is a histogram-based feature extraction method. After the pre-registration of the face data, a frontal view of the face model is obtained, where the tip of the nose is at the origin in the Cartesian coordinate system. The distribution of depth values of the normalized face model describes the characteristics of an individual facial surface. In order to obtain more detailed information about the local geometry, the 3D model is divided into several sub areas which are orthogonal to the symmetry plane of the face. The features are extracted from the depth value distribution in each sub-area. The feature vector dimension is $N_{\mathrm{F}} = 476$. A full description of this algorithm is provided in [ZSBF08].

For both feature extraction algorithms, the raw feature vectors they produce are used as input of the template protection system as described in Section 2. Hence, no further signal processing is performed.

3.1.3 Testing Protocols

The performance testing protocol consists of randomly selecting 50% (130) subjects as the training set and the other subjects as the test set, this is referred to as the training-test-set split. The template protection system parameters such as the quantization thresholds, used within the *Bit Extraction* module, are estimated on this training set. Hereafter, the test set is randomly split into an equally sized fusion-training and evaluation set containing around 65 subjects each. All the training needed for fusion is thus performed on the fusion-training set and the reported performance is obtained from the evaluation set. From the evaluation set, 5 samples of each subject are randomly selected as the enrolment samples while the remaining samples are considered as the verification samples. This split is referred to as the enrolment-verification split. The protected template is generated using all the enrolment samples and compared with each verification sample.

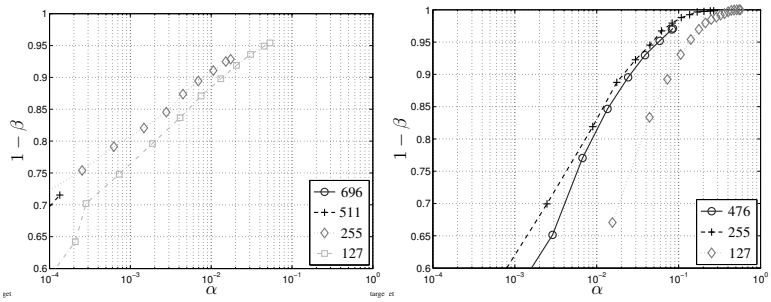
The training-test-set split is performed five times, while for each split the enrolment-verification split is performed five times. From each enrollment-verification split we measure the β_{tar} (the false non-match rate (FNMR, β) at the targeted false match rate (FMR, α) of $\alpha_{tar} = 0.25\%$) and the equal-error rate (EER), which is the error rate achieved at the operating point where both FNMR and FMR are equal. With use of the 25 measurements we estimate the 95% confidence interval (ci) defined as $ci = 1.96\sigma_{EER}/\sqrt{(25)}$ for the EER case while using $\sigma_{\beta_{tar}}$ for the β_{tar} case, respectively. Note, that the splits are performed randomly, however the seed at the start of the protocol is always the same, hence all the splits are equal for the performance tests at feature-, score-, and decision-level fusion. Hence, the splitting process does not contribute to any performance differences.

3.2 Experiment Results

3.2.1 Feature-level Fusion

Similar to the works [KGK$^+$07, KSA$^+$05, LT03], we average the $N_{\mathrm{e}} = 5$ enrolment samples before entering the template protection scheme. By averaging the samples the measurement noise and the biometric variability are suppressed. Hence there will be less bit-errors and the binary representation will be more robust.

The achieved performances for different n_{c} settings are portrayed by the ROC curves in Figure 2(a) and (b) for algorithms Algo1 and Algo2, respectively. Furthermore, the EER and β_{tar} details are given in Table 2. The table provides the ci for both EER and β_{tar} and their operating point provided as the relative Hamming distance (RHD). The right column of the table provides the effective secret size $|\mathbf{K}_f|$ of the template protection system at the specific fusion level. Because a single protected template is created at feature-level



(a) Algo1 (b) Algo2

Figure 2: ROC curves at feature-level fusion for different n_c settings for the (a) Algo1 and (b) Algo2 algorithm.

fusion, $|\mathbf{K}_f|$ is equal to k_c of the ECC. On the other hand, k_c is determined by the t_c setting that leads to a α close to the target α_{tar}, but smaller. This is exactly the ECC setting with a BER just larger than the operating point in RHD corresponding to β_{tar}. Entries in the table indicated with quotes cannot be reached in practice because of the ECC-limitation, however we are able to estimate them because of the Hamming distance classifier assumption as discussed in Section 2. Entries with "x" can neither be reached nor estimated.

Note that the ROC curves are limited because of the ECC-limitation. In order to reach larger α and smaller β values it is required to tolerate and thus correct more bit errors. However, the error correcting capability of an ECC is limited. From the results we can conclude that both algorithms perform optimally at a codeword size of $n_c = 255$. These settings are used in the score- and decision-level fusion analysis. Compared to the Algo2 algorithm, Algo1 has a better performance but a smaller secret size (see Table 2, right column).

Table 2: The EER and β_{tar}, and their ci and operating point for the individual algorithms Algo1 and Algo2 at different settings of n_c. The last column is the effective secret size $|\mathbf{K}_f|$ which is equal to the secret size k_c of the ECC at the operating point t_c for achieving α_{tar}.

n_c	*EER* [%]	*RHD* [%]	β_{tar} [%]	*RHD* [%]	$\lvert\mathbf{K}_f\rvert$ [bits]
Algo1					
696	"3.76 ± 0.25"	"38.8"	"16.13 ± 1.93"	"33.62"	x
511	"3.69 ± 0.30"	"35.2"	"15.19 ± 1.79"	"28.77"	x
255	"4.02 ± 0.41"	"27.5"	15.84 ± 2.10	19.61	21
127	4.88 ± 0.47	23.6	18.95 ± 2.01	14.96	29
Algo2					
476	5.44 ± 0.35	22.1	37.69 ± 3.14	11.76	x
255	5.06 ± 0.30	10.2	30.25 ± 2.88	1.96	215
127	8.92 ± 0.33	3.9	89.57 ± 1.20	0.00	120

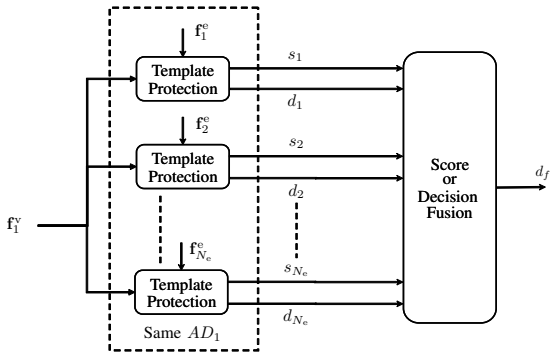
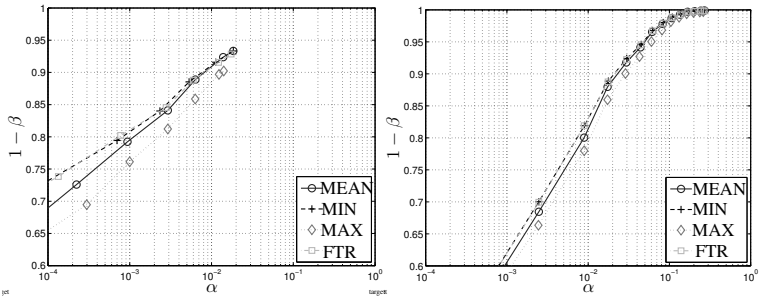


Figure 3: The general implementation of multi-sample fusion at score- or decision-level.

3.2.2 Score-Level Fusion

A general implementation of the template protection system at score- or decision-level fusion is depicted in Figure 3. A protected template is created for each of the N_{e} enrolment samples. Note that the RCS quantization scheme as discussed in Section 2 uses multiple enrolment samples in order to estimate the necessary statistics, hence we use all the N_{e} enrolment samples to determine the N_{B} most reliable components and is used as such in each N_{e} template protection systems portrayed in Figure 3. Within the *Score- or Decision-level Fusion* module the scores $\{s_1, s_2, \ldots, s_{N_{\mathrm{e}}}\}$ are combined into a single fused score s_f from which the decision d_f is taken based on a score threshold. Note that a score is valid only when there is a match from the corresponding template protection system and occurs when $s_i \leq t_{\mathrm{c}}$. Therefore we set the error-correcting capacity t_{c} to its maximum (t_{c}^*) in order to obtain a valid score for the largest range possible. Consequently, the secret size used for each of the N_{e} protected templates is equal to nine bits and does not depend on the score threshold. Hence, at score-level fusion the score threshold determines the operating point of the ROC curve and not the ECC setting. Combination methods such as the minimum (MIN), the maximum (MAX), and the mean (MEAN) of the scores are used in order to obtain s_f. For the MEAN method we take the mean of the valid scores only, while the MIN and MAX methods are based on all the scores. We take the maximum based on all the scores because if there is a single invalid score it should lead to a non-match. Furthermore, for each method, if all the scores are not valid it will automatically lead to a non-match.

The ROC curves at the optimal setting of $n_{\mathrm{c}} = 255$ are depicted in Figure 4 with the details in Table 3. As a comparison, we included the ROC curve obtained at feature-level fusion indicated as "FTR". Because it suffices to guess a single $\mathbf{f}_{\mathrm{B}}^{\mathrm{e}}$ from one of the N_{e} protected templates to breach your privacy, the effective secret size $|\mathbf{K}_f|$ of the template protection system at score-level fusion for each method is also nine bits. Consequently we have omitted them from the table. The results indicate that taking the MIN method leads to the best performance, however the difference is not significant when considering the ci. Furthermore, the MIN method ROC curve is very close to the ROC from feature-level fusion (FTR). Note that for the Algo1 algorithm it is not possible to estimate the EER for



(a) Algo1 (b) Algo2

Figure 4: ROC curves at score-level fusion compared to the feature-level (FTR) curves for the (a) Algo1 and (b) Algo2 algorithm.

Table 3: The EER and β_{tar}, and their ci and operating point for the score-level fusion experiments with $n_{\mathrm{c}} = 255$.

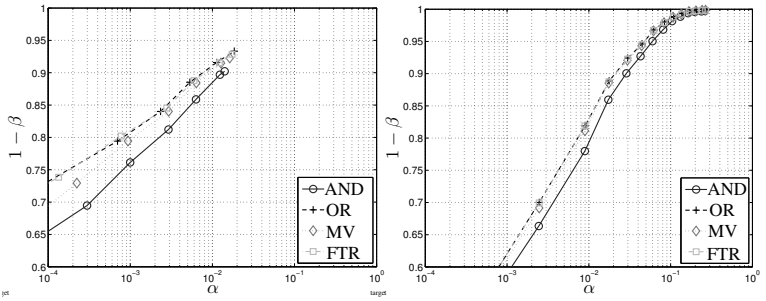
Method	*EER* [%]	*RHD* [%]	β_{tar} [%]	*RHD* [%]
Algo1, $n_{\mathrm{c}} = 255$				
MEAN	x	x	16.45 ± 2.08	20.00
MIN	x	x	15.74 ± 2.09	19.61
MAX	x	x	19.48 ± 2.08	20.39
Algo2, $n_{\mathrm{c}} = 255$				
MEAN	4.96 ± 0.28	10.6	31.46 ± 3.23	2.35
MIN	4.87 ± 0.30	10.2	29.90 ± 3.29	2.35
MAX	5.49 ± 0.29	11.4	33.49 ± 3.08	2.35

all the methods, because the EER is at an operating point greater than t_{c}^{*}, hence there are no valid scores.

We also observed that the ROC curves, especially for Algo2, are very similar. At further analysis we discovered that the ROC curves converge to a single one when decreasing n_{c}. This can be explained as follows. When selecting the most reliable components many enrolment samples from the same subject have an identical binary representation $\mathbf{f}_{\mathrm{B}}$. For example, for the $n_{\mathrm{c}} = 255$ case 75% of the enrolled subjects have no differences between the binary representation $\mathbf{f}_{\mathrm{B}}$ of its N_{e} enrolled samples for the Algo1 algorithm and 92% for the Algo2 algorithm, respectively. For the $n_{\mathrm{c}} = 127$ case, the likelihood increases to 99% and 100%, respectively.

3.2.3 Multi-Sample Fusion at Decision Level

Similar to the score-level fusion case a protected template is created for each N_{e} samples and compared with the single verification sample. However, the *Score- or Decision-level Fusion* module combines the decision $\{d_1, d_2, \ldots, d_{N_{\mathrm{e}}}\}$ into a single fused decision d_f. Methods such as the OR-rule, AND-rule, and majority voting (MV) are used in order to obtain d_f. For the AND-rule method, all the decisions have to be a match in order for the



(a) Algo1 (b) Algo2

Figure 5: ROC curves at decision-level fusion compared to the feature-level (FTR) curves for the (a) Algo1 and (b) Algo2 algorithm.

Table 4: The EER and β_{tar}, and their ci and operating point, and the effective secret size $|\mathbf{K}_f|$ for the decision-level fusion experiments with $n_{\mathrm{c}} = 255$.

Method	*EER* [%]	*RHD* [%]	β_{tar} [%]	*RHD* [%]	$\lvert\mathbf{K}_f\rvert$ [bits]
Algo1, $n_{\mathrm{c}} = 255$					
AND	"4.76 ± 0.40"	"29.0"	19.48 ± 2.08	20.39	21
OR	"3.95 ± 0.39"	"27.1"	15.74 ± 2.09	19.61	21
MV	"4.11 ± 0.44"	"27.8"	16.62 ± 2.05	20.00	21
Algo2, $n_{\mathrm{c}} = 255$					
AND	5.49 ± 0.29	11.4	33.49 ± 3.08	2.35	207
OR	4.87 ± 0.30	10.2	29.90 ± 3.29	2.35	207
MV	4.89 ± 0.28	10.2	30.78 ± 3.27	2.35	207

final one to be a match too, while for the OR-rule case only a single match leads to a final match. For the MV method more than half of the decisions should be a match in order to have a final match.

Again, it suffices to break a single protected template for the adversary to know $\mathbf{f}_{\mathrm{B}}^{\mathrm{e}}$, hence the effective secret size $|\mathbf{K}_f|$ is equal to the secret k_{c} corresponding to the ECC setting.

The experimental results are portrayed in Figure 5 with the performance details in Table 4. As a comparison, we included the ROC curve obtained at feature-level fusion indicated as "FTR". From these results we can conclude that the OR-rule fusion method consistently leads to a better performance, followed by the MV method, and the worst performance is with the AND-rue method. However, the difference is not significant. Compared to feature-level fusion results, the OR-rule methods leads to a similar ROC curve. The ROC curves, especially for the Algo2 algorithm, are very similar due to the same reason as as discussed in the previous section where it was noticed that the reliable binary representation $\mathbf{f}_{\mathrm{B}}$ is very similar for every N_{e} samples.

3.2.4 Summary and Discussions

We have compared performances of multi-sample fusion at feature-, score-, and decision-level. At the optimal setting of $n_c = 255$ we do not observe a significant performance differences between either feature-, score-, and decision-level fusion method. The effective secret size $|\mathbf{K}_f|$ is the same at feature- and decision-level fusion, and at its smallest at score-level fusion. Taking into account that at score and decision level fusion a protected template has to be made and stored for each N_e enrolment sample but only a single one at feature level, we can conclude that the best multi-sample fusion method is at feature level. For security and privacy reasons it is also not desired to store multiple protected templates, which could facilitate the attacker with hacking the protected template and either obtain the secret or the biometric data itself. Furthermore, a single protected template has a smaller storage capacity requirement.

When carefully analyzing the score- and decision-level fusion results, we can also conclude that the MIN-score and OR-decision methods have precisely the same performance, similarly for the MAX-score and AND-decision methods. The explanation for the MAX-score and AND-decision case is that if the maximum score is a match it would imply that all the other $N_e - 1$ scores are also a match, which is also the requirement for the AND-decision fusion method. The MIN-score and OR-decision performance similarity can be explained by the fact that both methods require at least a single individual comparison to be a match in order for the final decision to be a match.

4 Conclusions

With this work we have shown that it is possible to apply multi-sample fusion with the HDS system at feature-, score-, and decision-level. Because the HDS system inherently has only a decision as the output, we adapted the system accordingly in order to have a score as output for the score-level fusion. As a distance score we took the number of bits the ECC had to correct. Furthermore, applying fusion with template protection at feature- or decision-level is straightforward and conventional. However, fusion at score-level is different due to the use of an ECC, which has a limited error-correcting capability. Consequently, for each template protection system there is only a valid score when there is a match.

Given the biometric database and feature extraction algorithms, our experimental results showed that at the optimal setting of $n_c = 255$ there are no significant differences between the best performance (ROC curves) obtained at feature-, score-, and decision-level. Because at feature-level fusion only a single protected template is created, which is better in terms privacy and security protection and storage, we can conclude that the optimal multi-sample fusion is at feature-level.

Acknowledgment

The authors would like to acknowledge the support of the partners within the 3DFACE project, a European Integrated Project funded under the European Commission IST FP6 program.

References

[BBGK08] Jeroen Breebaart, Christoph Busch, Justine Grave, and Els Kindt. A Reference Architecture for Biometric Template Protection based on Pseudo Identities. In *BIOSIG*, Darmstadt, Germany, September 2008.

[BRC60] R. C. Bose and D. K. Ray-Chaudhuri. On a class of error correcting binary group codes. *Information and Control*, 3(1):68–79, March 1960.

[CR07] Ee-Chien Chang and Sujoy Roy. Robust Extraction of Secret Bits from Minutiae. In *Int. Conf. on Biometrics*, pages 750–759, Seoul, South Korea, August 2007.

[DRS04] Y. Dodis, L. Reyzin, and A. Smith. Fuzzy Extractors: How to generate strong secret keys from biometrics and other noisy data. In *Advances in Cryptology - Eurocrypt 2004, LNCS 3027*, pages 532–540, 2004.

[GIA06] Berk Gökberk, M. Okan Irfanoglu, and Lale Akarun. 3D Shape-based Face Representation and Feature Extraction for Face Recognition. *Image and Vision Computing*, 24(8):857–869, August 2006.

[ISO09] ISO/IEC JTC1 SC27. CD 24745 - Information technology - Security techniques - Biometric template protection, 2009.

[JS02] Ari Juels and Madhu Sudan. A Fuzzy Vault Scheme. In *Proc. of the 2002 International Symposium on Information Theory (ISIT 2002)*, Lausanne, 2002.

[JW99] Ari Juels and Martin Wattenberg. A Fuzzy Commitment Scheme. In *6th ACM Conference on Computer and Communications Security*, pages 28–36, November 1999.

[KGK+07] Emile J. C. Kelkboom, Berk Gökberk, T. A. M. Kevenaar, A. H. M. Akkermans, and M. van der Veen. "3D Face": Biometric Template protection for 3D Face Recognition. In *Int. Conf. on Biometrics*, pages 566–573, Seoul, Korea, August 2007.

[KSA+05] Tom A. M. Kevenaar, Geert-Jan Schrijen, Antonius H. M. Akkermans, Michiel van der Veen, and Fei Zuo. Face Recognition with Renewable and Privacy Preserving Binary Templates. In *4th IEEE workshop on AutoID*, pages 21–26, Buffalo, New York, USA, October 2005.

[LT03] Jean-Paul Linnartz and Pim Tuyls. New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates. In *4th Int. Conf. on AVBPA*, 2003.

[NJ08] Karthik Nandakumar and Anil K. Jain. Multibiometric Template Security Using Fuzzy Vault. In *International Conference on Biometrics: Theory, Applications and Systems*, pages 1–6, 2008.

[NJP07] K. Nandakumar, A. K. Jain, and S. Pankanti. Fingerprint-based Fuzzy Vault: Implementation and Performance. In *IEEE Transactions on Information Forensics and Security*, pages 744–757, Decmber 2007.

[PFS+05] P. Jonathon Phillips, Patrick J. Flynn, Todd Scruggs, Kevin W. Bowyer, Jin Chang, Kevin Hoffman, Joe Marques, Jaesik Min, and William Worek. Overview of the Face Recognition Grand Challenge. In *IEEE CVPR*, volume 2, pages 454–461, June 2005.

[RCCB07] Nalini K. Ratha, Sharat Chikkerur, Jonathan H. Connell, and Ruud M. Bolle. Generating Cancelable Fingerprint Templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):561–572, April 2007.

[RNJ06] Arun A. Ross, Karthik Nandakumar, and Anil K. Jain. *Handbook of Multibiometrics*. Springer, 2006.

[TAK+05] Pim Tuyls, Antonius H. M. Akkermans, Tom A. M. Kevenaar, Geert-Jan Schrijnen, A. M. Bazen, and Raymond N. J. Veldhuis. Pratical Biometric Authentication with Template Protection. In *5th International Conference, AVBPA*, Rye Brook, New York, July 2005.

[TG] Pim Tuyls and Jasper Goseling. Capacity and Examples of Template-Protecting Biometric Authentication Systems. In *Biometric Authentication Workshop ECCV2004*.

[ZSBF08] Xuebing Zhou, H. Seibert, C. Busch, and W. Funk. A 3D face recognition algorithm using histogram-based features. In *Eurographics 2008 Workshop on 3D Object Retrieval*, pages 65–71, Crete, Greece, April 2008.

Challenges for the Implementation and Revision of International Biometric Standards Demonstrated by the Example of Face Image Data

Peter Ebinger and Margarida Castro Neves
Security Technology Dept., Fraunhofer Institute for Computer Graphics Research IGD
Fraunhoferstr. 5, 64283 Darmstadt, Germany
{peter.ebinger|margarida.castro-neves}@igd.fraunhofer.de

René Salamon and Oliver Bausinger
Federal Office for Information Security (BSI)
Godesberger Allee 185-189, 53175 Bonn, Germany
{rene.salamon|oliver.bausinger}@bsi.bund.de

Abstract: Travel documents such as the electronic passport (ePass) ensure that each person can be uniquely identified by a single document. The development of new ePass security chip technologies allows for the inclusion of biometric properties in the data carrier of the ePass. The International Civil Aviation Organization (ICAO) has determined a personal photograph as being the interoperable feature for all global travel documents; ICAO [Gro04] regulations reference quality requirements for facial images as defined in ISO standard ISO/IEC 19794-5 [Intb]. Project FIReBIRDs goal is to prepare an international facial image database for conformity tests based on ISO/IEC 19794-5 [Intb], to analyze the requirements in the regulating documents, and to develop suggestions for adaptations and extensions of these standards.

The FIReBIRD database shall provide a well-defined ground truth for level 3 conformance testing. For this purpose the specifications in the standard were thoroughly analyzed and in some parts refined to allow for a precise definition of ground truth. We show with two examples that there might be a defined common-sense definition for some parameters, but they are not measurable and their specification is not scientifically founded: the definition of full frontal view and the definition of eye and hair colors. Our results show that specifications and requirements should always be checked for necessity, practicability and usability and that a continued review and revision of biometric standards is necessary.

1 Standards and Guidelines: History and Development

An identity or travel document such as the electronic passport (ePass) ensures that a person can be clearly tied to the document and be verified (in the traditional sense) by sight check. Supplementing conventional optical security features with new digital security chips has allowed the inclusion of biometric information that more effectively binds each document with an individual, thus introducing an additional layer of identity verification.

The power of biometric verification with the gross capacity of available storage raises several questions: which biometric features should be included in passports, which features should be mandatory, which optional, how will interoperability be ensured? In which way should the biometric feature be stored in country A so that it can be used for verification at border control of country B? These questions illustrate the obvious need for international standardization.

For quite some time the international body responsible for passport standards has been the International Civil Aviation Organization (ICAO), a sub-organization of the United Nations. They specified the photograph and thus the biometric properties of the face as the globally interoperable feature to be stored on a chip, referring the activities of the working group for the international standardization in the field of biometrics[1]. For this aim the standard ISO/IEC 19794-5 Biometric data interchange formats - Part 5: Face image data [Intb] was produced and is now referenced by the ICAO [Gro04].

Many countries have adopted these specifications. In Germany for example, biometrically enhanced passports (called "ePass") based on these standards have been issued since 2005. Quality demands on facial images corresponding to [Gro04] or [Intb] are implemented by German authorities in [Bun, table 6]. Biometrically enhanced travel documents have become increasingly common in their use throughout the world and the reliability of the biometric mechanisms is no longer generally questioned. One question remains however: Are the defined standards and specifications applicable?

The following parts of the paper are organized as follows: Section 2 provides a description of standard implementation and conformance testing followed by a definition of ground truth. The objectives and the realization of the project FIReBIRD are outlined in section 3. In section 4 the general revision process of standards and subsequently related findings of FIReBIRD are presented. Lessons learned finalize the paper in section 5.

2 Standard Implementation and Conformance Testing

In this section we describe experiences with the implementation of the standards mentioned above and how the conformance of biometric systems that are based on them can be tested.

2.1 Standard Implementation

The implementation of these standards and their application revealed some issues that were not foreseen when originally released. Problems in everyday life (e.g. rejection of photographs by passport offices) have led to some workarounds. Photographers want to raise the acceptance rate of face images they produce in order to satisfy an increased

[1] This is the Subcommittee "Biometrics" of the Joint Technical Committee of ISO and IEC (ISO/IEC JTC1/SC37).

number of their customers. On ePass applications image properties are primarily checked by means of a sample photo table. Template and quality assurance (QA) software checks additional photographic image properties such as pose, head/image size, width-to-height ratio and photographic image properties. Experiences with the QA software show that a flawless assessment of facial images based on the current standard is not in every case possible.

Practical experiences with the use of biometric systems for face recognition have shown that certain image characteristics and scene properties such as pose variations have a considerable impact on the recognition performance. Other properties however are far less important for identification than previously suspected. This has shown the need for a scientifically based approach to address these issues.

2.2 Conformance Testing

Data produced by one biometric system or component should be able to be processed by systems or components from other vendors. ISO/IEC 19794-1 Information Technology – Biometric data interchange formats – Part 1: Framework [Inta] defines biometric data interchange formats to ensure vendor independency. Verification mechanisms are needed to check conformance claims of vendors regarding their biometric products. ISO/IEC 29109-1 – Conformance Testing Methodology for Biometric Interchange Records Format Part 1: Generalized conformance testing methodology [Intc] defines a methodology for testing the conformance for various parts of ISO/IEC 19794.

ISO/IEC 29109-1 defines three level of conformance testing:

1. *Level 1 Data Format Conformance* Field by field and byte by byte conformance checking with the specification, both in terms of fields included and the ranges of the values in those fields.

2. *Level 2 Internal Consistency Checking* Testing the internal consistency of the biometric data, relating values from one part or field of the data to values from other parts.

3. *Level 3 Content Checking* Testing that biometric data produced by a system is a faithful representation of the subject.

ISO/IEC 29109-1 [Intc] summarizes conformance requirements for each modality (in our example for face image data) in a requirement table based on ISO/IEC 19794. Products or implementations can comply with a subset of these requirements as some of them are defined as mandatory and others as optional. It is important that all requirements are precisely defined so that they are unambiguous and can be correctly implemented and followed. In particular for face images in travel documents it is important that standard conformance is achieved. Passports are used worldwide and there is a variety of face recognition products and vendors to choose from. Therefore, only clearly specified requirements and a sound

standard enable suppliers of facial image processing software to implement standard conformant and interoperable systems.

Standards have no effect as long as they are not applied and used. Applying a standard means to implement systems that are conformant to the standard. Being conformant to a standard means that input data, output data and processes of the system are valid in respect to data format and content as defined by the standard.

The reliability of conformance tests depends on the comprehensibility of the testing scheme and the test data used. To generate conformance testing data, a measure for the classification of valid and invalid values regarding the standard is needed. This measure should allow to determine the degree of validity of a testing data record. For every property the standard deals with the following has to be clearly defined:

1. whether the testing data record is valid or invalid,
2. if the data record is valid: where inside the boundaries of validity the data record lies,
3. if the data record is invalid: where outside the boundaries of validity the data record lies.

Regarding test data it is absolutely necessary to know which part of it is valid and what part is invalid in respect to which part of the standard.

2.3 Ground Truth

The term ground truth was originally used in the analysis of aerial photographs and satellite imagery in which data are gathered at a distance with the objective to relate image data to real features and materials on the ground. In this context ground truth refers to reliable information that is collected "on location", in contrast to the information that is captured by remote sensing which has to be interpreted and categorized afterwards. Ground-truth data enables the calibration, training and evaluation of systems and algorithms for remote-sensing and interpretation and analysis collected data.

Although the term ground truth is commonly used in the field of biometrics (including related ISO standards) there is no exact definition by ISO yet. There have been some discussions to include the term ground truth into the Working Draft for the Standing Document 2, Harmonized Biometric Vocabulary [Inth]. The discussed definition pointed out that ground truth data should be captured by other means than the normally used measuring instrument. This way the measuring instrument can be validated with sufficient accuracy.

ISO/IEC 19795-2, Information technology – Biometric performance testing and reporting – Part 2: Testing methodologies for technology and scenario evaluation [Intg] distinguishes between ground truth for technology evaluations and for scenario evaluations. In the context of technology evaluations ground truth refers to known associations between

data samples and source of samples whereas for scenario evaluations it is described as associations between system decisions and independently recorded sources of presented samples.

Definition In this context we define *ground truth* as *reliable biometric data* captured within a *defined setup and known parameters* which are *well documented* and available as metadata.

The provision of ground truth test data based on the international standards is of basic importance for performance tests and conformity tests of facial image data. To meet these requirements a pool of facial images containing both kinds of images – images that are valid and those invalid according to ISO/IEC 19794-5 [Intb] – is collected by the FIReBIRD project as described in the following section.

3 FIReBIRD: Project Aim and Realization

In 2008 the Facial Image Recognition Benchmark including Realistic Disturbances (FIReBIRD) [ENSS08] project was started by the Federal Office for Information Security BSI jointly with Fraunhofer IGD.

3.1 Project Aim

FIReBIRD aims at assuring and improving the quality of systems for processing facial images based on a scientifically grounded implementation of the standards mentioned in the above section (see Fig. 3.1). For this purpose a facial image database shall be created based on the requirements defined in the standards that can be used for conformity and performance tests of systems for processing facial images (e.g. systems for an automated face recognition and/or systems for quality assessment of facial images based on ISO/IEC 19794-5 [Intb]). Furthermore the requirements in the regulating documents shall be analyzed and suggestions be developed for adaptations and extensions of the standard.

A concept for the development of an internationally composed facial image database has been prepared. This concept has been internationally coordinated in cooperation with the US-American National Institute of Standards and Technology (NIST) and the British National Physical Laboratory (NPL).

3.2 Project Realization

The requirements defined in ISO/IEC 19794-5 [Intb] concerning photographic and phototechnical image properties are subject to a revision. Based on an analysis of the relevant

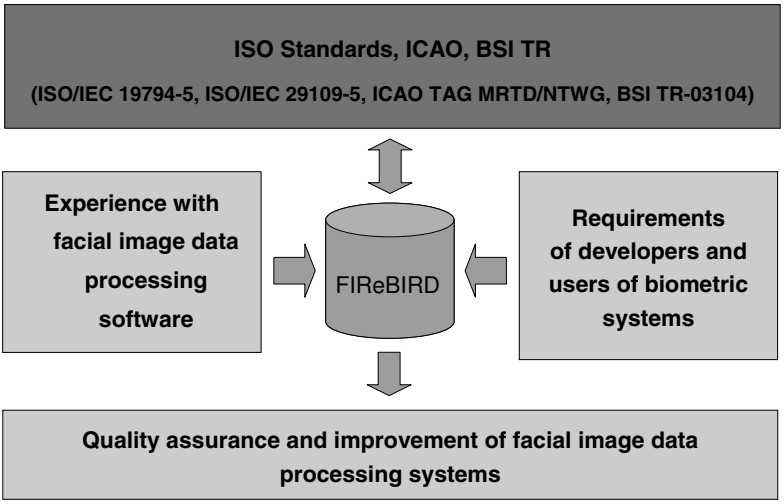


Figure 1: Interaction of FIReBIRD with biometric standards, developers and users of biometric systems

image properties the qualitative size of the image database is determined. A ground truth is defined by specifying and describing a precise and universally applicable reference value or a reference point for each property respectively.

Morphologic face features are also addressed and recorded as morphologic peculiarities (such as certain face or nose shapes, the mouth line, the special manifestation of the eye area, eye, skin and hair color and hair type) may have an impact on the performance of face recognition systems. The "semantics" of the face based on state-of-the-art anthropological and forensic findings are captured. Schematic representations are generated allowing a classification of faces. These facial properties shall be stored in the database as meta data for each facial image for each identity respectively.

4 Standard Revision

Most ISO standards require periodic revision because of technological evolution, new methods and materials and/or new quality and safety requirements. ISO has therefore established the general rule that all ISO standards should be reviewed at intervals of not more than five years.

Accordingly also the international standard ISO/IEC 19794-5 [Intb] is periodically revised and has undergone several extensions and modifications represented by the following documents:

- a first (informative) addendum [Intd] providing more detailed descriptions of photographic scenarios for taking suitable photos,
- a first technical corrigendum [Inte] correcting typos,
- a second technical corrigendum [Intf] considerably softening the tolerances for the criteria mentioned above.

One of the outcomes of FIReBIRD is to give some feedback on the revision process of related standards. For this purpose suggestions shall be made based on the analysis of the demands on facial images and the experiences with the verification of sovereign documents for inclusion in subsequent releases of ISO/IEC 19794-5 [Intb] and [Bun] (or related amendments to these documents respectively).

To allow an automated but reliable quality assurance of the presented facial images no image properties should be enforced that are not automatically measurable and/or calculable.

The following aspects were particularly affected:

- head size relative to the image size,
- width of the head relative to the image width,
- horizontal centering of the image, and
- roll angle (rotation about the horizontal back to front (z) axis).

FIReBIRD demonstrated that the true reason for these problems in the specification of requirements for facial images was the definition and the measurement of ground truth data and reference points (e.g. full frontal positioning of the head) for all relevant image properties. In particular "soft" properties – such as morphologic features, head positioning and color representation – are difficult to measure and therefore it is not easy to define quality requirements for them. The findings of FIReBIRD show that it is necessary to considerably extend tolerances where necessary and to limit the standards to measurable properties.

4.1 Refining the Definition of Ground Truth

Standards often deal with properties that are clearly defined, but also with properties that are hard to measure.

On the one side, for example, [Intb] specifies the relation of face height to width, or the range of valid widths and heights of images. These properties can be easily measured using a ruler or counting pixels: There is a well-defined reference/zero point, as well as a defined optimum value and there are well-defined algorithms to determine the values. For these properties there are generally accepted standards or established definitions and methodologies that define measurement and processing.

On the other side, the standard also defines properties that are not as easy to determine, e.g. the range of valid pitch of the head. In this case there is a defined common-sense optimum value, but there is no well-defined reference point and scale. However, without them it is impossible to exactly measure a property.

To make bad things worse the character of a test data record often cannot be completely described using properties specified in the standard. A facial image, for example, can be described more exactly if some basic information about the person shown on the image is given, e.g. age, hairdo, eye, hair or skin colors. However, most of these additional properties (as pitch of head mentioned above) do not have well-defined reference points and they are therefore hard to measure. However, for some of them this might not be obvious.

So how can the problem of measurability be solved? A practical approach: If there is no standardized measure, define and build one.

The following requirements should hold for a ground truth measure:

1. The measure has to be close to reality.
2. The measure has to be internationally reproducible.
3. The measure has to be applicable.
4. The reference points have to be clearly separated from each other.

Within FIReBIRD we applied the requirements described above to determine measures that can be applied to collect ground truth data for facial images.

4.2 Definition of Ground Truth for Eye, Hair and Skin Color

One of the challenges within FIReBIRD is to define measures for eye, hair and skin colors. Tables for eye and hair color referring to reality and scientific knowledge about the typical appearance of human beings reference are defined as described in the following.

ISO/IEC 19794-5 [Intb] specifies seven *eye colors*: “black”, “blue”, “brown”, “gray”, “green”, “multi-colored” and “pink” where “pink” probably refers to the eye color of people who have albinism. These seven classes may be sufficient if we have to describe eye colors for traveling purposes (in identity documents). In case of traveling or migration the border control staff is first of all interested in reliably verifying and distinguishing eye colors. When building a database such as the FIReBIRD database – for performance or conformance testing it is necessary to describe the classification and measuring equipment as precisely as possible. For this purposes we use a more comprehensive eye color classification scheme as it is defined in the ISO standard.

Our goal is a reliable and unambiguous classification of eye colors during the acquisition of facial images. Therefore eye colors are categorized into five color classes with three color depths each. To provide a realistic representation of eye colors to allow an easy and

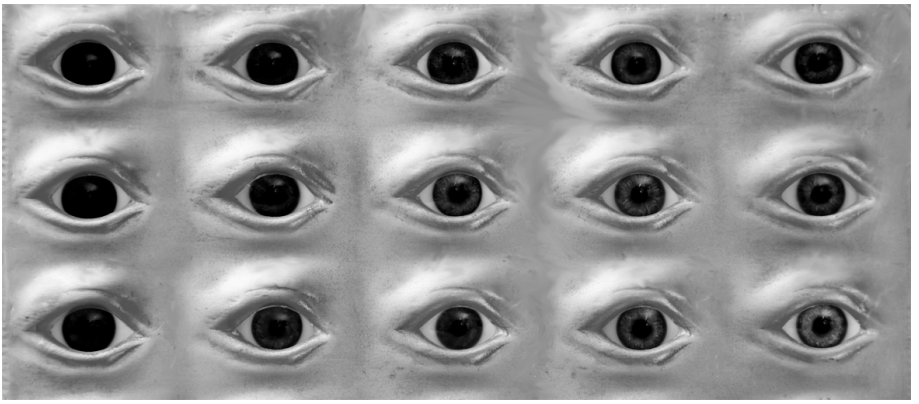


Figure 2: Box with glass eyes to categorize eye colors into five color classes (from left to right: brown, grey-brown, multiple, grey-blue and blue) with three color depths each (from top to bottom: dark, medium, bright)

precise classification by human operators these 15 colors are represented by glass eyes in a framed box covered with a plate of eyelids (see figure 4.2).

Using our extended eye color table we want to reliably classify the eye colors for more than 99% of the subjects. We hope that we can also demonstrate that an extended eye color table does not necessarily lead to an unreliable, ambiguous and/or slow classification process and that our color table is closer to reality than the ISO eye color categorization. If our experiments show that our classification scheme works as expected we will recommend to extend and redefine the eye color table in the ISO standard based on our eye color table. If the classification process does not work as expected or if a redefinition of the standard is not be possible we could try to map our extended eye color table to ISO eye colors by rearranging and grouping several eye colors of our table and assign them to one of the ISO eye colors.

Six *hair colors* are specified by ISO/IEC 19794-5 [Intb]: “black”, “blonde”,“brown”, “gray”, “white”, and “red”. An additional category covers the case of no hair and therefore no hair color (“bald”). This is a very simplistic and rough classification scheme, but probably sufficient for traveling purposes. The same considerations and expectations apply to hair colors analogously to those described above for eye colors.

For a more detailed capturing of hair colors we propose to use 10 color depths (from black to brown to blond) with another three natural red colors (light red, medium red, dark red). 5 stages of grey (0%, 25%, 50%, 75% and 100% grey) and 5 additional colors (blue, green, yellow, clear red) were added to cover the overall range of natural and artificial hair colors. These color categories are – in analogy to glass eyes for eye colors – represented by a ring of artificial hair.

Skin color classification using artificial color tables poses some problems since available color tables are based on clear colors which makes a comparison with multi-pigmented

skin very difficult. This may lead to false classification or even the lack of a suitable reference class for some skin types. Therefore, it is investigated if a spectrophotometer may be used for an objective skin-color categorization.

First experiences with the classification scheme for eye, hair and skin colors defined above are under development.

4.3 Definition of Ground Truth for Full Frontal View

In the current development of the revision process of 19794-5 (latest version 2nd CD as of January 2009), the following differences in comparison to the first revision are already visible.

The problem of defining a zero degree reference point in pitch and yaw (see figure 4.3) is at least acknowledged, stating that the definition of zero pitch and yaw is “not obvious”. As a partial aid and based on the inclusion of 3D image representations in the base standard, the Frankfurt horizontal (defined by a line through the tragion and the lowest point of the right eye socket) is at least included, although not used as a normative definition.

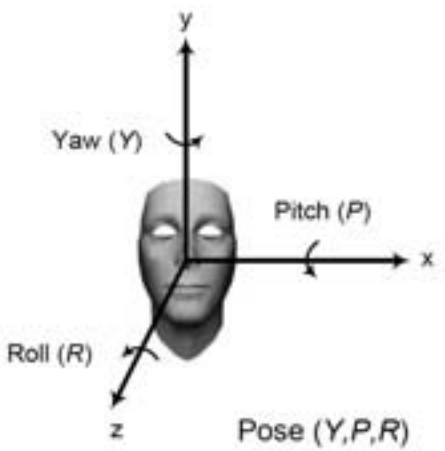


Figure 3: The definition of pose angles with respect to the frontal view of the subject according to ISO/IEC 19794-5 [Intb]

In general, the standard now tries to be more precise in its definition, e.g. it has been given an upper bound for an acceptable thickness of problematical heavy glasses frames (not more than 5% of the images inter-eye distance), or, as an other example, the definition of equal subject lighting has been enhanced by a formula for automatic computation.

The best-practice guide (in Annex A) has been refined and extended by several definitions for recommended image properties, e.g. a technical definition of hair covering the eyes and rims of glasses covering the eyes was added.

The general trend in the revision process that can be deduced from these observed changes:

- Much care has been taken to be more precise on the specification of several technical requirements where possible.
- The limitations of this approach have been recognized, although a sensible definition of pose error is still not given (because of the impossibility of establishing a useful ground truth), the requirement has still been kept in the revision of the standard. This was mainly based on the feeling of many participants that a normative requirement on pose was and is still necessary.

As a side note: Based on the introduction of the 3D image types in the base standard and the possibility of having both 2D and 3D representations of the same person in the record, in some settings a better way of determining pose deviations based on the 3D representation might be possible. Therefore, it is valuable to specify these pose properties in the standard since there are application domains of the standard beyond electronic passports or similar use cases.

5 Standards and Guidelines: Lessons Learned

In particular the second technical corrigendum [Intf] shows the particularities of the standard ISO/IEC 19794-5 [Intb]. Experiences with the application of the standard show a need for corrections in fundamental elements of related standards. Improved requirements are now available for applications that deal with the quality assurance of images as well as the assignment and production of electronic passports.

In ISO standardization processes a standard is usually reviewed every three to five years resulting in a continuance of stipulations, revisions or withdrawals of specifications. Accordingly ISO/IEC 19794-5 [Intb] is also currently under revision. Now the time pressure for the international group of experts to (re-)define requirements for facial image properties is lower than when the first version of the standard was released. The second version of the standard is planned for 2011.

The following conclusions can be drawn for the implementation and revision of standards:

- Specifications and requirements should always be checked for necessity, practicability and usability.
- Application improves the standard.
- Time pressure is an enemy of quality.
- Continued review and revision is always necessary.

These tenets should be taken into account in the development of future standards so that revision and extension efforts are kept to a minimum ensuring an efficient and target-oriented revision process.

References

[Bun] Bundesamt für Sicherheit in der Informationstechnik. BSI TR-03104 Annex 1 (QS-Gesicht) – Technische Richtlinie zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für Pässe, Version 2.1.1 – Qualitätsanforderungen bei der Erfassung und Übertragung der Lichtbilder als biometrische Merkmale für elektronische Pässe.

[ENSS08] Peter Ebinger, Margarida Castro Neves, René Salamon, and Helmut Seibert. International Database of Facial Images for Performance and ISO/IEC 19794-5 Conformance Tests. In *BIOSIG 2008*, pages 165–174, 2008.

[Gro04] International Civil Aviation Organization Technical Advisory Group 15 Machine Readable Travel Documents/New Technologies Working Group. Biometrics Deployment of Machine Readable Travel Documents, Version 2.0, May 2004.

[Inta] International Organization for Standardization. ISO/IEC CD 19794-1 Information Technology – Biometric data interchange formats – Part 1: Framework.

[Intb] International Organization for Standardization. ISO/IEC CD 19794-5 Information Technology – Biometric data interchange formats – Part 5: Face Image Data.

[Intc] International Organization for Standardization. ISO/IEC FDIS 29109-1 – Conformance Testing Methodology for Biometric Interchange Records Format Part 1: Generalized conformance testing methodology.

[Intd] International Organization for Standardization. ISO/IEC IS 19794-5:2005, Information Technology – Biometric data interchange formats – Part 5: Face Image Data – Amendment 1 – Conditions for Taking Photographs for Face Image Data.

[Inte] International Organization for Standardization. ISO/IEC IS 19794-5:2005, Information Technology – Biometric data interchange formats – Part 5: Face Image Data – Technical Corrigendum 1.

[Intf] International Organization for Standardization. ISO/IEC IS 19794-5:2005, Information Technology – Biometric data interchange formats – Part 5: Face Image Data – Technical Corrigendum 2.

[Intg] International Organization for Standardization. ISO/IEC IS 19795-2:2007, Information technology – Biometric performance testing and reporting – Part 2: Testing methodologies for technology and scenario evaluation.

[Inth] International Organization for Standardization. JTC 1/SC 37 Biometrics – WD Standing Document 2 Version 11 (SD 2), Harmonized Biometric Vocabulary.

Spectral Selection for a Biometric Recognition System Based on Hand Veins Detection Through Image Spectrometry

F. Cortés, J. M. Aranda, R. Sanchez–Reillo[1], J. Meléndez, F. López

Infrared Laboratory (LIR). Physic Department / Instituto Pedro Juan de Lastanosa
[1]University Group for Identification Technologies
Universidad Carlos III de Madrid
Avda. Universidad, 30; 28911 – Leganes (Madrid)
francisco.cortes@uc3m.es

Abstract: This paper presents the result of a work orientated to the spectral optimization of the acquisition devices in vascular biometrics systems. Spectral windows are proposed which will allow to design a multispectral system with a few and well defined bands, obtaining a more robust and reliable device, compared with the standard single band systems. This is in accordance to general trend of electro-optical and infrared acquisition systems in the field of the detection and remote sensing, where the work focus is on obtaining optimized bands. To carry out this work a Hyperespectral Imaging System (HIS) has been used as the acquisition system. In order to analyze the large amount of information and to select the spectral bands, a Principal Component Analysis (PCA) has been done.

I. INTRODUCTION

The need of implementing biometric systems in different scenarios of our daily life derives from the importance of making an automatic, objective and reliable recognition or authentication. In this context, vascular systems appear as one of most safe and difficult to be corrupted.

Some authors point out that the one of the major drawbacks of vascular biometric acquisition system is his response in outdoor environments [1]. Others study which are the ideal environmental conditions in terms of humidity and temperature [2]. In any case, the acquisition system must be as robust as possible, independently of the different environment conditions, light intensity, etc, in order to provide the same signal for the same pattern.

Optical Properties of the Skin

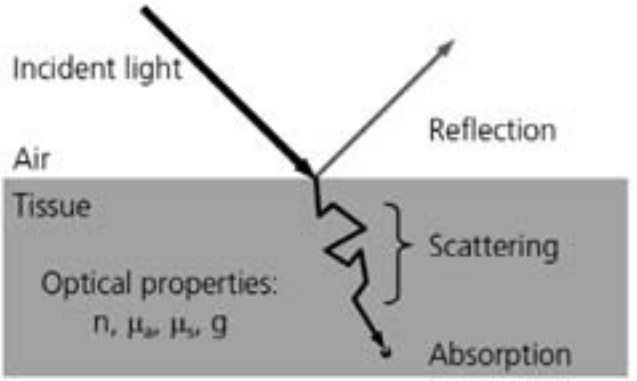


Figure 1.- Main phenomena in the light-tissue interaction [4].

When the radiation interacts with the tissue, a series of process take place which depend on the wavelength and the size of the skin particles. In the case of Visible (VIS) and Near InfraRed (NIR) wavelengths the scattering coefficient is an order of magnitude larger than the absorption coefficient, so the predominant phenomenon will be scattering [3].

There are three principal components in the hand: tissue, veins and in many cases fuzz. Of all of those components the veins have the larger absorption coefficient due to the presence of haemoglobin (Hb and HbO_2) (figure 2) [4]. For that reason it seems reasonable to easy think that the veins should present a contrast with the tissues of the neighbourhood.

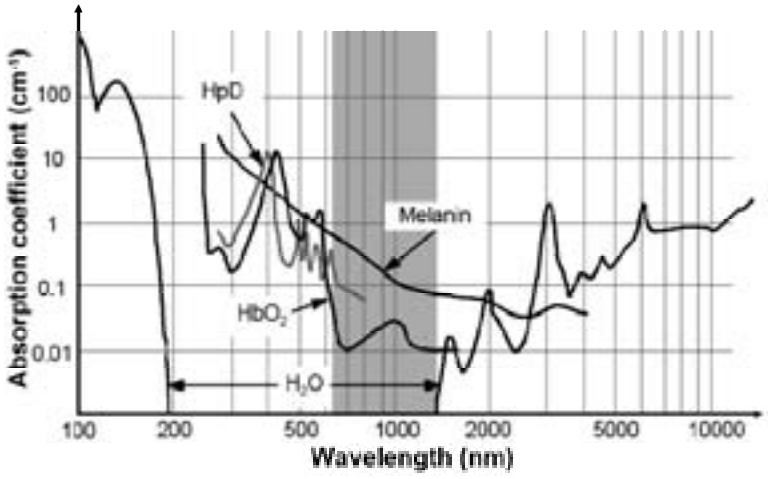


Figure 2.- Curve of the absorption coefficient of the skin componets. The shape HbO_2 show a high absorption coefficient between 400 and 550 nm [4].

Spectral Selection: Hyper and Multi Spectral Systems

The trend of the electro-optical acquisitions systems in diverse fields dealing with detection is to work in a few different bands in order to optimize operative detection making up systems able to give the main information to make a decision in seconds [5]. These few bands must be well selected depending of the application, varying in the centre wavelength and bandwidth. This is what is known as Multispectral Systems. In contrast, Hyperspectral Imaging (HIS) has a very high spectral resolution, and is used here in order to provide spectral optimization of the multispectral system. From a high spatial and spectral resolution hyperespectral image is possible to define the univocal information, eliminating the non-valid or redundant spectral information. That resultant information could be given in terms of number of bands, centre wavelength and bandwidth. Our aim in this work is to follow this methodology to design a multispectral instrument optimized in bands to detect the pattern veins of a hand.

The HIS used in this paper is made up by an optics which focuses the light coming from the scenario, a Michelson interferometer as a device to provide spectral resolution and finally a Focal Plane Array (FPA) detector which is sensitive to the wavelength corresponding to the visible (VIS) and the near infrared (NIR) that confers to the system the spatial resolution.

II. IMAGING SPECTROMETRY: SELECTION OF THE SPECTRAL RANGE

The study presented in this paper has been done in the VIS (0.4 - 0.75μm) and NIR (0.75 - 1.1 μm) spectral region. In the state of the art revision, some works had been revised with cameras at different regions, as middle wavelength infrared (MIR) from 1.5 to 5 μm, or thermal infrared (TIR) from 7 to 14 μm, and the most relevant conclusions were that the most appropriate region is the VIS-NIR, because this is the region where environmental conditions are not so influent [6]. The principle to generate the image is different in the case of the VIS-NIR range than in the MIR or TIR cases [7]. In the latter ones, the image is formed by temperature contrast due to the self emission of radiance of the body by the fact to be over 0 K, so it is not necessary to illuminate. But in the case of a VIS or NIR sensor, due to Wien Law that describes the displacement of the wavelength of peak emission as a function of the temperature $\lambda_{max}(\mu m) = \frac{2897.8}{T(K)}$ (see figure 3), the body temperature is not enough to emit a signal large enough to be read by a VIS-NIR sensor. For that reason is necessary to illuminate the scenario with an external light source. This is one of the main drawbacks of the VIS-NIR range versus the MIR or TIR window.

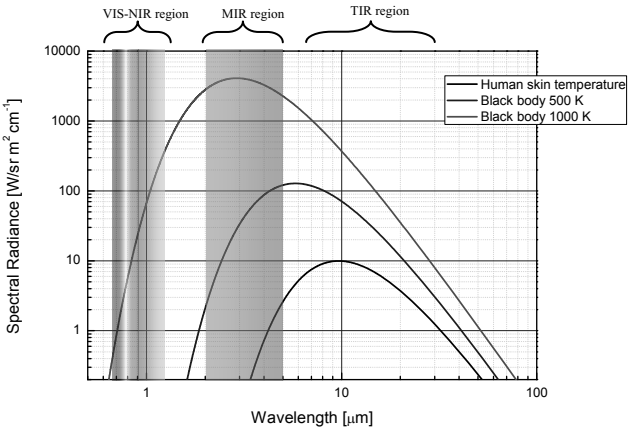


Figure 3.- Planck's Law for black bodies at different temperatures. It shows that the curve corresponding to the human body emission (black curve) is not enough to emit detectable signal in the VIS-NIR region.

According to the illumination, the sun was chosen as the light source, because his spectra cover the entire VIS-NIR region. A previous simulation of the sun irradiance has been performed. That simulation was made with Modtran software [8].

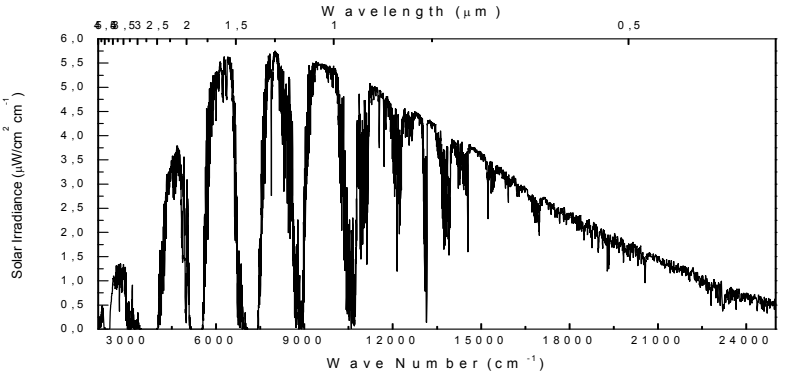


Figure 4. – Sun irradiance simulation in the earth surface with MODTRAN software for 0.4 to 5 μm.

The output obtained is shown in figure 4. The sun light covers the entire VIS-NIR region with the exception of some zero valleys that are not very relevant for that paper.

The sun allows two different possibilities for illumination: direct or diffuse emission. The direct illumination was obtained by exposing the hand skin directly to the sun rays. To obtain the diffuse illumination the hand was placed in a shadowed place.

The HIS used in this paper is a Fourier Transform spectroradiometer based on a Michelson interferometer with a charge coupled device (CCD) sensor doped with Si to work in the VIS and NIR spectral regions (figure 5). The main characteristics are shown in table I.

Table I. - Sensor characteristics used in this paper

Spectral Range, and Resolution	Array Size	Sensing Technology	FOV	Focal Distance
0.4-1.1μm, 0.1μm	1280 x 1024	CCD, 12 bits	15 mrad	50mm

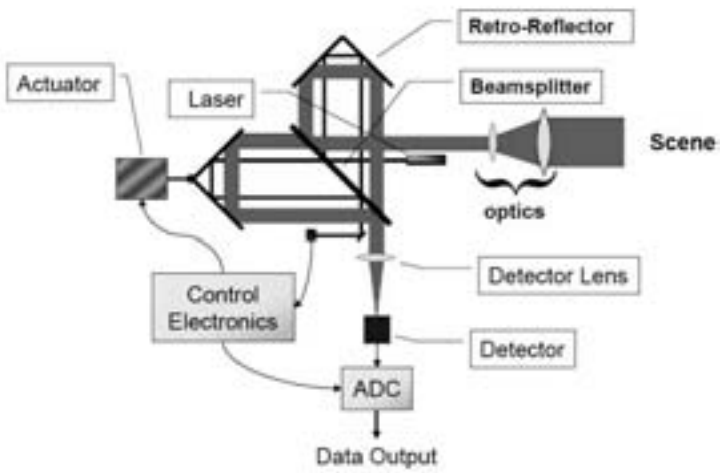


Figure 5. - Layout of the Michelson Interferometer of the System used.

Spectral resolution is obtained by means of a Michelson interferometer, which produces constructive or destructive interference for the different wavelengths as a function of the sweep of a mirror, focusing the image in the detector matrix conforming so, as a function of time, an interferogram at each detector. Over that interferogram the Fast Fourier Transform (FFT) is applied to obtain the spectra cube image, where, instead of time, the z axes correspond to wavelength [9].

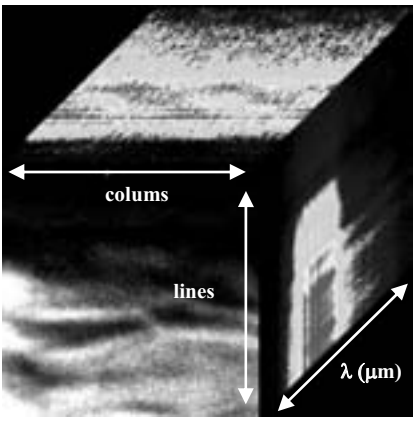


Figure 6.- Data cube of a hand acquired with the Spectral Imaging.

The result is a cube image from 0.4 to 1.1 μm as show in figure 6, are units digital counts in the case of working in emitance mode. The instrument allows obtaining reflectance, absorbance or emitance spectra. In the case of reflectance or absorbance spectra is necessary to have a reference or background in order to generate them. In the case of emitance spectra, the instrument measures the received signal. In this paper the emitance mode has been used, eliminating so the possible errors with the background reference. Obviously, the data cube image obtained in this mode is a composition of different reflectance or absorbance spectra due to the different characteristics of the surface skin.

III. METHODOLOGY AND PROCEDURES DESCRIPTION

After selection of the VIS-NIR spectral window to perform the study, the methodology followed started by preparing a measure campaign considering the coverage of many different illumination cases, and capturing different hands and different parts of the hand. After that, a post-process of the datacube was necessary, in order to adapt the datacube to the analysis algorithm. Finally, the spectral characterization of the scenario (veins, hand skin and others) has been done demonstrating a qualitative different between both spectral characteristics.

In order to have enough images to validate the study, different parts of the hands were acquired, such as the palm, back of the hand and wrist. All of them were taken with different illumination conditions (diffused and direct).

In order to study and extract the correct information, Principal Component Analysis (PCA) was applied in the datacube [10]. With hyperspectral images that tool is useful due to the big amount of different information (spatial and spectral) within a datacube. Also the PCA is a very powerful tool in some applications where reducing the amount of data is critical, keeping only the necessary information and discarding the redundant, noisy, or simply the non-valid information. PCA is an algebraic technique that diagonalizer the covariance matrix of the data. For a database of m bands, it provides an eigenvector matrix of mxn elements.

This matrix provides a method to analyze efficiently the datacube spectra. The first eigenvector corresponds to the maximum covariance eigenvalue. The linear combination of bands formed with their components as coefficient is the first principal component (PC 1), an image that accounts for the maximum variance of data. The second column of the matrix is the eigenvector of the PC 2 containing the maximum variance after the PC 1, and so on for the rest of the PC's.

The study of the PC's provides a systematic means to distinguish the main target of interest under study (i.e. the veins). Usually, the PC1 image is "mean" images that contain the overall variations due to illumination (shade, bright areas, etc.). The successive PC contains fine information related to the different responses of the object in the scenario; and it is to be expected that some of them provide an enhanced "vein image". The eigenvector associated will have a specific special shape and when that spectral shape is defined, it will be possible to define suitable spectral bands for a multispectral system for vein detection. In this study, the spectral bands have been created by a synthetic image composed by an average of the spectral images dictated by the spectral shape defined in the PCA study.

IV. EXPERIMENTAL RESULTS

In the first measurement campaign the main different possibilities were covered: Diffuse and direct radiation, and palm, back of the hand and wrist.

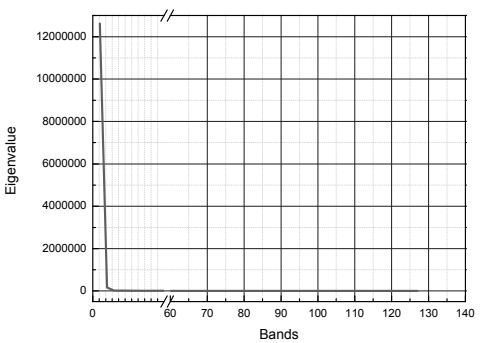


Figure 7.- PC eigenvector representation.

All the datacubes are composed of 127 spectral bands from 400 to 1100 nm. In order to study the spectra and reduce the amount of information, the PCA was performed. In the figure 7 the value of the each eigenvalues are represented in decrease order. The study of this graph let to know how many of eigenvalue, that will be correspond with the number of PC bands, which will be necessary for dispose of the entire information. According to the graph to recompose the most of the information is possible, using only two or three bands. In the figure 8 is shown the obtained image for all the spectral range of the system (400 – 1100 nm) and the three firsts PC's bands of a datacube. The PC 1 is an image composed by contributions of the almost all the bands; we can appreciate that is very similar to the broadband image. The PC 2 causes the enhancement of the veins with a negative contrast between veins and the tissue. Finally, the PC 3 shows other objects in the scenario as fuzz and skin texture. This information is not relevant for our proposes but could be useful for other application. The following PC's have not been shown because they only contain noises, redundant or non valid information for our study, as show the PC 4.

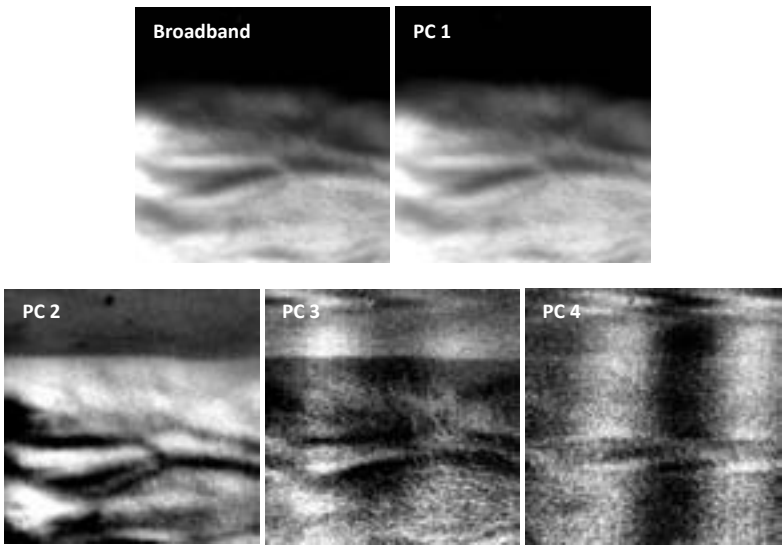


Figure 8. – Top: left the broadband image from 400 to 1100 nm; right: the PC 1. Bellow is showed the rest PCA's.

The main conclusion is that PC 2 is where the information related to vein detection is contained. In order to study the PC 2 and extract the most information as we can, the eigenvector components corresponding to that PC was represented in a graph as a function of wavelength of each of 127 bands of the HIS. The result is shown in figure 9, where results are represented. That correlation values present a singular shape, and that shape is kept for all the datacube acquired.

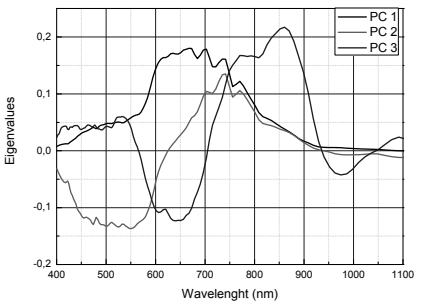


Figure 9. – Eigenvalues of the three first PC's of the datacube showed.

That composition of PC 2 band can be divided in three different regions:

- **Region I:** 400 – 600 nm: A valley is appreciated with negative values.
- **Region II:** 650 – 850 nm: The eigenvector components take positive values in the shape of a crest.
- **Region III:** 700 – 1100 nm: The eigenvector components are close to zero.

The contrast in the value of eigenvector components between the region I and II reflects the spectral contrast in haemoglobin absorption that can be seen in Figure 2 where the absorption coefficients [in cm^{-1}] of the main components of the tissue are represented, haemoglobin has a high absorption coefficient around 475 nm [4]; that means; that the high concentration of haemoglobin (150 g/l), increases the radiation absorption of the veins at that wavelengths. This is in agreement with the results in terms of spectral windows.

V. DATA PROCESSING

After the spectral pre-selection was done, the next step was to perform a data processing based on techniques of enhancement of the target versus background, in order to validate the result.

Firstly, a synthetic image composed from hyperspectral images was created to simulate a broadband image, obtained with a suitable optical filter. This technique trying to simulate a real image, acquired with a real camera with a certain broadband. The synthetic image corresponding to the first broadband selection was created getting the mean of all the bands from 400 to 600 nm (band 1). The second synthetic image generated was the corresponding to the mean of all the bands from 650 to 850 nm (band 2), as is shown in the figure 10. With those processed images a bi-spectral system is simulated.

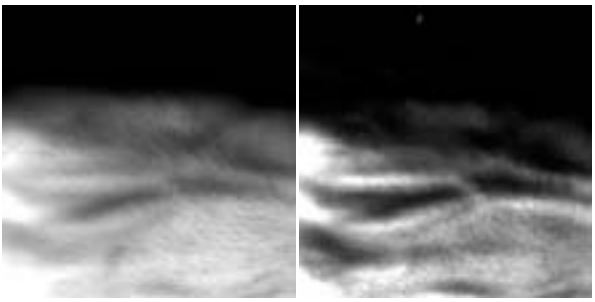


Figure 10.- Left: synthetic image between 400 to 600 nm (band 1); right: synthetic image between 650 to 850 nm (band 2).

Applying PCA over synthetics images generated is obtained two new PC images (figure 11) where is possible to appreciate the enhancement of the veins at the PC 2.

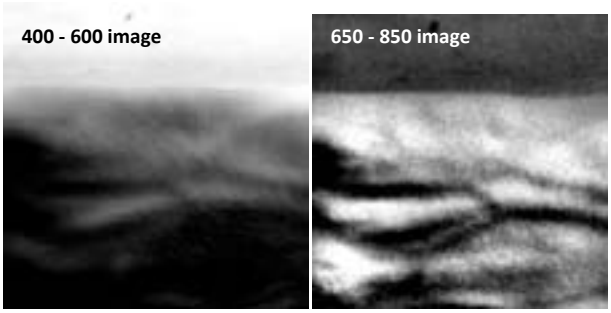


Figure 11.- PCA with the two synthetic images B1 and B2. In the PC 2 is possible to distinguish the veins with high contrast

Comparing the veins contrast in the PC 2 obtained with the images of the HIS with PC 2 obtained with the synthetic images we can appreciate that the contrast is very similar or even better in the case of the PC 2 of the synthetic image as show the figure 12.

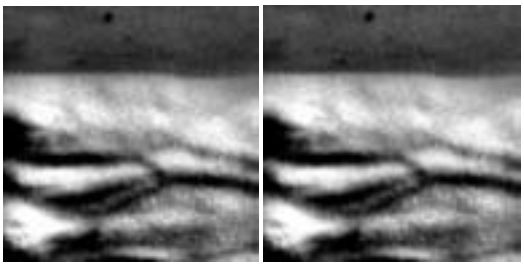


Figure 12.- Right: PC 2 obtained with the two synthetic images; left: PC 2 obtained with the images of the HIS

VI. CONCLUSIONS AND FUTURE WORKS

This paper describes the procedure to perform the spectral selection for a bi-spectral imaging system for vascular biometrics in the VIS-NIR region. The instrument used for this study has been a hyperspectral camera in the VIS-NIR region with a high spectral resolution in order to perform a detailed spectral analysis.

Hyperspectral images have made possible to define two bands which optimize the detection of the dorsa veins of the hands by means of principal component analysis. This selection has demonstrated to be robustness with respect to environment conditions because the hand was illuminated with the sunlight, what means that there was no control over the illumination. The requirement of controlled illumination was one of the main drawbacks of the previous sensors for vein pattern recognition.

In spite of this, our aim for a future research work is a system based on illumination with a more powerful light than the sun in order to be able to detect the veins of the palm, that have not been seen with the sun illumination. The incident sun irradiance is quite low, and this implies that the light cannot penetrate very deeply into the skin, as in the cases where the illumination is performance with devices such as LED matrix, xenon lamps, etc.

Another future work proposed is to perform an experimental validation with the defined optical filter in a standard camera.

VII. ACKNOWLEDMENTS

The authors acknowledge the financial supported by Ministerio de Educación of Spain and Instituto Pedro Juan de Lastanosa.

VIII. REFERENCES

[1] R. Sanchez-Reillo, B. Fernandez Saavedra, J. Liu-Jimenez, C. Sanchez-Avila. "*Vascular Biometric Systems and Their Security Evaluation*"

[2] W. Lingyu, G. Leedham, "*Near- and Far- Infrared Imaging for Vein Pattern Biometrics*", Proceedings of the IEEE International Conference on Video and Signal Based Surveillance (AVSS'06), IEEE, 2006. [3] Tuchin, Valery. ''*Handbook of Optical Biomedical Diagnostics"*. SPIE Press Bellingham, WA, (USA) 2002.

[4] Soto Thompson, Marcelo "*Photodynamic Therapy utilizing Interstitial Light Delivery Combined with Spectroscopic Methods*", Doctoral thesis, Lund Institute of Technology, Sweden, 2005

[5] S. Briz, A. J. de Castro, J. M. Aranda, J. Meléndez and F. López. "*Reduction of false alarm rate in automatic forest fire infrared surveillance system*", Remote Sensing of the Environment. Vol. 86, pp. 19-29, Ed. Elseiver Science Inc., 2003.

[6] Kuo-Chin, Chih-Lung Lin, "*The Using of Thermal Images of Palm-dorsa Vein-patterns for Biometric Verification*", Proceedings of the 17th International Conference on Pattern Recognition (ICPR'04), IEEE, 2004
[7] Holst, Gerald C. ''*Common Sense Approach to Thermal Imaging*''. JCD Publishing and SPIE Optical Engineering Press, 1st ed., Florida and Washinton (USA) 2000.
[8] Ontar Corporation. "*PcModWin3 Manual*", Ontar Corporation, North Andover, Massachusetts, January, 1996.
[9] Chang, Chein-I, "*Hyperspetral Imaging: techniques for spectral detection and classification*", 2003
[10] Richards, J.A.; Jia, Xiuping. "*Remote Sensing Digital Image Analysis*". 3rd ed. Springer-Verlag, Berlin, Germany, 1999.

The Extended Access Control for Machine Readable Travel Documents*

Rafik Chaabouni† Serge Vaudenay

EPFL
CH-1015 Lausanne, Switzerland
http://lasecwww.epfl.ch

Abstract: Machine Readable travel documents have been rapidly put in place since 2004. The initial standard was made by the ICAO and it has been quickly followed by the Extended Access Control (EAC). In this paper we discuss about the evolution of these standards and more precisely on the evolution of EAC. We intend to give a realistic survey on these standards. We discuss about their problems, such as the inexistence of a clock in the biometric passports and the absence of a switch preventing the lecture of a closed passport. We also look at the issue with retrocompatibility that could be easily solved and the issue with terminal revocation that is harder.

1 Introduction

Since 2004, a majority of countries have adopted the ICAO standard [19, 22] for Machine-Readable Travel Documents (MRTD). It specifies how to store and use biometrics in passports to have more secure identification of the holder. Since it is based on the RFID technology [12], an access control is necessary for privacy protection. The optional one proposed in the ICAO standard is based on symmetric-key cryptography with a key printed on the passport. It is called Basic Access Control (BAC), offers very little privacy protection, and is the only mechanism which can be used to protect mandatory data groups.

Privacy is a big concern for holders. Indeed, on May 17, 2009, 49.9% of electors voted against the introduction of the biometric passport in Switzerland, presumably for privacy reasons.

To strengthen privacy, the European Union adopted an Extended Access Control (EAC) [33] to have a reasonably secure privacy protection for other data groups. It is based on public-key cryptography and requires a public key infrastructure to be deployed

*This work was partially funded by the European Commission through the ICT program under Contract ICT-2007-216676 ECRYPT II.

†Supported by the Swiss National Science Foundation, 200021-124575

for readers. Since passports are not online, they cannot receive certificate revocation lists. Thus, revocation can only be based on expiration date. Unfortunately, passports do not have a clock so they can only compare the validity period with the latest accepted certificate date.

EACv1 protects against cloning but only in the situation where it is being used in a country reading EAC. Countries reading EACv1 but being unauthorized to pass terminal authentication could use privacy-enhanced protocols, but it is not mandatory.

EACv2 may make sure that passports are only read by authorized terminals so the cloning issue may be solved. Indeed, EACv2 goes further by protecting access by EAC even ICAO-mandatory data groups, even for countries unauthorized to read other data groups. Unfortunately, ICAO-mandatory data groups must be readable by countries not implementing EAC so this protocol is likely to be bypassed for interoperability reasons.

Related work A substantial amount of work has already been achieved on MRTD. Juels, Molnar and Wagner [13] presented in 2005 one of the first (if not the first) security analysis on e-passports. They identified several flaws in the ICAO standard, namely clandestine scanning, clandestine tracking, skimming then cloning, eavesdropping, biometric data-leakage and weaknesses in the cryptographic setups of the ICAO standard. Kc and Karger [14] exposed in 2005 their research on similar tracks and introduced some other attacks, namely the "splicing" attacks and the "fake finger" attacks. In 2006, Kosmerlj et al. [15] studied the weakness of facial recognition. Hoepman et al. [11] focused in 2006 on passive attacks against BAC and gave some thoughts on biometrics. They showed that the entropy of the symmetric key used between the reader and the MRTD is less than 80 bits and can easily be guessed. Regardless of the knowledge of this secret key, they also explained how an MRTD can be traced back to individuals or groups in the classical case of skimming. Hancke [8] and Carluccio et al. [6] reported in 2006 experimental attacks against BAC. Hancke showed a practical eavesdropping together with a relay attack, and Carluccio et al. emphasized on the traceability issue of MRTD. Liu et al. [18] explained how to make a passive decryption attack. Danev, Heydt-Benjamin and Čapkun [7] demonstrated in 2009 how to uniquely identify MRTD through the physical-layer of RFID tags. They explained that this fact can help in the determination of cloned passport while on the other hand supress location privacy.

Hlaváč and Rosa [10] studied in 2007 the case of Active Authentication (AA) and presented a man-in-the-middle cloning attack against AA. AA is also subject to challenge semantics attacks as shown in [32].

Lehtonen et al. [16] proposed in 2006 a potential solution for MRTD. As a necessary optical contact has to be achieved between a reader and the MRTD, to retrieve the MRZinfo, they proposed to combine with the actual RFID chip an optical memory device. This later will enable the establishment of a secure channel as a line of sight is necessary. Hence eavesdropping and skimming will no longer be possible. Herrigel and Zhao [9] proposed to use a digital watermarking technique to increase the seed entropy which is readable by optical scanning. However the main disadvantage of these two papers is that a hardware change has to be done on passports.

Vaudenay and Vuagnoux [35] presented in 2007 a survey on existing protocols for MRTD and their corresponding weaknesses, namely the ICAO standards (BAC and AA) and the EU standard (EAC). Lekkas and Gritzalis [17] worked in 2007 on the possibility to use the ICAO standard in order to build a globally interoperable Public Key Infrastructure. However they came up with negative conclusions due to several lacks such as the lack of passport revocation mechanism. Pasupathinathan, Pieprzyk and Wang [28, 29, 30] achieved in 2008 a formal security analysis on the Australian e-passport and identified several flaws in EACv1, after which they proposed an enhanced version called OSEP. They introduced the need to execute terminal authentication before chip authentication. Abid and Afifi [1] in 2008 incorporated in OSEP the use of elliptic curves.

All these research pushed the "Bundesamt für Sicherheit in der Informationstechnik", in charge of the EAC standardization, to present a new version (EACv2) in October 2008 and to add minor changes in May 2009 (version 2.01).

Nithyanand [27] released in 2009 a first survey on EACv2, that claimed that EACv2 solved all the previous problems except the vulnerability of reading a passport with an outdated date by a reader with an expired certificate. Unfortunately this is not the only problem left with EACv2.

Monnerat, Vaudenay and Vuagnoux [25] focused in 2007 on the privacy concerns attached to the release of passport Security Object Document (SOD). It leaks the hash of protected data groups and also evidence on private data. (See also [34]) Monnerat, Pasini and Vaudenay [24] constructed in 2009 an Offline Non-Transferable Authentication Protocol to achieve a Zero-Knowledge proof of knowledge of a valid SOD.

Structure of the paper The aim of this paper is to provide a general survey on the MRTD standard evolution and explain what are the remaining problems. Moreover we will propose directions for the next generation in order to suppress these problems. We will first explain and give the drawbacks of the RFID, the ICAO standard, the EACv1 and the EACv2 respectively in section 2, 3, 4 and 5. In section 6 we will provide our potential solutions and conclude in section 7.

2 ISO Standard for RFID

In order to discover the RFID tags in proximity, according to the ISO standard for RFID [12], readers send a discovery signal. Any RFID tag receiving this signal will reply with a specific identifier in order to allow readers to enter in communication with them. For regular RFID tags, this identifier is constant to enable an easy way to track chips. However this property is not always desirable for tags especially when location privacy needs to be protected. This the case for MRTD. The solution proposed by the ISO standard is to use a session-dependent randomly generated identifier. This solution has been adopted by almost all countries. Unfortunately, there are discrepancies in the way it is implemented [25]. There are other protocol implementation differences such as availability of optional features, lower layer protocols ar speed of transmission which allow to identify a passport

nationality [35].

It is a well known fact that privacy must be addressed accross all protocol layers [4]. As a matter of fact, recent work by Danev et al. [7], shows that any RFID tag can be accurately identified according to his physical-layer communication properties, namely by some kind of radio fingerprint. Although their work uses this property to enable cloning detection, the straightforward drawback is the tag tracking possibility.

Furthermore, the distance to eavesdrop or to interact with RFID tags is highly underestimated. According to an announcement from the Swiss Federal Office of Communication (OFCOM) [2] in November 2008, and even though currently commercialized readers can interact only within few centimeters, it would be possible by changing readers antenna to access MRTD from far away (up to 25 meters). In addition to this, radio communication between a legitimate reader and a passport induce a signal on the power line and can be captured 500 meters away.

3 ICAO Standard and BAC

Following the ICAO standard, passports must provide passive authentication for two mandatory data groups:

- Data group DG1 is a digital copy of the printed Machine Readable Zone (MRZ) which included some basic information about the holder: name, nationality, gender, date of birth, as well as passport serial number and expiration date.
- Data Group DG2 is a digital picture of the face which is optimized for automatic face recognition.

Passive authentication is performed by means of the Security Object of the Document (SOD), which is essentially a digital signature of the list of the hash of data groups together with the certificate of the verifying key. This certificate is computed by the issuing country and the root verifying key of the PKI is assumed to be authenticated by special protocols. Following the state of the art on cryptography, digital signatures are unforgeable so identities can no longer be forged by malicious people.

Biometric identification is mostly performed by 2D facial recognition, and soon by fingerprint as well. It could use iris recognition but this technology does not seem to be implemented yet. One problem is that 2D-facial recognition is pretty weak and that fingerprint could be fake. Fake fingerprint can be made using candy [23] or medecine against constipation [5].

Passports could limit themselves to providing DG1, DG2, and SOD in a pretty passive way. Indeed, it could have been printed using 2D barcode. But ICAO preferred RFID-based technology to accommodate more data and functionalities. Radio access then opened the way to privacy threats and require passports to implement some access control.

The ICAO standard includes an optional Basic Access Control (BAC), based on 3DES [3], which essentially consists in making the reader prove that it knows some piece of infor-

mation on the printed MRZ. This information called MRZinfo consists of the passport serial number, the date of birth of the person, and the expiration date of the passport. That is, BAC uses symmetric-key cryptography with an access key which is printed on the passport. Furthermore, MRZinfo has a pretty low entropy (following [20], an entropy of roughly 56 bits). So far, BAC is implemented in every passports we have seen.

BAC is followed by some key agreement to open secure messaging. Again, it is all based on symmetric cryptography with a low-entropy initial key (the MRZinfo), so it does not resist to passive adversaries.

The ICAO standard also includes an optional Active Authentication (AA) protocol which is based on a digital signature scheme. It protects against cloning attacks but is time-consuming for the powerless chip. As far as we know, it is only implemented in Belgium and the Czech Republic. Moreover AA is not secure against man-in-the-middle attacks [10] and leads to privacy concerns by adding semantics within the challenge [33].

Clearly, the advantages of the ICAO passports is that identities are unforgeable and that access to the chip requires knowing MRZinfo. Unfortunately, there are many drawbacks.

First of all, the cryptographic protocols do not resist passive adversaries. Since AA is seldom used, it does not resist to cloning attacks. Furthermore, MRZinfo grants an unlimited permanent access: once the adversary gets it, she can access to the chip without the consent of the holder. Contrarily to popular belief, the release of DG2 and SOD is not privacy insensitive. Releasing DG2 means releasing an optimized picture which is used as a reference template for biometric recognition. Once an adversary gets it, he can train himself to match the template, so releasing DG2 can ease identity theft. Hence the assumption 2.3 in section IV of [20] is wrong.

> The digitally stored image of the face is assumed not to be privacy-sensitive information. The face of the MRTD holder is also printed in the MRTD and can be readily perceived.

In addition to this, releasing SOD means providing transferable evidence of the correctness of the identity. For instance, it could be used as an undeniable proof for true date of birth for someone who tries to make his age a taboo.

4 EAC v1

The European EAC standard [32] was made to add better protection for non-mandatory data groups such as DG3: the fingerprint template. It includes

- secure messaging based on ECDH [31];
- a chip authentication protocol, protecting against cloning attacks;
- a terminal authentication protocol.

Terminal authentication is meant to be mandatory for accessing non-mandatory data groups, but mandatory data groups must remain readable without EAC due to the ICAO standard.

In the terminal authentication protocol, the reader proves that he owns the secret key associated to a given public key. Typically, this proof consists of signing a challenge from the passport. The public key has a certificate chain whose root belongs to the home country of the passport. That is, authorization is given to readers by signing a certificate with a given validity period. One problem is that passports do not have any reliable clock. So, they keep in memory a trusted past date which plays the role of a clock. When they check the validity of a certificate, they just check that the expiration date is posterior to the clock value. If verification succeeds and the issuing date of the certificate is posterior to the clock value, the clock value is replaced. Clearly, passports which do not run terminal authentication often will not even have a reliable approximation of a clock. Others may have a date which is precise within a few weeks. Consequently, a terminal certificate may be usable a long time after expiration to read passports.

The details of the general PKI required to authenticate readers at terminal station is described in the EACv2 standard [33].

The advantage of EAC is that we now have anti-cloning protection, a better key agreement resisting passive adversaries, and we can handle time-limited privileges to different readers. A problem is that revocation is based on a pretty weak clock. We still have privacy issues related to releasing DG2 and SOD to anyone. Also, the hash of protected data groups leaks from the SOD [33].

5 EACv2

EACv2, released in 2008 then updated in May 2009, describes among other specifications the PKI for terminals. This PKI is composed of three types of entities, namely Country Verifying Certificate Authorities (CVCAs), Document Verifiers (DVs) and Terminals. Every country will be required to have its own CVCA issuing MRTD and DV Certificates. DVs are organizational units within countries. Their role is to enable the certification link between its terminal readers and CVCAs. Hence they need to apply for a DV Certificate at each CVCAs corresponding to the country of MRTD that might be encountered by its Terminals. DVs are also in charge of creating and maintaining Terminal Certificates for each Terminal location. The validity period and the access rights of the terminal certificate are inherited from the DV Certificate. Obviously, these restrictions can be further reduced by the decision of the DV in charge of the terminal. Equivalently, the validity period and the access rights contained in the DV certificate is decided by the CVCA issuing the certificate.

The access rights for all data groups is encoded in binary in each certificate as an object identifier according to the role of the certificate holder (inspection systems, authentication terminals or signature terminals). A member in the certificate chain cannot provide more access rights than what it has itself. Thus to determine the access rights of a partic-

ular reader, the MRTD has to compute the boolean AND of all the binary authorization contained in the certificate chain.

EACv2 resolves one of the issue of EACv1, namely the privacy issue linked to releasing DG1, DG2, and SOD. The main difference introduced is in the order of authentication between a chip and the terminal that is attempting to read it. In this new specification the terminal authentication must be performed before the chip authentication. EACv2 even introduces a replacement for BAC, namely PACE. PACE is a state-of-the-art password-based access control resisting active attacks. Another improvement is that the access password for PACE is now a specific secret printed inside the passport and no longer any private data which has other purposes such as MRZinfo.

This modification could be considered at a first glance as a major improvement. Indeed by forcing authentication of the terminal before the chip authentication, we restrict the release of DG2 and SOD only to officially allowed terminals. However this is not the case in a full view of the specifications. By reading carefully the specifications of the EACv2 in [33], we can read in section 3.1.1 the following note:

> **Note:** According to this specification it is RECOMMENDED to require Extended Access Control to be used even for less-sensitive data. If compatibility to ICAO [20, 21] is REQUIRED, the MRTD chip SHALL grant access to less-sensitive data to terminals authenticated by Basic Access Control. The relevant inspection procedures are described in Appendix G.

What this note states is that if compatibility to ICAO is required then the MRTD must behave as in the ICAO standard. In other words, any fake terminal reader can require from the MRTD to use the crippled ICAO standard.

Furthermore the date contained in the MRTD is still an approximation of the current date. The date is updated only with national domestic certified dates, i.e. certificate effective dates (date of the certificate generation), contained in a national domestic CVCA certificate, a DV authorization certificate issued by the national domestic CVCA, or an accurate terminal certificate, i.e. a terminal certificate issued by an official domestic DV. As an MRTD will rarely encounter a domestic terminal, it is more likely that its date will be updated through the certificate effective date contained in a foreign DV. Hence the revocation of terminals is not fully solved.

6 Directions for the Next Generation

RFID switch In order to avoid traceability of passports, the current solution that people have is to place their MRTD in a faraday cage. Obviously this solution is cumbersome. For the case of biometric passport a better solution would be to incorporate an RFID switch to desactivate the chip. Some sensors could also detect if the passport is opened or closed and manipulate the switch accordingly. When the passport is closed the RFID tag

would simply ignore all discovery signals sent by readers and in order to interact with the passport, the later would need to be opened. This solution is logical as the access password for PACE printed inside the passport is supposed to be scanned by border patrols.

BAC abolishment Several changes need to be brought in the current EACv2 specifications. The fist element to take into consideration is that BAC should be abolished. In order to comply with the ICAO standard, the later should stop mandating DG1, DG2 and SOD available without EAC. EAC has to be imposed outside Europe in order to fully deploy its capacity. As for the EAC and ICAO standards, it only requires dropping a few lines in the documents.

Deployment does not necessarily imply a heavy PKI for terminals. A country not ready to have such a PKI could still use a dummy one with a single key shared to all readers. The passport issuing country, aware of it, could adjust the read access to mandatory data groups and keep the possibility to stop renewing a certificate for this key if the reading country does not make enough efforts to avoid leakage of the secret key. EAC-reading is a matter of software update and is inexpensive. Therefore, the only obstacle to making pure EAC mandatory is purely political.

Time-based revocation To be more accurate on the date contained in the MRTD, we propose to have identity checks even when leaving a domestic country or a community space if the community space members trust each others. For instance, some domestic clock-update booths could be made available on a voluntary basis before departure. As the identity check will correspond to an interaction with an accurate terminal, the date in the MRTD will be updated with the terminal certificate effective date. The date contained in the MRTD is still an approximation in this scenario, however with reduced date error when compared to EACv2. Finally, future chips might be equipped with a real clock.

Repetition-based revocation To decrease the issue of terminal corruption, terminal authentication could be improved by using reputation-based trust mechanisms. For instance the current terminal authentication would be appended by a $(t, n, \tau, \eta)-$threshold authentication proof, where a terminal can authenticate itself only if it collaborates with t neighbor connected terminals out of n and τ DV out of η. After completion of their proof, terminals should not be able to become offline for next authentication proofs. This add-on will resolve the problem of a single stolen terminal as a malicious party will have to corrupt at least t terminals and τ DV. However note that this solution does not resolve the case where a whole country is corrupted and no more trusted.

The ultimate trust mechanism would be an authentication proof involving the home CVCA. That is, passport would communicate to their own authority to check revocation status (like OCSP [26]).

7 Conclusion

In conclusion we can attest on the improvement brought by EACv2 with their new specifications. However further work is still needed. For instance as retrocompatibility is enabled in the MRTD to use ICAO with BAC instead, the whole security meaning behind EAC falls. The last issue concerns terminal revocations. Due to the inexactitude of date in MRTD, a terminal can fake its authentication even after its expiration date in his certificate. The frequency of date modification in MRTD is clearly not enough. A solution may be based on a threshold authentication proof in terminal authentications. Maybe future technologies will make it possible to have a real clock in passports, which would make easier solutions feasible.

Another remaining big concern relates to the overall RFID technology. Currently, it is easy to distinguish passports from different countries without any direct contact. The only way to protect against it is to prevent the chip from responding. That is, an on/off switch must be missing, or at least a sensor which switches off the chip when the passport is closed.

References

[1] M. Abid, H. Afifi. Secure E-Passport Protocol Using Elliptic Curve Diffie-Hellman Key Agreement Protocol. In *Proceedings of the 2008 The Fourth International Conference on Information Assurance and Security (IAS'08)*, Washington, DC, USA, pp. 99–102, IEEE, 2008.

[2] Abklärungen über die Datenauslesung auf Distanz beim biometrischen Pass. *Bundesamt für Kommunikation BAKOM*, 28 November 2008. `http://www.schweizerpass.admin.ch/etc/medialib/data/passkampagne/e-paesse.Par.0004.File.tmp/Messbericht_Bakom.pdf`

[3] ANSI X9.52. Triple Data Encryption Algorithm Modes of Operation. ANSI. 1998.

[4] G. Avoine, P. Oechslin. RFID Traceability: A Multilayer Problem. In *Financial Cryptography and Data Security, 9th International Conference (FC 2005)*, Roseau, The Commonwealth of Dominica, Lecture Notes in Computer Science 3570, pp. 125–140, Springer-Verlag, 2005.

[5] C. Barral, A. Tria. Fake Fingers in Fingerprint Recognition: Glycerin Supersedes Gelatin. In *Formal to Practical Security: Papers Issued from the 2005-2008 French-Japanese Collaboration*, Lecture Notes in Computer Science 5458, pp. 57–69, Springer-Verlag, 2009.

[6] D. Carluccio, K. Lemke-Rust, C. Paar, A.-R. Sadeghi. E-Passport: The Global Traceability or How to Feel Like an UPS Package. In *Information Security Applications (WISA'06)*, Juju Island, Korea, Lecture Notes in Computer Science 4298, pp. 391–404, Springer-Verlag, 2007.

[7] B. Danev, T.S. Heydt-Benjamin, S. Čapkun. Physical-layer Identification of RFID Devices In *Proceedings of the 18th USENIX Security Symposium (USENIX'09)*, Montreal, Canada, pp. to appear, USENIX, 2009.

[8] G.P. Hancke. Practical Attacks on Proximity Identification Systems (Short Paper). In *2006 IEEE Symposium on Security and Privacy (S&P'06)*, Berkeley, CA, USA, pp. 328–333, IEEE, 2006.

[9] A. Herrigel, J. Zhao. RFID identity theft and countermeasures. *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, vol. 6075, pp. 366–379, 2006.

[10] M. Hlaváč, T. Rosa. A Note on the Relay Attacks on e-Passports: the Case of Czech e-Passports. Technical reports 2007/244. IACR.
http://eprint.iacr.org/2007/244

[11] J.-H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk, R. Wichers Schreur. Crossing Borders: Security and Privacy Issues of the European e-Passport. In *Advances in Information and Computer Security, First International Workshop on Security (IWSEC'06)*, Kyoto, Japan, Lecture Notes in Computer Science 4266, pp. 152–167, Springer-Verlag, 2006.

[12] ISO/IEC 14443. Identification Cards — Contactless Integrated Circuit(s) Cards — Proximity Cards. ISO. 2001.

[13] A. Juels, D. Molnar, D. Wagner. Security and Privacy Issues in E-Passports. In *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm'05)*, Washington, DC, USA, pp. 74–88, IEEE, 2005.

[14] G. S. Kc, P. A. Karger. Preventing Attacks on Machine Readable Travel Documents (MRTDs). *Cryptology ePrint Archive*, Report 2005/404.

[15] M. Kosmerlj, T. Fladsrud, E. Hjelmås, E. Snekkenes. Face Recognition Issues in a Border Control Environment. In *Advances in Biometrics, International Conference (ICB 2006)*, Hong Kong, China, Lecture Notes in Computer Science 3832, pp. 33–39, Springer-Verlag, 2006.

[16] M. Lehtonen, T. Staake, F. Michahelles, E. Fleisch. Strengthening the Security of Machine Readable Documents by Combining RFID and Optical Memory Devices. Presented at *Developing Ambient Intelligence: Proceedings of the First International Conference on Ambient Intelligence Development (Amid'06)*, 2006. In *Developing Ambient Intelligence: Proceedings of the First International Conference on Ambient Intelligence Development (Amid'06)*, Sophia Antipolis, France, pp. 253–267, Springer, 2006. to appear in International Journal of Information Security (IJIS)

[17] D. Lekkas, D. Gritzalis. E-Passports as a Means Towards the First World-Wide Public Key Infrastructure. In *Public Key Infrastructure, 4th European PKI Workshop: Theory and Practice (EuroPKI 2007)*, Palma de Mallorca, Spain, Lecture Notes in Computer Science 4582, pp. 34–48, Springer-Verlag, 2007.

[18] Y. Liu, T. Kasper, K. Lemke-Rust, C. Paar. E-Passport: Cracking Basic Access Control Keys. In *On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS (OTM Confederated International Conferences CoopIS, DOA, ODBASE, GADA, and IS 2007)*, Vilamoura, Portugal, Lecture Notes in Computer Science 4804, pp. 1531–1547, Springer-Verlag, 2007.

[19] Machine Readable Travel Documents. Development of a Logical Data Structure — LDS For Optional Capacity Expansion Technologies. Version 1.7. International Civil Aviation Organization. 2004.
http://www.icao.int/mrtd/download/technical.cfm

[20] Machine Readable Travel Documents. Part 1: Machine Readable Passport, Specifications for Electronically enabled Passports with Biometric Identification Capabilities. International Civil Aviation Organization. ICAO Doc 9303, 2006.
http://www2.icao.int/en/MRTD/Pages/default.aspx

[21] Machine Readable Travel Documents. Part 3: Machine Readable Official Travel Documents, Specifications for Electronically enabled Official Travel Documents with Biometric Identification Capabilities. International Civil Aviation Organization. ICAO Doc 9303, 2008. http://www2.icao.int/en/MRTD/Pages/default.aspx

[22] Machine Readable Travel Documents. PKI for Machine Readable Travel Documents offering ICC Read-Only Access. Version 1.1. International Civil Aviation Organization. 2004. http://www.icao.int/mrtd/download/technical.cfm

[23] T. Matsumoto. Gummy and Conductive Silicone Rubber Fingers. In *Advances in Cryptology, 8th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2002)*, Queenstown, New Zealand, Lecture Notes in Computer Science 2501, pp. 574–576, Springer-Verlag, 2002.

[24] J. Monnerat, S. Pasini, S. Vaudenay. Efficient Deniable Authentication for Signatures. In *Applied Cryptography and Network Security, 7th International Conference (ACNS 2009)*, Paris-Rocquencourt, France, Lecture Notes in Computer Science 5536, pp. 272–291, Springer-Verlag, 2009.

[25] J. Monnerat, S. Vaudenay, M. Vuagnoux. About Machine-Readable Travel Documents: Privacy Enhancement Using (Weakly) Non-Transferable Data Authentication. In *International Conference on RFID Security 2007*, Málaga, Spain, pp. 13–26, University of Málaga, 2008.

[26] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams. 1999 *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*. RFC. RFC Editor.

[27] R. Nithyanand. The Evolution of Cryptographic Protocols in Electronic Passports. *Cryptology ePrint Archive*, Report 2009/200.

[28] V. Pasupathinathan, J. Pieprzyk, H. Wang. Formal Security Analysis of Australian E-passport Implementation. In *Sixth Australasian Information Security Conference (AISC 2008)*, Wollongong, NSW, Australia, pp. 75–82, ACS, 2008.

[29] V. Pasupathinathan, J. Pieprzyk, H. Wang. An On-Line Secure E-Passport Protocol. In *Information Security Practice and Experience, 4th International Conference (ISPEC 2008)*, Sydney, Australia, Lecture Notes in Computer Science 4991, pp. 14–28, Springer-Verlag, 2008.

[30] V. Pasupathinathan, J. Pieprzyk, H. Wang. Security Analysis of Australian and E:U: E-passport Implementation. *Journal of Research and Practice in Information Technology*, vol. 40, num. 3, pages 187–205, 2008.

[31] SEC 1: Elliptic Curve Cryptography. v1.0, Certicom Research, 2000. http://www.secg.org/secg_docs.htm

[32] Technical Guidelines TR-03110. Advanced Security Mechanisms for Machine Readable Travel Documents — Extended Access Control (EAC). Version 1.11. Federal Ministry of the Interior. Bundesamt für Sicherheit in der Informationstechnik. 2008.

[33] Technical Guidelines TR-03110. Advanced Security Mechanisms for Machine Readable Travel Documents — Extended Access Control (EAC). Version 2.01. Federal Ministry of the Interior. Bundesamt für Sicherheit in der Informationstechnik. 2009.

[34] S. Vaudenay. E-Passport Threats. *IEEE Security & Privacy*, vol. 5, num. 6, pages 61–64, 2007

[35] S. Vaudenay, M. Vuagnoux. About Machine-Readable Travel Documents. *Journal of Physics: Conference Series*, vol. 77, num. 012006, 2007. http://www.iop.org/EJ/article/1742-6596/77/1/012006/jpconf7i_77_012006.pdf

SAMLizing the European Citizen Card

(Extended Abstract)*

Jan Eichholz[1], Detlef Hühnlein[2], Jörg Schwenk[3]

[1] Giesecke & Devrient GmbH, Prinzregentenstraße 159, 81677 München,
jan.eichholz@gi-de.com

[2] secunet Security Networks AG, Sudetenstraße 16, 96247 Michelau,
detlef.huehnlein@secunet.com

[3] Ruhr Universität Bochum, Universitätsstr. 150, 44780 Bochum
joerg.schwenk@rub.de

Abstract: While the use of Federated Identity Management and Single Sign-On based on the Security Assertion Markup Language (SAML) standards becomes more and more important, there are quite a few European countries which are about to introduce national ID cards, which are compliant to the European Citizen Card (ECC) specification prTS 15480. The present contribution shows how these two seemingly opposite approaches may be integrated in a seamless and secure fashion such that it is possible to use the security features of the ECC in a federated scenario, which allows easy integration of Service Providers.

1 Introduction

In the area of Identity Management there seem to be two major trends at the moment, which are addressed in the EU funded project STORK[1]: On the one hand side, Federated Identity Management solutions are increasingly used in practice as they allow to implement Single Sign-On and facilitate the integration of Service Providers. The Security Assertion Markup Language (SAML), which has been developed by OASIS, plays a central role in the implementation of Federated Identity Management. On the other side quite a few European countries are about to introduce national ID cards, which are compliant to the European Citizen Card specification [CEN15480-1, CEN15480-2, CEN15480-3, CEN15480-4]. Hence it is natural to investigate how both approaches can be integrated such that systems which aim at implementing the eService directive [2006/123/EC] may combine the security of the ECC with the easy integration of Service Providers in SAML.

The rest of the paper is structured as follows: Section 2 explains how the ECC may be "SAMLized" and how an ECC-specific SAML-profile may look like, which may be used as starting point for the development of further specifications in STORK and standardization in CEN TC 224 WG 15 and/or OASIS Security TC. Within the full paper, a

*The full paper is available at http://www.ecsec.de/pub/SAMLizing-ECC.pdf.

[1] See www.eid-stork.eu

background chapter provides the necessary information on the Security Assertion Markup language and the European Citizen Card supporting the Extended Access Control (EAC) protocol [BSI-TR-03110(V2.01)] and briefly considers related work.

2 Secure Integration of the ECC into a SAML-environment

In order to implement the eService-Directive [2006/123/EC] it is necessary that European citizen are able to use their national identification token (e.g. an ECC-compliant ID-card) to authenticate at some eService in another EU Member State. As long as not all eServices across Europe directly support the ECC-compliant authentication protocols, such as EAC for example, the use of Federated Identity Management techniques, e.g. based on SAML, may ease the integration of eServices and hence facilitate the implementation of the eService-Directive. On the other side it is necessary to seriously analyze security aspects of such a construction, as a naive integration of a highly secure national ID-card into a SAML-environment may considerably degrade the overall security.

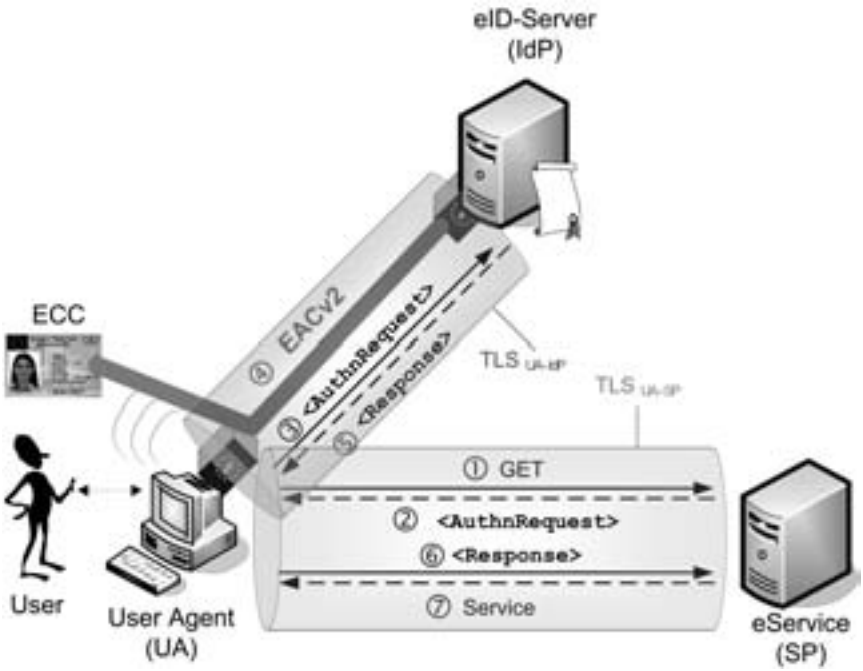


Figure 1: Combined ECC-3 and SAML architecture

As explained in Section 2.1 there are three main approaches for the secure integration of the European Citizen Card into a SAML-environment. First SAML may be bound to the involved TLS-sessions (cf. Section 2.2). Second the two TLS-sessions may be bound together and may be bound to the EAC-session (cf. Section 2.3). Third it is possible to

bind the SAML-Assertion directly to the EAC-protocol (cf. Section 2.4). Finally, the pros and cons as well as the possible combination of these approaches are discussed in Section 2.5.

2.1 Overview, requirements and threats

In order to allow Users, which are equipped with EAC-based eID tokens, to access the services of a Service Provider (SP), which only supports SAML, it is a straightforward approach to make use of a specific eID-Server, which supports both EAC and SAML and may serve as Identity Provider (IdP), which "translates" an EAC-based authentication context into an appropriate SAML-Assertion, which may be consumed by the Service Provider.

The applied protocol (see Figure 1) is very similar to the SAML-protocol for an enhanced client, which is capable of performing an EAC-based authentication in step 4. Furthermore it can be seen in Figure 1 that besides the EAC-channel between the ECC and the eID-Server there may be two TLS-channels (TLS_{UA-SP} between the User Agent and the Service Provider (eService) and TLS_{UA-IdP} between the User Agent and the Identity Provider (eID-Server)).

The major goal for the integration of the ECC into a SAML-environment is that the Service shall be accessible to the User (Agent) in step (7) if and only if an EAC-based authentication has been successfully performed in step (4). Furthermore it may be desirable to have the option to include cryptographic evidence into the SAML-Assertion transported in steps (5) and (6) such that it can be proved at a later point in time (e.g. at court) that the SAML-Assertion indeed was generated with a valid European Citizen Card (ECC).

However as explained in [SAML-SecP(v2.0)] there are a number of threats against SAML-based solutions, which need to be considered to end up with a secure system. We only consider man-in-the-middle (MitM) attacks and refer to [SAML-SecP(v2.0)] for other security aspects related to SAML.

If the TLS-channels are established in an anonymous mode, in which no X.509-certificates are used, it is clear that an attacker may mount a MitM-attack as depicted in Figure 2, steal the SAML-Assertion contain in the `Response`-element in order to impersonate the User at the eService.

In a similar fashion an attacker may mount a MitM-attack, if only the TLS-servers (i.e. the eID-Server, the eService and the attacker) are equipped with X.509-certificates and the User is not able to recognize the difference between the certificates presented within the TLS-handshakes. Note that this is a realistic assumption since studies have shown that typical internet users tend to ignore TLS security indicators [DTH06], and that it currently may even be possible to fake trustworthy looking TLS server certificates [SLW09].

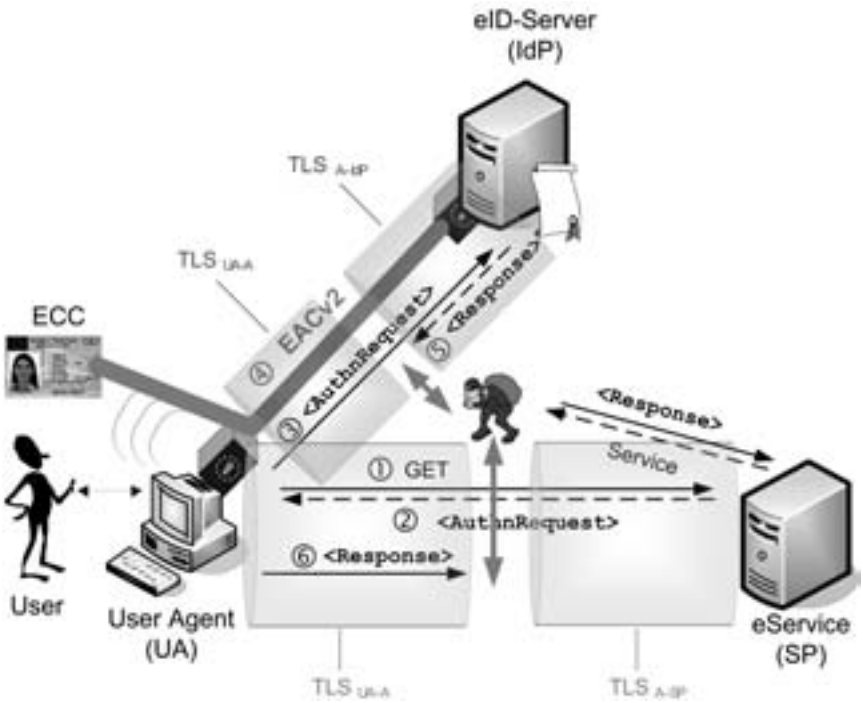


Figure 2: Man-in-the-Middle-Attack against SAML

2.2 Secure Binding of SAML to TLS

In order to thwart attackers, which try to steal a SAML token, e.g. Assertion or an Artifact, one may provide a cryptographic binding between the SAML token and the underlying TLS-channel.

In previous work, we identified three methods to bind SAML tokens to a specific TLS session. By binding the token to the session, the eService may deduce that the data he sends in response to the SAML token will be protected by the same TLS-channel, and will thus reach the same client who has previously sent the token.

- **TLS Federation [BHS08].** In this approach, the SAML token is sent inside an X.509 client certificate. The SAML token thus may replace other identification data like distinguished names. The certificate has the same validity period as the SAML token.
- **SAML 2.0 Holder-of-Key Web Browser SSO and Assertion Profile [SAML-HoKAP, SAML-HoKWebSSO].** Here again TLS with client authentication is used, but the client certificate does not transport any autorization information. Instead, the SAML token is bound to the public key contained in this certificate, by including this key in a Holder-of-Key assertion. The security of this approach has

independently been analyzed in [GJMS08].

- **Strong Locked Same Origin Policy [GLS2008].** Whereas the previous approaches relied on the server authenticating (in an anonymous fashion) the client, in this approach we strengthen the client to make reliable security decisions. This is done by using the servers public key as a basis for decisions of the Same Origin Policy, rather than the insecure Domain Name System.

2.3 Secure Binding of TLS to EAC

Since the EAC authentication can be performed over any communication link, it is even possible to successfully complete it over two TLS-channels between the User Agent and the eID-Service with a MitM-attacker in between (cf. Figure 2). Note that the MitM-attack does not affect the EAC-authentication itself, but only allows the attacker to intercept the SAML-Assertion, which is issued as a result of the EAC-authentication. In order to avoid this kind of attack one may include TLS-specific values in the EAC-protocol in order to provide a cryptographic binding between TLS and EAC.

For this purpose we first investigate *which* TLS-specific parameters may be included into the EAC protocol and then we briefly discuss *how* these values may precisely be incorporated into EAC such that the TLS- and EAC-channels are cryptographically tied together.

2.3.1 TLS-specific parameters for potential inclusion in EAC

We consider the following values from a TLS handshake for inclusion in EAC:

- **Certificates or other messages of the TLS-Handshake Protocol.** While it should be easy to access these values using a browser plugin or a server component, it would not be sufficient to use those parameters as they do not depend on both communication partners. Furthermore the used certificates are typically not session specific.
- **Premaster secret.** This value can only be used if a cipher suite using Diffie-Hellman key exchange is chosen. If RSA encryption is used, the MitM-attacker can simply decrypt the premaster secret chosen by the browser, and re-encrypt it for the server.
- **Master secret.** The master secret, or any value derived from it, can be used, since the two nonces sent by browser and server are used to compute it. While a derivation mechanism for the master secret is described in [Resc09] this mechanism does not seem to be supported by popular browsers.
- **Finished message.** Another approach would be to use one of the two Finished messages, since this value is derived from the master secret, and it is sent protected only by the TLS record layer. Thus it should be easy for a browser plugin, or a server component, to access it.

- **Pre-shared key between the eID-Server and eService.** In [BSI-TR-03112-7] it is described how to provide a binding between the two TLS-connections using a pre-shared-key (PSK) known to the eID-Server and the eService. The PSK may be generated by the eID-Server, the eService or both and is transported from the eService to the User Agent over the first TLS-channel (TLS_{UA-SP} in Figure 1) and used for the establishment of the second TLS-channel between the User Agent and the eID-Server (TLS_{UA-IdP} in Figure 1) as specified in [RFC4279].

  In addition to the binding of the two TLS-channels the PSK may also be used to provide a binding of the TLS-channels to the EAC-channel.

In particular the last two values seem to fulfill our requirements very well and may serve as input for a binding of TLS to EAC.

2.3.2 Integration of TLS-specific values into EAC

It remains to discuss how the TLS-specific values may be integrated into EAC. For this purpose there are the following general options induced by the structure of the EAC-protocol:

- **Terminal Authentication.** The Terminal Authentication (cf. [BSI-TR-03110(V2.01), Section 4.4]) roughly consists of the following three steps:

  1. As a first step in the Terminal Authentication protocol the ECC verifies the Card-verifiable-Certificate (CVC) provided by eID-Server.

     In order to provide a cryptographic link between the X.509 certificate used in TLS and the CVC used in EAC it would be possible to include (a hash value of) one certificate as an extension into the other certificate. For the inclusion of the CVC into an X.509-certificate one may use the `CVCert`-extension defined in [ISO18013-3, Section C.7.2.1]. In order to include the hash value of an X.509-certificate in a CVC it would be necessary to define a corresponding extension in an amendment of [BSI-TR-03110(V2.01), Annex C.3]. On the other side it would – from a theoretical point of view – be possible that the Card-verifiable-Certificates are directly used in TLS in a similar fashion as one may use OpenPGP-keys (cf. [RFC5081]).

  2. Next the eID-Server generates an ephemeral key pair, which is especially used in the Chip Authentication protocol described below. As explained in Section 2.4 the private ephemeral key may be derived from a secret, which is shared by the eService and the eID-Server.

  3. Finally a challenge is obtained from the ECC and signed by the eID-Server.

     This challenge contains an identifier derived from the ephemeral PACE-key of the ECC, a nonce generated by the ECC, an identifier derived from the ephemeral public key of the eID-Server which is generated in the previous step and possibly additional so called ”Authenticated Auxiliary Data” (AAD) (cf. [BSI-TR-03110(V2.01), Annex A.6.5]). The AAD are normally used for age verification, document validity verification and community ID verification,

but it seems to be possible to use the AAD to convey the TLS-specific value discussed above such that the TLS-channel is cryptographically bound to the EAC-channel, which effectively removes the MitM-attack described above (cf. Figure 2).

- **Chip Authentication.** In the Chip Authentication (cf. [BSI-TR-03110(V2.01), Section 4.3]) the static public key of the ECC and the ephemeral public key of the eID-Server generated in step 2 above is used to agree on a common key, which is used to derive secure messaging keys and authenticate the chip of the ECC. Without significant changing the protocol and the related smart card implementation it seems to be the only option to use the TLS-specific value as seed for the generation of the ephemeral private key of the eID-Server and the keys necessary to verify this construction would provide access to the secure messaging channel between the eID-Server and the ECC. Please refer to Section 2.4 for the use of this feature in the context of SAML.

2.4 Secure Binding of SAML to EAC

For sensitive use cases it may be necessary to enable the eService, which only has access to the SAML-Assertion, to verify that the authentication indeed has been performed using an authentic ECC and that the attributes conveyed in the SAML-Assertion indeed have been read out from the ECC in a secure EAC-session. In order to achieve this a cryptographic binding between SAML and EAC may be constructed as explained in the following.

The authentication of the ECC is achieved by the chip authentication protocol, which basically is a Diffie-Hellman (DH) key exchange using static keys on the chip side. The resulting keys are used for secure messaging later on. On the other side the eID-Server would usually generate an ephemeral DH key pair using a random seed. In our case however the ephemeral private key is derived from a shared key which has been agreed upon by the eService and the eID-Server. This allows the eService to add own random data to the key generation process and more importantly it allows the eService to verify that the authentication has been performed with a trustable ECC and that sensitive attributes contained in the SAML-Assertion indeed have been read out from the ECC in a secure EAC-session (see Figure 3).

Before sending the SAML `<AuthnRequest>` to the eID-Server, the eService generates an ephemeral DH key pair $(\tilde{S}K_{SP}, \tilde{P}K_{SP})$ and sends the public key $\tilde{P}K_{SP}$ together with the domain parameters $\mathcal{D}$ within the SAML `<AuthnRequest>` to the eID-Server. The additional data may be placed within the `<AuthnRequest>.<RequestedAuthnContext>.<AuthnMethod>.<AsymmetricKeyAgreement>` structure for example.

Upon receiving the `<AuthnRequest>` the eID-Server also generates an ephemeral DH key pair $(\tilde{S}K_{IdP}, \tilde{P}K_{IdP})$ using the domain parameters $\mathcal{D}$ chosen by the eService. Using $\tilde{P}K_{SP}$ and $\tilde{S}K_{IdP}$, the eID-Server calculates the common key which is used to derive the ephemeral private key $\tilde{S}K_{CA}$ and the corresponding $\tilde{P}K_{CA}$, which is used in the Chip Authentication protocol.

After the eID-Server has successfully performed the EAC protocol with the ECC, he received the data $(\mathcal{D}_{ECC}, PK_{ECC}, EF.CardSecurity, r_{ECC}, T_{ECC})$ from the ECC, which can be used to verify the genuineness of the ECC.

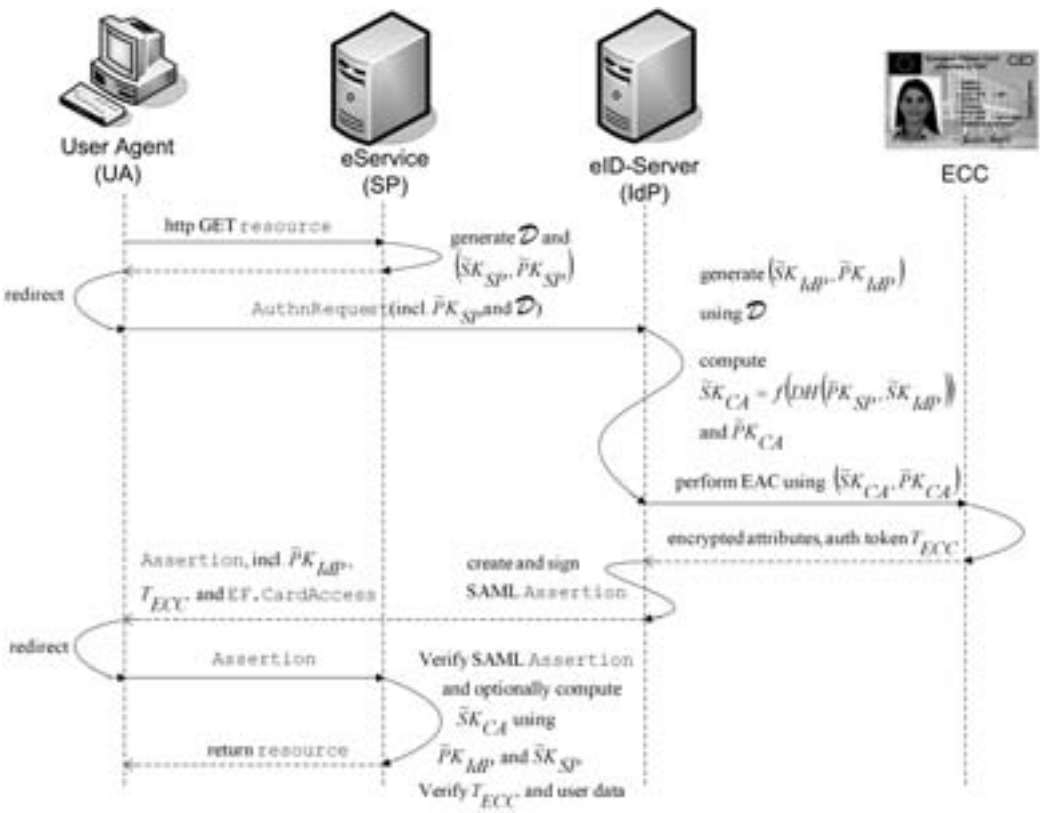


Figure 3: Command Flow for eService Authentication Token verification

Within the SAML response element `<Response>.<Assertion>.<AuthnStatement>.<AuthnContext>` – which is an instance of [SAML-Auth(v2.0), Section 3.4.15] – the necessary verification data can be placed and hence be made available to the eService. Using $\tilde{P}K_{IdP}$ and $\tilde{S}K_{SP}$ the eService is able to compute the private key $\tilde{S}K_{CA}$ used in the Chip Authentication protocol. Afterwards it may use $\tilde{S}K_{CA}$ and PK_{ECC} to compute the secure messaging keys and hence verify the validity of the authentication token T_{ECC}.

Since the eService now has the secure messaging keys of the EAC-channel, it may be possible that the eID-Server does not decrypt the data received from the ECC, but instead places the secure messaging cryptograms received from the ECC within an `Encrypted-`

`Attribute`-element within the Assertion. To retrieve the plain value of the attributes, the eService needs to decrypt the `EncryptedAttribute`-element with the derived secure messaging key.

2.5 Discussion of different approaches and recommendations

In this section it remains to discuss the different approaches presented above and derive recommendations for the secure integration of the European Citizen Card into a SAML-environment.

Since for example the mechanisms [SAML-HoKWebSSO, SAML-HoKAP] mentioned in Section 2.2 are independent from the applied authentication protocol they may of course be used in the ECC-context.

In case of an ECC which supports the EAC protocol however it is possible to provide a tighter and probably more secure binding between EAC, TLS and SAML.

Among the different options discussed in Section 2.3 one may in particular include TLS-specific values as additional "Authenticated Auxiliary Data" (AAD) into the Terminal Authentication step within the EAC protocol in order to provide a strong binding between TLS and EAC. If there is already a pre-shared key (PSK) between the eID-Server, the eService and the User Agent as required by [BSI-TR-03112-7] one may include (the hash value of) this value as AAD in EAC. Alternatively one may use the (hash value of the concatenation of the) Finished Messages of the TLS-channels as input to the EAC-protocol. While the eID-Server has direct access to the Finished Messages of TLS_{UA-IdP} the corresponding value for TLS_{UA-IdP} would need to be transported in encrypted form to the eID-Server and may be included in the optional `<Extensions>`-element within `<AuthnRequest>`.

Whether it makes sense to introduce a cryptographic link between the CVC used for EAC and the X.509-certificates used for TLS mainly depends on organizational aspects such as the respective certificate lifetime and involved enrollment procedures.

In order to provide a direct binding between SAML and EAC and especially if the eService requires a proof that the authentication was performed with a trustable ECC, it is highly recommendable to use the mechanism introduced in Section 2.4. This proposal seems to be especially attractive from a practical point of view as it may help to solve liability issues introduced by the delegation of the sensitive authentication step to the eID-Server.

Finally for maximum security one may combine the different proposals and link SAML to TLS (cf. Section 2.2), TLS to EAC (cf. Section 2.3) and SAML to EAC (cf. Section 2.4).

3 Conclusion

Based on the discussion in the previous sections it seems that the integration of the European Citizen Card into a SAML-environment has the potential to solve many open issues related to the acceptance of ECC based authentication protocols, fast deployment and easy integration into existing web service infrastructures, which already (are about to) use SAML.

However, the slightly increased complexity of the system introduces additional threats as an attacker may for example act as Man-in-the-Middle and steal the SAML-Assertion and finally impersonate the User which has been securely authenticated based on the ECC. In order to prevent such attacks various mechanisms have been proposed which provide a cryptographic binding between SAML, TLS and EAC. Furthermore the binding between SAML and EAC may be helpful to solve liability issues due to the introduction of the eID-Server acting as trusted third party.

To sum up we solved security problems which are also present in many other Federated Identity Management scenarios, we greatly simplify the introduction of ECC into existing web service infrastructures, and we introduced an approach which may help to solve liability issues related to the delegation of the sensitive authentication step.

References

[2006/123/EC] *Directive 2006/123/EC of the European Parliament and the Council of 12 December 2006 on Services in the Internal Market*. Official Journal of the European Union, L 376/36, 27.12.2006. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:376:0036:0068:EN:PDF, 2006.

[BHS08] BUD P. BRUEGGER, DETLEF HÜHNLEIN, and JÖRG SCHWENK. *TLS-Federation – A secure and Relying-Party-friendly approach for Federated Identity Management*. In *Proceedings of* BIOSIG 2008: Biometrics and Electronic Signatures, volume 137 of *Lecture Notes in Informatics (LNI)*, pages 93–104 (GI-Edition, 2008). http://www.ecsec.de/pub/TLS-Federation.pdf.

[BSI-TR-03110(V2.01)] FEDERAL OFFICE FOR INFORMATION SECURITY (BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK). *Advanced Security Mechanism for Machine Readable Travel Documents - Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI)*. Technical Directive (BSI-TR-03110), Version 2.01. http://www.bsi.bund.de/english/publications/techguidelines/tr03110/TR-03110_v201.pdf, 2009.

[BSI-TR-03112-7] FEDERAL OFFICE FOR INFORMATION SECURITY (BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK). *eCard-API-Framework – Protocols*. Technical Directive (BSI-TR-03112), Version 1.1, Part 7. http://www.bsi.bund.de/literat/tr/tr03112/, 2009.

[CEN15480-1] COMITÉ EUROPÉEN DE NORMALISATION (CEN). *Identification card systems - European Citizen Card - Part 1: Physical, electrical and transport protocol characteristics*. CEN/TS 15480-1 (Technical Specification), 2007.

[CEN15480-2] COMITÉ EUROPÉEN DE NORMALISATION (CEN). *Identification card systems - European Citizen Card - Part 2: Logical data structures and card services*. CEN/TS 15480-2 (Technical Specification), 2007.

[CEN15480-3] COMITÉ EUROPÉEN DE NORMALISATION (CEN). *Identification card systems - European Citizen Card - Part 3: European Citizen Card Interoperability using an application interface*. CEN 15480-3 (Working Draft), 2009.

[CEN15480-4] COMITÉ EUROPÉEN DE NORMALISATION (CEN). *Identification card systems - European Citizen Card - Part 4: Recommendations for European Citizen Card issuance, operation and use*. CEN 15480-4 (Working Draft), 2009.

[DTH06] RACHNA DHAMIJA, J. D. TYGAR, and MARTI HEARST. *Why phishing works*. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pages 581–590 (ACM, 2006). http://graphics8.nytimes.com/images/blogs/freakonomics/pdf/Why_Phishing_Works-1.pdf.

[GJMS08] SEBASTIAN GAJEK, TIBOR JAGER, MARK MANULIS, and JÖRG SCHWENK. *A Browser-based Kerberos Authentication Scheme*. In SUSHIL JAJODIA and JAVIER LÓPEZ (editors), *Computer Security - ESORICS 2008, 13th European Symposium on Research in Computer Security, Málaga, Spain, October 6-8, 2008. Proceedings*, volume 5283 of *Lecture Notes in Computer Science*, pages 115–129 (Springer, 2008).

[GLS2008] JÖRG SCHWENK, LIJUN LIAO, and SEBASTAN GAJEK. *Stronger Bindings for SAML Assertions and SAML Artifacts*. In *Proceedings of the 5th ACM CCS Workshop on Secure Web Services (SWS'08)*, pages 11–20 (ACM Press, 2008).

[ISO18013-3] *ISO/IEC 18013-1: Personal Identification – ISO Compliant Driving Licence – Part 3: Access control, authentication and integrity validation*. International Standard, 2009.

[Resc09] E. RESCORLA. *Keying Material Exporters for Transport Layer Security (TLS)*. IETF Internet Draft, v6. http://www.ietf.org/id/draft-ietf-tls-extractor-06.txt, July 2009.

[RFC4279] P. ERONEN and H. TSCHOFENIG. *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*. Request For Comments – RFC 4279. http://www.ietf.org/rfc/rfc4279.txt, December 2005.

[RFC5081] N. MAVROGIANNOPOULOS. *Using OpenPGP Keys For Transport Layer Security Authentication*. Request For Comments – RFC 5081. http://www.ietf.org/rfc/rfc5081.txt, November 2007.

[SAML-Auth(v2.0)] JOHN KEMP, SCOTT CANTOR, PRATEEK MISHRA, ROB PHILPOTT, and EVE MALER. *Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, 15.03.2005. http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf, 2005.

[SAML-HoKAP] TOM SCAVO. *SAML V2.0 Holder-of-Key Assertion Profile*. OASIS Committee Draft 02, 05.07.2009. http://www.oasis-open.org/committees/download.php/33236/sstc-saml2-holder-of-key-cd-02.pdf, 2009.

[SAML-HoKWebSSO] N. KLINGENSTEIN. *SAML V2.0 Holder-of-Key Web Browser SSO Profile*. OASIS Committee Draft 02, 05.07.2009. http://www.oasis-open.org/committees/download.php/33239/sstc-saml-holder-of-key-browser-sso-cd-02.pdf, 2009.

[SAML-SecP(v2.0)] FREDERICK HIRSCH, ROB PHILPOTT, and EVE MALER. *Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, 15.03.2005. http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf, 2005.

[SLW09] MARC STEVENS, ARJEN LENSTRA, and BENNE DE WEGER. *Chosen-prefix Collisions for MD5 and Applications*. Submitted to Journal of Cryptology. https://documents.epfl.ch/users/l/le/lenstra/public/papers/lat.pdf, June 2009.

Sanitizable Signatures: How to Partially Delegate Control for Authenticated Data

Christina Brzuska Marc Fischlin Anja Lehmann
Dominique Schröder

Darmstadt University of Technology, Germany
www.minicrypt.de

Abstract. Sanitizable signatures have been introduced by Ateniese et al. (ESORICS 2005) and allow an authorized party, the sanitizer, to modify a predetermined part of a signed message without invalidating the signature. Brzuska et al. (PKC 2009) gave the first comprehensive formal treatment of the five security properties for such schemes. These are unforgeability, immutability, privacy, transparency and accountability. They also provide a modification of the sanitizable signature scheme proposed by Ateniese et al. such that it provably satisfies all security requirement. Unfortunately, their scheme comes with rather large signature sizes and produces computational overhead that increases with the number of admissible modifications.

In this paper we show that by sacrificing the transparency property —thus allowing to distinguish whether a message has been sanitized or not— we can obtain a sanitizable signature scheme that is still provably secure concerning the other aforementioned properties but significantly more efficient. We propose a construction that is based solely on regular signature schemes, produces short signatures and only adds a small computational overhead.

1 Introduction

Digital signatures usually provide integrity and authenticity of digital data. This, in particular, implies that even slight modifications of the data make the signature invalid. There are, however, some cases where allowing such modifications while retaining the authenticity to a certain extend may be desirable. For example,

- Governmental organizations like the World Health Organization (WHO) may ask medical facilities to provide medical records for infectious disease surveillance programs. Allowing the administration of such facilities to sanitize parts of the records (which are authenticated by medical personal through signatures) like patient names or information about psychological treatments eases the overhead. At the same time it still marks the resulting data as authenticated by medical personal.
- Authenticated multimedia data like videos may require some editing, e.g., because of graphic content or to insert local commercials into the data.

- Authenticated routing information as in the Secure Border Gateway Protocol needs to be updated frequently, while the reliability of the data must be ensured.

As another example, consider the recent discussion about German identity cards and the digital data stored on the card [Bun08]. The data includes common information about the holder like the name, date of birth and address. These data are not signed, though, to guarantee deniability of transactions —else a party retrieving such signed data can show this as a proof for a transaction to third parties— and to possibly enable modifications by subordinate authorities to volatile data like the address (see [BKMN08]). Note that in the non-digital case local authorities today can easily change the address by placing an (authenticated) sticker on the identity card. In the digital case, any signature over the holder's data would prevent such modifications (unless the issuing authority would bequeath the signing key, which is of course not recommended).

Enter sanitizable signatures. The notion of sanitizable signatures has been introduced by Ateniese et al. [ACdMT05]. Similar notions have been considered concurrently by Steinfeld et al. [SBZ01] and Miyazaki et al. [MSI+03]. The idea behind sanitizable signatures is that the signer delegates the signing rights of parts of the message to a designated party, the sanitizer. The sanitizer, given a message and a signature of the signer, can then modify the predetermined parts of the message and still produce a valid signature for the new message. A verifier of this new signatures is then assured that (a) the fixed message parts have been authenticated by the signer, and (b) that only the designated sanitizer can make admissible modifications.

Sanitizable signature are thus an expedient solution to the scenarios above. For the digital identity card, for example, the issuing authority can delegate the rights to modify the address data to a local authority, but leave other data like the name or the date of birth immutable. Citizens would then be assured that the data has only been generated by (local or superior) authorities.[1]

Sanitizable signatures come with five security properties, described informally in [ACdMT05] and rigorously in [BFF+09]:

UNFORGEABILITY. Resembles the common unforgeability notion for regular signatures: besides the signer and the sanitizers no one should be able to produce signatures for new messages.

IMMUTABILITY. Confines the power of a malicious sanitizer, i.e., the sanitizer should not be able to change other parts of the message than the intended ones.

PRIVACY. Sanitization steps should remove *any* information about the original data of the sanitized parts. This is for instance important for the medical surveillance example, and usually holds in an information-theoretic sense.

[1] Note that this solves the modification problem but does not address the deniability issues discussed before. Still, for applications where the receiver is considered to be trustworthy, say, the police, deniability may be a minor issue. In addition, since our solution below is for example rather generic, it can potentially be combined with privacy-enhancing solutions in order to overcome the deniability problem.

ACCOUNTABILITY. In case of a dispute about the origin each party can contribute to settle the dispute. A malicious signer or sanitizer cannot frame the other party.

TRANSPARENCY. One cannot distinguish between signatures created by the signer or the sanitizer.

The aforementioned work of Brzuska et al. [BFF+09] defined these properties with game-based definitions and gave a construction based on the protocol in [ACdMT05], provably meeting these five requirements. The signature length, however, is quite large and the computational overhead grows with the number of admissible modifications. The construction also relies on specific number-theoretic assumptions.

Our results. We show that dropping the transparency requirement —thus allowing to distinguish genuine signatures of the signer from signatures produced by the sanitizer— yields significantly more efficient solutions: We present a construction allowing short signatures, signature generation time comparable to regular signatures and based on arbitrary (but secure) signature schemes.

Basically, the signer in our construction signs the fixed message parts m_{FIX} and the description of the admissible modifications ADM together with the sanitizer's public key pk_{san} to get a signature σ_{FIX}. In addition, the signer generates another signature σ_{FULL} for the entire message (including modifiable parts). Then the full signature is given by $\sigma = (\sigma_{\text{FIX}}, \sigma_{\text{FULL}}, \text{ADM}, pk_{\text{san}})$.

To sanitize the message and replace (some of) the modifiable message parts the sanitizer changes the message m to m' accordingly and then creates the new signature σ' by signing m' with its signing key and replacing σ_{FULL} by the derived signature σ'_{FULL}. The entire signature for the sanitized message is given by $\sigma' = (\sigma_{\text{FIX}}, \sigma'_{\text{FULL}}, \text{ADM}, pk_{\text{san}})$.

We show that the construction above achieves unforgeability, immutability, accountability and privacy. It is clearly *not* transparent as one can easily distinguish under whose public key the second signature component verifies. As for the identity card example, transparency is usually neither provided by the solutions for "non-digital" identity cards, because the sticker is clearly visible given the card. Still, transparency may be a desirable security goal in some settings, say, if a recent change of the address entails discrimination. An example might be a landlord who is only willing to rent out to tenants which have not moved recently.

Our solution comes with several advantages over previous approaches, besides its generality and efficiency improvements. First, since we analyze the solution in terms of the security notions of [BFF+09] for sanitizable signatures, the solution really guarantees the desired goals, and these formally stated goals can be scrutinized. Also, our solution allows handy hierarchical extensions. That is, the sanitizer is allowed to change parts of a message, and can authorize a subordinate authority to modify some of these parts. To this end, the sanitizer issues certificates for public keys of local authorities such that they can make further modifications by replacing the second signature component and appending their public key together with the certificate to the signature.

2 Outline of the Construction

Our construction works as follows: Both the signer and the sanitizer each hold a key pair $(sk_{\text{sig}}, pk_{\text{sig}})$ and $(sk_{\text{san}}, pk_{\text{san}})$, respectively, of a secure signature scheme. The signature schemes used by the signer and the sanitizer can be distinct but we use the same scheme for sake of simplicity. To sign a message m and allowing modifications by the sanitizer with public key pk_{san}, the signer first picks a description ADM of the admissible message parts which are changeable by the sanitizer, and those parts m_{FIX} which are fixed. Then the signer computes the signature by signing the fixed part and the entire message (prepended with a bit to indicate the difference):

$$\sigma = (\sigma_{\text{FIX}}, \sigma_{\text{FULL}}) = (\mathsf{Sign}(sk_{\text{sig}}, (0, m_{\text{FIX}}, \text{ADM}, pk_{\text{san}})),\ \mathsf{Sign}(sk_{\text{sig}}, (1, m, pk_{\text{san}}, pk_{\text{sig}}))).$$

We assume that ADM (and possibly pk_{san}, if not linked to the signature somewhere else) become part of the signature. As an example, ADM might be of the form $(t, 6, 110000)$, indicating that a message consists of 6 blocks, each of bit length t and the sanitizer is allowed to change the first two blocks.

The sanitizer can now modify the message, yielding message m', and replace the signature part σ_{FULL} with a self-generated signature under pk_{san} (but leaving σ_{FIX} untouched):

$$\sigma' = (\sigma_{\text{FIX}}, \sigma'_{\text{FULL}}) = (\sigma_{\text{FIX}}, \mathsf{Sign}(sk_{\text{san}}, (1, m', pk_{\text{san}}, pk_{\text{sig}}))).$$

To verify a signature σ resp. σ' for a message m with respect to pk_{sig} the verifier first recovers the fixed part m_{FIX} by inspecting ADM. Then the verifier checks the validity of the signature part σ_{FIX} with respect to $(0, m_{\text{FIX}}, \text{ADM}, pk_{\text{san}})$, and then verifies that the second part of the signature either verifies under the signer's or the sanitizer's public key. If both properties hold then the verifier accepts.

Let us briefly revisit the security notions for sanitizable signatures [ACdMT05, BFF+09] and discuss if the scheme above achieves these notions. A formal approach follows in the next section.

UNFORGEABILITY. We need to argue that no one except for the signer and the designated sanitizer can create valid signatures for new messages. The unforgeability of the underlying signature scheme guarantees that one cannot forge signatures for the fixed part, including pk_{san}, and thus any forgery for the second part must necessarily be either for the sanitizer's public key or the signer's public key. But then the unforgeability of the sanitizer's and signer's signatures guarantee security for our sanitizable scheme. Note that prepending the bit 0 and 1 to the messages in the two signatures prevents "mix-and-match" attacks in which the adversary abuses the first signature component for the second part.

IMMUTABILITY. Guarantees that a malicious sanitizer cannot change inadmissible blocks. This follows from the unforgeability of the signer's scheme, protecting the fixed part of the message.

PRIVACY. Message parts which are replaced cannot be recovered, because the sanitizer removes those parts and signs the derived message from scratch. The information about the original data is hidden information-theoretically.

ACCOUNTABILITY. Neither party can claim that a message-signature pair originates from the other party, unless this party has really signed the corresponding message before. This again follows from the unforgeability of the underlying signature scheme. Note that, in practice, this may require some certification of the owner of the sanitizer's public key pk_{san}, or else the signer could create fake public keys on behalf of the sanitizer.

TRANSPARENCY. Does not hold. One can easily distinguish signatures generated by the signer from those produced by the sanitizer by inspecting the second signature part.

An interesting feature of the solution above is that the sanitizer itself can now act as a certificate authority and delegate rights further. To allow a subordinate sanitizer the sanitizer now acts as the signer and generates σ_{FULL} as $(\sigma^{\text{san}}_{\text{FIX}}, \sigma^{\text{san}}_{\text{FULL}})$ by dividing the message further into a part $m^{\text{san}}_{\text{FIX}}$ which the subordinate sanitizer should not be allowed to change, and into a variable part. The lack of transparency then again allows to decide upon the origin.

3 Technical Details of the Construction

We first present the formal structure of sanitizable signatures and then introduce our construction according to this structure. We next discuss the security notions in detail and finally show that our construction is secure according to these notions.

3.1 Sanitizable Signatures

The following definitions are taken from [BFF+09]. With our solution in mind, we simplify the presentation whenever possible. For example, our solution does not require an explicit Proof algorithm to identify the origin (signer or sanitizer), so we drop it from the formal descriptions.

Recall that our construction is based on a regular signature scheme $\mathcal{S} = (\mathsf{SKGen}, \mathsf{SSign}, \mathsf{SVf})$ which consists of three efficient algorithms where SKGen on input 1^n, the security parameter in unary, returns a key pair (sk_0, pk_0); algorithm SSign on input sk_0 and a message $m \in \{0,1\}^*$ returns a signature σ; and algorithm SVf for input pk_0, m, σ returns a decision bit d for accept ($d = 1$) or reject ($d = 0$). We assume completeness in the sense that any signature generated via SSign is also accepted by SVf. *Unforgeability under adaptive chosen message attacks* of regular signature schemes says that for any efficient algorithm $\mathcal{A}$ the probability that $\mathcal{A}$ with input pk_0 and access to a signing oracle $\mathsf{SSign}(sk_0, \cdot)$ for $(sk_0, pk_0) \leftarrow \mathsf{SKGen}(1^n)$ outputs a pair (m^*, σ^*) such that $\mathsf{SVf}(pk_0, m^*, \sigma^*) = 1$ and m^* has never been submitted to the signing oracle, is negligible.

A sanitizable signature scheme SanSig is now a tuple of efficient algorithms $(\mathsf{KGen}_{\text{sig}}, \mathsf{KGen}_{\text{san}}, \mathsf{Sign}, \mathsf{Sanit}, \mathsf{Verify}, \mathsf{Judge})$ such that:

KEY GENERATION. The key generation algorithms for the signer and sanitizer, respec-

tively, allows both parties to generate key pairs (for security parameter n, given as input):

$$(pk_{\text{sig}}, sk_{\text{sig}}) \leftarrow \mathsf{KGen}_{\text{sig}}(1^n), \qquad (pk_{\text{san}}, sk_{\text{san}}) \leftarrow \mathsf{KGen}_{\text{san}}(1^n)$$

SIGNING. The signing algorithm of the signer takes the signer's secret key sk_{sig}, a message $m \in \{0,1\}^*$ the public key pk_{san} of the designated sanitizer and a description ADM (used to identify the fixed part m_{FIX} of m). It outputs a signature (or $\perp$, indicating an error):

$$\sigma \leftarrow \mathsf{Sign}(m, sk_{\text{sig}}, pk_{\text{san}}, \text{ADM}).$$

We assume that ADM, pk_{san} are recoverable from any signature $\sigma \neq \perp$.

SANITIZING. The sanitizer's algorithm Sanit takes a message $m \in \{0,1\}^*$, a signature σ, the public key pk_{sig} of the signer and the secret key sk_{san} of the sanitizer. It first modifies the message m according to the modification instruction MOD and then computes a new signature σ' for the modified message m'. It outputs m' and σ' (or possibly $\perp$ in case of an error).

$$(m', \sigma') \leftarrow \mathsf{Sanit}(m, \text{MOD}, \sigma, pk_{\text{sig}}, sk_{\text{san}})$$

VERIFICATION. The Verify algorithm checks the validity of a signature σ for a message m with respect to the public keys pk_{sig} and pk_{san} and outputs a bit $d \in \{\texttt{true}, \texttt{false}\}$:

$$d \leftarrow \mathsf{Verify}(m, \sigma, pk_{\text{sig}}, pk_{\text{san}})$$

JUDGE. The algorithm Judge takes as input a message m and a valid signature σ, the public keys of the parties, and outputs a decision $d \in \{\texttt{Sig}, \texttt{San}\}$ indicating whether the message-signature pair has been created by the signer or the sanitizer:

$$d \leftarrow \mathsf{Judge}(m, \sigma, pk_{\text{sig}}, pk_{\text{san}})$$

As usual we demand minimalistic functional properties of sanitizable signature schemes such that the verifier always accepts signatures generated by the honest signer or sanitizer, and that the judge decides correctly if the data has been formed correctly.

3.2 Construction

In order to describe our scheme formally we assume that ADM and MOD are (descriptions of) efficient deterministic algorithms such that MOD maps any message m to the modified message $m' = \text{MOD}(m)$, and $\text{ADM}(\text{MOD}) \in \{0,1\}$ indicates if the modification is admissible and matches ADM, i.e., $\text{ADM}(\text{MOD}) = 1$. For example, for messages $m = m[1] \ldots m[k]$ divided into blocks $m[i]$ of equal bit length t, ADM might contain t and the indices of the modifiable blocks, and MOD essentially consists of pairs $(j, m'[j])$ defining the new value for the j-th block.

We also let FIX_{ADM} be an efficient deterministic algorithm which is uniquely determined by ADM and which maps m to the immutable message part $m_{\text{FIX}} = \text{FIX}_{\text{ADM}}(m)$, e.g., for block-divided messages m_{FIX} is the concatenation of all blocks not appearing in ADM. To exclude trivial examples we demand that admissible modifications leave the fixed part of a message unchanged, i.e., $\text{FIX}_{\text{ADM}}(m) = \text{FIX}_{\text{ADM}}(\text{MOD}(m))$ for all $m \in \{0,1\}^*$, MOD with $\text{ADM}(\text{MOD}) = 1$. In addition, we also need that the fixed part must be maximal given ADM, i.e., $\text{FIX}_{\text{ADM}}(m') \neq \text{FIX}_{\text{ADM}}(m)$ for $m' \notin \{\text{MOD}(m) \mid \text{MOD with } \text{ADM}(\text{MOD}) = 1\}$ (else FIX_{ADM} mapping to the empty string would for example be a valid instantiation).

Construction 3.1 (Sanitizable Signature Scheme) *Let $\mathcal{S} = (\mathsf{SKGen}, \mathsf{SSign}, \mathsf{SVf})$ be a regular signature scheme. Define the sanitizable signature scheme $\mathsf{SanSig} = (\mathsf{KGen}_{sig}, \mathsf{KGen}_{san}, \mathsf{Sign}, \mathsf{Sanit}, \mathsf{Verify}, \mathsf{Judge})$ as follows:*

KEY GENERATION. *Algorithm KGen_{sig} generates on input 1^n a key pair $(pk_{sig}, sk_{sig}) \leftarrow \mathsf{SKGen}(1^n)$ of the underlying signature scheme, and algorithm KGen_{san} for input 1^n analogously returns a pair $(pk_{san}, sk_{san}) \leftarrow \mathsf{SKGen}(1^n)$.*

SIGNING. *Algorithm Sign on input $m \in \{0,1\}^*$, sk_{sig}, pk_{san}, ADM sets $m_{\text{FIX}} = \text{FIX}_{\text{ADM}}(m)$ for the algorithm FIX_{ADM} determined by ADM, and computes*

$$\sigma_{\text{FIX}} = \mathsf{SSign}(sk_{sig}, (0, m_{\text{FIX}}, \text{ADM}, pk_{san})), \sigma_{\text{FULL}} = \mathsf{SSign}(sk_{sig}, (1, m, pk_{san}, pk_{sig}))$$

using the underlying signing algorithm. It returns $\sigma = (\sigma_{\text{FIX}}, \sigma_{\text{FULL}}, \text{ADM})$.

SANITIZING. *Algorithm Sanit on input a message m, information MOD, a signature $\sigma = (\sigma_{\text{FIX}}, \sigma_{\text{FULL}}, \text{ADM})$, keys pk_{sig} and sk_{san} first recovers $m_{\text{FIX}} = \text{FIX}_{\text{ADM}}(m)$. It then checks that MOD is admissible according to ADM and that σ_{FIX} is a valid signature for message $(0, m_{\text{FIX}}, \text{ADM}, pk_{san})$ under key pk_{sig} (for pk_{san} included in sk_{san}). If not, it stops outputting $\perp$. Else, it derives the modified message $m' = \text{MOD}(m)$ and computes*

$$\sigma'_{\text{FULL}} = \mathsf{SSign}(sk_{san}, (1, m', pk_{san}, pk_{sig}))$$

and outputs m' together with $\sigma' = (\sigma_{\text{FIX}}, \sigma'_{\text{FULL}}, \text{ADM})$.

VERIFICATION. *Algorithm Verify on input a message $m \in \{0,1\}^*$, a signature $\sigma = (\sigma_{\text{FIX}}, \sigma_{\text{FULL}}, \text{ADM})$ and public keys pk_{sig} and pk_{san} first recovers $m_{\text{FIX}} = \text{FIX}_{\text{ADM}}(m)$. It then checks that $\mathsf{SVf}(pk_{sig}, (0, m_{\text{FIX}}, \text{ADM}, pk_{san}), \sigma_{\text{FIX}}) = 1$ accepts σ_{FIX} as a valid signature and that either $\mathsf{SVf}(pk_{sig}, (1, m, pk_{san}, pk_{sig}), \sigma_{\text{FULL}})$ or $\mathsf{SVf}(pk_{san}, (1, m, pk_{san}, pk_{sig}), \sigma_{\text{FULL}})$ verifies as $\texttt{true}$, too. If so, it outputs 1, declaring the entire signature as valid. Otherwise it returns 0, indicating an invalid signature.*

JUDGE. *The judge on input $m, \sigma, pk_{sig}, pk_{san}$ parses σ as $(\sigma_{\text{FIX}}, \sigma_{\text{FULL}}, \text{ADM})$ and outputs $\texttt{Sig}$ if $\mathsf{SVf}(pk_{sig}, (1, m, \text{ADM}, pk_{san}), \sigma_{\text{FULL}})$ validates as true, else if $\mathsf{SVf}(pk_{san}, (1, m, pk_{san}, pk_{sig}) = 1$ then it returns $\texttt{San}$. Note that one of these two verification must work, as Judge is only run on valid pairs (m, σ).*

Completeness of signatures generated by the signer and sanitizer follows easily from the completeness of the underlying signature scheme and the fact that FIX_{ADM} leaves the fixed

message parts unchanged for modified messages. There is a negligible probability that a signature of the signer or the sanitizer also verifies under the other party's other key, yielding possibly a wrong answer from the judge. We ignore this issue here for simplicity, because one can easily circumvent this problem by having each party also prepend a bit to the signature, indicating the origin (0 for signer and 1 for sanitizer). The judge can then also check that this bit matches its decision.

3.3 Security of Sanitizable Signatures

Here we recall the security notions for sanitizable signatures given by Brzuska et al. [BFF+09] (except for transparency which we do not define formally since our scheme does not achieve it). We note that Brzuska et al. [BFF+09] show that signer and sanitizer accountability together imply unforgeability, and that transparency implies privacy. Hence, in principle it suffices to show immutability, accountability and transparency. However, since we drop the latter requirement we need to show privacy from scratch. In this version we omit the formal descriptions of the security properties for space reasons.

Unforgeability. Unforgeability demands that no outsider should be able to forge signatures under the keys of the honest signer and sanitizer, i.e., no adversary should be able to compute a tupel (m^*, σ^*) such that $\mathsf{Verify}(m^*, \sigma^*, pk_{\text{sig}}, pk_{\text{san}}) = \texttt{true}$ without having the secret keys $sk_{\text{sig}}, sk_{\text{san}}$. This must hold even if one can see additional signatures for other input data, including the message-signature pairs and the public keys. This allows to capture for example scenarios where several sanitizers are assigned to the same signer.

Immutability. This property demands informally that a malicious sanitizer cannot change inadmissible blocks. In the attack model below the malicious sanitizer $\mathcal{A}$ interacts with the signer to receive signatures σ_i for messages m_i, descriptions ADM_i and keys $pk_{\text{san},i}$ of its choice, before eventually outputting a valid pair (m^*, σ^*) and pk^*_{san} such that message m^* is not a "legitimate" transformation of one of the m_i's under the same key $pk^*_{\text{san}} = pk_{\text{san},i}$. The latter is formalized by requiring that for each query $pk^*_{\text{san}} \neq pk_{\text{san},i}$ or $m^* \notin \{\text{MOD}(m) \mid \text{MOD with } \text{ADM}_i(\text{MOD}) = 1\}$ for the value ADM_i in σ_i, i.e., that m^* and m_i differ in at least one inadmissible block. Again, giving the adversary the possibility to ask the signer about other sanitizer keys $pk_{\text{san},i}$ covers the case that the signer interacts with several sanitizers at the same time.

Accountability. Accountability says that the origin of a (sanitized) signature should be undeniable. There are two types of accountability: *Sanitizer accountability* says that, if a message has not been signed by the signer, then even a malicious sanitizer should not be able to make the judge accuse the signer. *Signer accountability* says that, if a message and its signature have not been sanitized, then even a malicious signer should not be able to make the judge accuse the sanitizer.

In the sanitizer-accountability game let $\mathcal{A}_{\mathsf{Sanit}}$ be an efficient adversary playing the role of the malicious sanitizer. Adversary $\mathcal{A}_{\mathsf{Sanit}}$ has access to a Sign oracle. Her task is to output a valid message-signature pair m^*, σ^* together with a key pk^*_{san} (with (pk^*_{san}, m^*) being different from messages previously signed by the Sign oracle) such that the judge still outputs "$\texttt{Sig}$", i.e., that the signature has been created by the signer.

In the signer-accountability game a malicious signer $\mathcal{A}_{\mathsf{Sign}}$ gets a public sanitizing key pk_{san} as input. She is allowed to query a sanitizing oracle about tuples $(m_i, \text{MOD}_i, \sigma_i, pk_{\text{sig},i})$ receiving answers (m'_i, σ'_i). Adversary $\mathcal{A}_{\mathsf{Sign}}$ finally outputs a tuple $(pk^*_{\text{sig}}, m^*, \sigma^*)$ and is considered to succeed if Judge accuses the sanitizer for the new key-message pair pk^*_{sig}, m^* with a valid signature σ^*.

Privacy. Privacy roughly means that it should be infeasible to recover information about the sanitized parts of the message. As information leakage through the modified message itself can never be prevented, we only refer to information which is available through the sanitized signature.

Our approach is based on an indistinguishability notion[2] where an adversary can choose pairs (m_0, MOD_0), (m_1, MOD_1) of messages and modifications together with a description ADM and has access to a "left-or-right" box. This oracle either returns a sanitized signature for the left tuple ($b = 0$) or for the right tuple ($b = 1$). The task of the attacker is to predict the random bit b significantly better than by guessing. Here we need the additional constraint that for each call to the left-or-right box the resulting modified messages are identical for both tuples and the modifications both match ADM, else the task would be trivial. We write $(m_0, \text{MOD}_0, \text{ADM}) \equiv (m_1, \text{MOD}_1, \text{ADM})$ for this.

3.4 Security of Our Construction

Theorem 3.2 *The sanitizable signature scheme in Construction 3.1 provides unforgeability, immutability, privacy and accountability.*

Proof. We only need to show immutability, accountability and privacy, as the signer- and sanitizer-accountability together imply unforgeability [BFF+09].

Immutability. Assume towards contradiction that our construction is not immutable. We show that this contradicts the unforgeability of the underlying signer's signature scheme, i.e., we show that an adversary who successfully breaks immutability can be used to forge signatures under the signer's public key.

Let $\mathcal{A}$ be an efficient successful adversary against immutability. Adversary $\mathcal{A}$ impersonates the sanitizer and has access to a signing oracle $\mathsf{Sign}(\cdot, sk_{\text{sig}}, \cdot, \cdot)$. We show that if $\mathcal{A}$ is able to find $(m^*, \sigma^*, pk^*_{\text{san}})$ such that $\mathsf{Verify}(m^*, \sigma^*, pk_{\text{sig}}, pk^*_{\text{san}}) = \texttt{true}$ and for all queries to

[2] Brzuska et al. [BFF+09] also discuss a simulation-based approach which is equivalent to the indistinguishability notion.

the signing oracle we have $pk^*_{\text{san}} \neq pk_{\text{san},i}$ or $m^* \notin \{\text{MOD}(m_i) \mid \text{ADM}(\text{MOD}) = 1\}$, then the forgery immediately gives rise to a forgery against the underlying signature scheme.

The validity of the sanitizable signature σ^* in the adversary's forgery attempt contains a valid signature σ^*_{FIX} for $(0, m^*_{\text{FIX}}, \text{ADM}^*, pk^*_{\text{san}})$ under the signer's public key, it thus suffices to show that this tuple has not been input into the signing algorithm. First observe that since the signatures for the entire message start with a 1-bit, we only need to consider signatures created for tuples with 0-bits. Hence, if $(0, m^*_{\text{FIX}}, \text{ADM}^*, pk^*_{\text{san}}) = (0, m_{\text{FIX},i}, \text{ADM}_i, pk_{\text{san},i})$ for a query then $\text{ADM}_i = \text{ADM}^*$ and $\text{FIX}_{\text{ADM}}(m^*) = \text{FIX}_{\text{ADM}}(m_i)$, thus (by assumption about FIX_{ADM}) m^* must be a valid modification $\text{MOD}(m_i)$ of m_i. Therefore this forgery attempt cannot satisfy the requirement $pk^*_{\text{san}} \neq pk_{\text{san},i}$ or $m^* \notin \{\text{MOD}(m_i) \mid \text{ADM}(\text{MOD}) = 1\}$.

Note that the formal argument requires to build an adversary $\mathcal{B}$ against the underlying signature scheme with oracle access to a signing oracle of that scheme. Then one shows that $\mathcal{B}$ can simulate $\mathcal{A}$'s attack on the sanitizable scheme and, in particular, the signer oracle in the immutability attack. But this is straightforward for our scheme, given the signing oracle of the underlying signature scheme.

Sanitizer-accountability. We show that if the sanitizer can make the judge falsely accuse the signer, then the sanitizer can break the unforgeability of the underlying signer's signature scheme. Let $\mathcal{A}_{\mathsf{Sanit}}$ be an efficient and successful attacker. She has access to a signing oracle $\mathsf{Sign}(\cdot, sk_{\text{sig}}, \cdot, \cdot)$ and outputs a fresh, valid triple $(pk^*_{\text{san}}, m^*, \sigma^*)$, where $(pk^*_{\text{san}}, m^*) \neq (pk_{\text{san},i}, m_i)$ for all $(pk_{\text{san},i}, m_i, \text{ADM}_i)$-queries to the signing oracle.

The triple output by $\mathcal{A}_{\mathsf{Sanit}}$ is such that $\mathsf{Judge}(m^*, \sigma^*, pk_{\text{sig}}, pk^*_{\text{san}}) = \texttt{Sig}$. This means that Judge considers σ^*_{FULL} and notices that σ^*_{FULL} is a valid signer signature for the message $(1, m^*, pk^*_{\text{san}}, pk_{\text{sig}})$. But since $(pk^*_{\text{san}}, m^*) \neq (pk_{\text{san},i}, m_i)$ for all i and as all signatures for the fixed part are signatures over messages prepended with a 0-bit, it follows that $(1, m^*, pk^*_{\text{san}}, pk_{\text{sig}})$ has not been signed before. The formal argument (building an adversary $\mathcal{B}$ against the signature scheme, mounting a black-box simulation of $\mathcal{A}$) follows again straightforwardly.

Signer Accountability. We show that a successful attacker against signer accountability can be used to forge signatures of the sanitizer's signature scheme. Let $\mathcal{A}_{\mathsf{Sign}}$ be an efficient successful adversary. She is given access to a sanitizing oracle, respectively, the sanitizer's signing oracle $\mathsf{Sign}(\cdot, sk_{\text{san}}, \cdot, \cdot)$ and outputs a fresh, valid triple $(pk^*_{\text{sig}}, m^*, \sigma^*)$, where $(pk^*_{\text{sig}}, m^*) \neq (pk_{\text{sig,i}}, m_i)$ for all $(m_i, \text{MOD}_i, \sigma_i, pk_{\text{sig,i}}, sk_{\text{san}})$-queries to the sanitizing oracle.

The triple output by the adversary is such that $\mathsf{Judge}(m^*, \sigma^*, pk^*_{\text{sig}}, pk_{\text{san}}) = \texttt{San}$, i.e., Judge inspects σ^*_{FULL} and verifies that σ^*_{FULL} is a valid sanitizer signature for the message $(1, m^*, pk^*_{\text{san}}, pk_{\text{sig}})$. Since the sanitizer only signs messages beginning with 1 and $(pk^*_{\text{sig}}, m^*) \neq (pk_{\text{sig,i}}, m_i)$ for all queries, it follows that the sanitizer has not input this message into its signature algorithm before. The forgery thus comprises a forgery for the basic signature scheme,

Privacy. Privacy is guaranteed information-theoretically: Since the left-or-right oracle only receives message pairs and modifications mapping to the same outcome, and the sanitizer signs this derived message from scratch, the output distribution is identical for both values of the bit b in the left-or-right oracle. □

3.5 Variations and Extensions

Our generic construction easily allows variations and extensions like hierarchical sanitizing. The sanitizer can delegate some of his rights to a subordinate sanitizer as follows. Let

$$(\sigma_{\text{FIX}}, \sigma_{\text{FULL}}) = (\mathsf{Sign}(sk_{\text{sig}}, (0, m_{\text{FIX}}, \text{ADM}, pk_{\text{san}})),\ \mathsf{Sign}(sk_{\text{sig}}, (1, m, pk_{\text{san}}, pk_{\text{sig}})))$$

be a signer's signature for the message m. It is clear that the sanitizer can only delegate rights concerning the admissible blocks of the message. He thus determines a "subset" $\text{ADM}_{\text{sub}} \subseteq \text{ADM}$ (with the meaning that $\text{ADM}(\text{MOD}) = 1$ whenever $\text{ADM}_{\text{sub}}(\text{MOD}) = 1$) that the subordinate sanitizer is allowed to modify. Let m' be the sanitizer's modification of the message m, and $\text{FIX}_{\text{ADM}_{\text{sub}}}$ map m' to the concatenation $m'_{\text{FIX},sub}$ of the message parts which are immutable for the subordinate sanitizer. Let pk_{SubSan} be the subordinate sanitizer's public key.

To delegate the rights the sanitizer now signs the messages

$$(2, m'_{\text{FIX,sub}}, \text{ADM}_{\text{sub}}, pk_{\text{sig}}, pk_{\text{SubSan}}) \text{ and } (3, m', pk_{\text{SubSan}}, pk_{\text{sig}}).$$

to obtain $\sigma^{\text{san}}_{\text{FIX}}$ and $\sigma^{\text{san}}_{\text{FULL}}$. The signature issued by the sanitizer consists of

$$(\sigma_{\text{FIX}}, \text{ADM}, \sigma^{\text{san}}_{\text{FIX}}, \sigma^{\text{san}}_{\text{FULL}}, \text{ADM}_{\text{sub}})$$

and possibly all the public keys. For sanitizing m' to m'', the subordinate sanitizer algorithm $\mathsf{SubSanit}$ leaves $(\sigma_{\text{FIX}}, \text{ADM}, \sigma^{\text{san}}_{\text{FIX}}, \text{ADM}_{\text{sub}})$ unchanged and creates a new signature $\sigma^{\text{san}}_{\text{FULL}}{}' = \mathsf{SSign}(pk_{\text{SubSan}}, (3, m'', pk_{\text{SubSan}}, pk_{\text{sig}}))$. As the final signature it outputs

$$(\sigma_{\text{FIX}}, \text{ADM}, \sigma^{\text{san}}_{\text{FIX}}, \sigma^{\text{san}}_{\text{FULL}}{}', \text{ADM}_{\text{sub}}).$$

Further hierarchical levels of sanitizers can be added accordingly.

Concerning flat hierarchies, in some settings it may be desirable to involve several sanitizer, say, a setting with personnel in a hospital. The extension of our scheme to such a setting is straightforward. For each message the authorized sanitizer set is chosen, and σ_{FIX} is a signer's signature over the message $(0, m_{\text{FIX}}, \text{ADM}, pk_{\text{san},1}, \ldots, pk_{\text{san},k})$, where $pk_{\text{san},1}, \ldots, pk_{\text{san},k}$ are the authorized sanitizers' public keys. In addition, let σ_{FULL} be a signer's or sanitizer's signature over the message $(1, m, pk_{\text{san},1}, \ldots, pk_{\text{san},k}, pk_{\text{sig}})$. For verifying the validity of a signature, one checks that σ_{FIX} is a valid signer signature over $(0, m_{\text{FIX}}, \text{ADM}, pk_{\text{san},1}, \ldots, pk_{\text{san},k})$ and that σ_{FULL} verifies for the message $(1, m, pk_{\text{san},1}, \ldots, pk_{\text{san},k}, pk_{\text{sig}})$ under pk_{sig} or under one of the authorized sanitizers' keys $pk_{\text{san},1}, \ldots, pk_{\text{san},k}$ (this key may be determined as part of the signature).

The construction described above produces signatures which are linear in the number of sanitizers. This shall be avoided in settings involving a huge number of sanitizers. In this case, instead of signing $(0, m_{\text{FIX}}, \text{ADM}, pk_{\text{san},1}, \ldots, pk_{\text{san},k})$, one signs $(0, m_{\text{FIX}}, \text{ADM}, pk_{CA})$, where pk_{CA} is the public verification key of a certificate authority, which provides certificates for each sanitizer key $pk_{\text{san},k}$. The sanitizer then attaches his $pk_{\text{san},k}$ as well as its certificate to the signature. Certificates are endowed with an expiration date so that keys are changed regularly. Therefore, it is necessary that the fixed part m_{FIX} of the message contains some information about the signing date, which is the case for identity cards.

Acknowledgments

We thank the anonymous reviewers for valuable comments. Marc Fischlin, Anja Lehmann and Dominique Schröder are supported by the Emmy Noether Program Fi 940/2-1 of the German Research Foundation (DFG). This work was also supported by CASED (www.cased.de).

References

[ACdMT05] Giuseppe Ateniese, Daniel H. Chou, Breno de Medeiros, and Gene Tsudik. Sanitizable Signatures. In *ESORICS*, volume 3679 of *Lecture Notes in Computer Science*, pages 159–177. Springer, 2005.

[BFF+09] Christina Brzuska, Marc Fischlin, Tobias Freudenreich, Anja Lehmann, Marcus Page, Jakob Schelbert, Dominique Schroeder, and Florian Volk. Security of Sanitizable Signatures Revisited. In *Public-Key Cryptography (PKC) 2009*, volume 5443 of *Lecture Notes in Computer Science*, pages 317–336. Springer-Verlag, 2009.

[BKMN08] Jens Bender, Dennis Kügler, Marian Margraf, and Ingo Naumann. Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. In *DuD — Datenschutz und Datensicherheit*, volume 3, pages 164–177. Vieweg, 2008.

[Bun08] Bundesministerium des Innern. Grobkonzept zur Einführung des elektronischen Personalausweises. (Version 2.0), July 2008.

[MSI+03] K. Miyazaki, S. Susaki, M. Iwamura, T. Matsumoto, R. Sasaki, and H. Yoshiura. Digital documents sanitizing problem. In *Technical Report ISEC2003-20*. IEICE, 2003.

[SBZ01] Ron Steinfeld, Laurence Bull, and Yuliang Zheng. Content Extraction Signatures. In *ICISC*, volume 2288 of *Lecture Notes in Computer Science*, pages 285–304. Springer, 2001.

A Survey of Distributed Biometric Authentication Systems

Neyire Deniz Sarier

Bonn-Aachen International Center for Information Technology
Computer Security Group
Dahlmann str. 2, 53113 Bonn Germany
denizsarier@yahoo.com

Abstract: In ACISP'07, Bringer et al proposed a new approach for remote biometric based verification, which consists of a hybrid protocol that distributes the server side functionality in order to detach the biometric data storage from the service provider. Besides, a new security model is defined using the notions of Identity and Transaction Privacy, which guarantees the privacy of the identity-biometrics relationship under the assumption of non-colluding servers. In this survey, we review the scheme of Bringer et al and the following biometric verification systems that improve upon it in terms of computation and communication complexity. In this context, we discuss about the recent result of Sarier, which describes a secure and efficient multi-factor authentication scheme with a different biometric storage method that results in reduced computation and database storage cost.
Keywords: Remote authentication, Biometric template security, Identity privacy, Distributed systems, Private Information Retrieval

1 Introduction

Biometric authentication systems are used in order to verify the claimed identity of a user based on his biometric characteristics. Although authentication information should be kept confidential, for biometrics this cannot be guaranteed since it is very easy to obtain biological information such as fingerprint, iris or face data through fingerprint marking or using a camcorder. In order to avoid the imitation attacks, biometric measurements should be performed in controlled environments, for instance under the supervision of an operator. Otherwise, spoof-resistant sensors and/or multi-factor authentication techniques should be employed that combine biometrics with token and/or password based authentication methods.

Biometric authentication could be categorized broadly as remote server or client end authentication, where in the first case, the remote server stores the reference biometric data and performs the matching. Although biometrics is assumed as public data, it should not be easy to obtain the biometric data by compromising the central server, where the biometrics of each user is often associated with his personal information. This also affects the social acceptance of the biometric systems especially when biometric data are stored in a central database which can be vulnerable to internal or external attackers.

The security and privacy protection of remote biometric-based verification systems is enhanced by implementing distributed biometric systems, where the goal is to detach the biometric data storage from the service provider and to guarantee the notions of identity and transaction privacy, which have been recently introduced as a new security model for biometric verification. In this model, the user U registers its biometric template in cleartext or in encrypted form at the database DB. Besides, U registers his personal information (i.e. identifier) and the index of the database storage location of his biometrics at the service provider SP. For biometric verification, U encrypts his biometrics using a homomorphic encryption scheme and sends this to SP, which retrieves the index of U to be used in a Private Information Retrieval (PIR) protocol between SP and DB. Finally, a decision is made after decryption or in the encryption domain by exploiting the homomorphic properties of the underlying encryption scheme. Current systems implementing this approach provide provable security in this new model, however, the (public) biometric data are stored as encrypted using the relatively slow public key schemes to provide the privacy of the identity-biometrics relation resulting in high database storage costs due to ciphertext expansion. Besides, some systems require a detached verification unit VU for the final decision, which increases the overall complexity of the system. Consequently, one has to design a secure and efficient remote biometric verification scheme for a distributed system with a detached biometric database, which minimizes the costs of storage, encryption and communication and thus, the scheme also becomes applicable to large scale systems. In this survey, we consider the schemes designed in the framework of Bringer et al.'s security model. The present contribution is largely based on the author's paper presented at ICB'09 [13] with a special focus on the complexity of the PIR.

2 Definitions and Preliminaries

2.1 Distributed Systems with Detached Biometric Storage

In recent years, the privacy protection and the secure storage of the biometric templates were addressed in a number of papers. As it is noted in [15], privacy protection not only means the attackers inability to compromise the biometric template but also the protection of the sensitive relationship between the identity and the biometric information of the user. To achieve this property, the storage of personal identity information should be separated from the storage of biometrics using the distributed structure of [4, 5, 6, 15, 13, 3], which is composed of the user U_i, the sensor client SC, the service provider SP and the database DB. Some systems require the use of a smartcard for a multi-factor authentication [13] and/or a detached verification unit VU (or a $Matcher$) [4, 3]. The entities of the system (i.e. U_i, SC, SP, VU and DB) are independent (i.e. not colluding) of each other and they are all assumed to be malicious except for the sensor client. This way, SP cannot obtain the biometrics of the user and can have business agreements with different parties that make the sensor client available to users at different locations. Also, DB could function as a trusted storage for different SP's. Since SC captures the biometric data and performs the feature extraction, this component could be installed as a Trusted Biometric Reader or

biometric smartcard readers could be used as in [1].

2.2 Assumptions

- Liveliness Assumption: This is an indispensable assumption for any biometric system as it guarantees with high probability that the biometrics is coming from a live human user.
- Security link Assumption: To provide the confidentiality and integrity of sensitive information, the communication channel between U_i, SC, SP, DB and VU should be encrypted using standard protocols.
- Collusion Assumption: Due to the distributed system structure, we assume that U_i, DB,VU and SP are malicious but they do not collude. Additionally, the sensor client is always honest.

2.3 Security Requirements

2.3.1 Identity Privacy:

Informally, this notion guarantees the privacy of the sensitive relationship between the user identity and its biometrics against a malicious service provider or a malicious database even in case of multiple registrations of the same user with different personalized usernames. Briefly, it means that the service provider or the database (or an attacker that has compromised one of them) cannot recover the biometric template of the user [15].

2.3.2 Transaction Privacy:

Informally, transaction anonymity means that a malicious database cannot learn anything about the personal identity of the user for any authentication request made to the service provider [15].

The formal definition of the notions Identity and Transaction privacy could be found in [4, 5, 6, 15, 3].

2.4 Private Information Retrieval (PIR)

In order to provide Transaction Privacy, the systems in [4, 5, 6, 15, 13] employ a number-theory based PIR system, which allows the SP to retrieve the i-th bit (more generally, the i-th item) from the DB consisting of n bits while keeping the value i private. The PIR of [7] has an additional benefit of retrieving more than one bit, and in particular many

consecutive bits [10]. In this context, a Private Block Retrieval (PBR) protocol enables a user to retrieve a block from a block-database and the PIR/PBR setting of [5] consists of the DB containing a list of N blocks $(R_1, ..., R_N)$ and the SP, which runs a PBR protocol to retrieve R_i for any $i \in [1, N]$. The communication cost of the single database PIR system of [7] has currently the best bound for communication complexity of $O(\log(n)+b)$ for an n-bit DB, where b is the bit-length of the block to be retrieved. However, the computational cost of number-theory based PIR's is roughly a modular multiplication per bit of DB, which limits the usability of these schemes except for very small DB's. In [8], the authors suggest to use batch codes to amortize the computational cost of PIR with a moderate increase on the communication cost, which is already very low. When the SP wants to retrieve k-bits (not necessarily consecutive) out of n-bit DB, batch code constructions can achieve $k^{1+o(1)}$ communication and $n^{1+o(1)}$ computation. Recently, [9] proposed a lattice-based PIR scheme, which is 100 times faster than number-theory based PIR's and has reasonable communication.

2.5 Homomorphic Encryption

To construct a number-theory based PIR protocol and/or to make an authentication decision in the encryption domain based on a certain metric, we need a secure cryptosystem that is homomorphic over an abelian group.
For a given cryptosystem with $(Keygen, Enc, Dec)$, the message space M and the ciphertext space C that are both groups, a homomorphic cryptosystem satisfies
$Dec(Enc(a) \star Enc(b)) = a * b$, where $a, b \in M$ and $*, \star$ represent the group operations of M, C respectively.

2.6 Secure Sketches

Most of the schemes in the literature assume that the biometrics is represented as a fixed binary string, which is usually obtained by quantizing the original biometric template via a scaler quantizer and the resulting binary string is combined with a secure sketch or fuzzy extractor using binary error correcting codes. The main purpose of a secure sketch is to correct the noise in the biometric measurement by using some public information PAR, which is derived from the original biometric template b. A secure sketch scheme consists of two phases.

- The **Gen** function takes the biometrics b as input and returns the public parameter PAR,
- The **Rep** function takes a biometric b' and PAR as input and computes b if and only if $\mathbf{dis}(b, b') \leq t$, where $dis()$ is the distance metric used to measure the variation in the biometric reading and t is the error tolerance parameter.

An important requirement for such a scheme is that the value PAR should not reveal too much information about the biometric template b. The first scheme of [5] and the schemes of [6, 15] implement a secure sketch protocol to test for equality using the homomorphic property of the encryption system.

3 Early Results

The first remote biometric verification scheme for distributed environments is described in [4], where the biometric template is assumed as a fixed binary string $b = (b_1, ..., b_M)$ that is stored as a plaintext in DB during the registration phase. For authentication, a user U_i sends his fresh encrypted biometric template $\epsilon(b')$ using Goldwasser-Micali scheme to SP resulting in a high transmission and computation cost due to individual encryption of each bit of b'. Next, SP runs a PIR protocol using the index of the database location of U_i to obtain U_i's encrypted biometric template $\epsilon(b)$ computed by the DB during the PIR. Transaction privacy is guaranteed by employing this PIR scheme between the SP and the DB with the communication cost linear in the size N of the user's in the DB. Next, SP computes $\nu_k = \epsilon(b'_k)\epsilon(b_k)$ mod $q = \epsilon(b'_k \oplus b_k)$ for $k \in [1, M]$ due to the homomorphic property of Goldwasser-Micali scheme. Finally, a detached unit called $Matcher$ with the secret key of the Goldwasser-Micali scheme decrypts the permuted ν_k's to compute the hamming weight and decides based on the threshold t to accept or reject the user U_i.

3.1 Analysis

The scheme of [4] is provably secure in the framework defined in section 2.3. However, a new attack with complexity exponential in N against this scheme is described in [3] that reveals the user's biometric data to SP. It is also noted that this attack can be avoided if the ciphertexts are re-randomized by the DB. In [4, 3], an independent verification unit called $Matcher$ is additionally required for the final decision, which increases the overall complexity of the system. As a result of the PIR system, the database performs $O(N)$ exponentiations modulo q, where q is an RSA modulus with $|q|$=2048 bits. Finally, the security of the system could be improved by storing the biometric data as encrypted as in the following schemes.

4 Improved Schemes

In [5], an extension to PIR system called as Extended Private Information Retrieval (EPIR) is presented, which is implemented for two different biometric verification schemes. In addition to the notion Identity Privacy (i.e. User Privacy), EPIR also satisfies the notion of Database Privacy, which means that the user (or the SP) does not learn anything about the other biometric entries. The main difference of this biometric authentication system is

the integration of a secure sketch scheme and the use of ElGamal encryption. This way, there is no need for a similarity metric for the final decision, instead the EPIR is used for equality testing. Particularly, the user U_i registers by sending R_i, namely the ElGamal encryption of its biometric sketch to DB and the parameter PAR is publicly available for reconstruction used in the secure sketch scheme. For authentication, the SC sends the encrypted biometric sketch C using the PAR and ElGamal encryption to SP, which is forwarded by SP to DB. For each entry $i \in [1, N]$, the DB selects a random r_i and computes $T_i = (C/R_i)^{r_i}$, where R_i is the ElGamal encryption of each user sketch stored in the system. Finally, SP runs a PIR protocol to obtain the value T_i corresponding to U_i and decrypts it using his secret key. If the result is 1, SP authenticates U_i, else rejects. In addition, [15] presents a slightly modified version of this scheme by simplifying the randomization step of the DB. Again, the same components, namely a PIR, secure sketch and ElGamal encryption scheme is considered. Apart from the computational cost of the PIR, the number of exponentiations computed by the DB is reduced from $O(4N)$ as in [5] to $O(2N)$ due to the use of a single random number instead of two different random numbers for the randomization of the ciphertexts.

Besides, the authors of [6] combine Goldwasser-Micali with Paillier encryption system in the Lipmaa's PIR protocol, where the latter is used in this PIR system to encode the requested index of U_i. Each biometric template is stored as an encrypted sketch using Goldwasser-Micali scheme, which is the scheme used to encrypt the fresh biometric template during authentication. Next, SP sends this data to the DB and Lipmaa's PIR protocol is applied by multiplying each of the DB's elements with the encrypted fresh template and by exploiting the homomorphic properties of the two encryption systems. The detached verification unit decrypts the resulting ciphertexts using the keys associated to Paillier and Goldwasser-Micali schemes to obtain a codeword c of U_i and checks the hash of c to the previously stored hash value for final decision. Similar to [5, 15], the scheme of [6] requires $O((M + 1)N)$ exponentiations modulo q^s ($s = 2$ with Paillier) and stores for each user $|q|M$ bits as encrypted sketch, where M is the bit-length of the sketch and $|q|$ is the size of an RSA modulus. Finally, another EPIR application for hamming weight is described in [5] using the BGN encryption system and a PIR, where the system does not employ a secure sketch.

5 Different Approaches

In [3], the authors describe a new distributed remote identification scheme by integrating a Support Vector Machine (SVM) to work as a multi-class authentication classifier. Particularly, the $|\mathbb{U}|$-class SVM implemented in [3] is described as follows: For each user $U_i \in \mathbb{U}$ with biometrics b_i, a mono classifier is trained using the remaining users $(\mathbb{U}/U_i)$ as the rejected class after extracting the biometric feature vector b_i of U_i. Next, a user profile $w^*_{\mathbb{U}}$ for each user U_i is constructed. Each user profile $w^*_{\mathbb{U}}$ consists of support vectors $SV_{i,j}$ and their weights $\alpha_{i,j}$, where $i = 1...S, j = 1...|\mathbb{U}|$. This will finish the registration phase of the system. For identification, each component of the feature vector b_i is encrypted by SC using Paillier encryption scheme and sent to the SP. SP forwards the encrypted bio-

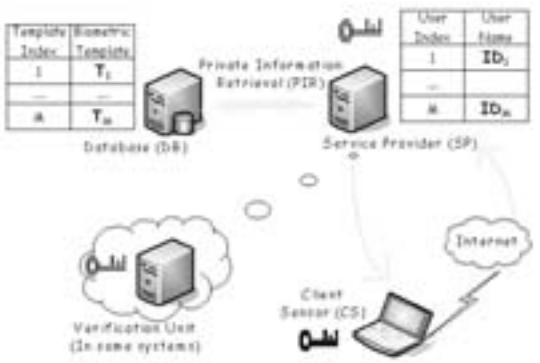


Figure 1: Overview of the current systems

metric data to DB, which computes the SVM classification values $class$ in the encryption domain by using the homomorphic properties of Paillier encryption system. Specifically, DB takes the profile data $w^*_{|\mathbb{U}|}$ and computes for each class $j \in [1, |\mathbb{U}|]$ the distance of b_i to the $w^*_{|\mathbb{U}|}$ in the encryption domain. Next, DB re-randomizes the resulting ciphertexts and sends the final vector $class$ of size $|\mathbb{U}|$ to SP, which permutes and re-randomizes this vector to $sclass$. Next, VU decrypts each component of $sclass$ and finds the index d of the maximum positive scaler contained in the decrypted vector. If there exists not such a positive index, VU sends $\perp$ to SP, else it sends d. Finally, SP recovers the identity of U_i using d and the inverse of the permutation used in $sclass$. The communication cost of this scheme is $O(N)$ ($N = |\mathbb{U}|$) and the computation cost is $O(N)$ exponentiations mod q^2.

5.1 An Efficient System

At ICB'09, Sarier proposed a new approach for a multi-factor biometric verification designed for distributed systems, which stores a random pool of features instead of the biometric templates of each user. Specifically, biometrics of a user is considered as a set of features and set overlap is used as the distance metric, where the threshold t represents the error tolerance in terms of minimal set overlap. Furthermore, the features of each user are randomly located as a separate entry in the central database instead of storing the biometric template (in cleartext or in encrypted form) of a user, which is a different technique from all the existing schemes, since each feature is stored only once by detecting the common features that are already stored in the database. Specifically, each of the features of arbitrary length are hashed using some collision-resistant hash function or mapped to an element of $\mathbb{Z}^*_p$ as in [2, 12] and stored in DB. Before this mapping, a secure sketch similar to the design of [14] could be implemented to improve the accuracy. The security of each feature is provided due to one-way hash function and the security of the communication channel is also provided via encryption. For this purpose, an Identity Based Encryption

(IBE) scheme such as Boneh-Franklin IBE to encrypt a random session key for AES and an efficient PIR protocol [7] is used, which allows SP to retrieve an item from the DB without revealing which item SP is retrieving. Based on this different approach for the database storage, the author presents a new remote biometric-based verification system achieving reduced storage and computational cost compared to the existing schemes.

Registration Phase: The registration phase consists of the following initialization of the components.

1. The four components of the system, namely, U_i with a smartcard, SC, SP and DB are initialized by the Private Key Generator (PKG) of the IBE system with the private keys $d_i, d_{SC}, d_{SP}, d_{DB}$, respectively. The secret key d_i of U_i is stored in the smart card of the user.

2. The user U_i presents its biometrics to the sensor client which extracts the feature set $B_i = (\mu_1, ..., \mu_k)$, where $\mu_i \in \mathbb{Z}_p^*$ of the user.

3. The user picks some random indexes $i_m \in \mathbb{Z}$ where $1 \leq m \leq k$ and registers his features at these locations of the database.

   If some of the locations are already occupied by other features, then the user selects other random indices. Also, if some of the features of the user are already stored in DB, then DB returns the indices of the common features. Thus, common features are not stored more than once, which decreases the total storage cost of DB.

4. The user U_i registers its personalized username at the service provider and stores the index list $Index_i = (i_1, ..., i_k)$ as encrypted with the public key of the SP in his smart card.

Verification Phase: The following figure shows the workflow of this phase.

In this phase, U_i inserts his smart card into the terminal of SC and presents its biometrics. The transmission of the biometric data between the reader SC and U_i's smartcard is secured using IBE for session key generation and AES for encryption similar to the system in [11]. Next, U_i sends a re-encryption of the stored $Index_i$ data to SP, which decrypts it to obtain the index list of U_i to be used in the PIR protocol between SP and DB. In Figure 2, the abbreviations denote the following: $B_i' = (\mu_1', ..., \mu_k')$ is the fresh template and E_k is the re-encryption of the encrypted index list $i_k \in Index_i$ of U_i. Using his biometric features μ_l, the user is able to compute the encryption of $H(r_l)$ as R_l for $l \in Index_i$, which are sent as encrypted to SP for final decision based on the threshold t. Here, $E_t^1 = r_t \oplus \mu_t$ and $E_t^2 = H(r_t \oplus \mu_t, H(r_t))$ for $t \in [1, N]$. Finally, $M_l = r_l \oplus \mu_l$ for $l \in Index_i$.

5.2 Analysis of the Protocol

- Identity-biometric template relation: At the registration phase, a user selects a random number for each feature of his biometrics and each feature is stored as a sep-

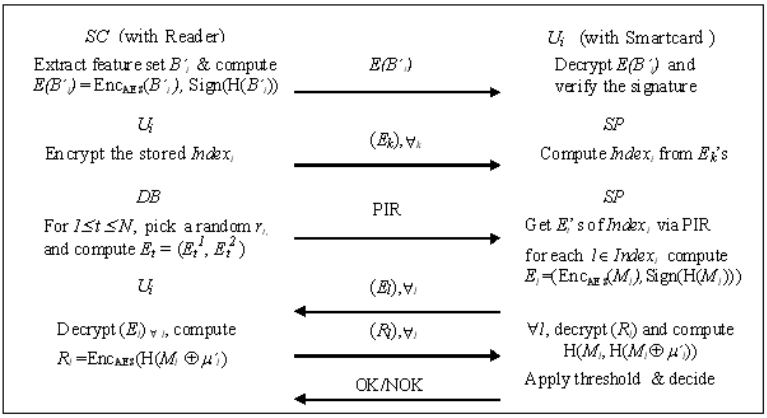


Figure 2: Verification phase of the Protocol [13]

arate entry using the randomly selected index. Hence, even if the database is compromised, the attacker would not be able to find an index that points to a biometric template stored as cleartext or encrypted. This also provides security against the database since it only stores a randomly ordered pool of features from different users, where each feature is hashed using a specific cryptographic hash function before it is stored in the database. Besides, when the same user registers at the service provider using different personalized (pseudorandom) usernames, than the service provider is not even aware of this situation since it does not store any index number corresponding to the database storage location.

- No single point of failure: In order to impersonate a user, the attacker needs to obtain both the biometrics and the smart card that stores the private key and the index list of the user. Besides, the user has to store only a private key for IBE and some index numbers in the smart card instead of his biometrics. When the user's smart card is lost or stolen, the user can obtain a new secret key from PKG and the index list by re-registering to the database.

- No need for PKI: Our scheme uses an efficient and anonymous IBE scheme such as Boneh/Franklin IBE for the generation of session keys for AES, hence, an eavesdropper (or a malicious database) on the communication channel cannot discover the identity of the user U_i since the ciphertext does not reveal anything about the identity of the recipient (and the sender for authenticated Boneh/Franklin IBE scheme) of the ciphertext since Boneh-Franklin IBE is an anonymous IBE scheme. Also, our design does not require a Public Key Infrastructure (PKI).

- Efficient memory storage: Since each feature is stored as a separate entry in the

database, there could be common features belonging to different users. Thus, during registration phase, the database could check for this situation and could return the indices of the previously stored features. This way, the size of the registered feature set and the total storage in the database could be smaller. Besides, since no biometric template is stored as an entry, there is no need to apply a public key encryption scheme such as ElGamal to store the biometric data as encrypted, where the ciphertext size is twice the plaintext size as in [15, 5]. Finally, the choice of the system parameters of [6, 4] result in a constraint on the size of the database, whereas our design is also suitable for a large scale central database that stores biometric data.

- Lower computational cost: In [6, 4], the database performs $O(N)$ exponentiations modulo q^2 [6] and modulo q [4], where q is an RSA modulus with $|q|$=2048 bits. Similarly, the schemes of [15, 5] require $O(N)$ exponentiations in group G, on which the ElGamal public key scheme is defined. The computational cost of our scheme is dominated by the $O(N)$ random number selections and $O(N)$ hash computations in order to encrypt each feature stored in the database using one time pad. Except for the session key generations, we use symmetric key encryption and lightweight cryptographic primitives, hence, our scheme is suitable for user's with smart cards. In the following table, we summarize various remote biometric-based authentication schemes that satisfy the security model described in section 2.

Table 1: Comparison of distributed remote authentication systems

Scheme	Computation Cost	Storage Cost at DB index	Storage Cost per user
System 1 [4]	M exponentiations + $(MN)/2$ multiplications	M bits	M bits
System 2 [6]	$O(N)$ exponentiations	$\|q\|M$ bits	$\|q\|M$ bits
System 3 [15]	$O(N)$ exponentiations	$2M$ bits	$2M$ bits
System 4 [5]	$O(N)$ exponentiations	$2M$ bits	$2M$ bits
System 5 [3]	$O(N)$ exponentiations	$\|q\|k$ bits	$\|q\|k$ bits
Our System	$O(N)$ random number + hash computations	$\|\mu\|$ bits	$(k-c)\|\mu\|$ bits

Abbreviations: N=total number of entries in the database; k=dimension of the feature vector of a user; M= bit-length of the biometric template; $|\mu|$= bit-length of a stored feature; c = number of common features of a user; $|q|$=size of an RSA modulus

5.3 Complexity of the PIR

The communication cost of the systems evaluated in Table 1 is dominated by the PIR, which is usually instantiated using the number-theory based PIR systems such as [7], which has currently the best bound for communication complexity of $O(\log(n) + b)$,

where b is the bit-length of the block to be retrieved from an n-bit DB. We assume that $M \approx k \cdot |\mu|$, where M is the size of the secure sketch.

Since the system of [13] has to retrieve k non-consecutive blocks of size $|\mu|$, a naive solution is to just run the PIR solution of [7] with complexity PIR independently k times, which results in the complexity of $k \cdot PIR$. However, in [10], the solution to the problem of retrieving k items that are not necessarily consecutive is presented using hashing. This way, the complexity is much smaller than the naive solution, namely $s \cdot PIR$, where $s = \sigma \log(k\mu)$ for $\mu \in \mathbb{Z}_p^*$. Furthermore, better performance is derived via explicit batch codes instead of hashing, since small values of k do not work with hashing. The reader is referred to [10] for a more detailed discussion of application of batch codes for amortizing the time complexity of PIR. Recently, [9] introduced an efficient noise-based PIR scheme, which is 100 times faster than all of the number-theory based PIR systems. The communication cost of [9] is not optimal as of [7], however, communication cost is not the main performance measurement of PIR as shown in the following table due to the enormous computational cost at the DB-end for number-theory based PIR schemes [9].

Scheme	Query		Download time	Bandwidth usage
	size	time		
Lipmaa's PIR	162 Kb	0,16s	33h	0.003%
Gentry and Ramzan's PIR [7]	3Kb	$\approx$ 0s	17h	0.016%
Noise-based PIR [9]	19Mb	19s	10min	7.2%

6 Conclusion and Future Directions

In this paper, we evaluated new designs for remote biometric based authentication protocols that follow the state-of-the-art security model for biometric authentication. In addition to the systems that store encrypted biometric sketches, we review the schemes with different database storage mechanisms that involve a SVM or a random pool of features, where the latter results in reduced storage cost even in small databases due to the single storage of the common features. Besides, this system could be applied to a variety of biometrics that could be represented by a feature vector. Also, the size of the stored biometric data is much smaller than existing systems that store biometrics as encrypted with public key encryption. We note that the compromise of the database (namely, a random pool of features) would not help any attacker in the recovery of a user's template, which could otherwise only be guaranteed by storing the biometric templates as encrypted. An interesting future work could be to improve the schemes that require a PIR using efficient storage methods and encryption systems.

Acknowledgement

The author is grateful to her supervisor Prof. Dr. Joachim von zur Gathen for his valuable support, encouragement and guidance.

References

[1] Atallah, M.J., Frikken, K.B., Goodrich, M.T., Tamassia, R.: Secure biometric authentication for weak computational devices. In Patrick, A.S., Yung, M. (eds.) FC 2005. LNCS, vol. 3570, pp. 357–371. Springer (2005)

[2] Baek, J., Susilo, W., Zhou, J.: New constructions of fuzzy identity-based encryption. In ASIACCS 2007, pp. 368–370. ACM (2007)

[3] Barbosa, M., Brouard, T., Cauchie, S., de Sousa, S.M.: Secure biometric authentication with improved accuracy. In Mu, Y., Susilo, W., Seberry, J. (eds.) ACISP 2008. LNCS, vol. 5107, pp. 21–36. Springer (2008)

[4] Bringer, J., Chabanne, H., Izabachène, M., Pointcheval, D., Tang, Q., Zimmer, S.: An application of the goldwasser-micali cryptosystem to biometric authentication. In Pieprzyk, J., Ghodosi, H., Dawson, E. (eds.) ACISP 2007. LNCS, vol. 4586, pp. 96–106. Springer (2007)

[5] Bringer, J., Chabanne, H., Pointcheval, D., Tang, Q.: Extended private information retrieval and its application in biometrics authentications. In Bao, F., Ling, S., Okamoto, T., Wang, H., Xing, C. (eds.) CANS 2007. LNCS, vol. 4856, pp. 175-193. Springer (2007)

[6] Bringer, J., Chabanne, H.: An authentication protocol with encrypted biometric data. In Vaudenay, S. (eds.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 109–124. Springer (2008)

[7] Gentry, C., Ramzan, Z.: Single-database private information retrieval with constant communication rate. In Caires, L., Italiano, G.F., Monteiro, L., Palamidessi, C., Yung, M. (eds.) ICALP 2005. LNCS, vol. 3580, pp. 803–815. Springer (2005)

[8] Ishai, Y., Kushilevitz, E., Ostrovsky, R., Sahai, A. Batch codes and their applications In STOC 2004. pp. 262–271. ACM (2004)

[9] Melchor, C.A., Gaborit, P. A fast private information retrieval protocol In ISIT 2008. pp. 1848 – 1852. IEEE (2008)

[10] Ostrovsky, R., Skeith, W.E.: A Survey of Single-Database Private Information Retrieval: Techniques and Applications In Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 393–411. Springer (2007)

[11] Park, B., Moon, D., Chung, Y., Park, J.W.: Impact of embedding scenarios on the smart card-based fingerprint verification. In Lee, J.K., Yi, O., Yung, M., (eds.) WISA 2006. LNCS, vol. 4298, pp. 110–120. Springer (2006)

[12] Sahai, A., Waters, B.: Fuzzy identity-based encryption. In Cramer, R. (eds.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer (2005)

[13] Sarier, N.D.: A new approach for biometric template security and remote authentication. In Tistarelli, M., Nixon, M. (eds.) Advances in Biometrics - ICB 2009. LNCS, vol. 5558, pp. 916–925. Springer (2009)

[14] Sutcu, Y., Li, Q., Memon, N.: Secure Sketch for Biometric Templates. In Chen, K., Lai, X. (eds) Advances in Cryptology - ASIACRYPT 2006. LNCS, vol. 4284, pp. 99–113. Springer (2006).

[15] Tang, Q., Bringer, J., Chabanne, H., Pointcheval, D.: A formal study of the privacy concerns in biometric-based remote authentication schemes. In Chen, L., Mu, Y., Susilo, W. (eds.) ISPEC 2008. LNCS, vol. 4991, pp. 56–70. Springer (2008)

BIOSIG 2009

Invited Conference Contributions

Quantitative Standardization of Iris Image Formats

Patrick Grother

Abstract: This paper gives performance-based results for the application of a leading recognition algorithm applied to standardized iris imagery. The implementation was evaluated in NIST's IREX program. The program was conducted in cooperation with the iris recognition industry to evaluated whether standardized image formats can be interoperable and compact. This is required for federated applications in which iris data is exchanged between interoperating systems, passed across bandwidth-limited networks, or stored on identity credentials. The study gave quantitative support to the revision of the ISO/IEC 19794-6 standard. This paper shows the effect of compression on false non-match rate and also, notably on false match rate also. The paper compares JPEG and JPEG 2000.

1 Introduction

The IREX program was initiated to expand a marketplace of iris-based applications based on standardized interoperable imagery. IREX is intended to bring iris recognition toward the level of maturity and interoperability of fingerprint biometrics and to support the iris as a second modality for large-scale identity management. The first goal was to support storage of biometrics on identity credentials, and its transmission across band-limited networks. This work [GTQS09] was conducted to support the ISO/IEC 19794-6 revision.

By standardizing an image format, and not a template, IREX complements considerable development of iris cameras particularly those for stand-off capture (where iris images are acquired at a few meters) and for mobile use. These cameras are technically capable of producing images in conformance to formal standards, although a few currently do not.

This paper is intended to introduce IREX by including results for one of nineteen algorithms submitted by ten participating organizations. It is labeled D2, and was submitted by Cambridge University. Similar algorithms have been published [Dau06]. The test was open worldwide, without fees nor qualification criteria except an ability to implement the API specifications[1]. A comprehensive set of results can be found in the IREX report [GTQS09].

Standard Images: Examples of the images considered in IREX are shown in Figure 1. The first format, KIND 3, is merely a cropped and centered iris image. The second format, KIND 7, is similarly cropped and centered, but also includes vital masking of the sclera and the eyelids. The masking operation is simply replacement of the pixel value with a fixed greyscale value. The final format, KIND 16, is a simplified version of the original ISO polar format. The iris texture between concentric circles inside the pupil and one outside the iris is sampled radially and circumferentially to form the polar record.

[1] See http://iris.nist.gov/irex/irex_api.pdf

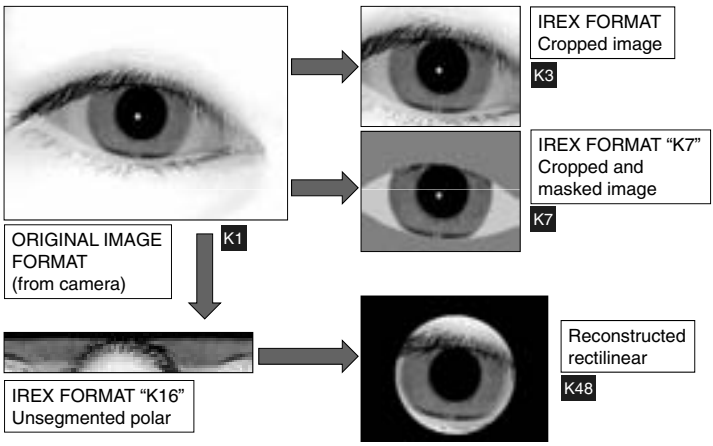


Figure 1: An iris image formatted in each of the three kinds.

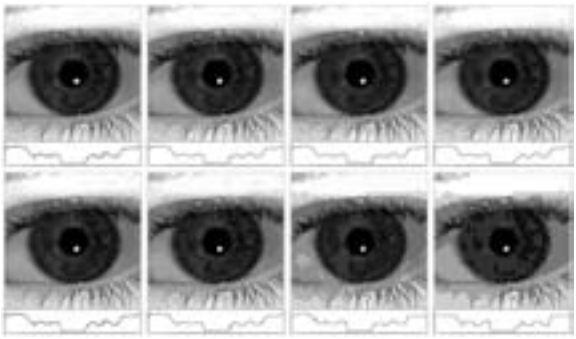
The KIND 7 format was defined and analyzed by Daugman [DD08, DD07]. Instantiation of conformant records requires fine detection of the iris-sclera and iris-eyelid boundaries (if any). This extends the requirement of the KIND 3 record which requires only coarse localization. The polar format was defined by Kim [Kim07] after the viability of the original non-concentric polar format was questioned. Instantiation of KIND 16 records requires detection of the pupil and the iris.

Prior work: This specific work follows other analyses of the application of compression to iris images [IBE05, DD08, RM07, MTU07]. While the studies reported promising results, they explored only the case in which enrollment and verification data are processed by a lone supplier's localization and matching algorithms. The exception [RM07] showed similar compression sensitivities for two different matching algorithms. The existing ISO/IEC 19794-6 indicates " a compression factor of 6:1 or less is recommended". This is an order of magnitude smaller than compression ratios published in the last two years [DD08, RM07]. The effect of compression on IREX formats is shown in Figure 2.

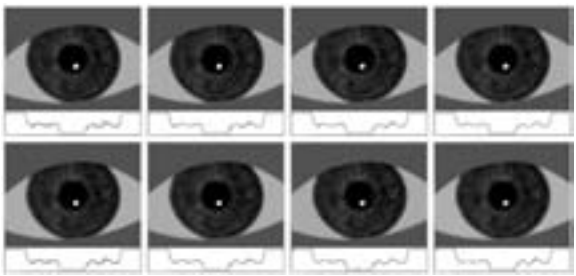
In 2008, Rakshit [RM07] applied the Monro [MRZ07], Tan [MTM+03] and Masek [MK03] iris recognition algorithms to 2156 images of 308 different eyes contained in the extended CASIA database [CAS07]. They used both JPEG and JPEG 2000 compressors at bit rates from 1.0 to 0.1 bits per pixel. They reported DET characteristics with FMR as low 0.0001. Additionally they gave the dependence of "FMR at the first false rejection" on bits-per-pixel and advanced this as their preferred metric. All comparisons involving compressed images were executed with compressed enrollment and verification images.

In 2007, Daugman [DD08, DD07] applied their iris recognition algorithms [2] to 1425 images of 124 people from the ICE 05 database [PSO+09]. All images were cropped to

[2] Specific hardware and software products identified in this report were used in order to perform the evaluations described in this document. In no case does identification of any commercial product, trade name, or vendor, imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products and equipment identified are necessarily the best available for the purpose.



(a) KIND 3



(b) KIND 7

Figure 2: A single ICE image with sizes, from left to right, uncompressed, 4KB, 3KB and 2KB. The two rows use JPEG 2000 and jpeg compression respectively. With this display process, the reader may not discern the compression and sampling artifacts in the first columns. Beneath each plot is a horizontal scanline across the center of each image.

320x320, centered, and compressed with JPEG[3] and with the JASPER implementation of JPEG 2000 [4]. They executed 12214 genuine and 1002386 impostor comparisons, and reported performance using DET characteristics with FMR as low as 0.00001. All comparisons were executed with compressed enrollment and verification images.

Ives et al. [IBE05, IBKS08] applied the Masek recognition algorithm to 756 images of 108 eyes present in the CASIA [CAS07] database, and to 20 images of both eyes of 50 people in the BATH database [Mon08]. The CASIA images were resized to 320x280 and compressed at ratios from 5:1 to 50:1. The BATH images, which had previously been compressed using JPEG 2000 at 16:1 in their full 1280x960 native format, were compressed from 20:1 to 50:1. They used both JPEG and JPEG 2000 implementations, in both lossy and lossless mode. They conducted 2268 genuine and 283122 impostor comparisons with the CASIA images and, respectively, 19000 and 1980000 comparisons with the BATH set. The study reported statistics for the Hamming distance distributions and stated performance in terms of equal error rate and the true accept rate at the threshold that

[3] Freely available from http://www.ijg.org/, downloaded June 22, 2009.

[4] Source code from http://www.ece.uvic.ca/m̃dadams/jasper/, downloaded April 4, 2008.

gave the lowest combined error count. The results show elevation of genuine scores but insensitivity of impostor scores under compression. For CASIA, this results in elevation of equal error rate, but this is not observed for BATH even at 50:1 compression.

2 Datasets

The IREX study employed data from three collections of iris images.

The Operational Database: The OPS operational dataset consists of two captures of the left and right irises of 8160 individuals. The 32640 images were collected using the PIER 2.3[5] camera from Securimetrics, now a division of L1 Identity Solutions. The files were extracted from a large multimodal database: A subject was included in the IREX partition if the subject's 10 fingerprints were matched by an operational AFIS implementation and if either iris matched using a commercial iris algorithm with comparison score below τ_1 or if both iris matched with a weaker threshold $\tau_2 > \tau_1$.

The involvement of an iris recognition algorithm in the dataset construction process means that recognition accuracy is likely to be high - more specifically that the iris left and right eye *pairs* are matchable (at some threshold). Thus we anticipate that any L-R fusion procedure should give error rates of zero for iris recognition algorithms of similar capability to X. Critically, however, this does not hold for single *images*, and non-zero matching error rates should be expected. The database is likely to be more representative of **enrollment** samples in which care had been taken to produce a pristine and matchable image. This makes the images suitable for the compression aspects of IREX because an identity credential would normally be populated with such images.

Some studies use the ALL-FAILURES subset to reduce the computational cost. This set is built by finding in the $N = 16320$ genuine KIND 1 comparisons the set B_i for SDK i that are falsely non-matched at a threshold fixed to give FMR = 10^{-4}. The result is the union $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 ... \cup \mathcal{B}_N$. and consists of 1335 genuine image pairs from 1144 subjects.

The BATH Database: NIST was provided with images of individuals collected by the University of Bath in the UK. The images were collected [Mon08] using a dedicated non-iris computer vision camera at a high resolution such that the uncompressed greyscale eight bit raster images had size 1280 x 640 pixels across the peri-ocular region. The main dataset is comprised of 29525 images from 800 individuals.

All of the raw images were down-sampled to 640 x 480 via 2 x 2 neighborhood averaging. This made the images conformant to the IREX test plan specification. The images were then passed to the I1 SDK to prepare KIND 3 instances. The record headers include iris diameter estimates. While the OPS and ICE datasets have median radii closer to 120 pixels, the BATH set has median at 135 with a significant fraction extending above 150 pixels. All BATH irises with diameter in excess of 340 pixels were discarded. The effect of this operation reduced the number of images to 23055 and the number of subjects to 664. This is what is used for all IREX analyses.

The ICE Database: This set of data was collected at the University of Notre Dame and

[5] http://www.l1id.com/files/20-pier2_4.pdf for the newer model. Link accessed July 21, 2009.

was provided to the authors by the MBGC program [ea08] at NIST. The set consists of 59558 images. An early subset was released under the ICE 05 development program.

The ICE corpus used in IREX consists of a left and right iris images collected from a university population over six semesters running from 2004 to 2006. The use of these images proved controversial in the ICE 2006 evaluation because the suppression of the LG 2200 camera's quality control apparatus caused operationally non-representative images (e.g. eyes closed, non-axial gaze, blur) to be present in the dataset. The presence of degraded images adversely affects iris recognition accuracy, and while more errors give statistical significance to FNMR estimates, the test results are less operationally relevant.

3 Metrics

This document quantifies accuracy and interoperability in terms of false non-match and false match error rates, FNMR and FMR. The quantities are computed empirically. If d is a dissimilarity score obtained by comparing two samples from the same person then $M(\tau)$ is the number of such scores above threshold:

$$M(\tau) = \sum_{d \in \mathcal{G}} H(d - \tau) \tag{1}$$

where $\mathcal{G}$ is the set of genuine comparison scores and $H(x)$ is the step function

$$H(x) = \begin{cases} 0 & x \leq 0 \\ 1 & x > 0 \end{cases} \tag{2}$$

The inequality placement is unconventional (for the Heaviside step function) and is used so that scores equal to the threshold correspond to acceptance. FNMR is then the fraction of genuine comparisons for which the score is above the operating threshold:

$$\text{FNMR}(\tau) = \frac{M(\tau)}{M(-\infty)} \tag{3}$$

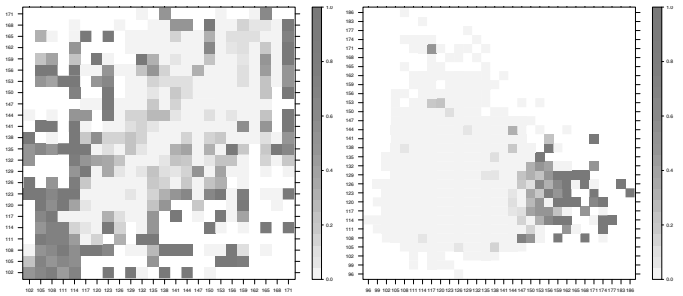
where $M(-\infty)$ is just the number of genuine comparisons considered. Likewise, when d denotes a score obtained by comparing samples from different persons, and $N(\tau)$ is the number of such scores below threshold, τ,

$$N(\tau) = \sum_{d \in \mathcal{I}} (1 - H(d - \tau)) \tag{4}$$

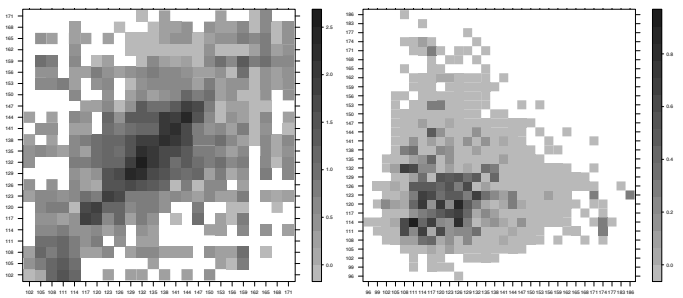
where $\mathcal{I}$ denotes the set of all impostor scores. FMR is then the fraction of impostor comparisons resulting in a score less that or equal to the operating threshold:

$$\text{FMR}(\tau) = \frac{N(\tau)}{N(\infty)} \tag{5}$$

where $N(\infty)$ is the number of impostor comparisons conducted. FMR is regarded as a measure of security, i.e. the fraction of illegitimate matching attempts that result in success. These error rates must be understood as being *matching* error rates, not *transactional*



(a) BATH FNMR D2 (b) OPS FNMR D2



(c) BATH Count (d) OPS Count

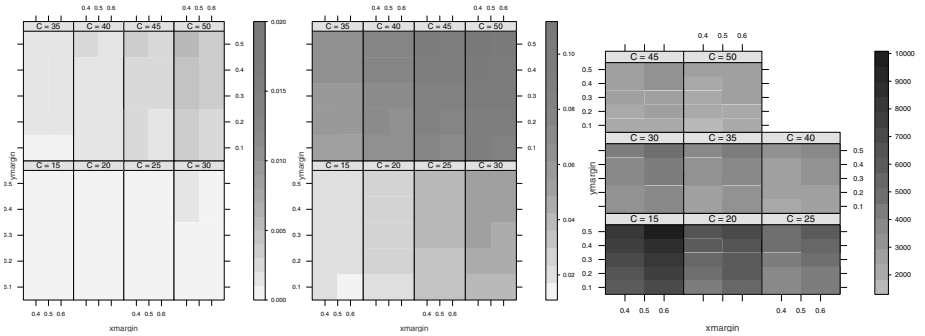
Figure 3: Dependency of false non-match rate on iris radius for the BATH and OPS datasets. The radii are quantized into three-pixel bins on $[100, 170]$. Cells are uncolored when the dataset did not contain any comparisons with those radii. Elsewhere, particularly away from the diagonal and in the corners, the number of comparisons is sometimes small such that there is considerable error in the FNMR estimates. The count of the comparisons is shown as $\log_{10}\ 1 + \textsc{count}(R_1, R_2)$, at bottom right.

rates (e.g. involving multiple attempts with one or two eyes). In IREX, any failure to make a template is held to cause any comparison involving that template to produce a comparison score of ∞. This guarantees that all comparisons give rejection.

4 Results

This section gives some quantitative results of the IREX study. It is confined only to the application of compression to the enrollment image. The more general network-based application, involving compression of both images, is not covered here.

Effect of iris radius: The question of whether performance is affected by iris size motivated the analyses of Figure 3. From the 2D comparison count maps, the BATH database contains a greater occurrence of atypical iris sizes than is present in the OPS database. These present problems as depicted in the heat maps which plot FNMR at fixed FMR for KIND 1 comparisons. On the OPS dataset there are fewer errors overall than on the BATH set. The errors that are present tend to occur when the genuine pair have moderately disparate iris sizes. While it is possible that outlying sizes are symptomatic of other



(a) FNMR and RMS CHANGE IN SCORE D2 (b) Image size (bytes)

Figure 4: At left, for KIND 3 records and the OPS database, the dependence of cFNMR on the vertical and horizontal iris cropping margins for various compression ratios. The center plot gives the RMS change in genuine scores. The use of conditional FNMR means that the plots exclude comparisons that were falsely rejected even before any compression was applied. All computations are driven by the bounding box coordinates reported by another IREX SDK (I1). The native KIND 3 instances are **not** used in this analysis. The number of bits per pixel is $8/C$, where C is the compression ratio. The iris radius varies and, because the cropping margins are fixed multiples of the radius, the image size varies. The final plot shows the compressed size, in bytes. This equals the width times height divided by C.

problems (e.g. out of focus images) a majority of the SDKs are immune to this. In the BATH database several SDKs almost always fail on images with small iris radii. A larger number fail for the case when the two radii differ substantially a lot (i.e. small vs. large).

These results have implications for the standard. While 640x480 pixels is the de facto standard *image* size the formal ISO/IEC 19794-6 only guides on iris size in a best practice annex. This is likely to be remedied in the revised ISO standard, per IREX input. Performance-related image attributes will be further refined in the new ISO/IEC 29794-6 *Iris Image Quality* standard.

The limits of cropping: Generation of the centered iris of the compact KIND 3 record requires cropping of the parent KIND 1 image in both the horizontal and vertical directions. The resulting iris is centered in a raster. It should have sufficient margin around it to allow iris detection algorithms to successfully fit the eyelid during segmentation. This issue is important because, under compression, a smaller (more tightly cropped) image can be compressed at higher bit rates to achieve a fixed size objective. Particularly for given a compression ratio C, an iris of radius R will be compressed to a size S bytes where

$$S = \frac{4(R + \Delta x)(R + \Delta y)}{C} \tag{6}$$

and the number of bits per pixel is $B = 8/C$. Thus, for the KIND 3 crop-only formats, the recognition performance will be a function of three independent variables: the vertical and horizontal cropping margins and the compression ratio. A user of the KIND 3 format can specify these and accept the variable size S from equation 6.

Figure 4 gives the results of a survey over these parameters for the various SDKs. Each plot shows the conditional FNMR for the entire OPS dataset as a heat map. It is plotted as a function of Δx and Δy at compression ratios of $C \in \{15, 20, 25, 30, 35, 40, 45, 50\}$ corresponding to bit rates $B \in \{0.53, 0.4, 0.32, 0.27, 0.23, 0.2, 0.18, 0.16\}$ respectively. The horizontal cropping margin takes on two values, $0.4R$ and $0.6R$. The vertical margin varies from $0.1R$ to 0.5 in steps of $0.1R$. The values currently adopted (July 2009) for the ISO/IEC 19794-6 are $\Delta x = 0.6R$ and $\Delta y = 0.2R$ so that image width and height are $w = 2(R + \Delta x)$ and $h = 2(R + \Delta y)$ respectively. The notable results follow.

Horizontal margin: Restriction to a horizontal margin of $0.4R$ is injurious in especially at high compression ratios. While SDK A1 is most tolerant of tighter horizontal cropping, enough false reject errors are observed at $\Delta x = 0.4R$ that the standard's requirement to use $\Delta x = 0.6R$ should be maintained.

Eye lash effects: In the vertical direction the use of *larger* margins is injurious to FNMR. The effect is explained by realizing that retention of the eye lashes in the image requires the JPEG 2000 compressor to dedicate more of its coding budget to the high frequency information associated with eye lashes.

Vertical margin: Very small margins are tolerable but, for robustness reasons, for other implementations where detection the iris boundary to within 10% of its radius may be problematic the current ISO standard specification of $\Delta y = 0.2R$ should be maintained.

Algorithmic resistance to compression: The matching algorithms exhibit different resistance to the iris texture-damaging effects of compression. For any given margin pair $(\Delta x, \Delta y)$, the D2 SDKs gives least growth in the error rate. Note that the quantity plotted is the FNMR conditioned on successful matching without compression. This measure is appropriate to model compression of enrollment quality instances.

Attainable file sizes: A more important result is that, for seven out of ten providers, compression at 25:1 (i.e. bits per pixel = 0.32) gives essentially undetectable increase in FNMR and this affords *mean* compressed raster sizes of fewer than 5 kilobytes[6].

The effect of compression: The application of lossy compression algorithms alters the pixel values in the iris region and in the limbic and pupillary boundary regions. When compression is high this damage is manifested as visible artifacts and measurable increases in false non-match error rates. Figure 5 shows the effect of compressing KIND 3 and KIND 7 images using JPEG and JPEG 2000 to attain file sizes from 6000 bytes down to 800 bytes. The response variable is the D2 genuine score on the left axis and a measure of separability on the right. The genuine score degrades more rapidly with JPEG compression. Also, by design, the cropped and masked KIND 7 record can be compressed to about half the size of the KIND 3 record for the same increase in genuine comparison score.

While the analogous figure for the D2 impostor distribution shows little change for all sizes and for both compressors, some IREX algorithms exhibit marked and unwanted elevation in FMR particularly for the JPEG algorithm.

DET characteristic: Figure 6 shows three DET characteristics for the D2 algorithm.

[6]For cropping margins of $\Delta x = 0.6R$ and $\Delta y = 0.6R$ the statistics on the number of bytes are: min = 2772, 25-th percentile = 4137, mean = 4501, median = 4574, 75-th percentile = 4937 and maximum = 7691.

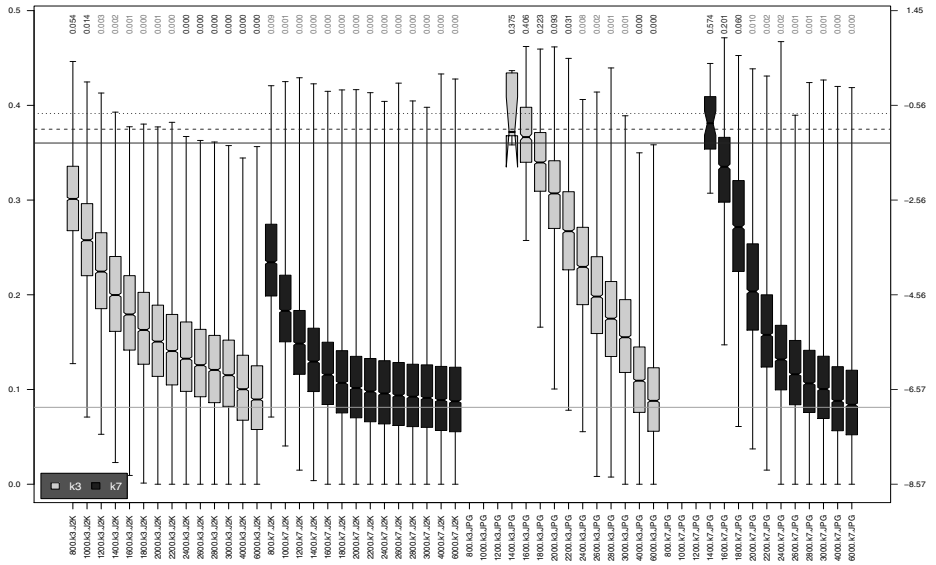


Figure 5: The distribution of D2 native genuine comparison scores by size of the compressed image, KIND and the compression algorithm. The images are from the OPS dataset. The right axis scale gives the corresponding value for $d' = (s - \mu_I)/\sqrt{0.5(\sigma_I^2 + \sigma_G^2)}$ for genuine score s. The boxplots only include comparison scores if the uncompressed version of the same image was matched below the FMR = 0.001 threshold. Above the boxes, in blue, are FNMR values at FMR = 10^{-3}. The three blue lines correspond, from the top, to FMR of $10^{\{-2,-3,-4\}}$. The lower grey line refers to the median score obtained from comparison of uncompressed KIND 3 images. Any comparison involving a failed template is excluded. Note that the iris record size on the horizontal axis is not evenly spaced above 3000 bytes.

These are for the baseline case of comparing uncompressed uncropped KIND 1 images, and for the cases of compressing the KIND 3 and KIND 7 images down to 2000 bytes using the JPEG 2000 algorithm and comparing those with uncompressed KIND 1 images.

Low FMR Performance The attraction of iris recognition, as articulated in the literature [Dau04], is that the impostor distribution is stable enough and sufficiently well characterized that a threshold may be set to give known very low false match rates. While it is the case with all biometric algorithms and modalities that the operating threshold can be set to give FMR values arbitrarily close to zero, the practical consequence for some modalities and applications is that the false rejection rates may become so high that the threshold is untenable. Commercial iris recognition cameras are specifically designed to capture irises that support low FMR operation. The dependency of FMR on threshold has been published for one class of algorithm [Dau04]. Indeed the claim of a known impostor distribution is an extremely attractive and valuable property for all biometrics and particularly for *one-to-many* applications where false match suppression is of paramount importance for large populations.

Table 1 shows the correspondence of the impostor empirical cumulative distribution func-

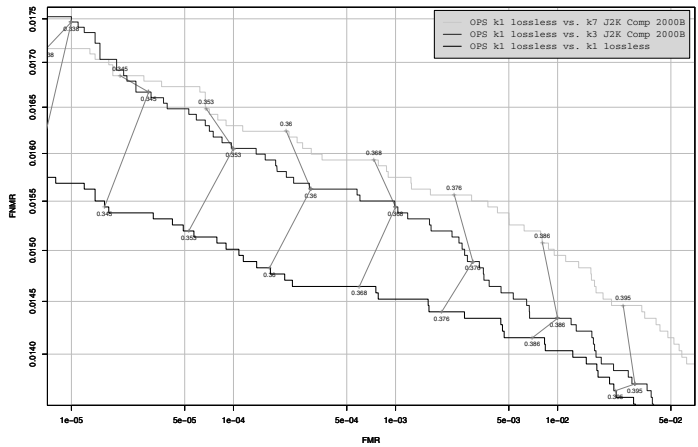


Figure 6: The DET characteristics for the uncompressed KIND 1 instances, and the two compact formats JPEG 2000 compressed to 2000 bytes. The OPS database was used. All images were produced natively. The grey lines link points of equal threshold. Note the FMR variation for some SDKs across KINDs. The poor FNMR performance of I1 on its KIND 3 instances may be due to its adherence to the $0.4R$ vertical cropping margin recommended by IREX. At a compression target of 2000 bytes this implied a lower bit rate than for other SDKs that cropped more closely.

(a) IEEE Trans. CSVT [Dau04]

Threshold HD	Published	D2
0.32	$3.8\ 10^{-8}$	$4.2\ 10^{-8}$
0.33	$2.5\ 10^{-7}$	$2.9\ 10^{-7}$
0.34	$1.4\ 10^{-6}$	$2.1\ 10^{-6}$
0.35	$7.5\ 10^{-6}$	$1.4\ 10^{-5}$

Table 1: Selected IREX estimates of FMR alongside previously published estimates. Cambridge indicated that that score normalization is used for D2. The IREX estimates are for the 1,165,868,160. OPS-ICE impostor comparisons.

tion computed here for KIND 1 ICE-OPS comparisons with values published by Daugman. This is done for empirical estimates for the score-normalized algorithm [Dau06]. The full FMR(τ) plots are given in [GTQS09]. This proximity is noteworthy in that neither dataset existed at the time the paper was written.

Lossless compression To avoid any damage to the iris texture, and elevation of FMR under lossy compression, this section gives results on how far the three IREX records can be compressed without *any* loss. The ISO/IEC 19794-6 allows use of JPEG 2000 and PNG lossless compressors. The median size of KIND 3 records prepared by D2 is about 50KB; This is achieved by cropping with $\Delta x = 0.6R$ and $\Delta y = 0.2R$. For KIND 7 records, lossless compression produces images with median size of 22KB. The improvement obviously due to the compressibility of the mask regions.

5 Conclusions

The IREX study attracted ten organizations into implementing the semantic aspects of the new ISO standard. This represents an order of magnitude expansion in the number of providers over the last half decade.

The compact interoperable images tested here occupy as little as 2 kilobytes. This makes them suitable for storage on ISO/IEC 7816 integrated circuit "smart card" identification tokens. This is somewhat larger than standard fingerprint minutia templates[7] but smaller than standard fingerprint images[8] and e-Passport face images[9]

The cropped-and-masked KIND 7 image format proposed for the ISO/IEC 19794-6 standard should be retained and advanced as the primary format for exchange of *compact* iris images. The false rejection performance attainable using this format approaches that available from the un-cropped and uncompressed parent images. This format should usually only be used in conjunction with the JPEG 2000 and PNG compression algorithms.

For applications without size, transport, or communications-related throughput constraints the uncompressed rectilinear record should be used either without cropping (KIND 1 or with (KIND 3). The latter crop-only format offers in many cases, improved error rates over the parent KIND 1 record. Instances may be JPEG 2000 -compressed to moderately low sizes. In both cases lossless compression may be effectively applied.

The cropped-and-masked KIND 7 format is particularly amenable to lossless compression. This allows iris records to be produced in the 20-40 kilobyte range. affords lossless compression down to the 60-80 kilobyte range. For some images, lossless compression will not be able to achieve a specific target size, and JPEG 2000 should be applied at a specifically targeted bit rate.

By empirical measurement of recognition error, the cropping operation used in preparation of KIND 3 and KIND 7 records should extend to no closer than 0.6 iris radii from the iris in the horizontal direction, and 0.2 radii in the vertical direction.

For some iris recognition algorithms, false match rates vary under compression. When extreme compression is applied to obliterate the iris texture some algorithms maintain low FMR; others do not and such behavior is contraindicated in identification applications.

The ISO/IEC 10918 JPEG compression algorithm should be deprecated. The presence of Discrete Cosine Transform blocking artifacts produces elevated false match rates.

References

[CAS07] CASIA. Specification of CASIA Iris Image Database - Version 1.0. Technical report, Chinese Academy of Sciences, March 2007. http://www.nlpr.ia.ac.cn/english/irdsirisdatabase.htm.

[7] Plain impression INCITS 378 minutia template with 38 six-byte minutiae takes 300 bytes.

[8] A 197ppmm ISO/IEC 19794-4 index finger, with 15:1 WSQ takes 6 to 10KB.

[9] A 90px eye-to-eye ISO/IEC 19794-5 token face, with JPEG at 15:1 with chrominance sub-sampling takes 15-20KB.

[Dau04] John Daugman. How Iris Recognition Works. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1):21–30, January 2004.

[Dau06] John Daugman. Probing the uniqueness and randomness of IrisCodes: Results from 200 billion iris pair comparisons. *Proc. of the IEEE*, 94(11):1927–1935, Nov 2006.

[DD07] John Daugman and Cathryn Downing. Effect of Severe Image Compression on Iris Recognition Performance. Technical report, University of Cambridge, Computer Laboratory, May 2007. Submitted as UK contribution to SC37 WG3, doc. N2125.

[DD08] John Daugman and Cathryn Downing. Effect of Severe Image Compression on Iris Recognition Performance. *IEEE Transactions on Information Forensics and Security*, 3(1):52–61, October 2008.

[ea08] P. J. Phillips et al. Overview of the Multiple Biometrics Grand Challenge. Technical report, National Institute of Standards and Technology, www.nd.edu/ kwb/PhillipsEtAlICB_2009.pdf [on June 24, 2009], 2008.

[GTQS09] P. Grother, E. Tabassi, G. W. Quinn, and W. Salamon. Performance of Iris Recognition Algorithms on Standard Images. Technical report, National Institute of Standards and Technology, September 2009. Published as NIST Interagency Report 7XXX.

[IBE05] Robert W. Ives, Bradford L. Bonney, and Delores M. Etter. Effect of Image Compression on Iris Recognition. In *Instrumentation and Measurement Technology Conference (IMTC)*, Ottawa, Canada, May 2005.

[IBKS08] R. W. Ives, R. P. Broussard, L. R. Kennell, and D.L. Soldan. Effects of image compression on iris recognition system performance. *Journal of Electronic Imaging*, 17, 2008. http://link.aip.org/link/?JEIME5/17/011015/1.

[Kim07] D. Kim. The unsegmented polar format. Technical report, Iritech Corp, November 2007. JTC001-SC37-N-2296 US NB Contribution on Compact Iris Format.

[MK03] Libor Masek and Peter Kovesi. MATLAB Source Code for a Biometric Identification System Based on Iris Patterns. Technical report, The School of Computer Science and Software Engineering, The University of Western Australia, 2003.

[Mon08] D. M. Monro. University of Bath Iris Image Database. Technical report, University of Bath, 2008. http://www.bath.ac.uk/elec-eng/research/sipg/irisweb/ [on June 22, 2009].

[MRZ07] Donald M. Monro, Soumyadip Rakshit, and Dexin Zhang. DCT-Based Iris Recognition. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 29(4):586–595, 2007.

[MTM+03] Li Ma, Tieniu Tan, Senior Member, Yunhong Wang, and Dexin Zhang. Personal Identification Based on Iris Texture Analysis. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25:1519–1533, 2003.

[MTU07] Stefan Matschitsch1, Martin Tschinder1, and Andreas Uhl. *Comparison of Compression Algorithms Impact on Iris Recognition Accuracy*, pages 232–241. Lecture Notes in Computer Science. Springer, Berlin / Heidelberg, August 2007.

[PSO+09] P. Jonathon Phillips, W. Todd Scruggs, Alice J. O'Toole, Patrick J. Flynn, Kevin W. Bowyer, Cathy L. Schott, and Matthew Sharpe. FRVT 2006 and ICE 2006 Large-Scale Experimental Results. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 99(1), 2009.

[RM07] Soumyadip Rakshit and Donald M. Monro. An Evaluation of Image Sampling and Compression for Human Iris Recognition. *IEEE Transactions on Information Forensics and Security*, 2(3-2):605–612, 2007.

Reverse Public Key Encryption

David Naccache[1], Rainer Steinwandt[2], and Moti Yung[3,4]

[1] École normale supérieure, Département d'informatique, Équipe de cryptographie, 45 rue d'Ulm, F-75230 Paris CEDEX 05, France
[2] Department of Mathematical Sciences, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431, USA
[3] Columbia University, Department of Computer Science, 1214 Amsterdam Avenue, New York, NY 10027, USA
[4] Google Inc, USA

david.naccache@ens.fr; rsteinwa@fau.edu; moti@cs.columbia.edu

Abstract. This exposition paper suggests a new low-bandwidth public-key encryption paradigm. The construction turns a weak form of key privacy into message privacy as follows: let $\mathcal{E}$ be a public-key encryption algorithm. We observe that if the distributions $\mathcal{E}(pk_0, \bullet)$ and $\mathcal{E}(pk_1, \bullet)$ are indistinguishable for two public keys pk_0, pk_1, then a message bit $b \in \{0, 1\}$ can be embedded in the choice of pk_b.
As the roles of the public-key and the plaintext are reversed, we refer to the new mode of operation as *Reverse Public-Key Encryption* (RPKE). We present examples of and variations on the idea and explore RPKE's relationship with key privacy, and we also discuss how to employ it to enable a new implementation of deniable encryption.

1 Introduction

System designers traditionally distinguish between *predictive*, *protective* and *reactive* security means.

Predictive security mechanisms are meant to sense that an attack is in preparation. Port scanning detection and critical function monitoring are typical predictive security functions.

Protective mechanisms must block or slow-down attacks. Encryption, signature, passwords and tamper-resistance all fall into the protective category.

Finally, should an attack succeed, *reactive* security functions must contain damage and allow system recovery.

Public-key encryption is a mature protective discipline. Indeed, current theory provides the practitioner with efficient and well-understood public-key encryption primitives with provable security guarantees.

In other words, considerable attention is currently being focused on the validity of the underlying *security guarantees*. In practice, security guarantees may fail for a variety of reasons.[5] Should this happen, replacing the underlying cryptographic functions is an option. As large-scale replacement can be impractical or costly, it is interesting to explore the existence of *reactive* fall-back public-key encryption modes whose security guarantees are only indirectly linked to the traditional system's security guarantees.

This work introduces such a mode of operation called *Reverse Public-Key Encryption* (RPKE). Denoting by $\mathcal{E} = \mathcal{E}(pk, m)$ a public-key encryption algorithm[6], the underlying idea is rather simple and intuitive: we start by assigning to each user *two* public keys pk_0 and pk_1 and a couple of message sampling algorithms $(\mathcal{M}_0, \mathcal{M}_1)$. The $\mathcal{M}_i$ depend on the specific properties of $\mathcal{E}$ but might be very simple and even have constant output (*i.e.*, $\mathcal{M}_0 = \mathcal{M}_1 =$ fixed constant).

We now assume that without the trapdoor information (sk_0, sk_1), encryptions[7] under pk_0 and pk_1 are computationally indistinguishable. The idea consists in public-key encrypting a message bit b by sending to the owner of (sk_0, sk_1) the quantity $c = \mathcal{E}(pk_b, \text{something})$.

Despite its simplicity, elaborating on this basic construction turns out to be worthwhile: even if the traditional public key encryption scheme built upon $(\mathcal{E}, \mathcal{D})$ does not offer strong provable security guarantees, using the "insecure" scheme in reverse encryption mode may still provide (low bandwidth) encryption with strong security guarantees. Thus RPKE can serve as a temporary fall-back mode, should (the traditional use of) $\mathcal{E}$ and $\mathcal{D}$ fail. In addition, as delineated in Section 4, when RPKE is concurrently used with traditional public-key encryption, a new form of deniable encryption may be obtained.

Throughout this paper we will use the acronym TPKE to refer to traditional, (*i.e.*, regular) public-key encryption.

This paper: after introducing the basic RPKE notion, we show how to create RPKE schemes from TPKEs featuring (a weak form of) key privacy. We then explore the connections between RPKE, TPKE and key privacy.

[5] *e.g.*, sudden algorithmic progress, the advent of new adversarial models, improper implementations, *etc.*

[6] $\mathcal{D} = \mathcal{D}(sk, c)$ being the corresponding decryption algorithm.

[7] Throughout this paper "encryption under pk_i", is to be understood as an abbreviation of "encryption under pk_i of messages sampled using $\mathcal{M}_i$".

Finally, Section 4 discusses how the concurrent use of TPKE and RPKE may serve as enabling mechanism for deniable encryption (a notion formalized in [CDNO97]).

This paper remains at the informal level, and the presented examples are not to be seen as fully worked out cryptographic schemes. We hope, however, that the presented ideas will stimulate further, more formal, follow-up work on reverse public key encryption.

Related work: to the best of our knowledge, RPKE has not been discussed in past literature so far. Nonetheless, given that RPKE might be interpreted as imposing a form of key privacy in a TPKE, we attract the reader's attention to the following references: following the formalization of key privacy in [BBDP01a], several key-privacy instantiations were proposed for RSA [HOT04], ElGamal [ZHI07] and McEliece [YCK+07]. Sufficient conditions for key privacy are given in [Hal05].

Group encryption [KTY07] can be interpreted in RPKE terms, too: the receiver's anonymity provided by group encryption hides the plaintext, while the authority's capability to remove anonymity corresponds to a reverse decryption capability. The idea of receiver anonymity also appears in the context of broadcast encryption [BBW06], but *the interpretation of such a privacy guarantee in encryption terms* is, to the best of the authors' knowledge, new.

In the light of the above, considering RPKE as a fall-back mode, raises the question of labeling the *basing of key and message privacy on different hardness assumptions* as a desirable cryptographic design goal.

2 Preliminaries and basic construction

As usual, we regard public key encryption as a collection of four (potentially randomized) polynomial time algorithms. We adopt the notation used in [BBDP01b].

Definition 1 (Traditional Public Key Encryption (TPKE)). *A (traditional) public key encryption scheme $\mathcal{P} = (\mathcal{G}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ consists of four polynomial time algorithms:*

- *A randomized common-key generation algorithm $\mathcal{G}$, taking as input a security parameter k and outputting a common key ck.*

– *A randomized key generation algorithm* $\mathcal{K}$ *transforming* ck *into a matching public/secret key-pair* (pk, sk)*:*

$$(pk, sk) \xleftarrow{R} \mathcal{K}(ck)$$

– *A randomized encryption algorithm* $\mathcal{E}$ *transforming* pk *and a plaintext* $m \in \mathfrak{M}(pk)$ *into a ciphertext* c*:*

$$c \xleftarrow{R} \mathcal{E}(\mathrm{pk}, m)$$

where $\mathfrak{M}(\mathrm{pk})$ *is the message space associated with* pk*.*

– *A deterministic decryption algorithm* $\mathcal{D}$ *transforming* sk *and* c *into the corresponding plaintext* m *or into an invalidity symbol* $\perp$ *not contained in any message space.*

For all $m \in \mathfrak{M}(\mathrm{pk})$ *the following relation must hold:*

$$\mathcal{D}(sk, \mathcal{E}(pk, m)) = m$$

In addition to the above definition, we silently assume the existence of a fifth algorithm $\mathcal{M}$ allowing to generate (draw) plaintexts from $\mathfrak{M}(pk)$:

$$m \xleftarrow{R} \mathcal{M}(pk) \;\text{ such that }\; m \in \mathfrak{M}(pk)$$

Typically, our instantiations of $\mathcal{M}$ will be trivial and under some circumstances even constant (*i.e.*, output a single plaintext message). It can be useful, however, to have the flexibility to choose a plaintext uniformly at random. We hence use the notation $m \xleftarrow{R} \mathcal{M}(pk)$ to denote (potentially randomized) plaintext message sampling. Moreover, we denote by

$$\mathrm{Im}(\mathcal{M}(pk)) \subseteq \mathfrak{M}(pk)$$

the set of possible outputs of $\mathcal{M}(pk)$ and assume that membership in $\mathrm{Im}(\mathcal{M}(pk))$ can be tested in polynomial time.

2.1 Reverse public-key encryption and key privacy

Given a public-key encryption scheme $\mathcal{P} = (\mathcal{G}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, we construct an RPKE $\mathcal{P}^{\mathrm{Rev}} = (\mathcal{G}^{\mathrm{Rev}}, \mathcal{K}^{\mathrm{Rev}}, \mathcal{E}^{\mathrm{Rev}}, \mathcal{D}^{\mathrm{Rev}})$ encrypting one-bit messages as follows:

Common-Key Generation: This algorithm is not altered, *i.e.*:

$$\mathcal{G}^{\mathrm{Rev}} = \mathcal{G}$$

Key Generation: $\mathcal{K}^{\mathrm{Rev}}$ runs $\mathcal{K}$ twice and obtains two independent key-pairs (pk_0, sk_0) and (pk_1, sk_1).

The public-key of $\mathcal{P}^{\mathrm{Rev}}$ is (pk_0, pk_1) and the secret-key is (sk_0, sk_1).

Encryption: for $b \in \{0,1\}$ we re-define the encryption process as:

$$\mathcal{E}^{\mathrm{Rev}}(pk, b) := \mathcal{E}(pk_b, m_b) \quad \text{where} \quad m_b \xleftarrow{R} \mathcal{M}(pk_b)$$

Put differently, the plaintext bit b determines whether we apply pk_0 or pk_1 to a plaintext m_b sampled from $\mathfrak{M}(pk_b)$.

Decryption: for a given ciphertext c, $\mathcal{D}^{\mathrm{Rev}}$ computes:

$$\begin{aligned} \tilde{m}_0 &\leftarrow \mathcal{D}(sk_0, c) \\ \tilde{m}_1 &\leftarrow \mathcal{D}(sk_1, c) \end{aligned}$$

$$\mathcal{D}^{\mathrm{Rev}}(sk, c) := \begin{cases} 0 & \text{, if } \tilde{m}_0 \in \mathrm{Im}(\mathcal{M}(pk_0)) \text{ and } \tilde{m}_1 \notin \mathrm{Im}(\mathcal{M}(pk_1)) \\ 1 & \text{, if } \tilde{m}_1 \in \mathrm{Im}(\mathcal{M}(pk_1)) \text{ and } \tilde{m}_0 \notin \mathrm{Im}(\mathcal{M}(pk_0)) \\ \perp & \text{, otherwise.} \end{cases}$$

Note that $\tilde{m}_i = \perp$ satisfies the condition $\tilde{m}_i \notin \mathrm{Im}(\mathcal{M}(pk_i))$.

Remark 1. While the above construction can be easily generalized to any polynomial number of public keys $pk_1, \ldots, pk_n$, in this paper, we restrict our discussion to the case $n = 2$. Similarly, one may consider a variant of reverse encryption with a single public key—cf. Example 3 below.

Before we proceed, let us provide a first informal RPKE example:

Example 1. For a k-bit RSA modulus n, let $H : \mathbb{Z}/n\mathbb{Z} \longrightarrow \{0,1\}^k$ be a random oracle. To encrypt a plaintext $m \in \mathbb{Z}/n\mathbb{Z}$ with public RSA key (n, e), the encryption algorithm computes the ciphertext as

$$c := (m^e \bmod n, H(m)) \quad .$$

Obviously, this scheme does not offer semantic security since the encrypted message can be checked. However, the reverse mode of operation yields a scheme (with small bandwidth) where guessing the (one-bit) plaintext appears harder, as we discuss next.

Embedding b in e: generate $n = pq$ and compute two private keys d_i such that $d_i \times \text{FDH}(i) = 1 \bmod \phi(n)$ for $i \in \{0, 1\}$, where

$$\text{FDH}: \{0,1\} \longrightarrow \left(\frac{\mathbb{Z}}{\phi(n)\mathbb{Z}}\right)^*$$

assigns a random number to each of the two possible plaintexts 0, 1. Encrypt $b \in \{0, 1\}$ as

$$c = (r^{\text{FDH}(b)} \bmod n, H(r))$$

where the redundancy $H(r)$ is used to spot the uniformly at random chosen $r \in_R \mathbb{Z}/n\mathbb{Z}$ during decryption.

Remark 2. Note that under the strong RSA assumption, decrypting the first element in c is hard, and the added redundancy (either given as a result of a random oracle over r or a few hard core bits of r) does not help in the decryption process.

Another option for hiding the key consists in using different moduli to implement reverse encryption:

Embedding b in n: generate two moduli n_i, fix e and let

$$d_i \times e = 1 \bmod \phi(n_i).$$

Let $B \gg \max\{n_i\}$ be a large bound (*e.g.*, $B = \lfloor \max\{n_i\}^{\frac{3}{2}} \rfloor$). Encrypt $b \in \{0, 1\}$ as

$$c = (r^e \bmod n_b) + r' \times n_b$$

for $r \in_R \mathbb{Z}/n_b\mathbb{Z}$ and $r' \in_R \{0, \ldots, \lfloor B/n_b \rfloor\}$ and provide $H(r, r')$ to allow spotting the correct decryption.

Intuitively, for an RPKE to be secure, encryptions under pk_0 and pk_1 must "look the same" without the trapdoors. It is easy to check that a TPKE offering key privacy in the sense of key indistinguishability is a sufficient condition for $\mathcal{P}^{\text{Rev}}$ to offer security in the sense of indistinguishable encryptions, here $\mathcal{M}(pk_b)$ can simply output a constant plaintext. For making this more precise, motivated by [BBDP01b], we define an adversary $\mathcal{A}_{\mathsf{ik}}$ running in two phases:

– At the find phase, $\mathcal{A}_{\mathsf{ik}}$ is given two public-keys (pk_0, pk_1) and outputs a plaintext m.

– At the guess phase, $\mathcal{A}_{\mathsf{ik}}$ is given the encryption of m under one of the pk_i and attempts to guess i.

Definition 2 (Indistinguishable Keys). *Let $\mathcal{P} = (\mathcal{G}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ be a public key encryption scheme. We say that $\mathcal{P}$ is* IK-CPA secure*, if for all polynomial time $\mathcal{A}_{\mathsf{ik}}$ the function*

$$\mathbf{Adv}^{\mathsf{ik\text{-}cpa}}(k) := \left|\Pr[\mathbf{Exp}^{\mathsf{ik\text{-}cpa\text{-}1}}(k) = 1] - \Pr[\mathbf{Exp}^{\mathsf{ik\text{-}cpa\text{-}0}}(k) = 1]\right|$$

is negligible.

Experiment 1 : $\mathbf{Exp}^{\mathsf{ik\text{-}cpa}}(k)$

for $b \in \{0,1\}$ **do**
  let $ck \xleftarrow{R} \mathcal{G}(k)$
  let $(pk_0, sk_0) \xleftarrow{R} \mathcal{K}(ck)$
  let $(pk_1, sk_1) \xleftarrow{R} \mathcal{K}(ck)$
  let $(m, state\_info) \xleftarrow{R} \mathcal{A}_{\mathsf{ik}}(\mathsf{find}, pk_0, pk_1)$
  let $c \xleftarrow{R} \mathcal{E}(pk_b, m)$
  let $\mathbf{Exp}^{\mathsf{ik\text{-}cpa\text{-}}b}(k) \xleftarrow{R} \mathcal{A}_{\mathsf{ik}}(\mathsf{guess}, c, state\_info)$
end for
return $(\mathbf{Exp}^{\mathsf{ik\text{-}cpa\text{-}0}}(k), \mathbf{Exp}^{\mathsf{ik\text{-}cpa\text{-}1}}(k))$

We now consider a second two-phase adversary $\mathcal{A}_{\mathsf{ind}}$ and define:

Definition 3 (Indistinguishable Encryptions). *(cf. [GM84,RS92]) Let $\mathcal{P} = (\mathcal{G}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ be a public key encryption scheme. We say that $\mathcal{P}$*

Experiment 2 : $\mathbf{Exp}^{\mathsf{ind\text{-}cpa}}(k)$

1: **for** $b \in \{0,1\}$ **do**
2: **let** $ck \xleftarrow{R} \mathcal{G}(k)$
3: **let** $(pk, sk) \xleftarrow{R} \mathcal{K}(ck)$
4: **let** $(m_0, m_1, state\_info) \xleftarrow{R} \mathcal{A}_{\mathsf{ind}}(\mathsf{find}, pk)$
5: **let** $c \xleftarrow{R} \mathcal{E}_{pk}(m_b)$
6: **let** $\mathbf{Exp}^{\mathsf{ind\text{-}cpa\text{-}}b}(k) \xleftarrow{R} \mathcal{A}_{\mathsf{ind}}(\mathsf{guess}, c, state\_info)$
7: **end for**
8: **return** $(\mathbf{Exp}^{\mathsf{ind\text{-}cpa\text{-}0}}(k), \mathbf{Exp}^{\mathsf{ind\text{-}cpa\text{-}1}}(k))$

is IND-CPA secure*, if for all polynomial time $\mathcal{A}_{\mathrm{ind}}$ the function*

$$\mathbf{Adv}^{\mathsf{ind\text{-}cpa}}(k) := \left|\Pr[\mathbf{Exp}^{\mathsf{ind\text{-}cpa\text{-}1}}(k) = 1] - \Pr[\mathbf{Exp}^{\mathsf{ind\text{-}cpa\text{-}0}}(k) = 1]\right|$$

is negligible.

Note that at Step 4 of $\mathbf{Exp}^{\mathsf{ind\text{-}cpa}}(k)$ *we require that* $m_0, m_1 \in \mathfrak{M}(pk)$ *with* $m_0 \neq m_1$ *and such that* m_0 *and* m_1 *are of equal length.*

If we assume the existence of a plaintext m_0 that can be encrypted under all public keys, then the following proposition establishes the IND-CPA security of RPKE.[8]

Proposition 1. *Denote by* $\mathcal{P}$ *an* IK-CPA *secure public key encryption scheme. If the sampling algorithm* $\mathcal{M}(pk)$ *has a constant output* m_0 *such that* $\forall pk: \ m_0 \in \mathfrak{M}(pk)$*, then* $\mathcal{P}^{\mathrm{Rev}}$ *as defined above is* IND-CPA *secure.*

Proof. (sketch) Suppose that there exists a polynomial time adversary $\mathcal{A}_{\mathsf{ind}}$ contradicting the IND-CPA security of $\mathcal{P}^{\mathrm{Rev}}$. As shown in Algorithm 1 and 2, we turn $\mathcal{A}_{\mathsf{ind}}$ into a polynomial time IK-CPA adversary $\mathcal{A}_{\mathsf{ik}}$ against $\mathcal{P}$. If $\mathcal{A}_{\mathsf{ind}}$'s guess d is correct, the so-constructed $\mathcal{A}_{\mathsf{ik}}$ has successfully

Algorithm 1 : find phase of IK-CPA adversary $\mathcal{A}_{\mathsf{ik}}$ against $\mathcal{P}$

1: **receive** $pk = (pk_0, pk_1)$
2: **launch** $\mathcal{A}_{\mathsf{ind}}(\mathsf{find}, (pk_0, pk_1))$
3: As $\mathcal{P}^{\mathrm{Rev}}$ encrypts only one bit, $\mathcal{A}_{\mathsf{ind}}(\mathsf{find}, \cdot)$ returns a triple $(0, 1, \mathit{state\_info})$.
4: **return** $(m_0, \mathit{state\_info})$ as the result of $\mathcal{A}_{\mathsf{ik}}(\mathsf{find}, \cdot, \cdot)$.

Algorithm 2 : guess phase of IK-CPA adversary $\mathcal{A}_{\mathsf{ik}}$ against $\mathcal{P}$

1: **receive** the IK-attack challenge $c \xleftarrow{R} \mathcal{E}(pk_b, m_0)$
2: **launch** $\mathcal{A}_{\mathsf{ind}}(\mathsf{guess}, c, \mathit{state\_info})$
3: **let** d be the value returned by $\mathcal{A}_{\mathsf{ind}}$.
4: **return** d

identified the public key used to encrypt m_0. □

Note that in our initial examples, not granting the adversary access to the message was crucial to achieving the necessary form of key privacy: the message basically played the role of internal random coins of the encryption process. However, as will be illustrated in Examples 3 and 4 below, reverse encryption can also be implemented in settings where the (traditional) plaintext is known, or even chosen, by the adversary.

[8] Assuming the existence of such a "universal plaintext" does not seem a major restriction—in all practical cryptosystem embodiments, one actually wants the *entire message space* to be independent of *pk*.

3 Examples of RPKE

Viewing the requirements of message privacy and key privacy as orthogonal (see [BBDP01a,BBDP01b,ZHI07]), reverse encryption seems attractive. Actually, indistinguishable keys are more than we need for secure RPKE: for secure RPKE it is enough to have *some* choice of plaintext pairs (m_0, m_1) for which ciphertexts of the forms $\mathcal{E}_{pk_0}(m_0)$ and $\mathcal{E}_{pk_1}(m_1)$ are computationally indistinguishable. Differing from the IK-CPA attack setting, an adversary against the IND-CPA security of $\mathcal{P}^{\mathrm{Rev}}$ is not allowed to choose a particular plaintext to distinguish between pk_0 and pk_1.

Example 2 (Reverse encryption without key privacy). Denote by $\mathcal{P}_2$ the following ElGamal public key encryption variant:

$\mathcal{G}$: fix a generator g of a cyclic group G of order q and a random oracle $H : G \times G \longrightarrow G$

$\mathcal{K}$: choose $a \leftarrow \{0, \ldots, q-1\}$ uniformly at random and return

$$(sk, pk) := (a, g^a),$$

the associated message space $\mathfrak{M}(pk)$ is the underlying cyclic group G.

$\mathcal{E}$: on input a public key $pk \in G$ and a message $m \in G$, choose a value $s \leftarrow \{0, \ldots, q-1\}$ uniformly at random and return the ciphertext

$$(g^s, pk^s \cdot m, H(pk, m))$$

$\mathcal{D}$: given a secret key sk and a ciphertext $(c_1, c_2, c_3) \in G \times G \times G$, the plaintext is:

$$m' := \begin{cases} c_1^{-sk} \cdot c_2 & \text{, if } c_3 = H(pk, c_1^{-sk} \cdot c_2) \\ \\ \perp & \text{, otherwise.} \end{cases}$$

Because of the poor use of the random oracle in the last ciphertext component, $\mathcal{P}_2$ obviosuly fails to offer IK-CPA or IND-CPA security.

However, letting $\mathcal{M}(pk)$ choose a plaintext $m \in_R G$ uniformly at random and assuming that the Decisional Diffie Hellman assumption holds in G, we obtain another encryption scheme $\mathcal{P}_2^{\mathrm{Rev}}$, operating in reverse mode (and has one-way security). The latter scheme is far less obvious to attack.

Our next example builds on an intentionally weakened Goldwasser-Micali scheme [GM84] and illustrates an RPKE variant with a single public key.

Example 3 (Reverse encryption without encryption). Consider the following public key encryption scheme which is obviously neither IND-CPA nor IK-CPA secure:

$\mathcal{G}$**:** (simply outputs the size of the public modulus n).

$\mathcal{K}$**:** choose a Blum integer $n = p \cdot q$ and

$$g \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* \quad \text{with} \quad \left(\frac{g}{p}\right) = \left(\frac{g}{q}\right) = -1$$

and return $(sk, pk) := ((p, q), (g, n))$; the associated message space $\mathfrak{M}(pk)$ is the set $\{0, 1\}$ and can be naturally extended to strings of bits (by concatenation of ciphertexts of the string's bits).

$\mathcal{E}$**:** on input $pk = (g, n)$ and a plaintext $m \in \{0, 1\}$, choose at random

$$r \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$$

and return the triple

$$(pk, m, r^2 \cdot g^{1-m})$$

$\mathcal{D}$**:** decrypt a ciphertext (pk, m, h) as:

$$m' := \begin{cases} 1 & , \text{if } \left(\frac{h}{p}\right) = \left(\frac{h}{q}\right) = 1 \\ 0 & , \text{if } \left(\frac{h}{p}\right) = \left(\frac{h}{q}\right) = -1 \\ \perp & , \text{otherwise.} \end{cases}$$

The above scheme, which sends send the plaintext as well, is naturally not a good encryption scheme anymore.

Now, consider a reverse public key encryption mode of the scheme, using only a single public key $pk := (g, n)$ which can be defined as follows:

- Fix a public key $pk := (g, n)$ with a message sampling algorithm $\mathcal{M}(pk)$ selecting $m \in_R \{0, 1\}^k$ uniformly at random (excluding the all ones string string 1^k).
- To encrypt an individual bit b in the reverse mode, compute first the local "generator" for this encryption operation as $g' := g^{(b+1) \bmod 2}$ (namely either use g or 1 as the encrypting "generator"). Then, bit by bit, encrypt the random (but now fixed) message m to produce the ciphertext as in the traditional scheme (*i.e.*, when $g' = g$ is used, the

string m will produce a quadratic non-residue for a 0 and a quadratic residue for a 1 in the last ciphertext component; when $g' = 1$ is used, the string m is just producing k quadratic residues, rather than really encrypting the messsage: thus it is easy to recognize, given the factorization of n, which is the b encrypted this way).

– In this reverse mode, a ciphertext decrypts to 0 if the ciphertext is a (traditional) encryption of the all ones string (since $g' = 1$ was used as the generator) and to 1 if the ciphertext encrypts m, otherwise the decryption returns an invalidity symbol $\perp$.

Without the factorization it is hard to tell what b is unless the quadratic residuosity assumption fails. Thus the reverse mode gives us security while our ciphertext includes the plaintext m itself (no message privacy in the traditional mode).

The fact that we employ g or $g^0 = 1$ as the generator can, in fact, be viewed as two cyptosystems.

Finally, we outline a possible reverse mode of operation in the context of identity-based cryptography.

Example 4 (Reverse encryption in an identity-based setting). Consider Boneh and Franklin's BasicIdent scheme [BF01,BF03]. The public system parameters can be specified as a tuple $(q, G_1, G_2, \hat{e}, n, P, P_{\text{pub}}, H_1, H_2)$:

– G_1 and G_2 are groups of prime order q; we write G_1 additively (with neutral element 0) and G_2 multiplicatively
– $\hat{e} : G_1 \times G_1 \longrightarrow G_2$ is an admissible bilinear map
– n fixes the length of plaintexts
– P is a generator of G_1
– $P_{\text{pub}} = s \cdot P$ is a random multiple of P, where $s \in_R \{1, \ldots, q-1\}$
– $H_1 : \{0,1\}^* \longrightarrow G_1 \setminus \{0\}$ and $H_2 : G_2 \longrightarrow \{0,1\}^n$ are random oracles

Implement two instances ($i \in \{0,1\}$) of this scheme:

$$P_{\text{pub}}^{(i)} := s_i \cdot P \quad \text{and} \quad d_i := s_i \cdot H_1(\text{Alice})$$

where the d_i represent the secret keys corresponding to the identity Alice.

Motivated by a result of Holt [Hol06], we can define an RPKE mode of BasicIdent as follows: Bob sends a plaintext $b \in \{0,1\}$ to Alice by

"encrypting the fixed message 0^n" under $P_{\text{pub}}^{(b)}$. In other words, Bob picks a random $r \in_R \{1, \ldots, q-1\}$ and sends to Alice the ciphertext

$$c := \left(r \cdot P, H_2 \left(\hat{e}(H_1(\text{Alice}), P_{\text{pub}}^{(b)})^r \right) \right)$$

To decrypt a ciphertext $c = (U, v)$ in reverse mode, Alice checks for which $b \in \{0, 1\}$ the condition $v = H_2(\hat{e}(d_b, U))$ holds.

4 RPKE and deniable encryption

Interestingly, RPKE may also find applications in settings where Alice and Bob share secret key material. In particular, we can use the method in the setting of deniable encryption (which we present here without a complete formalization).

Let (n, e) be Alice's RSA public key and denote by $d = e^{-1} \bmod \phi(n)$ Alice's secret key. We further assume that before interaction starts, Alice generates a secret κ, a random message $r \in_R \mathbb{Z}/n\mathbb{Z}$ and a random mask $s \in_R \{0, 1\}^k$.

κ is used as key for an information-theoretically secure message authentication code (MAC) denoted by f.

The values r and $t' := s \oplus f_\kappa(r)$ are given to Bob.

We consider two low bandwidth modes of operation for encrypting a plaintext bit $b \in \{0, 1\}$:

TPKE**:** In this mode Bob encrypts b by sending

$$c := (r^e \bmod n, t)$$

where r is a random integer such that $r \bmod 2 = b$, and $t \in_R \{0, 1\}^k$ is a randomly chosen tag .

RPKE**:** In this mode Bob encrypts b as in Example 1. Namely by sending $c := (r^{\text{FDH}(b)} \bmod n, t')$ where t' is the secret pre-agreed with Alice. After creating c, Bob erases r. Alice uses (r, s, κ) to determine which exponent was initially used by Bob.

Suppose that we allow concurrent usage of TPKE and RPKE. Namely, Bob sends b in one of the above modes without informing Alice in advance which of the two modes was used.

Alice can try both possible plaintexts in reverse mode and, should the redundancy checks succeed or fail, determine if TPKE was used. However,

Alice can still claim to a third party that RPKE was used: Alice selects a random bit $\tilde{b}$ and decrypts by exponentiation with $\text{FDH}(\tilde{b})^{-1} \bmod \phi(n)$ to obtain a random RSA plaintext $\tilde{r}$. To construct a matching redundancy check, Alice chooses a random MAC key $\tilde{\kappa}$, computes a matching tag $f_{\tilde{\kappa}}(\tilde{r})$ and opens the value $\tilde{s} := f_{\tilde{\kappa}}(\tilde{r}) \oplus t'$, which is consistent with t'.

Conversely, claiming that an RPKE-decrypted ciphertext is actually valid in TPKE mode is straightforward.

The above assumed a one-time operation based on a shared one time key. We can extend this to many time operation by producing the values from a pseudorandom generator that is one-way and erasing the values used in past operations. The parties share initial seeds and at a point they are asked to deny a message the generator's state does not remember the shared values. Deniability now relies on the fact that the values claimed are impossible to verify computationally.

5 Conclusion and further research

This paper presented a new public-key encryption paradigm, allowing to turn a weak form of key privacy into message privacy. While our discussion makes a first attempt to formalize the concept, it clearly falls short of presenting a thorough treatment of the subject. In fact, a number of questions arise which deserve further exploration. For instance, bandwidth could be improved if (in our definition of $\mathcal{P}^{\text{Rev}}$ in Section 2.1) a construction allowing to distinguish between the two $\perp$ sub-cases

$$\text{if } \tilde{m}_0 \in \text{Im}(\mathcal{M}(pk_0)) \text{ and } \tilde{m}_1 \in \text{Im}(\mathcal{M}(pk_1))$$

$$\text{if } \tilde{m}_0 \notin \text{Im}(\mathcal{M}(pk_0)) \text{ and } \tilde{m}_1 \notin \text{Im}(\mathcal{M}(pk_1))$$

could be exhibited. Devising such an extension is an interesting problem left unanswered by this paper. Combining such a construction with an n-key-pair scheme (as in Remark 1) would allow encoding in a linear size ciphertext an exponentially large plaintext space.

Reverse encryption and digital signatures. Another open question, related to reverse encryption, is the transformation of *certain* digital signature schemes into public-key encryption schemes: at the minimalist extreme we can regard a one-bit public-key encryption algorithm $\mathcal{E}$ as an algorithm that does not encrypt anything, but generates "valid strings" $c = \mathcal{E}(pk, r)$. A "valid string" is a string c that satisfies a confidential validity predicate

$\mathcal{D}(sk, c) = \texttt{true}$. Here "validity" stands for the transmission of the bit one whereas invalidity will stand for the transmission of the bit zero.[9]

Consider now a digital signature scheme with probabilistic signing algorithm $\mathcal{S}$ and deterministic verification algorithm $\mathcal{V}$ producing digital signatures on messages m such that:

$$\sigma \leftarrow \mathcal{S}(sk, m) \implies \mathcal{V}(pk, m, \sigma) = \texttt{true}$$

If—amongst other conditions—given sk one cannot infer pk (this is not a misprint) and if σ cannot be verified using sk alone, then $\mathcal{S}$ and $\mathcal{V}$ could potentially be turned into encryption and decryption algorithms of a public-key encryption scheme as follows: publish sk and give pk to the receiver (only). To encrypt a one, pick a random message and sign it. To encrypt a zero, send a random string. A different starting point could be a construction using two different types of redundancy in the message that is signed—say along the following line: use a message recovery signature scheme and either sign a message of the form $r \parallel H(r)$ or of the form $H(r) \parallel r$ with a randomly chosen r. The signature scheme has to be such that knowledge of pk is essential for being able to distinguish these cases (and given the secret key, it is hard to determine it).

Acknowledgment

We thank Eike Kiltz for several interesting comments regarding this work.

References

[BBDP01a] Mihir Bellare, Alexandra Boldyreva, Anand Desai, and David Pointcheval. Key-Privacy in Public-Key Encryption. In Colin Boyd, editor, *Advances in Cryptology – ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 566–582. Springer-Verlag, 2001.

[BBDP01b] Mihir Bellare, Alexandra Boldyreva, Anand Desai, and David Pointcheval. Key-Privacy in Public-Key Encryption. Available at `http://cseweb.ucsd.edu/~mihir/papers/anonenc.html`, September 2001. Full version of [BBDP01a].

[BBW06] Adam Barth, Dan Boneh, and Brent Waters. Privacy in Encrypted Content Distribution Using Private Broadcast Encryption. In Giovanni Di Crescenzo and Aviel D. Rubin, editors, *Financial Cryptography and Data Security, 10th International Conference, FC 2006*, volume 4107 of *Lecture Notes in Computer Science*, pages 52–64. Springer-Verlag, 2006.

[9] Invalidity may either be achieved by just sending a random c which will be very probably invalid or by an "intelligent" construction of a deliberately invalid c.

[BF01] Dan Boneh and Matt Franklin. Identity-Based Encryption from the Weil Pairing. In J. Kilian, editor, *Advances in Cryptology – CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer-Verlag, 2001.

[BF03] Dan Boneh and Matt Franklin. Identity-Based Encryption from the Weil Pairing. *SIAM J. of Computing*, 32(3):586–615, 2003. Extended abstract appeared in [BF01].

[CDNO97] Ran Canetti, Cynthia Dwork, Moni Naor, and Rafail Ostrovsky. Deniable Encryption. In *Advances in Cryptology — CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 90–104. Springer-Verlag, 1997.

[GM84] Shafi Goldwasser and Silvio Micali. Probabilistic Encryption. *Journal of Computer and System Sciences*, 28(2):270–299, April 1984.

[Hal05] Shai Halevi. A sufficient condition for key-privacy. Cryptology ePrint Archive: Report 2005/005, January 2005. Available at `http://eprint.iacr.org/2005/005`.

[Hol06] Jason E. Holt. Key Privacy for Identity Based Encryption. Internet Security Research Lab Technical Report 2006-2, Internet Security Research Lab, Brigham Young University, March 2006. Available at `http://isrl.cs.byu.edu/pubs/isrl-techreport-2006-2.pdf`.

[HOT04] Ryotaro Hayashi, Tatsuaki Okamoto, and Keisuke Tanaka. An RSA Family of Trap-Door Permutations with a Common Domain and Its Applications. In Feng Bao, Robert Deng, and Jianying Zhou, editors, *Public Key Cryptography – PKC 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 291–304. Springer-Verlag, 2004.

[KTY07] Aggelos Kiayias, Yiannis Tsiounis, and Moti Yung. Group Encryption. In Kaoru Kurosawa, editor, *Advances in Cryptology – ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Computer Science*, pages 181–199. Springer-Verlag, 2007.

[RS92] Charles Rackoff and Daniel R. Simon. Non-interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack. In Joan Feigenbaum, editor, *Advances in Cryptology – CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 433–444. Springer-Verlag, 1992.

[YCK+07] Shigenori Yamakawa, Yang Cui, Kazukuni Kobara, Manabu Hagiwara, and Hideki Imai. On the Key-Privacy Issue of McEliece Public-Key Encryption. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-17*, volume 4851 of *Lecture Notes in Computer Science*, pages 168–177. Springer-Verlag, 2007.

[ZHI07] Rui Zhang, Goichiro Hanaoka, and Hideki Imai. Orthogonality between Key Privacy and Data Privacy, Revisited. In Dingyi Pei, Moti Yung, Dongdai Lin, and Chuankun Wu, editors, *Information Security and Cryptology – Inscrypt 2007*, volume 4990 of *Lecture Notes in Computer Science*, pages 313–327. Springer-Verlag, 2007. Preliminary full version available at `http://staff.aist.go.jp/r-zhang/research/KeyPrivacy.pdf`.

BIOSIG 2009

Further Conference Contributions

Classification of Skin Diseases and Their Impact on Fingerprint Recognition

Martin Drahanský[1], Eva Březinová[2], Filip Orság[1], Dana Lodrová[1]

[1]Faculty of Information Technology, Brno University of Technology
Božetěchova 2, CZ-61266, Brno
{drahan, orsag, ilodrova}@fit.vutbr.cz

[2]Faculty of Medicine, Masaryk University
Komenského nám. 2, CZ-66243, Brno
141896@mail.muni.cz

Abstract: This article describes different skin diseases which could have the influence to the process of fingerprint acquirement. There are many people, who suffer under such diseases and are therefore excluded from the set of users of a biometric system and could not e.g. get a visa to the USA or use an access biometric system installed in a company, where they work.

1 Introduction

Skin diseases represent a very important, but often neglected factor of the fingerprint acquirement. It is impossible to say in general how many people suffer from skin diseases, because there are so many various skin diseases – please refer e.g. to [1][2][3][4][5], but we must admit that such diseases are present in our society. When discussing whether the fingerprint recognition technology is a perfect solution capable to resolve all our security problems, we should always keep in mind those potential users who suffer from some skin disease.

In the following text, several skin diseases are introduced, which attack hand palms and fingertips. These are divided into three subcategories (the list is however more longer – see [7]): diseases affecting a) *only the papillary line structure*, b) *only the skin color* and c) *both papillary line structure and skin color*.

The subcategory of skin diseases affecting only the skin color are the least dangerous for the quality of the fingerprint image [9][10]. In fact, only one fingerprint technology can be considered as sensitive to such diseases – the optical technology, but if FTIR-based (Frustrated Total Internal Reflection) optical sensors are used, the change of skin color may have no influence on the quality of the resulting images. The case of the other two subcategories is different. If the structure of papillary lines has changed, it is often impossible to recognize the original curvatures of papillary lines and therefore it is impossible to decide whether the claimed identity is the user's identity.

The situation after successful recovery of a potential user from such skin diseases is, however, very important for the possible further use of fingerprint recognition devices. If the disease has attacked and destroyed the structure of papillary lines in the epidermis layer of the skin, the papillary lines will not grow in the same form as before (if at all) and therefore such user could be restricted in his/her future life by being excluded from the use of fingerprint recognition systems, though his fingers don't have any symptoms of a skin disease any more.

2 Examples – Change of Papillary Line Structure

We can put the following diseases as examples of change of papillary line structure: *furuncle* (Fig. 1a) [6] is an acute, round, tender, circumscribed perifollicular staphylococcal abscess that generally ends in central suppuration; *Pitted keratolysis* (Fig. 1b+c) [6][4] is a bacterial infection of the plantar stratum corneum; *Fingertip eczema* (Fig. 1d) [1] is a very dry, chronic form of eczema of the palmar surface of fingertips; it may be the result of an allergic reaction or may occur in children and adults as an isolated phenomenon of unknown cause; *Verruca vulgaris* (Fig. 2a) [6] – common warts are a significant cause of concern and frustration of certain patients. The prevalence reaches 50% in those persons with the direct contact with meat; *Scleroderma* [4] is a multisystem disorder characterized by inflammatory, vascular, and sclerotic changes of the skin and various internal organs, especially the lungs, heart, and gastro-tract (Fig. 2b); *Cellulitis* [121] is manifested by tender, warm, erythematous plaques with ill-defined borders. Occasionally, linear red macules proximal to the large plaque are seen too.

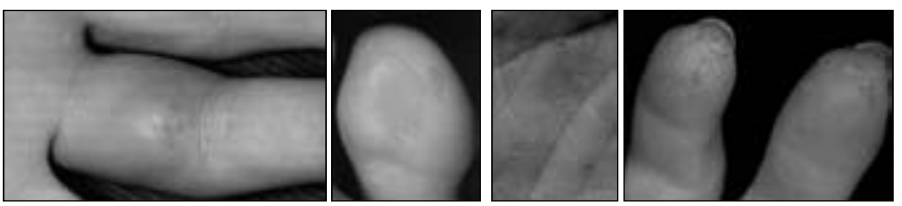


Fig. 1 (from left): a) Staphylococcal abscess in a diabetic patient [6]; b) Pitted keratolysis [6]; c) Palmar pits [4]; d) Fingertip eczema [1].

3 Examples – Change of Skin Color

We can put the following diseases as examples of change of skin color: *Hand-Foot-and-Mouth disease* (HFMD) (Fig. 2c) [6] is usually a mild illness. It primarily affects children from 2 to 10, but exposed adults may also develop the disease; *Infective endocarditis*, sepsis and septic shock [4] (Fig. 2d) are very serious systematic infections with high associated morbidity and mortality rates. Groups of risk [4] are people at the age of 30 to 40, elderly people with valve sclerosis and patients with intravascular prostheses; *Tinea of the hand* (Fig. 2e) [1] has the same appearance as the dry, diffuse, keratotic form of tinea on the soles.

Fig. 2 (from left): a) Verruca vulgaris [4][6]; b) Scleroderma [4]; c) Hand-foot-and-mouth disease [6]; d) Infective endocarditis [4]; e) Tinea of the hand [1].

4 Examples – Change of Papillary Line Structure and Skin Color

We can put the following diseases as examples of change of papillary line structure and skin color: *Hand eczema* [1][3] is an inflammation of the hands (Fig. 3a). Hand dermatitis is common in industrial occupations: it can threaten job security if inflammation cannot be controlled; *Pompholyx* (*dyshidrosis*) [1] is a distinctive reaction pattern of unknown etiology presenting as symmetric vesicular hand and foot dermatitis. Pustular psoriasis [8][3] (Fig. 3b) of the palms and soles may resemble pompholyx; *Psoriasis* (Fig. 3c) [3][4] is thought to be a hereditary disorder that requires an interplay of genetic and environmental factors for full clinical expression; *Raynaud's phenomenon* (RP) [4] is digital ischemia that occurs on exposure to cold and/or as a result of emotional stress (Fig. 3d).

Fig. 3 (from left): a) Subacute and chronic eczematous inflammation [1]; b) One variant of pompholyx [1]; c) Psoriasis [3]; d) Raynauld's phenomenon – acrogangrene [4].

5 Summary

It is clear from each subsection that either the color of the skin or the structure of papillary lines on the fingertip could be influenced. If only the color has changed, some of optical fingerprint scanners might be influenced and so this change is not crucial. On the other hand, the change of skin structure is very significant, because if papillary lines are damaged, it is impossible to find the minutiae and therefore to recognize the person. If we are unable to recognize/enroll a person, then such person cannot use the biometric system based on the fingerprint recognition technology, and therefore the implementing company has a big problem – how to authorize such person, if they don't want to use PINs (Personal Identification Numbers) or other authorization methods.

Some of these diseases are only temporary, i.e. after the healing of such disease, the papillary line structure or color is restored and the user is again able to use his/her fingers for the fingerprint recognition in authorization tasks in security systems. However, some diseases leave irrecoverable finger damage restraining a new growth of papillary lines and respective user is then unable to use his/her fingerprints for appropriate recognition tasks in automated fingerprint security systems.

Another problem regarding the papillary lines has been published in [11], where the influence of medicine Xeloda® (against cancer – see http://www.xeloda.com) is discussed that this has a destructive influence on papillary lines. Patients using this medicine are not able to be enrolled or verified in the biometric systems using fingerprint recognition. However, there are other drugs with possibly similar influence (where the occurance of hand-and-foot syndrome has been described), e.g. Cytosar-U®, FUDR®, Idamycin® or Doxil®.

Acknowledgements

This research has been done under the support of the following three grants: "*Security-Oriented Research in Information Technology*", MSM0021630528 (CZ), "*Information Technology in Biomedical Engineering*", GA102/09/H083 and "*Education of Liveness Testing in Subject Biometric Systems*", FR2525/2009/G1.

References

[1] Habif, T.P.: *Clinical Dermatology*, 4th Edition, Mosby, China, 2004, p. 1004, ISBN 978-0-323-01319-2.

[2] Moll, I.: *Dermatologie*, 6th Edition, Thieme – Dual Reihe, Germany, 2005, p. 592, ISBN 3-13-126686-4.

[3] Weston, W.L., Lane, A.T., Morelli, J.G.: *Color Textbook of Pediatric Dermatology*, Mosby Elsevier, China, 2007, p. 446, ISBN 978-03-23049-09-2.

[4] Wolff, K., Johnson, R.A., Suurmond, D.: *Color Atlas and Synopsis of Clinical Dermatology*, 5th Edition, McGraw-Hill, USA, 2005, p. 1085, ISBN 0-07-144019-4.

[5] Konkoľová, R.: *Korektivně dermatologické metody* (*Corrective Dermatologic Methods*), Maxdorf – Jessenius, Prague, CZ, 2001, p. 114, ISBN 80-85912-54-6.

[6] James, W.D., Berger, T.G., Elston, D.M.: *Andrew's Diseases of the Skin – Clinical Dermatology*, 10th Edition, Saunders Elsevier, Canada, 2006, p. 961, ISBN 0-8089-2351-X.

[7] Drahanský, M.: *Fingerprint Recognition Technology: Skin Diseases, Image Quality and Liveness Detection*, Habilitation Thesis, FIT BUT, 2008, p. 153.

[8] Vlašín, Z., Jedličková, H.: *Praktická dermatologie v obrazech a schématech* (*Practical Dermatology in Illustrations and Schematics*), Vladerma, Brno, CZ, 2001, p. 251, ISBN 80-238-6966-3.

[9] Chirillo, J., Blaul, S.: *Implementing Biometric Security*, Wiley Publishing, USA, 2003, p. 399, ISBN 0-7645-2502-6.

[10] Jain, A.K., Flynn, P., Ross, A.A.: *Handbook of Biometrics*, Springer-Verlag, 2008, p. 556, ISBN 978-0-387-71040-2.

[11] http://wissen.de.msn.com/photogallery_msn.aspx?cp-documentid=10756299&imageindex=3

Supplemental Biometric User Authentication for Digital-Signature Smart Cards

Olaf Henniger, Ulrich Waldmann

Fraunhofer Institute for Secure Information Technology
Rheinstr. 75
D-64295 Darmstadt, Germany
olaf.henniger@sit.fraunhofer.de
ulrich.waldmann@sit.fraunhofer.de

Abstract: This paper specifies how biometric verification methods can be applied in addition to PIN verification on digital-signature smart cards in compliance with established smart-card standards. After successful PIN verification, multiple digital signatures can be created; each signature creation, however, is preceded by biometric verification.

1 Motivation

Tamper-resistant, personal smart cards are used for the secure storage of private signature keys and as protected environment for the creation of digital signatures [DIN V 66291-1, Pie08, EN 14890-1]. For checking the access rights on the protected functions of a digital-signature smart card, also biometric features of the cardholder can be used in addition, or as alternative, to a secret PIN (personal identification number). The strengths of biometric methods lie in their relative ease of use. If sufficiently resistant against direct and indirect attacks, biometric user authentication methods can strengthen the binding of digital signatures to the legitimate signature-key owner since biometric characteristics are bound to a certain person. For user authentication prior to digital-signature creation, handwritten signatures show particular promise as they have found acceptance for a long time and are regarded as evidence of a deliberate decision of the signer.

In order that a successful verification cannot be feigned to the smart card whose signature-creation function is to be protected, the biometric features should be compared inside the smart card itself. On-card comparison offers the additional advantage that the biometric reference data of the legitimate cardholder never leave the smart card and remain protected against misuse in case the card is tampered with. It would be best if all steps of biometric verification – from biometric data capture over pre-processing, the extraction and comparison of features up to the accept/reject decision – were carried out within the protected smart card. Though prototypes of smart cards with an integrated biometric sensor already exist, we consider only the case that the sensor is off-card and biometric feature data is sent to the smart card for on-card comparison.

In case that a biometric user authentication method shows only a moderate attack resistance, it should be used only in addition (and not as an alternative) to PIN verification [SigV01]. We focus on this case. [TR-03115] suggests that the users must authenticate themselves once by entering their PIN and that afterwards multiple digital signatures can be created, before each of which the users must authenticate themselves by presenting their biometric characteristics. This paper specifies how to realise this in compliance with pertinent smart-card standards [ISO/IEC 7816-4]. This is new ground, not covered yet in digital-signature card specifications [DIN V 66291-1, Pie08, EN 14890-1].

Other aspects, such as how to convey the required format of the biometric probe to the off-card application [ISO/IEC 7816-11] and how to ensure that the biometric probe data handed over at the card interface are captured anew and not fed in by way of bypass or replay attacks [EN 14890-1], are out of scope of this paper because specified elsewhere.

2 Specification of user authentication procedure

2.1 Data objects

The on-card signature-creation application holds the private key needed for the creation of digital signatures. The private key is called PrK.

For user authentication prior to digital-signature creation, the application shall use a PIN consisting of at least six digits [EN 14890-1] and may, in addition to the PIN, also use a biometric reference (BR). PIN and BR are each associated with

- a retry counter indicating the number of remaining allowed verification attempts and
- a security status evaluation counter indicating how often the security status achieved after successful user authentication may be used until re-verification is required.

The initial values of the retry counters $\mathrm{PIN.RC_{start}}$ and $\mathrm{BR.RC_{start}}$ indicate the supported maximum number of verification attempts. $\mathrm{PIN.RC_{start}}$ should typically be 3 [EN 14890-1]. $\mathrm{BR.RC_{start}}$ depends on the chosen biometric method. The initial values of the security status evaluation counters $\mathrm{PIN.SSEC_{start}}$ and $\mathrm{BR.SSEC_{start}}$ should both be 0. Their maximum values $\mathrm{PIN.SSEC_{max}}$ and $\mathrm{BR.SSEC_{max}}$ indicate the supported maximum number of uses of the security status after successful verification. $\mathrm{PIN.SSEC_{max}}$ should be n with $n \geq 1$ or represent "infinity". $\mathrm{BR.SSEC_{max}}$ should be m with $1 \leq m \leq n$.

2.2 Access rules

Each access rule for data objects on the card consists of two parts: an access mode that indicates specific card commands and a security condition that is required to be met in order to get access to the object using that access mode. A security condition is expressed in terms of security statuses that may result from completion of authentication procedures. When trying to access a protected object, the card operating system checks whether the security condition is satisfied. If not, access to the object is denied, and an appropriate error message such as "Security status not satisfied" is returned.

The access rules for PIN, BR, and PrK should be set as described in Table 1 through Table 3. The tables also list actions to be executed when accessing PIN, BR, and PrK.

Table 1 Access rules for PIN

Access mode	Security condition	Actions to be executed
CHANGE REFERENCE DATA or RESET RETRY COUNTER	Application-specific/out of scope (e.g. successful master PIN verification)	− Change PIN and/or − PIN.RC := $PIN.RC_{start}$
VERIFY	ALWAYS	If PIN.RC > 0, then − Decrement PIN.RC − If the value from the command data field matches the PIN, then • PIN verification successful • PIN.RC := $PIN.RC_{start}$ • PIN.SSEC := $PIN.SSEC_{max}$
Other	NEVER	None

Table 2 Access rules for BR

Access mode	Security condition	Actions to be executed
CHANGE REFERENCE DATA	Application-specific/out of scope (e.g. successful master PIN verification)	Change BR
VERIFY	PIN.SSEC > 0 (PIN verification successful)	If BR.RC > 0, then − Decrement BR.RC − If the probe from the command data field matches BR, then • Biometric verification successful • BR.RC := $BR.RC_{start}$ • BR.SSEC := $BR.SSEC_{max}$
Other	NEVER	None

Table 3 Access rules for PrK

Access mode	Security condition	Actions to be executed
PSO: COMPUTE DIGITAL SIGNATURE	(PIN.SSEC > 0) AND (BR.SSEC > 0) (PIN verification and biometric verification successful)	− Decrement PIN.SSEC − Decrement BR.SSEC − Compute digital signature
Other	NEVER	None

2.3 User authentication procedure

[ISO/IEC 7816-4] describes how to specify conjunctions and disjunctions of security conditions, but not how to specify the temporal ordering of security conditions. Still, a two-stage user authentication procedure can be realised as follows: Security condition for accessing PrK is successful PIN verification and successful biometric verification, while security condition for biometric verification is successful PIN verification. This enforces that biometric verification is preceded by successful PIN verification.

The security status achieved after successfully verifying PIN or BR remains valid up to a reset of the card, the selection of a different on-card application, or until the associated security status evaluation counter (SSEC) reaches 0. The security status achieved after successful biometric verification should be reset after each PSO: COMPUTE DIGITAL SIGNATURE command. The security status achieved after successful PIN verification may remain valid for multiple subsequent commands.

2.4 Special cases

If the initial value of BR.SSEC (before any verification attempt) represents "infinity", then the biometric user authentication is skipped. The PIN verification is skipped if the initial value of PIN.SSEC is set to represent "infinity". In case that the attack resistance of the biometric user authentication method is assessed as "high", the PIN verification could be switched off without damage.

3 Outlook

The proposed solution for applying biometric user authentication methods in addition to PIN verification is being implemented in prototype OpenPGP cards with biometric on-card comparison. In OpenPGP cards, which do not aim at "qualified" electronic signatures (which have the same legal effects as handwritten signatures on paper), the biometric user authentication may even replace the PIN verification for convenience.

In spite of their ease of use and their strong binding to persons, biometric methods are barely used in products for creating qualified electronic signatures. One reason is that, as yet, no biometric product has attained a sufficient security certificate. This is not only because the security of biometric products may still need to be improved, but also because the IT security evaluation methodology needs to be adjusted to biometric products.

References

[DIN V 66291-1] Pre-standard DIN V 66291-1:2000. Chip cards with digital signature application/function according to SigG and SigV – Part 1: Application interface

[EN 14890-1] European Standard EN 14890-1:2008, Application interface for smart cards used as secure signature creation devices – Part 1: Basic services

[ISO/IEC 7816-4] International Standard ISO/IEC 7816-4:2005, Information technology – Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange

[ISO/IEC 7816-11] International Standard ISO/IEC 7816-11:2004, Information technology – Identification cards – Integrated circuit cards – Part 11: Personal verification through biometric methods

[Pie08] A. Pietig: Functional specification of the OpenPGP application on ISO smart card operating systems. Vers. 2.0, 2008

[SigV01] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV). 2001

[TR-03115] Bundesamt für Sicherheit in der Informationstechnik: Komfortsignatur mit dem Heilberufsausweis. Technische Richtlinie TR-03115, Vers. 2.0, 2007

Tamper-proof and privacy-protected fingerprint identification systems

Michael Schwaiger

secunet Security Networks AG
michael.schwaiger@secunet.com

Abstract: In this paper alternatives of tamper-proof and privacy-protected biometric identification systems are shown. One approach to secure such databases is to use cryptography. With its help it is possible to highly protect a system from any external attacker but an internal attacker still has direct access to all stored biometric data. This risk shall be avoided by using biometric encryption with another approach. In the following both approaches will be described and compared.

1 Introduction

Basically, it is possible to store biometric data on secure hardware (e.g. smartcards) which stays in possession of the owner. Nevertheless, there are lots of use cases where a central storage of biometric data in large databases is advantageous and preferred. Accordingly, interest in security of these databases arouses, too. Threats and possible points of attack [BCP+04] on biometric systems have to be taken seriously because misuse of biometric data can have serious and long-lasting implications. As opposed to passwords or cryptographic keys compromised biometric data cannot be changed. One main focus when collecting biometric data in large databases is data protection. According to national data protection laws in Europe biometric data need special protection as they allow other people to determine the identity of a person. Furthermore, they need suitable protection because it might be possible that sensitive information about the state of health of the corresponding person is extracted from the biometric feature.

This paper suggests two approaches to protect stored fingerprint data in identification systems. More detailed information regarding this topic can be found in [Sch09] and [MMJP03].

2 Conventional biometric solution

Biometrics itself does not offer any security mechanisms to protect captured and stored biometric data. One possibility is to use cryptography to protect the data. To ensure that only authenticated applications are communicating with the central database SSL/TLS

client authentication based on digital certificates is used. After the server's authenticity is verified and the SSL/TLS handshake is finished successfully the communication to the database system is encrypted. While every user of the system has the possibility to authenticate himself to the system not every user shall be allowed to enrol, delete, or modify other users. This is the job of the biometric enrolment operator. He is in possession of a secure token holding a signature certificate. By signing the template and adding the digital signature to the template the integrity of the fingerprint template can be ensured. Furthermore, after transmitting the template via the encrypted SSL/TLS communication link to the central system the digital signature is verified. Thus, it is ensured that only biometric enrolment operators (which have a secure token with a valid certificate) can enrol, delete, and modify users. On identification, the digital signature, which was created during enrolment, of all possible candidates of the identification process is verified. Only if the signature is valid this user will be added to the candidate list. Returning the candidate list to the local application again is SSL/TLS encrypted. Attacking any software parts of the whole system might lead to serious implications. Therefore, all software is digitally signed by code signatures. Every single software part is only executed if the digital signature is valid and thus no modifications were done.

Another characteristic of the system is the one-way approach. It ensures that biometric data can only be accessed in one direction. Only biometric enrolment operators who are in possession of a token (and the stored certificate) are eligible to enrol, update, or delete users and their fingerprint features. It is not possible to get the stored biometric information from the database and return it to the application. This is achieved by disabling all functions from the according communication interface which can read data from the database. Thus, once biometric data is stored in the database it does not leave the central system anymore. Only a unique identifier of the identified candidate is returned to the application.

The afore described architecture has been realised with a biometric middleware approach – secunet biomiddle [BNS07]. secunet biomiddle implements among other things the standardised BioAPI 2.0 Framework [ISO06] which is a modular interface for biometric devices and algorithms. The client application communicates with the biomiddle server which invokes calls to Biometric Service Providers (BSP). They implement the actual behaviour of the attached device or algorithm.

By using all mentioned security features many points of attack on biometric identification systems can be obviated. The use of SSL/TLS ensures that an attacker cannot read and change the data while transmitting it to the central system and back to the client application. It ensures authenticated access to the system and prevents attackers from replaying identification decisions. Creating and storing the digital signature of the minutiae template guarantees the integrity of the biometric data in the database. Furthermore, using code signatures prevents manipulating all applications and obviates Trojan horse attacks on feature extraction and matching algorithms. Finally, the one-way approach does not allow external attackers to get stored biometric data from the database. Nevertheless, an internal attacker who already has access to the database can read and misuse the stored biometric data. Encrypting the stored data would be one solution but is not feasible when using an identification system. As a result, only by using the mentioned cryptographic

mechanisms it is not possible to secure the biometric data in such a way that internal attackers cannot misuse the data. For this reason, some approaches which consider this issue were developed. Biometric encryption is one way to solve this problem.

3 Approach using biometric encryption

Biometric encryption can also protect the stored biometric data from an internal attacker. When using biometric encryption a verification string is stored as a reference instead of the biometric template. As an advantage the original biometric data cannot be reconstructed from the verification string. This feature is achieved by a function which cannot be calculated in the other direction. Only if the user is presenting his biometric feature which is similar to the enroled feature he can be authenticated. Additionally, some of the biometric encryption approaches also offer the possibility to extract a cryptographic key from the data.

One of these schemes is the BioKey approach [KMN09] which was designed and implemented by the German Federal Office for Information Security (BSI) and secunet Security Networks AG. It is a variant of the Fuzzy Vault scheme of Juels and Sudan [JS02]. The BioKey approach has some modifications compared to the original Fuzzy Vault scheme. Firstly, the entropy of one fingerprint is too low to design an approach which is resistant against known attacks [Mih07]. Thus, the system is designed to work with eight different fingerprints. To compensate rotations and translations of the fingerprint image instances an internal matching algorithm determines so called reliable minutiae within the given fingerprints during enrolment. A reliable minutia is a minutia which appears in a configurable amount of instances of the same fingerprint. As a result, minutiae which do not appear regularly in the captured fingerprint images (e.g. minutiae in edge regions of the image) will not be processed. This increases the authentication rate because minutiae which do not appear in every instance of the captured fingerprint image will be omitted during authentication. Secondly, there is a minimum limit of reliable minutiae per finger needed for a successful enrolment. Investigations showed that the matching rate increases drastically by using this requirement. Nevertheless, this results in a higher rejection rate during enrolment.

As an example, the BioKey approach was integrated to the conventional biometric solution. Now, an internal attacker who wants to misuse the stored verification string only succeeds with a certain probability. When choosing the right parameters of the algorithm this probability is less than 2^{-100} for each attempt. This is too low to start efficient attacks on the BioKey approach.

4 Summary and outlook

By using cryptography it is possible to achieve a high security level for biometric systems. As shown in the conventional approach, the integrity of the data and the authenticated

access to it as well as the encryption of the communication links between local and remote systems can be ensured. With the one-way approach it is not possible anymore to get the stored biometric data from the database. The approach using biometric encryption, however, adds more security to the system. The stored data itself is now protected against misuse, too. No more biometric raw data needs to be stored. Thus, the privacy of the biometric data is ensured as according to data protection laws. Nevertheless, there are some security concerns about this biometric encryption system as described in [Sch09] and [Mih07]. Also disadvantages in practicality of the BioKey approach need to be considered. Long template generation and identification time as well as a high failure to enrol rate are the major disadvantages. When designing and implementing a tamper-proof and privacy-protected fingerprint identification system these facts have to be taken into account. On the one hand more security and privacy for the stored data can be achieved; on the other hand the practicality is much lower than using the conventional approach. To establish biometric encryption for public usage, some more research has to be invested. The German Federal Office for Information Security (BSI) and secunet Security Networks AG are now optimising the developed approach regarding reliability and speed of the algorithm.

So far the BioKey approach is not fast enough and error-prone to be used as a privacy-protected identification solution. Nevertheless, the conventional approach offers high security for the stored biometric data as well. Many of these security features will also be necessary in the approach using biometric encryption, even if the BioKey algorithm will be optimised to be used in a real scenario.

References

[BCP+04] Ruud M. Bolle, Jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha, and Andrew W. Senior. *Guide to Biometrics*. Springer-Verlag, New York, 2004.

[BNS07] Marco Breitenstein, Markus Nuppeney, and Frank Steffens. *Biometrische Middleware basierend auf BioAPI 2.0.* In *Tagungsband BIOSIG 2007*, 2007.

[ISO06] ISO/IEC 19784-1:2006. *Information technology – Biometric application programming interface. Part 1: BioAPI specification*. ISO/IEC JTC 1/SC37, 2006.

[JS02] Ari Juels and Madhu Sudan. *A Fuzzy Vault Scheme*. In *Proceedings of IEEE International Symposium on Information Theory*. IEEE Press, 2002.

[KMN09] Ulrike Korte, Johannes Merkle, and Matthias Niesing. *Datenschutzfreundliche Authentisierung mit Fingerabdrücken*. In *Datenschutz und Datensicherheit*, volume 5, 2009.

[Mih07] Preda Mihailescu. *The Fuzzy Vault for fingerprints is Vulnerable to Brute Force Attack*. *ArXiv e-prints*, 0708.2974, 2007.

[MMJP03] Davide Maltoni, Dario Maio, Anil K. Jain, and Salil Prabhakar. *Handbook of Fingerprint Recognition*. Springer-Verlag, New York, 2003.

[Sch09] Michael Schwaiger. *Entwurf, Implementierung und Analyse von Varianten einer manipulationssicheren und datenschutzgerechten biometrischen Identifikationslösung*. Master's thesis, FH Oberösterreich, Campus Hagenberg, Austria, 2009.

On-line Signature Biometrics using Support Vector Machine

Aitor Mendaza-Ormaza, Oscar Miguel-Hurtado, Ivan Rubio-Polo, Raul Alonso-Moreno

University Group for Identification Technologies (GUTI) - Dpt. Electronics Technology
University Carlos III of Madrid
Avda. Universidad, 30
E-28911 Leganés (Madrid); SPAIN
{amendaza, omiguel, irubio, ramoreno}@ing.uc3m.es

1 Introduction

Handwritten signature has long been established as the most diffuse mean for personal verification in our daily life. It is commonly, in general, in all kind of legal documents and transactions. Therefore, within all biometric modalities, signature is probably the widest accepted. On the other hand, signature is a behavioural characteristic of individuals, and therefore is considered being weaker against fraud. Signature verification is the process in which, for a given signature who belongs to a user, a decision is made whether the signature has been made by that user, a genuine signature, or has been made by another user, a forgery signature. Typically, forged signatures have been classified into three groups: (1) random, (2) simple and (3) skilled [SB00]. The different methods for signature verification can be divided in two main groups: off-line (static) and on-line (dynamic). The off-line techniques are based in processing the digitalized grey-scale image of the signature written on a paper. On the contrary, on-line techniques take into account dynamic characteristics of the signature such as pressure exerted, tilts, position or velocity of the stylus. All this signals provide, not only information of the signature, but also information about the act of signing, which is consider more related to the specific user.

2 Support Vector Machines

SVM is a learning method introduced by V. Vapnik [CV95][Va95], for two-group classification problems. The machine maps the input vectors, with a non-linear mapping, to a very high-dimension feature space. In this feature space a decision surface (a hyperplane) is built which maximizes the distance from either class to the hyperplane and separates the largest possible number of points belonging to the same class on the same side (maximal margin between the vectors of the two classes). Therefore the misclassification error of data both in the training set and test set is minimized.

The basic algorithm of the SVMs uses linear thresholds. But with a simple change of the function (kernel) of the algorithm, $K(u,v)$, the SVMs can be used to learn other thresholds such as, Radial Based Functions (RBF) networks, or N-layer sigmoid neural networks. Authors have used a one-against-all approach. N genuine signatures are taken for one class, and M skilled forgeries are taken as the data for the other class. With this set, an SVM is trained and a model is obtained for each user.

3 Database and signal pre-processing

3.1 Data used for this work

The study of features extracted form a signature and the experimental evaluation of the on-line signature verification system was carry out thanks to the MCyT-Signature-Database Corpus, which is publicly available. This database is constituted of 100 different users. Each user has produced 25 genuine signatures, and 25 skilled forgeries are also captured. To capture the signatures of the database, a Wacom Intous A6 USB graphic tablet was used.

3.2 Pre-processing and Derived Features

The raw signals captured at MCyT need pre-processing to reduce noise and irrelevant information. In this paper the following pre-processing steps are used: i) Smoothing of the five temporal functions (x-axis, y-axis, pressure, azimuth and inclination) by a low pass filter to eliminate the noise introduced by the graphic tablet in the data capture. ii) Time normalization. iii) Location normalization: x-axis and y-axis temporal function are normalized through the mean of those function. iv) Size normalizing: x-axis and y-axis are normalized through the norm of the 2 dimension vector [x,y]. Pressure, azimuth and inclination are normalized by their maximum values. v) We then calculate the Speeds and Acceleration of the coordinates x-axis, y-axis, pressure, azimuth and inclination.

3.3 Features Study and Discrimination

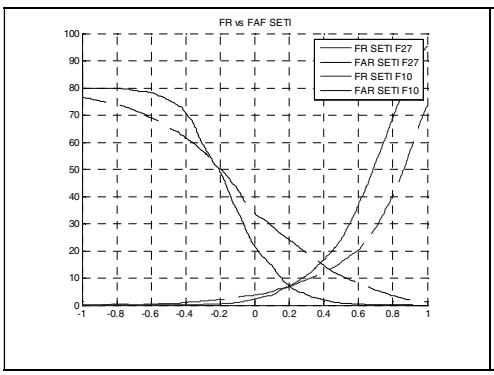
In order to use the most suitable set of features for on-line signature verification, a set of 138 features has been analyzed. This set of 138 features is obtained considering all signals given in the database (x, y, pen pressure p, pen azimuth az, pen inclination in). Also, as mentioned before, speeds and accelerations have been considered (sx, sy, sp, saz, sin, ax, ay, ap, aaz, ain). More precisely, for each of the primary coordinates captured directly by the tablet, 10 features have been analyzed. This means 50 features for a single signature. For each speed (s) and acceleration (a) (sx, sy, sp, saz, sin, ax, ay, ap, aaz, ain) of the primary coordinates, 8 features have been analyzed. Again, this means 80 features extracted from the 5 speeds and 5 accelerations. Moreover, 8 global features have also been analyzed. Therefore, a total of 138 features are obtained.

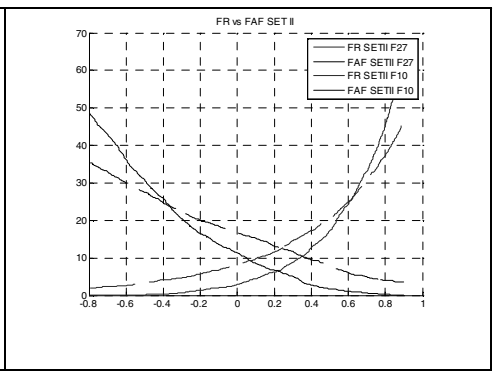
In order to obtain the optimal features for biometric verification, analysis using Fisher's Ratio has been done. In order to reduce even further the number of features obtained by mean of the Fishers' Ratio, a Principal Component Analysis (PCA) has also been employed. PCA can be defined as a process to get a few linear combinations which can be used to summarize data, losing as little information as possible. As it will be shown in the next section, a subset of features has been made up with a really small loss of discrimination.

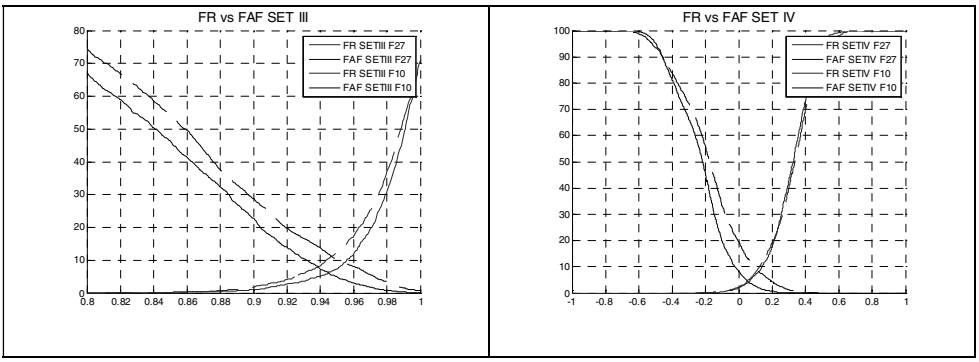
4 Experimental Results

A Classification's Error study has been carried out to measure discriminative power of the subset of features. Taking the first subset of features from Fisher's Ratio, the PCA process to discard features has been carried out. This has been done calculating the Classification's Error in each step to know the discriminative power of the feature subsets. The results obtained has lead to the authors to select two subsets, one of 27 features, and a second of only 10 features for applications where the data-size has a critical significance. The Classification's Error obtained is of 5% with the 27 Feature Set and of 6.5% with the 10 Feature Set. Once the two subsets have been chosen, a complete experimental evaluation for the proposed SVM algorithm has been conducted on MCyT Signature Database. Forgeries are classified into Random forgeries and Skilled ones. All signatures in database, both genuine and forgeries, from others users will be used as random forgeries for a determined user. Two parameters have been studied to know their influence in the authentication task: i) Number of signatures taken for enrolment process. It has been carried out experiments using 4 sets: 5 genuine and 5 skilled forgeries (set I), 5 genuine and 10 skilled forgeries (set II), 10 genuine and 5 skilled forgeries (set III) and 10 genuine and 10 skilled forgeries (set IV). ii) Number of Features. Both subsets, with 10 and 27 features have been analyzed.

The results obtained by the authors shows that the use of unbalanced sets of training signatures (sets II and III) only moves the EER in the FRvsFAF graphic to the left of the zero (set II) or to the right of the zero (set III). The improvement of the error trade-off curves between sets I and IV is very small and is not worth the effort of the user in the enrolment phase.







5 Conclusion

This paper introduces a complete methodology for feature selection using Fishers' Ratio in a first steep, and Principal Component Analysis to fine tune the selection. This has been applied to on-line handwritten signature biometrics. Also, throughout this work, Support Vector Machines has revealed as a successfully model for this biometric modality. This paper studied how the different parameters of the SVM and the appropriate choosing of elements for training (number of Features, number of signatures) are critical to obtain good performance of the system.

6 Acknowledgements

Authors would like to thank J. Ortega-Garcia and J. Fierrez-Aguilar for the provision of the MCyT Signature Database. This work has been funded by the Spanish Ministry of Science and Education (TEC2006-12365).

Bibliography

[CV95] C.Cortes and V.Vapnik, "Support-vector networks. Machine Learning", vol. 20, pp. :273-297, Nov. 1995.

[SB00] Sansone and Vento, "Signature Verification: Increasing Performance by a Multi-Stage System", Pattern Analysis & Applications, vol. 3, pp. 169–181, 2000.

[Va95] V.Vapnik, "The Nature of Statistical Learning Theory", Springer, 1995.

A Note on the Protection Level of Biometric Data in Electronic Passports

Harald Baier, CASED / Hochschule Darmstadt,
baier@cased.de

Tobias Straub, Duale Hochschule Baden-Württemberg Mannheim,
straub@dhbw-mannheim.de

Abstract: Following regulations of the EU Council in 2004, the member states have deployed electronic passports according to ICAO standards. Such documents contain an embedded radio frequency chip for storing personal data. The chip of a first generation German passport only duplicates the information which is already printed on the passport. In the current second version there are now also two fingerprints as additional biometric attributes apart from the digital facial image of the document owner.

The note at hand concentrates on attack vectors of biometric characteristics contained in the RF chip and discusses which threats towards fingerprints are thwarted. Our gist is to point to the low protection level of the facial image on the one hand and the high protection level of fingerprints on the other hand although both biometric characteristics are easy to gather.

1 Introduction

Following the regulation 2252/2004 of the Council of the European Union, Germany started in November 2005 to deploy the first generation of electronic passports (abbreviated ePass 1.0 in this document). Each ePass 1.0 contains a radio frequency chip (RF chip), which stores electronically the printed data in different data groups (DG). As a biometric attribute, the ePass 1.0 stores the facial image of its owner in data group 2 (DG2, see e.g. [KN07]). The choice of an RF chip and the organization of the data groups was due to international commitments as standardized by the International Civil Aviation Organization (ICAO) for machine-readable travel documents (MRTDs).[1]

In order to comply entirely with the regulation, Germany came up with a second generation of electronic passports (ePass 2.0) in November 2007. Besides the data of DG1 and DG2, the ePass 2.0 stores in data group DG3 two fingerprints of its owner (typically the two forefingers[2]). While fingerprints are currently checked in an automated fashion by inspection systems, the facial image is still controlled by a border official.

Up to now, the discussion on the security of electronic travel documents focuses on the wireless communication channel and the privacy issues [JMW05, MVV07, HHJ+06]. This

[1] see Document 9303, Part I, Volumes 1 and 2, `http://www.icao.org`

[2] see Passgesetz § 4, Abs. 4: `http://bundesrecht.juris.de/bundesrecht/pa_g_1986/`

is due to the fact that sniffing attacks and unauthorized access requests to the passport are much easier to put in practice than with a contact chip. In this note, we concentrate on alternative attack vectors to gather fingerprints with or without using the ePass 2.0. Some real-world attacks are described and assessed in Section 2. In Section 3 we come to the conclusion that facial images on the one hand and fingerprints on the other hand require the same protection level.

We aim at initiating a discussion on protection levels of different biometric characteristics. To our mind facial images and fingerprints are rather public and thus their protection level is comparable. Finally, we emphasise that we do not address the question whether biometric authentication is superior or not to other user authentication methods.

2 Attack Vectors on Fingerprints

In this section we reason about the appropriateness of the protection mechanisms for biometric data in electronic passports. Both in the public discussion accompanying the legislation process and among privacy experts it is up to now common sense that fingerprints have to be considered sensitive personal data[3]. At the same time the digital facial image of the ID card holder is deemed less critical as it can be captured easily anyway.

However, we argue that in the context of electronic passports threats towards fingerprints and towards facial images are comparable.[4] As we show below, our main argument is that fingerprints are also very easy to capture – even in the presence of sophisticated protection mechanisms like EAC (Extended Access Control, see e.g. [BSI08]), which we nevertheless consider a sound protocol to prevent unauthorized access to stored fingerprint images.

2.1 Gathering Fingerprints by Real-World Attacks

There are obvious and easy ways to obtain fingerprints which have not been discussed thoroughly in the context of passport security mechanisms. The key point is that each person carries her biometric characteristics with herself all the time. Hence it is not necessary to use a passport or other ID card as an attack vector, but the person herself will suffice. This has already been anticipated when considering the facial image as less sensitive information. We claim that this holds also true for fingerprints when taking into account practical real-world attacks. Here we distinguish two categories.

Analogue attacks without victim's active interaction: In everyday life it is virtually impossible for a human to avoid leaving fingerprints on objects that may fall into the hand of an attacker. Consider for instance doorknobs, handrails, a coffee cup, a hotel key card, or even a piece of (glossy) paper. Five years ago the German Chaos Computer Club (CCC)

[3] [KN07, p.178]: *Sensitive personenbezogene Daten wie Fingerabdrücke bedürfen eines besonders starken Schutzes [...].*

[4] Interestingly enough classical paper-based passports of some nations (e.g. from Africa) comprise fingerprints besides the facial image.

has already demonstrated how cheap it is to digitize a fingerprint and to prepare a dummy.[5] We estimate the cost to be less than 5 euros. Thus even less experienced attackers may use analogue fingerprints to surmount automated fingerprint authentication systems.

Digital attacks with victim's active interaction: There are two ways to obtain a person's fingerprint by interacting with her: Voluntarily and under pressure.

1. *Voluntarily*: Using some kind of social engineering or persuasion, an attacker may request the user to show her passport (as this is common practice in business transactions, e.g. when renting a car) and ask to provide the fingerprint as 'additional security measure to prevent misuse'. In this case the attacker only pretends to check it against the one stored in the ID card's chip (which he is not able to access). Such an attack is likely to succeed when users are not completely sure which parties are entitled to access fingerprints. We are very interested which result a lifelike study would deliver. We estimate that there would be a success ratio high enough to make this method promising for an interested attacker.

2. *Using Pressure*: A typical example is the recording of fingerprints and facial images by U.S. border control personnel in the aftermath of the 9-11 terror attacks. For a traveller to the U.S., the only alternative to providing biometric characteristics at the airport is to board the return flight. It is obvious that rogue nations will circumvent EAC by proceeding in a similar way.

2.2 Attacks on the Enrollment Process

Besides the storage medium of fingerprints (i.e. ePass 2.0) privacy concerns also seem appropriate concerning the enrollment procedure, that is the process of taking and storing fingerprints in the registry office and transmitting them to ID card producers.

In the context of biometrics it is a fundamental question where to store the reference data. In view of the ePass 2.0 a centralized nationwide database is currently not allowed.[6] While the protection provided by the chip is very high there seem to be probable attacks in order to apply for an authentic passport which contains the fingerprints of a different person:

1. A malware attack on the IT system of the registry office in order to steal or exchange fingerprints during enrollment has already been demonstrated.[7]

2. In order to call attention to potential weaknesses the CCC has published the fingerprint of the German Minister of the Interior, Wolfgang Schäuble, and asks citizens to apply for an ePass 2.0 using a dummy made out of it.[8]

[5] http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml

[6] With the deployment of electronic passports in Switzerland fingerprints will be stored in a central database (http://www.heise.de/newsticker/meldung/137989). Similar plans are discussed in the Netherlands (http://www.nrc.nl/international/Features/article2059482.ece).

[7] http://wiso.zdf.de/ZDFde/inhalt/9/0,1872,7510025,00.html,

[8] http://ccc.de/images/misc/schaeuble-attrappe.png?language=en

3 Conclusion and Future Prospects

We conclude from the real-world threats presented in Section 2 that it is easy to get fingerprints even if they are protected by EAC. We point out that this is simply a consequence of the fact that every individual carries his biometric characteristics with him all the time and that even a less-experienced attacker may harvest fingerprints without active interaction of his victim. In particular we do not consider this a weakness of biometrics or the cryptographic protocols.

We therefore assert that facial images and fingerprints require the same protection level in general. In case of electronic passports this means that either both should be protected by Basic Access Control (BAC, see e.g. [KN07]) or EAC. Because of the low threshold to get either a facial image or a fingerprint, BAC is sufficient to our mind.

To emphasize this assumption we quote the Ministry of the Interior[9] in the context of discussing the relevance of publishing the fingerprint of Wolfgang Schäuble: *So habe gerade das Bundesinnenministerium vor Einführung des E-Passes betont, dass es kaum Unterschiede zwischen einem Passfoto und dem elektronisch gespeicherten Fingerabdruck gebe.* Consequently for the prospective electronic ID cards in Germany, the same protection level for fingerprints and facial images will be implemented (using EAC and PACE [BKMN08]).

As a future work a classification of protection levels of biometric data should be developed. Since facial images are very easy and fingerprints are rather easy to gather, they belong to the class of 'public biometric characteristics'. In contrast, biometric data of iris, retina or veins belong to the 'private' class. Additionally, a study based on the *voluntarily digital attack* from Section 2.1 should be accomplished to confirm our assumption of this note.

References

[BKMN08] J. Bender, D. Kügler, M. Margraf, and I. Naumann. Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. *Datenschutz und Datensicherheit (DuD)*, 3:173–177, 2008.

[BSI08] BSI. *Advanced Security Mechanisms for Machine Readable Travel Documents*. TR-03110. German Federal Office for Information Security, 2008.

[HHJ+06] J.-H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk, and R. Schreur. Crossing Borders: Security and Privacy Issues of the European e-Passport. *IWSEC*, pages 152–167, 2006.

[JMW05] A. Juels, D. Molnar, and D. Wagner. Security and Privacy Issues in E-Passports. *IEEE. SecureComm 2005*, pages 74–88, 2005.

[KN07] D. Kügler and I. Naumann. Sicherheitsmechanismen für kontaktlose Chips im deutschen Reisepass. *Datenschutz und Datensicherheit (DuD)*, 3:176–180, 2007.

[MVV07] J. Monnerat, S. Vaudenay, and M. Vuagnoux. About Machine-Readable Travel Documents – Privacy Enhancement Using (Weakly) Non-Transferable Data Authentication. *RFIDSEC '07*, 2007.

[9] `http://www.heise.de/newsticker/meldung/105701`

Biometrie – Beschleuniger oder Bremser von Identitätsdiebstahl

Christoph Busch

Hochschule Darmstadt
CASED
Mornewegstr. 32
64293 Darmstadt
christoph.busch@h-da.de

Abstract: Der Beitrag betrachtet die Fragestellung, ob Biometrie als Beschleuniger oder Bremser von Identitätsdiebstahl betrachtet werden sollte. Dazu werden Szenarien betrachtet, in denen umfangreich Gesichtsbilddaten gesammelt werden. Diese Szenarien werden anhand etablierter Definitionen analysiert. Ferner werden Vorfälle von Identitätsmissbrauch betrachtet und eine Bewertung von Schutzmechanismen gegeben.

1 Einführung – Suchen und Sammeln

Die Qualität und Macht von Suchmaschinen hat in einem Ausmaß an Bedeutung gewonnen, das noch vor 10 Jahren undenkbar war. Die effizienten Suchdienste von Google gehören zu den Arbeitswerkzeugen, die täglich von Jedermann genutzt werden. Nicht überraschend, dass der Börsenwert von Google trotz Finanzkrise noch über 100 Milliarden US-Dollar liegt und das Unternehmen damit weltweit die wertvollste Marke am Aktienmarkt darstellt – vor Microsoft, Coca-Cola und IBM. Auch nicht überraschend, dass es einerseits immer wieder neue Versuche zur Nach-Ahmung dieses Erfolges gibt, wie jüngst die Produktankündigung ‚WolframAlpha'[Heise09a], und andererseits immer neue Suchfunktionalität ergänzt wird, um Marktpositionen auszubauen oder zu erobern. Wo liegt nun der Bezug zur Biometrie?

Nicht einmal drei Jahre ist es her, dass Google mit dem Zukauf des Unternehmens Neven Vision eine Biometrie-Technologie erwarb, die zu den besten verfügbaren Technologien gehörte wie der Anfang 2007 publizierte Face Recognition Vendor Test [FRVT2006] bestätigte. Die Spekulationen zum Hintergrund dieses Kaufs sind inzwischen Realität: Seit September letzten Jahres ist die Gesichtserkennung in Google-Picasa integriert. Aber auch kleine Unternehmen bieten mit neuen Produkten wie dem ‚Photo Finder' eine Technologie [pf09], die mit erstaunlicher Erkennungsleistung Bildarchive und Plattfomen wie facebook durchsucht- mit dem Ziel, Personen in unterschiedlichen Aufnahmesituationen wiederzufinden. ICAO-kompatible Aufnahmen wie sie im elektronischen Reisepass erwartet werden sind das nicht – und es funktioniert dennoch (leidlich).

Was vor Jahren noch Utopie war und als paranoider Gedanke abgetan wurde, das ist heute Realität: Die verbesserte Leistung der Gesichtserkennung macht den Aufbau von Personen-Bewegungs-Profilen möglich. Hinzu kommt die Bildaufzeichnung im öffentlichen Raum, die mit der wohlgemeinten Absicht aufgestellt werden, von Straftaten abzuschrecken oder sie zu vereiteln. Die signaltechnische Qualität von Raumüberwachungskameras führt zu einer immer höheren Bildauflösung, so dass eine Verknüpfung mit den oben genannten Bildspeichern technisch möglich wird. Von informationeller Selbstbestimmung der betroffenen Person kann man in diesem Fall faktisch nicht mehr sprechen. Die verpflichtend vorgeschriebenen Hinweise auf installierte Überwachungskameras werden nur zu leicht in der auch im Straßenalltag vorhandenen Informationsflut übersehen. Die neuerlich wieder fortgesetzten StreetView-Aufnahmen auf deutschen Straßen regen die Phantasie der besorgten Datenschützer weiter an, auch wenn die Plattformbetreiber versichern, dass Gesichter in dem Erweiterungsdienst von Google Maps nicht kenntlich würden.

2 Flüchtige biometrische Gesichtsbilder

Mitunter wird durch den Einsatz von Biometrie ein neues Risiko des Identitätsdiebstahls vermutet [ttt08]. Kann die Biometrie als Beschleuniger eines Identitätsdiebstahl betrachtet werden? Und wenn das ein konkretes Risiko sein sollte - welche Handlungsempfehlungen ergeben sich dann aus den oben geschilderten profilbildenden Gegebenheiten?

- Erstens die Einsicht, dass persönliche Bilder nicht unbedacht in öffentlichen Internet-Bildspeichern wie facebook verteilt werden sollten; der Austausch der Erinnerungsphotos von der letzten Firmenfeier kann auch in zugangsgeschützten Bereichen oder verschlüsselt erfolgen, wenn kein Intranet zur Verfügung steht.
- Zweitens das Verständnis, dass zweidimensionale Bilder eine Repräsentation einer ‚flüchtigen' biometrischen Charakteristik darstellen. Flüchtig ist eine Charakteristik dann, wenn sie auch ohne explizite Einwilligung der betroffenen Person erfasst und verarbeitet werden kann [ross06]. Auch der an einem Glas hinterlassene analoge Fingerabdruck zählt dazu.

- Drittens die Hoffnung, dass zweidimensionale Gesichtsbilder in Zwei-Faktor-Authentisierungsverfahren die Sicherheit steigern können. So war es ein Ziel der Einführung biometrischer Pässe, die Bindung des Passinhabers an den Pass zu stärken und somit das Risiko der Weitergabe (Vermietung) eines Passes und Nutzung durch eine Dritte Person zu reduzieren. Es wird erwartet, dass durch die biometrische Verifikation ein Missbrauch durch Weitergabe deutlich reduziert werden kann [zier2007]. Eine solche technische Prüfung wird bereits heute an vielen Grenzkontrollpunkten in Portugal vorgenommen und mit dem Projekt easyPASS ab August 2009 auch am Frankfurter Flughafen getestet werden.
- Viertens die Gewissheit, dass zweidimensionale Gesichtsbilder wie andere flüchtige Modalitäten nicht alleinstehend für eine sichere unüberwachte Zugangskontrolle ausreichen. Das Anfertigen von Plagiaten ist schlicht zu einfach. Für die logische und physikalische Zugangskontrolle ergibt sich daher die Notwendigkeit zur Messung von nicht-flüchtigen biometrischen Charakteristiken wie der dreidimensionalen Gesichtsgeometrie [bus2008] oder den Fingervenen[hart2009], deren Gegenwart nicht durch ein einfaches Plagiat vorgetäuscht werden kann.

3 Identitätsdiebstahl

Die beiden Begriffe Biometrie und Identitätsdiebstahl werden oft in einem Zusammenhang benutzt ohne dabei jedoch Klarheit über die Bedeutung der Begriffe zu haben.

3.1 Klärung der Begrifflichkeiten

Die Internationale Standardisierungsorganisation (ISO) hat eine klare Definition des Terminus Biometrie erarbeitet: „*automated recognition of individuals based on their behavioural and biological characteristics*“ [iso-sc37]. Schwieriger ist die Definition der Identität, da dieser Begriff nicht nur bei der körperlichen Erkennung von natürlichen Personen sondern auch im Zusammenhang von Personengruppen und deren Gedanken- und Stimmungwelt verwendet wird. Hier formuliert die ISO: „*Structured collection of an entity's attributes, allowing this entity to be distinguished and recognized from other entities within given contexts*“, wobei unter entity (Entität) eine ausgeprägte Existenz verstanden wird, die in einem Kontext einzigartig ist [iso-sc27]. Entitäten können natürliche Personen sein, aber auch Organisationen sowie aktive und passive Objekte. Der Tatbestand eines Diebstahls ist hingegen klar im §242 des Strafgesetzbuchs definiert: „*Wer eine fremde bewegliche Sache einem anderen in der Absicht wegnimmt, die Sache sich oder einem Dritten rechtswidrig zuzueignen, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.“*

3.1 Bewertung der Szenarien

Kommen wir zurück zur Betrachtung eines möglichen Identitätsdiebstahls. Zunächst wäre aus juristischer Sicht die Frage zu beantworten, ob das Sammeln von mehr oder weniger frei zugänglichen Bildern als Diebstahl im Sinne von §242 Strafgesetzbuch betrachtet werden kann. Wenn nicht - welcher Tatbestand ist gegebenenfalls zutreffender? Sicherlich ist die Verknüpfung von gesammelten Bildern und Überwachungsbildern ohne gesetzliche Grundlage als unrechtmäßig zu betrachten. Eine Einwilligung der betroffenen Personen liegt ja bei nicht-kooperativer Erfassung der Bilder nicht vor.

Unabhängig von der juristischen Bewertung für das oben beschriebene Gesamt-Szenario Raumüberwachung ergibt sich aus technischer Sicht jedoch als Ergebnis, dass Biometrie *nicht* als ein Beschleuniger von Identitätsdiebstahl betrachtet werden kann. Es wird in der Betrachtung deutlich, dass ein aufgezeichnetes zweidimensionales Bild nur *ein* Identitätsattribut einer Person ist – allerdings ein Attribut, das sonderlich flüchtig ist.

Ein Identitätsdiebstahl bedeutet aber doch mindestens die Kontrolle über einen umfangreichen oder vollständigen Satz von Identitätsattributen. Unter diesem Verständnis ist die - von der betroffenen Person unbemerkt durchgeführte - Beschaffung eines zweidimensionalen Lichtbildes daher kein Identitätsdiebstahl.

4 Identitätsmissbrauch

Ein Identitätsmissbrauch hingegen ist klar definierbar als Nutzung des Identitätsdiebstahls zum Schaden der betroffenen Person, wobei das vorrangige Interesse des Angreifers in aller Regel eine finanzielle Bereicherung ist. Das Risiko, Opfer eines solchen Ereignisses zu werden, ist in den vergangenen Jahren dramatisch gestiegen. Das Identity Theft Resource Center berichtet für das Jahr 2008 eine Zunahme von 47% im Vergleich zum Vorjahr [idtc2009a]. Die Liste der Einzelvorfälle dokumentiert zum Beispiel Kreditkartenbetrug, Kontenraub und Bankbetrug und zeigt die zur Beschaffung der notwendigen Informationen eingesetzte Spannbreite von Angriffen. Diese reichen von manipulierten Kartenlesern über Phishing-Angriffe bis hin zu ausgefeilten Social-Engineering-Angriffen, die zur unbedachten Preisgabe von sensitiven Daten motivieren. Diese Gefahren sind auch für Deutschland ein größer werdendes Problem, wie die Statistiken des Bundeskriminalamtes belegen [bka2008]. Hierzulande steigt die Zahl der Angriffe auf Geldautomaten um 50% pro Jahr. Der dadurch entstandene Schaden in 2007 wurde auf ca. 21 Millionen Euro beziffert. Hinzu kommt die zunehmende Manipulation von Point-of-Sales (POS)-Terminals zur Durchführung von Skimming-Angriffen. Diese Statistik lässt sich weiter fortführen – die Geschwindigkeit, mit der uns das Problem begegnet, wird jedoch schon mit diesen Zahlen deutlich. Es bleibt dabei den geschädigten Opfern auch nur ein schwacher Trost, wenn nach dem Diebstahl der Identitäts-Informationen der eigentliche Missbrauch im Ausland getätigt wird. Inländische Bankautomaten überprüfen die integrierten Sicherheitsmerkmale der Karte und können daher ein Duplikat vom Original unterscheiden.

5 Zusammenfassung

Identitätsdiebstahl wird ein zunehmend kritisches Problem, für das bald griffige Lösungen gefunden werden müssen. Der den Finanzbereich betreffende Anteil kann bald jeden Bürger betreffen. Der durch diese Art von Identitätsdiebstahl angerichtete Schaden ließe sich bremsen, wenn europaweit für großvolumige Transaktionen, neben den Faktoren Besitz (Original-Karte) und Wissen (Pin) auch die Präsentation und Überprüfung einer nicht flüchtigen biometrischen Charakteristik erforderlich wird. Die biometrischen Modalitäten der drei-dimensionalen Gesichtserkennung und der Venenerkennung sind zu diesem Zweck besonders geeignet.

Literaturverzeichnis

[Heise06] Heiseticker: Google erweitert Picasa um Gesichtserkennung, http://www.heise.de/newsticker/meldung/76881, August 2006

[Heise09a] Heiseticker: "Antwortmaschine" Wolfram Alpha im ersten Test, http://www.heise.de/newsticker/meldung/137330, Mai 2009

[apc08] APC: Google Picasa gets face recognition, http://apcmag.com/Google_Picasa_gets_face_recognition.htm, September 2008

[FRVT2006] J. Philips: NISTIR 7408 - FRVT 2006 and ICE 2006 Large-Scale Results, März 2007

[pf09] Face.Com: Photo Finder on facebook, http://www.face.com/, April 2009

[Heise09b] Heiseticker: Google macht wieder Fotos für Street View, http://www.heise.de/newsticker/meldung/135281, Mai 2009

[ttt08] TeleTrust Whitepaper: Datenschutz in der Biometrie, http://www.teletrust.org/uploads/media/Datenschutz-in-der-Biometrie-080521.pdf, Mai 2008

[ross06] A. Rossnagel: Biometrie – Schutz und Gefährdung von Grundrechten, Tagungsband Biometrie und Datenschutz – der vermessene Mensch, Peter Schaar (Editor), Juni 2006

[zier2007] J. Ziercke: Stellungnahme zum Passgesetz, Expertenanhörung im Innenausschuss des Deutschen Bundestages, April 2007

[bus2008] C. Busch, A. Nouak: 3D-Gesichtserkennung für die unbeaufsichtigte Grenzkontrolle, in Tagungsband Sicherheit 2008, GI-LNI, April 2008

[hart2009] D. Hartung: Venenbilderkennung, in DuD 6/2009, Juni 2009

[iso-sc37] ISO/IEC JTC1 SC37 SD2 Harmonized Biometric Vocabulary, Feb. 2009

[iso-sc27] ISO/IEC JTC1 SC27 A Framework for Identity Management, June 2009

[idtc2009a] Identity Theft Resource Center: Security Breaches 2008, http://www.idtheftcenter.org/artman2/publish/lib_survey/Breaches_2008.shtml, März 2009

[idtc2009b] Identity Theft Resource Center: 2009 ITRC Breach Report, http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml#, Mai 2009

[bka2008] Bundeskriminalamt: Aktuelle Herausforderungen in der Kriminalitätsbekämpfung, http://www.bka.de/pressemitteilungen/2008/pm080328.html, März 2008

GI-Edition Lecture Notes in Informatics

P-1 Gregor Engels, Andreas Oberweis, Albert Zündorf (Hrsg.): Modellierung 2001.

P-2 Mikhail Godlevsky, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications, ISTA'2001.

P-3 Ana M. Moreno, Reind P. van de Riet (Hrsg.): Applications of Natural Language to Information Systems, NLDB'2001.

P-4 H. Wörn, J. Mühling, C. Vahl, H.-P. Meinzer (Hrsg.): Rechner- und sensorgestützte Chirurgie; Workshop des SFB 414.

P-5 Andy Schürr (Hg.): OMER – Object-Oriented Modeling of Embedded Real-Time Systems.

P-6 Hans-Jürgen Appelrath, Rolf Beyer, Uwe Marquardt, Heinrich C. Mayr, Claudia Steinberger (Hrsg.): Unternehmen Hochschule, UH'2001.

P-7 Andy Evans, Robert France, Ana Moreira, Bernhard Rumpe (Hrsg.): Practical UML-Based Rigorous Development Methods – Countering or Integrating the extremists, pUML'2001.

P-8 Reinhard Keil-Slawik, Johannes Magenheim (Hrsg.): Informatikunterricht und Medienbildung, INFOS'2001.

P-9 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Innovative Anwendungen in Kommunikationsnetzen, 15. DFN Arbeitstagung.

P-10 Mirjam Minor, Steffen Staab (Hrsg.): 1st German Workshop on Experience Management: Sharing Experiences about the Sharing Experience.

P-11 Michael Weber, Frank Kargl (Hrsg.): Mobile Ad-Hoc Netzwerke, WMAN 2002.

P-12 Martin Glinz, Günther Müller-Luschnat (Hrsg.): Modellierung 2002.

P-13 Jan von Knop, Peter Schirmbacher and Viljan Mahni_ (Hrsg.): The Changing Universities – The Role of Technology.

P-14 Robert Tolksdorf, Rainer Eckstein (Hrsg.): XML-Technologien für das Semantic Web – XSW 2002.

P-15 Hans-Bernd Bludau, Andreas Koop (Hrsg.): Mobile Computing in Medicine.

P-16 J. Felix Hampe, Gerhard Schwabe (Hrsg.): Mobile and Collaborative Busi-ness 2002.

P-17 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Zukunft der Netze –Die Verletzbarkeit meistern, 16. DFN Arbeitstagung.

P-18 Elmar J. Sinz, Markus Plaha (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2002.

P-19 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3.Okt. 2002 in Dortmund.

P-20 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3.Okt. 2002 in Dortmund (Ergänzungsband).

P-21 Jörg Desel, Mathias Weske (Hrsg.): Promise 2002: Prozessorientierte Methoden und Werkzeuge für die Entwicklung von Informationssystemen.

P-22 Sigrid Schubert, Johannes Magenheim, Peter Hubwieser, Torsten Brinda (Hrsg.): Forschungsbeiträge zur "Didaktik der Informatik" – Theorie, Praxis, Evaluation.

P-23 Thorsten Spitta, Jens Borchers, Harry M. Sneed (Hrsg.): Software Management 2002 – Fortschritt durch Beständigkeit

P-24 Rainer Eckstein, Robert Tolksdorf (Hrsg.): XMIDX 2003 – XML-Technologien für Middleware – Middleware für XML-Anwendungen

P-25 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Commerce – Anwendungen und Perspektiven – 3. Workshop Mobile Commerce, Universität Augsburg, 04.02.2003

P-26 Gerhard Weikum, Harald Schöning, Erhard Rahm (Hrsg.): BTW 2003: Datenbanksysteme für Business, Technologie und Web

P-27 Michael Kroll, Hans-Gerd Lipinski, Kay Melzer (Hrsg.): Mobiles Computing in der Medizin

P-28 Ulrich Reimer, Andreas Abecker, Steffen Staab, Gerd Stumme (Hrsg.): WM 2003: Professionelles Wissensmanagement – Erfahrungen und Visionen

P-29 Antje Düsterhöft, Bernhard Thalheim (Eds.): NLDB'2003: Natural Language Processing and Information Systems

P-30 Mikhail Godlevsky, Stephen Liddle, Heinrich C. Mayr (Eds.): Information Systems Technology and its Applications

P-31 Arslan Brömme, Christoph Busch (Eds.): BIOSIG 2003: Biometrics and Electronic Signatures

P-32 Peter Hubwieser (Hrsg.): Informatische Fachkonzepte im Unterricht – INFOS 2003

P-33 Andreas Geyer-Schulz, Alfred Taudes (Hrsg.): Informationswirtschaft: Ein Sektor mit Zukunft

P-34 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 1)

P-35 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 2)

P-36 Rüdiger Grimm, Hubert B. Keller, Kai Rannenberg (Hrsg.): Informatik 2003 – Mit Sicherheit Informatik

P-37 Arndt Bode, Jörg Desel, Sabine Rathmayer, Martin Wessner (Hrsg.): DeLFI 2003: e-Learning Fachtagung Informatik

P-38 E.J. Sinz, M. Plaha, P. Neckel (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2003

P-39 Jens Nedon, Sandra Frings, Oliver Göbel (Hrsg.): IT-Incident Management & IT-Forensics – IMF 2003

P-40 Michael Rebstock (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2004

P-41 Uwe Brinkschulte, Jürgen Becker, Dietmar Fey, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle, Thomas Runkler (Edts.): ARCS 2004 – Organic and Pervasive Computing

P-42 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Economy – Transaktionen und Prozesse, Anwendungen und Dienste

P-43 Birgitta König-Ries, Michael Klein, Philipp Obreiter (Hrsg.): Persistance, Scalability, Transactions – Database Mechanisms for Mobile Applications

P-44 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): Security, E-Learning. E-Services

P-45 Bernhard Rumpe, Wofgang Hesse (Hrsg.): Modellierung 2004

P-46 Ulrich Flegel, Michael Meier (Hrsg.): Detection of Intrusions of Malware & Vulnerability Assessment

P-47 Alexander Prosser, Robert Krimmer (Hrsg.): Electronic Voting in Europe – Technology, Law, Politics and Society

P-48 Anatoly Doroshenko, Terry Halpin, Stephen W. Liddle, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications

P-49 G. Schiefer, P. Wagner, M. Morgenstern, U. Rickert (Hrsg.): Integration und Datensicherheit – Anforderungen, Konflikte und Perspektiven

P-50 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 1) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-51 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 2) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-52 Gregor Engels, Silke Seehusen (Hrsg.): DELFI 2004 – Tagungsband der 2. e-Learning Fachtagung Informatik

P-53 Robert Giegerich, Jens Stoye (Hrsg.): German Conference on Bioinformatics – GCB 2004

P-54 Jens Borchers, Ralf Kneuper (Hrsg.): Softwaremanagement 2004 – Outsourcing und Integration

P-55 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): E-Science und Grid Adhoc-Netze Medienintegration

P-56 Fernand Feltz, Andreas Oberweis, Benoit Otjacques (Hrsg.): EMISA 2004 – Informationssysteme im E-Business und E-Government

P-57 Klaus Turowski (Hrsg.): Architekturen, Komponenten, Anwendungen

P-58 Sami Beydeda, Volker Gruhn, Johannes Mayer, Ralf Reussner, Franz Schweiggert (Hrsg.): Testing of Component-Based Systems and Software Quality

P-59 J. Felix Hampe, Franz Lehner, Key Pousttchi, Kai Ranneberg, Klaus Turowski (Hrsg.): Mobile Business – Processes, Platforms, Payments

P-60 Steffen Friedrich (Hrsg.): Unterrichtskonzepte für inforrmatische Bildung

P-61 Paul Müller, Reinhard Gotzhein, Jens B. Schmitt (Hrsg.): Kommunikation in verteilten Systemen

P-62 Federrath, Hannes (Hrsg.): „Sicherheit 2005“ – Sicherheit – Schutz und Zuverlässigkeit

P-63 Roland Kaschek, Heinrich C. Mayr, Stephen Liddle (Hrsg.): Information Systems – Technology and ist Applications

P-64 Peter Liggesmeyer, Klaus Pohl, Michael Goedicke (Hrsg.): Software Engineering 2005

P-65 Gottfried Vossen, Frank Leymann, Peter Lockemann, Wolffried Stucky (Hrsg.): Datenbanksysteme in Business, Technologie und Web

P-66 Jörg M. Haake, Ulrike Lucke, Djamshid Tavangarian (Hrsg.): DeLFI 2005: 3. deutsche e-Learning Fachtagung Informatik

P-67 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 1)

P-68 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 2)

P-69 Robert Hirschfeld, Ryszard Kowalcyk, Andreas Polze, Matthias Weske (Hrsg.): NODe 2005, GSEM 2005

P-70 Klaus Turowski, Johannes-Maria Zaha (Hrsg.): Component-oriented Enterprise Application (COAE 2005)

P-71 Andrew Torda, Stefan Kurz, Matthias Rarey (Hrsg.): German Conference on Bioinformatics 2005

P-72 Klaus P. Jantke, Klaus-Peter Fähnrich, Wolfgang S. Wittig (Hrsg.): Marktplatz Internet: Von e-Learning bis e-Payment

P-73 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): “Heute schon das Morgen sehen“

P-74 Christopher Wolf, Stefan Lucks, Po-Wah Yau (Hrsg.): WEWoRC 2005 – Western European Workshop on Research in Cryptology

P-75 Jörg Desel, Ulrich Frank (Hrsg.): Enterprise Modelling and Information Systems Architecture

P-76 Thomas Kirste, Birgitta König-Riess, Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Informationssysteme – Potentiale, Hindernisse, Einsatz

P-77 Jana Dittmann (Hrsg.): SICHERHEIT 2006

P-78 K.-O. Wenkel, P. Wagner, M. Morgenstern, K. Luzi, P. Eisermann (Hrsg.): Land- und Ernährungswirtschaft im Wandel

P-79 Bettina Biel, Matthias Book, Volker Gruhn (Hrsg.): Softwareengineering 2006

P-80 Mareike Schoop, Christian Huemer, Michael Rebstock, Martin Bichler (Hrsg.): Service-Oriented Electronic Commerce

P-81 Wolfgang Karl, Jürgen Becker, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle (Hrsg.): ARCS´06

P-82 Heinrich C. Mayr, Ruth Breu (Hrsg.): Modellierung 2006

P-83 Daniel Huson, Oliver Kohlbacher, Andrei Lupas, Kay Nieselt and Andreas Zell (eds.): German Conference on Bioinformatics

P-84 Dimitris Karagiannis, Heinrich C. Mayr, (Hrsg.): Information Systems Technology and its Applications

P-85 Witold Abramowicz, Heinrich C. Mayr, (Hrsg.): Business Information Systems

P-86 Robert Krimmer (Ed.): Electronic Voting 2006

P-87 Max Mühlhäuser, Guido Rößling, Ralf Steinmetz (Hrsg.): DELFI 2006: 4. e-Learning Fachtagung Informatik

P-88 Robert Hirschfeld, Andreas Polze, Ryszard Kowalczyk (Hrsg.): NODe 2006, GSEM 2006

P-90 Joachim Schelp, Robert Winter, Ulrich Frank, Bodo Rieger, Klaus Turowski (Hrsg.): Integration, Informationslogistik und Architektur

P-91 Henrik Stormer, Andreas Meier, Michael Schumacher (Eds.): European Conference on eHealth 2006

P-92 Fernand Feltz, Benoît Otjacques, Andreas Oberweis, Nicolas Poussing (Eds.): AIM 2006

P-93 Christian Hochberger, Rüdiger Liskowsky (Eds.): INFORMATIK 2006 – Informatik für Menschen, Band 1

P-94 Christian Hochberger, Rüdiger Liskowsky (Eds.): INFORMATIK 2006 – Informatik für Menschen, Band 2

P-95 Matthias Weske, Markus Nüttgens (Eds.): EMISA 2005: Methoden, Konzepte und Technologien für die Entwicklung von dienstbasierten Informationssystemen

P-96 Saartje Brockmans, Jürgen Jung, York Sure (Eds.): Meta-Modelling and Ontologies

P-97 Oliver Göbel, Dirk Schadt, Sandra Frings, Hardo Hase, Detlef Günther, Jens Nedon (Eds.): IT-Incident Mangament & IT-Forensics – IMF 2006

P-98 Hans Brandt-Pook, Werner Simonsmeier und Thorsten Spitta (Hrsg.): Beratung in der Softwareentwicklung – Modelle, Methoden, Best Practices

P-99 Andreas Schwill, Carsten Schulte, Marco Thomas (Hrsg.): Didaktik der Informatik

P-100 Peter Forbrig, Günter Siegel, Markus Schneider (Hrsg.): HDI 2006: Hochschuldidaktik der Informatik

P-101 Stefan Böttinger, Ludwig Theuvsen, Susanne Rank, Marlies Morgenstern (Hrsg.): Agrarinformatik im Spannungsfeld zwischen Regionalisierung und globalen Wertschöpfungsketten

P-102 Otto Spaniol (Eds.): Mobile Services and Personalized Environments

P-103 Alfons Kemper, Harald Schöning, Thomas Rose, Matthias Jarke, Thomas Seidl, Christoph Quix, Christoph Brochhaus (Hrsg.): Datenbanksysteme in Business, Technologie und Web (BTW 2007)

P-104 Birgitta König-Ries, Franz Lehner, Rainer Malaka, Can Türker (Hrsg.) MMS 2007: Mobilität und mobile Informationssysteme

P-105 Wolf-Gideon Bleek, Jörg Raasch, Heinz Züllighoven (Hrsg.) Software Engineering 2007

P-106 Wolf-Gideon Bleek, Henning Schwentner, Heinz Züllighoven (Hrsg.) Software Engineering 2007 – Beiträge zu den Workshops

P-107 Heinrich C. Mayr, Dimitris Karagiannis (eds.) Information Systems Technology and its Applications

P-108 Arslan Brömme, Christoph Busch, Detlef Hühnlein (eds.) BIOSIG 2007: Biometrics and Electronic Signatures

P-109 Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, Marc Ronthaler (Hrsg.) INFORMATIK 2007 Informatik trifft Logistik Band 1

P-110 Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, Marc Ronthaler (Hrsg.) INFORMATIK 2007 Informatik trifft Logistik Band 2

P-111 Christian Eibl, Johannes Magenheim, Sigrid Schubert, Martin Wessner (Hrsg.) DeLFI 2007: 5. e-Learning Fachtagung Informatik

P-112 Sigrid Schubert (Hrsg.) Didaktik der Informatik in Theorie und Praxis

P-113 Sören Auer, Christian Bizer, Claudia Müller, Anna V. Zhdanova (Eds.) The Social Semantic Web 2007 Proceedings of the 1st Conference on Social Semantic Web (CSSW)

P-114 Sandra Frings, Oliver Göbel, Detlef Günther, Hardo G. Hase, Jens Nedon, Dirk Schadt, Arslan Brömme (Eds.) IMF2007 IT-incident management & IT-forensics Proceedings of the 3rd International Conference on IT-Incident Management & IT-Forensics

P-115 Claudia Falter, Alexander Schliep, Joachim Selbig, Martin Vingron and Dirk Walther (Eds.) German conference on bioinformatics GCB 2007

P-116 Witold Abramowicz, Leszek Maciszek (Eds.) Business Process and Services Computing 1st International Working Conference on Business Process and Services Computing BPSC 2007

P-117 Ryszard Kowalczyk (Ed.) Grid service engineering and manegement The 4th International Conference on Grid Service Engineering and Management GSEM 2007

P-118 Andreas Hein, Wilfried Thoben, Hans-Jürgen Appelrath, Peter Jensch (Eds.) European Conference on ehealth 2007

P-119 Manfred Reichert, Stefan Strecker, Klaus Turowski (Eds.) Enterprise Modelling and Information Systems Architectures Concepts and Applications

P-120 Adam Pawlak, Kurt Sandkuhl, Wojciech Cholewa, Leandro Soares Indrusiak (Eds.) Coordination of Collaborative Engineering - State of the Art and Future Challenges

P-121 Korbinian Herrmann, Bernd Bruegge (Hrsg.) Software Engineering 2008 Fachtagung des GI-Fachbereichs Softwaretechnik

P-122 Walid Maalej, Bernd Bruegge (Hrsg.) Software Engineering 2008 - Workshopband Fachtagung des GI-Fachbereichs Softwaretechnik

P-123 Michael H. Breitner, Martin Breunig, Elgar Fleisch, Ley Pousttchi, Klaus Turowski (Hrsg.)
Mobile und Ubiquitäre Informationssysteme – Technologien, Prozesse, Marktfähigkeit
Proceedings zur 3. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2008)

P-124 Wolfgang E. Nagel, Rolf Hoffmann, Andreas Koch (Eds.)
9th Workshop on Parallel Systems and Algorithms (PASA)
Workshop of the GI/ITG Speciel Interest Groups PARS and PARVA

P-125 Rolf A.E. Müller, Hans-H. Sundermeier, Ludwig Theuvsen, Stephanie Schütze, Marlies Morgenstern (Hrsg.)
Unternehmens-IT: Führungsinstrument oder Verwaltungsbürde
Referate der 28. GIL Jahrestagung

P-126 Rainer Gimnich, Uwe Kaiser, Jochen Quante, Andreas Winter (Hrsg.)
10th Workshop Software Reengineering (WSR 2008)

P-127 Thomas Kühne, Wolfgang Reisig, Friedrich Steimann (Hrsg.)
Modellierung 2008

P-128 Ammar Alkassar, Jörg Siekmann (Hrsg.)
Sicherheit 2008
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)
2.-4. April 2008
Saarbrücken, Germany

P-129 Wolfgang Hesse, Andreas Oberweis (Eds.)
Sigsand-Europe 2008
Proceedings of the Third AIS SIGSAND European Symposium on Analysis, Design, Use and Societal Impact of Information Systems

P-130 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
1. DFN-Forum Kommunikations-technologien Beiträge der Fachtagung

P-131 Robert Krimmer, Rüdiger Grimm (Eds.)
3rd International Conference on Electronic Voting 2008
Co-organized by Council of Europe, Gesellschaft für Informatik and E-Voting.CC

P-132 Silke Seehusen, Ulrike Lucke, Stefan Fischer (Hrsg.)
DeLFI 2008:
Die 6. e-Learning Fachtagung Informatik

P-133 Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, Christian Scheideler (Hrsg.)
INFORMATIK 2008
Beherrschbare Systeme – dank Informatik
Band 1

P-134 Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, Christian Scheideler (Hrsg.)
INFORMATIK 2008
Beherrschbare Systeme – dank Informatik
Band 2

P-135 Torsten Brinda, Michael Fothe, Peter Hubwieser, Kirsten Schlüter (Hrsg.)
Didaktik der Informatik – Aktuelle Forschungsergebnisse

P-136 Andreas Beyer, Michael Schroeder (Eds.)
German Conference on Bioinformatics GCB 2008

P-137 Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.)
BIOSIG 2008: Biometrics and Electronic Signatures

P-138 Barbara Dinter, Robert Winter, Peter Chamoni, Norbert Gronau, Klaus Turowski (Hrsg.)
Synergien durch Integration und Informationslogistik
Proceedings zur DW2008

P-139 Georg Herzwurm, Martin Mikusz (Hrsg.)
Industrialisierung des Software-Managements
Fachtagung des GI-Fachausschusses Management der Anwendungsentwick-lung und -wartung im Fachbereich Wirtschaftsinformatik

P-140 Oliver Göbel, Sandra Frings, Detlef Günther, Jens Nedon, Dirk Schadt (Eds.)
IMF 2008 - IT Incident Management & IT Forensics

P-141 Peter Loos, Markus Nüttgens, Klaus Turowski, Dirk Werth (Hrsg.)
Modellierung betrieblicher Informations-systeme (MobIS 2008)
Modellierung zwischen SOA und Compliance Management

P-142 R. Bill, P. Korduan, L. Theuvsen, M. Morgenstern (Hrsg.)
Anforderungen an die Agrarinformatik durch Globalisierung und Klimaveränderung

P-143 Peter Liggesmeyer, Gregor Engels, Jürgen Münch, Jörg Dörr, Norman Riegel (Hrsg.)
Software Engineering 2009
Fachtagung des GI-Fachbereichs Softwaretechnik

P-144 Johann-Christoph Freytag, Thomas Ruf, Wolfgang Lehner, Gottfried Vossen (Hrsg.)
Datenbanksysteme in Business, Technologie und Web (BTW)

P-145 Knut Hinkelmann, Holger Wache (Eds.)
WM2009: 5th Conference on Professional Knowledge Management

P-146 Markus Bick, Martin Breunig, Hagen Höpfner (Hrsg.)
Mobile und Ubiquitäre Informationssysteme – Entwicklung, Implementierung und Anwendung
4. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2009)

P-147 Witold Abramowicz, Leszek Maciaszek, Ryszard Kowalczyk, Andreas Speck (Eds.)
Business Process, Services Computing and Intelligent Service Management
BPSC 2009 · ISM 2009 · YRW-MBP 2009

P-148 Christian Erfurth, Gerald Eichler, Volkmar Schau (Eds.)
9th International Conference on Innovative Internet Community Systems
I^2CS 2009

P-149 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
2. DFN-Forum Kommunikationstechnologien
Beiträge der Fachtagung

P-150 Jürgen Münch, Peter Liggesmeyer (Hrsg.)
Software Engineering
2009 - Workshopband

P-151 Armin Heinzl, Peter Dadam, Stefan Kirn, Peter Lockemann (Eds.)
PRIMIUM
Process Innovation for Enterprise Software

P-152 Jan Mendling, Stefanie Rinderle-Ma, Werner Esswein (Eds.)
Enterprise Modelling and Information Systems Architectures
Proceedings of the 3rd Int'l Workshop EMISA 2009

P-153 Andreas Schwill, Nicolas Apostolopoulos (Hrsg.)
Lernen im Digitalen Zeitalter
DeLFI 2009 – Die 7. E-Learning Fachtagung Informatik

P-154 Stefan Fischer, Erik Maehle Rüdiger Reischuk (Hrsg.)
INFORMATIK 2009
Im Focus das Leben

P-155 Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.)
BIOSIG 2009:
Biometrics and Electronic Signatures
Proceedings of the Special Interest Group on Biometrics and Electronic Signatures

P-156 Bernhard Koerber (Hrsg.)
Zukunft braucht Herkunft
25 Jahre »INFOS – Informatik und Schule«

The titles can be purchased at:

Köllen Druck + Verlag GmbH
Ernst-Robert-Curtius-Str. 14 · D-53117 Bonn
Fax: +49 (0)228/9898222
E-Mail: druckverlag@koellen.de