NTNU

Norwegian University of
Science and Technology

FiPrAD - A Guideline for Fingerprint Presentation Attack Database Creation

Author(s)

Ahmed S. M. Madhun

Bachelor in Information Security
20 ECTS
Department of Information Security and Communication Technology
Norwegian University of Science and Technology,

30.11.2018

Supervisor Dr. Marta Gomez-Barrero
Prof. Dr. Christoph Busch

Sammendrag av Bacheloroppgaven

Tittel:	**FiPrAD - En retningslinje for oppretting av fingeravtrykk presentasjon angrep database**
Dato:	30.11.2018
Deltakere:	Ahmed S. M. Madhun
Veiledere:	Dr. Marta Gomez-Barrero Prof. Dr. Christoph Busch
Oppdragsgiver:	Biometrics and internet security research group **(da/sec)**
Kontaktperson:	Dr. Marta Gomez-Barrero, marta.gomez-barrero@h-da.de
Nøkkelord:	Biometrics, Fingertrykk, database, presentasjonsangrep, sikkerhet, foskning, Engelsk
Antall sider:	73
Antall vedlegg:	7
Tilgjengelighet:	Åpen

Sammendrag:

I dag er biometriske systemer implementert i en stor andel personlige digitale enheter slik som smarttelefoner og datamaskiner, fordi det tilfører disse enhetene en høyere grad av sikkerhet med tanke på identifisering av disse enhetenes rette eier. Fingeravtrykk er en av de mest brukt biometriske egenskaper. Fingeravtrykk teknologi er anvendt i flere ulike områder som flyplasser, grensekontroller, og politistasjoner. Disse enhetene kan være sårbare for presentasjonsangrep ved å presentere falske fingre/gummifingre til fingeravtrykks enhet. For å forsikre at presentasjonsangrep (PA) blir oppdaget finnes det flere PA databaser og deteksjonsmetoder tilgjengelig for bli implementert og testet i virkelige miljøer. I denne avhandlingen, og ifølge vår metodikk, presenterer vi (1) en retningslinje for opprettelse av databaser med presentasjonsangrep, (2) en liste over sårbarheter i eldre sensorer (Crossmatch og Lumidigm), og (3) en liste med evaluerte PA instrumenter (PAI).

Summary of Graduate Project

Title:	**FiPrAD - A Guideline for Fingerprint Presentation Attack Database Creation**
Date:	30.11.2018
Authors:	Ahmed S. M. Madhun
Supervisor:	Dr. Marta Gomez-Barrero Prof. Dr. Christoph Busch
Employer:	Biometrics and internet security research group **(da/sec)**
Contact Person:	Dr. Marta Gomez-Barrero, marta.gomez-barrero@h-da.de
Keywords:	Biometrics, Fingerprint, Database, Presentation Attacks, Security, Research, English
Pages:	73
Attachments:	7
Availability:	Open

Abstract:

Nowadays, biometric recognition systems are widely implemented in many personal devices like smartphones and laptops, as it provides higher security while identifying the real owners of these devices. Fingerprint is one of the most used biometric characteristics. Fingerprint technologies are applied in areas such as airports, border control, police stations, etc. These devices may be vulnerable to presentation attacks by presenting a fake finger/gummy finger to the capture device. To ensure that these presentation attacks (PA) are detected, several PA databases and presentation attack detection methods are available to be implemented and tested in real environments. In this thesis and according to our methodology, we are presenting (1) a guideline for presentation attack database creation, (2) a list of vulnerabilities in the legacy sensors (Crossmatch and Lumidigm), and (3) a list of evaluated PA instruments (PAIs)

Acknowledgments

Finally, by delivering this thesis I finish my double bachelor degree in Information Security and Software Engineering. It has been three and a half years of hard working, to achieve this goal. Firstly, I want to thank my employer and first supervisor for this thesis Dr. Marta Gomez-Barrero for being my host and provide me with this opportunity to do my second bachelor thesis in da/sec. Also, I want to thank Prof Dr. Christoph Busch for being my supervisor in this project and provide me with all needed feedback along the way.

Also, I have to thank all the nice people I have met in Darmstadt, with a special thank to Lena for her support and motivation. Moreover, da/sec group that has provided a very good working environment for me and all other bachelor and master students. A special thank for the KGB group for providing cakes each Friday. It has been very nice to spend my internship in this place with all of you.

Besides, I would like to give a special thank for the people in the international office in Gjøvik (Tatiana Fedorova & Anneli Østlien), the people in the international office in Darmstadt (Annabelle Bijelic) and Prof. Erik Hjelmås for doing their best to make this internship happen, and offering me this experience.

I must thank the people who inspired me to perform my bachelor thesis as an internship abroad a mention as well. By that, I mean all international students in NTNU Gjøvik during the study year of 2017/2018. With a special mention to the following international students: Alexa, Doreen, Florian, Maria, Cristian, Jesus, Jovanie, Lukas, Ann-Kristin, Dafina, Zyg, Sherif, Nadile and Yvon. Also my best friends in Gjøvik; Osama and Maher.

One more thank to all bachelor students in both degrees (15HBPUA & 15HBISA) for creating a good atmosphere during the whole study period. Thanks for being together through all nerves and stress (and fun) of these bachelors. Also, thanks to all the professors during the whole period for their work to make us what we are now. Specially, Simon McCallum for providing the LaTeX-template for us to use.

Last but not least, a huge thank to each and every member of my family for their support along the way to achieve this goal. A double bachelor has been achieved, and a master will follow it later someday. Who knows, maybe a double one too :-) !

Once Again, Thank You All !!

Preface

This is a bachelor thesis report in information security written and performed by the student:

Ahmed S. M. Madhun - 471189
ahmed.madhun@stud.ntnu.no

He is a double bachelor student at NTNU Gjøvik, performed his other bachelor degree already in software engineering.

This project was done as a part of an internship that the student had in Germany in Darmstadt. He worked for almost six months as a student researcher in the researching group da/sec, besides being an Erasmus student in Hochschule Darmstadt – University of Applied Sciences and a master student in information security at NTNU Gjøvik.

This project is a part of a bigger project called BATL, where da/sec is a member of the BATL project. Also, this report represents the student's bachelor project. Including his process, product and result during the whole period. The employer of this project and the first supervisor is **Dr. Marta Gomez-Barrero**.

Contents

List of Figures

List of Tables

Abbreviations

2D	Two-Dimensional
3D	Three-Dimensional
AFIS	Automated Fingerprint Identification System
APCER	Attack Presentation Classification Error Rate
BATL	Biometric Authentication with a Timeless Learner
BIS	Bachelor in Information Security
BPCER	Bona fide Presentation Classification Error Rate
BPM	Best Practice Manual
BPU	Bachelor in software Engineering
BTP	Biometric Template Protection
da/sec	Biometrics and Internet Security Research Group
DB	Database
dpi	Dots Per Inch
EU	European Union
FMR	False Match Rate
FNMR	False Non-Match Rate
FI	Frontal Illumination
FOP	Fiber Optic Plates
FTA	Failure to Acquire
FV	Finger Vein
FVC	Fingerprint Verification Competition
GDPR	General Data Protection Regulation
h_da	Hochschule Darmstadt - Darmstadt University of Applied Sciences
ID	Identity Document
IMRaD	Introduction, Methods, Results, and Discussion
ISO	International Organization for Standardization
LSCI	Laser Speckle Contrast Imaging
NBL	Norwegian Biometrics Laboratory
NFIQ	***NIST*** Fingerprint Image Quality
NIST	National Institute of Standards and Technology
NTNU	Norwegian University of Science and Technology
TOE	Target of Evaluation
PA	Presentation attack
PAD	Presentation attack detection
PIN	Personal Identification Number
PCB	Photosensitive Circuit Board
PHRP	Protecting Human Research Participants
SD	Special Databases
SDK	Software Development Kit
SQL	Structured Query Language
SWIR	Short Wave Infrared Imaging
TIR	Total Internal Reflection
US	United States
UV	Ultraviolet

Glossary

artefact An artificial object or representation presenting a copy of bometric characteristics or synthetic biometric patterns [3]. 13, 14, 30–32, 42, 52, 56, 60, 61

attack presentation classification error rate Proportion of attack presentations using the same ***PAI*** species incorrectly classified as bona fide presentations in a specific scenario [11]. 14

authentication The process of confirming a biometric claim through biometric comparison [12]. 1, 2, 7–9, 15

behavioural characteristics Referring to the behavior and body movement of a specific person [13]. 1, 7

biological characteristics Referring to a physical part(s) of a human body, which are unique for each defined person [13]. 1, 7, 9

biometric claim It claims that a biometric capture subject is or is not the bodily source of a specified or unspecified biometric reference [12]. xiii, 9

biometric enrollment database Database of biometric enrolment data record(s) [12]. xiv, 9, 10

biometric probe biometric sample or biometric feature set input to an algorithm for use as the subject of biometric comparison to a biometric reference(s) [12]. xiii–xv, 9, 11, 12

biometric reference one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used as the object for biometric comparison [12]. xiii–xv, 9–12

biometric reference identifier A pointer to a biometric reference data record in the biometric reference database [12]. 9

biometrics Automated recognition of individuals based on their biological or behavioural characteristics [1]. xii, 1, 5–9, 12, 14, 15, 23, 30, 36, 58, 63, 67, 82

bona fide presentation A standard interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system [11]. x, xiii, 2, 3, 12, 14, 18, 19, 33, 34, 39, 52, 53, 55, 56, 65, 87

bona fide presentation classification error rate Proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario [11]. 14

comparison Estimation, calculation or measurement of similarity or dissimilarity between biometric probe(s) and biometric reference(s) [12]. xiii, xiv, 9, 11, 39, 65

concealer A subversive biometric capture subject who attempts to avoid being matched to their own biometric reference [12]. 13, 31, 32

consent Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her [14]. 17

edgeoscopy the analysis of minutiae points and galton details. 24

fingerprint An impression of the friction ridges of all or any part of the finger [15]. ix, xii, xiv, 1–6, 8, 11, 14, 16–18, 20–44, 46, 47, 49, 51–53, 55, 60, 61, 63–68

gait The act of walking involves the complex interaction of muscle forces on bones, rotations through multiple joints, and physical forces that act on the body [16]. 1, 8

identification Proof of identity, also known as the process of searching against a biometric enrollment database to find and return the biometric reference identifier(s) attributable to a single individual [12]. xii, 9, 22, 23, 32, 38–40, 49

imposter A subversive biometric capture subject who attempts to being matched to someone else's biometric reference [12]. ix, 11–13, 30–32, 51, 61, 66

keystroke dynamics A behaviour biometric modality that measures how a person types on a keyboard, and based on that information authenticates of identifies a person [17]. 1

latent Inadvertent impressions left by fingers on surfaces of objects [18]. 22, 23, 25, 26, 28, 30, 33, 61

liveness detection Measurement and analysis of anatomical characteristics or involuntary reactions, in order to determine if a biometric sample is being captured from a living subject present at the point of capture [3]. 14, 31, 32, 34

mated A comparison of a biometric probe and a biometric reference from the same biometric data subjects [12]. 11

minutiae points The major features of a fingerprint image and are used in the matching of fingerprints [19]. xiv, 11, 22, 24, 28, 29, 31, 32, 43

non-mated A comparison of a biometric probe and a biometric reference from different biometric data subjects [12]. 11

poroscopy the analysis of sweat pores. 24

presentation attack Presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system [3]. xii, xiii, xv, 4, 6, 12–14, 16, 19, 30

presentation attack detection An automated determination of a presentation attack [3]. xii, 6, 14, 16, 34

presentation attack instrument A biometric characteristic or object used in presentation attack [3]. 2, 3, 13

usability The extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use [20]. 8, 14

verification The process of validation of an identity claim by checking the biometric probe against the biometric reference of the claimed identity (1-to-1) [21]. 9, 33, 38–40, 49

vulnerabilities A weakness of an asset or group of assets that can be exploited by one or more threats [22]. 2–4, 12, 42

1 Introduction

1.1 Introduction to biometric security

Nowadays, the term biometric security is also known as Biometrics. It refers to "automated recognition of individuals based on their biological or behavioural characteristics" [1]. Biometric characteristics are unique from one human to another, which makes them a good feature for recognizing a specific person by his/her characteristics. Those characteristics are further divided into biological characteristics and behavioural characteristics.

The category of biological characteristics refers to a physical part(s) of a human body, which are unique for each subject (i.e., person). The most known and widely used characteristics in this category include: fingerprint, iris and face. On the other hand, the category of the behavioural characteristics refers to the behavior and body movement of a specific person, for example a human's gait (manner of walking), keystroke dynamics (manner of typing on a keyboard) or signature style [13].

Biometric security can also be presented as using the aforementioned characteristics above as a recognition method to identify the different users on hardware devices (e.g., smartphones and laptops) or software solutions (e.g., mobile applications).

This thesis will only focus on the biological feature fingerprint as an authentication method for different subjects.

1.2 Fingerprint recognition technology

In the last few years, most of the usual electronic devices like smartphones, laptops and smart assistant devices allow the ability of using the user's fingerprint to access the device. Fingerprint is known as "an impression of the friction ridges of all or any part of the finger" [15]. It has a unique pattern that is formed during early foetal life, between the 3rd-5th months of pregnancy.

Besides all other biometric characteristics, fingerprint is considered one of the most practical ones. It does not require much effort from its user, it is faster to access than a Personal Identification Number (***PIN***-code) or password, and it is hard to spoof. Thus, this technology is already widely used, and will be more used in the future as a security method to protect sensitive environments and our private data. Additionally, most countries have added the fingerprint to their passports (e.g., Norway [23]).

1.3 Presentation Attack

This term is shortened and known as ***PA***, which will be further used in this thesis.

According to the ***ISO*** [1] standard 30107-1 ([3]), ***PA*** is "a presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system". In other words, it is an attack on a biometric recognition system (i.e., sensor), done by an attacker that presents a fake biometric characteristic of him/her self or other

[1] International Organization for Standardization

users known or unknown to the system.

PAs can be performed against any biometric system using several different objects and materials that are defined as a presentation attack instrument (***PAI***, e.g., using a face mask or a gummy finger). Nowadays, most of the recognition systems have built-in technologies that detect these kinds of ***PA***s. On the other hand, attackers are also improving their ***PA***s to break into these new technologies in biometric systems.

The opposite term of ***PA*** is known as bona fide presentation, which is defined according to [3] as "a standard interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system". Which means all attempts by an user known to the system (i.e., registered in the system) whom presenting his/her biometric characteristic to a biometric system. In some cases, bona fide presentation could be done by an unknown user to the system (e.g., a user that thinks that he/she is known to the system, but they are not known to the system).

1.4 Presentation Attack Detection

This term is shortened and known as ***PAD***, which will be further used in this thesis.

PAD is defined as "an automated determination of ***PA*** [3]". It includes the technologies and methods that are used to define if a simple presentation of a biometric characteristic is a ***PA*** or bona fide presentation during the data capturing phase. By doing so, ***PA***s will be detected.

A ***PAD*** method can be any technique implemented as a hardware or a software solution to the biometric system. An example of the hardware solution can be adding a piece of hardware to detect the heartbeat movement during the authentication [24]. On the other hand, software solutions are algorithms to process and analyze the extracted data from the capture subject [7], e.g., applying image quality checking on the captured sample [25] or detection of sweat pores on the ridges of fingerprint [26].

1.5 Problem description

The ***PA***s are improved by attackers to gain access to biometric systems. Several known and unknown materials are used to perform ***PA***s. Therefore, there is a need of applying different ***PA***s scenarios on different fingerprint recognition sensors to discover their vulnerabilities and limitations. Then, create ***PAD*** methods to prevent different known and unknown attacks against any biometric system. Due to this fact, a project called ***BATL*** ([27]), Biometric Authentication with a Timeless Learner, is running by several members of institutions and universities [28]. The ***BATL*** system includes three modality-specific ***PAD*** modules (i.e., face, iris and fingerprint), each of them extracts various types of features from the input. Decisions from all modality-specific ***PAD*** modules as well as an additional unknown attack detector are all fused to produce a robust decision to discriminate bona fide presentation from ***PA***s. In other words, the goal of ***BATL*** project is improving the performance of ***PAD*** techniques.

The ***BATL*** project presents a new fingerprint sensor [29]. This sensor captures fingerprint images using four different technologies. These technologies are:

- Short Wave Infrared Imaging (***SWIR***)
- Laser Speckle Contrast Imaging (***LSCI***)

- Finger Vein (***FV***)
- Frontal Illumination (***FI***)

This project is a part of the ***BATL*** project, and as mentioned in Section 1.1, this project is focusing only on fingerprint ***PA***s and ***PAD*** methods. In order to create the ***PA*** scenarios, there is a need of creating a database of fingerprints ***PAI*** (real and fake fingerprints), both for creating the test objects for different ***PA***s and use the database for further research.

The desired database should consist of both PAs and bona fide presentations collected from N number of users using the ***BATL*** sensor and two other legacy sensors (Crossmatch and Lumidigm), which are commercially available on the market.

1.6 Project motivation, goals and research question

This project had predefined motivation, goals and a research question to be achieved (i.e., original scope). During the project period, the original scope faced a risk of not being achieved because of the delay on delivering the ***BATL*** sensor. Therefore, a modification of the original scope needed to be considered as a countermeasure to handle the mentioned risk. This is discussed in detail in the discussion chapter (Chapter 8) in Section 8.1.1. This includes the mentioned risk, and the countermeasure that was taken to handle it.

Furthermore, the next section describes the motivation, goals and research question of the original scope (Section 1.6.1) and the current project scope (Section 1.6.2).

1.6.1 Original scope

The main goals of the project, before any modification, were to (1) collect presentation attack instruments (***PAI***s), (2) fabricate fingerprint ***PAI***s, (3) acquire both ***PA***s and bona fide presentation samples with a set of innovative sensors (i.e., ***BATL*** sensor) and legacy sensors, (4) create a fingerprint database, and (5) apply existing ***PA*** techniques to the acquired samples in order to detect the fake fingers.

The following effect goals, result goals, and research questions were desired for the original scope:

Effect goals

- Clarify the predefined fingerprint ***PA***s by preforming the attacks on some specific sensors (i.e., ***BALT*** sensor and legacy sensors [Crossmatch and Lumidigm]).
- Verify the security around the different fingerprint detection sensors.

Result goals

- A fingerprint database, to use for further projects and research.
- A list of detected vulnerabilities attached to each fingerprint sensor, so it can be taken into consideration to implement ***PAD*** methods for them in later projects.
- A list of valid fingerprint ***PA***s, and clarify the strengths, weaknesses and likelihood of each attack to be performed.

Research question

The purpose of this project is summarized in one main research question presented as following:

> **Is there a correlation between the difficulty in creating the *PAI* and the vulnera-**

> **bility of the sensor to it?**

In order to answer the main question, it is divided into three sub-questions:

1. *What is the degree of difficulty for creating different* ***PAI****s?*
2. *How vulnerable are legacy sensors to the fabricated* ***PAI****s?*
3. *Are the* ***BATL*** *sensors more robust to the selected* ***PAI****s than the legacy sensors?*

The first sub-question is answered by doing the task of fabricating the ***PAI***s, and the other two sub-questions can be answered by applying the ***PA***s on the desired sensors.

1.6.2 Current project scope

Due to the ***BATL*** sensor delay and the project time constraint, the current project scope has been chosen to follow the original scope with minor changes (see Chapter 8, Section 8.1.1 for details). The main goal of the current project is to perform a pilot version of the original scope. This includes the same steps mentioned in the previous section. However, only the available sensors (i.e., legacy sensors [Crossmatch and Lumidigm]) will be used to capture the pilot database. This leads to the following effect-, result goals and research questions to the current project scope:

Effect goals

- Clarify the predefined fingerprint ***PA***s by performing the attacks on the legacy sensors.
- Verify the security around the inbuilt fingerprint ***PAD*** methods in the legacy sensors.

Result goals

- A list of detected and undetected attacks by the legacy sensors. This includes:
  - List of vulnerabilities attached to each of the legacy sensors.
  - List of ***PA***s that cannot be captured by each of the legacy sensors, so it does not need to be performed again when the original project runs (also, to avoid unnecessary time consumption).
- A guideline (i.e., Best Practice Manual [***BPM***]) for ***PA*** database creation to be considered on the original project.
- A list of evaluation for the performed ***PA***s based on attack potential common criteria presented in ***ISO*** standard 19989-1 ([10]).

Research question

This pilot project will be able to answer most of the predefined research questions in the previous section (i.e., Original scope). However, the research questions related to the ***BATL*** sensors will not be possible to be solved by this pilot project because it was not possible to have access to this sensor. Furthermore, creating a guideline of presentation attack database creation adds the following research question to be answered:

> **How can the fingerprint data in a *PA* database affect further researches in the field of *PA* and *PAD*?**

In other words, this is the research questions for the current project scope are summarized as follows:

> **Is there a correlation between the difficulty in creating the *PAI* and the vulnerability of the sensor to it?**

1. *What is the degree of difficulty for creating different* ***PAI****s?*
2. *How vulnerable are legacy sensors to the fabricated* ***PAI****s?*

How can the fingerprint data in a *PA* database affect further researches in the field of *PA* and *PAD*?

1.7 About this thesis

1.7.1 The employer

Dr. Marta Gomez-Barrero is the employer for this project. She is a postdoctoral researcher at Darmstadt University of Applied Sciences - Hochschule Darmstadt (***h_da***). The employer is a part of the ***BATL*** project, and has some Bachelor and Master thesis topics published online about ***PAD*** on fingerprint, iris and face recognition.

1.7.2 The author

The task performer is the student Ahmed S. M. Madhun, from the Norwegian University of Science and Technology (***NTNU***). This is a Bachelor thesis in Information Security (***BIS3900***)[30], and also a part of an internship in Biometrics and Internet-Security Research Group (***da/sec***) and ***h_da***.

Student experience

The student is a double Bachelor student, performing Bachelor in Software Engineering (***BPU***) and Bachelor in Information Security (***BIS***). The student has previous experience with doing a Bachelor thesis in ***BPU*** early this year. The student has followed the study program for ***BIS*** at ***NTNU***. It included courses in different fields in information security, e.g., network security, software security and risk management. However, the student has no previous experience in the field of biometric security. Therefore, this thesis is challenging and offers a new experience to gain.

1.7.3 Supervisor

Prof. Dr. Christoph Busch is the student's supervisor for this project. He is a biometric systems specialist in the field of IT-Security, and a professor at ***NTNU***. He is following the student's working process, provides feedback, and ensures that the student is *on track* during the project period.

1.7.4 Project period

The project period is defined by the student and the employer to run during the period of 15$^{\text{th}}$June-30$^{\text{th}}$November. Appendix A contains a full description of the project plan that was defined at the beginning of the project. Also, Appendix B presents the midterm review of the plan, which includes the considered changes to the original plan as described earlier in Section 1.6.

1.7.5 About the report

The report is written in English because the project is a part of an internship, and English is the communication language between the employer, the supervisor and the student.

In the PDF-version of this report, it is possible to navigate through the document by clicking on items in table of contents, given references, glossary and abbreviations.

Abbreviations in the document are given as a bold text, and the definition of each can be found in the glossary.

This report contains references for other related works. For dated references, only the edition cited applies. For undated references, the last edition of the referenced document (including any amendments) applies.

Report structure

The content of this report is divided into ten chapters, and structured based on ***IMRaD*** [2] format, as Table 2 shows below.

Nr#	**Chapter name**	**Chapter goal(s)**
I: 1	Introduction	Representing the problem description, project's motivation and goals, and involved members.
2	Basic Theory	This chapter is written for readers with no previous experience in the topic of Biometrics. It presents the basic knowledge needed about the biometric security before going further in depth.
M: 3	Requirements Specification and Methodology	Presents the project's requirements in depth, and the methodology assigned to each requirement in order to be achieved.
4	Literature Review	Goes in depth into fingerprint's recognition, presentation attack and presentation attack detection. By presenting a literature background.
R: 5	Fingerprint PA Database Creation Guideline	Presents the guideline (i.e., ***BPM***) proposal on how to create a fingerprint ***PA*** database.
6	Pilot Presentation Attack Database	Presents the first result of this project; the pilot database that is created, and the process of creating it.
7	Presentation Attacks Evaluation	Presents the result of evaluating the applied ***PA***s based on the evaluation factors presented in [10].
D: 8	Discussion	Presents a discussion of the taken decisions related to the project and the process during the thesis period.
9	Conclusion	Presents a conclusion of the project work, self evaluation, and future work.

Table 2: Thesis structure

[2] Introduction, Methods, Results, and Discussion

2 Basic Theory

This chapter is written to give all readers the needed theory about the topic before presenting it in depth in further chapters. The chapter will answer the reader's following questions: (1) What is Biometrics? (2) Why is it used in security? (3) How trusted is using Biometrics as authentication method? (4) How to secure biometric systems?

2.1 Authentication

Everyone uses different devices to store their sensitive information, either physical data (e.g., personal documents like passports and ID-cards) or digital data (e.g., personal pictures and digital documents). Information is an important and valuable asset for its owner(s), and there are many people who are interested in collecting personal information of other people for different reasons. Such reasons could be profit grounds or even blackmailing the owner of the information [17]. Information could be stored in several ways like a safe for physical data, or personal computers and smartphones for digital data. Therefore, it is very important to apply information security techniques on these devices. Thus, only genuine owners get access to the data stored in these devices.

2.1.1 Authentication modes

In general, authentication is important in order to deny unauthenticated users from accessing protected resources. As presented in [8], there are three different authentication modes that are known and used nowadays; Possession, Knowledge and Biometrics.

- *Possession* refers to a tool that only the user(s) owns physically (e.g., keys or ***ID***-cards). The main idea is that the owner(s) of this property has the privilege to use it.
- *Knowledge* refers to something the only the user(s) knows (e.g., ***PIN***-code or passwords). This method is built on the idea of having a secret, thus, the knowledge needs to be a secret in order to be used in secure authentication[8].
- *Biometrics*, as mention in Section 1.1 refers to either a biological characteristics or behavioural characteristics that only a specific user has in the biological case or does in the behavioral case.

Table 3 below shows an overview over the different modes by representing examples, advantages and drawbacks of each.

Authentication mode	**Examples**	**Advantages**	**Drawbacks**
Possession	- ***ID***-card - Passport - Key - Transponder	- A new one could be issued - It is quite standard, although moving to a different country, facility, etc. - Easy to carry and simple to use	- It can be stolen - A fake one can be issued - It can be shared - One person can be registered with different identities
Knowledge	- ***PIN***-code - Password - Lock combinations - Secret answer	- It is simple and economical method - Easy to replace when a problem appears	- It can be guessed or cracked - Good passwords are difficult to remember - It can be shared - One person could be registered with different identities
Biometrics (biological and behavioural)	- Fingerprint - Face - Iris - Voice - Gait	- It cannot be lost, forgotten, guessed, stolen, shared, etc. - It is quite easy to check if one person has several identities - It can provide a greater degree of security than the other ones	- In some cases, a fake one can be issued - It is neither replaceable nor secret - If a personal biometric data is stolen, it is not possible to replace it

Table 3: Authentication modes (examples, advantages and drawbacks) [8, 9]

Nowadays, most of the solutions that require authentication use more than one authentication mode to increase the security. An example is the combination of the credit card and ***PIN***-code, where the credit card presents the possession and the ***PIN***-code is a secret knowledge known by the user. Thus, problems like stolen and sharing the method cannot be easily performed by the attackers. This way of using multiple methods is suggested in [31].

Using multiple authentication modes increases the security for sure, but the usability should be taken into consideration before applying the different authentication modes [32]. Usability is defined as the extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use [20]. So, asking users to hold multiple keys or know multiple passwords gives a bad user experience because users prefer to use less effort and time in any service.

A presented security solution that has been widely used and proved its worth in the last decade is Biometrics; such as fingerprint or face recognition as the only authentication method to access a service (e.g., today's smartphones).

2.2 Biometric authentication

As mentioned earlier, *Biometrics* is "automated recognition of individuals based on their biological or behavioural characteristics" [1]. Biometrics represents the users as themselves, because each user has unique and different characteristics. Using these characteristics, different biometric systems can recognize and authenticate the users.

As Table 3 shows, Biometrics solves many drawbacks that are presented in the traditional authentication modes (i.e., possession and knowledge). It cannot be stolen, shared, forgotten and guessed. However, its drawbacks are quite critical. It is not replaceable in case of being lost in any unexpected damage to the human body. Also, it is not a secret to hide, and in most of cases it is visible to everyone. Biometrics - specially in case of biological characteristics - could be spoofed by creating a fake copy of the characteristics. Of course, that depends on what kind of biological characteristics, the spoofing materials and sensing technology are used.

2.2.1 Authentication process

To gain access to any device protected by a biometric security as for all other security methods (e.g., password), users need to be authenticated. To authenticate users there is a need that each user gets identified and verified. Also called the process of identification and the process of verification, and both are know as authentication methods. In Biometrics,

- *Authentication* is "the process of confirming a biometric claim through biometric comparison" [12].
- *Identification* is "the process of searching against a biometric enrollment database to find and return the biometric reference identifier(s) attributable to a single individual (1-to-N)" [12].
- *Verification* is "the process of validation of an identity claim by checking the biometric probe against the biometric reference of the claimed identity (1-to-1)" [21].

Under authentication, the biometric claim proposes that a biometric capture subject is or is not the bodily source of a specified or unspecified biometric reference. A biometric reference denotes to one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used as the object for biometric comparison [12]. Furthermore, comparison is "estimation, calculation or measurement of similarity or dissimilarity between biometric probe(s) and biometric reference(s)". Additionally, biometric probe biometric sample or biometric feature set input to an algorithm for use as the subject of biometric comparison to a biometric reference(s).

On the other hand, under identification, the biometric enrollment database is "a database of biometric enrolment data record(s)". How it works is explained in Section 2.2.2. Meanwhile, biometric reference identifier is "a pointer to a biometric reference data record in the biometric reference database" [12].

So, to simplify it, during authentication, the subject claims an identity and the biometric reference connected to that identity is taken from the database. This reference is then compared to the biometric probe that the user provides early in the process and if the comparison between the reference and the probe is positive, then the user will get access to the system. This is illustrated in the Figure 1 (identification) and 2 (verification).

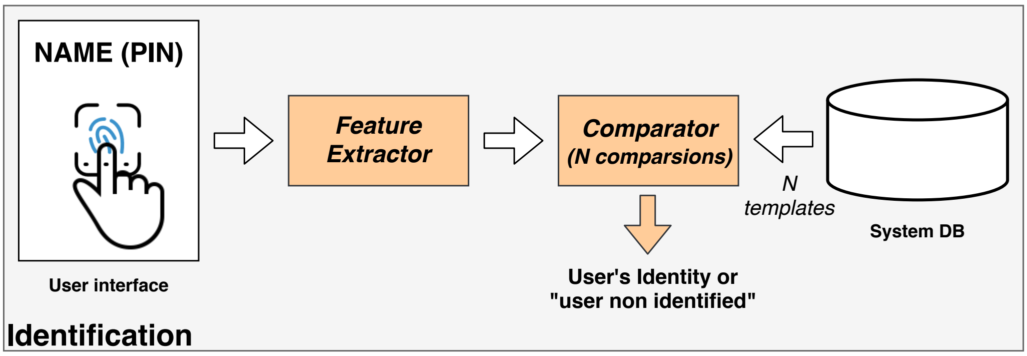


Figure 1: Block diagram of identification, as presented in [1]

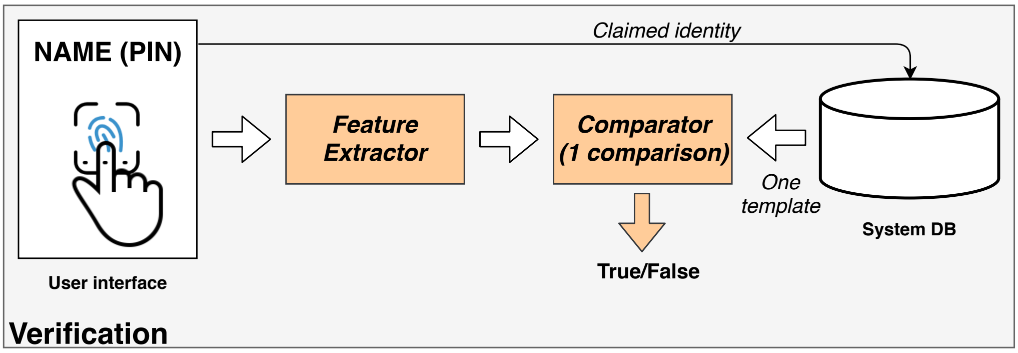


Figure 2: Block diagram of verification, as presented in [1]

2.2.2 Enrollment process

Users have to be enrolled in the biometric enrollment database in order to be identified and verified. When a user first enrolls to a biometric system, a biometric reference of his/her data is created and the authentication process uses this reference. During this process the reference is stored in the database and linked to the user's identity. Figure 3 shows the workflow of the enrollment process.

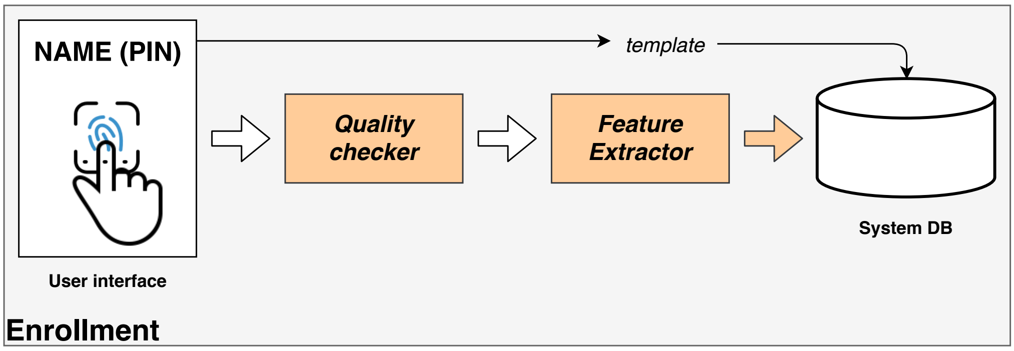


Figure 3: Block diagram of enrollment, as presented in [1]

As it may be observed, and as described in [33], the biometric template is created for each user at the beginning of the enrollment process by recording different biological and non-biological data of the user and these data are considered to a biometric sample.

It is from this sample that the unique features are captured and extracted. The samples are then converted into a biometric template which in turn is used for the purposes of identification and verification. For example in case of the fingerprint, the image of the fingerprint is analyzed and the information about the location and orientation of the so called minutiae points is extracted. The minutiae points information is then stored while the fingerprint image is never stored for security reasons [34, 17]. These security reasons are exactly the drawbacks. If the biometric characteristic is compromised, it cannot be replaced (e.g., give a subject a new finger).

2.3 Biometric recognition systems

Biometric recognition systems work as mentioned earlier by enrolling the users into the system and then authenticating them by identifying and verifying them. As all other systems it could be vulnerable to attacks. In this thesis, the focus is on Presentation Attacks (***PA***), as will be later explained in Section 2.4. The attacker in this kind of attacks is defined by the term *imposter* according to [12]. Imposter is "a subversive biometric capture subject who attempts to be not being matched to someone else's biometric reference". This term will be further used in this thesis.

Biometric systems are not always completely accurate, and cannot recognize the person without errors. So, it is possible that some errors appear while processing the decision, because the system is measuring the similarity between the extracted features from the biometric probe to the stored biometric reference. Two of the most common errors to happen according to [35, 36] are *False Match* and *False Non-Match* errors. A False Match error occurs when an imposter user gets access to the system as a genuine user without any reaction from the system, also in other words, an imposter accepted. The comparison that are used in False Match error is defined as a non-mated comparison, where the system does the comparison of a biometric probe and biometric reference taken from different subjects [12]. On the other hand, a False Non-Match occurs when a genuine user is not recognized by the system and gets rejected, in other words, a genuine rejected. The comparison used in this case is defined as mated comparison, where the system does the comparison of a biometric probe and biometric reference from the same subject [12].

The performance of biometric systems is measured in terms of the probability that a False Match and a False Non-Match occurs. The probability of each error is defined by the terms: False Match Rate (***FMR***) and False Non-Match Error (***FNMR***). ***FMR*** and ***FNMR*** depends on a predefined *threshold* that expresses how well a reference and probe should match. Once the biometric system calculates the difference between the reference and the probe, the result is compared to the threshold to see if access will be granted or not. If the distance is below the threshold, then the user gets access, and a rejection will face the user if the distance was over the threshold. The calculation of ***FMR*** and ***FNMR*** according to the definition in [12] are as follows:

$$\mathrm{FMR} = \frac{\sum(\mathrm{NonMatedScores} <= \mathrm{Threshold})}{\mathrm{NumberOfNonMated}}$$

$$\mathrm{FNMR} = \frac{\sum(\mathrm{MatedScores} > \mathrm{Threshold})}{\mathrm{NumberOfMated}}$$

Where according to [12, 17]:

- *NonMated Scores*: A numeric value resulted from the calculation similarity between biometric probe and the biometric reference of imposters.
- *Threshold*: Numerical value at which a decision boundary exists.
- *Mated Scores*: A numeric value resulted from the calculation similarity between biometric probe and the biometric reference of genuine users.

There is a need to mention that the threshold's value should be defined differently from one case to another. For example, airports require high security to deny criminals from crossing boarders. On the other hand, schools do not require such a high security as airports, because students should be able to enter lecture rooms and meeting rooms even if the system does not recognize them because of an error. Figure 4 illustrates this examples, where the airport is presented as a high threshold case (the graph to the left in Figure 4), and the school is presented as a low threshold case (the graph to the right of the same figure). Keep in mind that the illustration of the graphs will depend on the used detection algorithm. In this case it is just an example to illustrate.

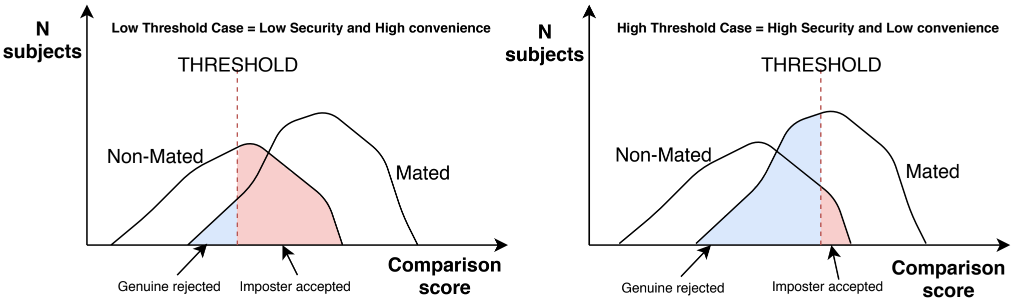


Figure 4: ***FMR*** and ***FNMR*** for two different Threshold values over the genuine (Mated) and imposter (Non-Mated) score distributions, (inspired by [2])

So in simple words, if a biometric system offers a high security and accuracy by defining a high threshold value, the system will have a high ***FNMR***. On the other hand, having a low threshold's value, will offer a high ***FMR***, and in this case many imposters will get access.

2.4 Biometric *PA*

A biometric system is similar to any other system as they are all vulnerable to attacks and could have vulnerabilities and limitations. Attacks on any biometric system can occur in any operation of the system's process-flow and be instantiated by any actor. Figure 5 shows points of attack in biometric systems as presented in [3].

All the attacks mentioned in Figure 5 are discussed in depth in [2, 37]. This thesis's topic focuses only on biometric-based attacks on the data capture subsystem by biometric capture subjects attempting to subvert the intended operation of the system, in other words, Presentation attacks (***PA***).

The opposite term to ***PA*** is known as a bona fide presentation. It is "the interaction of the biometric capture subject and the biometric capture subsystem in the fashion intended by the policy of the biometric system". In other words, all legal attempts by genuine users to access the biometric system by using the biometric capture subsystem and their own Biometrics characteristic(s).

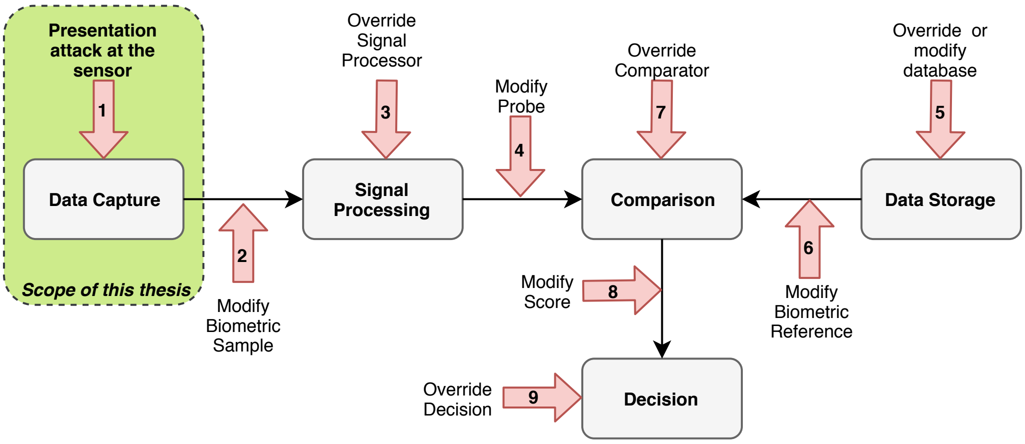


Figure 5: Points of attack in a biometric system (as presented in [2, 3])

2.4.1 Imposters and Concealers

*PA*s could be performed by two types of biometric subjects; imposter and concealer. Imposter were previously defined in Section 2.3 as a subversive biometric capture subject who attempts to being recognized as an individual other than him/herself. This could be performed either by attempting to be recognized to the system as a specific individual known to the system, or any individual known to the system. The other biometric subject, concealer, is "a subversive biometric capture subject who attempts to evade being recognized as any individual known to the system". Both terms are defined in [3, 12].

2.4.2 *PAI*

A presentation attack instrument is "a biometric characteristic or object used in presentation attacks". According to [3], *PA*s on the sensor using *PAI*s are mainly categorized into two categories; artificial or human-based characteristics. However, there is a third category of other natural cases such as animal-based and plant-based *PAI*s. This is presented in Figure 6.

The term artefact refers to "an artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns". This term will be further used in this thesis. There are several artefact's materials that are known and can be easily detected (e.g., silicon, gelatine and 3D printed fingers). But since attackers are also improving their *PA*s, there will be other materials that are unknown to biometric systems, and that should be taken into considerations further so new and unknown *PA*s get detected.

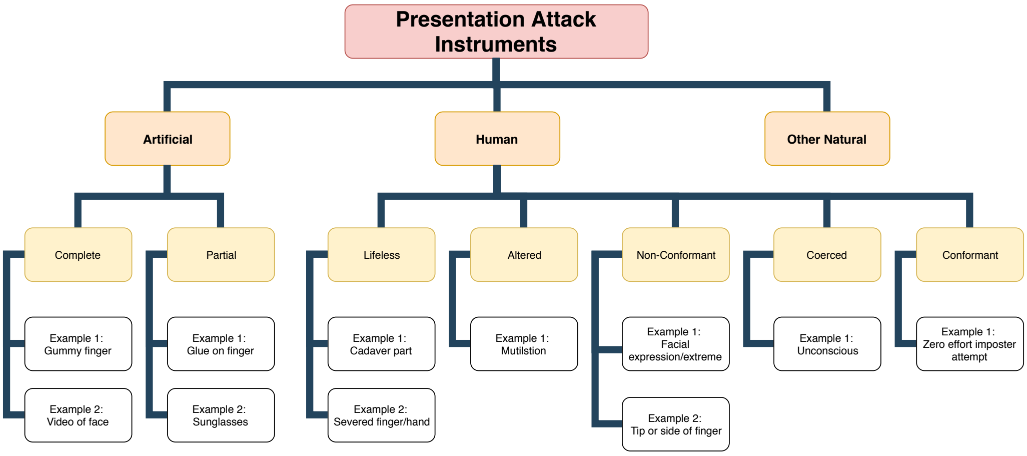


Figure 6: ***PAI*s** categories and examples (as presented in [3])

2.5 Biometrics *PAD*

In order to prevent ***PA*s**, presentation attack detection (***PAD***) methods should be implemented into the biometric data capture subsystem (i.e., where ***PA*s** attacks occurs at the first stage). ***PAD*** is "an automated determination of a presentation attack" [3]. It refers to any technique either software-based or hardware-based to be able to automatically distinguish between bona fide presentation (i.e., real or live Biometrics characteristic(s)) and ***PA*s** using ***PAI*s** [3, 29]. It should be taken into consideration that a detected attack could occur due to accessibility or usability of a subject and not an attempt to attack the system at all.

According to [11], ***PAD*** defines other error rates. Some of the errors are analogous to the previous mentioned error rates in Section 2.3. The error rates that are in focus for this thesis are defined as follows according to [11]:

- Attack presentation classification error rate (***APCER***) refers to error rates of ***PA*s** that are incorrectly classified as bona fide presentations. This is analogous to ***FMR***.
- Bona fide presentation classification error rate (***BPCER***) refers to error rates of bona fide presentations that are incorrectly classified as ***PA*s**. This is analogous to ***FMNR***.

Both of the new terms will be further used in this thesis under the topic of ***PAD***.

In [3], ***PAD*** methods are categorized into two types; PAD methods through *data capture subsystem* and through *system-level monitoring*. Figure 31 in Appendix C shows an overview of these categories and subcategories.

2.5.1 *PAD* through data capture subsystem

This category is further subcategorized into into six categories; (1) *artefact detection*, which detects features of an artefact (e.g., electrical impedance of "finger" on sensor is outside typical range or the surface of the artefact). (2) *Liveness detection* that works by detecting if the biometric characteristic is captured by a living subject. Challenge-response method is a good example of a liveness detection and it is described in the next paragraph. (3) *Alteration detection* detects features characteristic of attempts to alter biometric feature (e.g., scar tissue on fingerprint). (4) *Non-conformance detection* works by detecting abnormalities that should not occur in a proper presentation (e.g., detection that illumination level not consistent with normal use). (5) *Coercion detection*, for example stress analysis from voice or facial emotion. (6) *Obscuration detection* which detects that feature have been partially or wholly blocked from the "view" of the sensor (e.g., detecting accessory covering part of the face, like hat or scarf.

Challenge response detection

This method is widely used in other areas, such as authentication. The main idea is to create a challenge and send it to the user to answer it, thus, the user awnser is called a response. In Biometrics, challenge-response is a method to detect if a subject is alive once the subsystem capture the data of the subject. This is done be applying an interaction between the subject and the capturing device. The capturing device can ask the subject for an involuntary response (e.g., Pupil size change) or voluntary response (e.g., asks subject to close the eyes or move the head) [8].

2.5.2 *PAD* through system-level monitoring

This category is subcategorized into four subcategories; (1) *Failed attempt detection counter*, for example suspected ***PA*** if there is a sequence of similar failed attempts. (2) *Geographic* and (3) *Temporal* combines both to detect if the location and time of a ***PA*** is infeasible or unusual for the identity matched. (4) *Video surveillance* as a judgment by human operator (or video analytic system).

3 Requirements Specification and Methodology

This chapter introduces all the requirements related to the project in detail. This includes project and employer requirements. It also presents the assigned methodology to achieve each of the employer requirements. This chapter answers the following questions: (1) What are the project and employer requirements that are defined? (2) What are the limitations to consider for this project? (3) What are the applied methodologies in order to achieve the desired results?

3.1 Project requirements

Project requirements are split into two categories; researching requirements and data collection requirements. Both are described in the following sections.

3.1.1 Research requirements

This project is running in a researching environment, where a huge amount of previous work, confidential, as well as non-confidential documents and data already exist. Therefore, it is needed that a task performer signs a research confidentiality agreement before getting access to these data. In the case of this project, such data are fingerprint databases and presentation attack detection software.

As mentioned in Section 1.5, this project is part of the ***BATL*** project, which is an international project that is coordinated by institutions from the United States (***US***). Also, the project will be handling human participants and data. Therefore, there is a need to perform an online course for Protecting Human Research Participants (***PHRP***). The course provides knowledge on handling human participants during research studies according to ***US*** laws. This knowledge is presented in the form of literature review of history, text slides, case studies and quizzes. At the end of the course, the participant gets a certificate valid for one year. The certificate for the task performer in this project can be found in Appendix D.

3.1.2 Data collection requirements

Achieving the goal of creating - a pilot version of - a fingerprint presentation attack database requires to collect sensitive and personal data for researching purposes. As the new General Data Protection Regulation (***GDPR***) has already been adopted early this year [38], the data collection process for this project should follow and adapt to the new regulation. The main reasons for this are:

- This project is running in Germany as it is a European country and hence a part of the European Union.
- Most likely, the collected data will be taken of European residents.

The ***GDPR*** demands that data processing is *lawful*, *fair* and *transparent* [39]. These terms are described briefly in the following:

Lawful Collecting, holding and using the personal data should ensure the confidentiality. In researching environments, the personal data is used to support legitimate researches or activities considered to be of public interest. In these cases the personal data is necessary to be stored [39, 40].

Transparent The controller (i.e., the task performer in this project) should be honest and open with the subjects about: (1) the data collection reasons, (2) how the data is stored, (3) if the data will be shared [39]. Also, the subjects should be informed by the controller about their right of controlling their data by accessing, deleting or modifying it if needed in future.

Fairly All participants must be treated fairly, and respected in case of refusing to participate [39].

Applying the GDPR

The ***GDPR*** defines the biometric data (i.e., fingerprint in this case) as personal data, which is a reference that leads to identify a person (data subject) [14]. Besides the fingerprint, this project collects other personal and non-personal data from the subjects. These data and its handling are described in Table 4.

The employer of this project provides a consent form that is proved by the institution and other relevant fields. This form need to be signed by all participants before any data collection starts. The form presents clearly the goal of the project, reasons of collecting the data, the confidentiality of the data, subject's rights and contact information of the employer and the institution. This form is provided in Appendix E.

The different data that this project collects are stored either in the database or the consent form (see Table 4 for detailed description). The only connection between the data in the database and its owner is the Subject ID, which can be found only in the consent form.

Once the original database is created in a later project, all the content of the pilot database will be deleted since it will not be useful anymore.

Data	**Collection reason**	**Stored in**	**Critical**	**Accessed by**
Fingerprint	Improving the security around fingerprint recognition	Local ***SQL*** Database & hard disk	Yes	Only authorized people
Age	Filter the data using the subjects' age	Local ***SQL*** Database & hard disk	No	Only authorized people
Phone / Email	To contact if needed	Consent form	Yes	Only authorized people
Name	For communication reasons	Consent form	Yes	Only authorized people

Table 4: Collected data for this project

3.2 Employer requirements and methodology

This section presents the expected results, and the methodology to achieve each of them. As mentioned earlier in section 1.6.2, the results of this project are as follows:

3.2.1 PA database creation guideline

The guideline for fingerprint ***PA*** database creation is the primary result of this project. It should cover the following elements:

- A process of creating a normal fingerprint database.
- A process of creating a fingerprint ***PA*** database.
- Procedures for using several types of sensors as touch, swipe and/or touchless-bases sensors.
- Procedures for creating the different ***PAI***s
- Procedures for using the ***PAI***s to apply the ***PA***s.
- Procedures for handling and providing instructions to the subject during the data collection.

Moreover, the guideline should implement the aforementioned elements as a list of instructions to follow in order to create a database. Additionally, this should be easy to use as a checklist by others who are interested in creating fingerprint database. This guideline helps to:

1. perform the process of creating the original database more efficiently,
2. discover areas for improvement for the original project, and
3. provide instructions that can be followed by others, in case the creation of the original database is performed by others, or in case of creating other fingerprint databases in the future.

The guideline should be based on knowledge introduced in the literature, and the experience gained by creating the pilot ***PA*** database (discussed later in Section 3.2.2). Additionally, the task performer can interview students and experts that have worked with fingerprint databases in order to gather more information and add further credibility to the guideline.

3.2.2 Pilot fingerprint PA database

Fingerprint ***PA*** database contains both ***PA***s and bona fide presentations, which makes it different from a normal fingerprint database that only contain bona fide presentations. The database for this project is a ***PA*** database. The goals of creating such a database are as follows:

- Discover areas of improvements in the creation process for the original project in the future.
- Test some of the known ***PAD*** methods on the content of this database as a part of this project.

The database in this project is created based on the already known procedures and knowledge presented in the literature. This refers to some known ***PA***s, and database criteria that are mentioned in the literature (discussed later in the literature review chapter [i.e., Chapter 4], Section 4.2 for ***PA***s and Section 4.4 for database criteria). Also, the database contains raw images and possible metadata collected using the available sensors; Crossmatch Guardian 200 and Lumidigm V302). The database works as a validation method to provide more credibility to the created guideline in this project.

PA database requirements

There are some requirements specified due to the creation of the pilot ***PA*** database in this project. These requirements are summarized as follows:

1. The database should contain data for at least 10 participants.
2. All participants should do both bona fide presentations and presentation attacks.
3. The database should contain most of the given ***PA***s created by the provided materials.
4. Bona fide presentation should be taken of all ten fingers of each participant.
5. Each participant should try two different ***PA***s on each index finger.
6. Both bona fide presentation and ***PA***s should be performed on the legacy sensors (Crossmatch and Lumidigm).

The desired PAs

The employer provided a list of ***PA***s that need to be performed during the data collection phase. This list is *confidential*, and therefore, it will not be revealed or attached to this thesis. However, the provided materials to perform these ***PA***s are listed below.

The provided materials

Many materials are provided by the employer for this project to fabricate several ***PAI***s and perform most of the desired ***PA***s as mentioned earlier. Figure 7 shows most of the used materials in this project, and Table 5 lists some of the important materials with a short description of each.

Material	**Description**
Silicone	Several types of silicone are provided. Also, the provided materials are chosen of several qualities.
Dragon-skin	Silicone with special harden ability. Several types and qualities are provided.
Playdoh	One playdoh type is provided, including several colors.
Glue	Several glue types are provided, with different hardness abilities.
Latex	Several latex types are provided. Also, the provided materials are chosen of several qualities.
Gelatine	Several gelatine types are provided, with different hardness abilities.
Wax	One wax type is provided with several colors, including the machine to create it.
Colors	Several colors to mix to the other materials in order to change the original color of the material.

Table 5: List of the used materials to build different ***PAI***s

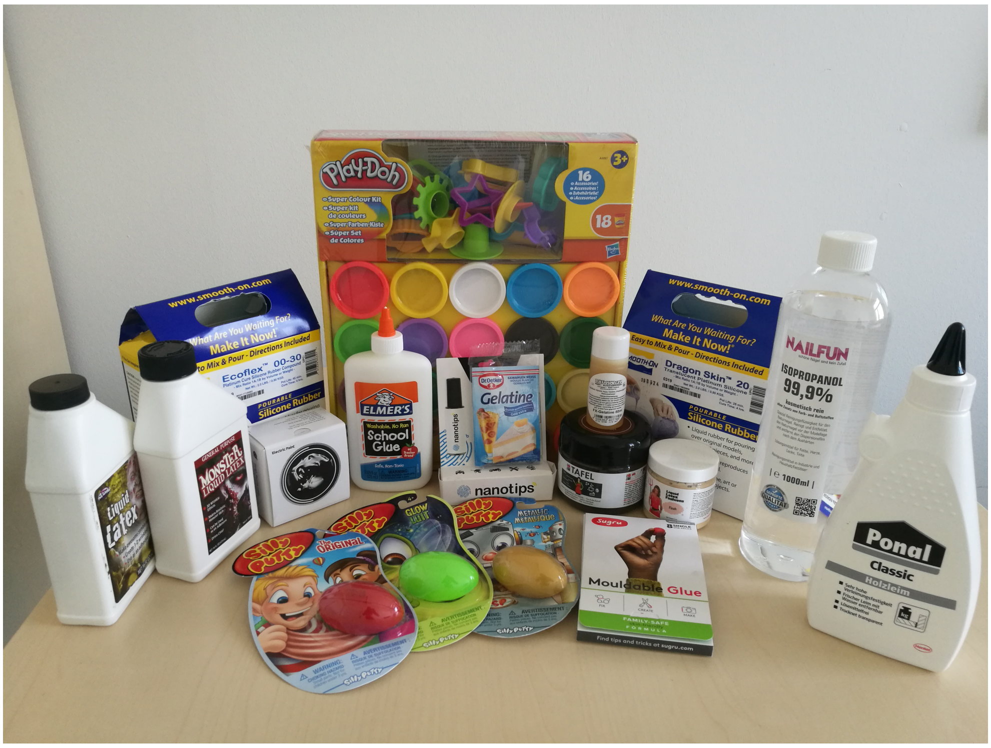


Figure 7: Most of the materials that are used to create ***PAI***s in this project

3.2.3 Evaluating PAs

In order to gain the best understanding of the ***PA***s impact to biometic systems - specially fingerprint-, this project provides a task to evaluate the applied ***PA***s based on the attack potential criteria presented in the ***ISO*** standard 19989 (i.e., [10]). The output of this evaluation is a list of ***PA***s and their attack potential impact. Furthermore, this list assists prioritizing between all ***PA***s based on the severity of each.

4 Literature Review

This chapter will focus on presenting the topic of fingerprint technology in depth. Including corresponding ***PA***s and ***PAD*** methods. Furthermore, it reviews the literature about fingerprint databases and their creation. The chapter provides answers of the following questions: (1) What is a fingerprint? (2) How can a fingerprint be analyzed in biometric systems? (3) What are the sensing technologies of a fingerprint? (4) How can a fingerprint be spoofed? (5) What ***PAD*** methods can be applied against the different spoofing methods? (6) Are there any limitations in the existing fingerprint databases?

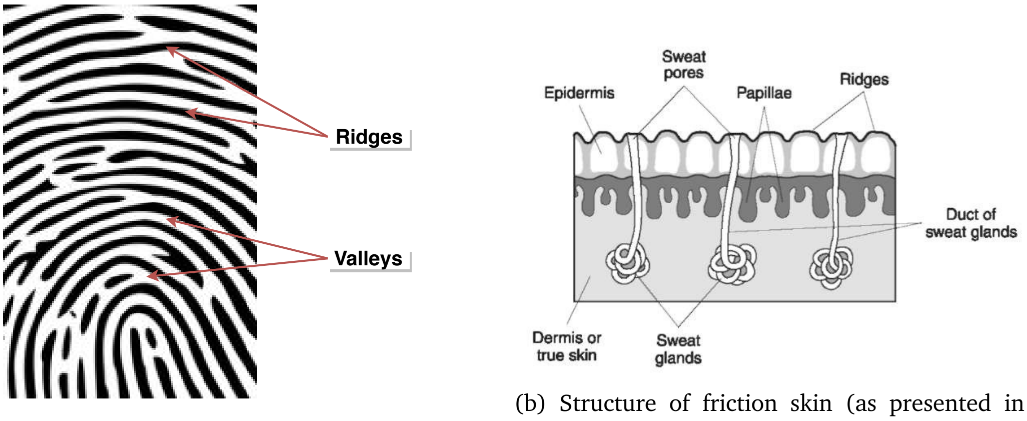
4.1 Fingerprint technology

For more information than provided in this section, the reader is referred to [7, 41, 42, 43].

4.1.1 Fingerprint formation

A fingerprint as mentioned in Section 1.2 is defined as "the impression of the friction ridges of all or any part of the finger" [15]. The finger skin consists of the so called friction ridges with pores. These ridges are already created during early foetal life; 3rd-5th month of pregnancy. However, it is one of the last recognizable characteristics to disappear after death. Figure 8a represents the ridges and valleys of a fingerprint.

A fingerprint is a well known biometric characteristic and it is a very unique biometric feature. It remains constant and does not change during the whole human life period. So, it grows in size, and the human body creates it randomly. Therefore, it is unique from a person to another even in cases of identical twins [35, 44].



(a) Ridges and Valleys on a fingerprint (as presented in [45])

(b) Structure of friction skin (as presented in [46])

Figure 8: Ridges and valleys on fingerprint in (a), and Structure of friction skin in (b)

The finger skin consists of two layers; *Epidermis* and *Dermis*. As Figure 8b shows, epidermis is the top layer, thinner than dermis and serves as a protective covering for the dermis. Dermis contains sweat and sebaceous glands that produces sweat and oil. It also contains a the so called *papillae*, which is responsible for the reproduction of the fingerprint pattern. So, minor cuts, burns and injuries to the fingerprint will just effect the appearance of the pattern a limited time. Usually, the outer layer of the fingerprint changes multiple times a year, which can be observed normally in case of injuries.

4.1.2 Fingerprint history

According to [41], human fingerprints have been discovered on a large number of archaeological artifacts and historical items. Which means that the ancient people were aware of the individuality of fingerprints, even if such awareness does not appear to have any scientific basis as mentioned in [42]. This was the case until the late sixteenth century. In 1864, the first scientific paper was published by Nehemiah Grew reporting his systematic study on the ridge, furrow and pore structure in fingerprints.

[47] is mentioning that the first detailed description of the anatomical formation of fingerprints was in 1788 by Mayer, where a number of fingerprint ridge characteristics were identified and categorized. Later, one of the most important milestones in the history of fingerprints occurred in 1809 when Thomas Bewick started using his own fingerprint as a trade mark for himself. In 1823, the first fingerprint classification scheme was proposed by Purkinje, which classified fingerprints into nine different categories based on the ridges formulation [47].

The foundation of modern fingerprint recognition was established by the findings of Henry Fauld and Herschel in 1880. Henry Fauld was the first to scientifically suggest the individuality of fingerprints based on empirical observations. Herschel asserted that he had practiced fingerprint recognition for about 20 years [41]. Later in 1888, one of the most important studies on fingerprint was published by Francis Galton, who presented the minutiae points and galton details.

Few years later, in 1899, the well-known "Henry system" of fingerprint classification was established by Edward Henry and his assistants. It was classifying the fingerprints of individuals based on their pattern. Early in the twentieth century, the formation of fingerprints was well understood. According to [41, 47], the biological principles of fingerprints was summarized as following:

1. Individual epidermal ridges and furrows have different characteristics for different fingerprints.
2. The configuration types are individually variable, but they vary within limits that allow for a systematic classification.
3. The configuration and minutiae points of individual ridges and furrows are permanent and unchanging.

"*The first principle constitutes the foundation of fingerprint recognition and the second principle constitutes the foundation fingerprint classification [41].*"

During the twentieth century, fingerprint recognition was formally accepted as a valid personal identification method and became a standard routine in forensics. Also, fingerprint identification agencies were set up worldwide and criminals fingerprint databases were created [42]. During the same century, various of fingerprint recognition techniques, including latent fingerprint acquisition, fingerprint classification and fingerprint comparison were developed.

Overtime, the databases could not handle the received requests, because of the huge amount of fingerprint data records that were stored in these databases. Keeping in mind that for each subject in the database there are at least ten records of all the subject's fingers. Therefore, in 1960s, a new investigation started by FBI department in UK and the Paris Police department to develop an automatic fingerprint identification systems (***AFIS***). The results were so successful that today almost every law enforcement agency worldwide uses ***AFIS*** [41].

Nowadays, fingerprints are one of the most developed technologies in Biometrics, and automated fingerprint recognition technologies have grown not only on the forensic systems, but also on civilian devices and applications. It is used as an identification method to recognize individuals and as an access control of several devices. It is integrated into mobile devices, personal computers, safes, etc. According to [48], fingerprint is faster to access than a ***PIN***-code once users get used to it. Besides, fingerprints provide a higher level of security as no two fingers can have the exact same dermal ridge characteristics, and it does not change with age or gets effected by any disease. It is easy to use by users, does not require any additional education, and reduces the amount of human effort. Fingerprint capturing devices are widely available on the market. Many of these devices do not require a high maintaining cost, and provide an extremely fast identification by identifying or rejecting the subject in a matter of seconds [49].

4.1.3 Fingerprint analysis

The ridges on the fingerprint can be visualized by lines. Once a finger directly touches any object, a copy of the fingerprint pattern will stick to the object. This is called a *latent*. The latent is an inadvertent impressions left by fingers on surfaces of objects [18]. It is generated without intention because of the oil and sweat on the finger. Usually, it is not visible, but sometimes a powder, lasers or alternative light source is needed to make it visible.

There are three levels of fingerprint analysis. Since this thesis is focusing on the topic of the ***PA***s and not the ***PAD***s, the following subsections describe briefly the three levels of fingerprint analysis:

Level 1: fingerprint pattern

As it may be observed, the formulation of the fingerprint pattern is different from a finger to another, not only fingers of different people, but also fingers of the same subject. There are three main categories for fingerprint pattern; *Arch*, *Loop* or *Whorl*. However, each fingerprint pattern can only be categorized into only one of the categories. Figure 9 shows the an example of the different patterns. The mentioned categories can be further subcategorized i.e. plain- or tented arch, right-, left- or twin- loop and plain- or accidental whorl.

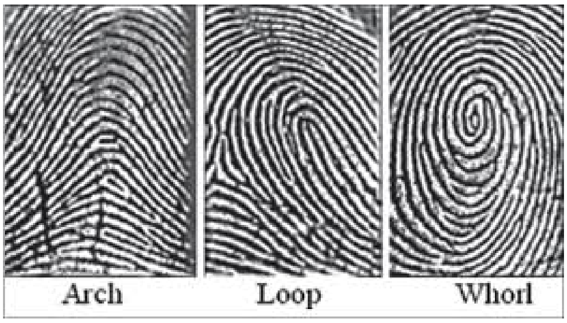


Figure 9: Fingerprint patterns (as presented in [4])

Level 2: Edgeoscopy

The fingerprint pattern contains more details that can be used for individual recognition. These details are known as the minutiae points and galton details. Edgeoscopy is the analysis of minutiae points and galton details. As described earlier in Section 2.2.2, minutiae points are the major features of a fingerprint image and are used in the matching of fingerprints [19]. On the other hand, galton details are the compositions of ridge endings or bifurcations. Figure 10 represents different examples of minutiae points and galton details.

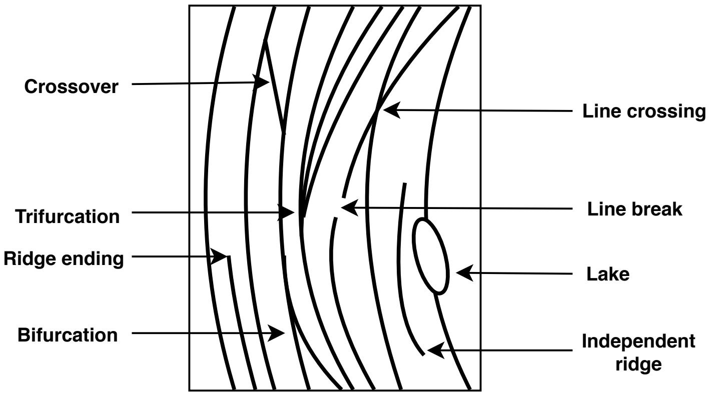


Figure 10: Example of minutiae points and galton details

Level 3: Poroscopy

Poroscopy is the analysis of sweat pores. The sweat glands - as in Figure 8b - produces sweat through sweat pores that exist on the ridges of the fingerprint. There are up to 2700 small pores in size the range of 60 µm. It is hard to visualize the pores because it requires a high ***dpi*** [1] camera (800 ***dpi*** or more) [50].

[1] Dots Per Inch

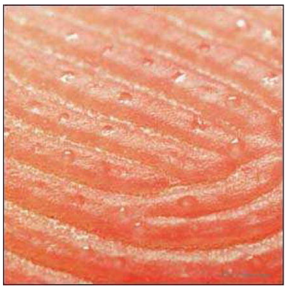


Figure 11: Sweat pores (as presented in [5])

4.1.4 Fingerprint capture process

A few years ago, before the capturing devices were developed, the fingerprint of a subject used to be captured using ink and paper to copy the pattern. Another method was by collecting the latent fingerprints at crime scenes. Both of these methods are traditional methods and can be defined as an *off-line* capturing process [51].

On the other hand, the *live-scan* term is referring to direct scanning of finger tips using electronic sensors. In this case, the sensor captures one or more digital biometric samples of the subject's fingerprint, and store it into one or many databases in different formats [51].

4.1.5 Fingerprint sensing technologies

Nowadays, numerous sensing technologies exist for capturing a fingerprint from its source. Additionally, many capturing devices (i.e., fingerprint sensors) also exist based on the known sensing technologies. Figure 12 shows an overview of the fingerprint sensing technologies and the sensors using these technologies. In general, fingerprint sensing technologies can be split into two main categories; touch-based (i.e., the fingerprint source touches the sensor in order to capture the fingerprint) and touchless-based (i.e., the sensor device captures the fingerprint from its source without requiring any contact).

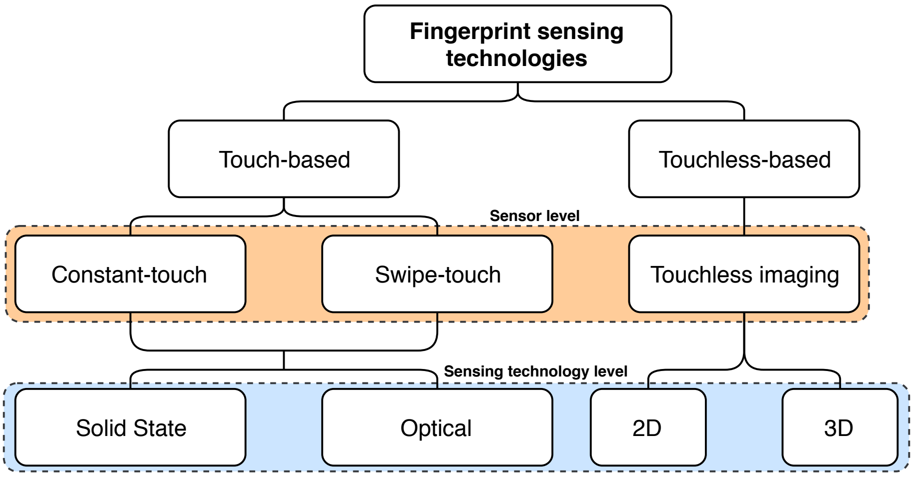


Figure 12: Fingerprint sensing technologies classification inspired by [6]

Touch-based

Furthermore, the group of touch-based technologies provides constant-touch sensors (i.e., "area scan" according to [6]) and swipe-touch sensors. The constant-touch sensors work by placing the fingerprint source on the sensor in order to capture an image of the fingerprint while the source does not move, where sometimes the movement of the source can affect the captured image. According to [7, 52], the touch-based sensors also suffer from problems, such as (1) latents are left on device surface after capturing, (2) skin deformation, and (3) hygienic issues.

On the other hand, the swipe-touch sensors require the fingerprint source to swipe over the sensor's surface in order to capture the images from a time-series acquired. This group of sensors provides the ability of coming in smaller sizes than the constant-touch sensors, which can be easily integrated into portable devices, and have a small cost factor [7]. However, these types of sensors can lead to higher Failure to Acquire (***FTA***) rate [7], which means a high chance of miscapturing the fingerprint because of reasons such as misplacing the finger or fast swiping.

Additionally, both the constant-touch and swipe-touch sensors use the optical and solid state sensing technologies [6]. These technologies are described as follows:

Optical sensing technologies

According to [7], and as displayed in Figure 13 (presented in the same citation), the optical sensing technologies are based on systems that contain:

- A photosensitive surface where the fingertip can be placed on.
- One or more light sources that face the surface.
- A glass prism or optical fibres under the surface to reflect the lights.
- A lens to capture the reflected light and capture the fingerprint on different resolutions.

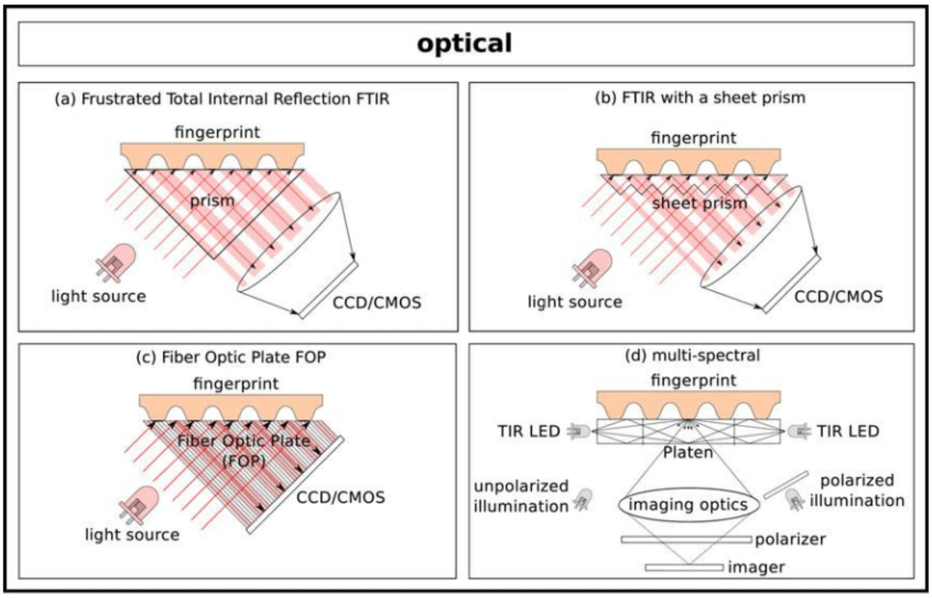


Figure 13: Optical sensing technologies as presented in [7]

The optical sensing technologies work as follows: (i) one or more light sources (as in Figure 13-d where multiple light sources allow various illumination conditions) that faces the surface where (ii) the fingerprint source is placed. The surface can be a prism (Figure 13-a), a sheet prism (Figure 13-b) or a Fiber Optic Plates (***FOP***) that (iii) reflect the valleys' light from the fingerprint to a photosensitive surface that (iv) collects the reflected light. Then, (v) a lens captures the fingerprint image [7].

Solid state sensing technologies

According to [7], the solid state technologies can be integrated in a single chip, which decreases the size and the cost factor. There are six different solid state technologies discussed in [7]. These are illustrated in Figure 14 as follows :

Pressure (Figure 14-e)

This technology uses the provided piezoelectric sensors cells which produce voltage when a pressure is applied to it by the fingerprint source. The variation of voltage from a cell to another helps to formulate the fingerprint, where it depends on whether the cell touches a ridge or not.

Capacitive (Figure 14-f)

In this technology, a two-dimensional array of micro-capacitor plates are provided in order to generate the fingerprint from its source using an electrical current. The valleys provide different results than the ridges while touching the micro-capacitor plates, which makes it possible to distinguish between both and create a fingerprint image.

Thermal (Figure 14-g)

Pyroelectric pixels exist in this technology in order to distinguish between the skin (i.e., ridges) and the air (i.e., valleys) based on the temperature. The heated pixels help to generate an image of the fingerprint.

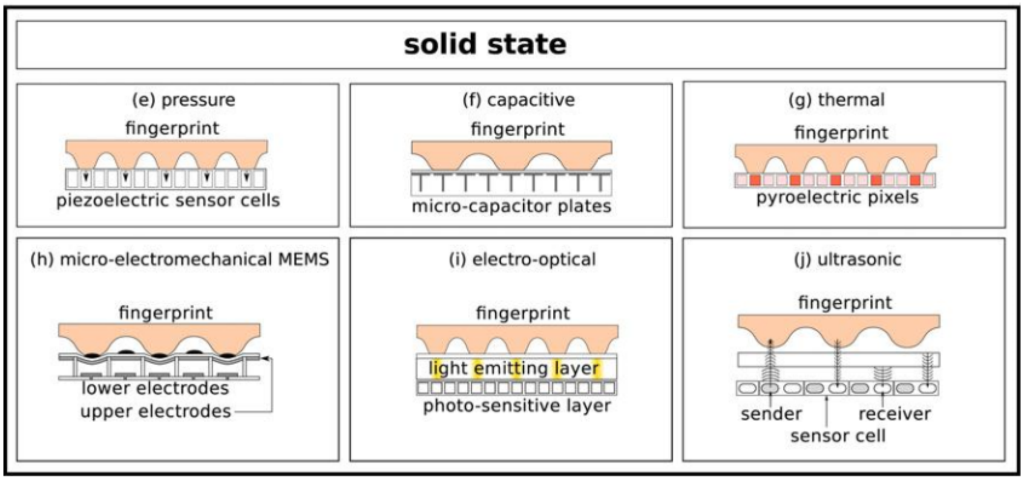


Figure 14: Solid state sensing technologies as presented in [7]

Micro-electromechnical (Figure 14-h)

This technology is based on the pressure technology. In this case, two layers of electrodes are provided (upper and lower electrodes), so the ridges from the fingerprint source push the cell capacitors on the upper electrodes causing a capacitance change between the lower and the upper electrodes, which can be used further to generate the fingerprint.

Electro-optical

Two layers are provided in this technology in order to obtain the fingerprint pattern; the light emitting layer and the photosensitive layer. As summarized in [7]:

> *"The light emitting layer emits light based on the electro potential on its surface. Since the fingerprint ridges touch the surface and the valleys do not, the electric potential varies across the surface generating a fingerprint representation that is captured by the photosensitive layer."*

Ultrasonic

A sensor cell that consists of both small sender and receiver cells of the acoustic signal. The sender cells transmit the signal against the surface where the fingerprint source is placed. This causes a reflection with differences in the acoustic impedance between the skin (i.e., ridges) and the air (i.e., valleys), which further helps to generate the fingerprint pattern.

Touchless-based

In contrast to the traditional touch-based technologies, touchless-based technologies try to reproduce the fingerprint from its source in a contactless manner by using the touchless imaging technique [6]. This is performed using one or more digital cameras that capture the fingerprint from distance. The touchless-based technologies try to solve the limitations of the touch-based technologies (e.g., latent on the surface after use, high ***FTA*** rate in swipe-based, and pressure effectiveness to the minutiae points). Additionally, this leads to increase the usability, where users do not require much effort or training to use it. However, the touchless-technologies provide limitations, such as noise, reflections, and more complex background than provided in the touch-based technologies, where the skin can be considered as a part of the background sometimes. These drawbacks can be overcome by several hardware and software solutions that are presented in the literature [43].

According to [43], the process of generating the fingerprint with such technologies is based on two processes. The first one is *acquisition*, where the image is captured. Furthermore, the second process is *computation of a touch-equivalent image*, which is responsible for extracting the fingerprint pattern form the image and reproduce it. Moreover, there are two classifications for touchless imaging; two-dimensional (***2D***) and three-dimensional (***3D***) technologies as illustrated in Figure 12. Both ***2D*** and ***3D*** have three factors to consider in order to capture and generate the fingerprint. These factors are presented as follows:

- Illumination (i.e., accepting an uncontrolled light condition, or applying one or more source lights).

- Camera resolution in order to gain a high quality and reveal the details.
- Distance between the fingerprint source and the camera.

Nowadays, more studies show that it is possible to provide more data about both the outer layer and inner layer of the finger. This is applied by adding different technologies to the existing ***2D*** and ***3D*** technologies, such as (i) Optical Coherence Tomography (***OCT***) in [53], ***SWIR***, and ***LCSI*** in [54]. Furthermore, the ***2D*** and ***3D*** are summarized as follows:

Two-Dimensional (2D)

This can be simply performed using a webcam or mobile phone camera, or using a more complex setup that includes more cameras or controlled illuminations. Additionally, a single point light source or more in different colors and wavelength conditions are applied in order to obtain best visibility of the ridge pattern from the fingerprint source. Moreover, algorithms for subtraction of any noise and background are applied in order to filter the fingerprint from the image. Then, other kind of algorithms are used to normalize the image in order to be a touch-equivalent image as provided by touch-based sensors [43].

Three-Dimensional (3D)

According to [43], ***3D*** technologies are more expensive to apply than ***2D*** technologies. However, they can provide more data about the fingerprint and the finger skin, which helps to ensure the accuracy. There are three different strategies to acquire ***3D*** imaging; (i) multiple-view, (ii) structured light techniques, and (iii) photometric stereo. The last two require user cooperation by waiting for a longer time without any movement to finish capturing.

4.1.6 Challenges of fingerprint sensors

As mention in the previous section, it is possible that fingerprint sensors capture a poor image quality, which can be referred to as noise images. This can happen for several reasons, such as (1) the finger state itself, in case of dirty, too dry or wet fingers, (2) the placement (e.g., part of the pattern is missing) and (3) the rotation of the finger on the scanner. This can be controlled in a controlled environment e.g., police station, but not in uncontrolled environments such as smartphones, where the users can behave differently than expected. (4) The pressure of the finger can also be a reason if the subject presses too much or too less. This effects the image and can hide the original minutiae points or cause false minutiae points. This can be controlled by adding an operator to control the pressure, or capture the fingerprint in a capture-less (touch-less) manner. (5) Scratches on the fingerprint can cause an image where the ridges are not completed as expected. (6) The background area of the finger can make it hard for the capturing device to determine the boarder of the fingerprint [7].

4.2 Fingerprints presentation attacks

For more information than provided in this section, the reader is referred to [7].

4.2.1 PAI fabrication

As mentioned earlier in Section 2.4, this thesis is focusing on spoofing methods during the data capturing process (i.e, against the sensor). As it may be observed, this case of spoofing is what this thesis refers to as presentation attack. The imposter presents a fake fingerprint to the sensor, either a copy of someone else's fingerprint, or he/she tries to hide his/her own by damaging it, so it does not get recognized by the sensor.

Following the ISO standard ([3]), the term of artefact is replacing the so called fake fingerprint, and it will be further used in this thesis. Keep in mind that the term of artefact is not limited to fingerprints, but also other biometrics.

4.2.2 PAI fabrication methods

According to [55], there are two classes of spoofing methods depending on the availability of the original finger during the fabrication process (i.e., artefact creating process). This is regardless to the manner of how the bona fide finger is available, where it can be obtained by blackmailing and violence against its victim or without the victim's knowledge by being under the effect drugs or anesthesia [7]. If the original finger is available during the fabrication, the spoofing method is called *direct casting*. In the other case, where the original finger is not available, it is called *indirect casting*.

The direct casting method uses the available original finger to create a copy of it. In order to create the copy, there is a need of a mould and an artefact. The materials to create both the mould and the artefact are mentioned in the next subsection (4.2.3). Meanwhile, the mould is a soft material which hardens with time, and the original finger is pressed against it to create a negative copy of the original finger and its fingerprint. As the mould plays the role of a form, several artefacts can be created. The artefact is created by a material used to fill up the mould in order to take a copy of the hardened fingerprint. To achieve best results during the fabrication process, the finger should be pressed gently to the mould, so all details get recorded. It is important that the finger and its subject does not move while touching the mould, otherwise the mould will not contain all details. Once the mould get hardened, the finger should try to leave the mould carefully.

Indirect casting is similar to the traditional forensic investigation in the crime scenes. Where the original finger does not exist to create a direct copy of it. However, a latent can be used instead of the original finger. One of the most common methods to handle the latent is the powder dusting, which is according to [56] routinely used. Using this method, the powder will stick to the latent fingerprint, makes it easier to visualize, and easy to capture pictures or even lifting it up using a special tape or glue [7]. The next stage is to digitize the latent by scanning it, and send the image further to a software application (e.g., image editor software) to recover the missed parts if needed [57]. Then the image can be converted to black and white mask, so it gets converted to a mould and artefact later. Section 4.2.3 describes the further process of using the black and white mask and the materials that are used to create both the mould and the artefact.

4.2.3 Fabrication materials

In the case of direct casting, the mould can be created using several materials such as thermoplastic, silicone, playdoh, plasticine, candle wax and so on. Some of the materials get hard faster than others (e.g., candle wax gets harden in less than a minute, while silicon and playdoh can take longer time). Also, the same materials can be used to create the artefact, besides of gelatine, latex and glue. However, it is important that the same materials cannot be used to create the mould and the artefact of the same ***PAI***, because there is a high chance that the simillar materials stick to each other, and it will not be possible to use either the mould or the artefact further.

When it comes to indirect casting, the black and white mask is printed to a thin transparent film by a laser printer. According to [57], this can be used directly as a mould because the toner deposit creates elevations on the surface of the film, similar to the expected ridges and valleys. An alternative way as they mentioned is to use the technology of a photosensitive circuit board (***PCB***, where the film with the fingerprint is put into the ***PCB***, and illuminated with ultraviolet (***UV***) light [7]. Further, the same materials as in the direct cast method can be used to create the mould and the artefact.

The quality of both the mould and the artefact -using the mentioned materials- cannot hold for a long time period, because of several reasons such as temperature, dust and so on. Therefor, a new suggested material to create the mould is using a 3D printer to create the mould [7]. The only limitation in this case is to use a printer that can draw the small details of the fingerprint in the original size of the finger. Keep in mind, this method can be also used to create a ***3d*** printed artefact, where the same limitation need to be considered.

It is easy too see that most of the materials are available to buy on the market or online shops. The quality of the fabrication, and the creation skill of the imposter are something that can be improved over time. Therefore, sensors are in need for ***PAD*** methods to prevent these ***PA***s of happening.

4.3 Fingerprint presentation attack detection

As mentioned earlier in Section 1.4, the ***PAD*** methods can be any technique implemented in form of hardware (i.e., data capture subsystem or sensor level) or software (i.e., system or algorithms level) solutions. Moreover, these techniques can be implemented through data capture subsystem, or through system level monitoring [3]. As mentioned earlier in Section 2.5, these are presented in the following: *(For more information than provided in this section the reader is referred to [7, 3])*

4.3.1 PAD through sensor level

In [7], the fingerprint ***PAD*** methods are classified as liveness detection and alteration detection. Additionally, more live case scenarios have been observed, and more classes have been established in [3]. The new classes are alteration detection, non-conformance detection, coercion detection, and obscuration detection. Figure 31 in Appendix C presents an overall illustration. A brief presentation is given for each of the aforementioned methods in the following:

Alteration detection

Fingerprint alteration is a case where the concealer tries to destroy or alter his/her fingerprint. Reasons for this can be (i) refusing to be enrolled to the system or (ii) refusing to be matched to someone already enrolled to the system. This is a problem that needs to be detected in general, but specially in areas such as border control and forensic investigations. Several methods to detect such alteration are presented in [58], such as analysis of minutiae points - and their orientation, orientation field, singular point destiny analysis, etc.

Artefact detection

Artefact fingerprints exist in several forms such as gummy fingers, overlays, ***3D*** fingers, etc. These can be used by an imposter who got access to a fingerprint which belongs to another genuine subject. Since it is hard for an artefact to contain the details of a real fingerprint, the detection methods can aim to detect the static details in the fingerprint such as sweat pore and the perspiration produced by them while touching the surface. This and other methods are discussed in depth in [7].

Coercion detection

For fingerprints, it is hard to detect if a provided presentation is a coercion presentation, which is considered as a ***PA***. However, theoretically it can be possible to detect such cases, where the presented finger is under stress by pulse oximetry or heartbeat movements. Both are described in [7].

Liveness detection

In some cases, a dead finger can be presented by the imposter. Several ***PAD*** methods exist today to detect a living fingers (i.e., liveness detection) such as (i) using ***LSCI*** technology to detect blood flows in the finger [59]. Other methods are (ii) multi-spectral properties, where the blood in the finger moves away from the tissues while performing a finger pressure. Additionally, as presented in [60], odor analysis studies expect that living fingers have different odor than fake fingers. More studies are presented in regarding liveness detection are presented in [7].

Non-conformance detection

For fingerprints, such case can be a partial presentation of the fingerprint. Nowadays, most of the sensors will not accept partial presentations neither for enrollment nor for identification. Also, worth to mention that errors as ***FTA***, will be the response for such an attack.

Obscuration detection

In some cases, the concealer tries to hide his own fingerprint pattern. An easy way to apply such scenario is hiding the minutiae points from the fingerprint by applying high pressure, so the differences between the ridges and valleys do not display normally. Such detection methods are applied already to some touch-based sensors, where they do not consider the presentation as valid and ask the user to present another one.

4.3.2 PAD system-level monitoring

Other information and resources can be provided to the system in order to increase the security and detect ***PA***s. The following are some ideas presented in [3]:

- **Failed attempt detection counter** - due to the failed attempt that can be performed while presenting a ***PAI***, it can be helpful to add a counter that detects a sequence failed attempts. It worth to mention that in some cases where the sensor usability is low, a genuine user will suffer from such detection method.
- **Geographic** and **Temporal** - if the location and time for a subject are known to the system, then, it is hard to fool the system if the time and location provided during the ***PA*** is different or far away from the last provided. Such detection method

will have a challenge in order to be accepted by individuals who claims that such information are private information.

- **Video surveillance** - One or more human operators can see subjects while presenting their fingerprints by a video monitoring. Such methods are in conflict of the idea of automating and digitizing the services that offer less human involvement in such processes.

4.4 Fingerprint databases

There are two types of fingerprint databases; (i) normal fingerprint databases and (ii) ***PA*** databases. The main difference is that ***PA*** databases contain fingerprint samples of both bona fide presentation and ***PA***s. On the other hand, normal fingerprint databases consist only of bona fide presentations. Furthermore, both databases can either be open source (i.e., publicly available), shared with the research community, or private databases (i.e., developed and used in-house). The following sections present both categories: *(For more information than provided in this section the reader is referred to [61])*

4.4.1 Fingerprint databases

This category of databases is the oldest, more used and better known than the ***PA*** databases. According to [61], such databases exist in several forms, such as:

- digital fingerprint cards acquired by the traditional paper-ink method as in some of ***NIST*** [2] Special Databases (***SD***),
- live-scan fingerprint databases using one or multiple sensors as in CASIA v5.0 database.
- Camera images using high or low resolution cameras (e.g., webcam),
- and latent fingerprint databases collected from investigation scenes.

Such databases can be used for several fingerprint areas of studies as fingerprint-identification/verification, -performance measuring, -template protection, -quality measuring, and etc.

Moreover, most of the databases are created for a specific purpose or study. An example of such case is the Fingerprint Verification Competition (***FVC***) that was organized in 2000,-02,-04, and 2006. The goals of such an international competition were to evaluate the new developed fingerprint verification methods based on a privately developed database before the competition end, and available for the research community after the competition.

According to [61], to gain best results from a database and to use it in several studies, the database should contain the following research challenges:

- **Multi-session** for each subject.
- **Multi-samples** of each fingerprint.
- **Multisensor** used to capture the same fingerprint.
- **Multi-resolution** images provided of each fingerprint.

[2] National Institute of Standards and Technology

4.4.2 Fingerprint PA databases

In general, this category of databases is newer than the aforementioned and is developed to improve the presentation attack detection methods. This type of databases contains several ***PA***s applied using several ***PAI***s that are further created using several spoofing materials. Two of the well-known ***PA*** are the ATVS and the Liveness detection (***LivDet***) Competition databases.

The ATVS databases consist of two different datasets collected from 17 subjects and contains both real and fake fingers. The first dataset contains ***PA***s generated with cooperation of its subject (i.e., direct casting). On the second one, no cooperation has been taken to generate the ***PAI***s and apply the ***PA***s (i.e., indirect casting). Both these datasets have as many ***PA*** samples as bona fide presentation samples [62]. Each subject applied four fingers (index and middle fingers from each hand), and four samples are captured of each.

The ***LivDet*** databases are created to test the submitted ***PAD*** systems and algorithms during the competition. The competition is arranged every two years, the first one started in 2009 and the last one was arranged in 2017. They use three or more sensors to capture fingerprints, and provide the same amount of captured samples of bona fide presentations and ***PA***s [7]. Moreover, they clarify the materials that are used to create the ***PAI***s.

5 Fingerprint PA Database Creation Guideline

This chapter presents the primary result of this project; a guideline (i.e., Best Practice Manual (***BPM***)) for fingerprint ***PA*** database creation, which includes the creation of a normal fingerprint database as well. The content of this chapter provides answers to the following questions: (1) How is the data collection process performed? and (2) How is the proposed guideline structured? In order to answer these questions, this chapter is split into two sections; Section 5.1-the data collection process, which presents the results of the applied methodology, and Section 5.2-the guideline proposal that presents the final result for a ***BPM*** for fingerprint PA database creation.

For a discussion about the guideline (such as the guideline's motivation, challenges, limitations, etc.), the reader is referred to the discussion chapter in Section 8.2.1.

5.1 Data collection process

As mentioned earlier in Section 3.2.1, the guideline is created based on knowledge presented in literature, the experience gained by creating the pilot database, and the interview sessions with students and experts who have worked with fingerprint databases. It is worth mentioning that the process of the data collection started by reviewing the literature to build a first-draft guideline, then, interviewing students and experts to gather more information and discuss further improvements, and finally finished by applying the guideline on the pilot ***PA*** database to validate it in a real fingerprint data collection scenario.

The process and results of each of the aforementioned methods can be summarized as follows:

5.1.1 Literature review results

To the best of our knowledge, there are no existing standards or guidelines for a fingerprint data collection or database creation protocol, which can be found in literature. The main reason for this is that most of the databases are created for a specific use-case, where the goals and usage are different from a database to another. Moreover, it is worth mentioning that it is hard to find documented limitations in the existing databases. Such limitations can be referred to as: (i) human error (i.e., by the controller) in labeling files or providing more or less instructions to the subjects than needed, and/or (ii) sensor limitations as the need for an external driver or software to perform the acquisition process. A possible explanation for not providing such information in the publications is limitation on the number of pages for the articles.

However, there are other information that can be found in literature, which can contribute to the proposed guideline such as:

- the research challenges that are presented in [61] (mentioned earlier in Section 4.4.1),
- the different study areas of fingerprints, and the metadata needed in each study.

- the need for more fingerprint data to test and improve machine learning and deep learning techniques that are used in the field of fingerprints.

All of the aforementioned points are considered as keynotes in the guideline. To summarize it, fingerprint databases that provide as much metadata as possible (about the subject, sensors, environment, etc), multi-sessions for each subject, multi-samples of each finger, and use multisensors are more convenient to use and provide better results than others.

5.1.2 Interview sessions

The interview sessions were one of the methods discussed to be used in this phase in order to collect data that can contribute to the guideline. These methods were online survey or interview sessions. The last mentioned method ended up being used for the purpose of data collection in this thesis. A discussion regarding that decision can be found in the discussion chapter, Section 8.1.3.

At the beginning of this phase, a first-draft of the guideline - based on the knowledge in literature - was created and ready to be used in the interview sessions in order to give the students and experts an idea of the desired goal. The guideline draft was updated after each interview session in order to gain better feedback and input in each new session. Also, changes between each round were noted and discussed in each new interview session. It is worth mentioning that the interview session started and ended by interviewing experts who have worked at least four years with fingerprint studies.

As a result of this phase, 12 persons were interviewed in total including six professors and six PhD and master students. Most of them are working in the Norwegian Biometrics Laboratory (***NBL***) and/or ***da/sec*** in Germany. Furthermore, three have worked with fingerprint ***PAD***, while the others worked on other areas related to fingerprints. Figure 15 shows a distribution between the number of interviewed persons (y-axis) and their experience working with fingerprints in years (x-axis in blue), while the distribution in orange (x-axis) shows the number of databases the people worked with.

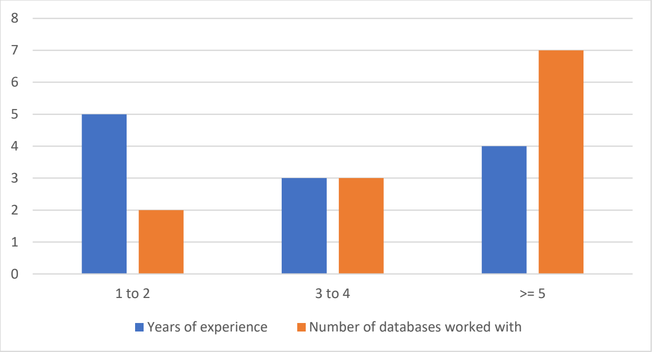


Figure 15: Distribution between years of experience and number of fingerprint databases were analyzed by the interviewed persons

The following questions were discussed during each interview:

- How many years have you worked with fingerprints?
- How many fingerprint databases have you worked with?
- What kind of limitations can a fingerprint database have?
- Did you experience any limitations that affected your result?
- What metadata do you think are needed in a fingerprint database?
- Do you have any feedback to add to the content in the given guideline? (after presenting the proposed guideline)

The interview sessions took a period of one week to perform due to the availability of the professors and students, where each session took between 20 to 25 minutes. This method was the most effective and resourceful for gathering information that contributes to the guideline proposal. The following summarizes important keynotes collected in this phase:

> **[a]** Fingerprint databases are often created to solve one or more use-cases in a specific study. In order to understand the usage of such databases in each of the studies, a classification of fingerprint study areas is needed.
>
> **[b]** Usually, a database contains only the required metadata for the purpose of the use-case, because it is considered as time consuming and effort demanding to collect more metadata than needed. Furthermore, the ***GDPR*** has strict rules for the collection of other sensitive data (e.g., skin color, ethnic group, etc.). Therefore, a classification of metadata - based on the strictness and efforts - is needed in order to assist choosing the possible metadata to collect in a database.
>
> **[c]** In general, a fingerprint database is often created either (1) to validate a purpose of a new study, sensor, or algorithm, or because (2) no other database covers the needed requirements for the new database. Such requirements can be missing one or more pieces of metadata, less provided subjects, few acquired samples of each fingerprint, and so on. Due to these facts, there is a need for a framework that proposes a database creation protocol that considers the reusability of a database in future research and studies by providing more data than required in the newly created database.

5.1.3 Pilot PA database experience

There are several goals to achieve by creating the pilot ***PA*** database in this project; The main goal is to apply and validate the proposed guideline and discover areas of improvements. Another goal is to provide a best practice manual (***BPM***) for creating ***PAI***s and performing the different ***PA***s. Furthermore, It is worth mentioning that getting acquainted with the processes of creating a database helps to set an estimation for the amount of time, effort, and resources needed to perform such process. The pilot ***PA*** database contributes to the guideline by the following keynotes:

> **[a]** Due to the amount of time and effort in each data collection session there is a need to automatize some processes, such as: metadata creation, data labeling and storing. This will minimize the risk of human error to occur by the controller.
>
> **[b]** Some sensors are already provided with ***PAD*** methods, which means that they can detect or refuse to capture some known ***PA***s. Therefore, a training phase is needed to get the controller acquainted with the provided equipment and materials. There is a need to (i) list the valid ***PA***s before the real data collection process starts, (ii) provide ***BPM*** for fabricating ***PAI***s and (iii) perform ***PA***s.

5.2 The guideline

The data collection phase provided keynotes to build a guideline model that can be followed as a reference framework or it can support training of controllers to creating a fingerprint ***PA*** database, or normal fingerprint databases. Furthermore, the guideline result includes classifications of the following:

- fingerprint areas of study,
- possible fingerprint metadata to collect, and
- noise samples in a fingerprint database.

As such classifications play a role in determining the purpose and the usage of any fingerprint database, all of these are discussed in the following:

5.2.1 Fingerprint study areas

Fingerprint databases are used in several areas of studies, both in industrial and academical research fields. These study areas are illustrated in Figure 16, and each of it is briefly described below:

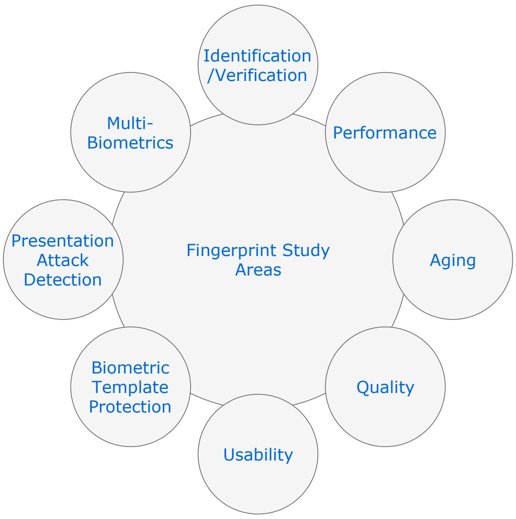

Identification /Verification
Performance
Aging
Quality
Usability
Biometric Template Protection
Presentation Attack Detection
Multi-Biometrics
Fingerprint Study Areas

Figure 16: Classification of fingerprint study areas

Identification / Verification

The processes of identification and verification are already described in Section 2.2.1. The aim of such studies is to develop identification and verification algorithms that provide a high accuracy rate and decrease the chance of getting error rates (e.g., ***FMR*** and ***FNMR***). Such algorithms are tested on fingerprint databases that contain raw captured images.

Performance

This study area focuses on optimizing the performance of the identification and verification methods. The aims are to quickly identify an individual from a huge fingerprint database, and verify if an individual claimed fingerprint matches the enrolled template in the database. Furthermore, such optimization is needed in order to process a huge amount of individuals in areas such as boarder control and airports.

Aging

New studies show that the quality of a fingerprint is effected by the age of its subject. Some publications have shown results that prove this fact, as in [63]. These results show that the fingerprint quality starts to decrease at some point of human life between the age of 40 and 50. The aging studies use fingerprint databases that provide the age of each subject as main metadata, besides the fingerprint images. Additionally, other metadata about the sensor and its resolution can play a role to future research in this field.

Quality

The focus in this area is to study the fingerprint image quality as it is considered as an important factor in a fingerprint comparison. According to [64], high quality fingerprint images are expected to increase the performance of a single identification / verification method compared to poor quality images. Due to this fact, ***NIST*** provides a software to measure the quality of fingerprint images called ***NIST*** Fingerprint Image Quality 2.0 (***NFIQ2.0***) [65]. Such quality values need to be considered as an important metadata in fingerprint databases.

Usability

Such studies focus on providing usability to the fingerprint capture devices (i.e., sensors). The aim is to provide sensors that minimize the possibility of acquiring noise samples as a result of human error (e.g., as misplacing the finger on the sensor). This includes integrating fingerprint sensors to smartphones, which are even more reliant on having good placement and less provided instructions to the users. Such studies use the raw captured images from the fingerprint databases to study the subject's behavior while presenting their fingers to the sensor.

Biometric Template Protection

This term is shortened and known as ***BTP***. It covers the protection of fingerprint templates as well as all other biometric modalities (i.e., biometric object such as finger, iris, etc), as they are considered as personal and sensitive data according to the ***GDPR*** [14]. According to ***ISO/IEC*** 24745 [66], Fingerprint template protection studies focus on providing security and privacy to the templates by offering (i) *unlinkability* (i.e., the ability of generating different templates from the same modality that do not match), (ii) *renewability* (i.e., the ability of revoking a leaked or lost template and renew the template without requiring new enrollment), and (iii) *irreversibility* (i.e., the ability of recovering a plain template and its feature are not valid unless using the secret used to protect the template) to the fingerprint templates.

Presentation Attack Detection

PAD studies focus on implementing solutions that distinguish between ***PA*** and bona fide presentation. This is based on (i) the known abilities of the real finger and its characteristics (e.g., blood flows and temperature), and (ii) and the known abilities of the ***PAI***s such as color, texture, etc. These studies require a database that contains several ***PA***s and bona fide presentations, besides providing metadata about each ***PA*** and the used materials to perform it.

Multi-Biometrics

These studies use multiple biometric characteristics put together to identify and verify a single person, which provides a higher security than using a single characteristic. Furthermore, this overcomes the limitation of a single characteristic, and makes use of more capabilities provided by other characteristics [67]. These studies use more or less the same databases as in the studies of identification/verification. An example is using iris and facial recognition as an access control.

5.2.2 Fingerprint metadata

In general, metadata provides more credibility to any study and research result. Also, it helps answering and creating new research questions for new studies. Therefore, this guideline lists all metadata possible to collect, and groups them up based on relatedness (e.g., subject, sensor, sample, etc.). Furthermore, two classifications are applied on the listed metadata as presented in Figure 17; (i) classification based on the required effort by the controller, and (ii) classification based on the strictness of the metadata. (i) is presented by boxes colored as follows:

- *Red* for high effort required: metadata requires a third party application to generate its value.
- *Orange* for medium effort required: metadata's values change according to each presentation, and are required to be provided multiple times.
- *Green* for minimum effort required: The data are static and only need to be provided once for each subject or each sensor used.

(ii) is presented as highlighted areas, which refer to personal and/or sensitive data. On the other hand, the blue boxes present metadata that face challenges to be classified (an explanation is provided later). The following describes Figure 17 more in depth:

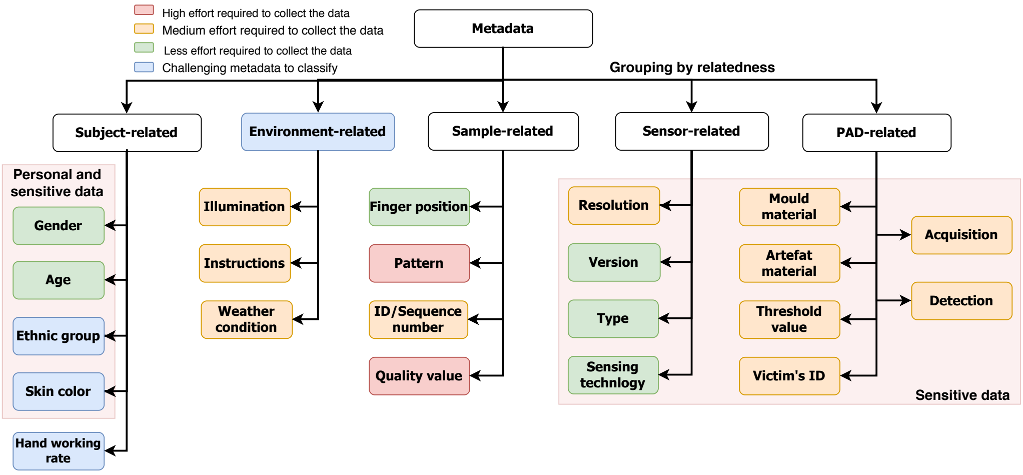


Figure 17: Classification of metadata that can be provided in fingerprint databases

The metadata are grouped into five main categories; metadata related to the subject, environment, fingerprint sample, sensor, and ***PAD***. Each are presented as follows:

Subject metadata

According to the ***GDPR***, most of these data are considered as personal and sensitive data, as it can lead to its subject. Usually, age and gender are common to be provided in previous research, as in [68]. On the other hand, there are other metadata that can be provided for future research, such as: subject's ethnic group, skin color, and hand working rate. The last one refers to the quality of the fingerprints based on the subject's work. For example, a construction site worker is expected to have poor fingerprint quality compared to an office worker. This can be solved by applying a rate between one and five, where five is poor quality and one is good quality fingerprints.

On the other hand, ethnic group and skin color are hard to classify, because the classification depends more or less on the purpose of the study. The challenge with facing these metadata are based on how detailed the classification should be. For instance, if a simple classification is provided then there is a risk of generalizing groups of people from different ethnic groups into one very large group (e.g., east- and west Asians would both be classified as Asian, however there are many differences within the group of Asians). On the other hand, classifying all these differences will result in an excessive amount of groups.

Environmental metadata

This category covers both the data collection environment and the outside environment. It is hard to classify the relevant metadata in this category, as it depends on the data collection process and purpose. For example, if data collection uses touch-less sensors that can be affected by the illumination, the illumination conditions (e.g., day light, artificial light, etc.) should be documented and provided as it can be used in future research and experimental reconstruction. Additionally, the given instructions to the subjects can be considered as metadata, where the subject behavior will be affected by the provided instructions (e.g., hard/low pressure, presenting time, and so on).

On the other hand, if a data collection process is using touch-based sensors, the acquisition process may be affected by the body temperature of the subject. Therefore, the weather condition (i.e., the temperature outside) is relevant to be reported as metadata, as subjects could have been outside before entering the experiment and currently have cold or dry fingers.

Sample metadata

Metadata related to each fingerprint sample carries out some important data as the finger position (i.e., index, middel, etc.), fingerprint pattern (early discussed in Section 4.1.3), quality value of the sample and ID/sequence number if multiple samples are provided. Not all sensors provide such information, and in most cases the controller needs to put an effort into enrolling these metadata. The ID/sequence number can be added manually by the controller after the acquisition of each image. This requires time, and in many cases it needs to be performed during the capture session and not afterwords. On the other hand, a third party software is needed to get the value of the image pattern and image quality. Most of them are open source projects such as ***NFIQ2.0*** that computes the quality of a given fingerprint sample.

Sensor metadata

Sensor information are static and can be reported once for the whole data collection process. Such information can be the sensor version, type (i.e., constant-, swipe-, or touchless sensor), applied sensing technology (e.g., multi-spectral, capacitive, etc.), and the capture resolution of the sensor. Sometimes a sensor can provide multiple images in several resolutions, this can require more effort by the controller to administer manually. Therefore, it is considered as a medium effort level.

PAD metadata

This category covers additional metadata that can be provided in ***PA*** databases. According to the knowledge gathered in the data collection phase, the following are information that are recommended in ***PA*** databases: type of (i) mould and (ii) artefact materials that refer to the used materials and their abilities. Moreover, (iii) the victim's ID can be used to compare the quality of the sample based on its original source. Some sensors detect a ***PA*** and refuse to acquire an image of it. Therefore, (iv) acquisition value (true for captured image or false refusing to capture the ***PA***) can be provided. Additionally, some sensors provide the ability to detect ***PA***s based on in-built algorithms. In such cases, a (v) threshold and (vi) detection result can be provided for further studies.

As it may be observed in Figure 17, both ***PA***s and sensor metadata are considered as sensitive data. This metadata can lead to information about succeeded ***PA***s and vulnerabilities on commercial sensors, as it can lead to more ***PA***s in real environments, where such commercial sensors are already used. This information should be handled and published carefully, in order to keep the damage at a minimum.

5.2.3 Fingerprint noise samples

A noise sample refers to a challenging fingerprint sample that requires more effort to handle than a normal sample. In many cases, noise samples can affect the result of a study, or even lead to errors while processing such samples on the software level. The data collection phase provided the following as possible noise samples that can be found in fingerprint databases: (Figure 18 shows an overview over the known noise samples)

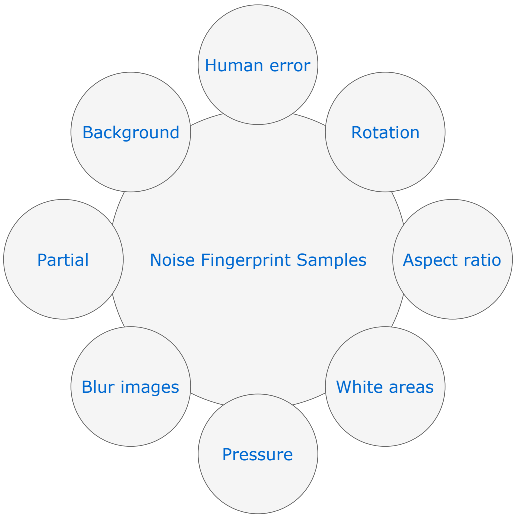


Figure 18: Classification of noise samples in fingerprint samples

Human error

Due to the fact that the data collection process is not fully automated in many cases, the controller is required to apply some manual operations. Such operations can be (i) image acquisition, (ii) sample labeling, or (iii) sample storing. These operations are vulnerable to human errors that need to be considered and mitigated. Recommendations to minimize these errors are to minimize the amount of manual operations that need to be performed by the controller. Additionally, reviewing the subject's data carefully after the acquisition of each sample and at the end of each session helps reducing such errors as well.

Rotation

This referrers to the rotation of the finger while presenting the fingerprint to the capture device. This leads to acquire a rotated fingerprint, which can be challenging to analyze by some systems that expect to have oriented samples. This can be mitigated in a controlled environment, where the controller can (i) provide instructions to prevent such situations to occur, and (ii) check the orientation of each sample after its acquisition.

Aspect ratio

Some sensors change the size of fingerprint images after the acquisition by changing the aspect ratio of the image. This can lead to a change of the ridges and valleys size. It is hard to mitigate such errors because it is applied on sensor level. However, if this was noticed, it should be documented and provided with the database.

White areas

A few sensors do not provide the ability to crop fingerprint images and remove the white border around the fingerprint pattern. This can be manually mitigated by cropping each image after each session or at the end of the data collection. Otherwise, this should be documented and provided with the database.

Pressure

Pressure is a known problem with touch-based sensors, as applying much or less pressure can affect the appearance on minutiae points. This can be mitigated in a controlled environment, where the controller can (i) provide instructions to prevent such situations to occur, and (ii) check each sample after its acquisition.

Blur images

This is a common noise in touchless-based sensors, where the captured images are blurry. The reason for this can be the distance between the capture device and the finger. Such noise can be mitigated by applying a (i) fixed distance between the camera and the finger, and (ii) provide this information as an instruction to the subjects. Moreover, the controller should (iii) check each sample after its acquisition.

Partial

This category of noise samples refers to samples that contain only a part of the fingerprint. It can happen when a subject presents a side of the finger to the sensor. The controller can mitigate such situations by (i) showing each subject the correct placement of the finger, and (ii) provide interactions that cover it. Furthermore, the controller should

(iii) check each sample after its acquisition.

Background

Another common noise in touchless-based sensors is the background of the image, since it can have a similar color as the skin, which makes it hard to distinguish between both. Nevertheless, another issue could be glare that faces the capture device, which can affect image quality of the finger and its fingerprint. This can be mitigated by applying a fixed acquisition environment that is tested by the controller in hand.

5.2.4 Guideline model

The following is a proposal for a comprehensive and complete guideline model that is recommended to be followed as a framework for the creation of fingerprint ***PA***-, as well as normal fingerprint databases. The guideline is created based on the previously collected keynotes (see Section 5.1) and the aforementioned classifications (i.e., fingerprint -study areas, -metadata, and -noise samples). Furthermore, it provides instructions of the following:

- Handling subjects during the data collection process.
- Safe storing of the collected data.
- Creating ***PAI***s and applying ***PA***s.
- Using different sensor types during the data collection (i.e., touch-, swipe-, touchless sensors).
- Publishing the database with the research community for future studies.

Figure 19 illustrates an overview of the proposed guideline. As it may be observed, the guideline model divides the fingerprint database creation process into three phases; pre-arrangement, data collection process, and post-arrangement. All of these are covered in detail below:

Pre-arrangement

This is the first stage of the database creation process, which must be applied before performing any data capturing process. The purpose of this phase is to (i) make a plan that covers the whole database creation process, which should be considered as a reference for any later phases of the project. Furthermore, (ii) a communication with the data authority needs be established to gain permission to start the data collection process. Moreover, (iii) a preparation phase is highly recommended to train the controller for the data collection process. The following provides more details:

Planning phase

This phase should provide a plan of the database creation process. The content of this plan should cover the following:

1) Data collection purpose:
This should cover (i) the objective of creating a fingerprint database, (ii) the reason for creating the new database instead of using an existing database, and (iii) the future usage of the new database.

2) Data collection process:
The content of this section should cover the details to create the database, such as (i)

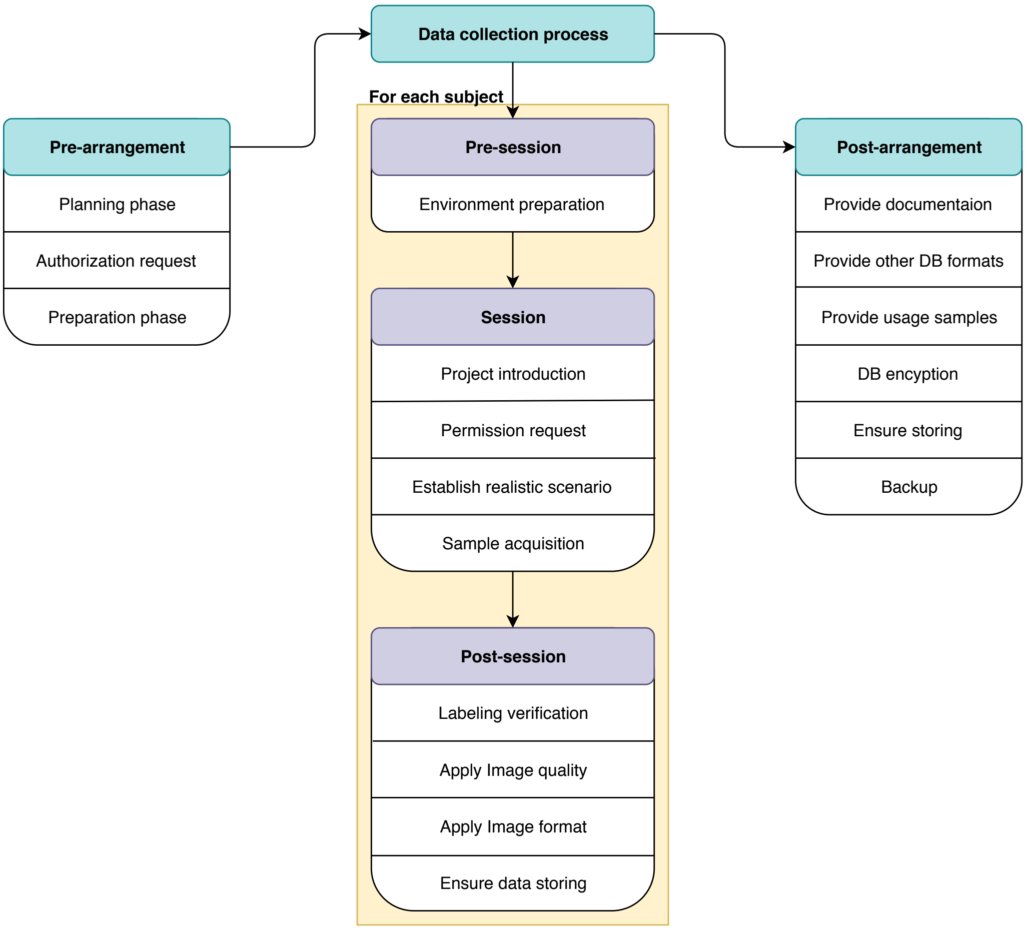


Figure 19: The guideline model

sensors, (ii) number of subjects, (iii) number of session for each subject, (iv) number of fingers from each subject, and (v) needed metadata. Additionally, the following should be considered for ***PA*** databases: (vi) number of ***PA***s, (vii) materials to fabricate ***PAI***s, and metadata related to the ***PA***s. Furthermore, this should include the strictness of the data collection process such as whether only high quality images will be acquired, or normal images in any quality as in a realistic scenario are allowed too. This depends on the purpose of the study.

3) Storing and sharing policy

The plan should include the policy for storing and sharing the collected data. Additionally, it should include the required procedures to store and share these data.

4) Roles and responsibilities

This section should provide names of the responsible individuals in the project and their roles, which includes both the project leader, controller, and other involved members. If the controller is not yet assigned, this should be updated once it is confirmed.

5) Status of the materials and equipment

This should provide a list of the equipment (i.e., sensors) and materials (in the case of ***PA***) used in the data collection, where each is attached with its status (i.e., ready to use, ordered, not available).

6) Assisting future research
This section should cover metadata beyond the current scope, which can be needed in future research. These metadata can save resources in future studies, where a new database is to be created because of missing metadata in the existing databases. This is challenging, since it is hard to define metadata that are needed for future research. Therefore, a list of metadata is previously provided in in Section 5.2.2, which can assist in making such decisions.

Authorization request

Nowadays, according to the ***GDPR***, the data authority should be contacted in order to gain permission to start the fingerprint data collection process. The Norwegian center for research data (***NSD***, [69]) is an example of such data authority in Norway.

Preparation phase

In this phase the following should be provided:

1) Establish a well-defined acquisition environment
The acquisition environment is recommended to be defined early, before starting the data collection process. This helps to establish a constant environment for all subjects and prevents any change that can further affect the samples in the database. Moreover, the chosen environment should adapt to the needs of the data collection process and the used equipment. For example illumination and the distance to an eventual touchless sensor, or dust that can affect the creation and storing of ***PAI***s.

2) Controller practicing
This phase should be used by the controller to get acquainted with the provided equipment and materials. The following are tasks to be performed by the controller during this phase:

- **Set up the sensor(s) and needed drivers for the data collection**
  The controller needs to know how to set up the sensors and use them in order to acquire fingerprint images. Some sensors require an own driver, or even a specific operating system. Therefore, the controller is recommended to spend time understanding the provided equipment.
- **Set up the needed third party software**
  Some software is recommended to have in order to gain certain metadata values as ***NFIQ2.0*** for image quality. Additionally, an image converter may be needed to apply a standard format for all images provided by several sensors.
- **Acquire fingerprint images**
  After setting up the sensors, the controller should acquire fingerprint images from each provided sensor. The following should be noticed: (i) the needed finger pressure to capture a good sample, (ii) provided image format, and (iii) additionally provided metadata (as some sensors provide ***NIST*** quality value to each sample).
- **Customized software**
  Due to the fact that the data collection process is vulnerable to human error by the controller, the controller is recommended to program a customized metadata generator (i.e., the controller add the metadata to the software and generates a file to add to the subject folder), sample counter (i.e., software to count the samples and order them based on the capture time), and/or subject folder creator (i.e., software to generate an empty folder for each subject and include all its sub folders and metadata). This can be done using Java, Python or another programming language. Furthermore, it is quickly done and saves time and effort during the data collection process.

- **Apply on test subjects**
  The controller is recommended to apply the data collection process on test subjects before carrying out the real experiment. This helps the controller getting acquainted with the process, time, and effort needed. Additionally, it helps to get an overview over the desired file structure to store the data and its metadata. Furthermore, this task provides areas of improvements before the data collection process. It is important to remove these data before starting the test data collection process.
- **Practice on fabricating PAIs**
  For ***PA*** databases, the controller should use some time to practice creating ***PAI***s using the provided materials, and gain experience creating highly accurate ***PAI***s. It is recommended that the controller takes notes of the results for future improvements while creating ***PAI***s. Such notes can be hardening time, material quality, etc.
- **Perform PAs and exclude irrelevant attacks**
  For ***PA*** databases, it is important to apply ***PA***s on the provided sensors before the real experiment, and exclude irrelevant ***PA***s. Irrelevant ***PA***s are defined as attacks that cannot be captured by the sensors, which means that the sensors include ***PAD*** methods to detect such ***PA***s.

Data collection process

As shown in Figure 19, this is the main stage in the database creation process. Nowadays, acquiring fingerprints faces a huge challenge, since subjects are more concerned with their privacy, due to the fact that fingerprints are used on a large scale (smartphones, application, and so on). The controller should not force the subject to join the data collection process. Instead, it is recommended to clarify the importance of such databases in future studies to increase the security and the privacy of fingerprint technology, which may play a role to convince the subject. Therefore, this phase may take more time than planned in order to be achieved.

The guideline recommends the following as a general note to the controller during this phase:

- Do not apply more than one subject at one time, as a high chance to perform mistakes by the controller and subjects.
- Plan to have a free time between each subject, as this time should be used to perform post-session activities by the controller. Also, the controller need to relax before starting the next session, as the focus is an important factor.
- For ***PA*** databases, create the ***PAI***s one or two days beforehand.
- Check the quality of the ***PAI***s after each session and consider if it is still valid to be used.
- Apply a daily backup, or hourly if necessary.

Furthermore, the guideline presents three phases for each session. As it may be observed, these are: pre-session (i.e., before the subject enters the session), during the session, and post-session (after the subject has left). The following presents these phases in detail:

Pre-session

Before each session starts, an environment preparation should be applied. Such preparations are considered as follows:

1) Prepare the consent form
The consent form should be printed and ready to be signed by the subject. Some subjects are expected to request a copy of their form, therefore, a scanner or printer is recommended.

2) Creation of the subject folder
The folder to store subject data should be created and labeled beforehand. This includes the main folder, all sub-folders and all metadata files that are necessary for storing data during the session.

3) Test sensors
It is recommenced to test the sensor before the subject enters the session to avoid any unexpected problems during the session. This includes cleaning the surface of the touch-based sensors.

4) Register the constant metadata
Some metadata are already known and can be registered before the session starts. These metadata can be sensor and environment related metadata, as described earlier in Section 5.2.2.

5) Register PAIs
In case of ***PA***s database, the ***PAI***s should be created and ready to be used beforehand. They should also be registered in the metadata file to save time.

Session

The session starts once the subject enters the acquisition environment. The session is split into four stages; 1) project introduction, 2) permission request, 3) establish realistic scenario, and 4) sample acquisition. These are described in the following:

1) Project introduction

In this stage, the controller is required to introduce the project to the subject. This should include the project's motivation, goals, and policy for storing, sharing, and handling the collected data.

2) Permission request

The controller is required to hand over the consent form to the subject and request the permission to enter the data collection process. Once the consent form is signed, a subject-ID should be assigned to the subject and documented by the controller. Furthermore, the controller can start acquiring other metadata from the subject, such as age, gender, and hard working rate (describer earlier in section 5.2.2).

Keep in mind, if it is planned to apply multiple sessions in the database, stage (i) and (ii) can be skipped after the first session to avoid redundancy.

3) Establish realistic scenario

In this stage, the controller tries to adapt the acquisition process as in a realistic scenario. The following are some recommendations to go by:

- **Acquire the finger in its original condition**
  The subject should not be asked to wash or clean their hands before acquiring the samples, as this would not be done in real environments.

- **Observe the usability of the sensor**
  The controller can let the subject try to acquire a *usability*-sample to observe the usability of the device without providing any instructions regarding the correct presentation of the finger. This can be useful data for new developed fingerprint sensors.

Keep in mind that this stage can be skipped if the database is planned to acquire only high quality fingerprint images, images without rotation, and so on.

4) Sample acquisition

At the beginning of this stage, the controller should provide the desired instructions to the subject, which includes information about pressure, finger placement, distance, and so on. It is highly recommended that the controller performs an acquisition once in front of the subject to show the expected correct acquisition. Then, the collection process of acquiring the subject's fingerprint images can start.

Furthermore, the controller should observe the subject while performing the acquisition and carefully insert the images to its correct location. It is important to do the following during the acquisition process:

- **Clean the surface of the touch-based sensors**
  This is recommended to be performed after each acquired sample, or once the subject changes from one acquisition finger to another.
- **Control the distance and illumination in touchless sensors**
  These two factors are important to control in order to minimize the noise samples caused by the touchless sensors.
- **Check the quality of each sample after its acquisition**
  The controller can check the captured image manually after its acquisition and determine whether it should be stored or is to be captured a new sample.
- **Acquiring more samples**
  It is highly recommended to acquire multiple samples of each finger. This helps further use of the database for identification / verification studies in the future, as well as helping to have a backup sample in case a noise sample is captured.

In case of planning multiple session per subject, the controller should plan the time for the next session with the subject before ending the session.

Post-session

Once the subject leaves the session, the controller is recommended to spend some time applying the following quality control procedures:

1) Labeling verification
Ensure the correct labeling of the subject's data, which include the naming and placement of each file.

2) Apply image quality
It is recommended to use ***NFIQ2.0*** software in this task to provide an image quality to each captured image. Then, the result (i.e., image quality value) of each image should be added to the metadata linked to the sample.

3) Apply image format
If the samples provided by several sensors are in different formats, it is recommended to convert the images into a standard image format for all sensors. Keep in mind to store the original file format.

4) Ensure data storing
Once the labeling is verified and the metadata is added, the controller should ensure the storing of the subject's data and the consent form.

Post-arrangement

This is the last stage in the database creation process. The following are recommendations for before publishing the database and using it in future studies:

1) Provide documentation
A documentation of the database should be provided and attached to the database when it is shared. Such documentation should cover the following:

- The usage policy of the database.
- Overview of the database, its structure, provided metadata, and file formats.
- The instructions provided to the subjects.

2) Provide other database formats
It is believed that ***SQL*** and ***XML*** databases are easier to use than the folder structure database, as it is easier to filter the database content based on the provided metadata using ***SQL***-statements or ***XML***-query. Therefore, it is recommended to duplicate the database and convert it to another format as ***SQL***.

3) Provide usage samples
It is recommended to attach filtering samples to the database. This can either be a few Python scripts or ***SQL***-statements, as they help understanding the structure of the database and how to use it.

4) Database encryption
Before storing the database or sharing it with other research studies, it is recommended to apply encryption to it, in case it gets lost or stolen. The decryption key of the database should be stored safely.

5) Ensure storing
The project leader is responsible to ensure the safe storing of the database.

6) Backup
It is very important to provide backups of the database, as it may get lost or the hardware could crash, where the data can risk of being lost.

It is important to keep track of the shared database after publishing it with the research community. If a subject requests to delete his/her data, this action should be performed both on the local and shared databases. The institution is required to communicate with all partners that have a copy of the database and give an order to remove the subject with a specific ***ID***.

6 Pilot Presentation Attack Database

This chapter presents the pilot ***PA*** database in this project. This includes the creation process of the pilot database and its final result. Furthermore, the following questions will be answered in this chapter: (1) What is the final result of the pilot ***PA*** database? (2) How is the data collection process performed? (3) What are the collected metadata? (4) How is the database structured?

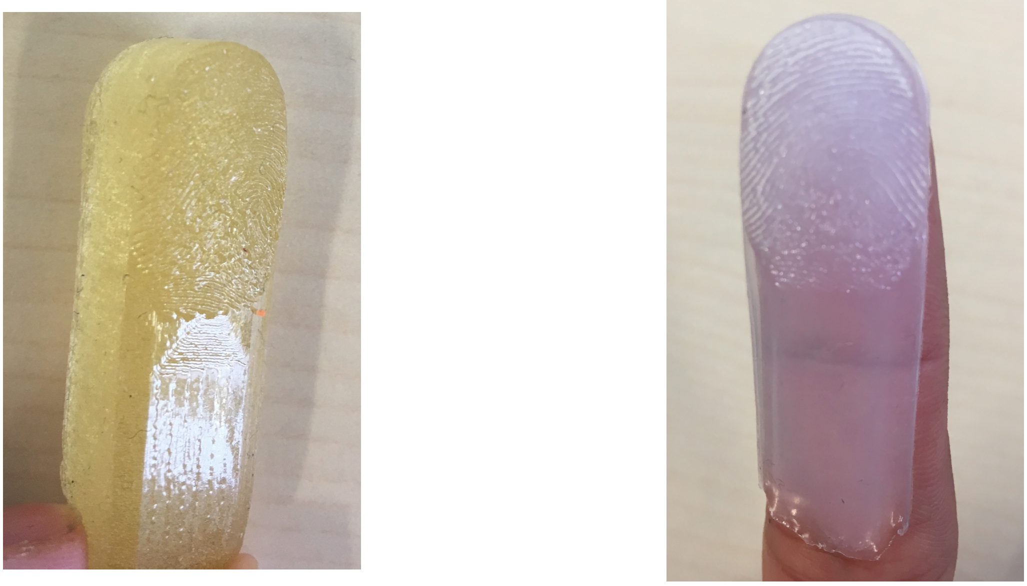
The reader is referred to Appendix F, which presents more additional figures regarding the database creation process.

6.1 Database creation process

This section presents the creation process of the pilot ***PA*** database in this project. Furthermore, the section is divided into two sub-sections, as follows:

6.1.1 ***PAI*s fabrication process**

To create a fingerprint ***PA*** database, two types of ***PA***s are performed in this project using fake finger- and overlays ***PAI***s. These are illustrated in Figure 20. As it may be observed, the fake finger illustrates a human finger. It is thick and has the same dimension as a normal finger. On the the other hand, the overlay is a thin layer that carries out the fingerprint, and requires the imposter to use his/her finger on the top of the overlay during the ***PA***. It is worth mentioning that overlay ***PAI***s are often used in sensors that capture the finger vein besides the fingerprint.

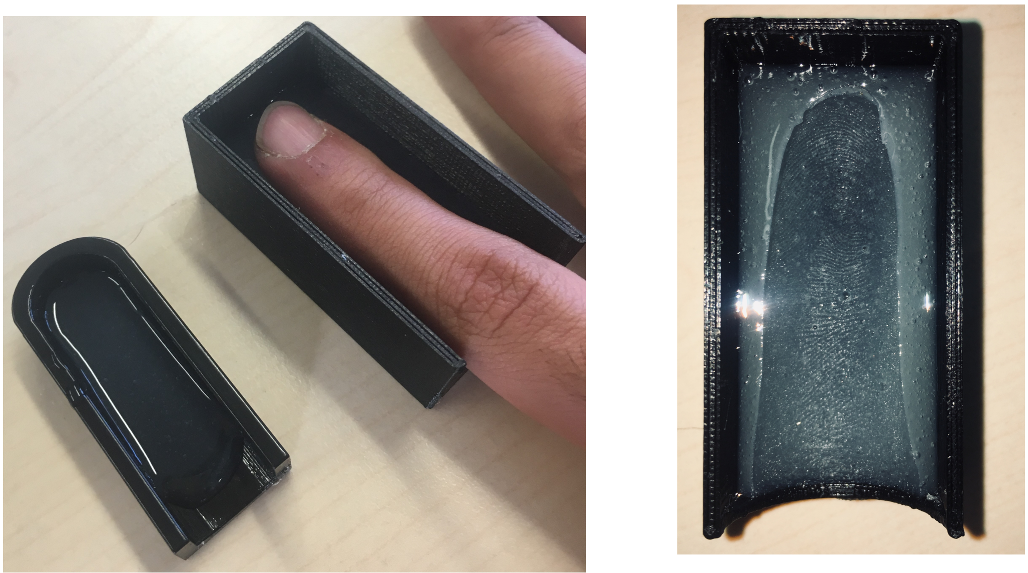


(a) Gelatine fake finger

(b) Silicone overlay

Figure 20: ***PA***s types: (a) gelatine fake finger ***PAI*** and (b) silicone overlay ***PAI***

The ***PA***s in this database are created from a ***3D*** printed mould, which contains a fingerprint from an open source database. Additionally, silicone moulds that carry out fingerprints from bona fide fingers are created and further used to create artefacts. For the silicone mould, a ***3D*** printed finger-form is used to hold the silicone while presenting the finger. Both moulds are shown in Figure 21a.



(a) ***3D*** mould and ***3D*** finger-form

(b) Silicone mould in a ***3D*** finger-form

Figure 21: The creation of silicone overlay and mould using ***3D*** mould and finger-form

6.1.2 Data collection process

During the data collection, the subjects are asked to present six bona fide presentations and four ***PA***s. The index, middle, and ring fingers of both right and left hands are captured for each subject. Furthermore, they are also named based on their position, as shown in Figure 22. The name consists of two letters, the first one is presenting the hand side (i.e., 'L' for left and 'R' for right), and the second letter presents the finger position (i.e., 'I' for index, 'M' for middle, and 'R' for ring).

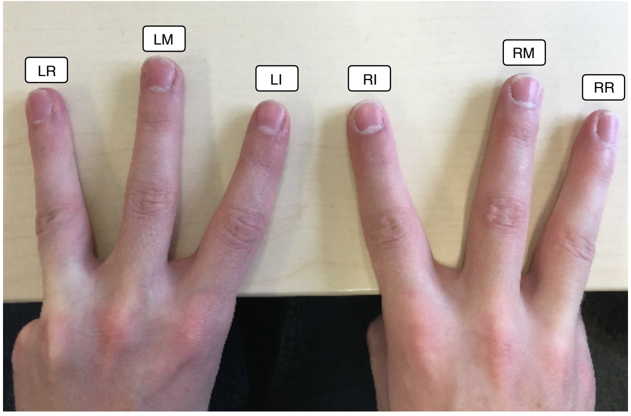


Figure 22: Bona fide fingers acquired in the pilot database

The pilot ***PA*** database in this project is created using two different sensors; Crossmatch Guardian 200-Rev 1 and Lumidigm v203. These sensors are shown in Figure 32 in Appendix F. As it may be observed, the Crossmatch sensor allows to capture multiple fingers in one acquisition. However, this feature is not used during the creation of the pilot database, and a single finger is captured in each acquisition. The main reason for this is the difficulty faced to crop the fingerprint images in order to only contain a single fingerprint in each image. This leads to generate big size image that contains the fingerprint formation in its original size and white areas around it. Moreover, the Crossmatch sensor allows to capture images of the whole finger. On the other hand, the Lumidigm v203 sensor is designed to capture a single fingerprint in each acquisition. Additionally, it is designed to capture the upper part of the finger, which also decreases the chance of capturing a partial image.

Furthermore, each of the sensors comes with a ***SDK*** that can be used to capture the fingerprint image and store it. Figures 34 and 35 in Appendix F present screenshots during the data capture process. As it may be observed, the Lumidigm ***SDK*** provides a ***NIST*** quality value, spoof score, and spoof decision in addition to the fingerprint image. These data are considered as metadata to be collected in the database. The ***NIST*** value gives a score between one to five, where one is considered to be a good quality and five is considered as a bad quality.

Bona fide presentations

The data collection process for each subject starts by applying all bona fide presentations on the Crossmatch sensor, then repeats the same actions on the Lumidigm sensor. Moreover, the surface of both sensors are cleaned after each presentation. Figure 33 in Appendix F shows a bona fide presentation on both Crossmatch and Lumidigm. Additionally, three samples of each fingerprint are further acquired in the database.

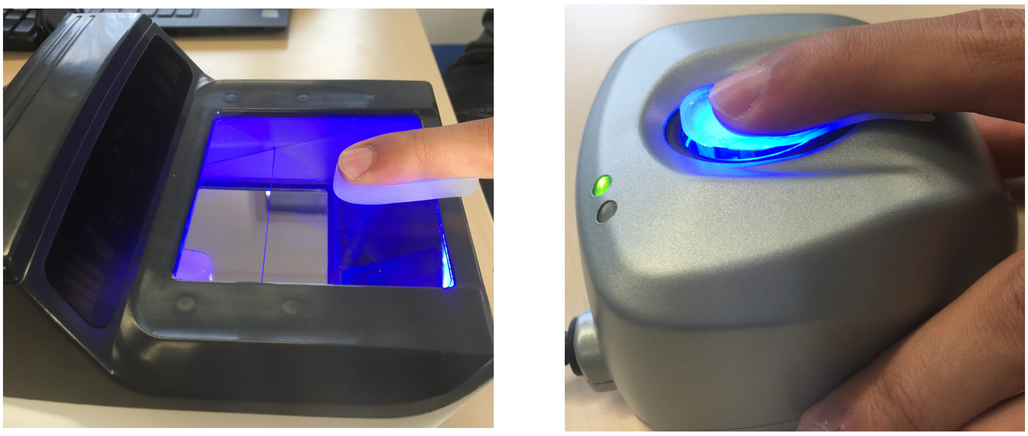
PA presentations

Four different ***PA***s are performed by each subject after bona fide presentations. These include different fake fingers- and overlays ***PA***s. Moreover, these ***PA***s are applied using either the left or right index of the subject, as shown in Figure 23. Additionally, three samples of each ***PA***s are aquired as in bona fide presentations.

Due to the fact that the provided sensors have inbuilt ***PAD*** methods, some ***PA***s are refused to be acquired by the Lumidigm sensor. Therefore, only the black-, white-, and sherbet playdoh fake fingers are captured, and not other colors as orange, red, green, etc., as these colors are easier to distinguish from normal skin color than white, black, and sherbet.

In case of ***PA***s, the spoof score provided by Lumidigm sensor has often a very high value. Therefore, there is an assumption regarding the creation of such high value by multiplying several values such as pressure, reflection, fingerprint size and maybe others unknown factors. An example of such spoof score value is shown in Figure 24. It shows the high spoof score by presenting a dragon-skin overlay ***PAI***.

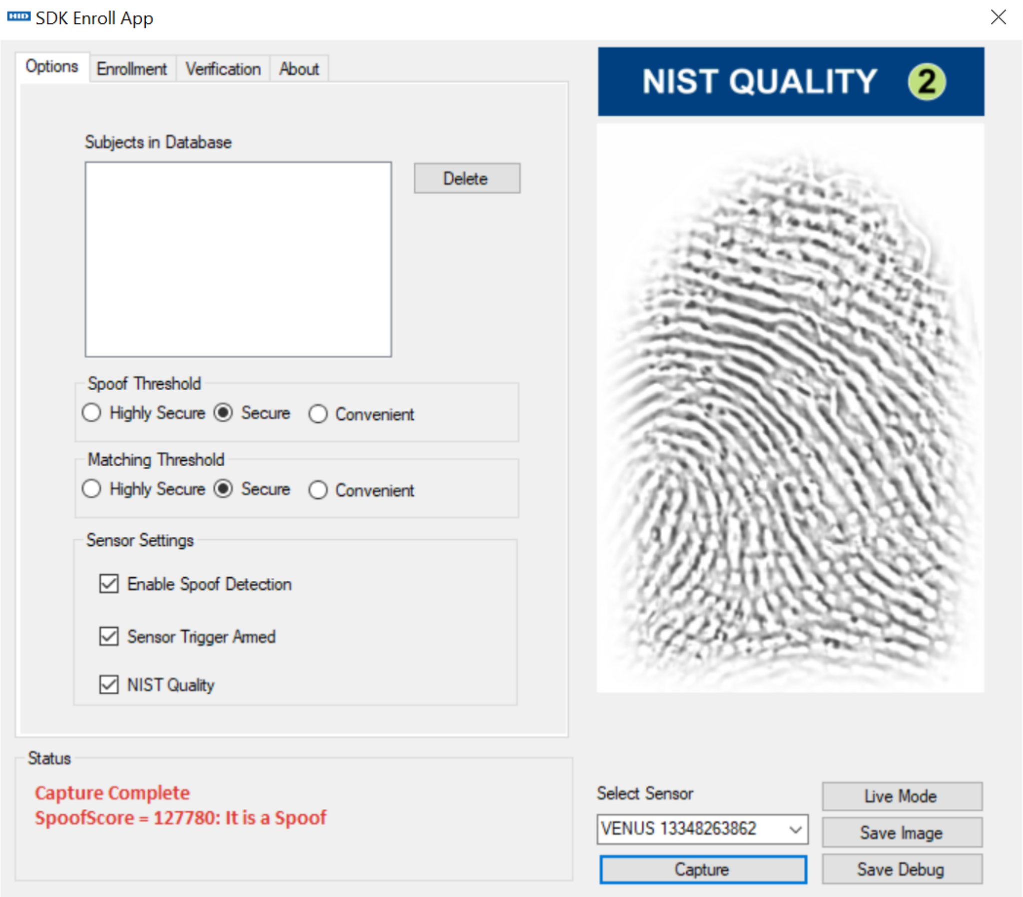
Moreover, it have been observed that the Lumidigm sensor provide a higher spoof score value on overlays attacks than fake fingers attack in general. This can be caused because of the difference in the applied pressure on both ***PA***s.



(a) Dragon-skin fake finger ***PA*** performed on Crossmatch sensor

(b) Silicone overlay ***PA*** performed on Lumidigm sensor

Figure 23: ***PA***s applied on Crossmatch and Lumidigm sensors



SDK Enroll App

NIST QUALITY 2

Subjects in Database

Spoof Threshold

○ Highly Secure ● Secure ○ Convenient

Matching Threshold

○ Highly Secure ● Secure ○ Convenient

Sensor Settings

☑ Enable Spoof Detection

☑ Sensor Trigger Armed

☑ NIST Quality

Status

Capture Complete
SpoofScore = 127780: It is a Spoof

Select Sensor

VENUS 13348263862

Figure 24: A spoof presentation is detected by the Lumidigm sensor

6.2 Database final result

The pilot fingerprint ***PA*** database in this project is created over a period of two weeks. It consists of ten subjects that present in total 60 bona fide fingers (index, middle, and ring fingers in both hands) and 40 ***PA***s (fake fingers and overlays). Moreover, three samples of each bona fide presentation and ***PA*** are captured. This leads to 360 bona fide samples (i.e., 180 samples of each sensor) and 216 ***PA***s samples (i.e., 120 samples captured by Crossmatch and 96 captured by Lumidigm). Figure 25 shows the different fingerprints from the created database.

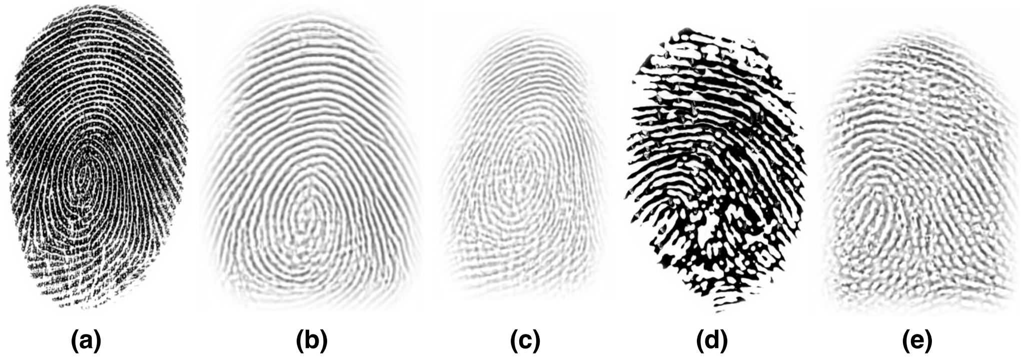


Figure 25: (a) bona fide fingerprint captured by Crossmatch, (b) bona fide fingerprint captured by Lumidigm, (c) bona fide fingerprint detected as ***PA***, (d) ***PA*** fingerprint captured by Crossmatch, (e) ***PA*** fingerprint captured by Lumidigm

Several materials such as playdoh (normal- and silly putty playdoh), silicone, gelatine, dragon-skin, and latex are used to create the different ***PAI***s to perform the ***PA***s in this database. Figure 26 shows the collection of some ***PAI***s after the data collection phase.

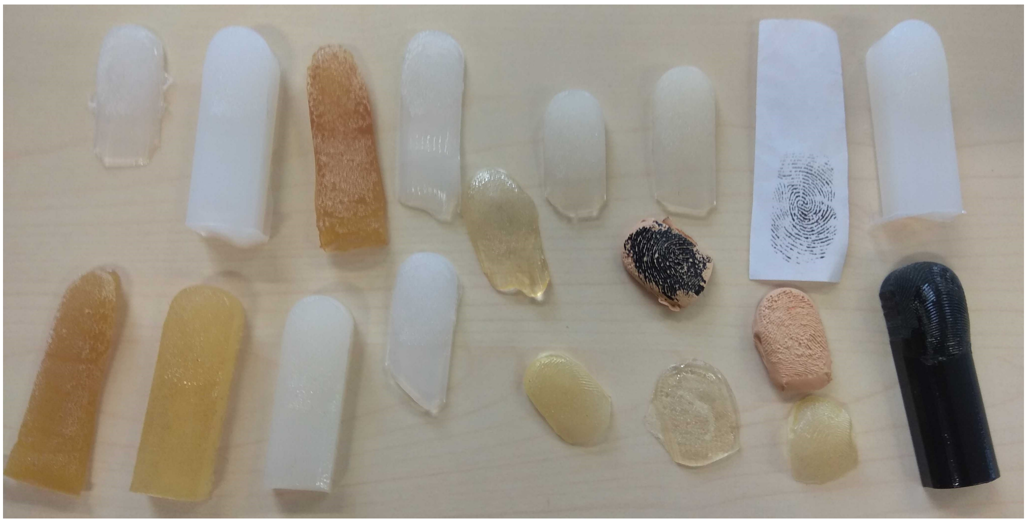


Figure 26: Some of the ***PAI*** collection after the data collection process

6.2.1 Database structure and collected metadata

The database in this project is folder structured, and due to the time constraints near to the deadline, no other database format is created. Furthermore, some metadata are prioritized to be collected than others, keeping in mind that this is a pilot ***PA*** database, and other metadata are planned to be collected on the future database. Both the data structure and collected metadata are illustrated in Figure 27.

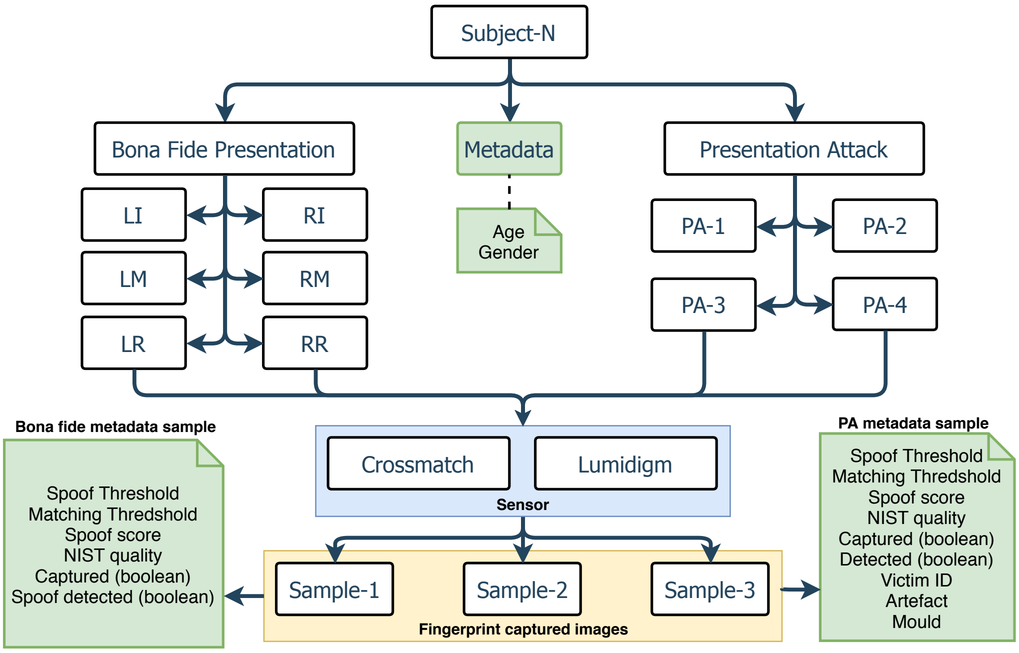


Figure 27: Data structure and collected metadata in the database

Each subject is presented as in a main folder named with the subject's id. This folder contains two sub folders; a Bona fide Presentation (BF) and a Presentation attack (PA) folder. Additionally, a text file contains the subject's age and gender as metadata.

Furthermore, the BF folder has six sub folders, where each presents the finger side and position (as described earlier in Section 6.1.2). On the other side, the PA folder contains four sub folders that present each performed ***PA*** by the subject. Moreover, all these folders have a two folders each that present Crossmatch- and Lumidigm samples, where each contains three samples of either bona fide presentations or ***PA***s in addition to a text file that presents the sample metadata.

Metadata attached to each bona fide sample captured by Lumidigm contain (i) Spoof Threshold, (ii) Matching Threshold, (iii) Spoof score, (iv) ***NIST*** quality value, (v) Captured ['true' if the sensor acquires the sample, and 'false' if no acquisition is performed], and (vi) Spoof detected ['true' if the sensor detects the bona fide presentation as a ***PA***, and 'false' if no spoof detection is given by the tool]. All these values can be found in Figure 24. Since Crossmatch does not have any ***PAD*** methods, only (v) is attached to the samples captured by the Crossmatch.

On the other side, the same metadata are collected for each ***PA*** sample excluding (vi). In addition to the aforementioned, the Victim ***ID***, artefact material name, and mould material name are collected.

7 Presentation Attacks Evaluation

This chapter represents the attack potential of ***PAI***s as presented in the ***ISO*** standard 19989-1:2018 ([10]). Moreover, this will be adapted to the created ***PAI***s in this project. This chapter answers the following questions: (1) What are the ***PA***s evaluating factors? (2) What is evaluation result of the ***PA***s performed in this project? (3) How can the evaluation result be used in future?

For more information than provided in this chapter about the ***PA***s evaluation, the reader is referred to [10].

7.1 ISO 19989 CD PA evaluation

The ***ISO*** committee draft 19989-1 defines an evaluation framework to assess an attack potential value for different ***PA***s. Furthermore, this framework defines two stages to evaluate the ***PA***s; (i) identification- and (ii) exploitation of attacks. Moreover, it evaluates the ***PA***s based on different factors that adapt to both stages. These stages and factors are presented in the following:

7.1.1 Evaluation stages

[10] presents two stages of ***PA*** evaluation. These are:

Identification of attacks

This stage presents a phase to train on fabricating ***PAI***, and discover if it is a useful attack that can successfully be applied on an instance of the target of evaluation (***TOE***, i.e., sensor). It can be running in a simple environment or even in a laboratory. In this stage, the output is a script that provides a step-by-step description of how to create and perform the attack in the exploitation phase. Keep in mind, it is not required to have the capture device in this stage. However, having a sensor increases the chance of a successful attack by demonstrating the attack and see the results before hand.

In the context of this project, this stage refers to the preparation phase before creating any ***PA*** database, where the controller spends time on fabricating ***PAI***s. This is considered as a training phase to gain experience that can be used further in the exploitation stage.

Exploitation of attacks

This stage corresponds to applying the script from the previous stage and perform the attack on an instance of the ***TOE*** in its exploitation environment. This stage covers the time frame from fabricating the desired ***PAI***, through performing the ***PA***, and finally, launching the attack.

In the context of this project, this phase refers to the session phase during the data collection process (presented earlier in Section 5.2.4). In this stage, the controller creates the ***PAI*** beforehand, and asks the subject to apply the ***PA*** on the sensor in order to do the exploitation and discover vulnerabilities.

7.1.2 Evaluation factors

There are six different factors to calculate the attack potential value of any ***PA***. [10] assesses different values to each factor based on the stage (i.e., identification or exploitation) of the attack. This is shown in Appendix G, Section G.1. Furthermore, these factors are presented as follows:

Elapse time

This factor presents the time required to create the ***PAI***s and apply the attack on the instance of ***TOE***. Additionally, this includes the time to set up or build any needed hardware or software equipment that assists to perform a successful ***PA***. As shown in Section G.1, the elapsed time can take (i) up to one day, (ii) up to one week, (iii) up to two weeks, (iv) up to one month, or (v) more than a month. The attack potential value of each is provided in Appendix G.

Expertise

The experience of the attacker is an important factor to consider for each ***PA***. The experience in this context refers to general knowledge about the materials, biometric characteristics, and the sensing technologies (i.e., not specific to the target system) required to be known by the attacker. [10] defines four levels of experience as follows:

- **Layman**: any person with regular level of education is capable to perform the attack.
- **Proficient**: any person with advanced knowledge in specific topics such as biometrics. Attackers that gain knowledge from online sources are considered in this level.
- **Expert**: Any person with advanced knowledge in several fields such as pattern recognition, computer vision, etc. Attacks that find new unpublished ways to fabricate the ***PAI***s are considered in this level.
- **Multiple experts**: this level considers attacks where several experts collaborate to carry out the attack.

The attack potential values of each of the aforementioned levels are provided in Appendix G, Section G.1.

Knowledge of target of evaluation

This factor refers to the amount of knowledge required to know about the target such as sensor implementation, data processing, image formats, etc. [10] categorizes this knowledge as follows:

- **Public information**: information that can easily be obtained from the internet, news, etc.
- **Restricted information**: information that is shared only "between" the developers and organizations that use the sensors.
- **Confidential information**: information that is only available internally in the organization and not shared with customers or others.
- **Critical information**: information that is known by certain people or groups within the organization.

The attack potential values of each of the aforementioned categories are provided in Section G.1 in Appendix G.

Window of Opportunity (access to TOE)

This factor refers to the difficulty level of access to the target and apply the ***PA***. [10] defines three difficulty levels: (i) easy, (ii) moderate, and (iii) difficult. The attack potential values for each of the aforementioned levels are provided in Section G.1.

Window of Opportunity (access to biometric characteristics)

This factor refers to the acquired biometric characteristic on the ***PAI*** used during the ***PA***. Moreover, it includes the quality of the fabricated biometric characteristic. [10] defines four levels in this factor: (i) immediate, (ii) easy, (iii) moderate, and (iv) difficult. The attack potential values for each of the aforementioned levels are provided in Section G.1.

Equipment

This factor refers to the used equipment to create the ***PAI*** and perform the ***PA***. [10] categorizes this factor into three categories as follows:

- **Standard equipment:** all materials and equipment that are easy to obtain.
- **Specialized equipment:** materials and equipment that are expensive to gain, not available in the standard market, and which require a specific formation to be used. An example of such equipment can be an advanced ***3D*** printer.
- **Bespoke equipment:** Very expensive equipment and materials with difficulty to access. An example for such material can be dental materials that can be used to create the mould.

The attack potential values of the aforementioned categories are given in Section G.1.

7.1.3 Vulnerabilities rating

[10] calculates values from each of the previous defined evaluation factors (in Section 7.1.2) by summarizing all the values together in order to generate a total value. Furthermore, the total value can be used to rate and categorize each ***PA***. This is shown in Appendix G, Section G.2. Moreover, Table 6 shows the relation between the total value of a *PA* and its rating.

Total value	*PA* rating
< 10	Basic
10-19	Enhanced-Basic
20-29	Moderate
30-39	High
=>40	Beyond-High

Table 6: The relation between ***PA***’s total value and its rating

7.2 Presentation attacks evaluation

This section presents an evaluation of the ***PA***s that are performed during the project. The evaluation is based on the earlier mentioned evaluation factors in Section 7.1 by [10]. As mentioned earlier in Section 6.1.1, two types of ***PA***s are used; fake finger- and overlay

PAs. Furthermore, these ***PA***s are created using several materials such as silicone, playdoh, dragon-skin, glue, latex, and gelatine. Table 7 shows the evaluation of ***PA***s performed in this project, and the following gives a description of it:

Factor	**Value**					
	Silicone	PLaydoh	Dragon-skin	Glue	Latex	Gelatine
Elapsed Time	One day	One day	One day	One week	One Week	One day
Expertise	Proficient	Proficient	Proficient	Proficient	Proficient	Proficient
Knowledge of TOE	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted
Window of Opportunity (Access to TOE)	Easy	Easy	Easy	Easy	Easy	Easy
Window of Opportunity (Access to Biometric characteristics)	Easy / Moderate	Moderate	Easy / Moderate	Easy / Moderate	Easy / Moderate	Easy / Moderate
Equipment	Standard / Specialized	Specialized	Standard / Specialized	Standard / Specialized	Standard / Specialized	Standard / Specialized

Table 7: Evaluation of ***PA***s performed in this project based on [10]

As it may be observed by Table 7, ***PA***s are categorized based on the used materials. This covers the usage of each material as a mould or an artefact, and the type of artefact whether it is a fake finger or an overlay.

In general, most of the ***PA***s can be performed in less than one day. Therefore, the materials such as silicone, playdoh, dragon-skin, gelatine, and hot glue have an elapsed time value of one day. On the other hand, materials such as wood glue, school glue and latex require a hardening time between two to three days.

The value of expertise, knowledge of ***TOE***, and Window of opportunity (Access to ***TOE***) are set to the same for all ***PA***s. The reasons for this can be summarized as follows:

- For expertise factor, the value refers to attackers with a basic knowledge about fingerprints and their pattern (the structure of the ridges and valleys on the ***PAI***s).
- For knowledge of ***TOE*** factor, restricted knowledge is more accurate than public, because the task performer has experience to interact with the sensors and how they work. However, this experience is limited and does not covers the tiny details.
- For window of opportunity (access to ***TOE***) factor, the value is set to easy, due to the fact that the sensors are fully available for the task performed to apply ***PA***s on it without applying any effort.

The factor of window of opportunity (access to biometric characteristics) is set either to easy or moderate for most of the applied ***PA***s. The value 'Easy' refers to overlays ***PA***s, and 'Moderate' refers to fake fingers ***PA***s. The main reason for this is that fake fingers carry out more details from the fingerprint, as the finger size and dimension. It is worth to mention that playdoh overlays are hard to create due to the softness ability of the playdoh material.

Finally, the equipment factor is set either to standard or specialized for most of the ***PA***s. The 'Specialized' value refers to ***PA***s that use a ***3D*** printed mould, which is expensive and hard to acquire due to the fact that it needs an expensive ***3D*** printer that prints the details of the fingerprint pattern in its original size. On the other hand, in cases of handmade moulds, most of the used materials are fully available on the market, therefore, it is set to 'Standard'. The playdoh ***PA***s only require a ***3D*** mould to gain most of the fingerprint details.

Furthermore, the rating for these ***PA***s can be calculated based on attack potential values (see Appendix G, Section G.1), and the attached values in Table 7. This will not be provided further as a result in this chapter, due to the amount of performed ***PA***s in this project.

7.2.1 Materials evaluation

In this section, the evaluation of the used materials in this project is based on the gained experience while fabricating the different ***PAI***s and apply the different ***PA***s. The following are evaluation keynotes:

1) Mould creation
Silicone, dragon-skin and mouldable-glue are considered as good materials to create moulds during the ***PAI*** fabrication phase. Specially, fast-hardening silicone and dragon skin as they get hard in a short time allowing the subject to apply less movement while presenting the finger.

2) Artefact creation
All materials can be used to create the artefacts. However, some materials such as normal playdoh and Silly 'Putty playdoh' suffer form acquiring the fingerprint details from the silicone, dragon-skin, and mouldable-glue mould. This is solved by using a ***3D*** printed mould.

3) *PAI* flexibility
Materials such as silicone, dragon-skin, latex, playdoh, and gelatine are flexible, and allow the imposter to apply pressure to it in order to acquire the full fingerprint pattern (on a touch-based sensor). On the other hand, materials such as glue and food gelatine are not flexible and cause a partial fingerprint acquisition during the capturing by a touch-based sensor.

4) Realistic *PAI*
Latex is the best material to provide a ***PAI*** with many similar abilities to a real finger, such as the softness, color similar to skin color, and flexibility.

5) Applying *PA*s
Playdoh ***PAI***s leave some dirt similar to the latent on the surface of any touch-based sensor. This should be cleaned before presenting the next presentation as it can affect the next captured image.

7.3 PAs evaluation future usage

The evaluation of ***PA***s in Section 7.2 and the evaluation of the materials in Section 7.2.1 help to prioritize the ***PA***s when creating a ***PAD*** method. This means ***PA***s with higher rate are required to be detected more often than attacks with less rate. Additionally, these evaluations help to understand the process of the ***PAI***s creation and the required effort by imposters to apply the different ***PA***s.

Furthermore, [10] presents the factors involved in a ***PA***, which can help to find areas of improvements when evaluating the different attacks. This makes it easier to determine whether a ***PA*** is valid on one or a group of sensors. Also, if a sensor is vulnerable to many ***PA***s or some attacks.

8 Discussion

This chapter presents the discussion points regarding the decisions taken by the task performer during the project period, which includes decisions more related to both the achieved result and the performed process.

8.1 Process discussion points

In this section, there are three discussion points to discuss related to the performed process in this project. Section 8.1.1 presents the delay of ***BATL*** sensor, which led to modify the project in October. Furthermore, Section 8.1.2 discusses the preparation phase of this project, which include its need and the knowledge gain as a result out of it. The final discussion point related to the guideline data collection methodology is discussed in Section 8.1.3. discussed in the following:

8.1.1 BATL sensor delay

In order to get the best out of this section, the reader is referred to read Appendix B in advance. There it is discussed how the student modified the original topic and the considered aspects regarding that. This section discusses the case of the delayed ***BATL*** sensor, the student progress while waiting for the sensor, the time needed by the student to take action regarding the case, and finally things that could have been performed better.

Several partners are involved in building and delivering the ***BATL*** sensor. This led to miscommunication between the partners. The sensor was planned to be ready before this project started, but it could not because of missing parts. Then, the partners communicated that it would be ready during August, which was not the case because of technical issues while building it. At this period of time, the student has made a progress in being practicing on fabricating ***PAI***s and writing the theoretical part of the thesis. In the student consideration, and by involving his employer and supervisor, this is convincing to wait until October to get the sensor and start the experiment which is considered as the main and only thing remaining in order to complete the project.

In October, the sensor was not yet ready and the student had to take action to determine the future of the project, taking into consideration both the unknown dates for handing in the report and the ***BATL*** sensor delivery. The performed action was a midterm review of the project (see Appendix B), which led to three meetings performed by the student and his supervisor, employer and the administrative in ***NTNU*** discussing the possibilities in order to complete the project. During this review, the student had to chose between modifying the topic and handing in his thesis on time, or accepting the delay of the ***BATL*** sensor and delaying the whole project.

The student chose to modify the scope of the project and deliver on time. This is considered by the student as the best option since it includes having the possibilities to:

- perform the original scope later as a part of other courses or private project,

- gain more knowledge about a new related topic, and
- handing in the bachelor thesis and graduate.

The student believes that the midterm review of the project status could have been performed in an earlier period of time. Also, the belief that the ***BATL*** sensor would be ready by October played a role in accepting the waiting time for it to complete working on the original scope.

8.1.2 Preparation phase

At the beginning of the project, there was a need to have a preparation phase before starting the main experiment (i.e., fabricating ***PAI***s, collecting data, and applying ***PAD*** methods on the created database). This was suggested by the employer in order to give the task performance the necessary knowledge to carry out the main experiment efficiently keeping in mind that the task performer is new to this field and that this gives him the opportunity to discover the areas of improvements before the main experiment. The goals of the preparation phase are summarized and presented in the following:

The task performer should use this phase to get acquainted with:

The literature

As described in the project plan (Appendix A in Section A.6.1), the thesis report was planned to be written in parallel during the execution of the project tasks. Therefore, the task performer used this period of the project to obtain the needed knowledge and write the literature part of the project. This knowledge was acquired by reading published papers, books and thesis that present previous work in the field of Biometrics and fingerprint. Most of these resources are listed in the Bibliography section.

Performing this literature review helped the task performer to get better understanding of the topic of fingerprint, its ***PA***s and ***PAD***-methods. Additionally, it helped to get an overview over some existing ***PA*** databases and their creation process, which furthermore, gives a background to create the ***PA*** database as it is the main result of this project. On the other hand, this makes it possible to take an early decision on the structure of the report and start writing its content early during the project.

Fabrication of PAIs using the provided materials

The ***PA***s need to be of high quality in order to increase the probability of a successful attack. This means that ***PAI***s need to be carefully created such that the transfer of the details from the original fingerprint to the ***PAI*** are as high as possible.

The task performer used the preparation phase to practice on creating the ***PAI***s and improve their qualities. This also helps to gain the knowledge about each ***PA***, such as the creation time, the difficulty of creation, and the skills needed by the attacker to create and perform such attacks.

Provided legacy sensors

As mentioned earlier in Section 1.6.2, two different sensors are used during the data collection phase; Crossmatch Guardian 200-Rev 1 and Lumidigm v203. Both are new versions and commercially available on the market. During the preparation phase, the task performer needed to set up the **SDK** [1] of both sensors in order to start capturing

[1] Software Development Kit

fingerprint images. Furthermore, several ***PA***s are performed on these sensors to check the quality of the ***PAI***s and understand the structure and format of the captured data by each sensor. This helped the task performer to prepare for the real data collection phase (later during the experiment). Additionally, it helped to have an expectation of what kind of data will be captured and stored in the database. By knowing these information, it saves time and effort during the real experiment.

Matlab environment and the provided PAD methods

The employer provided ***PAD*** software to run on the database once it is created. Also, a test database was provided, so the task performer could run the software and get results, as the same action will be performed on the new created database. The software is written using Matlab environment, which is an unfamiliar knowledge to the task performer. Therefore, the preparation phase provided the time and materials to the task performer to get acquainted with Matlab environment, the software and the format of the result that the software produce.

8.1.3 Guideline data collection methodology

As mentioned earlier in Section 5.1.2, online survey and interview sessions are the two methods discussed to be used in order to collect data that can contribute to the created guideline. Due to the time constrains, only one of these methods had to be chosen, and the interview sessions method was chosen in the end. The main reasons for choosing this decision are summarized in the following:

- Interview sessions provide two way communication, which allow the task performed to ask further questions, discuss the received answers, and ask for details if needed.
- There is a high chance to receive less answers, or misunderstood answers on online surveys, as there is a high chance for not taking it seriously.
- The data collection time frame is short, and online surveys can take longer time to be collected.

The result presented in Chapter 5 shows that interview sessions was a successful method to be used. It helped to generate a guideline-draft after each interview session and discuss the changes on each draft in the upcoming interview session.

8.2 Result discussion points

This section presents three topics related to the final result in this project. Section 8.2.1 discusses the motivation, challenges and limitations to the proposed guideline. In Section 8.2.2, the result is discussed based on the early defined research questions in this project (see Section 1.6.2). Finally, a discussion is given in Section 8.2.3 regarding the task performer contribution in this project.

8.2.1 Guideline discussion

To the best of our knowledge, there are no existing standards and/or guideline that provide a detailed framework to support the creation process of a fingerprint database or a ***PA*** database. This gives the motivation to propose a fingerprint database creation guideline, which also covers the creation of normal fingerprint database as well.

Furthermore, this is challenging because the creation process of each database is different, and mostly it depends on the usage purpose and the type of sensors used. Due to this fact, it is challenging to propose a general guideline that can be used for several purposes (i.e., studies), and adapts to all types of sensors (e.g., touch-based and touchless sensors). Additionally, the new data protection regulation in Europe (***GDPR***) introduces a new challenge to consider during the creation process of any fingerprint database. Due to all aforementioned challenges, this project introduces a guideline proposal for fingerprint ***PA*** database creation that consider the previously mentioned challenges.

The proposed guideline recommends everyone who is creating a fingerprint database to consider future research and studies, by providing extra metadata than neeeded in any new created database. As according to the knowledge gained by interviewing experts in this field, most of the databases nowadays are created because of the missing metadata in the existing databases. This can be considered as limitation, as not many people agree on spending extra time and effort on providing additional metadata for other studies. However, there is a believe that such recommendation can help in saving time and effort for future research.

Moreover, the proposed guideline should never be considered as neither perfectly complete nor constant. The guideline should be used in future creation of fingerprint databases in order to discover areas of improvements, which can be used as an update to the guideline and add further credibility to it. Additionally, the guideline is used during the project to create a pilot ***PA*** database. By doing so, some areas of improvements are discovered and later covered in the guideline. Therefore, there is a need to apply the guideline in some future databases in order to get feedback to improve it.

8.2.2 Answering the research questions

Two research questions are presented earlier in Section 8.2.2. These questions and their answers are presented in the following:

> **How can the fingerprint data in a *PA* database affect further researches in the field of *PA* and *PAD*?**

Data in a fingerprint ***PA*** database are either images of bona fide presentations and ***PA***s, or metadata related to the subject and each sample. Several studies have shown that these data play an important role in studies related to ***PA*** and ***PAD***. The results in this project also confirms the importance of the stored data in such databases. As mentioned in Section 5.2.3, fingerprint ***PA*** databases are vulnerable to have the same noise samples as normal databases. These noise samples can affect any study related to fingerprint ***PA*** or ***PAD***. Therefore, the number of such noise samples should be minimized in ***PA*** databases.

Moreover, the metadata presented earlier in Section 5.2.2 add more credibility to any research in the field of ***PA*** and ***PAD***. In ***PA*** and ***PAD*** studies, there is a need to detect ***PA***s before applying the comparison process. To do so, the name of the materials used to create the ***PAI***s are highly recommended to be provided attached to each ***PA*** sample.

Fingerprint ***PA*** databases should contain as many samples as possible (divided equally between bona fide and ***PA***s. These samples need to be acquired using several commercial sensors and smartphones devices as they are widely used nowadays. Additionally, vulnerabilities in these sensors should be published carefully, and consider that it can affect enterprises and civilians that use these sensors daily.

> **Is there a correlation between the difficulty in creating the *PAI* and the vulnerability of the sensor to it?**

The pilot fingerprint ***PA*** database in this project (see Chapter 6) shows that the difficulty level to creating ***PAI***s are low. This means that some ***PA***s can easily be performed by imposters without requiring much effort or knowledge. Furthermore, most of the materials are available on the market. However, such ***PA***s are usually detected because of the inbuilt ***PAD*** methods in most of the available sensors.

As mention earlier in Section 6.1.2, the Lumidigm is provided with inbuilt ***PAD*** methods that detected all the performed ***PA***s against it. Also, in some cases it refused to capture some ***PA***s as playdoh. This means that the Lumidigm sensor is not vulnerable to any of the applied ***PA***s. On the other hand, the Crossmatch sensor did not react to any of the presented ***PA***s, and it accepted to capture all ***PA***s. Therefore, it is hard to determine whether the Crossmatch sensor is vulnerable to the performed ***PA***s or not.

Moreover, there is a correlation between the difficulty in creating the ***PAI*** and the vulnerabilities of the sensor. This is confirmed by the evaluation of ***PA***s in [10] (presented earlier in Chapter 7), where several factors are involved in the evaluation process. High values in factors such as equipment costs and availability, imposter expertise, and knowledge about the target sensor gives a high chance of applying a successful ***PA*** on the target sensor.

8.2.3 Task performer contribution

The project's motivation, tasks and goals are defined by the employer. Due to this fact, the task performer is require to show his contribution to the project outside the predefined tasks and goals. Therefore, this section presents some of the decisions that are taken by the task performer during the project. This is not limited to all the performed activities that are presented earlier in this thesis.

During the preparation phase, there was a problem with fabricating ***PAI***s in form of fake fingers by using a mould that contains a bona fide finger. There was a need of a form to hold the finger inside it while the silicone gets harden. Therefore, the task performer created a ***3D*** printed finger form to use it further during the ***PAI*** fabrication process. This form is shown in earlier Figure 21.

Additionally, once the project scope was modified to be a guideline for database creation, the task performer chose the overall methodology and the process of the guideline creation. This was done after presenting the ideas to the employer and supervisor, who further approved the methodology. The methodology include interviewing experts and students that use or have experience with fingerprint databases. Moreover, the task performer led the guideline creation process, and had own responsibility over it.

9 Conclusion

This chapter concludes this thesis by providing a summary of the performed processes and the achieved results. Furthermore, it presents the suggested future work, and self evaluation by author. Finally, a final comment is given from the author to the reader.

9.1 Summary

The goal of this thesis was to create a fingerprint ***PA*** database that can be used in future research related to ***PA*** and ***PAD*** studies. Due to the delayed delivery of the ***BATL*** sensor, the scope was modified to be a guideline proposal for fingerprint ***PA*** database creation, which includes the creation of normal fingerprint databases as well. Additionally, a pilot ***PA*** database was created using the existing sensors; Crossmatch Guardian 200-Rev 1 and Lumidigm v203. This database was a validation method to the created guideline in order to discover areas of improvements. Moreover, an evaluation of the performed ***PA***s based on the ***ISO*** standard 19989-1 ([10]) was performed.

The guideline proposal provide a detailed framework for fingerprint database creation, and can be further used as a checklist by the controller while performing the data collection, or as a training for new controllers that are about to start a database creation process. Furthermore, the guideline proposal covers the advantage of having multiple sensors, sessions, and samples. It also recommends to consider future research while creating a fingerprint database by applying additional metadata that uses the database in future studies.

9.2 Future work

This guideline will be used to create fingerprint databases in the future at ***da/sec***. This helps to discover areas of improvements and adapt the guideline to several scenarios (e.g., environment and sensors). There is already one project in ***da/sec*** that started to use the guideline to create a touchless fingerprint database.

Moreover, the original ***PA*** database is considered as future work for this project when the ***BATL*** sensor is delivered. There is a possibility for the author to create the original database in the future as a part of the biometrics course (IMT4126) in the master program.

The author is interested in creating a fingerprint database using multiple smartphone devices. Thes reason for this is that such databases are hard to find nowadays.

9.3 Self evaluation

During this project, the author gained experience in the research field by working in a research environment, and international experience by spending the thesis period in Germany as a part of Erasmus period. Moreover, the author gained a new knowledge in the field of biometrics and fingerprints, which were not part of the the bachelor program.

In this thesis the author showed the ability to work in systematic ways, having reflective capabilities, and being able to conduct scientific assessments, as the presented requirements in [30]. This includes solving the task in a scientific way and by applying correct methodologies. Furthermore, the author shows the skill of searching and identifying relevant scientific literature, and documenting and presenting the results in a systematic way.

The student believes that the evaluation of risks and their handling could have been performed better during the project planning period. This refers to the delayed delivery of the ***BATL*** sensor. However, the author also shows the ability of managing to handle such risks during the project and managed to deliver results that meets the requirements.

9.4 Final Comment and acknowledgment

The author believes that the goals of creating a guideline proposal for fingerprint ***PA*** database creation and creating a pilot ***PA*** database are achieved and meets the desired requirements of this thesis. He is also satisfied with the final result and the gained knowledge and experience. Final thanks is given to everyone who joined the data collection phase of in this project to create a pilot ***PA*** database, and for everyone else who helped reviewing this thesis and its content.

Bibliography

[1] Jain, A. K. 2004. An Introduction to Biometric Recognition. *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY*, 14(1), 4–20.

[2] Ratha, N. K., Connell, J. H., & Bolle, R. M. 2001. Enhancing securityand privacy inbiometrics-basedauthentication systems. *IBM SYSTEMS JOURNAL*, 40(3), 314–634.

[3] Information technology – Biometric presentation attack detection – Part 1: Framework. Standard, International Organization for Standardization, Geneva, CH, January 2016. ISO 30107-1:2016(E).

[4] Rajagopalan, S. S. 2016. DERMATOGLYPHIC ANALYSIS OF NON-SYNDROMIC ORAL CLEFTS CASES, UNAFFECTED FAMILY MEMBERS AND CONTROLS.

[5] Marasco, E. & Sansone, C. 2012. Combining perspiration- and morphology-based static features for fingerprint liveness detection. *Pattern Recognition Letters*, 33(9), 1148 – 1156. URL: http://www.sciencedirect.com/science/article/pii/S0167865512000128, doi:https://doi.org/10.1016/j.patrec.2012.01.009.

[6] Memon, S., Sepasian, M., & Balachandran, W. Dec 2008. Review of finger print sensing technologies. In *2008 IEEE International Multitopic Conference*, 226–231. doi:10.1109/INMIC.2008.4777740.

[7] Busch, C. 2013. Presentation attack detection methods for fingerprint recognition systems: a survey. 3(4), 219–233. doi:10.1049/iet-bmt.2013.0020.

[8] Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A. W. 2003. *Guide to Biometrics*. Springer Professional Computing.

[9] Faundez-Zanuy, M. 07 2006. Biometric security technology. 21, 15 – 26.

[10] Security techniques – Criteria and methodology for security evaluation of biometric systems – Part1: Framework. Community version, International Organization for Standardization, Geneva, CH, 2018. ISO/IEC CD 19989-1:2018(E).

[11] Information technology – Biometric presentation attack detection – Part 3: Testing and reporting. Standard, International Organization for Standardization, Geneva, CH, 2017. ISO 30107-3:2017(E).

[12] Busch, C. Harmonized biometric vocabulary. (Visited Jul. 2018). URL: https://christoph-busch.de/standards.html.

[13] Jain, A. K. 2007. Technology: Biometric recognition. *Nature*, 449(207), 38–40. doi:http://dx.doi.org/10.1038/449038a.

[14] ***EU:*** European Union & Intersoft Consulting. General data protection regulation (***gdpr***) - article 4 - definitions. (Visited Aug. 2018). URL: https://gdpr-info.eu/art-4-gdpr/.

[15] SWGFAST. 2009. Peer Reviewed Glossary of the Scientific Working Group on Friction Ridge Analysis, Study and Technology (PDF). 1–8. (Visited Jul. 2018). URL: https://web.archive.org/web/20120304171549/http://www.swgfast.org/documents/glossary/090508_Glossary_2.0.pdf.

[16] Chambers, H. G. & Sutherland, D. H. 2002. A Practical Guide to Gait Analysis. *Journal of the American Academy of Orthopaedic Surgeons*, 10(3), 222–231.

[17] Tome, M. & Zace, M. 2018. The impact of physical restrictions on the typing behaviour.

[18] K Jain, A. & Feng, J. 01 2011. Latent fingerprint matching. 33, 88–100.

[19] Thakkar, D. Minutiae based extraction in fingerprint recognition. (Visited Jul. 2018). URL: https://www.bayometric.com/minutiae-based-extraction-fingerprint-recognition/.

[20] Ergonomics of human system interaction – Part 11: Usability: Definitions and concepts. Standard, International Organization for Standardization, Geneva, CH, 2018. ISO 9241-11:2018 (EN).

[21] Mayhew, S. June 2012. Explainer: Verification vs. identification systems. (Visited Jul. 2018). URL: https://www.biometricupdate.com/201206/explainer-verification-vs-identification-systems.

[22] Information technology – Security techniques – Information security risk management (second edition). Standard, International Organization for Standardization, Geneva, CH, 2011. ISO 27005:2011.

[23] NRK & NTB. Jan 2010. Passene får fingeravtrykk. (Visited Oct. 2018). URL: https://www.nrk.no/norge/fingeravtrykk-i-pass-fra-paske-1.6960875.

[24] Drahansk¿, N¿tzel, & Funk. June 2006. Liveness detection based on fine movements of the fingertip surface. In *2006 IEEE Information Assurance Workshop*, 42–47. doi:10.1109/IAW.2006.1652075.

[25] Galbally, J., Marcel, S., & Fierrez, J. Feb 2014. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. *IEEE Transactions on Image Processing*, 23(2), 710–724. doi:10.1109/TIP.2013.2292332.

[26] Manivanan, N., Memon, S., & Balachandran, W. September 2010. Automatic detection of active sweat pores of fingerprint using highpass and correlation filtering. *Electronics Letters*, 46(18), 1268–1269. doi:10.1049/el.2010.1549.

[27] ODNI & IARPA. 2016. IARPA-BAA-16-04 (thor). https://www.iarpa.gov/index.php/research-programs/odin/odin-baa.

[28] da/sec. Batl: Biometric authentication with a timeless learner. (Visited Jul. 2018). URL: https://dasec.h-da.de/projects/current-projects/batl/.

[29] Gomez-Barrero, M., Kolberg, J., & Busch, C. Towards Fingerprint Presentation Attack Detection Based on Short Wave Infrared Imaging and Spectral Signatures. *da/sec - Biometrics and Internet Security Research Group*, 1–10.

[30] Gjøvik, N. Bis3900 - bachelor's thesis - information security. (Visited Jul. 2018). URL: https://www.ntnu.edu/studies/courses/BIS3900.

[31] Stallings, W. *Computer Security: Principles and Practice, Global Edition*. Pearson Education India.

[32] Braz, C. & Robert, J.-M. 2006. Security and usability: The case of the user authentication methods. In *Proceedings of the 18th Conference on L'Interaction Homme-Machine*, volume 21, 199–203. doi:10.1145/1132736.1132768.

[33] Das, R. 2006. An introduction to biometrics. *Keesing Journal of Documnts & Identity*, (17), 3–6. (Visited Jul. 2018). URL: http://biometricnews.net/wp-content/uploads/2017/01/Biometrics_Article_Introduction_To_Biometrics.pdf.

[34] Jain, A., Bolle, R., & Pankanti, S. 2006. Biometrics: Personal Identification in Networked Society.

[35] Jain, A. K., Ross, A., & Pankanti, S. 2006. Biometrics: A Tool for Information Security. *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, 1(2), 125–143.

[36] Jaiswal, S., Bhadauria, S. S., & Jadon, R. S. 2011. Biometrics: Case Study. *Journal of Global Research in Computer Science*, 2(10), 19–48.

[37] stephen j. elliott & Kukula, E. P. 2009. A Definitional Framework for the Human-Biometric Sensor Interaction Model. *BSP A Laboratory and Purdue University*, 1–6.

[38] ***EU:*** European Union. Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation). (Visited Aug. 2018). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[39] Author, G. 4 2018. Gdpr: What researchers need to know. (Visited Aug. 2018). URL: https://www.insight.mrc.ac.uk/2018/04/16/gdpr-research-changes/.

[40] ***EU:*** European Union & Intersoft Consulting. General data protection regulation (***gdpr***) - article 6 - lawfulness of processing. (Visited Aug. 2018). URL: https://gdpr-info.eu/art-6-gdpr/.

[41] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. 2009. *Handbook of Fingerprint Recognition*. Springer Publishing Company, Incorporated, 2nd edition.

[42] C. Lee, H. & R. E. Gaensslen, R. 01 2001. *Advances in Fingerprint Technology*. 2nd edition.

[43] Labati, R., Genovese, A., Piuri, V., & Scotti, F. 05 2014. Touchless fingerprint biometrics: A survey on 2d and 3d technologies. 15.

[44] Han, Y., Ryu, C., Moon, J., Kim, H., & Choi, H. 2005. A study on evaluating the uniqueness of fingerprints using statistical analysis. In *Information Security and Cryptology – ICISC 2004*, Park, C.-s. & Chee, S., eds, 467–477, Berlin, Heidelberg. Springer Berlin Heidelberg.

[45] Jain, A. K., Flynn, P., & Ross, A. A. 2007. *Handbook of Biometrics*. Springer-Verlag, Berlin, Heidelberg.

[46] Tutorials, W.-W.-H. I. D. & Information. Forensic sciences - visualization. (Visited Aug. 2018). URL: http://what-when-how.com/forensic-sciences/visualization/.

[47] Moenssens, A. 1971. *Fingerprint Techniques*. Inbau law enforcement series. Chilton Book Company. URL: https://books.google.de/books?id=aF6qQgAACAAJ.

[48] Karthikeyan, S., Feng, S., Rao, A., & Sadeh, N. M. 2014. Smartphone fingerprint authentication versus pins : A usability study.

[49] Thakkar, D. 12 reasons to consider fingerprint authentication. (Visited Jul. 2018). URL: https://www.bayometric.com/12-reasons-consider-fingerprint-authentication/.

[50] Manivanan, N., Memon, S., & Balachandran, W. September 2010. Automatic detection of active sweat pores of fingerprint using highpass and correlation filtering. *Electronics Letters*, 46(18), 1268–1269. doi:10.1049/el.2010.1549.

[51] Maltoni, D. *A Tutorial on Fingerprint Recognition*, 43–68. Springer Berlin Heidelberg, Berlin, Heidelberg, 2005. URL: https://doi.org/10.1007/11493648_3, doi:10.1007/11493648_3.

[52] Lee, C., Lee, S., & Kim, J. 2006. A study of touchless fingerprint recognition system. In *Structural, Syntactic, and Statistical Pattern Recognition*, Yeung, D.-Y., Kwok, J. T., Fred, A., Roli, F., & de Ridder, D., eds, 358–365, Berlin, Heidelberg. Springer Berlin Heidelberg.

[53] Breithaupt, R., Sousedik, C., & Meissner, S. March 2015. Full fingerprint scanner using optical coherence tomography. In *3rd International Workshop on Biometrics and Forensics (IWBF 2015)*, 1–6. doi:10.1109/IWBF.2015.7110228.

[54] Gomez-Barrero, M., Kolberg, J., & Busch, C. November 2018. Towards multi-model finger presentation attack detection. doi:10.1049/el.2010.1549.

[55] Espinoza, M., Champod, C., & Margot, P. 2011. Vulnerabilities of fingerprint reader to fake fingerprints attacks. *Forensic Science International*, 204(1), 41 – 49. URL: http://www.sciencedirect.com/science/article/pii/S0379073810002331, doi:https://doi.org/10.1016/j.forsciint.2010.05.002.

[56] Thamnurak, C., Bunakkharasawat, W., Riengrojpitak, S., & Panvisavas, N. 2011. Dna typing from fluorescent powder dusted latent fingerprints. *Forensic Science International: Genetics Supplement Series*, 3(1), e524 – e525. Progress in Forensic Genetics 14. URL: http://www.sciencedirect.com/science/article/pii/S1875176811002617, doi:https://doi.org/10.1016/j.fsigss.2011.10.009.

[57] Wiehe, A., Olsen, O., & Skarderud, F. L. 2004. Attacking fingerprint sensors.

[58] Gottschlich, C., Mikaelyan, A., Olsen, M. A., Bigun, J., & Busch, C. Sept 2015. Improving fingerprint alteration detection. In *2015 9th International Symposium on Image and Signal Processing and Analysis (ISPA)*, 83–86. doi:10.1109/ISPA.2015.7306037.

[59] Keilbach, P., Kolberg, J., Gomez-Barrero, M., Busch, C., & Langweg, H. Sept 2018. Fingerprint presentation attack detection using laser speckle contrast imaging. In *BIOSIG 2018*, 49–58.

[60] Baldisserra, D., Franco, A., Maio, D., & Maltoni, D. 2005. Fake fingerprint detection by odor analysis. In *Advances in Biometrics*, Zhang, D. & Jain, A. K., eds, 265–272, Berlin, Heidelberg. Springer Berlin Heidelberg.

[61] Sankaran, A., Vatsa, M., & Singh, R. 2015. Multisensor optical and latent fingerprint database. *IEEE Access*, 3, 653–665. doi:10.1109/ACCESS.2015.2428631.

[62] ATVS, B. R. G. Instructions for downloading atvs-ffp db. (Visited Nov. 2018). URL: http://atvs.ii.uam.es/atvs/ffp_db.html.

[63] Galbally, J., Haraksim, R., & Beslay, L. Sept 2018. Fingerprint quality: a lifetime story. In *BIOSIG 2018*, 27–36.

[64] Olsen, M. A., Smida, V., & Busch, C. 2016. Finger image quality assessment features - definitions and evaluation. *IET Biometrics*, 5, 47–64.

[65] NIST. Development of nfiq 2.0. (Visited Nov. 2018). URL: https://www.nist.gov/services-resources/software/development-nfiq-20.

[66] Information technology – Security techniques – Biometric information protection. Standard, International Organization for Standardization, Geneva, CH, June 2011. ISO/IEC 24745:2011.

[67] Ross, A. & Jain, A. K. Sept 2004. Multimodal biometrics: An overview. In *2004 12th European Signal Processing Conference*, 1221–1224.

[68] Gafurov, D., Bours, P., Yang, B., & Busch, C. March 2010. Guc100 multi-scanner fingerprint database for in-house (semi-public) performance and interoperability evaluation. In *2010 International Conference on Computational Science and Its Applications*, 303–306. doi:10.1109/ICCSA.2010.71.

[69] NSD. Nsd - norwegian centre for research data. (Visited Nov. 2018). URL: http://www.nsd.uib.no/nsd/english/index.html.

A Project Plan

A.1 Introduction

Nowadays, most of the usual electronic devices like smart phones, laptops and smart watches allows the ability of using the user's fingerprint to access the device. It is faster to access than a PIN code or password, more secure since it is unique from a user to another and *hard to spoof*. The last mentioned fingerprint's ability is the state of the art for this project, also ***fingerprint Presentation Attack Detection (PAD)***. Since fingerprints are more in use now, it became more vulnerable to presentation attacks. Therefore, the aim of this project is to apply an experiment on fingerprint detection sensors to test and discover their vulnerabilities.

A.2 Goals and Scope

A.2.1 Project's goals

The main goal of this project is to (1) collect Presentation Attack Instrument (PAI), (2) create a fingerprint database, (3) fabricate fingerprint Presentation Attacks (PA), (4) acquire presentation attacks and real samples with a set of innovative sensors, (5) apply existing presentation attack techniques to the acquired samples in order to detect the fake fingers. After a meeting with the employer of this project -Dr. Marta Gomez-Barrero-, the following effect goals and result goals are wanted for this project:

Effect goals

- Clarify the predefined fingerprint presentation attacks (PA) by preforming the attacks on some specific sensors.
- Verify the security around the different fingerprint detection sensors.

Result goals

- A fingerprint database, to use for further projects and research.
- List of detecting vulnerabilities attached to each fingerprint sensor, so it can be taken into account to implement presentation attack detection (PAD) methods for it in later projects.
- A List of valid fingerprints presentation attacks, clarify the strengths, weaknesses and likelihood of each attack to be preformed.

A.2.2 Project's scope

Brief description of the project

This project is a part of a bigger project called ***BATL***; Biometric Authentication with a Timeless Learner. It is a joint research project with the USC's Viterbi School of Engineering Computer Science Department, Idiap Research Institute, Hochschule Darmstadt, Norwegian University of Science and Technology, TREX Enterprises and Northrop Grumman Corporation Grumman Corporation.

The biometric research group at Hochschule Darmstadt in cooperation with the Norwegian Biometrics Laboratory (NTNU) participates in the following tasks:

- Presentation Attack Detection for Fingerprint.
- Presentation Attack Detection for Iris.

Dr. Marta Gomez-Barrero in Center for Research in Security and Privacy (CRISP) is the responsible for this project. A part of this project is preformed as a bachelor thesis for the student Ahmed S. M. Madhun in Information Security degree at NTNU-Gjøvik, and it is a part of an internship in Hochschule Darmstadt – University of Applied Sciences (h_da).

The task is to preform a fabricate presentation attacks following the predefined guidelines on the existed and innovative sensors. In order to do this, a fingerprint database should be created.

Timeframe

The internship period will be from 15.06.2018-30.11.2018. After the final date, the work on the project will cease regardless of the project's state unless arrangements are made. Since this is a bachelor thesis and the student wants to perform other tasks to gain experience in other fields of biometrics security, the bachelor thesis will have its own time frame from 15.05.2018-31.08.2018. After the thesis period, the student will be working on other topics or extending this topic to a larger scope, and be enrolled as an Erasmus student in h_da.

Employer's scope

Requirements / limitations for project and final report:

- A fingerprint database creation of at least 20 participants.
- The presentation attacks will be created using the provided materials by the employer.
- The presentation attacks will be preformed on the provided sensors by the employer.
- Final paper of the work should be delivered within predefined deadlines.

Student's scope

The following requirements/limitations the student has to deliver/do for this project:

- A project plan, contains scheduling of the different phases during the project (Delivered to the supervisor).
- A final report to be graduated in Bachelor in Information Security BIS3900 at NTNU Gjøvik (Delivered to NTNU Gjøvik).
- Run an experiment to collect fingerprints and create the database with at least 20 participants.
- A reflection report of the internship and project period (Delivered to the supervisor).

The following item(s) will not take a part in this bachelor thesis project during the bachelor period:

- Create a detection method for fingerprints.

A.2.3 Processing of information

The collection of fingerprints is considered as a private, sensitive data and should follow the GDPR protection law. Therefore, the processing of handling/storing it should be clarified early in the project between the employer and the student. The data that will be collected should be randomized by the participant numbers. The participants should sign up on a consent form that clarify the purpose of the work and the handling of the data.

Take the form should also collect the contact information for the participants. in case there is a need for another round of PAI, or updating the data yearly for further research.

A.3 Organization

A.3.1 Organizational structure

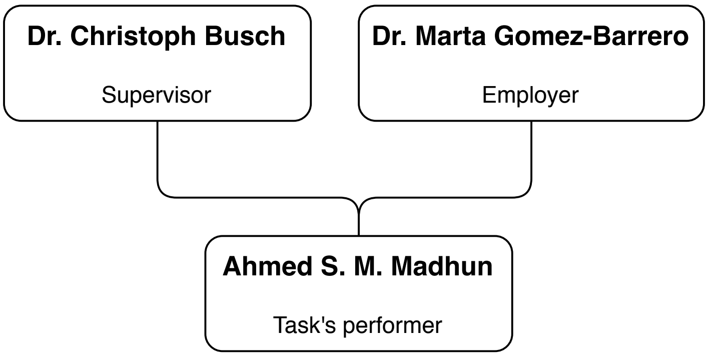


Figure 28: The organizational structure of this project

A.3.2 Roles

The following roles have been specified for this project:

- **Employer & Product Owner** - Dr. Marta Gomez-Barrero-
  - Ensure the quality of the student's works and proof that it matches the wished requirements.
  - Provide the needed equipment for the student during the defined period.
- **Supervisor** - Dr. Christoph Busch
  - Follow the student's working process.
  - Provide feedback, and ensure that the student is *on track*.
- **Student & task's performer** - Ahmed S. M. Madhun
  - Responsible for project's time management and delivering the requirements of the project within the deadlines.

A.3.3 Time management and meetings

During this project, the student works Monday-Friday in the same lab with other students. The student is also responsible to maintain the communication with his employer. A meeting between the employer and the students is defined as once each week by default, and could be changed later according to the process and time management.

The employer is responsible for the meetings between the supervisor and the student. It is already defined to be once each month because of the availability of the supervisor.

A.4 Risk Management

This section will contains the risks that could appear during this project. Each risk will be evaluated relative to it's likelihood to happen and consequence if a risk occurs. In the risk analysis subsection under, it's defined the likelihood and consequence on a scale from one (1) to five (5). Where one is defined as *None Critical* and five is considered *Critical*.

A.4.1 Risk analysis

Nr#	Risk	Likelihood	Consequence	Countermeasure
1	The project is not completed before the deadline or delivery delay. Reasons could be Backup lost, poor estimate of points in activities, or delay in receiving the needed equipment.	2	5	Yes
2	Major changes in requirements specifications from employer.	1	4	No
3	Loss of resources (data or report).	2	5	Yes
4	Project shutdown	1	5	No
5	The final product does not match the requirements of the employer.	1	4	Yes
6	The project is not delivered on time because of the delay on receiving the sensor.	3	5	Yes

Table 8: Project's risks

Note: The risk number six was added to the table in August, as a result of the unexpected delay of the *BATL* sensor.

A.4.2 Countermeasures

To ensure the quality of the student's work in the project, a list of countermeasures for the mentioned risks is listed in the table below.

Nr#	Risk Countermeasures
1	The student is using a form of an agile working process. So, both the quality of the work and the delivery should be matching the requirements.
3	The data and the report of the project is vulnerable to be lost. Therefore, it should be stored and protected. Also, a buck-up of data will be often during the project period. The report is hosted in ShareLaTex cloud storage and a back-up form time to time should be taken.
5	The student should organize the work and share the process with the supervisor and employer to ensure that he is following the right track.
6	The case can be modified in order to make the student complete his thesis. However, the topic is interested for the student and wish to wait 1 or a half month to see the final result of the delay.

Table 9: Project's risk countermeasures

A.5 Planning & Rapport

A.5.1 Working process

Due the task's requirements from the employer, the project is divided into four phases. The figure below shows the planned phases under the project period.

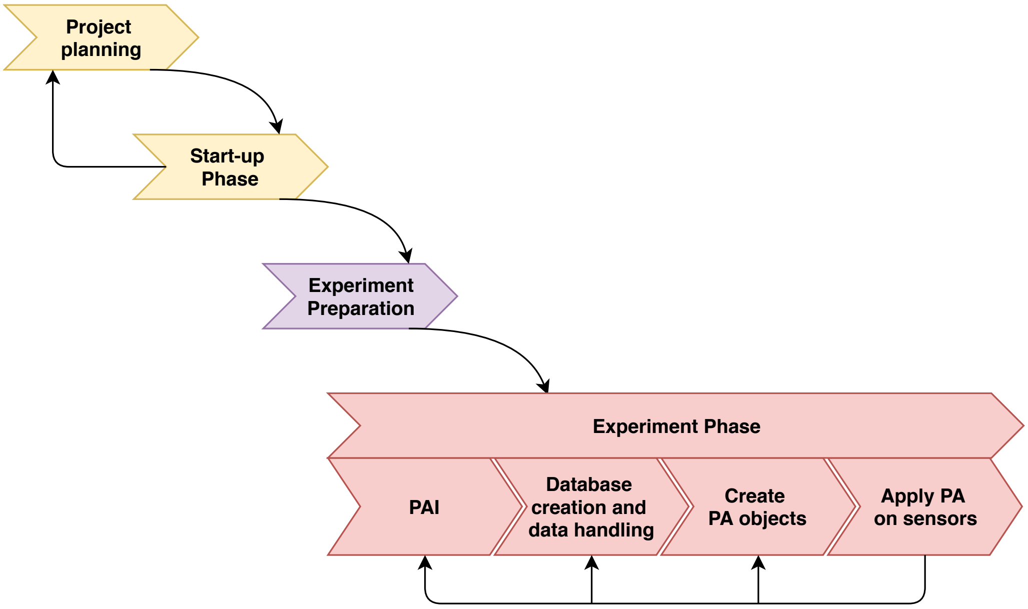


Figure 29: Working process during the project

- **Phase 1 - Project planning**
  - Define the goals of the project.
  - Set up a plan of the working process.
  - Establish communications with the supervisor and the employer.
- **Phase 2 - Start-up phase**
  - The student use the period to obtain the relevant knowledge for the project,

by reading relevant papers and previous projects.

- It is possible that during this phase to change the predefined project planned if needed.

- **Phase 3 - Experiment Preparation**
  - The student use this time to prepare for the experiment by getting more known with the provided materials and sensors.
- **Phase 4 - Experiment Phase**
  - The experiment contains phase contains 4 sub-phases that should run in parallel:
    - **Phase 4.1 - Presentation Attack Instruments**
    - **Phase 4.2 - Database creation and data handling**
    - **Phase 4.3 - Create presentation attacks objects**
    - **Phase 4.4 - Apply presentation attacks on sensors**

The report (thesis) will be written in parallel with all phases, based on the previous experience the student have.

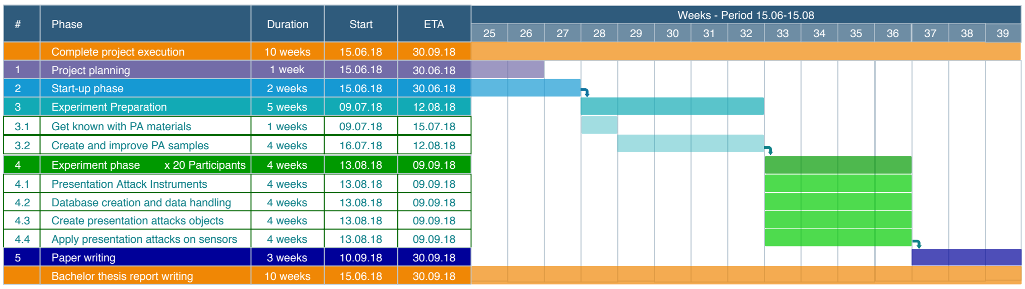
A.5.2 Experiment's Notes

The reason for running all the sub-phases at the same time under the experiment is to insure that the quality of the PA objects are good to preform the PA on the sensors. The same sub-phases will be preformed for at least 20 participants.

A.6 Schedule

A.6.1 Gantt diagram

The figure below is a gantt diagram that shows how are the mentioned phases in A.5.1 are divided over ten weeks (Thesis's period as mentioned in A.2.2).



#	Phase	Duration	Start	ETA
	Complete project execution	10 weeks	15.06.18	30.09.18
1	Project planning	1 week	15.06.18	30.06.18
2	Start-up phase	2 weeks	15.06.18	30.06.18
3	Experiment Preparation	5 weeks	09.07.18	12.08.18
3.1	Get known with PA materials	1 weeks	09.07.18	15.07.18
3.2	Create and improve PA samples	4 weeks	16.07.18	12.08.18
4	Experiment phase x 20 Participants	4 weeks	13.08.18	09.09.18
4.1	Presentation Attack Instruments	4 weeks	13.08.18	09.09.18
4.2	Database creation and data handling	4 weeks	13.08.18	09.09.18
4.3	Create presentation attacks objects	4 weeks	13.08.18	09.09.18
4.4	Apply presentation attacks on sensors	4 weeks	13.08.18	09.09.18
5	Paper writing	3 weeks	10.09.18	30.09.18
	Bachelor thesis report writing	10 weeks	15.06.18	30.09.18

Figure 30: Gantt chart of the project flow and phases timing

Project planning is taking a part of this project at the very start, and it is estimated to take one week of work. During the project planning, the student will use the time to obtain knowledge for this project. Since the topic is quite new for the student, this phase are estimated to take two weeks.

One of the sensors that are provided by the employer will need some time to be ready for the experiment. Therefore, the student is asked to perform a preparation for the experiment in the five weeks before sensors are ready to be used in the experiment. Once the sensor are ready to be used, the experiment period will start and it is estimated to take 4 weeks. It is suggested by the employer to apply one participant everyday, because there are four sub-phases that need to run at the same day for each participant.

The student will use the last three weeks of the project to write the paper for the employer. This is still optional but the student has the motivation for it. The bachelor thesis report writing will be running in parallel during the whole project. This should be reviewed again by the end of September.

B Midterm review

This appendix presents the meeting log of the midterm review, which consists of three separate meetings between the student, his supervisor, his employer and the administrative responsible from ***NTNU***. It took a place on the 15th of October. However, it was planned to be performed early in October, but it got delayed because of the the availability of the involved members. This review covers (1) the status of the project according to the original project plan (see Appendix A) before the meetings, and (2) the future plans/steps that need to be considered in order to complete the project. Also, to ensure that the student is on the right track with the new goal.

B.1 Status of the project before the meeting

The student used the period leading up to the meeting on training for the database acquisition (particularly on the fabrication of ***PAI***s, which is not a trivial task), obtaining knowledge about the topic, and writing the theory part of the thesis (Introduction, Basic knowledge, Literature review, and preparation for the main experiment).

The ***BATL*** sensor was planned to be ready at the begging of October, but is still not ready to be used and faces some technical issues that increase the delay period of the project. Also, until this day, the student was not informed about a specific deadline date to hand in the thesis. However, it was known that the project should be submitted and evaluated during the autumn semester 2018, which initially seemed feasible with the original deadline for the ***BATL*** sensor.

B.2 Summary of the meeting

During the meeting, the student was informed about the new delay of the ***BATL*** sensor, and the deadline date to hand in the project report (i.e., the thesis). Also, the student presented an overview over the project status to the involved members to gain feedback in order to consider future work due to the deadline.

The following two main factors were discussed during the meeting:

1. **The student stick to the chosen topic and accept the delay of the project, and deliver the thesis in spring 2019.**
   The main reasons for considering such a factor are that (1) the student already gained so much experience (i.e., practical and theoretical knowledge) about the topic, (2) the student interest to perform the topic, and (3) the progress that were made already by the student in writing the final report.

2. **The student changes the chosen topic to a new one, and hand in the requirements for the thesis on time.**
   The reasons to consider such a factor are summarized as follows: (1) The student has interest in finishing the thesis on time. Also, an important factor is (2) the extra knowledge that the student can gain from changing the topic.

B.3 The student's decision

The student chose to change the topic in order to deliver the thesis on time. Also, it is worth mentioning that the student is currently a master student in Information Security at ***NTNU*** Gjøik. This allows the student to consider doing the original topic (i.e., Fingerprint Presentation Attack Database Creation) as a part of the Biometrics course in the next semester. By doing so, the student will gain experience in a new topic and have the chance to do the old topic that interests him.

Furthermore, the student has to choose a new topic. The available choices were either a new topic or a topic related to the original. Due to the project time constraint, the student chose a related topic with approval from his supervisor.

B.4 Modifying the topic

In order to modify the original topic to a new one, several elements has been taken into consideration, such as:

- **The predefined project's motivation, goals and research question.**
  There is a possibility to partly answer the research question (see Chapter 1 in Section 1.6). This can be performed by running a pilot version of the main project (i.e., creating a ***PA*** database) using the available sensors (Crossmatch and Lumidigm).
- **The possibility that another student performs the original project.**
  In case the student will not have time in the future to come back to perform the original project, another student can run the project instead. In this case, there is a need to share the experience with the new student and minimize the time consumption. This can be performed by creating a guideline of how to create a ***PA*** database. Also, keeping in mind that this can be considered in other projects.
- **The amount of work that has to be performed by the student as a Bachelor project**
  The student is asked to evaluate the performed ***PA***s based on the attack potential of ***PAI***s based on the ***ISO*** standard.
- **The project time constraint gets near the deadline**
  By the end of today, there are seven weeks to the deadline for the project requirements. Therefore, the student will be performing as much as possible of the mentioned modifications in order to deliver good content on time.

C Types of *PAD*

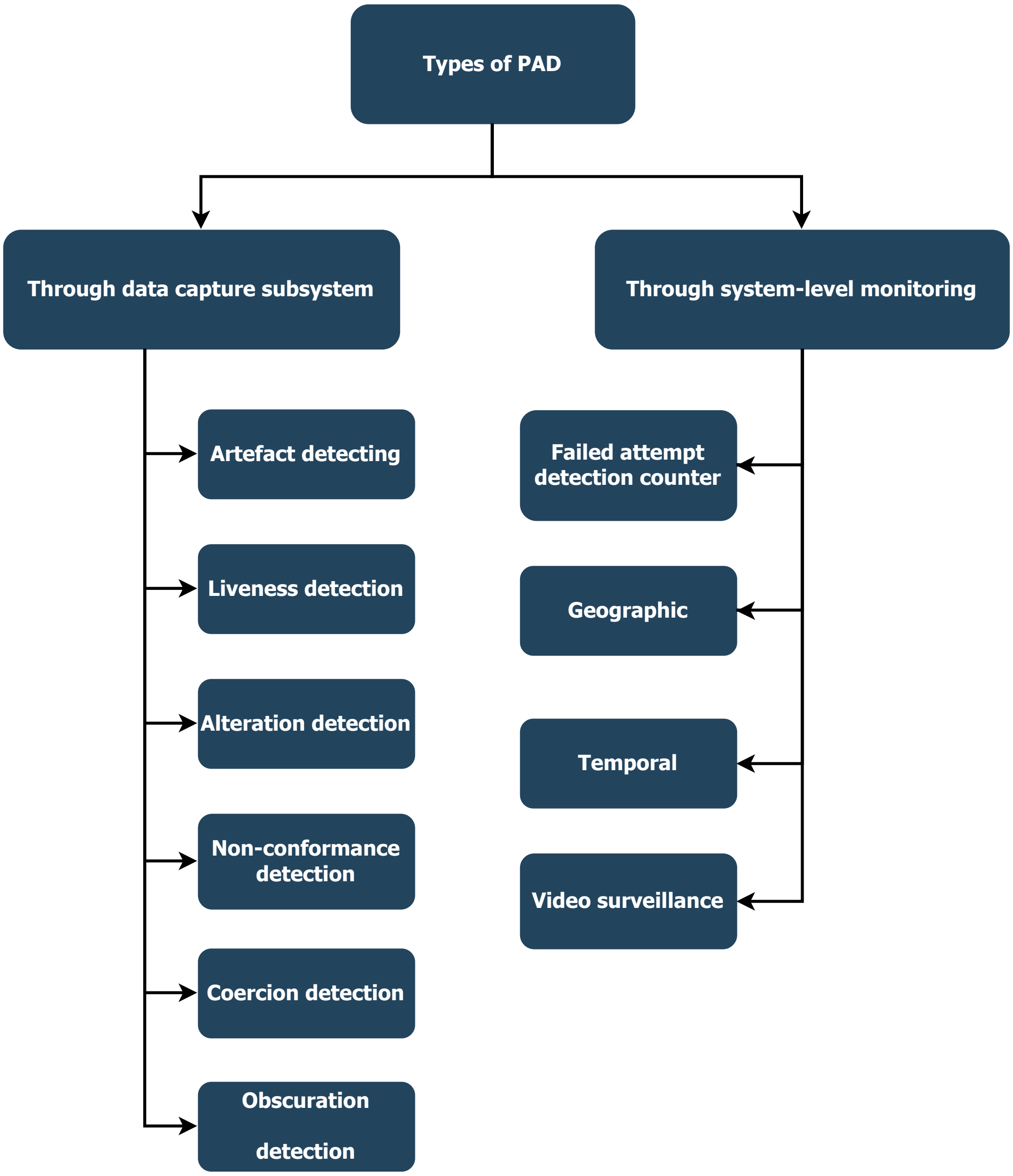
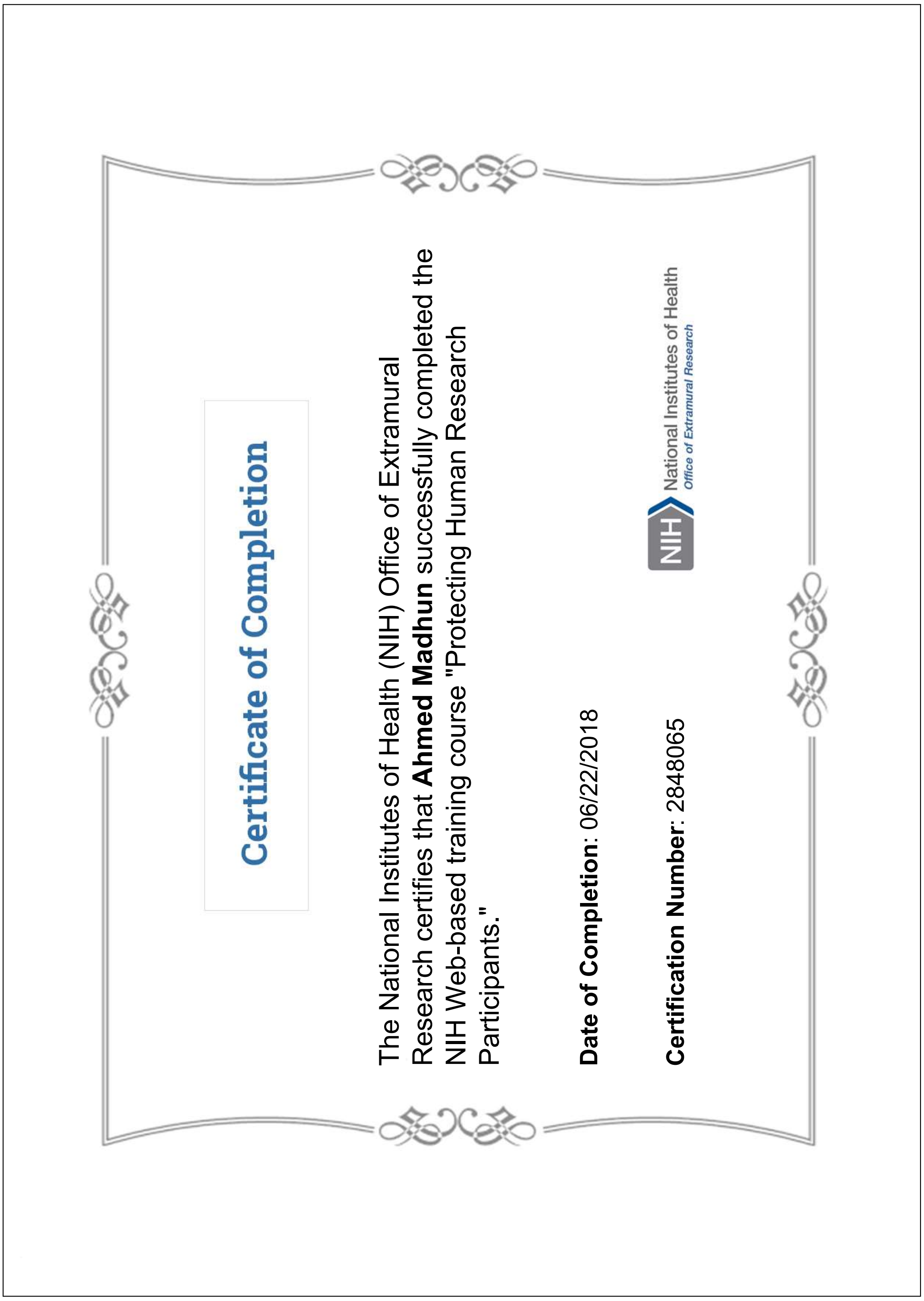


Figure 31: Categories and subcategories of ***PAD***'s types (as presented in [3])

D PHRP certification



Certificate of Completion

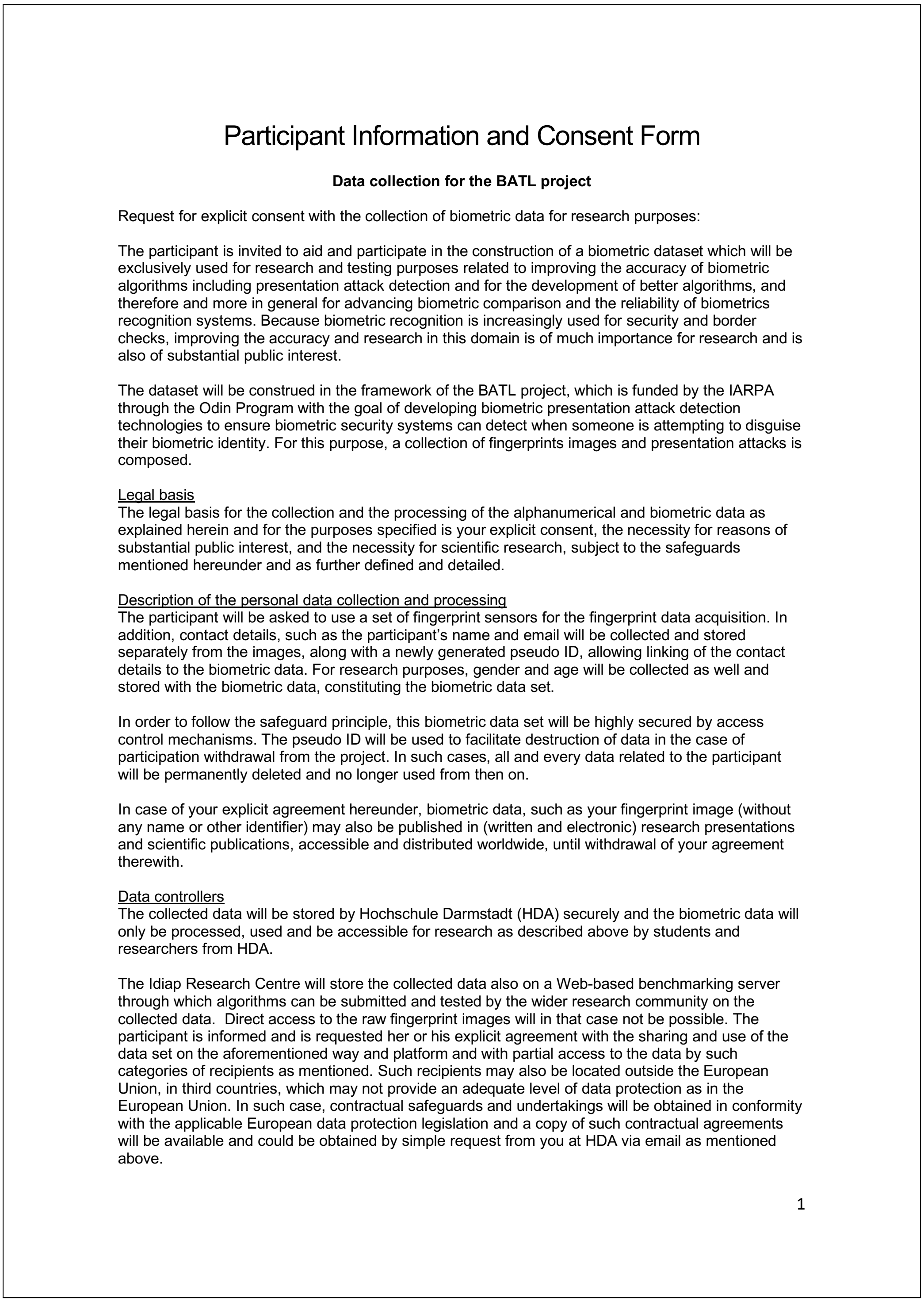
The National Institutes of Health (NIH) Office of Extramural Research certifies that **Ahmed Madhun** successfully completed the NIH Web-based training course "Protecting Human Research Participants."

Date of Completion: 06/22/2018

Certification Number: 2848065

NIH National Institutes of Health
Office of Extramural Research

E Consent from



Participant Information and Consent Form

Data collection for the BATL project

Request for explicit consent with the collection of biometric data for research purposes:

The participant is invited to aid and participate in the construction of a biometric dataset which will be exclusively used for research and testing purposes related to improving the accuracy of biometric algorithms including presentation attack detection and for the development of better algorithms, and therefore and more in general for advancing biometric comparison and the reliability of biometrics recognition systems. Because biometric recognition is increasingly used for security and border checks, improving the accuracy and research in this domain is of much importance for research and is also of substantial public interest.

The dataset will be construed in the framework of the BATL project, which is funded by the IARPA through the Odin Program with the goal of developing biometric presentation attack detection technologies to ensure biometric security systems can detect when someone is attempting to disguise their biometric identity. For this purpose, a collection of fingerprints images and presentation attacks is composed.

Legal basis
The legal basis for the collection and the processing of the alphanumerical and biometric data as explained herein and for the purposes specified is your explicit consent, the necessity for reasons of substantial public interest, and the necessity for scientific research, subject to the safeguards mentioned hereunder and as further defined and detailed.

Description of the personal data collection and processing
The participant will be asked to use a set of fingerprint sensors for the fingerprint data acquisition. In addition, contact details, such as the participant's name and email will be collected and stored separately from the images, along with a newly generated pseudo ID, allowing linking of the contact details to the biometric data. For research purposes, gender and age will be collected as well and stored with the biometric data, constituting the biometric data set.

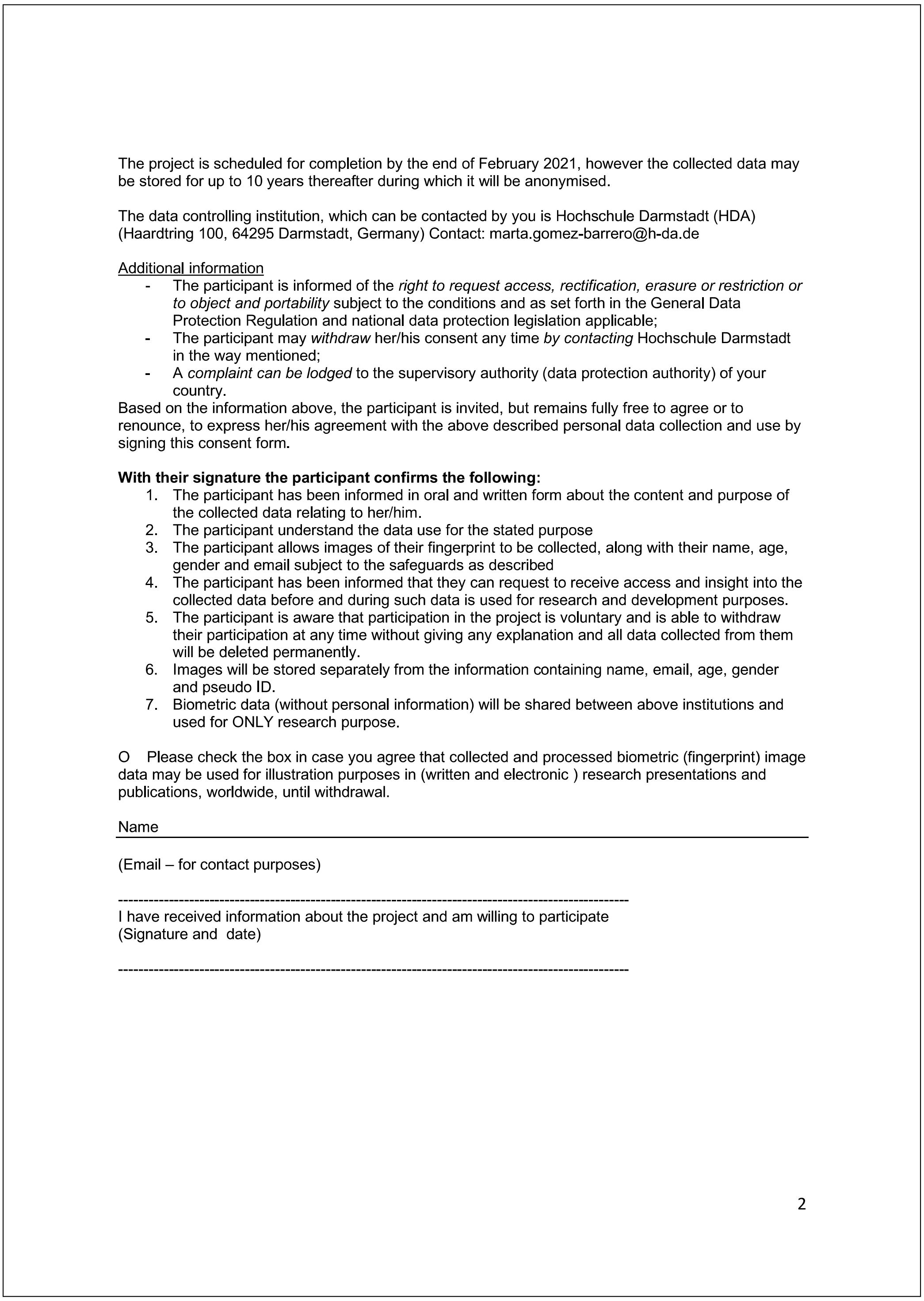
In order to follow the safeguard principle, this biometric data set will be highly secured by access control mechanisms. The pseudo ID will be used to facilitate destruction of data in the case of participation withdrawal from the project. In such cases, all and every data related to the participant will be permanently deleted and no longer used from then on.

In case of your explicit agreement hereunder, biometric data, such as your fingerprint image (without any name or other identifier) may also be published in (written and electronic) research presentations and scientific publications, accessible and distributed worldwide, until withdrawal of your agreement therewith.

Data controllers
The collected data will be stored by Hochschule Darmstadt (HDA) securely and the biometric data will only be processed, used and be accessible for research as described above by students and researchers from HDA.

The Idiap Research Centre will store the collected data also on a Web-based benchmarking server through which algorithms can be submitted and tested by the wider research community on the collected data. Direct access to the raw fingerprint images will in that case not be possible. The participant is informed and is requested her or his explicit agreement with the sharing and use of the data set on the aforementioned way and platform and with partial access to the data by such categories of recipients as mentioned. Such recipients may also be located outside the European Union, in third countries, which may not provide an adequate level of data protection as in the European Union. In such case, contractual safeguards and undertakings will be obtained in conformity with the applicable European data protection legislation and a copy of such contractual agreements will be available and could be obtained by simple request from you at HDA via email as mentioned above.

1



The project is scheduled for completion by the end of February 2021, however the collected data may be stored for up to 10 years thereafter during which it will be anonymised.

The data controlling institution, which can be contacted by you is Hochschule Darmstadt (HDA) (Haardtring 100, 64295 Darmstadt, Germany) Contact: marta.gomez-barrero@h-da.de

Additional information

- The participant is informed of the *right to request access, rectification, erasure or restriction or to object and portability* subject to the conditions and as set forth in the General Data Protection Regulation and national data protection legislation applicable;
- The participant may *withdraw* her/his consent any time *by contacting* Hochschule Darmstadt in the way mentioned;
- A *complaint can be lodged* to the supervisory authority (data protection authority) of your country.

Based on the information above, the participant is invited, but remains fully free to agree or to renounce, to express her/his agreement with the above described personal data collection and use by signing this consent form.

With their signature the participant confirms the following:

1. The participant has been informed in oral and written form about the content and purpose of the collected data relating to her/him.
2. The participant understand the data use for the stated purpose
3. The participant allows images of their fingerprint to be collected, along with their name, age, gender and email subject to the safeguards as described
4. The participant has been informed that they can request to receive access and insight into the collected data before and during such data is used for research and development purposes.
5. The participant is aware that participation in the project is voluntary and is able to withdraw their participation at any time without giving any explanation and all data collected from them will be deleted permanently.
6. Images will be stored separately from the information containing name, email, age, gender and pseudo ID.
7. Biometric data (without personal information) will be shared between above institutions and used for ONLY research purpose.

O Please check the box in case you agree that collected and processed biometric (fingerprint) image data may be used for illustration purposes in (written and electronic) research presentations and publications, worldwide, until withdrawal.

Name

(Email – for contact purposes)

I have received information about the project and am willing to participate
(Signature and date)

F Additional Figures

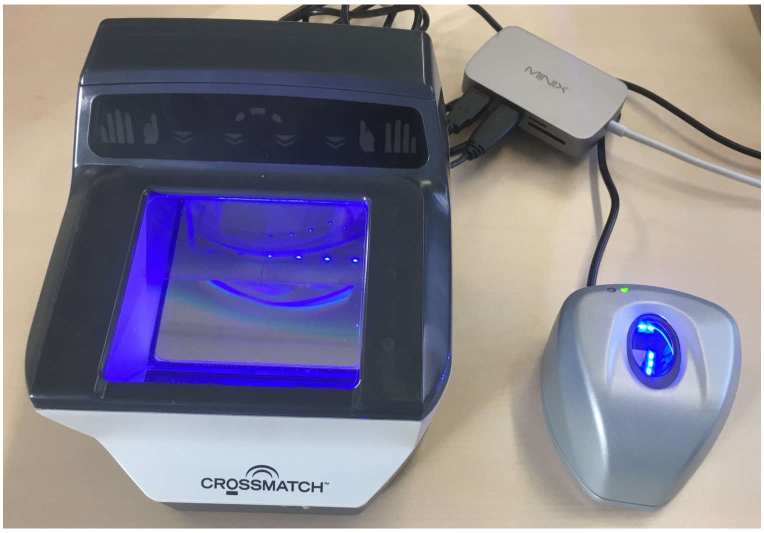
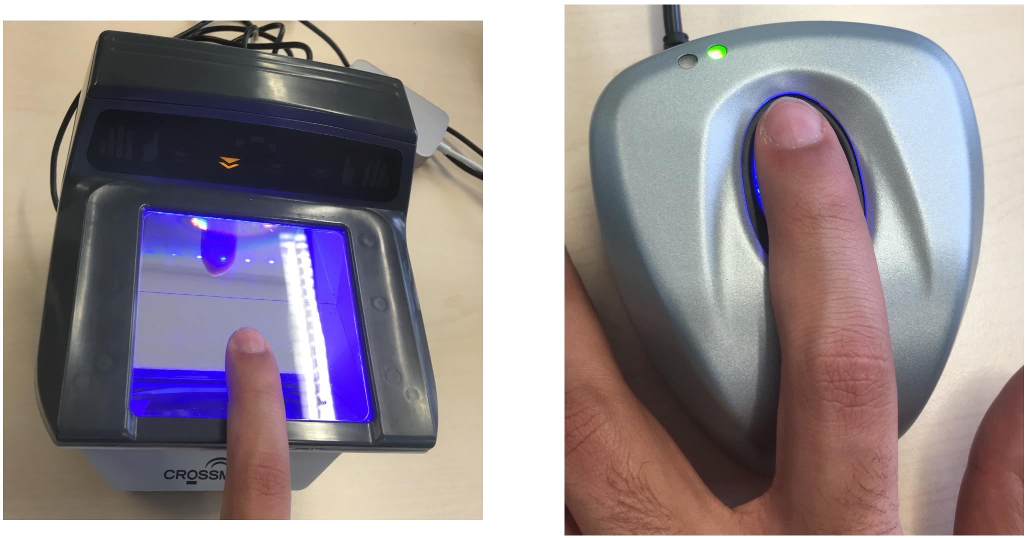


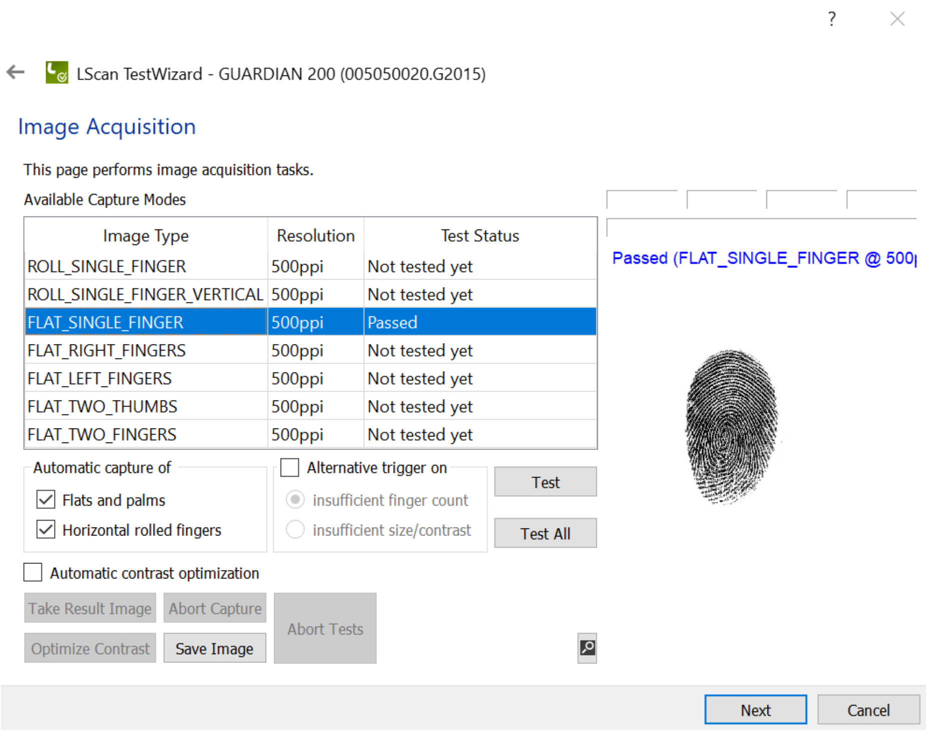
Figure 32: Crossmatch Guardian 200-Rev 1 sensor on the left side and Lumidigm v203 on the right side



(a) Bona fide presentation on Crossmatch sensor

(b) Bona fide presentation on Lumidigm sensor

Figure 33: Bona fide presentation on Crossmatch and Lumidigm sensors



LScan TestWizard - GUARDIAN 200 (005050020.G2015)

Image Acquisition

This page performs image acquisition tasks.

Available Capture Modes

Image Type	Resolution	Test Status
ROLL_SINGLE_FINGER	500ppi	Not tested yet
ROLL_SINGLE_FINGER_VERTICAL	500ppi	Not tested yet
FLAT_SINGLE_FINGER	500ppi	Passed
FLAT_RIGHT_FINGERS	500ppi	Not tested yet
FLAT_LEFT_FINGERS	500ppi	Not tested yet
FLAT_TWO_THUMBS	500ppi	Not tested yet
FLAT_TWO_FINGERS	500ppi	Not tested yet

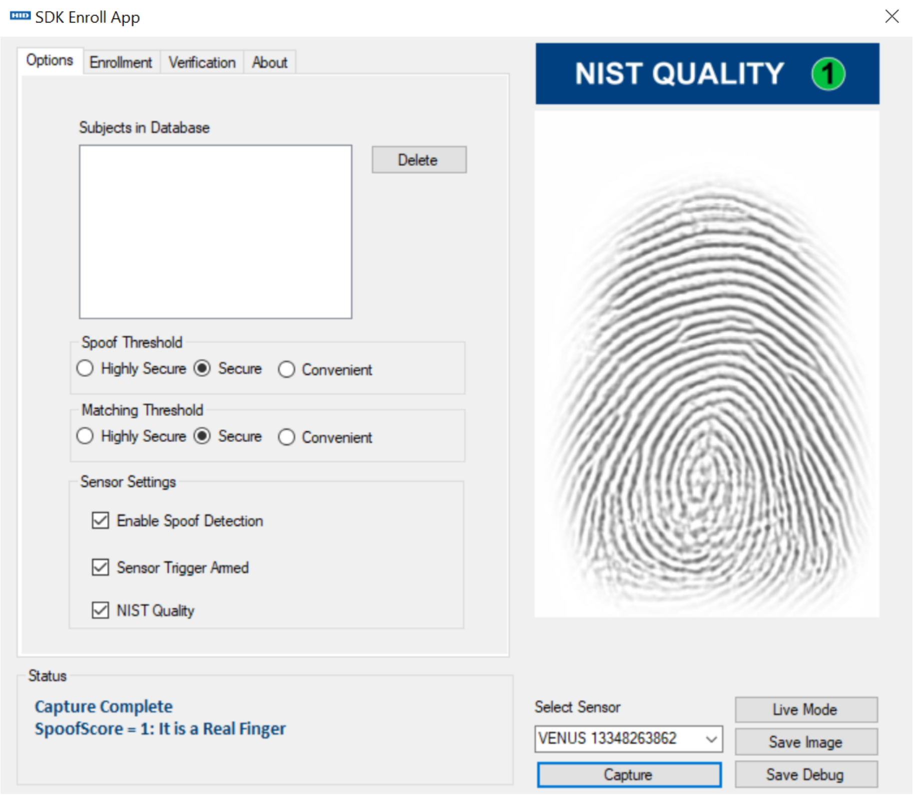
Passed (FLAT_SINGLE_FINGER @ 500|

Automatic capture of
☑ Flats and palms
☑ Horizontal rolled fingers

☐ Alternative trigger on
● insufficient finger count
○ insufficient size/contrast

☐ Automatic contrast optimization

Figure 34: Screenshot while using Crossmatch sensor



SDK Enroll App

NIST QUALITY 1

Subjects in Database

Spoof Threshold
○ Highly Secure ● Secure ○ Convenient

Matching Threshold
○ Highly Secure ● Secure ○ Convenient

Sensor Settings
☑ Enable Spoof Detection
☑ Sensor Trigger Armed
☑ NIST Quality

Status
Capture Complete
SpoofScore = 1: It is a Real Finger

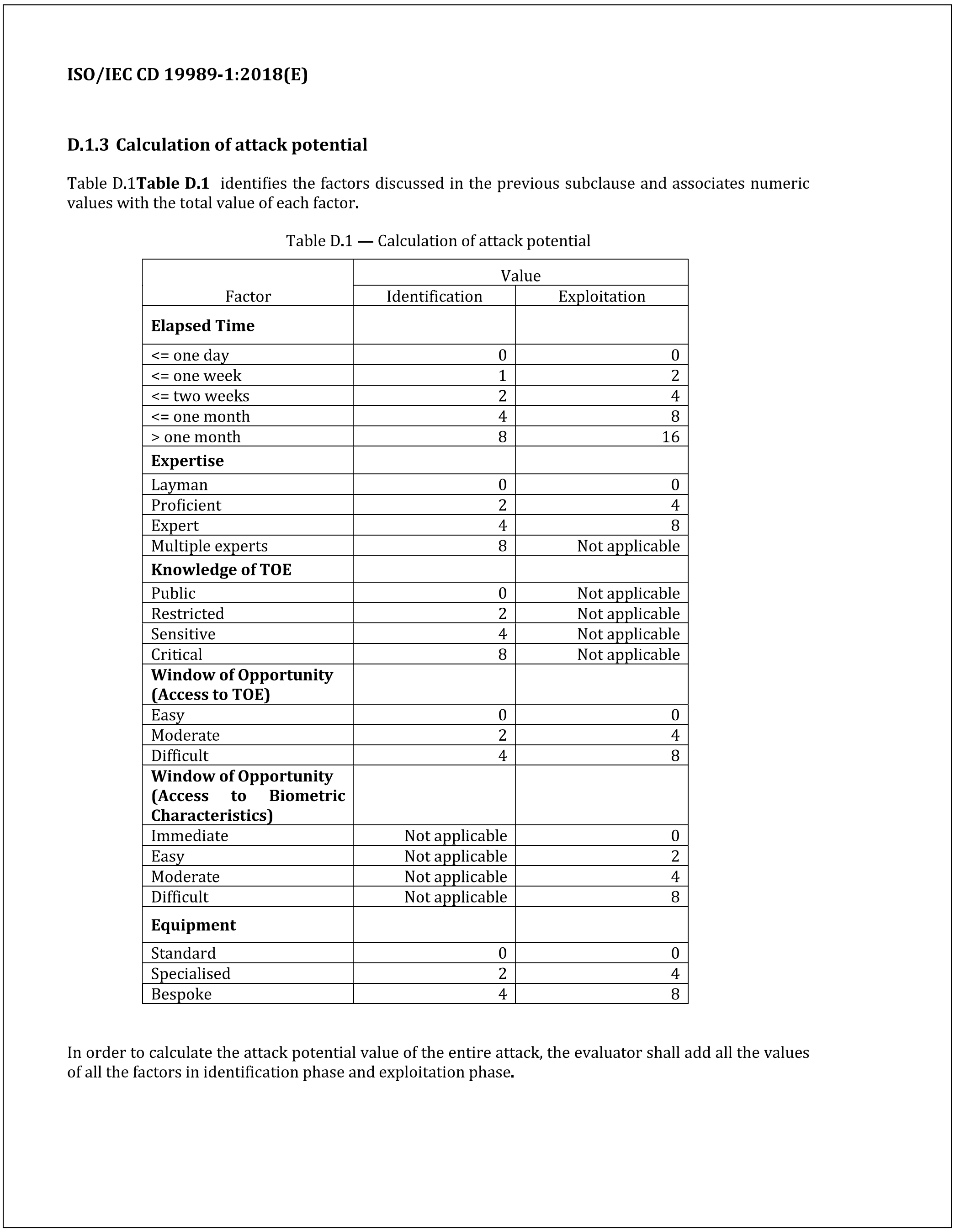
Select Sensor
VENUS 13348263862

Figure 35: Screenshot while using Lumidigm sensor

G ISO CD - Calculation of attack potential

G.1 Attack potential values

This appendix presents the attack potential values assessed to each factor as presented in the ***ISO*** CD 19989-1:2018(E) [10].



ISO/IEC CD 19989-1:2018(E)

D.1.3 Calculation of attack potential

Table D.1**Table D.1** identifies the factors discussed in the previous subclause and associates numeric values with the total value of each factor.

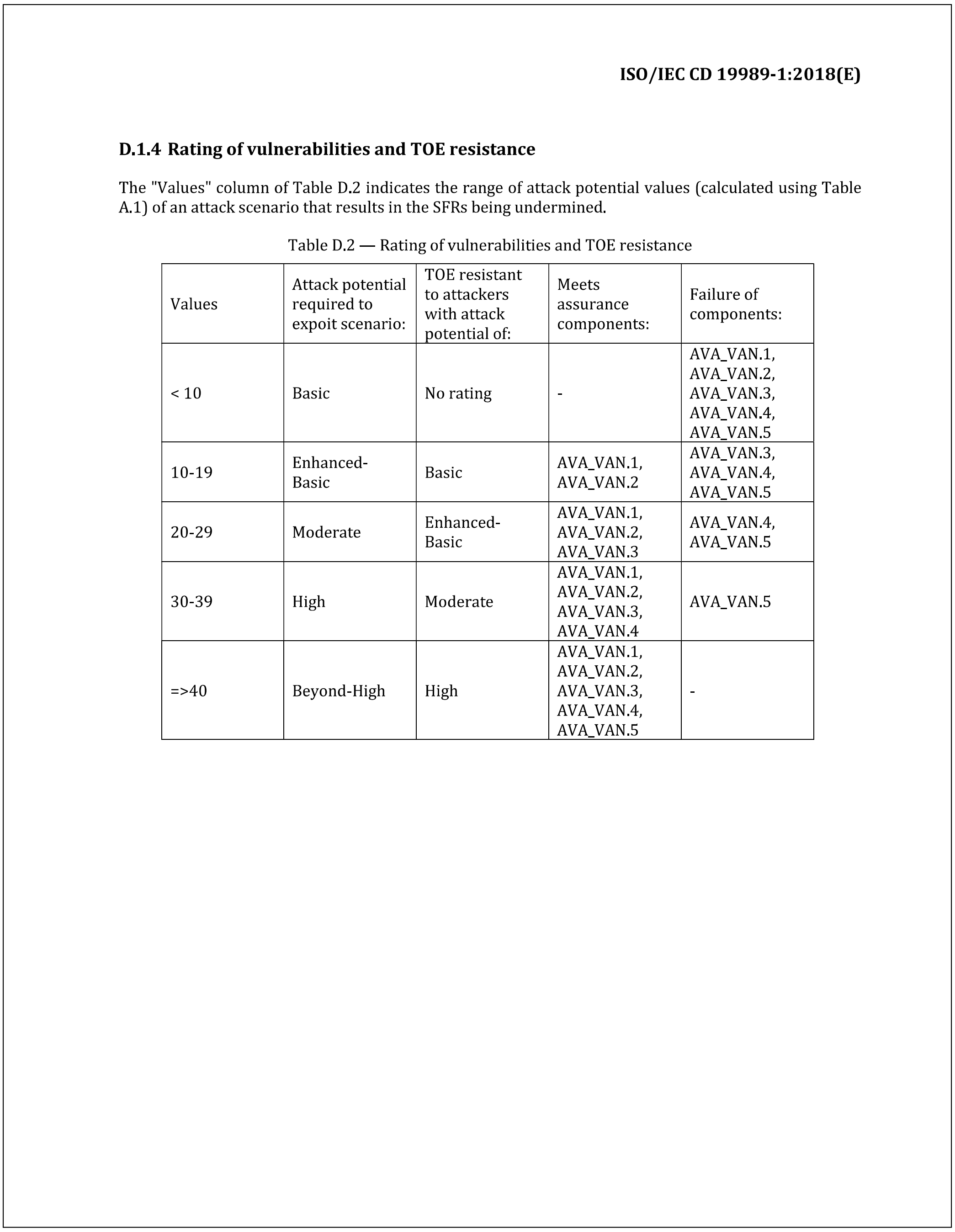
Table D.1 — Calculation of attack potential

Factor	Value	
	Identification	Exploitation
Elapsed Time		
<= one day	0	0
<= one week	1	2
<= two weeks	2	4
<= one month	4	8
> one month	8	16
Expertise		
Layman	0	0
Proficient	2	4
Expert	4	8
Multiple experts	8	Not applicable
Knowledge of TOE		
Public	0	Not applicable
Restricted	2	Not applicable
Sensitive	4	Not applicable
Critical	8	Not applicable
Window of Opportunity (Access to TOE)		
Easy	0	0
Moderate	2	4
Difficult	4	8
Window of Opportunity (Access to Biometric Characteristics)		
Immediate	Not applicable	0
Easy	Not applicable	2
Moderate	Not applicable	4
Difficult	Not applicable	8
Equipment		
Standard	0	0
Specialised	2	4
Bespoke	4	8

In order to calculate the attack potential value of the entire attack, the evaluator shall add all the values of all the factors in identification phase and exploitation phase.

G.2 Presentation attack rating

This appendix presents the ***PA***s rating defined in the ***ISO*** CD 19989-1:2018(E).



ISO/IEC CD 19989-1:2018(E)

D.1.4 Rating of vulnerabilities and TOE resistance

The "Values" column of Table D.2 indicates the range of attack potential values (calculated using Table A.1) of an attack scenario that results in the SFRs being undermined.

Table D.2 — Rating of vulnerabilities and TOE resistance

Values	Attack potential required to expoit scenario:	TOE resistant to attackers with attack potential of:	Meets assurance components:	Failure of components:
< 10	Basic	No rating	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
10-19	Enhanced-Basic	Basic	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
20-29	Moderate	Enhanced-Basic	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
30-39	High	Moderate	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=>40	Beyond-High	High	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-