

Hamza Azim
Milosz Antoni Wudarczyk
Kristian Amundsen Øhman-Norén

Smartphone Presentation Attack Detection using TrueDepth

Bachelor's thesis in Bachelor in Computer Science Engineering &
Bachelor in Digital Infrastructure and Cyber Security
Supervisor: Kiran Raja
May 2022

Hamza Azim
Milosz Antoni Wudarczyk
Kristian Amundsen Øhman-Norén

Smartphone Presentation Attack Detection using TrueDepth

Bachelor's thesis in Bachelor in Computer Science Engineering &
Bachelor in Digital Infrastructure and Cyber Security
Supervisor: Kiran Raja
May 2022

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Abstract

Automated Presentation Attack Detection (PAD) is essential to protect facial recognition systems from potential security breaches. A multitude of stable, effective and accurate PAD systems exist today. In the current landscape within the field of PAD, the majority of the systems considered to be the most effective, use RGB-imaging exclusively. In reality, more dimensions and factors beyond the standard RGB-data produced by a standard camera can be taken into account when attempting to stop a presentation attack from happening.

The research on how each type of supplemental data effects the detection of presentation attacks, is largely unexplored territory. Little publicly available material has proposed a solution that takes advantage of depth data from mobile devices. One way this data that can be collected, is by using the widely available TrueDepth sensor available in the majority of new iPhones being manufactured today. This thesis focuses on researching how the depth data that is generated through the use of these sensors can be utilized effectively in PAD. It utilizes a new, TrueDepth-driven approach to PAD. The results produced in conjunction with this thesis contribute directly to the currently ongoing research on development of PAD methods for the future.

Sammendrag

Automatisk angrepsgjennkjennning ved ansikts-autentisering (PAD) er en viktig del av å kunne beskytte ansiktsgjennkjennings-systemer fra alvorlige potensielle sikkerhetsbrudd. I dag eksisterer et flerfoldig antall stabile, effektive og nøyaktige systemer for PAD. I dagens PAD-landskap er de beste PAD-algoritmene beregnet for bruk på RGB-bilder. I virkeligheten kan flere dimensjoner og faktorer enn et standard kamera tas i betraktning når et presentasjons-angrep blir forsøkt oppdaget.

Forskningen rundt hvor mye slik tilleggsdata kan påvirke prosessen av ansikts-basert angreps-gjennkjennning er i dag lite utforsket. Ikke en eneste offentlig-tilgjengelig artikkel har forsket på løsninger for PAD som tar dybde-data fra smart-telefoner i bruk. Slik dybde-data kan hentes direkte ut fra flere moderne telefoner, deriblant Apples iPhone, gjennom dens innebygde TrueDepth-sensor. Denne oppgaven tar for seg forskning rundt hvordan dybde-dataen som kan hentes fra denne typen sensorer kan effektivt brukes til PAD. Resultatet av denne oppgaven bidrar direkte til den pågående forskningen innen utvikling av fremtidsrettede PAD-metoder.

Preface

The bachelor's thesis "Smartphone Presentation Attack Detection using TrueDepth" has been written by Hamza Azim, Milosz Antoni Wudarczyk, and Kristian Amundsen Øhman-Norén. It is a bachelors thesis written as part of the Institute of Computer Science and Informatics, by the Norwegian University of Science and Technology. The thesis and its execution found place in the entirety of the Spring-semester of 2022 (Jan-May).

The project was issued by Mobai AS, a company working on modern solutions for biometric identification. They work on researching and developing solutions to automate authentication in a fast and secure way. Mobai utilizes presentation attack detection (PAD) algorithms to detect when presentation attack are being administered in human verification operations.

We would like to issue an extra special thanks to our supervisor, Kiran B. Raja, for his continued availability, support and supervision for this thesis and project. We owe a great deal of gratitude to his tireless work alongside us on this thesis.

Glossary

Attack Presentation Classification Error Rate(APCER) - Proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations in a specific scenario [1]

Bona fide presentation - Biometric presentation without the goal of interfering with the operation of the biometric system [2].

Bona fide Presentation Classification Error Rate(BPCER) - Proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario [2].

Equal Error Rate (EER) - value at which the Type I and Type II error proportions are equal. In the case of biometrics, EER corresponds to value where FAR equals FRR or in the context of presentation attack detection, APCER equals BPCER. The equal error rate can be not directly observable from the Type I and II error proportions but can require interpolation [3].

False Acceptance Rate (FAR) - Proportion of biometric transactions with false biometric claims erroneously accepted [3].

False Reject Rate (FRR) - proportion of verification transactions with true biometric claims erroneously rejected [3].

Neural Network (NN) - Network of primitive processing elements connected by weighted links with adjustable weights, in which each element produces a value by applying a nonlinear function to its input values, and transmits it to other elements or presents it as an output value. Whereas some neural networks are intended to simulate the functioning of neurons in the nervous system, most neural networks are used in artificial intelligence as realizations of the connectionist model. Examples of nonlinear functions are a threshold function, a sigmoid function, and a polynomial function [4].

Overfitting - generation of a ML model that corresponds too closely to the training data, resulting in a model that finds it difficult to generalize to new data [5].

PAI Species - Class of presentation attack instruments created using a common production method and based on different biometric characteristics [2].

Presentation Attack(PA) - Presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system [2].

Presentation Attack Detection(PAD) - Automated determination of a presentation attack [1].

Receiver Operating Characteristic(ROC) - Plot of the rate of false positives (i.e. impostor attempts accepted) on the x-axis against the corresponding rate of true positives (i.e. genuine attempts accepted) on the y-axis plotted parametrically as a function of the decision threshold [6].

Type I Error - Rejection of the null hypothesis when in fact it is true. A Type I error is an incorrect decision. Hence, it is desired to keep the probability of making such an incorrect decision as small as possible [7].

Type II Error - Failure to reject the null hypothesis when in fact the null hypothesis is not true. In fact, a Type II error is an incorrect decision. Hence, it is desired to keep the probability of making such an incorrect decision as small as possible. Type II errors commonly occur in situations where the sample sizes are insufficient to reveal a departure from the null hypothesis [7].

Table of Contents

Abstract	i
Sammendrag	ii
Preface	iii
Glossary	iv
Table of Contents	vi
List of Figures	ix
List of Figures	ix
List of Tables	xi
List of Tables	xi
Code Listings	xii
1 Introduction	1
1.1 Introduction	1
1.2 Background	2
1.3 Problem Description	4
1.4 Scope	4
1.4.1 Overarching Goal	4
1.4.2 Task Specification	4
1.4.3 Functional Specifications	5
1.4.4 Domain Model	6
1.4.5 Non-functional Specifications	6
1.4.6 Operational Specifications	7
1.5 Contributions	7
1.6 Thesis Structure	7
2 State of the Art for Presentation Attack Detection	9
2.1 Liveness cue based PAD methods	9
2.1.1 Motion based methods	9
2.1.2 Non-Intrusive motion based methods.	10
2.1.3 Intrusive motion based methods	12
2.1.4 Remote PhotoPlethysmography(rPPG)	12
2.2 Texture cue based methods	14
2.2.1 Static texture-based methods	14
2.2.2 Local Binary Pattern	15
2.2.3 Deep Learning Based Methods	18
2.2.4 Dynamic texture-based methods	19

2.3	3D geometric cue and pseudo depth based methods	21
2.3.1	3D geometry based methods	21
2.3.2	Pseudo-depth map-based methods.	21
2.4	Smartphone focused PAD methods	22
2.5	Multiple cues	23
2.5.1	Liveness cues and Texture cues	23
2.5.2	Texture and 3D Geometry cues	23
2.6	PW_MAD	23
3	Data Collection and Processing	25
3.1	iOS Depth Capture Application	25
3.1.1	Application	25
3.1.2	Requirements	27
3.1.3	Output	27
3.2	Datasets	27
3.2.1	Protocols	28
3.2.2	Dataset creation	28
3.2.3	Dataset expansion	29
3.2.4	External Datasets	30
4	Proposed Approach for PAD	32
4.1	Data processing	32
4.1.1	Main functionality	32
4.2	"PWD_PAD" repository	34
4.2.1	Implementation	34
4.2.2	Architecture	36
4.2.3	Plotting	36
4.2.4	RGB compatibility	36
4.2.5	Depth compatibility	37
4.2.6	RGB-D compatibility	37
5	Results and Experimental Analysis	39
5.1	Experiment protocols	39
5.2	Results	40
5.2.1	RGB based PAD	40
5.2.2	Depth based PAD	44
5.2.3	RGB-Depth based PAD	46
5.3	Discussion	49
5.3.1	Advantages	49
5.3.2	Limitations	49
6	Conclusion	51
6.1	Conclusion	51
6.2	Achieved Goals	51
6.3	Further Work	52
7	Organization	53
7.1	Meetings	53
7.1.1	Work Sessions	54

7.1.2	Supervisor Meetings	54
7.1.3	Task-issuer Meetings	54
7.2	Development Model	55
7.3	Summary of Development Phases	56
7.3.1	Planning Phase	56
7.3.2	Development Phase 1	56
7.3.3	Development Phase 2	56
7.3.4	Development Phase 3	57
7.3.5	Concluding Phase	57
7.4	Quality Assurance	57
7.4.1	Cooperative Efforts	57
7.4.2	Code Quality	58
7.4.3	Performance and Optimization	58
7.4.4	Structure	59
7.4.5	Documentation	59
7.4.6	Testing	59
7.5	Discussion	60
7.5.1	Scope	60
7.5.2	Work Environment	61
7.5.3	Group Composition	61
7.5.4	Security and Ethics	62
8	Development Process	64
8.1	Depth detection Module	64
8.2	Neural Network Implementation	66
	Bibliography	68
	Appendix	75
A	Original Task Specification	75
B	Group Contract	77
C	Project Contract	84
D	Confidentiality Contract	92
E	Project Plan	95
F	Meeting Summaries	105
G	Timetables	178
H	Depth Data Collection: Protocol	185
I	Depth Data Collection: Consent Form	187
J	Development Process: Micro-Movements	190
K	External Libraries & Dependencies	191
K.1	NumPy	191
K.2	OpenCV	191
K.3	PyTorch & torchvision	191
K.4	MediaPipe	191

List of Figures

1.1	Types of Presentation attacks [11]	3
1.2	Domain Model	6
2.1	Visualization of how the FDD algorithm functions [14]	10
2.2	This figure illustrates the OFL images obtained with a genuine face (a) in comparison with a photo attack (b). [15]	11
2.3	This figure illustrates blinking activity being given a numerical value that measures the distance between the eyelids. 0 is set for the threshold of them being closed, and negative for being open. [14]	12
2.4	This figure illustrates the process of segmentation of the facial regions and their processing through a selection of methods before classifying them to be genuine or fake. [27]	15
2.5	Segmentation of the facial regions. [27]	16
2.6	LBP Color space conversion. [13]	17
2.7	This figure illustrates the architecture of the deep learning network that was utilised in [47]	20
2.8	Using 2D landmarks to make 3D estimations [48].	21
2.9	Visualisation of the proposed motion stack method [51]	22
3.1	DepthCapture Application iOS User Interface	26
3.2	iOS process flow	27
3.3	Examples of behaviours in the protocol	28
3.4	Examples of captured bona fide images	30
3.5	Examples of captured PA (presentation attack) images	31
4.1	Development Model	33
4.2	Process flow of constructing RGB-D images.	33
4.3	Illustrated process flow based on depth mask face detection.	34
4.4	PWD_PAD neural network model	36
5.1	ROC curves of RGB based PAD tested against the KMH dataset with no edge-cases targeting RGB.	40
5.2	Examples of images which have been classified incorrectly for the models in Table 5.1	41

5.3	ROC curves of RGB based PAD tested against the KMH dataset with challenging cases targeting RGB.	41
5.4	Examples of images which have been classified incorrectly for the models in Table 5.2	42
5.5	ROC curves of RGB based PAD tested against the OULU dataset. . .	43
5.6	ROC curves of Depth based PAD tested against the KMH dataset with no edge-cases targeting depth.	44
5.7	ROC curves of Depth based PAD tested against the KMH dataset with challenging cases targeting RGB.	45
5.8	ROC curves of RGB-D based PAD tested against the KMH dataset with no challenging cases targeting RGB-D.	46
5.9	Examples of images which have been classified incorrectly for the models in Table 5.6	46
5.10	ROC curves of RGB-D based PAD tested against the KMH dataset with challenging cases targeting RGB.	47
5.11	Examples of images which have been classified incorrectly for the models in Table 5.7	48
5.12	RGB-D and RGB based PAD, tested against KMH dataset, with varying percentages of challenging cases targeting RGB	48
7.1	Development Model	55

List of Tables

5.1	Table containing BPCER 5%, BPCER 10%, EER threshold and the EER percentage for each trained model as well as the average, based on models in Figure 5.1	40
5.2	Table containing BPCER 5%, BPCER 10%, EER threshold and the EER percentage for each trained model as well as the average, based on models in Figure 5.3	42
5.3	Table containing BPCER 5%, BPCER 10%, EER threshold and the EER percentage for each trained model as well as the average, based on models in Figure 5.5	43
5.4	Table containing BPCER 5%, BPCER 10%, EER threshold and the EER percentage for each trained model as well as the average, based on models in Figure 5.6	44
5.5	Table containing BPCER 5%, BPCER 10%, EER threshold and the EER percentage for each trained model as well as the average, based on models in Figure 5.7	45
5.6	Table containing BPCER 5%, BPCER 10%, EER threshold and the EER percentage for each trained model as well as the average, based on models in Figure 5.8	46
5.7	Table containing BPCER 5%, BPCER 10%, EER threshold and the EER percentage for each trained model as well as the average, based on models in Figure 5.10	47

Code Listings

4.1	Depth data decompression	33
4.2	Depth data decompression	35
4.3	Convolution input layer supporting RGB-D	37

Chapter 1

Introduction

1.1 Introduction

Facial Recognition systems are widely used across border control, law enforcement, surveillance systems, and other parts of society where identification and authentication is needed. It has the potential of becoming the prime method of biometric authentication due to its non-intrusive nature, ease of use, and availability of sensors. Following the release of the iPhone X in 2017, Apple started discouraged using fingerprint as the main method of biometric authentication, in favor of depth-backed facial recognition [8]. Apple's position as a market leader pushed other companies to follow suit and implement their own facial recognition system solutions. Some simply added 2D facial recognition systems using RGB cameras, others contributed to the market with their own innovations, but the iPhone's TrueDepth-sensor is the one that has persisted through the years. Samsung implemented iris scanners whereas Huawei, OnePlus, Oppo, Google and Vivo implemented RGB based solutions. There has also been attempts of depth-sensors on varieties of mobile device competitors, using a depth-architecture referred to as "Time of Flight" [9]. As of February 2022, Apple's iPhone line holds 63.51% of total market share within Norway [10]. All iPhone models (other than SE line) released after 12th September 2017 opted to employ facial recognition as their preferred method of biometric security and come equipped with TrueDepth sensors [8].

Smartphones today are one of the most useful tools in the hands of a consumer. With these devices, a consumer has the expectation of being able to perform most tasks in a secure and convenient manner using biometric authentication. The task-issuer of this thesis, Mobai AS, is based out of Norwegian market and primarily provide smartphone based authentication services.

Despite face recognition offering convenience, the systems are often vulnerable to presentation attacks. This vulnerability does not exclude the services offered by Mobai AS, and detection of these attacks is important to ensure security. Images of a subjects face are often readily available on various internet-based platforms such as social media. These images can be used to create attack instruments, such

as printed images or replay images/videos, to attempt a presentation attack. If undetected, such attacks can heavily compromise facial recognition systems, and thus arises a need for Presentation Attack Detection (PAD). Presentation Attack Detection is Automated determination of a presentation attack [1]. A Presentation Attack (PA) is a presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system [2]. The main goal of these interference is to falsely authenticate a subject. The security and privacy aspects of the usage of this technology makes Presentation Attack Detection (PAD) more relevant than ever before.

This thesis has developed a presentation attack detection algorithm using the TrueDepth sensors available on iPhones. We make use of TrueDepth sensors for achieving higher security PAD systems as compared to using RGB images alone from iPhones. Presentation attacks can introduce distortions and alterations to the captured RGB images [11], [12]. With the usage of depth-data, these types of attacks could be detected with ease, compared to an system only using RGB-data. The nature of paper-based and display-based attacks are that the attack-images are printed/displayed on a flat surface. Therefore, by using depth, we hypothesize that PAD will be easier to uncover/detect these types of attacks.

In this thesis we research, and demonstrate the effect usage of the iPhone's TrueDepth system for PAD has on facial recognition. While the thesis primarily focuses on using depth information to increase accuracy and reliability of PAD-algorithms, we demonstrate the developed PAD approach can also be used to detect attacks using strictly RGB images.

1.2 Background

When using a smartphone to authenticate a user, one must have a level of trust to the end user. Low trust level becomes unacceptable in a high sensitivity application such as banking. Once authenticated into a mobile banking application, one would have access to banking information, taking out loans, block and replace credit cards and transfer money. This can lead to life-ruining consequences for the target, if subject to a authentication-based attack. Therefore, when authenticating a user into a mobile bank solution, we need to be absolutely certain that the user are legitimate and securely authenticated.

With an unsupervised smartphone, if an attacker has access to an image of a target, one could potentially gain unauthorized access to the target's accounts and perform actions that the target does not wish to happen. To prevent these attacks, Mobai AS, is working to develop a solution that can lead to a high grade of certainty when verifying a user. To be able to stop such attacks, one must detect and prevent various types of attacks that may frequently occur.

Figure 1.1 illustrates the different types of presentation attacks one may encounter in such a scenario. These can be split into two main sections such as 2D attacks and 3D attacks. 2D attacks can be either in still image form (photo) or in video form. Photo attacks can further be divided into two main vectors- Print and

display attacks. Print attacks are defined as images of a person that have been printed out by an impostor that is trying to impersonate them. One must also take into account that there are multiple types of printers and printer paper that may be used here, and some may be more effective in bypassing PAD algorithms than others. The impostor may also create the printed images with eye region visible to fool the PAD systems using eye gaze functions, or wrap the mask around their actual face in order to seem more legitimate[11]. Another form of 2D attack would be to play a video through a mobile phone, laptop or tablet to imitate the movements of a real person. Video replay attacks are a more complex form of 2D attacks. They introduce more intrinsic information such as eye blinking, and replicate human movements to a much greater effect than simple images to mimic liveliness. [13].

3D attacks are much more complex and difficult to perform. They require that the impostor wears a mask in the attempt to fool the PAD systems or warp the image around face region. These masks can be divided into two primary parts - rigid and flexible. Rigid masks are more accessible than ever before, and can be easily created using cheap 3D printers. One could simply print such a mask and paint it to impersonate the target. A flexible silicone mask on the other hand is much more expensive and difficult to produce. These are, however, also some of the best at fooling some PAD systems [11]. A 3D mask is able to reconstruct facial artifacts more realistically. The silicone based face masks can be challenging to detect using PAD algorithms [13] due to these factors. Due to the aforementioned market share of iPhones with 3D sensors, presentation attacks using 3D masks can be foreseen to increase, in near future creating the need for better PAD systems.

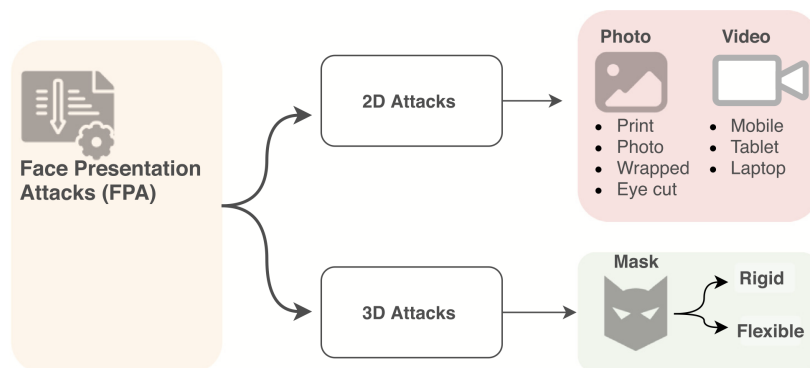


Figure 1.1: Types of Presentation attacks [11]

1.3 Problem Description

Detection of attacks of facial-based biometric authentication systems is considered to be the main problem area for this task. The thesis focuses on creating a PAD system for detecting 2D printed and replay attacks using TrueDepth data from Apples mobile devices, specifically the iPhone. In addition, the thesis also considers warped 2D attacks, and simulates various attacks and how these can be detected by utilizing deep learning with TrueDepth-data.

Within the area of PAD for smartphones, we focus on unsupervised setting where the user is allowed to use the smartphone based biometric authentication anywhere. First and foremost, the mobile and unsupervised aspect of smartphones assume the potential for a variety of environments. In certain environments this can cause difficulties to detect presentation attacks, as the clarity and quality of the captured image might not be optimal. Less optimal conditions leads to a facial authentication system in a compromised state, if no proper mitigation-measures are present.

We are thus expected to develop a system which can detect presentation attacks at various levels of complexity and implementing the detection algorithms. The focus of the task is to increase the robustness of the already-existing PAD-system of Mobai AS application, by developing a package that explores new implementations and methods for PAD.

1.4 Scope

1.4.1 Overarching Goal

The goal of this project is to develop a working prototype package for presentation attack detection, that can be utilized by the task issuer within their mobile authentication application. The product should also be usable in other products of which the task-issuer delivers, but this specific package will focus on the verification-side of the business. The package should be able to effectively and quickly perform presentation attack detection using new methods of attack detection.

1.4.2 Task Specification

The specified task of the project defines its main goal. The main task description describes: "Use computer vision to create prototypes for attack detection" (Appendix A). It further describes that the task is to create prototype(s) based on one or more of a pre-set of concepts that exist within the topic of presentation attack detection. These concepts are defined as: Micro-movements, Eye-gaze, and Depth-detection.

After deliberation and discussion with the task-issuer of the project, the task was further refined. The specifications gathered after these deliberations are rooted in increasing robustness within the already-existing presentation attack detection

software of the task-issuer. The topics mentioned in the task specification are all challenging topics, and we decided to focus on developing a PAD system that utilized TrueDepth data for PAD.

This topic is not only new to the task-issuer and their software, but also a fairly unexplored topic within presentation attack detection in general. The main reason is the vendor specific way of using depth sensors to obtain depth-data is not widely explored within most modern mobile devices.

In addition to this, the task was specified with implicit focus on operability on mobile devices with respect to time, execution and resource usage. The developed package would further be specified to work on mobile device data.

1.4.3 Functional Specifications

The function(s) developed over the course of this project shall:

- Implement prototype functions of presentation attack detection utilizing one, or more, of the following aspects:
 - Micro-movements between background and subject
 - Eye-gaze of a subject
 - Depth-Data from mobile device (TrueDepth (iOS) or Time Of Flight (Android))
- Iterate over a set number of sequential frames of a video from a front-facing smartphone camera, and use this data to determine if a presentation attack is happening or not.
- Present an output that describes the probability rate of attack detection during facial biometric authentication attempts.

1.4.4 Domain Model

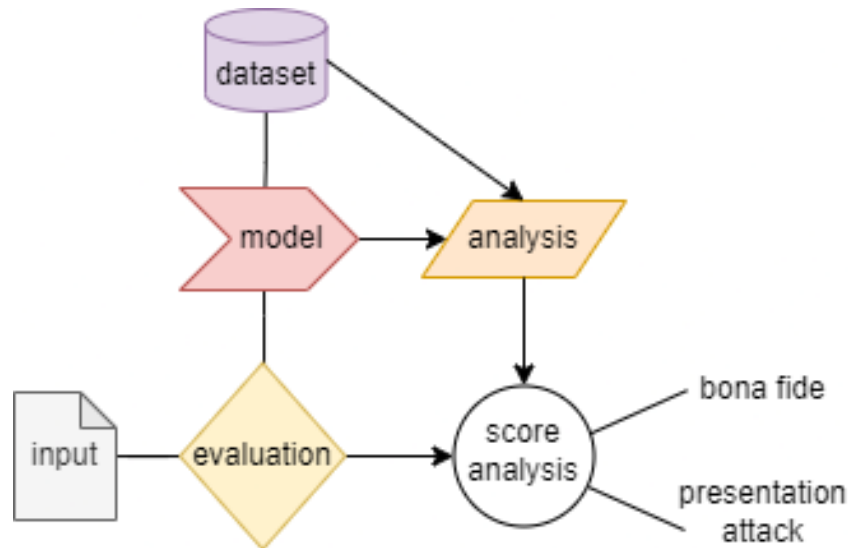


Figure 1.2: Domain Model

1.4.5 Non-functional Specifications

The non-functional specifications are defined by the principles of operations, of which the main package shall follow to ensure flexibility, modularity, and operability.

The package is developed with a multitude of non-functional aspects in mind. These aspects include:

Performance - You: The package should perform such as not to impede, stagger or slow the operation of the main application. This is ensured through multiple methods, which all have been thoroughly tested.

Security and Privacy - The package shall follow security principles, which ensure secure processing of highly sensitive data. All operations within the project shall also ensure laws and regulations of privacy, like the General Data Protection Regulations (GDPR), are upheld.

Usability and Maintainability - The package itself is developed with the same programming language as the task-issuers already-existing software. This ensures ease of usability, as the compatibility will automatically integrate and translate to the task-issuers already-existing operative application. Maintainability is ensured through thorough documentation and structure, which is included in both the source code (as pydoc), and in addition other documents (ReadMe). The code structure is built upon a foundation of programming standards. This includes, but not limited to, class-structure standardization, loose coupling of operations and high cohesion of functions.

Reliability - For this thesis, this related mostly to the idea of sturdiness. The package must be reliable enough to not hinder the operations of the full application of the task-issuer. This aspect is ensured through thorough and continuous testing.

1.4.6 Operational Specifications

The package is, as previously described, scheduled to be included as a part of an already-existing system for presentation attack detection. The package exists as a set of functions that each serve one method of the topics described above, and is programmed in the desired programming language, python, as expressed by the task issuer. The operational specifications themselves are locked behind a wall of confidentiality. The task-issuers main application is something the group has not gained access to, and therefore know little about.

1.5 Contributions

The thesis has made multiple contributions to the field of PAD. Most notably by demonstrating the utility of information collected by the TrueDepth cameras that are available on iPhones. Notable changes were also made to assist with the usability of an open source project which allows for the extraction of TrueDepth data. Further, an adapted PAD algorithm that utilizes this TrueDepth data in conjunction with RGB-imaging to create an end-to-end PAD system can be defined as another important contribution. This system is able to perform PAD on standalone RGB images, standalone depth images, in addition to images that are a combination of the two. Finally, noting the lack of availability of datasets with depth information, this thesis also contributes a new dataset which contains both RGB and TrueDepth data. The new “KMH” dataset counts 50 unique subjects and contains 198 bona fide video samples and 150 presentation attack samples. All of these samples also contained a matching TrueDepth layer. 8 of these subjects were asked to participate as “Challenging cases”. These samples were taken in sub-optimal conditions (imperfect lighting, dark background, etc.). These samples totaled 32 bona fide and 24 attacks.

1.6 Thesis Structure

The thesis is structured in a logical way. Firstly, the scientific research and development is focused on in Chapter 2. This chapter provides a look at what the current state of the art methods for PAD consist of. This chapter lays a foundation for the main topic of the thesis.

Further, Chapter 3 and Chapter 4 present a comprehensive look at the technical design and implementation of both the data collection-part of the project, as well as an in-depth look at the proposed PAD-solution developed through the

project. Then, the results of the experiments conducted as part of the project shortly follow. Complete with commentary and discussion, which can be found in Chapter 5.

Then, to assure continuity, the thesis presents the conclusion in Chapter 6 thereafter. This is to highlight the results that were found, and discussed, in the chapter previous. Lastly, there are two chapters containing organizational aspects of the thesis project, and discussion of important topics in regards to project execution. Lastly, in Chapter 8, the development process for the project is described in detail. This is done in chronological order, and is there to give a broader image of the processes that happened throughout the project, and how we ended up with the results we got. These two chapters have been placed last, after the conclusion, to ensure the thesis could be read like a research-topical article (Chapter 1 to Chapter 6), while also allowing the group to share organizational aspects of the project without it interfering with the research this thesis presents.

Chapter 2

State of the Art for Presentation Attack Detection

This chapter serves as an overview of the development within the field of PAD. It achieves this by highlighting some of the more noteworthy advances in the field, in a chronological manner. This chapter also outlines various methods of PAD that are currently utilized, and how they relate to the thesis and its contents. This includes the State of the Art framework of which the thesis bases itself on.

2.1 Liveness cue based PAD methods

Liveness cue based methods were some of the first methods developed for PAD. These methods attempt to detect the dynamic physiological signs of life in an image. This includes eye blinking, facial expression changes, mouth movement and changes in facial expressions [13]. In addition to these movement based methods, rPPG or *Remote PhotoPlethysmoGraphy* is another method which detects pulse beats in order to detect whether or not there is a legitimate person behind the camera. These methods can be classified as intrusive or non-intrusive, depending on whether it acts independently of the subject of authentication (non-intrusive) or if it requires human interaction to authenticate a subject (intrusive).

2.1.1 Motion based methods

Motion based methods can effectively detect static presentation attacks such as most photo attacks, since these do not contain any dynamic information[13]. On the other hand, motion based methods are not nearly as effective against video replay attacks. These contain signs of liveness such as eye blinking, head movements, facial expression changes and so forth. For this reason, interactive motion based methods were introduced. With these, the user is prompted to perform an activity or a series of activities to verify their legitimacy. These actions include head movement, eye blinking, mouth opening, etc. Motion based methods are more effective

at detecting video attacks, but are often more intrusive for the user. Based on this fact, these methods are classified as intrusive to the subject.

2.1.2 Non-Intrusive motion based methods.

In 2004, non intrusive liveness based methods were developed by Li et al. [14] to detect photo based presentation attacks. Here the authors proposed to use a method called Frequency Dynamic Descriptor(FDD). This is shown in 2.1. This figure illustrates how the FDD algorithm sees a live face (A being the face and C how the algorithm interprets it) in contrast to how it sees a PA(Fig B displaying the PA, and Fig D displaying how the FDD algorithm sees it). The FDD would be calculated by using a 3 step solution- extracting every fourth image in the given set of data, for each image an energy value of t is defined using an equation, and finally calculating the standard deviation of the resulting flag values. This will give the FDD of the given image set [14]. This method is not very computationally expensive.

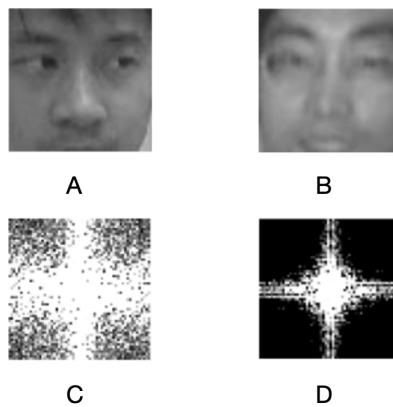


Figure 2.1: Visualization of how the FDD algorithm functions [14]

A technique for evaluating liveness meant to work directly within RGB color spaces was developed by researchers in Halmstad University[14], [15] from 2005 to 2007. This team developed a non- intrusive method to detect the differences in motion patterns between 2D planar photographs, and 3D legitimate users. These authors proposed the use of Optical Flow Lines(OFL). This process is illustrated in 2.2. In the figure, motion is illustrated with dark pixels and stillness with white. One can observe that in the photo attack, constant movement is present. Through their testing and produced results, this technique seems to be incredibly effective in PAD. Using a limited data set of 200 live and 200 non-live images, this method claims that 'No live sequence scored below 0.5', and only having 3 non-live sequences that scored the same. All other live sequences achieved a greater

liveness-score and vice versa for the non-live sequences. This concludes to an error rate of 0.75% in their first paper[14]. With continued development, however, the authors were able to improve the results. Using a greater database of 400 each live and non-live images to base their testing on, their Equal Error Rate(EER) fell to 0.5%. The same technique was used in another paper in 2009 [16]. The authors do note that most video replay attacks will successfully fool this PAD solution in addition to it being ineffective when the subject is wearing eye glasses. All OFL based methods are also susceptible to changes in illumination levels.



Figure 2.2: This figure illustrates the OFL images obtained with a genuine face (a) in comparison with a photo attack (b). [15]

Eye blinking was suggested as a method to distinguish between a face and a facial photo in 2007 [17], [18]. As eye blinking is a physiological behavior that occurs approximately 15-30 times per minute [13]. This will make it so that almost all consumer grade cameras will be able to recognize this behavior. The threshold to be able to consistently identify eye blinking was evaluated at being at least 15 frames per second. Through use of complex mathematical functions for image processing to assign values to the eyes, the authors proposed a method using Conditional Random Fields(CRF) that proved to be more effective than the previously used Hidden Markov Model. This is due to the CRF model taking into account a larger number of dependencies. The method assigning a 'blink' value to an eye can be illustrated in figure 2.3. This method, like all other eye-blinking based methods is effective against printed photo attacks. However, is susceptible to eye-cut attacks, video replay attacks, masks and all others that have the ability to simulate blinking.

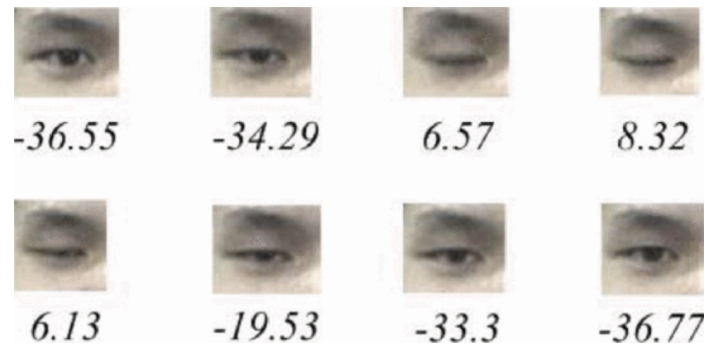


Figure 2.3: This figure illustrates blinking activity being given a numerical value that measures the distance between the eyelids. 0 is set for the threshold of them being closed, and negative for being open. [14]

2.1.3 Intrusive motion based methods

Intrusive methods (or interactive methods) utilize a challenge that the user must complete to prove their legitimacy. This can include but is not limited to blinking, smiling, turning their head a certain way, giving a facial expression or uttering a word or number that has a predictable mouth movement.

Kollreider et al. [19] first proposed an interactive method in 2007 that could effectively detect a subject's legitimacy. This method proposed the subject to utter a sequence of randomly generated digits. It used the same method of optical flow lines previously mentioned and illustrated figure 2.1. This method could both detect a face and the mouth movement by using these aforementioned OFLs.

It is also noted in the paper written by Ming et al. [13] that emerging deep-fake technology can be a challenge for emerging intrusive methods. These are becoming increasingly available for the general public. Deep-fakes can realistically stitch a 3D map of the target onto an attacker's face to easily recreate the tests created by these intrusive algorithms. However, to combat this, recently there has been an advancement in detection against video attacks. This method is known as Remote PhotoPlethysmoGraphy(rPPG) and were first developed in 2016.

2.1.4 Remote PhotoPlethysmoGraphy(rPPG)

rPPG methods can detect blood flow in the face using only RGB images in a non intrusive way. they use the way that light penetrates and reflects off of the skin to analyze the legitimacy of the end user. Photo, video and mask attacks font have a natural periodical variation in the rPPG signal that they emit. However, high quality video replay attacks with good recording conditions and high screen quality can also display this periodic variation. Some thin high quality masks may also be able to replicate the natural rPPG variation in a 'real person'.

The first rPPG methods were developed in 2016 by Li et al. [20]. The method used by the authors of this article was to first identify an area of bare facial skin such as cheeks, nose, mouth and chin since the forehead and eyes may be obscured by either glasses or hair. With cardiac pulse, the color value of facial skin will change. This method will take the raw value of the pixel in each channel inputting the values as R(raw), G(raw) and B(raw). The reason that bare skin will change color with blood flow is that the capillaries within will carry blood to the face as the heart pumps. The authors of this paper used Local Binary Patterns (LBP) as a baseline to compare their results to. LBPs are further explained in Section 2.2.2. They used a variety of different data-sets to ensure quality in their final product. The authors conclude that the final product is robust against high quality 3D mask attacks where LBP is ineffective in comparison. In addition, it is able to maintain its performance against print attacks. It is yet ineffective against video attacks. The authors conclude by proposing LBP be used as a complementary PAD algorithm. Combination of multiple algorithms will be further discussed under the multiple cues section (Section 2.5) later in this paper.

Another novel rPPG based method was proposed in 2016 that exploited the characteristics of rPPG data that was extracted from 3D face masks. In comparison to the aforementioned method, this one has 3 key differences[13]. These are:

- rPPG signals are extracted from multiple facial regions rather than just the lower face region.
- The correlation of any two regions were used as a discriminative feature by assuming that the heartbeat is consistent. Robust regions that contain a consistent heartbeat signal are emphasized, and regions with weaker heartbeat signals are weakened.
- The now weighted signals are fed into a support vector machine to detect 3D mask attacks[13].

In 2017, "PPGSecure: Biometric presentation attack detection using photoplethysmograms" was proposed by Nowara et al. [21] as an improvement to already-existing rPPG methods. This is another rPPG based method that used local rPPG signals. This method used a similar framework as the first proposed 2017. The rPPG signals are extracted from three facial regions in addition to two background regions. One from the left and one from the right side of the face. The background areas are used for elevated robustness against noise due to variation in light levels that may effect it. The calculated noise is subtracted from the facial regions to achieve this effect. This information is then again fed into a support vector machine. The rPPG signals used by PPGSecure are more effective than the previously mentioned rPPG methods proposed by Liu et al. [22] in some data-sets.

A deep-learning based approach was proposed in 2018 by Liu et al. [23]. This method also combined the rPPG estimation with 3D geometric cues. This was done to tackle photo attacks and 3D mask attacks, in addition to the video replay attacks all previous rPPG methods were susceptible to. There will be given more

detail in the multiple cues section (Section 2.5) of this report.

A method for predicting the presence of Deep-Fakes was proposed in 2019 by Fernandes et al. [24]. This model uses bona fide images to train a model, and then use this to predict the heart rate of a deep-fake. The authors were able to develop a novel approach to detect the heart rates of deep-fake videos due to thousands of epochs of training their algorithm.

A more sophisticated method was proposed in 2017 by Ciftci et al. [25]. This method used multiple biological cues instead of only rPPG signals that were then fed into a deep convolutional neural network to discriminate against legitimate users and deep-fakes.

2.2 Texture cue based methods

Texture cue based methods are some of the most popular PAD methods. This is because they are non-intrusive and capable of detecting almost all known types of attacks such as photo, video and even some mask attacks. Where liveness cue based methods rely on aspects such as blinking, mouth movement and blood flow, in the case of rPPG based methods, to detect *HOW* alive a face is. Texture based methods can narrow it down to a binary identifying whether or not a face is alive. Texture cue based methods can also be further split into their respective subcategories: static texture-based methods and dynamic texture-based methods. The static methods mainly extract spatial or frequency features of a similar image where the dynamic methods explore spatio-temporal aspects of entire sequences of video.

2.2.1 Static texture-based methods

The first attempts at using static texture based methods for PAD were developed in 2004, by Li et al. [14]. This method used the same fourier spectra that was illustrated in Figure 2.1. However, the texture based part of this proposal relies on high-frequency descriptors. This would then create a fourier spectra that is used to illustrate realness.

The idea of faces having a unique reflection pattern was explored and modeled in 2010 by Tan et al. [26]. The authors were able to model the reflective patterns of a genuine alive face and print attacks. The main idea behind this project was that the print attack face is more likely to have more distortions than the genuine alive face. The authors tested several classifiers. Among these were Sparse nonlinear Logistic Regression (SNLR) and Support Vector Machines (SVM). Of these, SNLR proved to be the more effective.

In 2011 a method was proposed to analyze the micro textures within the image by using Bidirectional Reflectance Distribution Functions(BRDF). The relevant values from the original image are extracted and plotted onto a histogram. The gradient of this is used to identify a alive image vs. an impostor image. This method is especially effective against detecting photo print and video attacks.

2.2.2 Local Binary Pattern

Local Binary Pattern or LBP is one of the most widely used algorithms and comes with multiple advantages. One of the reasons for the popularity of LBP is its robustness against illumination changes. LBP is an incredibly efficient method for texture feature extraction. This method transforms the image into an array or image of integer labels that describe how the image appears in each of these regions. The pixels are divided into arrays where the value of each is compared to the central threshold to extract the texture features. The basic operation of the LBP function is illustrated in figure 2.4.

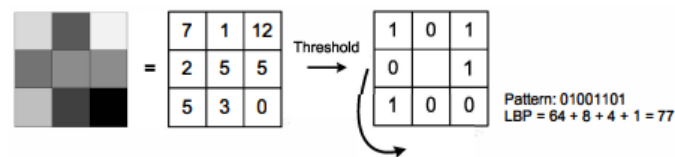


Figure 2.4: This figure illustrates the process of segmentation of the facial regions and their processing through a selection of methods before classifying them to be genuine or fake. [27]

The first proposal to use LBP as a PAD method was by Määtä et al. [28]. In the proposed method, the facial region of a subject was extracted into a 64x64 image. After this operation, two LBP algorithms were ran on it. These were to output their data as histograms. The culmination of the data in these histograms was to then be run through a SVM classifier to detect the presence of photo or video attacks. The authors also note that this method is much more effective than the previously proposed method of using reflection patterns, outlined by Tan et al. [26]. The authors use the same dataset as the report utilizing reflection patterns [26] to find that the LBP based algorithm is significantly more effective in comparison. Both authors report findings using Area Under Curve(AUC). The reflection based method [26] reports a AUC result of 0.94 where the LBP based method reports a result of 0.99.

The same authors extended their work in 2012 [29]. Through this work they added two more texture features- Histogram Oriented Gradients(HOG) and Gabor Wavelets. In conjunction with the previously proposed LBP PAD technique, the PAD method was only made more robust. In this method, each output is sent into a separate linear SVM. The fusion of the scores from the three SVMs is applied to generate a final decision as to whether or not an attack is taking place.

The same authors further continued their research in 2013, by proposing to use the upper body region in addition to the facial region to attempt to spot an attack in a paper on context based anti spoofing [30]. To achieve this, they created a cascade of the upper body region and a spoofing medium detector based off of histogram of oriented gradients and the linear support vector machines from the

previous proposal. This method achieved fantastic results especially against video-centric attack vectors. However, the authors note that this method is specialized against specific attack scenarios and can not rule out all vectors of attack. This method is also especially effective against poorly performed PAs.

The same year, another method was proposed by Yang et al. [27]. This method takes a different approach to the classification method. The authors propose to first isolate the face into the regions that are the most important in modern PAD-algorithms - right and left eye, nose and mouth. Then the face contour region and the original image are divided into 2×2 images to obtain 8 more images. These are then fed into different texture features such as LBP, HOG and Local Phase Quantization (LPQ). Each component has low level features extracted. A high-level descriptor of these components is then extracted to create a histogram of these representations which is finally fed into a SVM to detect PAs. This method is further illustrated in figure 2.5. This figure illustrates the process of segmentation of the facial regions and their processing through a selection of methods before classifying them to be genuine or fake.

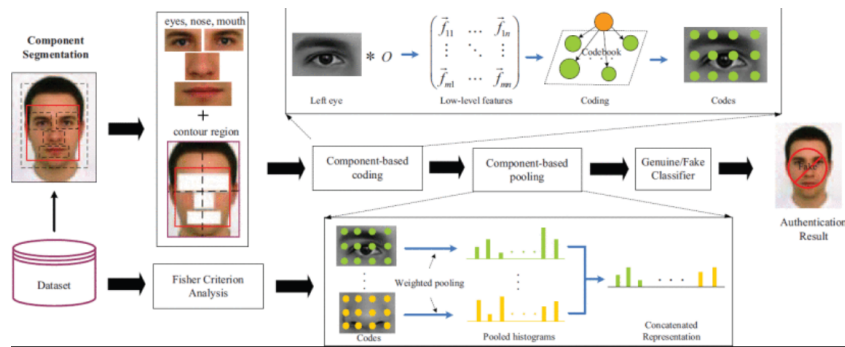


Figure 2.5: Segmentation of the facial regions. [27]

The first methods for attempting to detect 3D mask attacks using LBP were proposed in 2013 by Kose et al. [31]. The authors also developed their own 3D mask database due to the lack of available 3D mask databases. In addition a depth based method to detect such mask attacks was also developed, but the authors concluded that LBP was more effective. The same authors then later proposed in their paper [32] to use combination of depth data and LBP to more effectively detect 3D mask attacks.

Image Quality Assessment (IQA) was first proposed as a method in 2013 and 2014 by Galbally and Marcel [33], then later after being joined by Fierrez [34]. This method makes the assumption that if a video or photo replay attack is being performed, it should have a different quality to the real sample as the image was captured twice and run through 3 mediums before being processed. These being the initial camera that takes the image, the medium used to perform the present-

ation attack, and finally the camera being used by the device taking the image. In contrast, a genuine attempt would only use the final camera as a medium. This could for example lead to structural distortions or inconsistencies in sharpness and contrast. These papers adopted a set of image quality measures- 14 in [33] and 25 in [34]. The individual scores were then combined into a singular image quality vector and fed into a Quadratic Discriminant Analysis(QDA) classifier. IQA is a method with potential within "multi-biometric" methods and can be used in iris and fingerprint PAD as well. The authors do note however that within their testing, it does not seem to perform as well as other texture based PAD systems.

Work on IQA based methods was continued later in 2015 by Wen et al. [12]. This method proposed to work completely within all RGB color-spaces. The purpose of this function bases itself in analysis of the chromaticity and color value, and diversity in the Hue, Saturation, Value(HSV) space. With a low input resolution, this can be difficult to detect, but this is what the method relies on. The imperfect color reproduction of printers and LCD screens means that there is a lower color diversity in a screen or a printed image than there is present in the image-capture of a bona fide human being. This method utilized a 121 dimensional image distortion feature that consisted of 101 dimension color diversity feature, a 15 dimension chromatic movement feature, a two dimension blurriness feature, and a three dimension blurriness detection feature. The output from these was then fed into two SVMs. One for photo and one for video attacks. This method shows promising results when compared to other texture based PAD methods.

One of the more interesting developments in the history of PAD was made in 2015 by Boulkenafet et al. [35, 36]. The authors used LBP to extract features in the HSV and YCbCr color spaces. Simply by utilizing different color spaces, LBP algorithms were able to achieve state of the art levels of performance. Even when compared to Component Dependent Descriptors and Convectional Neural Network reliant PAD methods. This work showed the possibilities of utilizing multiple color spaces for use in PAD. This method is further illustrated in Figure 2.6. This figure illustrates the process of converting the original image into multiple color spaces and then using LBP and SVMs to perform presentation attack detection.

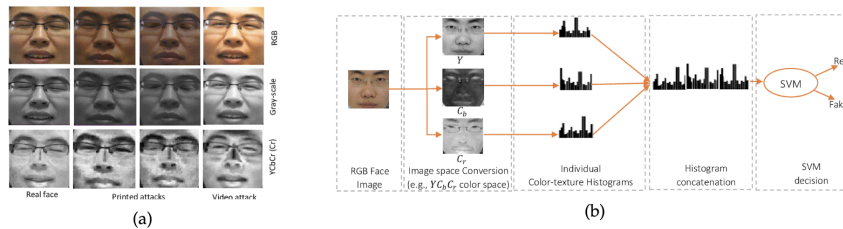


Figure 2.6: LBP Color space conversion. [13]

2016 was an equally eventful year in the development on PAD methods. The first method of smartphone focused PAD was proposed by Patel et al. [37]. The authors utilized multi scale LBP in conjunction with image quality based color moment features [13]. These were then turned into a singular vector that was fed into an SVM. In addition, a new strategy was proposed- To quickly filter out poor attacks before employing the more sophisticated SVMs to find out whether an attempt is legitimate or not. The authors also proposed to attempt to detect the bezel of the vector of the attack such as the white bezel of the paper or a black bezel around a screen in addition to the inter-pupillary distance(IPD) of the face in the image. The IPD will be used to see if an attempt will even be accepted at all. If the IPD is too large(The face is too close to the camera) or too small (face too far from camera), then the authentication-attempt will be rejected. This will also ensure to a great extent that the potential bezel will be detected as well. The bezel detection checks if for example the pixels stay relatively consistent for 50-60 pixels on all 4 sides. If so, the attempt will be marked as an attack. The threshold for qualification of a bezel will however vary depending on the IPD as well. This will successfully filter out 95% of the poorest attacks [37]. On the other hand it may also generate a large number of false positives if the user is for example wearing a black tshirt in front of a black background, white in front of white etc.

2.2.3 Deep Learning Based Methods

In recent times there has been a spike in popularity of deep learning based methods of PAD. Here the researchers focus on designing neural networks that are better suited to learn the best texture features rather than designing texture features that are more advanced as was done in the previous methods.

in 2014, the first proposed method for using convolutional neural networks(CNN) was proposed [38]. This method used the AlexNet[39](a 1000-way softmax) network in a different way than what is common nowadays. It set a binary classification to a SVM to decide if the attempts made are real or fake, and replacing the hand crafted features that were previously present with the features that AlexNet was learning. This method proved to be more effective when the image was enlarged to 1.8-2.6x the face area, reiterating the findings in previous works that show that adding more contextual information to the input will lead to a result that is more likely to be correct[27, 30]. CNNs were proven to be effective against PAs. This method surpassed almost all state of the art methods for photo and video replay attacks. This led to the following research-wave on CNN-based PAD systems.

The first end-to-end DL-framework made for PAD was proposed in 2016 - CaffeNet [40]. Based on one-path AlexNet [39], CaffeNet was a 2 way softmax-function that replaced the earlier 1000 way softmax of AlexNet to a binary classifier - genuine or fake. The authors of CaffeNet trained two separate CNNs that would work together to more effectively perform PAD. One was trained on aligned face images, and the other on enlarged images that included some of the back-

ground behind the subject. These CNNs then each voted on whether or not the attempt made was genuine or not. This method surpassed all existing state of the art systems that existed at the time.

In 2018 a method to detect PAs through detection of noise in an image was proposed [41]. This method identified PAs that were made up of two parts- The original RGB-image, and the noise. Noise can include but is not limited to: blurring, reflection or a moiré-pattern. This work estimated the noise in a genuine image to be zero. Thereby, presentation attacks could be detected by analyzing an image for the amount of noise that is present. To estimate the noise in each image, a Generative Adversarial Network (GAN) based CNN was used. This method showed superior performance when compared to other state of the art works such as [23]. The authors also claimed that this method could be used to detect makeup attacks by assigning makeup as a noise type.

In 2019 a new method was proposed- using Deep Pixelwise Binary Supervision(DeepPixBiS) based on DenseNet [42]. This method assigns a 1 or 0 value for each face pixel deciding on each whether or not it is genuine or fake, and then takes the mean value of all of the pixel values to then decide whether or not the image is genuine or fake. This method shows a promising result for both photo and video attacks.

2.2.4 Dynamic texture-based methods

Dynamic texture based methods differentiate themselves from static texture based methods by extracting spatio-temporal features using a sequence of images and analyzing them instead of extracting spatial features from single images.

The first method that utilized dynamic LBP was proposed in 2012 and 2014. This method was called LBP-TOP(three Orthogonal planes). This method took into account time alongside the traditional x and y coordinate calculations that were performed. The LBP function is applied to each of these. As with most of the earlier motioned LBP based methods, the result is then fed into a SVM. These authors continued their work in 2013 [43]. Among the proposals from this later work, they suggested using more and varied data sets to train their model. Another suggestion was to use a score based system where the model was trained on each dataset. Then the normalized score off each output would be used as the final output. The main drawback of the second proposed method is that if a new attack type is discovered, they must retrain the machine to be able to detect it.

A method to use motion magnification was proposed in 2013[44]. This method will enhance the motion available in an image beforehand. The authors claim that motion magnification will enhance the amount of texture available from the optimized video. The authors utilized a pre-existing method called Histogram of Optical Flows (HOOF). HOOF was made to calculate the optical flow vectors between frames of a video at fixed intervals. HOOF is less expensive computationally than LBP-TOP. The greatest drawback of this method however is that it needs to collect a very large number of frames(<200). Therefore this method is not reasonable in

commercial use.

A similar method was proposed to use the Fourier spectra of a video rather than the optical flow lines present in 2012 and 2015 [45, 46] in a similar fashion to the aforementioned paper by Li et al. [14]. The objective of this method was to try and identify the amount of noise caused by a PA. LBP and HOG can then be used on the filtered image's rhythm of the texture features and then fed into a SVM. The objective here is to capture the noise introduced by a presentation attack such as the moire effect.

Deep Learning was first proposed as a method for PAD in 2015 by Xu et al [47]. This method utilized deep learning to extract the spatial texture features of a frame. These frames are then sampled from the input video using a time step. The architecture of the deep learning model was based on long short-term memory (LSTM) in addition to CNNs. The outputs from the LSTM of each CNN branch was used to learn the temporal relations between frames. The outputs of the LSTM units then connect to a softmax layer that finally outputs the PAD classification for the frame. The authors note that excluding unnecessary information (in this case image pixels outside of the facial region) can assist the PAD method. The architecture of the deep learning network is illustrated in Figure 2.7.

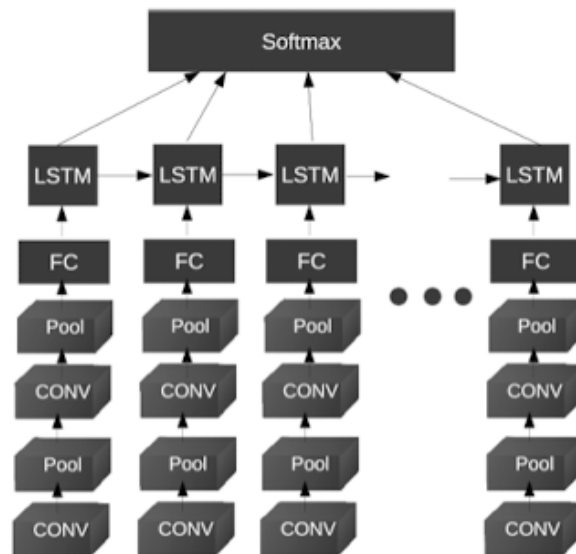


Figure 2.7: This figure illustrates the architecture of the deep learning network that was utilised in [47]

2.3 3D geometric cue and pseudo depth based methods

These methods use 3d geometry based cues to discriminate between genuine faces and attacks. They aim to detect the 3D figure of a face and distinguish it from a 2D planar presentation attack. Theoretically, these PAD methods should be incredibly effective against 2D photo and video attacks. The most widely used method for achieving this is by using the 2D images captured by the RGB camera to attempt to create a 3 dimensional map of the face.

2.3.1 3D geometry based methods

A 3D geometry based method to detect photo attacks was proposed in 2013 by Wang et al. [48]. This method used 2D facial landmarks to reconstruct the 3D structure of the face. The 3D reconstruction of a genuine 3d face and a 2D image of a face are very different in this method as illustrated in Figure 2.8. This figure shows how the method utilizes the facial landmarks to make an estimated 3D map of the face. As shown in Figure 2.8, the reconstructed 3D structure of a genuine face in comparison to a 2D photo attack is apparent. These 3D coordinates are then fed into a SVM that determines whether or not it is a presentation attack. This approach is however flawed. it requires multiple viewpoints of the face in question to be able to draw a realistic 3D map instead of being able to use a single image. Not having enough frames available can lead to inaccuracies. In addition it is susceptible to inaccuracies in the detection of facial landmarks that are to be used in plotting the 3D coordinates for the face.

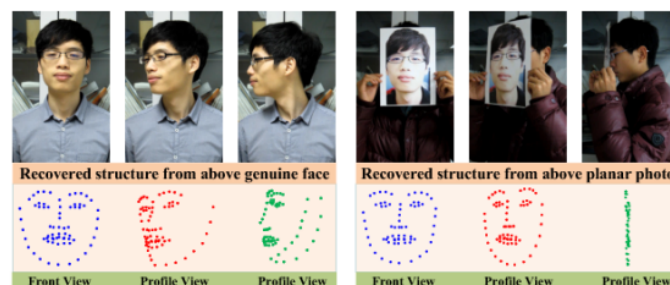


Figure 2.8: Using 2D landmarks to make 3D estimations [48].

2.3.2 Pseudo-depth map-based methods.

When using 3D sensors, the depth map of a face image can be captured directly. However, it is possible to calculate or estimate the depth map of a face image using 2D sensors, by utilizing concepts from computer vision in conjunction with deep learning. The forms of these that we are most familiar with may be facial filters on smartphone applications such as Snapchat, Instagram and Facebook Messenger.

On its own however, pseudo depth is not the most effective PAD method and is often used in conjunction with other methods.

The first proposed method that utilized pseudo depth for PAD came in 2017, proposed by Atoum et al. [49]. This method was designed to detect video replay attacks and printed photo attacks since the depth map of a face has varying height values where a flat surface of a screen or piece of paper does not. An 11-layer fully connected CNN was used in this work. The authors estimated the ground truth of a face image using a state of the art 3D face model fitting algorithm, and set the value for a planar attack to be 0. The estimated depth maps were then fed through an SVM that was trained using the ground truth to detect planar PAs.

Face Anti-spoofing Temporal-Depth networks (FAS-TD) were proposed in 2018 Wang et al. [50]. These aimed to expand pseudo depth mapping to videos. The FAS-TD networks captured motion and depth information given by video. This method was effective at capturing short and long term motion patterns of both real faces and planar PAs by integrating optical flow guided feature blocks and convolutional gated recurrent unit modules to a neural network architecture. In addition it improved the single frame performance from the previous method.

2.4 Smartphone focused PAD methods

An approach for smartphone based PAD was proposed in 2015 that utilized the entire range of focus that the smartphone was capable of [51]. This method assumes that the end user will be holding the smartphone in their hand, so the resulting images will be influenced by a phenomenon known as *motion parallax*. The method proposes taking multiple images that have focal points set at each available point between infinity (far away) and zero(close). This will then result in a *motion stack*. The aligned stack images are then used to determine whether or not a presentation attack is taking place. The accuracy of the alignment is assisted by using optical flow. This process is illustrated in Figure 2.9. This method focuses on using the information from varying focus for bona fide versus attack images.

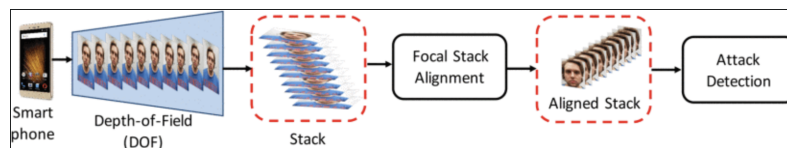


Figure 2.9: Visualisation of the proposed motion stack method [51]

2.5 Multiple cues

Multiple cue systems are much more difficult to fool than lone systems, as they can assure a greater PAD-accuracy, as it covers multiple grounds. These systems can for example often combine liveness and texture cues and/or 3D geometric cues to create a system more robust than any of these systems alone. The scores obtained from each are then fused to determine if the input image is a real face or not.

2.5.1 Liveness cues and Texture cues

In 2017 a paper combining texture cues and eye blinking was proposed by Pan et al. [52]. The authors used a eye blinking model that they had previously proposed to detect eye blinking. The authors combined this with a texture cue based model that checked the coherence between between the background and the actual background. The reference image is taken without the user being present. If the user is genuine, the background texture should theoretically be identical. In contrast, if a video or picture is presented, then the background region around the face should be different. LBP features are extracted from several points around the facial region. If an impostor is detected either by the eye blinking liveness cue or by the texture cue background comparison, access is denied.

2.5.2 Texture and 3D Geometry cues

In 2017 one of the most important methods of PAD was proposed. The method combined patch-based geometric cues and pseudo depth-map cues. The method uses a two stream CNN. The pseudo depth map method was described in the Section 2.3.2. The CNN used in this method utilize 7 layers and focuses on local features of the image.

2.6 PW_MAD

Recent works have also started investigating the pixel level information for detecting presentation attacks [42, 53–55]. The core of this proposal is to exploit the pixel level inconsistencies that are apparent in attack attempts.

The key element of this thesis is to exploit pixel level inconsistencies in attacks in contrast to bona fide attempts of authentication to detect presentation attacks. This is referred to as Pixel Wise Presentation Attack Detection(PW-PAD) [42, 54, 55]. PW-PAD aims to create a pixel wise supervision approach that trains a network to be able to know whether or not a pixel belongs to an attack rather than the entire image. PW-MAD was based on the DenseNet[56](specifically DenseNet-121) architecture. The authors of PW-MAD modified the architecture of DenseNet to accommodate their needs. DenseNet was limited to only have two dense blocks

and two transition blocks and only one fully connected layer that produced a binary output instead of the convolutional layer. The convolutional layer had a kernel size of 1×1 to generate the feature map for pixel wise supervision. The feature map that this layer generates is used to supervise the training of the network in a pixel-wise manner. The network is trained by using pixel wise and binary supervision.

The success of PW-PAD has been well adopted for other problems such as morphing attack detection in 2021 [53]. Inspired by the recent success of this specific method, the group aims to adopt this approach in this thesis. By utilizing concepts from PW_MAD, and introducing depth-data as an additional data-matrix in the images, as well as alterations of models and systems from PW_MAD to accommodate the challenges depth-data brings.

Chapter 3

Data Collection and Processing

As mentioned earlier in this thesis, we unaware of or knew of the existence of publicly available datasets that contained TrueDepth data from iPhones. This chapter details the process of collecting data for the project.

3.1 iOS Depth Capture Application

The iOS depth capture application was developed based on a publicly available open source project [57]. Certain alterations were made to the application to better suit the data collection process.

3.1.1 Application

The mobile DepthCapture-app is forked from an open source project developed by Eyal Fink [57]. The reason behind utilizing open source software lies behind the groups lack of experience with Swift, the predominant programming language for the iOS-platform. Seeing as the main PAD-package would be written in Python, learning an entirely new language with a different structure to achieve one sub-task, would be out of scope for this project. This was the reason why the group ended up using an open source project as a base of operations, rather than an entirely self-programmed software.

The key feature additions and changes made in our application are listed as below:

- **Redesigned UI** - The application introduces a more user-friendly graphical user-interface, while keeping the core functionality of the original application. The main reason behind the UI changes are rooted in usability and availability-aspects related to data-collection. The changes were deemed highly necessary, as the process of data-collection would involve many different people of varying skill and background interacting with the app. The original UI did not work properly for the purpose intended, as the buttons were not large enough and the placement was not user friendly. This of-

ten lead to a user performing incorrect actions when collecting data. The camera-view was also increased to look more encompassing for users. The further UI-changes can be viewed in Figures 3.1a and 3.1b.

- **Total number of captured frames** - The application was further customized to capture an unlimited amount of frames of depth-data. The original version only collected 60 frames. Seeing as we wanted to collect data from a large amount of individuals, this change was needed. It was used to gather more data than the original capacity of the application could handle.



(a) Old App UI



(b) New App UI

Figure 3.1: DepthCapture Application iOS User Interface

The application has two simple buttons in addition to a view of the camera feed of the phone. Each button signalizes a start-point of data-capture, and a stop-point. The data that is saved after capturing one recording, is then saved within the AppData-folder on the device. The app was put together with no previous Swift experience, and therefore some features could be conceived as inconvenient. At this stage, the application can only save one recording at a time. This deemed it necessary to download the mobile AppData-container from the iPhone between each capture, then restart the app to clear the AppData-container for a new capture. This is the current state of the application leaving much room for improvement. Further work on improving the iOS application was deemed out of scope.

The main purpose of the development of this application is to demonstrate for the task-issuer how depth-data could be collected from Apple mobile devices.

This was one of the task-issuers direct demands for the group, when we started re-searching PAD with depth. The app was also used to create our TrueDepth-dataset "KMH_Depth". Further work within depth detection demonstrates the methods by which data can be used within the scope of the PAD software. Snippets of the source code used for the application could be utilized to gain access to TrueDepth-data within their own mobile software for iPhone. This would give the task-issuer full control over the TrueDepth-data of each individual user of their application.

3.1.2 Requirements

The application was only intended for internal use for data-collection, and therefore need to be compiled and ran in the Xcode IDE on a macOS-machine. In other words, the application exists only locally on the device once compiled. As a consequence, the app also requires an Apple Developer license to deploy onto an iPhone. This is mainly due to Apples strict limitations for mobile-devices, directly rooted in security. For this project, the task-issuer issued one of the group members an Apple Developer account, which made the compilation and deployment possible.

3.1.3 Output

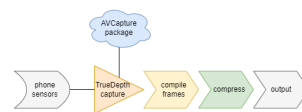


Figure 3.2: iOS process flow

The main function of the application is to harvest data from the TrueDepth sensors on the iPhone. the application outputs the data in two files. The first is an RGB video that is output by the front facing camera. The second is a raw array of data points produced each frame by the TrueDepth sensor array. As the latter is a highly compressed form of raw data in a unspecified format, it needs hereafter processed using the decompression script which is also developed by Eyal Fink [57] in Jupyter. This script was then translated to python and implemented as a part of the package as a whole. Following this implementation, more adjustments and improvements were developed to fit the groups use-case. This method is apart of the depth mask module discussed later in Section 4.1.1.1.

3.2 Datasets

The datasets used during the project consisted of an internal KMH dataset and an external OULU dataset. Dataset construction process followed a set of protocols for bona fide data collection and attack data creation. This was meant to provide a wide variety of RGB-D data to current and future research works. The KMH

dataset was collected at the NTNU i Gjøvik campus following the protocols as explained in the section below.

3.2.1 Protocols

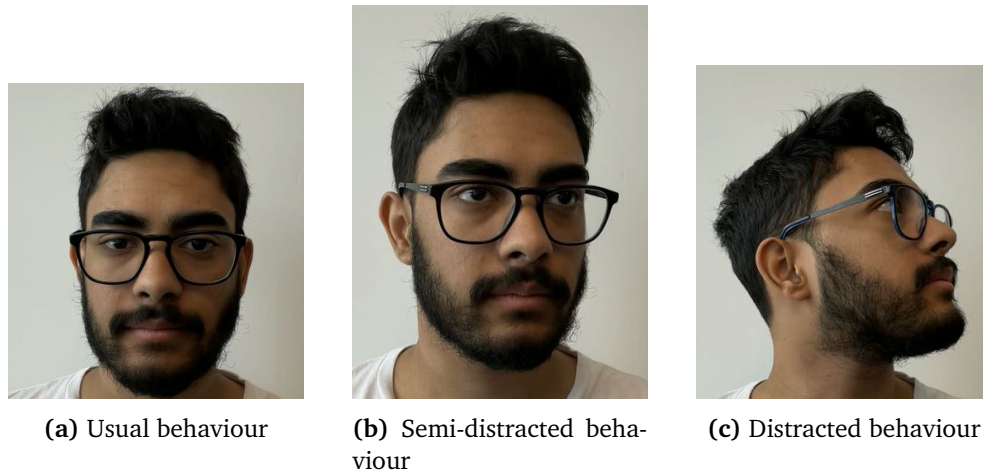


Figure 3.3: Examples of behaviours in the protocol

1. Usual behaviour: Full focus on phone, demonstrated in Figure 3.3a
2. Semi-distracted behaviour: Semi focus on phone, demonstrated in Figure 3.3b
3. Distracted behaviour: Little to no focus on phone, demonstrated in Figure 3.3c
4. Varied behaviour: Varied focus on the phone throughout the recording, change in background

3.2.2 Dataset creation

In early stages, it was assumed that such data would be provided to us, however when the publicly available data was examined, it was found that multiple factors we deemed necessary were either undefined or incorrect. The most important variable here was TrueDepth data. This forced a change in focus and scope to include data collection. This is a natural development in a research-focused development project. This is where we found our primary research task. In order to ensure a high quality in functionality and results, large amounts of data would have to be cultivated. Data collection quickly became one of the larger objectives in this project.

The data itself was captured using the DepthCapture application. There exists further technical specifications of this mobile application at Section 3.1. As previously described, we started with developing a small batch of depth-data to investigate the structure of the depth data from TrueDepth-cameras of iOS-devices. After this analysis had been done, and methods had been developed to interpret

the depth-data, the need for data became glaringly obvious for further development. This is where the expansion process of the dataset began.

3.2.3 Dataset expansion

To ensure a high quality dataset, and ability to produce conclusive results, we concluded that the bona fide part of the dataset would have to be increased in size. Variation in terms of lighting condition's, backgrounds and attentiveness levels, had to be thought of. In addition, edge cases, where we would assume the program would fail, would also have to exist within the dataset.

Before any data had been collected for the dataset, a protocol for data collection was created. This protocol outlined four situational data entries per subject. These included various attention-levels, a change in background, and various camera point-of-views for each of the four data capture session. This protocol was developed to ensure the dataset would portray realistic behavior for mobile facial authentication scenarios. This protocol is further elaborated upon in Section 3.2.1.

After the protocol had been finalized, the process of recruiting subjects for the dataset began. This required extensive research on privacy regulations and guidelines, and the group was certain to comply with relevant laws and regulations regarding privacy and data-handling. Especially the General Data Protection Regulations (GDPR) throughout the entire process. To be able to legally collect data, we were obliged to collect consent from each subject participating in the dataset. The task-issuer issued a detailed data privacy compliance contract for each subject to sign. The contract itself is included in Appendix I. For privacy reasons, the names, signature, e-mail, and phone number of each subject is not included in the appendix-document. The contract included in Appendix I is simply the clauses that each subject agreed to before participating in data-collection.

The primary method for data collection was to approach individuals on campus and ask if they were willing to participate. This led to a diverse group of individuals from a variety of different ethnic backgrounds to the extent that it was possible within the number of willing participants we were able to recruit. In the beginning of the data-collecting process, we aimed for a conservative 25 subjects for the bona fide section of the dataset. A majority of the responses by professors and co-students were interpreted as positive. Participation-levels were higher than initial expectations. As a result, we ended up collecting data of 50 unique subjects. 8 of which are defined as challenging cases, in medium to low light conditions. Examples of some of the bona fide data captured are shown in Figure 3.4

Subsequently, when all bona fide data had been collected, we moved onto simulating various attacks for each individual included in the dataset. The simulated attacks covered primarily level 2 presentation attacks. One still frame of each subject were printed on matte A4-paper. Each print were then used to simulate a standard paper-based presentation attack. In addition, a morphed paper-attack was also created with the same printed image-frame. As a last attack-attempt, a



Figure 3.4: Examples of captured bona fide images

display video-attack was conducted for each bona fide individual. This attack-type works by replaying a video of a subject, in an attempt to fool the PAD and classify the authentication attempt as bona fide. Examples of the above mentioned attack types are showcased in Figure 3.5.

The final dataset, which we named "KMH_real_depth", is both diverse and large in size. It includes 198 bona fide videos, with 50 unique subjects. It also features various presentation attack attempts for each individual. In addition, there are 8 "challenging cases" included, meant to challenge RGB-based PADs. Each individual clip contains a RGB video, as well as the corresponding TrueDepth-data in the form of a greyscale video. The dataset's use-case for this project is mainly for training and testing the deep learning model, trained using the neural network discussed in Section 4.2.

3.2.4 External Datasets

In addition to the internal KMH dataset, our approach for PAD was also evaluated on a more comprehensive external dataset, known as OULU [58]. This measure was primarily utilized to assess generalize-ability. These tests allowed for observation of the performance degradation when the models faced data which varied,

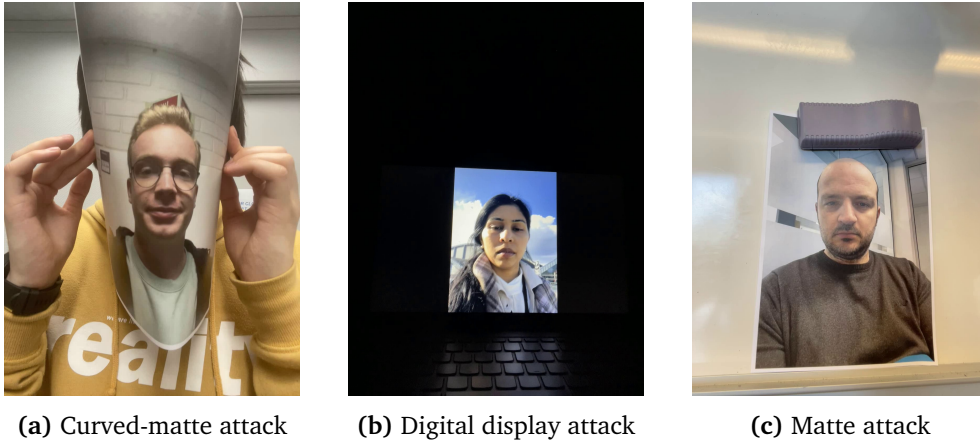


Figure 3.5: Examples of captured PA (presentation attack) images

with respect to individuals, lighting conditions, and device types. The external dataset (OULU) contained data only within standard RGB-imaging, and lacked depth. The dataset was still deemed useful, as it could still be used for training and testing the RGB-based PAD models for comparison with the TrueDepth-based model. Thus, we have employed the OULU dataset for illustrating the challenges of deep-learning-driven PAD-methods when using RGB data alone, as shown in Section 5.2.1.

Chapter 4

Proposed Approach for PAD

4.1 Data processing

4.1.1 Main functionality

The various functionalities of the data-processing repository have been constantly adjusted throughout the projects life-cycle. The reason behind this, is the constantly evolving nature of the package. The main functionality, in addition to testing, serve to process and sort the internally created "KMH" dataset. As testing became more sophisticated, and required dedicated methods, the functionality was moved to another repository mentioned later in this chapter. The change was made due to the resulting output of the code being produced in another directory, making it convenient to use the methods and graph the results there. The data processing aspect remains and is what the repository is used for.

By default the repository is meant to work on the collected internal KMH dataset, but can be adjusted to fit any dataset and perform various operations through its mutually exclusive methods. Though the main purpose serves to process the KMH dataset for the purposes of training a Deep Learning based model.

The program has a multitude of options, passed as python arguments, to adjust the way the dataset is processed. Besides from the dataset path and output dimensions of the images, the program allows the user to choose the following:

- The total amount of images they wish to have in the final split
- How the user wishes the train/test/dev split to be generated (percent-wise)
- The individuals that will be included in each split, or if the splits should be random
- Inclusion or exclusion of edge cases from the KMH dataset
- Whether or not images deemed "Non-viable" should be included
- if a readME with useful information should be generated after the dataset is processed

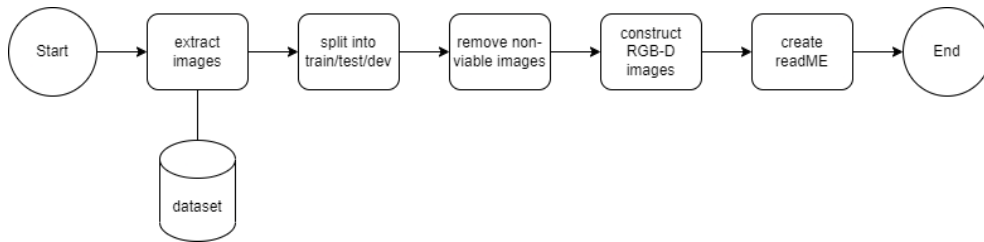


Figure 4.1: Development Model

The process flow is as follows:

1. Extract images as JPG's from the "KMH" dataset and detect face, the process illustrated in Section 4.1.1.1
2. Sort images into a train / test / dev split based on percentages
3. Remove all non-viable images (images in the dataset determined to not be fit for model training in this use-case scenario)
4. Construct RGB-D images, saved as PNG's, Section 4.1.1 illustrates the process flow for this operation
5. Construct readME with useful information

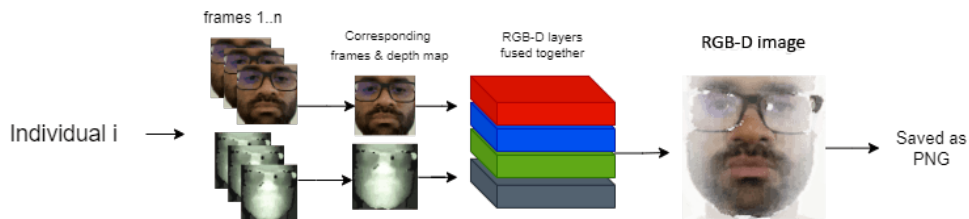


Figure 4.2: Process flow of constructing RGB-D images.

4.1.1.1 Depthmask module

```

1 def reconstruct_depth_data(self, data, dimensions):
2
3     # Dimension parameters
4     w = dimensions[0]
5     h = dimensions[1]
6
7     # Frame count
8     frame_count = int(len(data) / w / h / 2)
9
10    # Reshaping
11    frames = np.frombuffer(data, np.float16).reshape((frame_count, h, w)).copy()
12
13    # Frame values translation
14    frames = np.nan_to_num(frames, 0)
15    maxim = frames.max()
16    imgs = (frames / maxim * 255.0).astype('uint8')
17
  
```

```

18 # Prepares images before returning
19 depth_frames = []
20 i = 0
21 while i < frame_count:
22     # Flips the image
23     depth_frames.append(np.flip(imgs[i, :, :].T, axis=1))
24     i += 1
25
26 return depth_frames

```

Code listing 4.1: Depth data decompression

The module exists as a file in the repository and contains multiple methods related to depth data processing. These are not meant to be directly used to gather depth data, but rather process it after it has been gathered. In the current implementation of the iOS application which allows for IR data capture, the depth files produced are stored as raw compressed depth data. Ideally the iOS application is adjusted in the future to automatically do this process and save the result as video files. This output data needs to be decompressed, reformed to fit the resolution dimensions and then split frame for frame. Methods in this module allow for such processing of the depth data. Code listing 4.1 showcases the method used for depth data decompression.

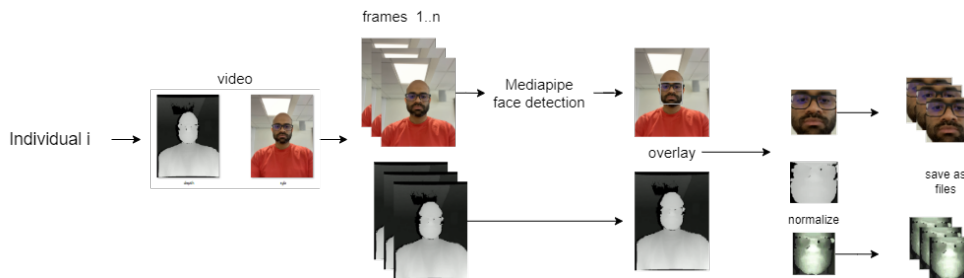


Figure 4.3: Illustrated process flow based on depth mask face detection.

Another important functionality of the module is tied to the preparation and sorting of the dataset itself. The data which the deep learning model is trained on is face data, and needs to be prepared as such. This method utilizes MediaPipe and the RGB image-frame to detect the face of the subject, and overlay the bounding box over both the RGB and related TrueDepth image. The cropped face images are then resized to given dimensions, [224, 224] being the default.

4.2 "PWD_PAD" repository

4.2.1 Implementation

Our approach uses pixel-wise and binary supervision to label the images. Each pixel is classified as either bona fide or a presentation attack. Such an approach

allows for smoother classification by pinpointing regions where attack or bona fide indicators are apparent.

```
1 class CumulativeLoss(Module):
2     def __init__(self, beta):
3         super().__init__()
4         self.criterion = BCELoss()
5         self.beta = beta
6
7     def forward(self, label, final_op, aux_op=None):
8         fin_loss = self.criterion(final_op, label)
9         if aux_op is not None:
10            aux_label = torch.ones((label.shape[0], 196)).type(torch.FloatTensor).
11            cuda()
12            for i in range(label.shape[0]):
13                aux_label[i] = aux_label[i]*label[i]
14                aux_loss = self.criterion(aux_op, aux_label)
15                cumulative_loss = self.beta*aux_loss + (1-self.beta)*fin_loss
16            else:
17                cumulative_loss = fin_loss
18            return cumulative_loss
```

Code listing 4.2: Depth data decompression

Both the pixel-wise and binary supervision use Binary Cross-Entropy (BCE) as their loss function's. The equation is as follows:

$$L_{BCE} = -[y * \log(x) + (1 - y) * \log(1 - x)]$$

y represents the ground truth label, whilst x is the predicated probability score. Our final loss is a combination of the two losses we calculate for pixel-wise and binary. This combination is weighed with a variable λ , by default and under the course of this project 0.5 is used, meaning both the losses are weighed equally in the resulting loss. The resulting total loss can be defined as:

$$L_{TOT} = \lambda * -[y * \log(x) + (1 - y) * \log(1 - x)] + (1 - \lambda) * -[y * \log(x) + (1 - y) * \log(1 - x)]$$

Additionally the implementation uses hyper-parameters as motivated in [42]. For this we use the ADAM optimizer with a learning rate of 10^{-4} and a weight decay of 10^{-5} .

4.2.2 Architecture

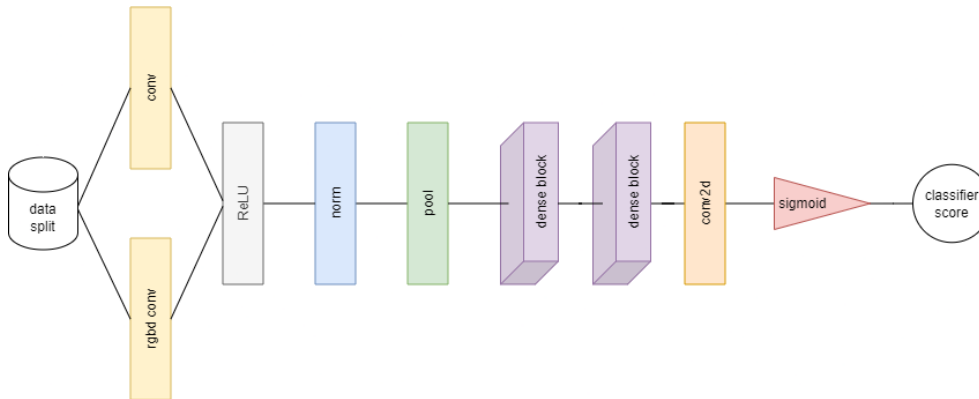


Figure 4.4: PWD_PAD neural network model

The network takes in images of shape $[224, 224, 3]$ as input. Since the amount of layers in the 3rd channel varies between RGB and RGB-D (RGBA) images, this needed to be adjusted. Based on the situation, the model uses one or the other input layer. The first convolutional layer takes in images of shape $[224, 224, 3]$, whilst the other one takes in images of size $[224, 224, 4]$ to accustom the RGB-D images.

The data is then normalized with the use of a ReLU activation function and a normalization layer, before being pooled to summarize it's feature map. The network utilizes two densely connected network layers for the classification. These layers are called DenseBlock's, and are based on the DenseNet architecture [56]. Utilization of the DenseNet architecture as the main classification layer was motivated by [53].

Further, a convolution layer with a kernel size of 1×1 produces a feature map which is used to supervise the training of the network. The result is put through a fully connected layer and a sigmoid activation to produce the final output, being a score between 0.00 and 1.00.

4.2.3 Plotting

The PWD_PAD implementation repository also contains a folder with various plotting files, allowing to display results from model testing. These files are the ones used to produce graphs in the results and conclusion section, relevant to the project.

4.2.4 RGB compatibility

The neural network was designed to take RGB images as input, training the RGB models went without issues. The clips were slip into frames and saved as images, the images were then used as training, validation and testing data for the models.

4.2.5 Depth compatibility

To adjust for training depth only models, the same sized input layer was used, only now the greyscale layer was copied over to each of the RGB layers, and used as input.

4.2.6 RGB-D compatibility

```
1 def rgbd_conv0():
2
3     conv0 = DenseNet.features.conv0
4     # Copy original layer attributes, with new in_channels
5     rgbd_conv0 = nn.Conv2d(in_channels=4, out_channels=conv0.out_channels,
6                             kernel_size=conv0.kernel_size, stride=conv0.stride, padding=conv0.padding, bias
7                             =conv0.bias)
8
9     weights = conv0.weight.clone()
10    with torch.no_grad():
11        rgbd_conv0.weight[:, :conv0.in_channels, :, :] = weights
12        rgbd_conv0.weight[:, conv0.in_channels:(conv0.in_channels+1), :, :] = conv0
13        .weight[:, 0:1, :, :].clone() # Clone the first weights to the new depth layer
14
15    rgbd_conv0.weight = nn.Parameter(rgbd_conv0.weight) # Explicitly register as
16    parameter
17
18    return rgbd_conv0
```

Code listing 4.3: Convolution input layer supporting RGB-D

Certain changes had to be made to the original model and the pyTorch implementation in order for the network to have the ability to process RGB-D images. Firstly, a new convolution input layer had to be made, it mostly mimicked the original one with one exception of the increased amount of layers on the 3rd channel, from 3 (RGB) to 4 (RGB-D). A function which creates this layer can be found in `model.py` and is used instead of the standard `conv0` layer if the `model_type` given upon execution is "rgb".

Another necessary change to accustom the implementation to RGB-D image was the adjustment of mean and std (standard deviation) values used for normalization in the `albumentation`'s package. Most standard networks expect RGB images consisting of 3 layers in the 3rd channel as input, and as such the produced variables for std and mean feature only 3 values. This has to be adjusted from the original values of `[0.229, 0.224, 0.225]` and `[0.485, 0.456, 0.406]` for std and mean respectively, to ones featuring a 4th value. As these 3 values for both std and mean were determined by processing millions of images, attempting to produce a similarly generalized value for RGB-D images would be out of our scope. Instead, we processed all the images in our internal KMH dataset to find the std and mean featuring 4 values, and only appended the 4th missing value, leaving the rest as was. The new values being: `[0.229, 0.224, 0.225, 0.476]` for

std and [0.485, 0.456, 0.406, 0.423] for mean. These values are rather vital as they are used to normalize the images before being processed.

Chapter 5

Results and Experimental Analysis

5.1 Experiment protocols

The results are based on models trained using the gathered internal KMH dataset. From the dataset, 10 unique splits have been created using the repository described in Section 4.1. Each split has around 2500 images, evenly split between bona fide and attacks. These are divided over the training, testing and validation sets, each containing 60%, 30% and 10% respectively of the amount.

In addition, the testing directory has an extra 500 challenging cases, evenly split over 8 individuals, none of which exist in the training or testing directories. These challenging cases are meant to test whether or not there is an advantage to utilizing depth RGB-D based PAD in contrast to only RGB based PAD.

The total image count is approximately 3000 images per split. The final split (which includes challenging cases) between train/test/val being 50%, 43% and 7%, respectively.

These challenging cases account for around 40% of the testing directory. In addition, other version's of the testing directory were made for each model, featuring testing directories made up of 60% and 80% challenging cases, meant for further analysis.

For comparison an external dataset was used. The dataset used was a split off of OULU, featuring both bona fide images as well as a variation of paper and display attacks. OULU offers a mix of illumination condition and image quality variations. Around 700 images were chosen to be used for testing purposes.

5.2 Results

5.2.1 RGB based PAD

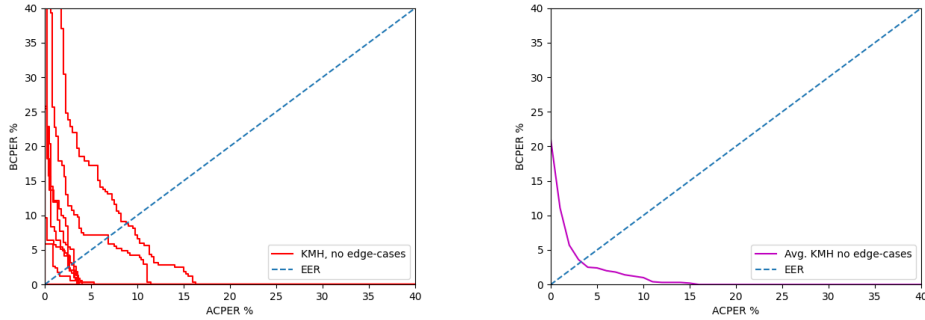


Figure 5.1: ROC curves of RGB based PAD tested against the KMH dataset with no edge-cases targeting RGB.

Model nr.	BPCER 5%	BPCER 10%	EER Threshold	Accuracy (1-EER)
1	0.3	0	0.818	98.4
2	0	0	0.792	96.8
3	0	0	0.618	100
4	0	0	0.85	97.3
5	7.1	4.2	0.632	93.1
6	0	0	0.796	97.5
7	0	0	0.7	97.1
8	0	0	0.936	100
9	17.9	8.2	0.548	91.2
10	0	0	0.741	100
Average	2.53	1.24	0.743	97.14

Table 5.1: Table containing BPCER 5%, BPCER 10%, EER threshold and the EER percentage for each trained model as well as the average, based on models in Figure 5.1

Models trained using only the RGB images performed exceptionally when tested against a testing set consisting of the internal KMH dataset, as shown in Figure 5.1. This is to be expected as it is common for models to perform well when faced with similar data on which they were trained on [13].



Figure 5.2: Examples of images which have been classified incorrectly for the models in Table 5.1

The models failed to correctly classify the attacks when the image quality wasn't ideal. This is to be expected, as the models were trained on ideal face conditions, after instructions from the project supervisors. At times, pictures which were less than ideal quality could make their way into the testing data, as the images were created at a frame by frame basis from the original video. This could cause blurry or less than ideal resulting images. Another factor for less than ideal output data could be attributed to failure of the face detection algorithm in place, as shown in select images in Figure 5.2.

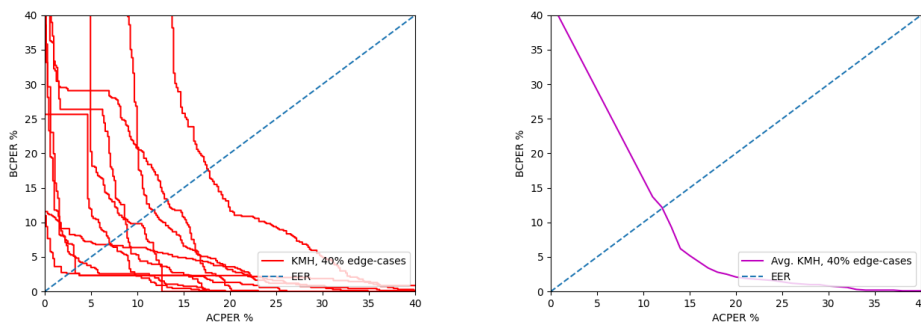


Figure 5.3: ROC curves of RGB based PAD tested against the KMH dataset with challenging cases targeting RGB.

Adjusting the testing set to consist of ca. 40% challenging cases, degradation in accuracy can be observed as shown in Figure 5.3. These challenging cases were designed to target RGB specifically, featuring varying lighting condition's. The average accuracy rate for the RGB based PAD went from 97.2% to 91.5% when the edge-cases were included, as shown in Tables 5.1 and 5.2. A increase of 5.7% in EER (model accuracy) is seen once challenging cases are included into the testing set of RGB based PAD.

Model nr.	BPCER 5%	BPCER 10%	EER Threshold	Accuracy (1-EER)
1	2.3	2.3	0.852	97.3
2	4.1	2.6	0.791	95.9
3	66.2	33.8	0.568	88.3
4	59.2	9.8	0.825	90.1
5	26.4	5.5	0.617	91.1
6	2.3	2.3	0.922	96.7
7	29.1	21.8	0.601	86.8
8	25.6	2.8	0.784	93
9	90.5	87.6	0.539	82.3
10	7.2	6.4	0.812	93.2
Average	31.29	17.49	0.731	91.47

Table 5.2: Table containing BPCER 5%, BPCER 10%, EER threshold and the EER percentage for each trained model as well as the average, based on models in Figure 5.3

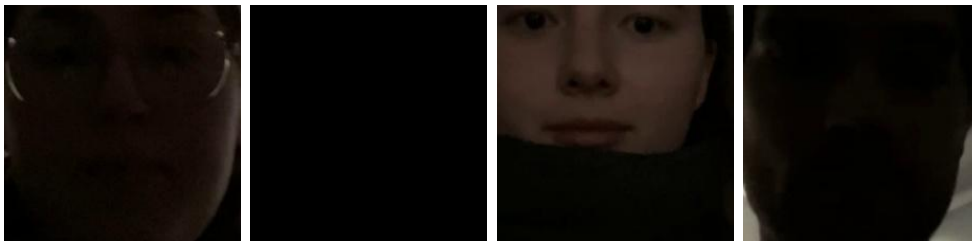


Figure 5.4: Examples of images which have been classified incorrectly for the models in Table 5.2

Looking at the images which the RGB based PAD failed to classify correctly, shown in Figure 5.4, a common pattern is observed. Images with low light conditions, where a limited amount of visible light was captured, proved a challenge for the RGB based PAD, as speculated earlier. The decline in model accuracy, alongside this emerging pattern, showcases a limiting factor for RGB when it comes to challenging cases with varying lighting conditions.

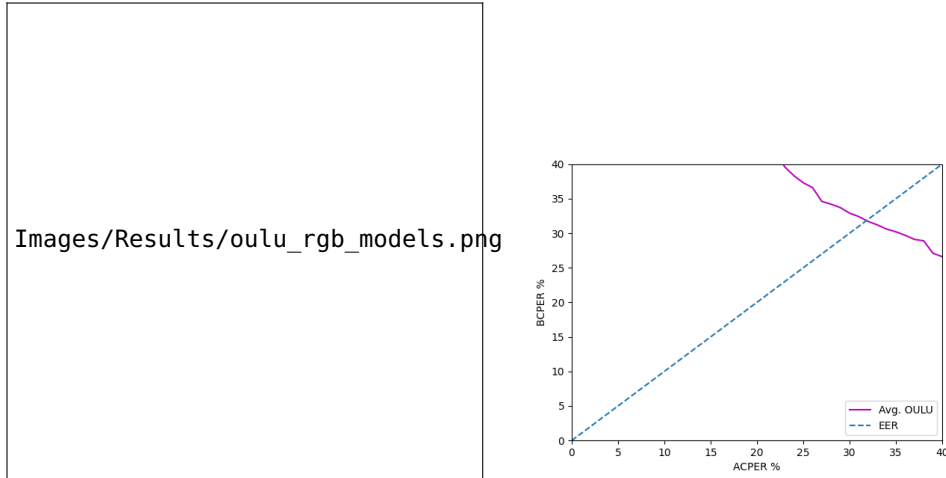


Figure 5.5: ROC curves of RGB based PAD tested against the OULU dataset.

Model nr.	BPCER 5%	BPCER 10%	EER Threshold	Accuracy (1-EER)
1	65.1	61.6	0.905	52.8
2	70.6	63.9	0.924	68.3
3	92.5	82.8	0.797	50
4	61.6	51.7	0.956	74.6
5	44.6	38.3	0.811	80.3
6	82.3	66.3	0.97	71.1
7	40	36.2	0.922	76.1
8	73.5	67.3	0.973	69
9	89.8	82.6	0.893	58.5
10	53.6	44.4	0.887	71.1
Average	67.36	59.51	0.904	67.18

Table 5.3: Table containing BPCER 5%, BPCER 10%, EER threshold and the EER percentage for each trained model as well as the average, based on models in Figure 5.5

When the RGB based PAD is tested against a more generalized dataset, in this case a split off of OULU, a massive decline in the model accuracy is observed in Figure 5.5, relative to the models tested against KMH in Figure 5.3. The resulting accuracy is not spectacular, with the 10 model average being 67% for OULU compared with the 91.5% to 97.2% for KMH, depending on if challenging cases are included or not, as shown in Tables 5.1 to 5.3.

From the average model accuracy values between Tables 5.1 to 5.3, the EER is still far apart, and the models perform far worse for a more comprehensive dataset, as opposed to its internal one. This is a common issue models face with generalize-ability, and is likely to also be the case for Depth and RGB-D based PAD if tested against a more generalized and sophisticated dataset. Although such a

dataset is not available to the project group in order to demonstrate this.

5.2.2 Depth based PAD

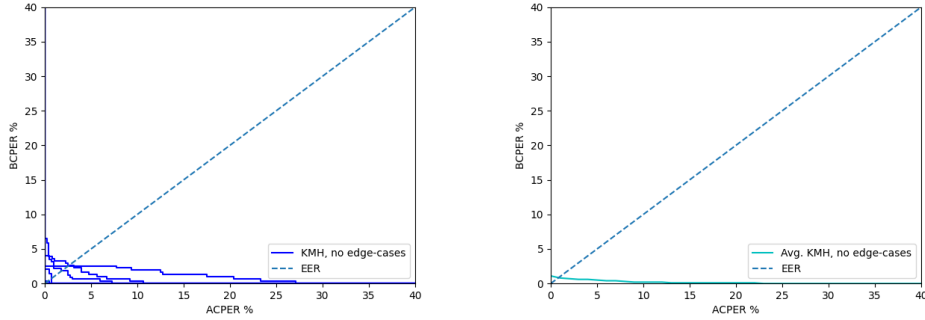


Figure 5.6: ROC curves of Depth based PAD tested against the KMH dataset with no edge-cases targeting depth.

Model nr.	BPCER 5%	BPCER 10%	EER Threshold	Accuracy (1-EER)
1	0	0	0.667	99.3
2	0	0	0.697	100
3	0	0	0.821	100
4	0	0	0.547	100
5	1.6	0.3	0.692	97.5
6	0	0	0.725	100
7	2.6	1.9	0.76	97.5
8	0	0	0.613	100
9	0.6	0	0.69	98
10	0	0	0.671	99.8
Average	0.48	0.22	0.688	99.21

Table 5.4: Table containing BPCER 5%, BPCER 10%, EER threshold and the EER percentage for each trained model as well as the average, based on models in Figure 5.6

The Depth based PAD performs exceptionally when tested against the internal KMH dataset as seen in Figure 5.6. This is, in a similar fashion to how the RGB based PAD performed in Figure 5.1.

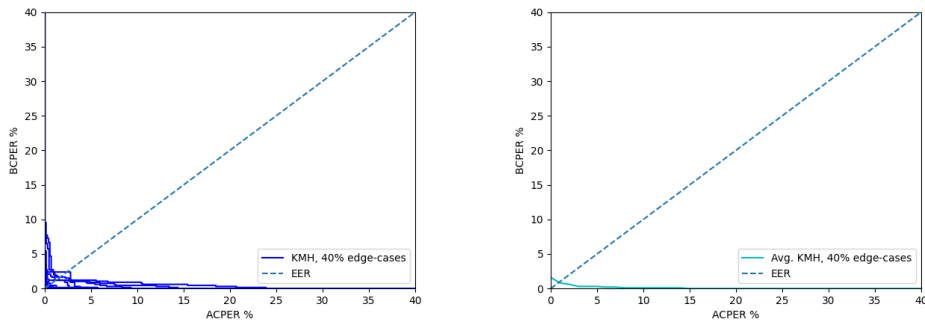


Figure 5.7: ROC curves of Depth based PAD tested against the KMH dataset with challenging cases targeting RGB.

Model nr.	BPCER 5%	BPCER 10%	EER Threshold	Accuracy (1-EER)
1	0	0	0.667	99.4
2	0	0	0.697	99.7
3	0.1	0	0.821	97.7
4	0.2	0	0.547	98.5
5	0.9	0	0.692	98.3
6	0	0	0.725	99.5
7	1.2	0.9	0.76	98.8
8	0	0	0.613	100
9	1	0.4	0.69	98.8
10	0	0	0.671	99.7
Average	0.34	0.13	0.688	99.04

Table 5.5: Table containing BPCER 5%, BPCER 10%, EER threshold and the EER percentage for each trained model as well as the average, based on models in Figure 5.7

Depth performs equally as well when challenging cases are featured, shown in Figure 5.7. These challenging cases are designed to target RGB and therefore pose no challenge for a Depth based PAD. If our dataset were to contain sophisticated level 3 attacks, such as 3D masks meant to challenge the Depth aspect, we can anticipate to see a similar trend of decline in model accuracy as we saw in Figure 5.3. Likewise, if these challenging cases targeting depth were to be tested against the RGB based PAD, we'd likely see it perform better than the Depth based PAD.

5.2.3 RGB-Depth based PAD

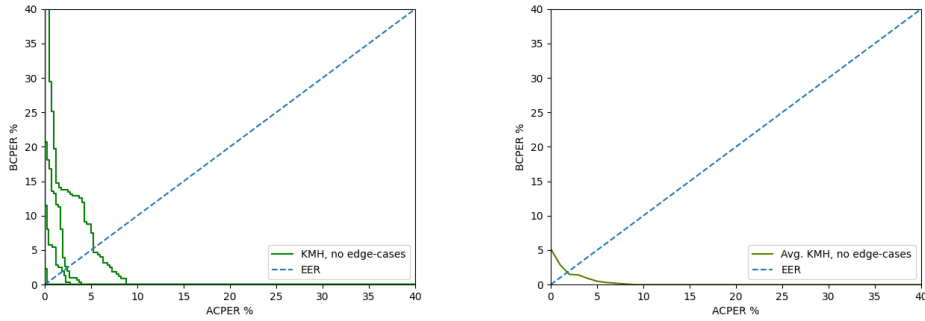


Figure 5.8: ROC curves of RGB-D based PAD tested against the KMH dataset with no challenging cases targeting RGB-D.

Model nr.	BPCER 5%	BPCER 10%	EER Threshold	Accuracy (1-EER)
1	0	0	0.669	100
2	0	0	0.667	100
3	0	0	0.576	99.8
4	0	0	0.583	97.5
5	0	0	0.768	100
6	0	0	0.829	100
7	0	0	0.543	98.1
8	0	0	0.645	100
9	9.1	0	0.558	94.8
10	0	0	0.83	100
Average	0.91	0	0.667	99.02

Table 5.6: Table containing BPCER 5%, BPCER 10%, EER threshold and the EER percentage for each trained model as well as the average, based on models in Figure 5.8



Figure 5.9: Examples of images which have been classified incorrectly for the models in Table 5.6

RGB-D performed exceptionally well against tests consisting of its internal

KMH dataset, as shown in Figure 5.8. The models misclassified images which were similar to the ones that the RGB based PAD struggled with, shown in Section 5.2.3. As discussed in Section 5.2.1, these types of images are not expected to be classified correctly as they are often illegible, and unsuitable for face authentication.

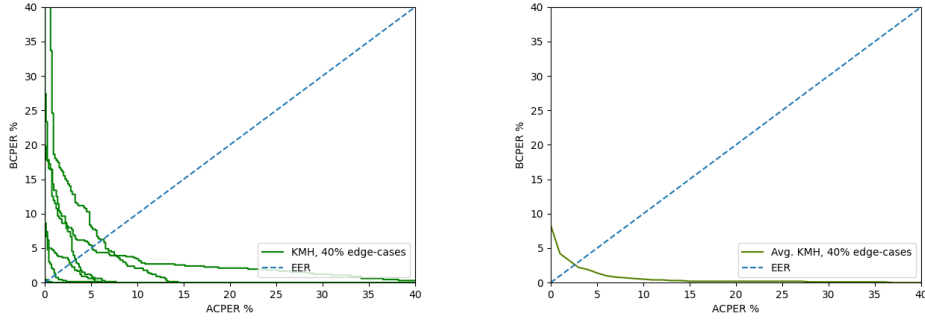


Figure 5.10: ROC curves of RGB-D based PAD tested against the KMh dataset with challenging cases targeting RGB.

Model nr.	BPCER 5%	BPCER 10%	EER Threshold	Accuracy (1-EER)
1	0	0	0.668	100
2	0.9	0	0.69	97.2
3	0.1	0	0.615	98.8
4	1.2	0	0.576	96.6
5	0	0	0.759	100
6	0	0	0.788	100
7	6	3.8	0.566	94.9
8	0	0	0.611	99.9
9	10.7	2.4	0.572	93.8
10	0	0	0.804	99.7
Average	1.89	0.62	0.665	98.09

Table 5.7: Table containing BPCER 5%, BPCER 10%, EER threshold and the EER percentage for each trained model as well as the average, based on models in Figure 5.10

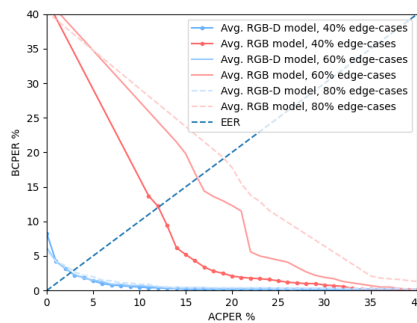
Testing the RGB-D based PAD against a testing set consisting of 40% challenging cases meant to target RGB, the models performed well with images classification, as shown in Figure 5.10. The challenging cases proved little challenge for the RGB-D based PAD, with an increase of 6.6% in model accuracy compared to the RGB based PAD, as shown in Tables 5.2 and 5.7.



(a)

Figure 5.11: Examples of images which have been classified incorrectly for the models in Table 5.7

The RGB-D based PAD managed to successfully classify most of the challenging cases which the RGB based PAD had trouble with, although some challenging cases were still classified incorrectly, shown in Figure 5.11a. These include cases where the RGB image was exclusively noise on a black background as no visible light was captured. Although these getting classified as potential presentation attacks might not be bad either. Images which fit the profile on the Depth side, but were completely lacking on RGB, cannot be getting classified as bona fide. Such images are prone to attacks with 3D mask's in the dark, and would not be suitable for face authentication.



(a)

Figure 5.12: RGB-D and RGB based PAD, tested against KMH dataset, with varying percentages of challenging cases targeting RGB

Alongside the challenging cases testing set featuring 40% challenging cases

meant to target RGB, additional sets were made. The additional sets contain 60% and 80% challenging cases and are meant to test the robustness of the RGB-D based PAD compared to the RGB based PAD.

Plotting all the results, the RGB based PAD can be seen worsening as the percentage of challenging cases increase, meanwhile the RGB-D based PAD stays relatively static as shown in 5.12a. This demonstrates an improvement in robustness, whilst accuracy is maintained when depth is considered, for a variety of conditions which challenge RGB. If our testing set were to feature challenging cases meant to target Depth as well, using RGB-D would likely have a cumulative effect, where depth would perform better due to RGB being a factor and vice versa.

5.3 Discussion

5.3.1 Advantages

Our approach explores a new dimension for PAD using depth-imaging through TrueDepth-sensors and RGB-D images. Using TrueDepth has its advantages, as it immediately allows for ruling out any kind of replay attack, be it paper or digital. TrueDepth also works in a much larger set of lighting conditions than what standard RGB is able to portray. RGB works well for liveliness detection through various methods as is discussed in 2.1, but struggles with variance of lighting conditions and luminosity between the foreground and background as can be seen in Figures 5.4 and 5.5. On the other hand, Depth doesn't face much issues with this, but struggles on the liveliness detection part and can be easily fooled by the use of 3D masks and alike. This lack of overlap suggests a possible complementary relationship, if the two models were to be combined. A combined model, RGB-D, has the potential of increasing robustness whilst still retaining accuracy for more generalized data.

5.3.2 Limitations

The results we produced were based on models trained on small dataset in comparison to other SOTA (2) approaches. This restricts the amount of testing and analysis which can be performed on the models. Such comprehensive depth datasets were not publicly available for the project group to use and lead to the construction of a somewhat limited internal depth dataset. Limitations of the internal KMH dataset restrict the scope of the results, as the dataset at its size lacks variety compared with some of the other more comprehensive datasets like OULU. One example of the internal dataset's shortcomings is the lack of a sophisticated 3D mask presentation attack meant to challenge depth. The group did not attain access to such sophisticated masks under the span of the project. Newly introduced use- or challenging-cases may cause the models to act in unpredictable

ways, something which needs to be pinpointed and adjusted for if generalizability is to be addressed.

Chapter 6

Conclusion

6.1 Conclusion

There exist many powerful algorithms that allow for stable and accurate detection of facial presentation attacks. In today's landscape, these functions all utilize standard RGB-imaging. In reality, there exists more dimensions and factors which could be used as supplement to the already-standard RGB-data that is used today. These additional dimensions could be utilized to increase the accuracy and robustness of the PAD-methods that already exist today.

The research on how much each type of supplemental data effects the detection of presentation attacks is largely unexplored territory. This thesis focuses on exploring how one specific type of data, the already widely accepted data-type of "depth", affects the accuracy and robustness of already-existing PAD-algorithms.

By exploring and utilizing depth data as a supplement to standard RGB-imaging with state of the art PAD algorithm, the results produced in conjunction with this thesis presented interesting revelations. These results show to the fact that adding an extra form of data to an existing RGB-matrix, in this case in form of depth, will improve the detection rate of presentation attacks with existing state of the art algorithms for PAD. The importance of depth-data was proved to be great, and it is safe to say that the implementation of depth-sensors within more smartphones would lead to higher security within biometric authentication in smartphones.

This thesis contributes to the ongoing research on methods of presentation attack detection. It manages to make progress, and define the importance of depth-data utilization within PAD by conducting comprehensive experiments using this data. The results presented by this thesis is indicated to be directly used within further development projects at Mobai AS.

6.2 Achieved Goals

Over the course of this project, we conducted a lot of research into various factors and dimensions of presentation attack detection. This is reflected in Chapter 2 of

the thesis. The research-aspect was not as apparent to us when we started working with the project, and we went into the project with a normal development project in mind.

After thorough work and research, we decided to hone in on a certain factor we found particularly interesting, and which had not been directly explored within PAD, which was the aspect of depth-data. We set out to produce prototype models based on the hypothesis, of depth-data having high importance for PAD, and analyze the results of these prototypes to either prove or disprove the hypothesis.

In the end, we managed to develop a package that produced results which supported the hypothesis, and thereby proved the importance of depth-data within PAD. This was, as per the scope re-definition of the thesis, the primary goal.

6.3 Further Work

There are a fair amount of points where the project could be further expanded. As according to the original task specification (Appendix A), the development of these PAD prototypes are intended within three topics of presentation attack detection: micro-movements, eye-gaze, and depth detection. This project tackled both micro-movements, which gave varying results and therefore is not included in the final package, and the most advanced of the three, depth detection. One topic that could be tackled by further adoption of the project, could be the development of an eye-gaze based presentation attack detection method. This was attempted, but was given a lower priority due to the high focus on depth-centered solutions.

In addition, there is also a prospect to expand the depth-data access to more than just iOS-devices. Expanding the depth-function to operate on Time of Flight Android depth-data is an important expansion, as more phone manufacturers will likely implement these sensors over the coming years, due to a new standard set by Apple with the widely popular iPhone-series of devices. We had no way of collecting data of the Time of Flight structure, due to both code complexity and availability of test-devices, and therefore could not test against this type of data, or produce data of this structure for the dataset.

A more generalized dataset containing depth data could also be produced, something akin to OULU in comprehensiveness, but including mobile depth data in addition to RGB-imaging. The current dataset produced as a part of this project was produced using one device, on one platform only. Ideally, even if restricting ourselves to iPhone-only depth imaging (TrueDepth), we would use different models of iPhone, which can vary slightly in the hardware that they come equipped with. This would be used to achieve as much variety as possible in the dataset that is being created. Introducing more variety would make the dataset more extensive, and as a consequence also more representative of actual use cases of these types of functions for PAD.

Chapter 7

Organization

The organizational aspects of a project of this scale is of high importance. To make the project work, and achieve the goals set, the organization and structure is an essential aspect. This chapter of the thesis covers general organizational aspects of the project, on a high level basis. A section of how quality has been assured for the project is also included. Project-related aspects are discussed within their own section at the end of this chapter.

7.1 Meetings

The meeting structure of the project was set early on. For this project, a meeting is defined by the sessions of which the group members meet and work on problems together. The structure followed a simple recurring structure, meetings were set to happen three times a week, at pre-defined times. These times were:

- Mondays 10:00-15:00
- Thursdays 10:00-17:00
- Fridays 10:00-15:00

Seeing as the structure itself was constant and stable, there was no real purpose for meeting summons. All meeting documentation was streamlined to one single document. This document gives an overview of all meetings held over the course of the project, and is included in Appendix F of this thesis. The document contains not only topics and issues for specific meetings, as such you would find in a meeting-summon document, but also features summaries of individual work between meetings, as well as cooperative work tackled during specific meetings. The topics and issues to tackle in one meeting was pre-written before the meeting itself, to ensure the group members had an overview of what needed to be done for each meeting. This document is an integral part of the project documentation.

The standard practice for meetings can be defined as physical. In these sessions, all group members would meet up on campus, and work together on common issues. During a short period in the starting-phases of the project, meetings were conducted digitally, on the Discord platform, due to Covid-19 complications.

Under other unique circumstances however, occasional meetings were also conducted digitally. Discord continued to be the preferred platform for digital meetings. In the later stages, when work was split on an individual level, the group found it more efficient to work from home, as it offered a work environment more free of distractions. Discord was also the preferred method of communication for the group, to keep in touch socially with non-work-related topics, which contributed to an improved team dynamic.

7.1.1 Work Sessions

Work sessions were important parts of the meetings themselves. Most "meetings" could be defined as such. Some meetings featured cooperative work on common issues, while others contained individual work. The Monday and Friday meetings were exclusively devoted to group-internal cooperative work. Other weekdays, individual work was conducted as per agreement in the preceding meetings. The usual structure for individual work was set in the beginning of the week, in the Monday meetings, with the deadline for each individual task being the subsequent meeting, on Thursdays.

7.1.2 Supervisor Meetings

Supervisor meetings were conducted on an infrequent basis. While the supervisor generally was available to us at all times, there was no need for constant exclusive meetings with him. The meetings with the supervisor happened on a call-basis, where we would call upon him when in need of guidance. The supervisor did participate in the weekly task-issuer meetings, where most of the supervision and task guidance took place. There were a few exclusive meetings with the supervisor, where he presented important theoretical aspects surrounding the task at hand.

7.1.3 Task-issuer Meetings

Task-issuer meetings occurred on a weekly basis. These meetings were usually held digitally, through a shared Microsoft Teams-channel where all members of the task-issuer organization that were related to the project were present in. The meetings themselves were scheduled to Thursdays, between 13:00 and 14:00. In these meetings, we continuously updated the task-issuer and supervisor with the current progress of the project. The progress was directly compared to the streamlined project-plan (featured as part of Appendix E). These meetings were not the only form of communication we had with the task-issuer and supervisor. The group was invited to a teams channel where all individuals connected to the project were present. This teams channel was also a medium for communication outside of the scheduled meetings. This includes, but was not limited to, asking for dataset to test and train our package with.

7.2 Development Model

The development model utilized in this project is largely based upon the iteration-based agile development model [59]. This development model is defined by work-grouping in form of "timeboxes", each sized the same for each iteration of the project.

For each iteration, also referred to as development phase in this project, the "timebox" was set to 3 weeks. Then, an additional week for testing the developed functions thoroughly was added for each phase. This made the total "timebox" for each iteration equal to 3+1. The goals for each "timebox" were largely pre-set in the planning-phase of the project, with some minor alterations as a consequence of progress-speed for each goal. In some cases, it was deemed necessary that some set goals needed to carry over into the next timebox, as it needed more work. In other cases, some issues from the consecutive timebox could be tackled within the current timebox, due to progress being more efficient than anticipated. This model is a more realistic approach to development in a research-centric environment. [59]

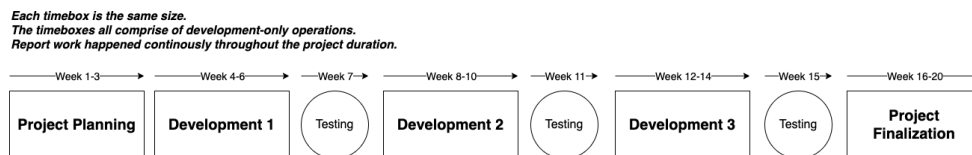


Figure 7.1: Development Model

In total, there were three main iterations for the project. Originally, each phase was planned to tackle one level of presentation attacks, incrementally. After the task-issuer made the scope more clear, this structure was slightly changed. The main purpose for the project was to make the task-issuers presentation attack detection for level 1 and 2 attacks more robust. The task-issuer made it clear that the focus for the project was detection of level 1 and 2 attacks, and not level 3 (most advanced) attacks. The group therefore shifted the focus a bit, to ensure that the requirements of the original scope were fulfilled.

At the same time, the group wanted to move into new territory for presentation attack detection. This is why we decided to focus on depth data exclusively in phase 2. This is due to there being little to no usage of depth-data, which is present in modern phones, within presentation attack detection in today's landscape.

The model choice is based on previous development experiences. For a research-centric project like this, this type of model is beneficial to allow full exploration and solution of each topic set within the project scope.

7.3 Summary of Development Phases

A comprehensive summary of each development phase can be found in Appendix F: "Meeting Documents". This section is dedicated to summarizing each phase in a short-hand project-conclusive format. For a full breakdown of the work done in each phase, visit Appendix F

7.3.1 Planning Phase

The planning phase is an integral part of every project of a larger scale. For this project, this phase primarily centered itself around getting a high-level view of the task at hand, and developing organizational models to achieve the defined goals of the project scope. In addition, contracts for internal collaboration, external collaboration, and confidentiality, were signed to ensure work on a professional level. The phase also laid out standards for communication, as well as schedules for both internal meetings, and task-issuer and supervisor meetings.

See Appendix B-E for further reference of what was conducted during this phase of development.

7.3.2 Development Phase 1

The group aimed to start from the bottom, with the simplest implementation of attack-detection we could imagine within the project scope. The first obstacle we faced, which surrounded this entire development phase, was the process of continuous development of a micro-movement function. The continuous development model was used to assure that everything worked accurately and effectively. As the project is largely research-centric, a lot of trial and error, and also continuous testing, was needed to develop the function. The micro-movement function was solved in this phase, and the initial results produced satisfactory attack detection. The function developed in this phase existed as a source of learning for the group, and the process of this development can be found in Appendix J. This function is not a part of the final package.

7.3.3 Development Phase 2

The focus for this phase was re-worked and we ended up working almost entirely on depth-centered solutions for presentation attack detection. This phase quickly became hyperfocused on collecting data containing TrueDepth-information. Developing data, including data with TrueDepth, was crucial for the project, since a specific dataset like this did not currently exist. To get to the point where we could collect data, we also needed to find out how to actually collect this kind of data from a mobile device. This, in addition to collecting a smaller batch of example data to develop the actual depth-sensing attack detection prototype, ended up taking up the majority of this development phase. The method developed in

this phase utilized machine learning algorithms, applied to the depth-based histograms of each individual frame of the subject video. The dataset developed in this phase was rather small, and was further developed in the next phase of development. The development of a TrueDepth-centered solution continued to a more advanced stage in the next development phase.

7.3.4 Development Phase 3

As the group moved onto more advanced methods of detecting presentation attacks, like utilizing deep learning in conjunction with TrueDepth-data, the third and last development phase consisted mainly of expanding the dataset we had developed in earlier stages, and utilizing the newfound data to test for thesis conclusive results. The development, and eventually completion, of this dataset took an immense effort to produce. The data itself was highly needed, due to the extensive training and testing we did to ensure our final results were definite. The testing resulted in conclusive results, which were further discussed and visualized in the concluding phase of the project.

7.3.5 Concluding Phase

The concluding phase of the project took place between the stable draft submission and the final delivery of the thesis. In this phase, the group focused more on the thesis report than anything else. The report-work amassed the entirety of this phase. As we already had completed close to 80% of the report over the course of second and third development phase of the project, the concluding phase consisted of re-structuring, reference-work, and finalizing unfinished parts of the report. We also had developed conclusive results in the previous development phase (3), and spent time on creating visualizations of the results. The results are displayed in chapter 5 of this report. A definite conclusion was also formed as a product of the results.

7.4 Quality Assurance

7.4.1 Cooperative Efforts

With the diversity within the group composition, the cooperation and sharing of expertise has been of high importance for the project. With a set of pre-defined roles and responsibilities correlating to each study program with specializations, each group member has contributed equally to the finished product, in different fields. The cooperative efforts have been a constant throughout the project, and we have generally aimed for a collaborative workflow with each task we have had at hand. Some tasks, like the highly advanced code structures and logic, or the project documentation, has mostly been handled by the main responsible within the field. With these main speciality-tasks, the other group members have served

as points of support, rather than full-on collaborators. It is through discussion and cooperation we have solved the high-level problems we have faced. The low-level problems, however, have been tackled on a case-by-case basis, mostly by the field-responsible of the issue it concerned.

7.4.2 Code Quality

Code quality is an important aspect of a package repository. A clean code repository leads to a better environment for development. We have made constant actions to ensure the code-base is checking boxes of industry standards of documentation and quality. These standards are related to an abundance of topics. These include: comprehensive in-code documentation, class and folder structure, version control usage, and more.

The code of the package features high cohesion, in the way that it functions as a single unit, with standardized inputs and standardized comprehensible output. This is part of generalized standards for code quality. In addition, the main package utilizes low coupling. The main factor that qualifies the code as low coupled, is the use of decoupled common functions. The utils-class, containing these functions, ensures cross-compatibility of functions (such as pre-processing actions) within the entire program. Every core function/class utilizes unique code to achieve the goal of the respective function/class in conjunction with cross-compatibility from nother classes. These concepts both contribute to the general code quality of the package.

7.4.3 Performance and Optimization

The code featured in the repositories follows best practices for python coding. Although performance was not a central part of the project, the quality of code execution assures efficiency by using the best external libraries and methods available. Alongside a comprehensive readME file in each repository, the code contains extensive PyDoc-documentation and has various cohesive and de-coupled utilities which can be repurposed and used in other projects.

To ensure proper performance for the package, there has been a series of trial-and-error operation for each operative function. For the original proposed scope of the package, it would need to run as a series of operations on a sequential series of images, with close-to no processing time. The group did try to prioritize this, even if the final package would serve as more of a prototype than a complete product.

Optimization measures done to ensure timely performance of the package include: pre-processing measures, order-of-operations, re-scheduling and more. It is through thorough testing, we have found the optimal measures that ensure performance is high enough to work on an almost-instantaneous basis. We tested each function with various pre-processing measures, and found that the primary source of performance-gain is gained by downscaling an image. At the same time, we analyzed the results of a such operation, and found the results of the down

scaled images to be nearly identical to a full-scale image, up to a certain point. We found the optimal performance-to-quality ratio through testing.

7.4.4 Structure

The structure of the package is built after principles that ensure future utility. The structure is constructed entirely based on the hierarchical file structure. This means that each folder, and its classes, is placed in a way which allude to the operations which ensue within the file.

The naming convention follows a traditional style. This means, that each file-name describes what the file itself contains, while at the same time also describes how they relate to other files within the repository. All files are named with the same convention, ensuring cohesiveness and consistency within each repository.

This also applies to the dataset, where a descriptive naming scheme, and corresponding folder structure, was set before the data-collection began. Both for internal group-sharing, and for future references and utilization, each file and folder is named in a consistent and organized way, to ensure the structure is sound, and of good quality.

7.4.5 Documentation

The documentation of the project also follow industry standards. All documentation, both package-, and project-related, have been highly prioritized throughout the duration of the project. The code-side documentation is done to ensure utility for future ventures within presentation attack detection, for external actors to use. The code repositories features a detailed README-file, with general information on utility and operability of the code itself. The more advanced and complex functionality ensnared in the code has been documented and explained through in-code documentation (PyDoc).

The project documentation is extensive, and covers the entirety of the project duration. The documentation includes this very thesis, and in addition, a comprehensive meeting-summary document. The meeting-summary document offers a unique look into the project progress, in a chronological manner. It follows the general standards of project documentation, and serve as the primary source of documentation for the entirety of the project. This document can be found in Appendix F.

7.4.6 Testing

With a project that exists within a research-centric environment, the testing process has largely been based on models of continuous testing. Continuous testing for this project was conducted primarily in a manual way. This is mainly due to the nature of the research-aspect, where trial-and-error is required to make progress. Implementing automated testing systems within the python package was considered to be counter-productive for this project.

The package itself existed in an ever-changing state for the entirety of the project. This required constant attention to what the code actually did, so that we were able to test the functionality at different stages of development. This consequentially made it difficult to utilize testing frameworks, as these are more geared towards projects which are solely development-based. This project bases itself in prototyping and research, and that is why the group ended up doing manual testing and analysis of results to ensure quality of operations for the project.

7.5 Discussion

7.5.1 Scope

The scope was defined early-on in the project. In conjunction with the task-issuer, the scope has been expanded throughout the course of the project. After the micro-movements function had been developed, and we started working on depth-detection, is when the scope was fully realized. Looking at the various elements that had to be tackled in relation to this topic, the group and task-issuer re-defined the scope in development phase 2 of the project.

While most of the scope-aspects set in the planning-phases of the project have been kept, parts of the scope have been altered throughout the duration of the project. This has solely been based on progress and time. The group anticipated the project to be a standard development project, and therefore planned out the scope accordingly. The scope was later re-defined to focus more on research than anticipated.

Rather than a standard development project, the project was defined as a research-centric development project. This is due to the usage of mobile depth-data being a topic of uncharted territory. To tackle this task, we would have to do much research, and in addition develop software in a foreign programming language for data-collection. No real, publicly available, datasets utilize mobile depth-data yet, and therefore a dataset also had to be cultivated as a part of the project. The research-focused work on this, in the groups eyes, ensure a project of importance for the future development of presentation attack detection. That is the main reason for the scope-change. The new scope focused entirely on depth-detection, and this is what the main subject of the project ended up being.

This scope change is a product of research and reflection. When researching the topics correlating with depth, we found unexplored territory, and therefore learned that a scope change was absolutely needed to manage the workload of the project. The main factor that helped us limit the scope this way was the task issuer and our supervisor. The group aimed for constant communication with both supervisor and representatives from the task-issuer, to ensure we stayed within the set scope at all times.

Time seemed to be the one of the main factors that limited our ability to produce the functionality we set out to develop. In many cases, some things would take more time than anticipated. This happened especially frequently, due to the

research-centric task the thesis tackles. In many cases, continuous testing and fine-tuning of each function had to be conducted to produce results of satisfactory quality. In addition, a lot of research had to be conducted to develop methods surrounding unexplored PAD-approaches. This process, relating to the research aspect of the task, was not something we initially had planned for. It ended up re-defining, and therefore also limiting, the scope by the largest margin.

7.5.2 Work Environment

We originally had planned to conduct most physical meetings on campus. Due to multiple circumstantial situations, the work environment was constantly re-considered for each week. The work environment largely depended on the work that was to be conducted during each meeting. The general rule for meetings were physical meetups on campus. The thought behind this, was to work through issues and problems in communion.

In addition, there were other physical limitations that hindered physical presence, including covid-19, and also other illness. There also was a period of time where Milosz had problems with his laptop, resulting in a work-from-home environment to ensure that every group member could do their work within the set meeting times. In this process, we also found that some of the group members tended to work more effectively in a work-from-home environment.

The work-environment for individualistic work was usually defined as work-from-home. Individual work is defined by when each group member had specified individual tasks to work on. Due to previous experiences in earlier stages of development, it was largely decided this kind of work could be done more efficiently in a work-from-home environment.

The last leg of the project, with mostly report writing remaining in terms of work, was also tackled in a work-from-home environment. In this phase, communication via digital platforms became crucial, as constant feedback was necessary for each part of the thesis report. In this last leg, the group met up on campus once a week to physically go through the most demanding issues of the report together.

The work environment choices for the project are all rooted in the future of work. Covid-19 pushed many professional work environments to a digital-physical hybrid workflow. A highly future-proof realistic approach to professional work, is what this project set out to accomplish. The future is hybrid work. This form of work has been observed for this project, and its benefits have been observed to be largely positive, and often more efficient.

7.5.3 Group Composition

The group composition is majorly based within the field of computer science. Two of the group members, Milosz and Kristian, are part of the Computer Science Engineering course. The last group member, Hamza, stems from Digital Infrastructure and Cybersecurity. This combination, while a bit unusual, has worked out

flawlessly. Each members specialization has complemented the others. The group composition has worked well.

All group members have asserted their own specialities. Milosz is the main programmer, and can be defined as the logic lead for the project. He is also proficient in data-handling and visualization of complex digital structures and networks. Kristian is the leader and supervisor of the group, and specializes in organization and leadership. His main responsibility can be defined as leadership and documentation. Hamza is the security expert, and has previous experience with risk assessment, modelling, and also possesses writing skill. His main responsibility lies within the final thesis report.

The roles have been asserted through previous collaboration experiences. Each group member has expressed their expertise, and the group has tried to respect and highlight each members specialities. This practice ensures that work gets done, in the way that it promotes each speciality, and motivates each member to do their work in the best possible way.

7.5.4 Security and Ethics

In an ever-changing society, which modernizes by each passing day, it is also important to consider the implications of such research on a societal and ethical level. Implementing smarter and more modern solutions for mundane manual tasks is a fundamental part of evolving society. This process in itself effectuates basic tasks which normally require more resources, in form of labor, and attention, in form of measures to ensure credibility and accountability.

As mobile phone device manufacturers aim for a new standard of biometric authentication, through facial recognition with depth-detection, it signifies a future of more ethically challenging processes of authentication. The reason behind this, is the fact that depth-data can be classified as much more sensitive than standard RGB-imaging. The data which is being collected can be perceived as more sensitive as it is not only the likeness of a person, but rather a full 3D representation of their face. If this type of data were to end in the hands of a malicious actor, it could be used to falsely identify and authenticate the subject the data concerns much more accurately, when compared to a RGB-based false authentication attempt (presentation attack). This project handles such data, and is therefore subject to high security measures.

It is important that data is kept secure and encrypted to keep the process of authenticating humans ethically viable. Especially considering the high grade of sensitivity of the data. For every process containing the handling of depth-data in this project, we have made sure to always follow the highest security-measures possible at a project of this scale. This was especially important in the data-collection efforts made towards our internal dataset. We made sure to follow all regulations and guidelines, like the General Data Protection Regulations (GDPR) when recruiting subjects for data-collection. All participants have consented to a GDPR-compliant contract regarding the data that was being collected and

its purpose. This can be found at Appendix I

Observing cues from phone-manufacturers, and recent societal conformities, it can safely be assumed that facial recognition has a high probability of becoming the primary authentication method for the future. The results this thesis presents represent a confirmation of the importance of depth-data in facial recognition authentication systems. This has implications for the future of biometric authentication. As long as the data of the subject prone to authentication is being properly protected, it can be safe, reliable, and convenient to utilize depth-data in these forms of authentication.

Chapter 8

Development Process

The development process of this project has been gradual, and not all of the described contents of this chapter has made it to the final product. This chapter describes how we worked through the various problems we faced when tackling this project, in chronological order. For elements that are not featured in the final package, but we spent time on, the development process can be found in Appendix J.

8.1 Depth detection Module

The development of the mobile depth-detection-based method for presentation attack detection turned out to be more challenging than anticipated. This topic is relatively new and no related literature in the field of presentation attack detection was discovered when working on this thesis. Therefore, the method had to be developed in a sequential manner. Firstly, we did not have access to any data related to this project. Mobile depth data is largely used within mobile device authentication measures, almost exclusively natively. This authentication is generally performed behind an encrypted layer that is a piece of the operating system. Applications generally utilize a solution such as FaceID on iOS-enabled devices or Facial Recognition on Android-enabled devices. The task issuer expressed that they rather would want to gather the raw depth-data from these smartphone depth-sensors, rather than use native services. This is principally based on the idea of full control of operations on an image and its data and metadata. Finding a way to gather this type of depth data became our first goal.

The total development of this module (Depth Detection) amassed the entirety of the second development phase. The module itself did not take long time to develop. The group did not realize that the process of collecting relevant data to test the module would be as challenging and time consuming as it was. We went into the development phase with the assumption that depth data produced with mobile phones would already exist and be readily available. The lack of research and development within this area of the PAD field lead to more challenging de-

velopment. Alongside this, due to the lack of availability of data, it was deemed necessary to develop an application to extract TrueDepth data from an iOS device.

After extensive research, a depth-extraction application for iOS devices was developed. This decision was based on multiple factors, including ease of development, availability of data-collection devices, and market-share-data of Apple-devices in the overarching applications functional geographical territory (Norway). iPhones are currently the most used mobile devices in Norway, with a current 63.51% market-share [10].

This mobile application was simply constructed by taking an open-source project for iOS TrueDepth-capture [57], and modifying it to fit the needs of the data-collection needed for the development of this module. The application records a video using both its RGB and TrueDepth cameras to produce two files. One of the RGB video and the other a compressed TrueDepth vector which contains frames corresponding to the RGB version. The choice of utilizing this open-source project, rather than a self-developed application, is based on the group members having no previous experience with Swift as a programming language. The syntax of this language is complex, and differentiates itself vastly from most of the languages we are familiar with. It would therefore be much more time-consuming to develop an entirely new depth-capture application. In addition, this would be far beyond what scope and requirements for the thesis were specified to be.

After the application had been modified, we deployed it onto an iPhone. The task-issuer provided one of the group members with an Apple Developer account, allowing for a much easier deployment-process. After altering the code of the application to suit the requirements of this thesis, we began the process of data collection. The data collected, as previously described, included both RGB-videos and corresponding True-Depth data. The data was constructed in a way to specifically test against most realistic scenarios of both bona fide and PA attempts of facial authentication. The RGB-data collected from the application was also utilized to test other modules from the package.

A small sample-batch of depth-data was created as soon as the application had been deployed. This data was primarily used as examples of data-structure, which was used to comprehend the data itself. This information was further used to develop the depth-module. The module begins by utilizing the face-detection package available in MediaPipe to find the coordinates of the facial region within the video frames. A bounding box is then drawn around the facial region. This bounding box is then used to delimit the face in the depth video. The function utilizes simple histogram-operations on the data-points for depth, including histogram equalization analysis to determine a depth mask for the subject. If the depth-data shows a high uniformity, the attempt is classified as an attack. This method seemed to be extremely effective at detecting paper and screen based attacks.

When the data had been fully realized, the testing of the depth module could ensue. After continuous testing and tweaking, the results showed that the module managed to detect most 2D-based attacks. Where the module showed less con-

sistent results was with 2D paper-masks. In the majority of cases, the histograms generated by 2D mask attacks and bona fide showed great similarity. This is also alluding to the same function being highly inefficient against detailed 3D-masks as well. To be able to detect these kinds of attacks, we would have to move onto more advanced concepts, which exist slightly out of the scope of this thesis. A decision was then made to continue development to work on implementation of a deep learning based approach to mitigate the aforementioned issue.

Through rigorous testing and implementation in accordance to the results of these tests over the course of a week, the module was able to consistently detect the majority of 2D PAs. This module is conditional such that it will work on iPhones that have TrueDepth capability (iPhone X and newer, excluding the SE line at the time of writing). However, the module has potential for future expansion as it accepts any depth matrix alongside RGB as its input data.

We chose to focus on depth, to see the potential improvement between RGB vs RGB-D models, and their potential in the future where mobile depth-sensing camera modules become a standard and much less of a niche topic.

8.2 Neural Network Implementation

After becoming more familiar with the depth data and its potential, the group elected to implement a deep learning module to assist the processing efficiency and data-handling potential of the package. Being a new topic within PAD, a deep learning approach is something that interested us greatly and something our supervisor advised us to explore.

The supervisor introduced us to an implementation of a state of the art deep-learning algorithm called PW_MAD [53]. This program is focused on morphing attack detection and further details on it can be found in the state of the art chapter of this report 2.6. We were also provided a python implementation of this program. This program is focused on PAD through only utilizing the RGB color space. By using a state of the art algorithm, we could then test the effect that the presence of depth data has on PAD.

The implementation in regards to it's design choices takes inspiration from [53] and [42]. It uses parts of the DenseNet[56] framework as a pre-trained network layer. We quickly got familiar with the structure of the implementation, and adapted the pre-existing code. Some changes had to be made to suit the project's needs, such as the network's adaptation to RGB-D images. This was done using best practice and led to increased usability in context to this project.

After the code adaptation, we further experimented by attempting to train some of the core models of the algorithm on the external OULU-dataset(RGB) and an early version of the internal KMH-dataset(RGB+TrueDepth). This led to very promising results that proved that the implementation worked as expected, and would be suitable to continue further testing with in the context of this thesis.

This is when the need for new data arose, as the data we had collected in earlier stages was insufficient. A decision to expand the pre-existing KMH dataset

was then made. This process is described in the previous section of this report 3. Following the extensive data collection, the data was then processed. The depth-data was processed by decompressing it into a video-file. The data was then sorted by each individual. Finally, the edge-cases that were created were isolated from the rest of the data. This concluded the data collection and processing efforts.

The processed dataset was than split. Splits were constructed to be used for training and testing the models. Separate models for RGB and depth were created. This is so that we could compare the results. The functions of the altered implementation of the PW_MAD algorithm were tested against split-parts of the internal KMH-dataset, as well as more generalized ones like the external OULU-dataset [58].

The PW_MAD model and repository had to be adjusted to be able to process RGB-D (RGB + Depth) images. These changes allowed for model training on the internal, TrueDepth-based dataset and compared with our other models to research and observe differences. The results that the trained models returned were then analyzed and graphed in a way that is easy for a reader to digest. These are presented in Chapter 5: Results and Experimental Analysis.

Bibliography

- [1] ISO, 'Iso/iec 39794-5:2019(en) information technology — extensible biometric data interchange formats — part 5: Face image data', International Organization for Standardization, Geneva, Switzerland, Tech. Rep., 2019. [Online]. Available: <https://www.iso.org/obp/ui/#iso:std:iso-iec:39794:-5:ed-1:v1:en:term:3.52>.
- [2] ISO, 'Iso/iec 30107-3:2017(en) information technology — biometric presentation attack detection — part 3: Testing and reporting', International Organization for Standardization, Geneva, Switzerland, Tech. Rep., 2017. [Online]. Available: <https://www.iso.org/obp/ui/#iso:std:iso-iec:30107:-3:ed-1:v1:en:term:3.2.1>.
- [3] ISO, 'Iso/iec 2382-37:2022(en) information technology — vocabulary — part 37: Biometrics', International Organization for Standardization, Geneva, Switzerland, Tech. Rep., 2022. [Online]. Available: <https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-3:v1:en:term:37.06.36>.
- [4] ISO, 'Iso/iec 2382:2015(en) information technology — vocabulary', International Organization for Standardization, Geneva, Switzerland, Tech. Rep., 2015. [Online]. Available: <https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en:term:2120625>.
- [5] ISO, 'Iso/iec tr 29119-11:2020(en) software and systems engineering — software testing — part 11: Guidelines on the testing of ai-based systems', International Organization for Standardization, Geneva, Switzerland, Tech. Rep., 2020. [Online]. Available: <https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:29119:-11:ed-1:v1:en:term:3.1.51>.
- [6] ISO, 'Iso/iec tr 29198:2013(en) information technology — biometrics — characterization and measurement of difficulty for fingerprint databases for technology evaluation', International Organization for Standardization, Geneva, Switzerland, Tech. Rep., 2013. [Online]. Available: <https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:29198:ed-1:v1:en:term:2.11>.
- [7] ISO, 'Iso 3534-1:2006(en) statistics — vocabulary and symbols — part 1: General statistical terms and terms used in probability', International Organization for Standardization, Geneva, Switzerland, Tech. Rep., 2006. [Online]. Available: <https://www.iso.org/obp/ui/#iso:std:iso:3534:-1:ed-2:v2:en:term:1.47>.

-
- [8] Apple, *Use faceid on your iphone or ipad pro*, <https://support.apple.com/en-us/HT208109>, May 2022. (visited on 1st May 2022).
- [9] A. Das, C. Galdi, H. Han, R. Ramachandra, J.-L. Dugelay and A. Dantcheva, 'Recent advances in biometric technology for mobile devices', in *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 2018, pp. 1–11. DOI: 10.1109/BTAS.2018.8698587.
- [10] StatCounter, *Mobile operating system market share norway*. [Online]. Available: <https://gs.statcounter.com/ios-version-market-share/mobile/norway> (visited on 5th Apr. 2022).
- [11] F. Abdullakutty, E. Elyan and P. Johnston, 'A review of state-of-the-art in face presentation attack detection: From early development to advanced deep learning and multi-modal fusion methods', *Information Fusion*, vol. 75, pp. 55–69, Nov. 2021. DOI: 10.1016/j.inffus.2021.04.015.
- [12] D. Wen, H. Han and A. K. Jain, 'Face spoof detection with image distortion analysis', *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 746–761, 2015.
- [13] Z. Ming, M. Visani, M. Luqman and J.-C. Burie, 'A survey on anti-spoofing methods for facial recognition with rgb cameras of generic consumer devices', *Journal of Imaging*, vol. 6, no. 12, p. 139, 15th Dec. 2020. DOI: 10.3390/jimaging6120139. [Online]. Available: <https://arxiv.org/abs/2010.04145>.
- [14] J. Li, Y. Wang, T. Tan and A. Jain, 'Live face detection based on the analysis of fourier spectra', in *SPIE Proceedings*, vol. 5404, SPIE, 25th Aug. 2004, pp. 296–303. DOI: 10.1117/12.541955.
- [15] K. Kollreider, H. Fronthaler and J. Bigun, 'Evaluating liveness by face images and the structure tensor', in *Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'05)*. IEEE, 2005, pp. 75–80. DOI: 10.1109/autoid.2005.20.
- [16] W. Bao, H. Li, N. Li and W. Jiang, 'A liveness detection method for face recognition based on optical flow field', in *2009 International Conference on Image Analysis and Signal Processing*, IEEE, 2009, pp. 233–236. DOI: 10.1109/iasp.2009.5054589.
- [17] G. Pan, L. Sun, Z. Wu and S. Lao, 'Eyeblick-based anti-spoofing in face recognition from a generic webcam', in *2007 IEEE 11th International Conference on Computer Vision*. IEEE, 2007, pp. 1–8. DOI: 10.1109/iccv.2007.4409068.
- [18] L. Sun, G. Pan, Z. Wu and S. Lao, 'Blinking-based live face detection using conditional random fields', in *Advances in Biometrics*, S.-W. Lee and S. Z. Li, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 252–260, ISBN: 978-3-540-74549-5.

-
- [19] K. Kollreider, H. Fronthaler, M. I. Faraj and J. Bigun, ‘Real-time face detection and motion analysis with application in “liveness” assessment’, *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 548–558, 2007. DOI: 10.1109/TIFS.2007.902037.
- [20] X. Li, J. Komulainen, G. Zhao, P-C. Yuen and M. Pietikainen, ‘Generalized face anti-spoofing by detecting pulse from face videos’, in *2016 23rd International Conference on Pattern Recognition (ICPR)*. IEEE, Dec. 2016, pp. 4244–4249. DOI: 10.1109/icpr.2016.7900300.
- [21] E. Nowara, A. Sabharwal and A. Veeraraghavan, ‘Ppgsecure: Biometric presentation attack detection using photoplethysmograms’, in *2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017)*. IEEE, May 2017, pp. 56–62. DOI: 10.1109/fg.2017.16.
- [22] S. Liu, P. C. Yuen, S. Zhang and G. Zhao, ‘3d mask face anti-spoofing with remote photoplethysmography’, in *Computer Vision – ECCV 2016*, B. Leibe, J. Matas, N. Sebe and M. Welling, Eds., Cham: Springer International Publishing, 2016, pp. 85–100, ISBN: 978-3-319-46478-7.
- [23] Y. Liu, A. Jourabloo and X. Liu, ‘Learning deep models for face anti-spoofing: Binary or auxiliary supervision’, in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*. IEEE, Jun. 2018, pp. 389–398. DOI: 10.1109/cvpr.2018.00048.
- [24] S. Fernandes, S. Raj, E. Ortiz, I. Vintila, M. Salter, G. Urosevic and S. Jha, ‘Predicting heart rate variations of deepfake videos using neural ode’, in *2019 IEEE/CVF International Conference on Computer Vision Workshop (ICCVW)*. IEEE, Oct. 2019. DOI: 10.1109/iccvw.2019.00213.
- [25] U. A. Ciftci, I. Demir and L. Yin, ‘Fakecatcher: Detection of synthetic portrait videos using biological signals’, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 1–1, 2020. DOI: 10.1109/TPAMI.2020.3009287.
- [26] X. Tan, Y. Li, J. Liu and L. Jiang, ‘Face liveness detection from a single image with sparse low rank bilinear discriminative model’, in *Computer Vision – ECCV 2010*. Springer Berlin Heidelberg, 2010, pp. 504–517. DOI: 10.1007/978-3-642-15567-3_37.
- [27] J. Yang, Z. Lei, S. Liao and S. Li, ‘Face liveness detection with component dependent descriptor’, in *2013 International Conference on Biometrics (ICB)*. IEEE, Jun. 2013, pp. 1–6. DOI: 10.1109/icb.2013.6612955.
- [28] J. Määttä, A. Hadid and M. Pietikäinen, ‘Face spoofing detection from single images using micro-texture analysis’, in *2011 international joint conference on Biometrics (IJCB)*. IEEE, 2011, pp. 1–7.
- [29] J. Määttä, A. Hadid and M. Pietikäinen, ‘Face spoofing detection from single images using texture and local shape analysis’, in *IET biometrics*, 1. IET, 2012, vol. 1, pp. 3–10.

-
- [30] J. Komulainen, A. Hadid and M. Pietikainen, 'Context based face anti-spoofing', in *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*. IEEE, Sep. 2013, pp. 1–8. DOI: 10.1109/btas.2013.6712690.
- [31] N. Kose and J.-L. Dugelay, 'Countermeasure for the protection of face recognition systems against mask attacks', in *2013 10th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG)*. IEEE, Apr. 2013, pp. 1–6. DOI: 10.1109/fg.2013.6553761.
- [32] N. Kose and J.-L. Dugelay, 'Shape and texture based countermeasure to protect face recognition systems against mask attacks', in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, Jun. 2013.
- [33] J. Galbally and S. Marcel, 'Face anti-spoofing based on general image quality assessment', in *2014 22nd International Conference on Pattern Recognition*, 2014, pp. 1173–1178. DOI: 10.1109/ICPR.2014.211.
- [34] J. Galbally, S. Marcel and J. Fierrez, 'Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition', *IEEE Transactions on Image Processing*, vol. 23, no. 2, pp. 710–724, Feb. 2014. DOI: 10.1109/tip.2013.2292332.
- [35] Z. Boulkenafet, J. Komulainen and A. Hadid, 'Face anti-spoofing based on color texture analysis', in *2015 IEEE international conference on image processing (ICIP)*, 2015, pp. 2636–2640.
- [36] Z. Boulkenafet, J. Komulainen and A. Hadid, 'Face spoofing detection using colour texture analysis', *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1818–1830, Aug. 2016. DOI: 10.1109/tifs.2016.2555286.
- [37] K. Patel, H. Han and A. K. Jain, 'Secure face unlock: Spoof detection on smartphones', *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 10, pp. 2268–2283, 2016. DOI: 10.1109/TIFS.2016.2578288.
- [38] J. Yang, Z. Lei and S. Z. Li, 'Learn convolutional neural network for face anti-spoofing', *arXiv*, Aug. 2014. DOI: arXiv:1408.5601. eprint: arXiv:1408.5601.
- [39] A. Krizhevsky, I. Sutskever and G. E. Hinton, 'Imagenet classification with deep convolutional neural networks', in *Advances in Neural Information Processing Systems*, F. Pereira, C. Burges, L. Bottou and K. Weinberger, Eds., vol. 25, Curran Associates, Inc., 2012. [Online]. Available: <https://proceedings.neurips.cc/paper/2012/file/c399862d3b9d6b76c8436e924a68c45b-Paper.pdf>.

-
- [40] K. Patel, H. Han and A. Jain, 'Cross-database face antispoofing with robust feature representation', in *Chinese Conference on Biometric Recognition*, Springer International Publishing, 2016, pp. 611–619. DOI: 10.1007/978-3-319-46654-5_67.
- [41] A. Jourabloo, Y. Liu and X. Liu, 'Face de-spoofing: Anti-spoofing via noise modeling', in *Computer Vision – ECCV 2018*. Springer International Publishing, 2018, pp. 297–315. DOI: 10.1007/978-3-030-01261-8_18.
- [42] A. George and S. Marcel, 'Deep pixel-wise binary supervision for face presentation attack detection', in *2019 International Conference on Biometrics (ICB)*, 2019, pp. 1–8. DOI: 10.1109/ICB45273.2019.8987370.
- [43] T. de Freitas Pereira, A. Anjos, J. De Martino and S. Marcel, 'Can face anti-spoofing countermeasures work in a real world scenario?', in *2013 International Conference on Biometrics (ICB)*. IEEE, Jun. 2013. DOI: 10.1109/icb.2013.6612981.
- [44] S. Bharadwaj, T. Dhamecha, M. Vatsa and R. Singh, 'Computationally efficient face spoofing detection with motion magnification', in *2013 IEEE Conference on Computer Vision and Pattern Recognition Workshops*. IEEE, Jun. 2013, pp. 105–110. DOI: 10.1109/cvprw.2013.23.
- [45] S. Da, A. Pinto, Pedrini, Helio, W. Schwartz and A. Rocha, 'Video-based face spoofing detection through visual rhythm analysis', in *25th SIBGRAPI Conference on Graphics, Patterns and Images*. 2012, pp. 221–228.
- [46] A. Pinto, W. Robson Schwartz, H. Pedrini and A. De Rezende Rocha, 'Using visual rhythms for detecting video-based facial spoof attacks', *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 1025–1038, May 2015. DOI: 10.1109/tifs.2015.2395139.
- [47] Z. Xu, S. Li and W. Deng, 'Learning temporal features using lstm-cnn architecture for face anti-spoofing', in *2015 3rd IAPR Asian Conference on Pattern Recognition (ACPR)*. IEEE, Nov. 2015, pp. 141–145. DOI: 10.1109/acpr.2015.7486482.
- [48] T. Wang, J. Yang, Z. Lei, S. Liao and S. Li, 'Face liveness detection using 3d structure recovered from a single camera', in *2013 International Conference on Biometrics (ICB)*. IEEE, Jun. 2013, pp. 1–6. DOI: 10.1109/icb.2013.6612957.
- [49] Y. Atoum, Y. Liu, A. Jourabloo and X. Liu, 'Face anti-spoofing using patch and depth-based cnns', in *2017 IEEE International Joint Conference on Biometrics (IJCB)*. IEEE, Oct. 2017, pp. 319–328. DOI: 10.1109/btas.2017.8272713.
- [50] Z. Wang, C. Zhao, Y. Qin, Q. Zhou and Z. Lei, 'Exploiting temporal and depth information for multi-frame face anti-spoofing', *CoRR*, vol. abs/1811.05118, 2018. arXiv: 1811.05118. [Online]. Available: <http://arxiv.org/abs/1811.05118>.

-
- [51] K. B. Raja, P. Wasnik, R. Raghavendra and C. Busch, ‘Robust face presentation attack detection on smartphones : An approach based on variable focus’, in *2017 IEEE International Joint Conference on Biometrics (IJCB)*, 2017, pp. 651–658. DOI: 10.1109/BTAS.2017.8272753.
- [52] G. Pan, L. Sun, Z. Wu and Y. Wang, ‘Monocular camera-based face liveness detection by combining eyeblink and scene context’, *Telecommunication Systems*, vol. 43, no. 3, pp. 215–225, 4th Aug. 2010. DOI: 10.1007/s11235-010-9313-3.
- [53] N. Damer, N. Spiller, M. Fang, F. Boutros, F. Kirchbuchner and A. Kuijper, ‘Pw-mad: Pixel-wise supervision for generalized face morphing attack detection’, in *Advances in Visual Computing*, G. Bebis, V. Athitsos, T. Yan, M. Lau, F. Li, C. Shi, X. Yuan, C. Mousas and G. Bruder, Eds., Cham: Springer International Publishing, 2021, pp. 291–304, ISBN: 978-3-030-90439-5.
- [54] M. Fang, N. Damer, F. Boutros, F. Kirchbuchner and A. Kuijper, ‘Iris presentation attack detection by attention-based and deep pixel-wise binary supervision network’, in *2021 IEEE International Joint Conference on Biometrics (IJCB)*, 2021, pp. 1–8. DOI: 10.1109/IJCB52358.2021.9484343.
- [55] M. Fang, F. Boutros and N. Damer, *Intra and cross-spectrum iris presentation attack detection in the nir and visible domains using attention-based and pixel-wise supervised learning*, 2022. arXiv: 2205.02573 [cs . CV].
- [56] F. N. Iandola, M. W. Moskewicz, S. Karayev, R. B. Girshick, T. Darrell and K. Keutzer, ‘Densenet: Implementing efficient convnet descriptor pyramids’, *CoRR*, vol. abs/1404.1869, 2014. arXiv: 1404.1869. [Online]. Available: <http://arxiv.org/abs/1404.1869>.
- [57] E. Fink, *Ios depth capture application*. [Online]. Available: <https://github.com/mantoone/DepthCapture> (visited on 5th Apr. 2022).
- [58] Z. Boulkenafet, J. Komulainen, L. Li, X. Feng and A. Hadid, ‘OULU-NPU: A mobile face presentation attack database with real-world variations’, in *12th IEEE International Conference on Automatic Face Gesture Recognition (FG 2017)*, 2017, pp. 612–618. DOI: 10.1109/FG.2017.77.
- [59] J. Rothman, *Create your successful agile project*. The Programmatic Programmers, 2017.
- [60] T. S. Silva, ‘Deeplab image semantic segmentation network’, Jan. 2018. [Online]. Available: https://sthalles.github.io/deep_segmentation_network/.
- [61] Numpy, *About: Numpy*. [Online]. Available: <https://numpy.org/about/>.
- [62] @. Opencv, *About: Opencv*. [Online]. Available: <https://opencv.org/about/>.
- [63] @. Pytorch, *About: Pytorch*. [Online]. Available: <https://pypi.org/project/torch/>.
- [64] P. C. Team, *Project description: Torchvision*, Mar. 2022. [Online]. Available: <https://pypi.org/project/torchvision/> (visited on 18th Mar. 2022).
-

-
- [65] M. Team, *About: Mediapipe*. [Online]. Available: <https://google.github.io/mediapipe/> (visited on 1st Apr. 2022).

A Original Task Specification

Use computer vision to create prototypes for Spoofing Detection

Project owner / company: Mobai AS

About Mobai: Mobai is a facial biometrics company working with ML and image processing to create products and solutions to enable trust in society. We are located at BrightHouse Mustad. We are used to working with students, and our reflection is that when we invest our time and dedication into helping the students it is both more fun and enables better academic results.

Thesis description: Face recognition based identity authentication system has become prevalent and been widely adopted around the world. One critical component of a face recognition system is to detect the person who is presenting in front of the camera is a live person and thus avoiding spoofs (attack instruments such as still images and videos). In this bachelor thesis we want to group to experiment with one or more techniques for detection attack detection. The task involves computer vision and AI/ML challenges. Create a prototype using minimum one of these approaches:

- Eye gaze detection is to track eye movements using deep learning techniques, which can be used to detect the user's
- Detecting head micro-movement can be used to prevent photo-based attacks (such as printing photo attack, or display a photo on an iPad), for instance, measuring the movement correlation between head/face and the background. If it is a photo-based attack, the head micro-movement direction shall be consistent to the background micro-movement
- Use True-Depth cameras (iPhone X+) or Time-of-flight for selected android phones to utilize depth information to detect spoofing attacks.

Contact person: Brage Strand, 40490411, brage@mobai.bio

We can participate on November 3rd.

B Group Contract



DEPARTMENT OF COMPUTER SCIENCE (IDI)

IDATG2900 - BACHELOR THESIS

Group Contract

Authors:

Hamza Azim, Milosz Antoni Wudarczyk, Kristian Amundsen Øhman-Norén

Spring, 2022

Table of Contents

1	Group Information	1
1.1	Group Members	1
1.2	Roles and Responsibilities	1
1.3	Communication	1
2	Work	1
2.1	Academic Goals	1
2.2	Task Goals	1
2.3	Work Expectations	1
2.4	Work models and style	2
3	Time-usage and Attendance	2
3.1	Attendance	2
3.1.1	Absences	2
3.2	Work Schedule	2
3.3	Workload	2
3.4	Responsibility	2
4	Consequences	3
4.1	Breach of contract	3
4.1.1	First Breach	3
4.1.2	Second Breach	3
4.1.3	Final Breach	3
4.1.4	Exception clauses	3
5	Signatures/Agreement	4

1 Group Information

1.1 Group Members

Hamza Azim - Digital Infrastructure and Cyber Security - hamzaa@stud.ntnu.no
Milosz Antoni Wudarczyk - Engineering in Computer Science - miloszaw@stud.ntnu.no
Kristian Amundsen Øhman-Norén - Engineering in Computer Science - kristaoh@stud.ntnu.no

1.2 Roles and Responsibilities

Hamza Azim - Security and network
Milosz Antoni Wudarczyk - Logic Lead
Kristian Amundsen Øhman-Norén - Group Leader and Organizer

1.3 Communication

All digital communication between group members is to be condoned within a designated server on the Discord application. General communication happens via text-based channels. Voice and video channels are to be utilized within designated meeting-hours. Physical meetings are expected to take place when the university deems it safe.

2 Work

2.1 Academic Goals

The academic goals set for this group project can be described as high (A). We aim to achieve the eureka prize for IIK/IDI.

2.2 Task Goals

The goals of the bachelor project is to create a python package that can successfully detect whether or not an attack is taking place when performing facial recognition. We seek to be able to detect level 1 and 2 attacks primarily, and if time permits, level 3 attacks.

2.3 Work Expectations

Work expectations are set at an individual level of which all group members each are individually responsible for their designated tasks. The work is expected to hold a sense of quality that live up to the high ambitions that are set. A focus on collaboration will allow us to make sure that all work is in line with the given requirements. There is also an expectation that each group member shows up to each scheduled meeting.

2.4 Work models and style

The CI (Continuous Integration) model will be used for the different phases of the project. Work expectations go hand in hand with established work models. The group intends to work in an agile style scrum environment. This effectively means that each group meeting will act like miniature sprints with pre-defined goals to reach for each meeting.

3 Time-usage and Attendance

3.1 Attendance

Each group member is expected to be available within the work schedule defined in this contract. If deemed absolutely necessary, clauses will allow for more work than scheduled, and each member is contractually obligated to accept this extra work. The group will be condoning physical work days, where we meet up and work through problems together. When physical meetings cannot be held, meetings will take place in a server on the Discord application, in a designated digital meeting space.

3.1.1 Absences

Absences will be taken seriously, unless they are for a good reason (doctors appointment, etc.). After 3 absences, the group member owes the others a pizza. If the group member has 10 percent absences, a formal warning will be sent to the member in addition to the coordinator (Kiran Raja). If the group member has 15 percent absences, the group member will be removed from the group.

3.2 Work Schedule

The group will meet for three work sessions a week. All of these meetings may not always be completely necessary, and there will be room to reschedule if there is a clash with other subjects or for personal reasons. The meetings are set as such: two 6-hour days (Monday and Friday) and one 8-hour day (Thursday).

For each meeting, 30-60min at the start of each day - meeting with recap of what has been done in the last meeting, and formulation of what needs to be done for the rest of the meeting. At the end of the day, there will be 15min-20min recap session of what has been accomplished on the current day.

3.3 Workload

Try, as far as it allows, to keep our free-time free, and be able to work through the task that is given within the specified schedule. Workload should be acceptable, and not too intensive, while at the same time we need to keep the workload realistically scaled with the task at hand. A plan for the project has been created in the form of a Gantt-diagram. In this diagram, scheduled workload is pre-calculated, and it is expected of each group member that the tasks listed are to be completed in the timeslot where they are placed.

3.4 Responsibility

Each group member is expected to take responsibility for their assigned task. Larger tasks will be split into smaller sections where we will collaborate to ensure completion, quality and consistency.

4 Consequences

4.1 Breach of contract

If a group member is found to breach any point established by this contract, a process will be initiated to ensure the work continues as planned. This process will be based on the number and severity of breaches.

4.1.1 First Breach

If a group member breaches this contract once, a friendly warning will be given. This will not result in any major consequences. This will also result the breach being a point on the agenda for the next meeting. A formal email will also be sent to all group members.

4.1.2 Second Breach

If a group member persists the breach, or performs breach of contract on any other point after the first breach, the project supervisor will be contacted, and a larger-scale meeting will take place to ensure the group member will follow the contract in the future.

4.1.3 Final Breach

If, after the last meeting with the supervisor, the breach persists, the group member who performs the breach will be cut off from the group, and will therefore be unable to re-enter the project.

4.1.4 Exception clauses

Personal reasons

If agreed upon within the group, and there is unanimous agreement, the group member will be exempt from a pre-decided number of meetings. However, if a member is unable to inform the group beforehand, and the group decides the absence may be exempt, this will also suffice.

Illness

If a group member is seriously ill, they are to be exempt from meetings until in good health.

Quarantine

As far as it is viable, the member should still attempt to attend the meetings digitally, unless their condition does not allow for that.

5 Signatures/Agreement

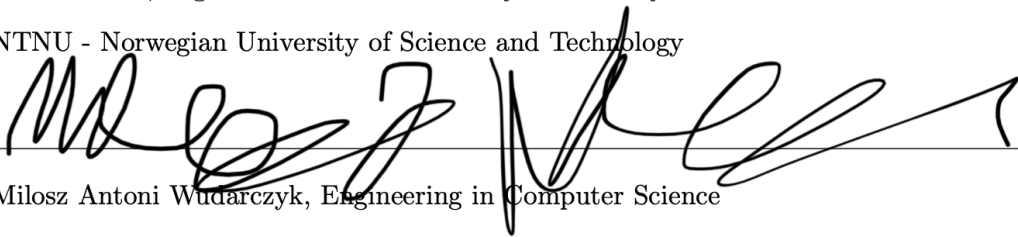
By signing this document, you are contractually accepting clauses for group collaboration in relation to this project. All points mentioned in this document serve as a point of reference for work ethic and responsibility for the entire duration of the project.

Signatures

Approved:  _____

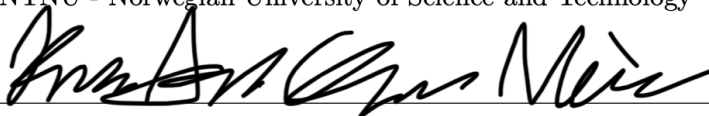
Hamza Azim, Digital Infrastructure and Cyber Security

NTNU - Norwegian University of Science and Technology

Approved:  _____

Milosz Antoni Wudarczyk, Engineering in Computer Science

NTNU - Norwegian University of Science and Technology

Approved:  _____

Kristian Amundsen Øhman-Norén, Engineering in Computer Science

NTNU - Norwegian University of Science and Technology

C Project Contract

Fastsatt av prorektor for utdanning 10.12.2020

STANDARDAVTALE

om utføring av studentoppgave i samarbeid med ekstern virksomhet

Avtalen er ufravikelig for studentoppgaver (heretter oppgave) ved NTNU som utføres i samarbeid med ekstern virksomhet.

Forklaring av begrep

Opphavsrett

Er den rett som den som skaper et åndsverk har til å fremstille eksemplarer av åndsverket og gjøre det tilgjengelig for allmennheten. Et åndsverk kan være et litterært, vitenskapelig eller kunstnerisk verk. En studentoppgave vil være et åndsverk.

Eiendomsrett til resultater

Betyr at den som eier resultatene bestemmer over disse. Utgangspunktet er at studenten eier resultatene fra sitt studentarbeid. Studenten kan også overføre eiendomsretten til den eksterne virksomheten.

Bruksrett til resultater

Den som eier resultatene kan gi andre en rett til å bruke resultatene, f.eks. at studenten gir NTNU og den eksterne virksomheten rett til å bruke resultatene fra studentoppgaven i deres virksomhet.

Prosjektbakgrunn

Det partene i avtalen har med seg inn i prosjektet, dvs. som vedkommende eier eller har rettigheter til fra før og som brukes i det videre arbeidet med studentoppgaven. Dette kan også være materiale som tredjepersoner (som ikke er part i avtalen) har rettigheter til.

Utsatt offentliggjøring

Betyr at oppgaven ikke blir tilgjengelig for allmennheten før etter en viss tid, f.eks. før etter tre år. Da vil det kun være veileder ved NTNU, sensorene og den eksterne virksomheten som har tilgang til studentarbeidet de tre første årene etter at studentarbeidet er innlevert.

1. Avtaleparter

Norges teknisk-naturvitenskapelige universitet (NTNU) Institutt: Institutt for datateknologi og informatikk (IDI)
Veileder ved NTNU: Kiran Raja e-post og tlf: kiran.raja@ntnu.no ,
Ekstern virksomhet: Mobai Ekstern virksomhet sin kontaktperson, e-post og tlf.: Brage Strand, Brage@mobai.bio , +4740490411
Student: Hamza Azim (hamzaa@stud.ntnu.no) Fødselsdato: 10.08.2000
Student: Milosz Antoni Wudarczyk (miloszaw@stud.ntnu.no) Fødselsdato: 18.12.2000
Student: Kristian Amundsen Øhman-Norén (kristaoh@stud.ntnu.no) Fødselsdato: 19.06.2000

Partene har ansvar for å klarere eventuelle immaterielle rettigheter som studenten, NTNU, den eksterne eller tredjeperson (som ikke er part i avtalen) har til prosjektbakgrunn før bruk i forbindelse med utførelse av oppgaven. Eierskap til prosjektbakgrunn skal fremgå av eget vedlegg til avtalen der dette kan ha betydning for utførelse av oppgaven.

2. Utførelse av oppgave

Studenten skal utføre: (sett kryss)

Masteroppgave	
Bacheloroppgave	X
Prosjektoppgave	
Annen oppgave	

Startdato: 17.01.2022

Sluttdato: 20.05.2022

Oppgavens arbeidstittel er:

«Presentation attack detection for smartphone face recognition»

Ansvarlig veileder ved NTNU har det overordnede faglige ansvaret for utforming og godkjenning av prosjektbeskrivelse og studentens læring.

3. Ekstern virksomhet sine plikter

Ekstern virksomhet skal stille med en kontaktperson som har nødvendig faglig kompetanse til å gi studenten tilstrekkelig veiledning i samarbeid med veileder ved NTNU. Ekstern kontaktperson fremgår i punkt 1.

Formålet med oppgaven er studentarbeid. Oppgaven utføres som ledd i studiet. Studenten skal ikke motta lønn eller lignende godtgjørelse fra den eksterne for studentarbeidet. Utgifter knyttet til gjennomføring av oppgaven skal dekkes av den eksterne. Aktuelle utgifter kan for eksempel være reiser, materialer for bygging av prototyp, innkjøp av prøver, tester på lab, kjemikalier. Studenten skal klarere dekning av utgifter med ekstern virksomhet på forhånd.

Ekstern virksomhet skal dekke følgende utgifter til utførelse av oppgaven:

Ingen planlagte innkjøp. Eventuelle behov skal godkjennes av kontaktperson før innkjøpet.

Dekning av utgifter til annet enn det som er oppført her avgjøres av den eksterne underveis i arbeidet.

4. Studentens rettigheter

Studenten har opphavsrett til oppgaven¹. Alle resultater av oppgaven, skapt av studenten alene gjennom arbeidet med oppgaven, eies av studenten med de begrensninger som følger av punkt 5, 6 og 7 nedenfor. Eiendomsretten til resultatene overføres til ekstern virksomhet hvis punkt 5 b er avkrysset eller for tilfelle som i punkt 6 (overføring ved patenterbare oppfinnelser).

I henhold til lov om opphavsrett til åndsverk beholder alltid studenten de ideelle rettigheter til eget åndsverk, dvs. retten til navngivelse og vern mot krenkende bruk.

Studenten har rett til å inngå egen avtale med NTNU om publisering av sin oppgave i NTNUs institusjonelle arkiv på Internett (NTNU Open). Studenten har også rett til å publisere oppgaven eller deler av den i andre sammenhenger dersom det ikke i denne avtalen er avtalt begrensninger i adgangen til å publisere, jf. punkt 8.

5. Den eksterne virksomheten sine rettigheter

Der oppgaven bygger på, eller videreutvikler materiale og/eller metoder (prosjektbakgrunn) som eies av den eksterne, eies prosjektbakgrunnen fortsatt av den eksterne. Hvis studenten skal utnytte resultater som inkluderer den eksterne sin prosjektbakgrunn, forutsetter dette at det er inngått egen avtale om dette mellom studenten og den eksterne virksomheten.

¹ Jf. Lov om opphavsrett til åndsverk mv. av 15.06.2018 § 1

Alternativ a) (sett kryss) Hovedregel

<input type="checkbox"/>	Ekstern virksomhet skal ha bruksrett til resultatene av oppgaven
--------------------------	--

Dette innebærer at ekstern virksomhet skal ha rett til å benytte resultatene av oppgaven i egen virksomhet. Retten er ikke-eksklusiv.

Alternativ b) (sett kryss) Unntak

<input checked="" type="checkbox"/>	Ekstern virksomhet skal ha eiendomsretten til resultatene av oppgaven og studentens bidrag i ekstern virksomhet sitt prosjekt
-------------------------------------	---

Begrunnelse for at ekstern virksomhet har behov for å få overført eiendomsrett til resultatene:

Løsningene vil være tett knyttet til Mobais produktområde. Vederlagsfri overføring av alt eierskap til alle resultater er en forutsetning for samarbeidet.

6. Godtgjøring ved patenterbare oppfinnelser

Dersom studenten i forbindelse med utførelsen av oppgaven har nådd frem til en patenterbar oppfinnelse, enten alene eller sammen med andre, kan den eksterne kreve retten til oppfinnelsen overført til seg. Dette forutsetter at utnyttelsen av oppfinnelsen faller inn under den eksterne sitt virksomhetsområde. I så fall har studenten krav på rimelig godtgjøring. Godtgjøringen skal fastsettes i samsvar med arbeidstakeroppfinnelsesloven § 7. Fristbestemmelsene i § 7 gis tilsvarende anvendelse.

7. NTNU sine rettigheter

De innleverte filer av oppgaven med vedlegg, som er nødvendig for sensur og arkivering ved NTNU, tilhører NTNU. NTNU får en vederlagsfri bruksrett til resultatene av oppgaven, inkludert vedlegg til denne, og kan benytte dette til undervisnings- og forskningsformål med de eventuelle begrensninger som fremgår i punkt 8.

8. Utsatt offentliggjøring

Hovedregelen er at studentoppgaver skal være offentlige.

Sett kryss

<input type="checkbox"/>	Oppgaven skal være offentlig
--------------------------	------------------------------

I særlige tilfeller kan partene bli enige om at hele eller deler av oppgaven skal være undergitt utsatt offentliggjøring i maksimalt tre år. Hvis oppgaven unntas fra offentliggjøring, vil den kun være tilgjengelig for student, ekstern virksomhet og veileder i denne perioden. Sensurkomiteen vil ha tilgang til oppgaven i forbindelse med sensur. Student, veileder og sensorer har taushetsplikt om innhold som er unntatt offentliggjøring.

Oppgaven skal være underlagt utsatt offentliggjøring i (sett kryss hvis dette er aktuelt):

Sett kryss

Sett dato

	ett år	
x	to år	31.01.2024
	tre år	

Behovet for utsatt offentliggjøring er begrunnet ut fra følgende:

Oppgaven omhandler produktområdet som betegnes som Presentation Attack Detection. Dette området anses for å være særlig sensitivt for Mobai både med tanke på kommersielle hensyn og IT-sikkerhetsmessige hensyn. Ønsker i prinsippet så lang utsettelse som mulig, men antar at to år bør være rimelig. Merk at bedriften er åpen for offentliggjøring tidligere hvis oppgaven blir av mindre sensitiv karakter.

Dersom partene, etter at oppgaven er ferdig, blir enig om at det ikke er behov for utsatt offentliggjøring, kan dette endres. I så fall skal dette avtales skriftlig.

Vedlegg til oppgaven kan unntas ut over tre år etter forespørsel fra ekstern virksomhet. NTNU (ved instituttet) og student skal godta dette hvis den eksterne har saklig grunn for å be om at et eller flere vedlegg unntas. Ekstern virksomhet må sende forespørsel før oppgaven leveres.

De delene av oppgaven som ikke er undergitt utsatt offentliggjøring, kan publiseres i NTNUs institusjonelle arkiv, jf. punkt 4, siste avsnitt. Selv om oppgaven er undergitt utsatt offentliggjøring, skal ekstern virksomhet legge til rette for at studenten kan benytte hele eller deler av oppgaven i forbindelse med jobbsøknader samt videreføring i et master- eller doktorgradsarbeid.

9. Generelt


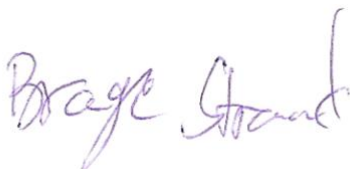

Denne avtalen skal ha gyldighet foran andre avtaler som er eller blir opprettet mellom to av partene som er nevnt ovenfor. Dersom student og ekstern virksomhet skal inngå avtale om konfidensialitet om det som studenten får kjennskap til i eller gjennom den eksterne virksomheten, kan NTNUs standardmal for konfidensialitetsavtale benyttes.

Den eksterne sin egen konfidensialitetsavtale, eventuell konfidensialitetsavtale den eksterne har inngått i samarbeidprosjekter, kan også brukes forutsatt at den ikke inneholder punkter i motstrid med denne avtalen (om rettigheter, offentliggjøring mm). Dersom det likevel viser seg at det er motstrid, skal NTNUs standardavtale om utføring av studentoppgave gå foran. Eventuell avtale om konfidensialitet skal vedlegges denne avtalen.

Eventuell uenighet som følge av denne avtalen skal søkes løst ved forhandlinger. Hvis dette ikke fører frem, er partene enige om at tvisten avgjøres ved voldgift i henhold til norsk lov. Tvisten avgjøres av sorenskriveren ved Sør-Trøndelag tingrett eller den han/hun oppnevner.

Denne avtale er signert i fire eksemplarer hvor partene skal ha hvert sitt eksemplar. Avtalen er gyldig når den er underskrevet av NTNU v/instituttleder.

Signaturer:

Instituttleder:	
Dato: 15/02/22	
Veileder ved NTNU: Kiran Raja	
Dato:	
Ekstern virksomhet: Mobai	
Dato: 29.01.2022	
Student: Hamza Azim	
Dato: 21.01.2022	

Student: Milosz Antoni Wudarczyk

Milosz A Wudarczyk

Dato: 21.01.2022

Student: Kristian Amundsen Øhman-Norén

Kristian Amundsen Øhman-Norén

Dato: 21.01.2022

D Confidentiality Contract

Fastsatt av prorektor for utdanning 10.12.2020

STANDARDMAL ved avtale om konfidensialitet mellom student og ekstern virksomhet i forbindelse med studentens utførelse av oppgave (master-, bachelor- eller annen oppgave) i samarbeid med ekstern virksomhet, jf. punkt 9 i standardavtale om utføring av oppgave i samarbeid med ekstern virksomhet.

Student ved NTNU: Hamza Azim Fødselsdato: 10.08.2000

Student ved NTNU: Milosz Antoni Wudarczyk Fødselsdato: 18.12.2000
--

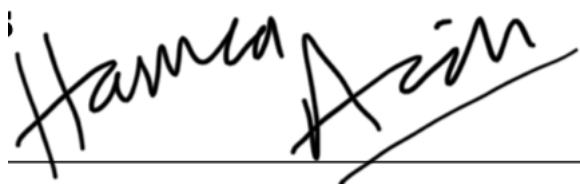
Student ved NTNU: Kristian Amundsen Øhman-Norén Fødselsdato: 19.06.2000
--

Ekstern virksomhet: Mobai AS

1. Studenten skal utføre oppgave i samarbeid med ekstern virksomhet som ledd i sitt studium ved NTNU.
2. Studenten forplikter seg til å bevare taushet om det han/hun får vite om tekniske innretninger og fremgangsmåter samt drifts- og forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde for den eksterne virksomheten. Det er den eksterne sitt ansvar å sørge for å synliggjøre og tydeliggjøre hvilken informasjon dette omfatter.
3. Studenten er forpliktet til å bevare taushet om dette i 5 år regnet fra sluttdato.
4. Kravet om konfidensialitet gjelder ikke informasjon som:
 - a) var allment tilgjengelig da den ble mottatt
 - b) ble mottatt lovlig fra tredjeperson uten avtale om taushetsplikt
 - c) ble utviklet av studenten uavhengig av mottatt informasjon
 - d) partene er forpliktet til å gi opplysninger om i samsvar med lov eller forskrift eller etter pålegg fra offentlig myndighet.

Signaturer

Student: Hamza Azim



Dato: 27.01.2022

Student: Milosz Antoni Wudarczyk

A handwritten signature in black ink, appearing to read 'Milosz Antoni Wudarczyk', written over a horizontal line.

Dato: 27.01.2022

Student: Kristian Amundsen Øhman-Norén

A handwritten signature in black ink, appearing to read 'Kristian Amundsen Øhman-Norén', written over a horizontal line.

Dato: 27.01.2022

Ekstern Virksomhet: Mobai AS

E Project Plan



DEPARTMENT OF COMPUTER SCIENCE (IDI)

IDATG2900 - BACHELOR THESIS

Project Plan

Author:

Hamza Azim, Milosz Antoni Wudarczyk, Kristian Amundsen Øhman-Norén

Spring, 2022

Table of Contents

1	Goal and Frameworks	1
1.1	Background	1
1.2	Project Goal	1
1.3	Frameworks	1
2	Scope	1
2.1	Problem Area	1
2.2	Scope Limiting Factors	2
2.3	Problem Statement	2
3	Project Organization	2
3.1	Group Members	2
3.2	Responsibilities and roles	2
3.3	Routines and rules	3
4	Planning, Follow-Up and Reporting	3
4.1	Meeting's structure	3
4.2	Points of decision	3
4.3	Summaries & reports	3
5	Organization of Quality Measures	3
5.1	Standards and Tools	3
5.2	Plans for testing	3
5.3	Risk Analysis	4
5.3.1	Risk assessment matrix	4
5.3.2	Identified risks	4
6	Plan for Project Execution	5
6.1	Gantt-diagram	5

1 Goal and Frameworks

1.1 Background

We have been tasked by Mobai, a security & biometrics company, to develop a working prototype for detection of facial-recognition spoofing attempts on the background of a Bachelor Thesis for NTNU during Spring of 2022.

1.2 Project Goal

The projects surrounds itself with developing a working prototype package which can be readily used by the task issuer to provide a higher level of security measures for related facial-recognition products. This prototype will have multiple levels of spoofing detection, which attempts to identify when such an attack occurs, as well as what the attack consists of.

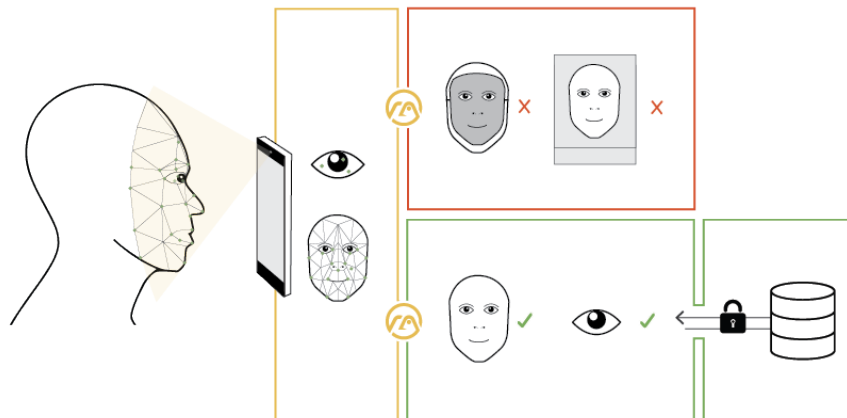
1.3 Frameworks

We will utilize an agile workflow consisting of a combination of frameworks suited best to our needs (Scrum-like continuous integration).

We use a Gantt-diagram (featured later in this document) to describe what we envision our progress will look like in terms of the different phases we will go through. Under the development phase, which makes up most of our plan, we use a Scrum-like approach, with a 3 week "long-sprint" followed by a "sprint review" used for feedback & revisions. During each week of the "sprint" we follow a model closely related to Continuous Integration. The Continuous Integration model aims to provide constant development on features in small cohesive updates.

2 Scope

2.1 Problem Area



Spoofing of facial-based authentication systems is the main problem area for this task. As that is the case, it is the main focus for our project, covering the entirety of the scope.

The types of presentation attacks which can be performed on facial-recognition-based authentication systems vary, both in execution and complexity. Complexity tends to scale with the difficulty of execution and difficulty of detection, with the more sophisticated attacks being harder to detect.

At the same time these attacks also tend to be harder to perform, often requiring substantial time, dedication and skill to successfully complete. The goal of such attacks is to trick the system into granting access or authenticating a user in cases where it shouldn't.

We will be focusing on detection of such presentation attacks on smartphones in particular, something which can pose many difficulties on its own. First and foremost, the mobile aspect of smartphones brings with it the potential for a variety of environments in which the user can find themselves in. In certain environments this can cause difficulties regarding presentation attack detection, as the clarity/quality of the captured image might not be optimal.

2.2 Scope Limiting Factors

The main scope limiting factors for this project will be our knowledge of python, implementation difficulties, as well as the libraries available to us. We have to also make ourselves content with the fact that new spoofing methods appear everyday and we cannot possibly develop something which would detect every form of attack & be 100% foolproof. That is not to imply our package will be of low quality, as the spoofing methods currently known to us and the way to detect them will be implemented in such a fashion as to assure high level of success.

Being that the group has little previous experience with python, it is something which will initially limit progress while we get used to the language. This should not be a major factor though, as learning a new programming language is not something new for the members of the group. Although, it is something which might affect a more significant factor, time. The main reason for the need of scope restriction is the amount of time we have to accomplish the task. Being limited to a couple of months, alongside unforeseen events, such as glitches & bugs as is often the case with code development, we have to carefully plan ahead to assure adequate leeway. Due to the time restraint, we will focus firstly on implementing less complex ways of detecting spoofing attacks, continuing onto more advanced methods as we progress.

2.3 Problem Statement

"Presentation attack detection for smartphone face recognition"

We are expected to develop a system which can detect spoofing attacks at various levels of complexity, implementing the detection algorithms as we go, based on how far we get. Meaning, we'll start at the base package being able to detect some rudimentary attacks (body & eye movement), gradually implementing new modules with the ability to detect more advanced attacks (3D modelling, "deepfakes" & masks).

3 Project Organization

3.1 Group Members

Hamza Azim - Digital Infrastructure and Cyber Security - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - Engineering in Computer Science - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - Engineering in Computer Science - kristaoh@stud.ntnu.no

3.2 Responsibilities and roles

Hamza Azim - Security, Report & Research

Milosz Antoni Wudarczyk - Development, Logic & Design

Kristian Amundsen Øhman-Norén - Documentation, Organization & Management

3.3 Routines and rules

Routines and rules are stated in high detail within a dedicated group contract. This contract has been created internally, with our own set of rules and standards. The group contract is, as its own entity, included at the end of this document.

4 Planning, Follow-Up and Reporting

4.1 Meeting's structure

Work meetings, internal to the group, happen three times a week:

Monday 10:00-16:00, Thursday 10:00-18:00, Friday 10:00-16:00

Status meetings with the supervisor and task issuer happen once a week:

Thursday 13:00-14:00

4.2 Points of decision

If the group comes to a crossroads regarding development of the package at which it cannot decisively choose the direction of work, a consultation meeting with the supervisor should be scheduled.

4.3 Summaries & reports

After each meeting, a summary is written of the work done, with conclusions of the present meeting & plans for next meeting. Alongside this, under development, notes & keywords are added to what will be the final report, to assure as much details and relevant information is featured and not forgotten.

5 Organization of Quality Measures

5.1 Standards and Tools

The designated programming language has been decided to be Python. We will be utilizing the newest version (3.9 as of writing) of the language. The group will be using PyCharm as an IDE, utilizing helpful plugin's such as "Code with me" to allow for synchronous coding between developers on the project. OS usage (Windows, Linux and macOS) for each group member varies, something which plays a positive role as it allows for testing of the package on differing systems & configurations.

5.2 Plans for testing

Mobai (the task issuer) and NTNU will provide physical masks, paper pictures, testing devices & more to assure we are able to perform tests on the functionality of the code. The test cases will be different for each development phase. This is due to the nature of the project's phases having different features. We will be continually discussing and developing unit tests at the end of each development phase in an attempt to streamline the testing process.

5.3 Risk Analysis

5.3.1 Risk assessment matrix

	High					
Likelihood	L4	1 2				
	L3					
	L2			4		
	L1				3 5	
	Low	C1	C2	C3	C4	High
		Consequence				

5.3.2 Identified risks

Identified risks concerning this project are elaborated upon below.

1- Group member is sick

Consequence: 1

Likelihood: 4

Context: Related to illness within the group that may lead to a group member being unable to attend meetings or perform assigned work. This is a likely scenario in current times with the frequency in cases of the COVID-19 virus. The group expects each member to follow the FHI guidelines to avoid sickness to the extent that it is possible.

2- Group member is unable to attend physical meetings

Consequence: 1

Likelihood: 4

Context: A member may be unable to attend meetings for a variety of reasons. To the extent that is possible, they will attend the meetings digitally. Internal meetings will be attended on discord, and meetings with mobai will be attended through their teams channel.

3- Loss of group member

Consequence: 4

Likelihood: 1

Context: A group member is removed from or leaves the group. This will leave more work for the rest of the group to do, and will likely affect the quality of both the bachelor thesis and the package to be delivered to mobai.

4- Processing time of code is unacceptable

Consequence: 3

Likelihood: 2

Context: The code written by the group is poorly optimised and is too resource taxing to be acceptable.

5- Data sets removed

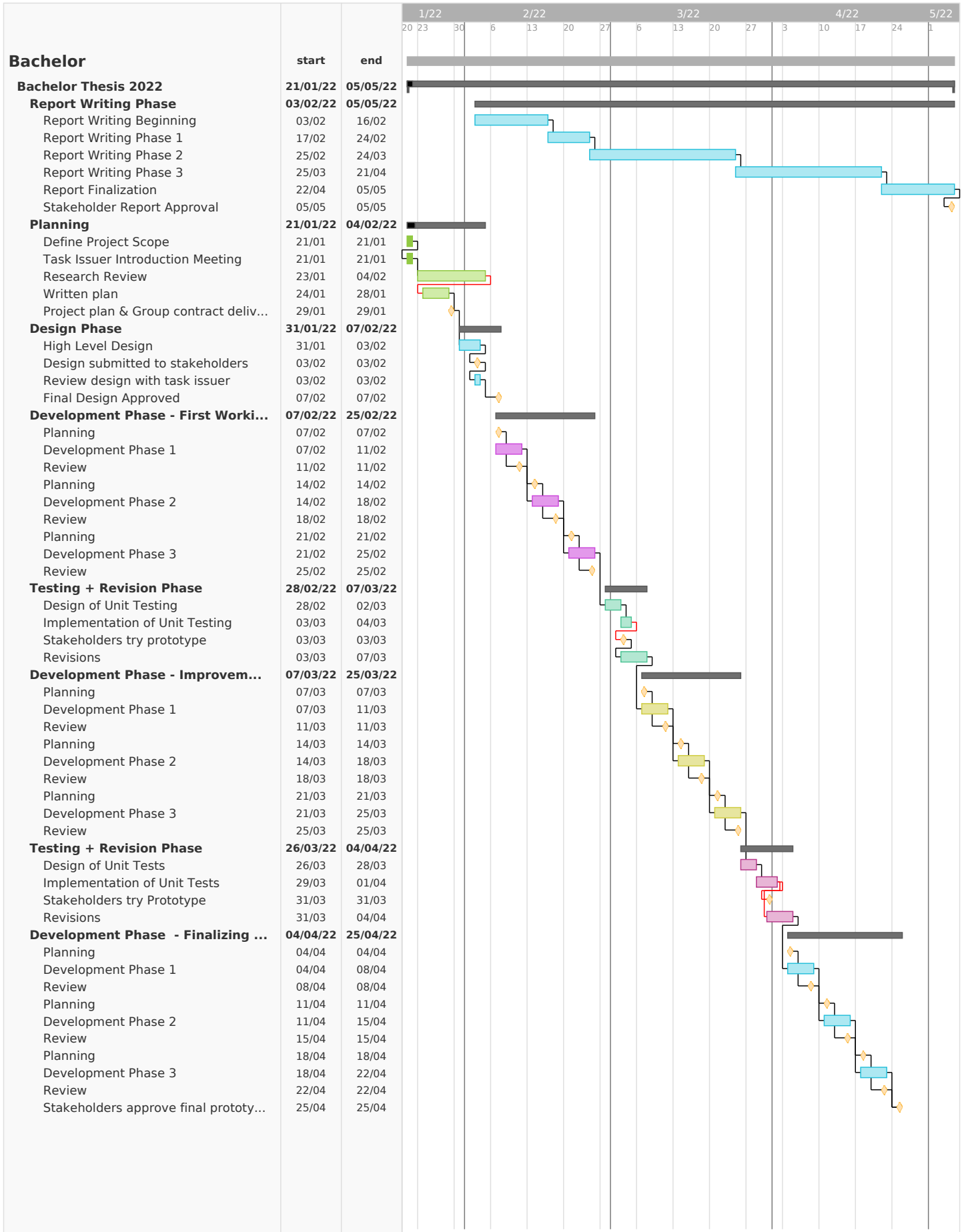
Consequence: 4

Likelihood: 1

Context: This includes images of people that will be used to analyse and score. In context to laws such as GDPR which can lead to Mobai or the group having to delete their data sets. This will greatly

6 Plan for Project Execution

6.1 Gantt-diagram



The Gantt-diagram describes the entire project and its phases in rich detail. This diagram illustrates how we plan to execute the project as a whole, and what actions each development phase requires. All this is put into a realistic timeline. Activities, milestones and points of decision have been decided, which have been added and labelled in the figure above.

F Meeting Summaries



DEPARTMENT OF COMPUTER SCIENCE (IDI)

IDATG2900 - BACHELOR THESIS

Meeting Summaries

Author:
Kristian Amundsen Øhman-Norén

Spring, 2022

MEETING SCHEDULE

The meetings have a set schedule for each week. This schedule consists of three internal group-meetings, as well as one meeting with our task-issuer and our supervisor. The schedule for the group-meetings are defined as:

Mondays 10:00-15:00

Thursdays 10:00-17:00

Fridays 10:00-15:00

The weekly meeting with the task-issuer and supervisor is scheduled to take place in the middle of each Thursday-meeting - at 13:00, lasting one hour.

This meeting schedule was slightly changed a few weeks into the project. All meeting-times were pushed back one hour, so they started at 11, rather than 10. As a consequence, each meeting also generally ended one hour later than scheduled. This decision was made based on common agreement within the group. The weekly task-issuer meeting remained in the same time-slot.

Table of Contents

1	Internal Introduction Meeting 17.01.2022	2
2	Introduction Meeting with Supervisor and Task issuer 21.01.2022	3
3	Meeting and work session for work on group contract and project plan 24.01.2022	4
4	Finalizing the Project Plan and update meeting with Mobai 27.01.2022	5
5	Initial Design Meeting 31.01.2022	7
6	Design Document Meeting 03.02.2022	8
7	Design Document QnA with Supervisor 04.02.2022	9
8	Development Phase 1: Planning Meeting 07.02.2022	10
9	Development Phase 1: High-Level Plan 07.02.2022	13
10	Dataset creation and task-issuer QnA 10.02.2022	14
11	Finalizing the Internal Dataset 11.02.2022	15
12	Pixel-comparison function development and testing 14.02.2022	16
13	Continuation of Micro-movement Detection and Task-Issuer Presentation 17.02.2022	17
14	Week Wrap-Up and Further Documentation 18.02.2022	19
15	New Dataset-data compilation and Task Splitting 21.02.2022	20
16	Presentation of current program state - and delving into depth 24.02.2022	22

17 Report Writing and Depth-Extraction 25.02.2022	24
18 Individual Work Meeting 28.02.2022	25
19 Task-issuer update 03.03.2022	26
20 Development Phase 1: Wrap-Up and Summary 07.03.2022	28
21 Development Phase 1: Summary 04.03.2022	29
22 Development Phase 2: Initialization 07.03.2022	32
23 Development Phase 2: High-Level Plan 07.03.2022	33
24 Analyzing results from optimized micro-movements-function 10.03.2022	34
25 Further Dataset Research 11.03.2022	36
26 Physical Task-Issuer Update Meeting 17.03.2022	37
27 Thesis Report and Depth-Data Work Session 18.03.2022	39
28 Internal Depth Dataset Expansion 25.03.2022	41
29 Thesis Report Writing and compiling new datasets 25.03.2022	43
30 Continuation of thesis report work and testing depth-function 28.03.2022	44
31 State of the Art function and thesis report writing 31.03.2022	45
32 Thesis Report Writing 01.04.2022	47
33 State of the Art Code Walkthrough 04.04.2022	48

34 Task-issuer and Supervisor update meeting 07.04.2022	49
35 Development Phase 2: Summary 04.04.2022	51
36 Development Phase 3: High-Level Plan 21.04.2022	54
37 Development Phase 3: Discussion meeting 21.04.2022	55
38 Further Data Collection 25.04.2022	57
39 Task-issuer update meeting: Dataset Development 28.04.2022	58
40 Stable draft meeting 02.05.2022	59
41 Results and conclusion discussion meeting 04.05.2022	60
42 Stable Draft Delivery 05.05.2022	61
43 Development Phase 3: Summary 05.05.2022	62
44 Report Results and Conclusion Discussion 09.05.2022	64
45 Discussing the Thesis Conclusion 12.05.2022	65
46 Report Discussion with Supervisor 16.05.2022	66
47 Finalizing Thesis for Quality Assurance 18.05.2022	67

PLANNING PHASE

1 Internal Introduction Meeting

17.01.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

Action Items

- Start the work on the group contract, and in addition look into what the project plan requires.
- Arrange a meeting with the task-giver and supervisor.
- Discuss what is important to ask the task giver and supervisor.
- Initiate the digital communication channel in Discord.

Highlights and Key Decisions

- An introductory meeting, where we discussed everything needing to be done in the month of january.
- Introduced the group contract, and started work on the project plan.
- We need to find out what the task actually consists of. What are we doing? We need to meet with the task giver as soon as possible to gain a better understanding of the task at hand.

Agreements

- No more meetings are necessary this week, as we can't do much more work before we've had our meeting with the supervisor and task giver. This meeting is expected to take place in the latter part of week 3.
- Individual work to be done until the next meeting consist mainly of looking over older bachelors theses to gain a picture of what is expected from the group in terms of work and project documentation.

Summary

A quick internal introduction meeting to formally start the project.

2 Introduction Meeting with Supervisor and Task issuer

21.01.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

Supervisor

Kiran Raja - kiran.raja@ntnu.no

Additional Participants

Hareesh Mandalapu - hm@mobai.bio

Erik Guoqiang Li - gl@mobai.bio

Action Items

- Gain a clearer understanding of what the project will contain, scope of the project, technologies that will be used, etc.
- Get a tentative title for the bachelor project.
- All group members should sign the collaboration agreement.

Highlights and Key Decisions

- A tentative title for the bachelor has been decided:
”**Presentation attack detection for smartphone face recognition**”
- Python will be the main language used. C++ could also be used, but both the supervisor and the task-issuer urged us to choose Python for the project. PyCharm has been decided to be the ideal IDE for the project.
- The final product will be a package that will be used in the Task-issuers application to detect attempted facial recognition (presentation) attacks of various degrees.
- All members signed the collaboration agreement.

Agreements

- Until the next meeting, it was agreed upon that each group member would individually look through examples of open source packages to use for development.
- Group members who deem themselves unfamiliar with Python should also take a look into the language, and familiarize themselves with the syntax, as well as basic features until the next meeting (24.01.22).
- all members should set up the IDE of choice - ”PyCharm”.

Summary

This meeting consisted of getting a more granular description of the task at hand. Mobai (task giver) and the project supervisor helped with this task, and we were able to construct a more detailed view of the project as a whole.

3 Meeting and work session for work on group contract and project plan

24.01.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Group members that were unfamiliar with Python have taken the "Python Basics" course on TryHackMe.com, and now feel more familiar with the language.
- Setup of the Python IDE "PyCharm" has been successfully executed for all members, and we are all able to run an example project from GitHub in the same Python version.

Action Items

- Continue, and perhaps even finish, both the Project Plan and the Group Contract.
- Construct a Gantt-chart, to gain a more detailed overview of the project as a whole within the pre-set timeline.

Highlights and Key Decisions

- Developed a detailed Gantt-chart to be included in the project plan document.
- Further development of the Group Contract and Project Plan. Some reformulation is required at this point, but we now have a nice almost-finished foundation for both of the documents.

Agreements

- Work individually on reading and rewriting parts of the two documents which are due at the end of the week (Group Contract and Project Plan).

Summary

This meeting consisted exclusively of work on both the Group Contract and the Project Plan. We came a long way from where we started at the start of the meeting. A Gantt-chart was also developed to granularly define a timeline of events for the entire project.

4 Finalizing the Project Plan and update meeting with Mobai 27.01.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

Supervisor

Kiran Raja - kiran.raja@ntnu.no

Additional Participants

Hareesh Mandalapu - hm@mobai.bio

Note: Both the Supervisor and Mobai-representative were only present between 13 and 14.

What has happened between last meeting and now?

- Advancements on both the project plan and the group contract, as a consequence of individual work. The group contract is now in a finished state, and the primary goal should be to get the project plan finished by the end of the day.

Action Items

- Finish the Project Plan
- Sign important documents - confidentiality contract and group contract
- Ask for advice from supervisor on how to improve the project plan in its current state.
- Gain more clarity on issues discussed in the meeting. Especially concerning confidentiality measures for the project. How confidential does the results have to be? Can we apply for the Eureka-prize without having to wait until the confidentiality period is over?
- Missing resources for Open-Source packages and other research-centric resources. Where are the resources promised in the last meeting? Only one single link has been published.

Highlights and Key Decisions

- Advanced the Project Plan to almost-completion - still needs some work on an individual level.
- Signed Group Contract and Confidentiality Agreement
- Gained clarity on the issue of task confidentiality. The issue was not as major as we thought after reading the collaboration contract. There is no worry about having to postpone the placement of the project on our individual CVs after the projects end.
- Mobai-representative assured they would put out more useful sources as soon as possible. At the time of writing, only one resource was made public.

Agreements

- Hamza said he would finish the last part of the project plan, regarding risk assessment, by the end of the day.

Summary

A lot of ground work for the project planning is now close to finalized. Important group project agreements have been signed and handed in.

5 Initial Design Meeting

31.01.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Hamza finished the risk assessment part of the project plan. Now the document is finished, and we can move onto the high level design phase of the project.
- Finished the planning phase, and important contracts and documents (such as the group contract and the project plan) have been delivered accordingly to deadlines. Everything is on track!

Action Items

- Discuss important features for the package, and at what levels should each feature be implemented? And with which methods can this be accomplished?
- Create a high-level map of ideas and features for future reference. The final high-level design should be ready for submission by the end of the week, if all goes according to plan.

Highlights and Key Decisions

- A high-level design diagram has been created. This diagram expresses core design elements for the different parts of the package. We intend to go into more detail for this figure on thursday.
- Questions for Mobai for the next meeting:
Does the application have input-scaling? Upscaling and downscaling, dependant on differing camera quality.
Is there a set image quality in the already-existing application?

Agreements

- Look into OpenCV until next time. How does Python interact with images?
(<https://www.youtube.com/watch?v=oXlwWbU8l2o>)

Summary

A shorter meeting, with discussion and formulation of core design elements of the package to be developed. More detail-oriented design document will come to fruition on thursday, when we gain more insight with the task issuer.

6 Design Document Meeting

03.02.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Further individual thoughts on design elements have been formed, and are to be discussed during this meeting.
- Individual homework research on OpenCV has been conducted. Ideas on how we can utilize the library to accomplish the task at hand has been formed.

Action Items

- Finish the high-level design document for approval at the meeting with the task issuer 13:00.
- Get the design approved, and get ready to start the development of the package.

Highlights and Key Decisions

- Finished the design document by 13:00, had it ready to show it off to task issuer for approval.
- Was supposed to show off the finished document in the meeting with the task issuer, but the issuer did not show up and failed to tell the group beforehand.

Agreements

- Nothing of substance can be done until we have the task issuers approval and thoughts on the design document. Since they did not show up for this meeting, and didn't warn us beforehand, the group is preparing for a setback of up to one week. If we can't get the design approved before the weekend, next week will be consisting of research, starting up the writing of the main report, and structuring the code-base to make it easier once we begin on the programming process.
- If we are unable to reschedule the task-issuer meeting, and also thereby are unable to get the design approved by the end of this week, the last meeting for this week, on Friday 04.02.22 will be cancelled.

Summary

This meeting did not go as expected. The group finished the design document for the program on time, and got it ready for task-issuer to weigh in and approve. Task issuer did not show up, some complications and delays will likely follow.

7 Design Document QnA with Supervisor

04.02.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

Supervisor

Kiran Raja - kiran.raja@ntnu.no

What has happened between last meeting and now?

- Scheduled a meeting with Kiran after last meeting, to discuss different topics regarding the design document.

Action Items

- Get feedback and approval on the design document.

Highlights and Key Decisions

- Gathered more information on how to perform matrix operations on images.
- Got general feedback, and approval, on the design document.
- Revelation:
We will only be writing functions, to later be integrated into the Task issuer's application. Image quality measurements and other pre-processing on the images will be done by the original app, and is something we don't have to worry about.

Agreements

- Look at the example of face recognition in python that the supervisor sent.
- New meeting with Supervisor has been arranged, with useful examples and background knowledge, on Monday 07.02.2022.

Summary

The high-level design has been approved, and we are back on track! Development Phase 1: "Minimum Viable Product/Prototype for level 1 attacks" will start up on monday.

8 Development Phase 1: Planning Meeting

07.02.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

Supervisor

Kiran Raja - kiran.raja@ntnu.no

What has happened between last meeting and now?

- Group members have individually looked at the examples sent by the Supervisor and gained an understanding of how OpenCV could work with facial recognition.
- Milosz has created a simple example project in python, that opens the camera on the device it's running on and shows matrix RGB-values for a single pixel in the terminal. For exploratory purposes. What is possible?
- Set up a GitHub-repository to be used for development and testing.

Action Items

- Set a concrete plan for the next 3 weeks: Development Phase 1.
- Create a flowchart of the general goal of development phase 1. What does this phase require, in terms of functionality. What functionality must be developed for the first phase of development to be considered successful? And how do we accomplish this? Set concrete deadlines for specific functions and delegate responsibilities.
- Make sure everybody is able to run demo-code
- Meet with Supervisor at 15:00:
Look further at examples of computer vision in python and gain a deeper understanding of how concepts from the task can possibly be implemented.

Highlights and Key Decisions

- Did research on how to separate foreground and background through various methods, and how one can measure micromovements this way.
- Created prototype using OpenCV and live camera feed in python. "Playing around" and getting to know both OpenCV and other Computer-vision-centered packages like "torchvision" and "deepv3" in python.
- Meeting with Supervisor:
 - We are putting systems together to detect an attack in an image or a video, before it comes to the Mobai application
 - Histograms, LBP, and other image processing concepts can be effectively used for face recognition, and also presentation attack detection.

Agreements

- Take 10 images of yourself, and use these to create attack scenarios for a dataset. For now, focus on level 1 attacks. Does not have to be fancy, just a simple little dataset from each group member. Milosz proposed to work on an automated solution for dataset creation for next meeting.

Summary

A exploratory meeting where we explored ideas and concepts from computer vision that can be further used and integrated into the code. Planned for development phase 1, which starts in the subsequent week.

DEVELOPMENT PHASE 1

9 Development Phase 1: High-Level Plan

07.02.2022

Phase Goals

- Lay out fundamental package framework
- Develop helper functions for testing & debugging
- Implementation of level 1 presentation attack detection methods
- Robust & accurate detection
- Unit tests & logs

Week 6: 07.02-13.02

Goals

- Familiarize ourselves with how OpenCV handles image objects and live camera feeds.
- Construct initial helper functions, such as frame sampling.
- Begin working out ways level 1 presentation attack detection methods could be implemented.
- Progress on detecting micro movements & background object detection

Week 7: 14.02-20.02

Goals

- Continue working on the level 1 presentation attack detection implementations.
- Set up testing environment and start testing
- Analyze results and use result-data to assess the current state of the function.

Week 8: 21.02-27.02

Goals

- Movement consistency & eye gaze
- Improve the level 1 presentation attack detection implementation's.
- Further testing: Edge cases & Robustness.
- Finalize the Level 1 Attack prototype. Present this prototype for the task issuer.

10 Dataset creation and task-issuer QnA

10.02.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

Supervisor

Kiran Raja - kiran.raja@ntnu.no

Additional Participants

Hareesh Mandalapu - hm@mobai.bio

What has happened between last meeting and now?

- Nothing major has happened since last time. Some group members have other courses to attend to, and has focused on this for the week.
- Milosz developed an automated dataset-creation tool in python that utilizes the webcam of the computer.

Action Items

- Make sure all members are able to run the code that allows for dataset-creation
- Ask task-issuer some questions regarding external datasets, access to their application, and if our dataset-function is as expected. Do we need to change anything?

Highlights and Key Decisions

- We are still on-track for this week. Some helper functions and logging has now been implemented.
- All members now have a functioning version of the dataset-creation function.
- Gained further knowledge on the task-issuer application, and when we can expect to gain access to it (in 1-3 weeks). Task-issuer also expressed that they would provide multiple external datasets in addition to the self-created one.
- Task-issuer also said that the dataset-function is satisfactory. A good tool to use for easy dataset creation.
- The internally created dataset should be done this week.

Agreements

- The meeting was disbanded a little earlier than expected. The group agreed to create individual datasets in the rest of the scheduled hours. The dataset is going to be utilized and explored further in the next meeting (08.02.22)

Summary

Dataset-creation is at the center of attention at this point. We need a substantial dataset to be able to test for various presentation attacks to figure how to detect them.

11 Finalizing the Internal Dataset

11.02.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- All group members, except one, has created a dataset. The last group member needs support from one of the other group members, as torchvision in python can only run single-threaded in macOS. This results in the images taking forever to process. The group member has created videos on their smartphone, to be processed in the program.

Action Items

- Kristian needs help with dataset-creation, as the torchvision-library for python is not optimized for macOS (program only running on one thread, needs computational help).

Highlights and Key Decisions

- Dataset is finished as per today. Both raw and binary frames have been created from either a live feed or a video input.
- As per the development plan, we are still on track.

Agreements

- Milosz wants to try experimenting with the dataset over the weekend. He expressed that some experimental code would be developed by the weekend. This code will be further explained upon and explored in the monday-meeting (14th of February).

Summary

A dataset-finalizing meeting, where we wrapped up the work-week and discussed what to do, and how to get ready, for the next week.

12 Pixel-comparison function development and testing

14.02.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Milosz implemented a function that compares movement between background and main subject between subsequent frames (checking for micro-movements) by comparing RGB-values of subsequent pixels.

Action Items

- Experiment and see how the different datasets interact with the pixel comparison function. Does the subjects behavior change the results? Does there seem to be an accurate estimation of similarity between frames of each behavioral dataset? And how do the datasets of the different persons compare to each other?
- How do we implement a function that can be used to identify these kinds of attacks?
- Does the pixel-comparison function yield any feasible results with the current dataset?

Highlights and Key Decisions

- Experimented with different parts of the dataset, and tested it against the comparison function. Found some surprising results, that it actually distinguishes attacks from real-life situations pretty well already, in this first iteration.
- Parts of the dataset that has been developed using a webcam seems to produce varying results. This needs to be discussed and explored more later this week.

Agreements

- Agreement to expand the dataset with more frames from the smartphone-camera. This task is mobile-centric, so it would make the most sense. Therefore, the group members which had their dataset-contribution made through webcam-footage has been tasked to make an additional part of the dataset using their smartphone.
- The existing images in the dataset from webcam-footage will be kept and tested further upon at a later point.

Summary

A testing-meeting for the pixel-comparison function, where we discovered both positives and negatives of this type of function, as well as the image test-set.

13 Continuation of Micro-movement Detection and Task-Issuer Presentation

17.02.2022

Participants

Group Members

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

Additional Participants

Hareesh Mandalapu - hm@mobai.bio

What has happened between last meeting and now?

- Further testing, and further dataset-exploring.
- Since Hamza didn't show up today, we were unable to get access to the new dataset-data that was supposed to be created for today.

Action Items

- Begin the documentation process for the package
- Look at new datasets from mobile
- Look at new data produced from the pixel-comparison-function using new dataset-data
- Show off the pixel-comparison function and its results (gathered in the monday-meeting) to the task-issuer

Highlights and Key Decisions

- No new additions to the dataset from the mobile platform, because of Hamza being sick.
- Started creating documentation in GitHub, including ReadMe and KanBan/Issue-tables.
- Task-issuer seems impressed with the results we got from processing our dataset with the pixel-comparison function.
- Task-issuer also uploaded a massive dataset for us to further test the code on.

Agreements

- The group agreed to give Hamza his first group-contract breach-strike. Not necessarily because he didn't show up for this meeting, but more about smaller things (such as coming up to 1 hour late on multiple occasions). We have been too lenient on this topic, but now is the time where we should enforce the group-contract-breaches to remind all members to work when they are supposed to. In the future meetings, we will enforce the group rules more strongly.
- There is agreement on how the tasks should be split. This information will be added to the KanBan/Issues-table on GitHub.
- The group agreed that it may be smarter to start one hour later, as that is normally when some members would show up. So from this day, all meetings now commence at 11:00. There will be a trial period of approximately one week, where we test if this change can work better with our workflow.

-
- With the new dataset (from task-issuer) being as large as it is (3,2GB), we agreed that we should segment the dataset into smaller batches, and test on them gradually. We should ask if we are allowed to process some of the data on a more graphically powerful computer at NTNU.

Summary

A meeting mainly covering organizational aspects of the project (mainly documentation), and getting feedback on everything we have done so far. Also gained a new important resource, an expansive dataset from the task-issuer

14 Week Wrap-Up and Further Documentation

18.02.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Analysis and testing on the new dataset which became available during the last meeting.

Action Items

- Wrap up the week. What remains for this weeks planned goals? What has been accomplished?
- Further documentation work in GitHub ReadMe and Issues-table (KanBan)
- Lay out the plan for next week

Highlights and Key Decisions

- Updated ReadMe to describe the functions more granularly.
- Updated Issues in GitHub to reflect on current work-tasks and who is assigned to what.
- Optimized Program - Resize of input images, and sequential execution of files in designated folders
- Tested the new dataset with the new code and compiled results in Excel file

Agreements

- Process data from the external dataset, so we can look at results in the coming week, and see how "well" the micromovement-detection works on a more expansive dataset.
- Hamza was tasked to look into eye-tracking in Python, and will attempt to implement a function that utilizes either PyGaze or MediaPipe for an eye-tracking solution.

Summary

A meeting where the week was concluded. Set plans for the following week, we seem to be on-track when compared to the initial plan.

15 New Dataset-data compilation and Task Splitting

21.02.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Milosz tested the external datasets with the `cv2.resize()` function, to see how our micro-movement function would work with images which are downscaled (from 720-1080p to 360p, 144p and 72p). This resulted in generally impressive results, as the images of lower resolution still yielded good results in terms of micro-movement tracking. As a result of this optimization-tactic, it made the program run substantially more efficient, lowering the processing time per frame from 10-20 seconds to 0.5-1 second.

Action Items

- Compile the data gathered from the new, externally-sourced dataset, to try to approximate voodoo-constants to accurately identify level 1 attacks.
- Split the further tasks for this week between group members:
 - Milosz is continuing on his mission to find the sweet-spot for quality-vs-performance for the micro-movement function.
 - Hamza is still tasked to both look into and try implementing eye-tracking.
 - Kristian is tasked to look further into depth detection, and see if it can be plausible to implement a such method within the scope of the task. Also, is this possible to do without TrueDepth or Time Of Flight?
- Update Issues in GitHub to reflect on the issued task for each member.

Highlights and Key Decisions

- Milosz tried to improve the results accuracy, but ultimately made no further improvements. Still working on finding the optimal spot for quality-vs-performance. Looks to be downscaling the image to 144p, and the background-masking even further to 72p. There are small tradeoffs in the results, but these are marginal compared to results from higher resolution images.
- Hamza looked into both face-tracking and eye-tracking, and is doing research to implement a solution for eye-tracking (via face-tracking) this week.
- Kristian did research on depth-data, and found that implementing an algorithm for depth-sensing on normal cameras would be far too compute-heavy for the scope of this task. This is due to the lightweight nature of the application these functions will be used for. Need to discuss with the task-issuer on Thursday, if we can get images with captured depth data (either TrueDepth or ToF) for a new dataset to test on. Then, if images can be provided, we can look further into how the depth-data is formatted.

Agreements

- It was agreed upon that each group member would work individually on their assigned task until Thursday.
- Kristian took the responsibility of lining up a full bachelors thesis report in Overleaf (creating a skeleton if you will), and will do this before the thursday meeting.

Summary

A meeting filled with task delegation, individual work, and some discussion of test results.

16 Presentation of current program state - and delving into depth

24.02.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

Supervisor

Kiran Raja - kiran.raja@ntnu.no

Additional Participants

Hareesh Mandalapu - hm@mobai.bio

Erik Guoqiang Li - gl@mobai.bio

What has happened between last meeting and now?

- Milosz developed a live-feed version of the program. It is a bit unstable as it currently stands, but could be a good tool to test both performance and accuracy of the program down the line, with a constant stream of frames.
- Hamza developed a lightweight solution to eye-tracking using concepts from OpenCV. This can be further used to determine the eye-gaze of the subject.
- Kristian developed a skeleton/outline of the main bachelors thesis report. Also did research on depth-sensing and how it can be used (with ToF or TrueDepth data).

Action Items

- Show off the current progress to the task-issuer.
- Ask questions about what to do next:
 - Suggestions for solutions in terms of eye-gaze. Any ideas on how to track eye-gaze in an efficient and accurate way?
 - Depth Data:
 - * How can we extract depth-data from sensors on phones with TrueDepth/Time of Flight?
 - * Can we get a dataset with depth-data from Mobai?
 - * What would you suggest we work on in terms of depth-sensing?

Highlights and Key Decisions

- Task-issuer seems, again, impressed with the new results. The micro-movement function works pretty well already, and real fast. The results again showed a clear separation between real subjects and attack attempts.
- Going into depth-data is going to be difficult. It is a multi-step process, where we need to start with extracting depth data. This is due to the task-issuer not having a way of doing this yet, and therefore lack any dataset containing depth.
- The next step is then to use this dataset to develop an attack detection method that uses depth data when available from the device the program is running on.
- Decided to go with a dataset from iOS, as no Android phones with Time of Flight were available at the moment.

Agreements

- Continue on the individual paths each group member was assigned to earlier in the week.
- Do individual research on depth-information.
- Gain access to the Apple Development platform from the task-issuer, so we can be able to deploy apps to iOS.

Summary

A forward-centric meeting with task-issuer, where we discussed where we could go next, both in terms of new features and improving existing ones.

17 Report Writing and Depth-Extraction

25.02.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Kristian was added to the Apple Developer platform, and explored how it works. Resolved some issues with the deployment of applications to iOS-devices. (by having dialog with task-issuer (administrators of the internal Apple Developer platform)).

Action Items

- Find how to extract depth data from TrueDepth Camera.
- What format is the depth-data? Is it readable? and how can it become readable?
- Continue on eye-tracking, how far has Hamza made it?
- Start writing theory and practice parts of the main report.

Highlights and Key Decisions

- Managed to extract data from TrueDepth-camera (comes in a complex file format. We have to find out how to use/visualize it soon)
- Started working towards how to make the depth-data processable and readable
- Hamza is still working on eye-tracking. Seems to be a difficult task. We should try to implement it using MediaPipe.
- Started the ground work on the main report (mainly theory-based parts).

Agreements

- Continue on our individual tasks
- Look further into the report, and what can be written at the current moment.

Summary

A meeting with great progress. We figured out how to extract raw depth data from an iPhone TrueDepth sensor. We will use this further, to collect depth-data and use this data for depth-development.

18 Individual Work Meeting

28.02.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Kristian developed a function in python that transforms the depth-data to make it readable. (by decompressing it and transforming it)
- Milosz started writing the main-report
- Hamza finished the eye-gaze prototype-function, and it is being tested on the live-feed-version of the testing framework

Action Items

- Gather more depth-data to use for more testing for the depth-prototype.
- Work further on individual tasks.
- Look into and discuss how the report work should be split between members. Also, agree on what can be written at this moment in time?

Highlights and Key Decisions

- Generated more depth-data. It is convoluted to extract, so it will take a long time to generate a massive dataset. Should show the code to the task-issuers in the next meeting and hear if they could assist in creating more data.
- This session can be described a work-session, where each group member worked individually on assigned task. These tasks have been previously discussed in the meeting summaries.

Agreements

- All members have agreed to participate in the report-writing class that is happening on Wednesday 02.03.22.
- A recurring theme of the last week, but keep on working on the individual tasks. All are progressing nicely.

Summary

An individual work session, with small interference's where discussion or help was needed.

19 Task-issuer update

03.03.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

Additional Participants

Hareesh Mandalapu - hm@mobai.bio

What has happened between last meeting and now?

- Individual work has gone well, and the iOS function has been updated to look better (updated GUI and UX-elements).
- Participated in the report-writing tutoring on Wednesday 02.03 as a group. Gained better insight into how to write the thesis-report
- Slightly updated the skeleton of the main thesis report

Action Items

- Show off the code for depth-data collection. And also show that we have been able to generate images out of the depth-data (even when the data is in a complex format).
- Questions for task-issuer:
 - We have a method for data extraction (depth). We need data. help.
 - Clarification of requirements for the thesis. Would like to get this in written form. Specify what you would like us to write in the thesis. If there are certain things that are not obvious to include, and those that seem to be so would ideally be specified.
- Continue with individual tasks.

Highlights and Key Decisions

- Task-issuer cannot provide a depth-dataset, so we will have to utilize the small dataset we created ourselves.
- Task-issuer explained that the hard criteria for the thesis itself must be formed together with other employees of their company. This will be provided soon.
- iOS code for depth-data gathering, that has been internally developed by the task-issuer, is going to be shared with us soon. The tool we have now, which is just a simple redesign of an already-existing application (that is not really optimized, and not of good quality).

Agreements

- The next meeting (tomorrow - Friday 04.03) is due to be shortened, due to some of the group members having to focus on other courses.
- This next meeting will focus on wrapping up Development Phase 1. What went well? What could have gone better? What went better than expected?

Summary

Another good work-session-meeting. Updates on the project as a whole, and how our product is coming along.

20 Development Phase 1: Wrap-Up and Summary

07.03.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Nothing overly noteworthy. Some small updates and tweaks on the depth-function. Some minor updates to the thesis-document

Action Items

- Wrap up and summarize Development Phase 1 in a wrap-up-document based on the plan we made.

Highlights and Key Decisions

- Summarized Development Phase 1. This summary is included on the next page of this "meeting-summaries" document.

Agreements

- Arranged meeting with Supervisor, scheduled for monday 07.03.22.
- Plan to plan Development Phase 2 in the following meeting.

Summary

A short meeting, where Development Phase 1 was finalized and summarized.

21 Development Phase 1: Summary

04.03.2022

Phase Goals

- The framework for the package itself has now been built and formed after common coding practices.
- Helper functions are under constant development, and we already have a lot of functions that we frequently use, to capture and process images, in the "helpers"-class of the function.
- We have developed a method that detects level 1 presentation attack detection using micro-movement. This function has been thoroughly tested, and has returns satisfactory results. There are some edge cases where the function fails to identify a real person (wearing headphones for example). These kinds of edge cases will be looked further into in development phase 2.
- The program at this stage is quite accurate, and robust. The only problem at this stage, is that it's fairly slow (0.5-1s per frame processed). For Phase 2, the function will be updated to support the MediaPipe library to increase performance.
- The package has been under continuous testing parallel to development. This was mostly conducted by manually utilizing functions for automation. We have tested a variety of datasets. We chose not to include automated testing yet due to the package being in such an early state. We plan on implementing automated testing towards the end of phase 2. At that stage, we expect the project to have more functionality for numerous detection methods in addition to being more standardized and stable.

Week 6: 07.02-13.02

Goals

- OpenCV and its libraries are used frequently in the current version of the package. The group is now familiar with the library, as well as Python as a programming language.
- Initial helper functions, including frame sampling, was developed during this week
- We did a lot of research on how to implement various detection methods this week. Found some open source packages that could be helpful.
- Created a simple, but inefficient, foreground and background separating function. This works by using a pre-trained deep-learning network to figure out where the human exists within a frame. This function will be optimized in the following weeks.

Week 7: 14.02-20.02

Goals

- Created a function for automatically creating a internal dataset for testing functions.
- Developed a function that uses the binary masks created by the foreground-background deep-learning tool to estimate pixel similarity. In practice this function is able to detect level 1 attacks pretty accurately, due to the pixel similarity on paper/screen being much more uniform than a real human would be. The function is fairly inefficient, but very effective. Optimizing this further will be one of the primary goals.
- The automated testing that was planned for development, cannot be developed quite yet. This is due to the program not being in a real stable state at the current moment. A lot of manual testing has been conducted, using test-data we spent time generating ourselves.

Week 8: 21.02-27.02

Goals

- Eye-gaze-detection development started. Research on the topic and an early-stage function for eye-gaze detection was developed this week.
- Decided to jump into depth-detection. This consisted of many steps. The first one being collection of depth data (from an iOS TrueDepth-camera). This was accomplished pretty quickly, even without any experience in Swift (the primary language for iOS development). We managed to accomplish this by using an open source package for depth-data extraction, and modified it to fit our needs. Also found a way to make the depth-data humanly-readable. This will be further explored in the next development phase.
- Detection of movement consistency, in relation to background objects, has not been tackled. This is due to the group's choice to rather move straight to depth-detection instead. Movement Consistency has been discussed, but the group decided to prioritize other functions. Movement Consistency has been cancelled.
- We presented the functionality in a meeting the following week (9). Since meetings have found place with the supervisor and task-issuer every week, we have received feedback continuously. This has also given the task-issuer an insight to our development. The task-issuer has expressed that the results so far have been impressive, and that we are on the right track.

DEVELOPMENT PHASE 2

22 Development Phase 2: Initialization

07.03.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

Supervisor

Kiran Raja - kiran.raja@ntnu.no

What has happened between last meeting and now?

- Milosz cleaned up code structure, and optimized the functions utilizing MediaPipe-libraries.
- Meeting with Supervisor has been arranged, and is happening today (11:00).

Action Items

- Show progress to Supervisor (since he hasn't been able to attend the task-issuer-meetings in the last few weeks)
- Hear what Supervisor has to say about further progress. And what to aim for in Development Phase 2.
- Lay out a high-level plan for Development Phase 2.

Highlights and Key Decisions

- Gained a lot of insight into how to plot graphs to reduce error in attack detection. Supervisor showed a lot of ways to plot graphs to determine determinants for attack detection.
- Planned out Development Phase 2 - which starts today.
- Developed code that processes data from functions to plot into graphs to determine attack-determinants.
- The Development Plan is included on the next page of this "meeting summaries" document.

Agreements

- Milosz is going to prepare the repository for Hamza to process data.
- Hamza expressed he would attempt to process the graphs using the new code before the next meeting.

Summary

A planning-meeting for Development Phase 2.

23 Development Phase 2: High-Level Plan

07.03.2022

Phase Goals

- Start the work on extensively writing select parts of the thesis report to a stable state.
- Have actual numbers to show how effective the current package is.
- Be able to determine when an attack actually happens (finding the dividing-factor for bonafide- and attack-scores).
- Fully develop eye-gaze and depth-detection attack-detection methods.
- Further dataset-expansion.

Week 10: 07.03-13.03

Goals

- Learn and understand a new tool for determinant-determination - SKLearn
- Process the data we have available and use the new frameworks to work out determination-variables for attack detection using micromovements.
- Continue individual work on both eye-gaze and depth-sensing functions. Finalizing these functions.
- Continuous development of the thesis document.

Week 11: 14.03-20.03

Goals

- Have eye-gaze and depth-sensing functions in a functional state.
- Develop new additions to the dataset, to make it even more expansive.
- Test the new functions (using eye-gaze and depth-detection), and run determination-algorithm to calculate EER and quality of detection.
- Analyze the tested functions.
- Continuous development of the thesis document.

Week 12: 21.03-27.03

Goals

- Finalize the two new functions (eye-gaze + depth).
- Tie all of the developed functions together, so that they interact with each other to create a final attack-detection result.
- Further Testing.
- Continuous development of the thesis document.

24 Analyzing results from optimized micro-movements-function

10.03.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

Additional Participants

Hareesh Mandalapu - hm@mobai.bio

What has happened between last meeting and now?

- Hamza processed the test data with the new, optimized version of the micromovements-function.
- Other group members have had their hands full with other courses this week, a project in another course is wrapping up (and is therefore focused on this exact week).

Action Items

- Meeting with task-issuer. Nothing of significance needs to be tackled in this meeting. We aim to update the task-issuer further, with how we plan to tackle the next few weeks (Phase 2). Also, we will discuss what they think so far. Are we still progressing in a way they would like us to? Is there anything we need to do different, or progress in another direction?
- Analyze results of optimized micromovements-function. Discuss if the eventual tradeoff in accuracy that is done in favor of performance is worth it. Do the results show to similar/better attack detection. Or is quality of detection worse as a direct consequence of performance gain. Important questions, as this method utilizes something entirely new.
- Continue work on the thesis-report.

Highlights and Key Decisions

- Meeting with task issuer:
 - Task-issuer wants to receive the iOS-code to develop a depth-dataset for us. Kristian sent this code right away.
 - Task-issuer also, again, expressed that they think we are doing really good. Also expressed that it is a good idea to go back to the deep-learning algorithm due to result being much more satisfactory compared to the new "optimized" version.
 - Discussed some plans going forward, and in addition some thoughts on the last development phase (3) (thought to be skin-texture and light-refraction).
- After going over the results from the optimized micromovements-function, we have collectively decided that the deep-learning model we used previously, with worse performance, is the one we are going to utilize in the final program. This is due to the much more accurate results it produces (in terms of attack detection), compared to the new, more performant MediaPipe-powered. function.
- Updated new subsections of the thesis report.

Agreements

- This week is progressing a little slower than expected, due to other courses and responsibilities for all members. This is partly reflected in the individual work that has been done this week. The main goal for this week is to continue to update the main report.
- Attempt to arrange a urgent meeting with supervisor to try and mend collaboration-issues we currently have with him and the task-issuer.

Summary

A meeting with some updates and discussion on the new micro-movement function. Further updates on the thesis report.

25 Further Dataset Research

11.03.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Conducted a urgent meeting with the supervisor, where we thoroughly discussed worries and issues we had about collaboration with both him and the task-issuers. He expressed that he would talk to the task-issuer and express our issues also to them.

Action Items

- Look into more datasets, as we need heaps more data to thoroughly test the various functions.
- Further discussions on collaboration- and motivation-issues related to the supervisor and task-issuer.

Highlights and Key Decisions

- Spent a lot of time to find and apply for access for relevant datasets (closed access). Also found some useful open-access/source datasets that we could utilize.
- We need to ask the task-issuer yet again to gain access to some more specialized data (can be public, but hopefully they have access to closed-access datasets)
- Assisted task-issuer with iOS-application for in-house depth-data capture.
- Noted some more key points to the collaboration-issue. Talked to representatives from the task-issuer, and our supervisor, as well as a third party, to attempt resolution of issues in relation to project collaboration and motivation.

Agreements

- The next meeting, Monday 14.03, is cancelled due to other course responsibilities (INGG2300 - Systems Engineering - Project). The next meeting will commence on Thursday 17.03.
- There are talks to finally arrange a physical meeting with the task-issuer.

Summary

More dataset-research, depth-data collection and further talks on collaboration-based issues.

26 Physical Task-Issuer Update Meeting

17.03.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

Supervisor

Kiran Raja - kiran.raja@ntnu.no

Additional Participants

Erik Guoqiang Li - gl@mobaio.bio

Hareesh Mandalapu - hm@mobaio.bio

What has happened between last meeting and now?

- The task-issuer meeting for this week has been scheduled to happen physically in the task-issuers locale at 1pm.
- Hamza has done extensive research on PAD - and noted a plethora of interesting finds from professional research articles. This is due to be used in the "State of the Art" section of our thesis report.

Action Items

- Participate in the meeting with task-issuer.
- The meeting schedule has been shared with us, and looks like this:
 - Demo from Task-issuer - To know what they are actually doing, and to illustrate the whole picture of Presentation Attack Detection in a
 - Short further introduction of FRS and PAD.
 - Thesis Work Status.
 - Planning for future work.
- Take notes from this meeting-session.
- Further research and report-writing.

Highlights and Key Decisions

- Task-issuer introduced important concepts and information on the products they aim to deliver, including the product where our package would be implemented.
- Finally got confirmation that a huge amount of data (for testing) is coming by the end of the day. This is something we have waited for for a long time.
- Future task-issuer-meetings will happen physically.
- State of the Art - part of the thesis report is being extensively researched and written, and is scheduled to be in a stable-draft format by the end of the week.
- Gained a more granular view of what the task-issuer actually wants us to do. This is: "Finish the planned level 1 and 2 detection methods". In our case, this is the Eye-gaze function and the Depth-data function. It is advised that we do not move on to more advanced methods (skin texture and light-refraction).

Agreements

- Due to Milosz having problems with his laptop, and had to return it, the meetings in the near future will happen remotely (so everybody has an opportunity to work (desktop)).
- Hamza is working on writing the state of the art part of the report, doing research and writing extensively on the topic.
- Milosz is working on depth-data, and how a presentation-attack can be detected using this data (when available).
- Kristian is working on further production of depth-data for a in-house dataset, as well as researching the state of the art of presentation attack detection.

Summary

A productive meeting with the task-issuer. A sense of purpose for this project has been formed, and the group now feels more motivated to keep going with the task at hand.

27 Thesis Report and Depth-Data Work Session

18.03.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Task-issuer sent heaps of datasets since yesterday. Spend some time today to download some of these - and look through the relevant datasets. Eventually, we could run parts of the datasets on the micromovements-function to check true EER of the function.
- Further research on state of the art has been conducted by multiple members.
- Further advancements have been made in relation to the depth-detection function for presentation attack detection.

Action Items

- A pure work-session for individual work.
- Milosz will focus on the depth-data function.
- Kristian and Hamza will continue on the state of the art-section of the thesis report. In addition, will look into and process parts of the new datasets.
- Look into the new datasets.

Highlights and Key Decisions

- Did reformatting of file-names for dataset.
- Researched HDF5-file compatibility for the OpenCV library
- Advances on depth-detection and presentation attack detection for depth-data. The function itself seems to be working, but due to a lack of data, it is not possible to fully test it. Focus for next weeks should be expansion of the internal depth-data dataset.
- Updated state of the art section of the report to include new methods that are currently used in the space of Presentation Attack Detection.

Agreements

- The group agreed to work remotely for the foreseeable future (except the task-issuer meetings). This is due to the PC-situation of one of the group members (Laptop in for repair, but has a stationary PC at home), to make sure every group member can work during the scheduled meetings.
- Due to an exam happening on wednesday next week, in Systems Engineering, the monday meeting has been cancelled yet again. This is the last time this will happen, as the final exam for this course is happening this week. After this, all meetings and work-sessions will be held as scheduled.

Summary

Dataset analysis and further state-of-the-art theory was conducted in this meeting. Some advances in the depth-sensing algorithm has been made, now we need more extensive data. Data with depth will be expanded over the next week.

28 Internal Depth Dataset Expansion

25.03.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

Supervisor

Kiran Raja - kiran.raja@ntnu.no

Additional Participants

Hareesh Mandalapu - hm@mobai.bio

What has happened between last meeting and now?

- Work on Systems Engineering for 2/3 of the group. The exam was held yesterday, and the course is now fully finished. Now the focus falls onto the bachelor thesis.
- Further research on state of the art articles. Now the writing of the section of the report begins.

Action Items

- Short task-issuer meeting. Topics for discussion:
 - Communicate what has been done over the last week.
 - What are we planning to do over the next week?
 - * Expand the internal depth-data dataset with bonafide, 2D-mask-attacks, paper-attacks, and display-attacks.
 - * Test micro-movements against the bigger datasets we now have access to.
 - * Further develop the report, as well as some new functions for the package (focus on depth)
 - What do we need from the task-issuer?
 - * Bonafide Depth Data (from iOS Application)

Highlights and Key Decisions

- Highlights from task-issuer meeting:
 - Got more insight into the thesis report structure.
 - Updated the task-issuer on progress, and reason for slower progression this week.
- Spent a lot of time expanding the internal depth-data dataset. Got about 1.5GB of additional data, with TrueDepth-data.
- New bonafide data was created the likeness of the group and two willing participants that signed the consent-release-form provided by task-issuer.

Agreements

- Agreement to work remotely for the following meeting.
- Kristian will compile and ready the new dataset before the next meeting.
- Depth-data has been collected, and we now are able to run the new depth-function and test its performance against this dataset.

Summary

Dataset creation meeting. Created a vastly more expansive internal dataset, with TrueDepth-data from iPhone.

29 Thesis Report Writing and compiling new datasets

25.03.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Kristian compiled and readied the new internal dataset, with iPhone TrueDepth, for testing.
- Research on thesis report - more state of the art theory.

Action Items

- Discuss who writes what in the report over the following week.
- Testing the new internal dataset against the micro-movements function, and experimenting with the depth-detection function on the same dataset.
- Start work on writing individual thesis report parts.

Highlights and Key Decisions

- Compiled OULU-dataset-files and readied for testing.
- Wrote organizational structure part of thesis report
- Wrote parts of the state of the art part of the thesis report

Agreements

- The weekend will be spent on rejuvenating some energy. Encouraged group members to write more on the thesis report over the weekend.
- Will pick up where we left on monday 28.03.

Summary

A research-centric meeting. Some compilation and renaming of datasets in our possession. This week has been highly data-centric, and most time in plenary has been spent expanding our data, specifically within depth. This data is needed to further develop the package.

30 Continuation of thesis report work and testing depth-function

28.03.2022

Participants

Group Members

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Milosz updated the code repository to include more python documentation, and some restructuring has also been conducted to improve operability of the code.

Action Items

- Discuss more around the thesis report, progress going forward, and what needs to be done by the end of the week.
- Explore and experiment with function that utilizes TrueDepth-data.
- Further expand the thesis report, on an individual basis.

Highlights and Key Decisions

- More updates on code structure, and overall architecture.
- More updates on the project report - specifically in the organizational- and program design-sections

Agreements

- Hamza failed to show up, without any fore-warnings to the other members. This will count as a breach of the group contract, and will count towards a penalty, as stated in the group contract.

Summary

A shorter work-centric meeting, with individual work being conducted.

31 State of the Art function and thesis report writing

31.03.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

Supervisor

Kiran Raja - kiran.raja@ntnu.no

Additional Participants

Hareesh Mandalapu - hm@mobai.bio

What has happened between last meeting and now?

- Hamza had a project in another course. Has therefore done minimal work this week.
- Kristian wrote a fair amount in the thesis-report - in the organizational part.
- Milosz ran our code through the Oulu-dataset, Protocol 2.

Action Items

- Meeting with task-issuer moved from 13:00 to 10:00 due to supervisors schedule.
- Look into the function results from the Oulu-dataset (EER, Histogram).
- Continue with thesis report work.

Highlights and Key Decisions

- Important information gathered from the task-issuer meeting:
 - Presented some results for the past week. Updated the supervisor on report-work, dataset-creation and
 - A SotA (State of the Art) algorithm for PAD (Presentation Attack Detection) will be shared, and we will need to run the datasets we have through this method and compare results with our own functions.
 - Representative from the task-issuer presented the SotA-algorithm, with DenseNet-network, and went through the basics of that code. Now our mission is to run it through one of the partitions of the Oulu-dataset and get tangible results to compare to our own function.
- Discussed some of the results from the Oulu-dataset. Our function is not looking promising in extreme conditions (low lighting, obfuscated face). This, however, seemed to be expected according to our supervisor.
- Updated the thesis report structure.
- Expanded Introduction and Development Process in thesis report.
- Appended new data to the depth-dataset.

Agreements

- For tomorrow's (01.04) meeting, there is almost exclusively continuation of work on the thesis report.
- Milosz is running the SotA-function over the Oulu-dataset to compare function results for our function vs SotA. Go over these results in the next meeting.

Summary

A report-writing meeting, with some updates from both supervisor and task-issuer regarding state of the art algorithms for presentation attack detection, and comparison of our results vs the SotA-results on the same dataset.

32 Thesis Report Writing

01.04.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Milosz ran the experimental depth-data-function through our internal dataset. Histogram and Histogrammic Equalization shows a clear attack pattern for most attacks, with the exception of curved paper, which is dangerously close (in terms of depth-data analysis) to bonafide authentication attempts.

Action Items

- Continue work on the thesis report - this is our top priority at the moment. A lot of work has to be put into the report to be able to progress as anticipated. A stable report draft has to be compiled and sent by May 5th.

Highlights and Key Decisions

- More progress has been made on the thesis report.
- Transferred and downloaded a sorted version of the 35GB Oulu Protocol 2 Dataset.

Agreements

- Further individual work on individual report parts over the weekend. Progress report on Monday 04.04.
- Hamza will process the sorted Oulu dataset over the weekend to analyze if different GPUs yield different results.

Summary

Another thesis report-centric work meeting.

33 State of the Art Code Walkthrough

04.04.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

Supervisor

Kiran Raja - kiran.raja@ntnu.no

What has happened between last meeting and now?

- A slower progression than anticipated over the weekend for the report. This is partly due to some sickness, plus responsibilities in other areas.
- Milosz developed a script, and converted the .avi-files from the Oulu-dataset to singular image frames in .jpg-format. This resulted in about 69GB of data in just images (250 000 images). This is due to the State of the Art function taking sequential images as input, rather than video-inputs.

Action Items

- Go through the PW-MAD-code (State of the Art for PAD) with supervisor - to understand the structure of the neural network built within the code, and how to run our data through the code.
- Upload new dataset-files (Oulu - .avi converted to images - 69GB) for internal access for group members.
- Make further advancements on the thesis report document.

Highlights and Key Decisions

- Gained a greater understanding of the PW-MAD-code (State of the Art), and how to run this State of the Art neural-network-based algorithm with our own datasets.
- Resolved issue with altered PW-MAD code repository - and the Python virtual environment-interpretter - to make every group member able to run the code.
- Made further advancements on the report document.

Agreements

- Individual work on individual parts of the thesis document until next meeting (thursday).

Summary

A State of the Art benchmarking meeting, readying the repository for image processing and recording of attack detection. In addition, some work on the thesis report was conducted.

34 Task-issuer and Supervisor update meeting 07.04.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

Supervisor

Kiran Raja - kiran.raja@ntnu.no

Additional Participants

Hareesh Mandalapu - hm@mobai.bio

What has happened between last meeting and now?

- Hamza read more articles on State of the art, and clarified future work that is necessary.
- Kristian wrote a large chunk of the development process-part of the thesis report. This part of the report is about 70% finished.

Action Items

- Need to inquire with task-issuer and supervisor about which of the two figures to use in the part about facial recognition.
- Ask supervisor about how we would write the State of the art chapter. How should this part be structured? had an idea to create a 'timeline' of development showing the progress in PAD Techniques year to year or within each technique, highlight the advances made every year. Either this or just highlight what the most relevant advances made that are relevant to our bachelor are year after year or within each subsection of PAD recognition.
- Ask about the detail-level of the figure describing the development model - in the report - how detailed should the figure be? Is the one Kristian made too detailed?
- Inquire supervisor about the state of the art function results for Oulu test-data.

Highlights and Key Decisions

- Focus on 2D Attacks when it comes to writing about SOTA
- Figure 2 within question (the new one) can be used as a secondary
- Add examples of each type off attack when discussing them using figure 1.
- Need to mention that in figure 2(new one) there are different attacks that we do not necessarily focus on.
- Updated task-issuer on progress in terms of SOTA-based detection method

Agreements

- The meeting tomorrow has been re-defined as an individual work session.
- Hamza will begin actually writing the state of the art chapter of the thesis report

-
- Kristian will work on summarizing development phase 2, and then finalize the project development process part of the thesis report.
 - Milosz is traveling, and is therefore unavailable for this session.
 - The next week (Week 15) will have no structured meetings, due to Easter. Group members will keep in contact through Discord when needed, and work on their assigned tasks. Easter will be a scheduled break for the project, and development phase 3 starts on Tuesday, 19th of April.

Summary

Some updates on package-progress, and some clarifications on

35 Development Phase 2: Summary

04.04.2022

Phase Goals

- Conducted extensive research on "state of the art" of presentation attack detection. This will become a large part of the theory part of the thesis report.
- Wrote and finalized "development process" part of the thesis report to a stable state.
- The package-development itself shifted some focus, when compared to the original plan, per request of the task-issuer and supervisor. The focus was shifted from multiple functions for attack detection, to mainly the depth-sensing function. The depth-function required an extensive amount of data to be created, as no compatible data is publicly available due to this being a new topic within PAD.
- Since the focus-shift, the eye-gaze function was shelved, and the full focus fell onto the depth-function.
- Towards the last week of this phase, the supervisor advised the group to start benchmarking our functions and compare results with the current "state of the art" for presentation attack detection. This process required a lot of both processing-power and time to complete.
- This phase became much more data-collection heavy than first anticipated. The data-collection itself lasted for a whole development week. As a consequence, some of the function development was slowed, and pushed into the next development phase.

Week 10: 07.03-13.03

Goals

- Figured out error-rates and determinants for attack detection for the package in its current state. Showed promising results on our chosen test-datasets.
- Gained access to a plethora of new closed-access PAD-specialized datasets. These would further be used in extensive testing attempts.
- Implemented a lightweight eye-gaze detection function using MediaPipe-libraries.
- Developed a function that utilizes iPhone TrueDepth-data to conduct attack detection. This was worked out with a small test-set of about 5 recordings with depth-data. At this point, due to lack of applicable data available, the depth-function development quickly went into a standstill-state. Development was agreed to resume once a proper dataset had been developed.

Week 11: 14.03-20.03

Goals

- Created the internal TrueDepth-dataset, simulating a large number of both bonafide authentication attempts, as well as multiple realistic attack scenarios, including most 2D-attacks. This dataset consists of close to 100 recordings of RGB-data with corresponding TrueDepth-data for each recording. The RGB-partition of the dataset will also be used for testing other attack detection functions.
- Continuous testing to determine EER (Equal Error Rate) and determinants for attack detection for each current function of the package.
- Supervisor and task-issuer shared code repository for the current state of the art algorithm for presentation attack detection. In the coming week, we needed to test our chosen dataset-partitions on this code.

Week 12: 21.03-27.03

Goals

- Work on state of the art result generation with our datasets. This data will be used to compare results with our own function results in the thesis report, to illustrate strengths and weaknesses when compared to what is currently the "best" within this topic.
- Extensive work on the thesis report document. The development process part of the report is now close to finished. The research of the "state of the art" part of the document has concluded, and a overarching vision of this section has been formed in collaboration with the supervisor.
- The focus of this week became data-collection, and report writing. The functions that were set to be developed, as per the plan, were not in a finished state at this point. This is rooted in both a shift in project-focus, and lack of appropriate data. The data for testing the current depth-function has now been fully collected, and is compiled and ready for usage. Development and testing of the function will continue in development phase 3.

DEVELOPMENT PHASE 3

36 Development Phase 3: High-Level Plan

21.04.2022

Phase Goals

- Gathering results from the package functions
- Complete the TrueDepth-dataset to test depth-based functions properly, and ensure functionality.
- Combine results into one attack-detection result for the package output.
- Finalize the report to a steady state (Deadline: 5th of May)
- Finalize the package to a steady state (Deadline: 5th of May)

Week 16: 18.04-24.04

Goals

- Continue developing the thesis report.
- Work on optimization of the current application functions. Developing more concrete results of the program.
- Plan for a final output of the program.

Week 17: 25.04-01.05

Goals

- Develop the output-parameter for attack detection.
- Fully develop the TrueDepth-dataset to a completed state.
- Compile program results and discuss this in the report
- Finalize the main parts of the report, in addition to results.

Week 18: 02.05-08.05

Goals

- Finalize the thesis report for approval by task issuer on Thursday 05.05.
- Finalize the program itself for approval by the same date as the report.
- Work on feedback gathered, and alter both the report and the program in relation to task-issuer feedback.

37 Development Phase 3: Discussion meeting

21.04.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Easter Break - all group members have had a scheduled break, and are now back in full action.
- Kristian wrote the development process part of the report - to a stable, present complete state.
- Hamza finalized research of SotA over the break. Worked on adding 100+ sources to the bibliography, to be used in this part of the thesis report. Continued on writing the part, and made some progress.

Action Items

- Summary meeting - how did the easter break go? got a chance to relax and rejuvenate? Ready to get back in to the thesis work?
- Formulate Development Phase 3 Plan.
- Discuss further development of both the code, and also the thesis report.
- Work on what we discussed.

Highlights and Key Decisions

- Easter seemed to have had a rejuvenating effect on the group, and we are now ready to get back into the task at hand.
- With two weeks left before a stable draft is due for delivery, there is pressure on the group to perform over the next few weeks. There is some work left to be done.
- Focus on the code should be to tie up loose ends, and bring the output to one standardized output (for the package-aspect of it).
- For the report, more individual parts have been assigned. Hamza is still working on the "State of the Art"-section, which is highly detailed and complex to write. Kristian finished up development process over the break, and will continue with project discussion next. Milosz will write the technical design and implementation part, as he has the most hands-on experience with the code.
- Formulated a high-level plan for development phase 3.

Agreements

- A lot of work is ahead of us. Tomorrows meeting has been re-defined as an individual work session. All group members will stay in touch, and update on progress in the digital Discord-channel.

Summary

A meeting, with the primary goal of starting up development phase 3. The urgency of the matter of the project became abundantly clear during this meeting, and we are ramping up individual work to ensure completion, of high quality.

38 Further Data Collection

25.04.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Over the last individual work-session, plus the weekend, as a consequence of continuous testing of the depth-function, there has again risen a need for more depth data. This is aimed for collection during the first half of this week.

Action Items

- Collect more depth data
- Continue thesis report work
- The work is split into a 2/1-formation, where 2 of the group members work entirely on collecting new depth-data. The last member will continue the thesis report work.

Highlights and Key Decisions

- Resolved issue with update in Xcode. Due to complications regarding OS and code versions, we were set back about 2 hours, and we were not able to collect as much data as originally planned.
- Collected 48 more depth data files from 12 unique individuals.
- Made further advancements on thesis report document.

Agreements

- There will be more data-collection sessions conducted through Wednesday of this week, 27.04. The data-collection sessions will not count as traditional meetings, but rather work sessions. The two group members conduction depth-data collection during this meeting, will be meeting and collecting an assortment of various depth data over the next few days.
- Hamza will continue with writing on the thesis report over the same period of time.

Summary

Another data-collection meeting for the ever-expanding TrueDepth dataset.

39 Task-issuer update meeting: Dataset Development 28.04.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

Supervisor

Kiran Raja - kiran.raja@ntnu.no

Additional Participants

Hareesh Mandalapu - hm@mobai.bio

What has happened between last meeting and now?

- Over the last days, Milosz and Kristian collected a large amount of depth data for the internal dataset. This took massive effort, but it is now considered to be complete. The dataset includes 50 unique individuals, with attack scenarios for each individual included in the bonafide part of the dataset (both digital, and paper-based attacks).

Action Items

- Show task-issuer and supervisor the completed dataset.
- Inquire supervisor on what should be included, in terms of results, in the thesis report.
- Hear feedback on the items showed off during the meeting.
- Produce results from the new dataset. Models need to learn from the new data. EER-graphs need to be graphed.
- Continue thesis report development.

Highlights and Key Decisions

- Task-issuer reminded us that the stable draft is due in one week
- Produce a set of slides (presentation) describing the project as a whole.
- Include a clear README-file in the final code for operability. We plan on including this, as is standard practice, this was just a subtle reminder.
- Include a README-file in the final dataset.

Agreements

- Now that everything is set, there is mostly individual tasks left to do this week. These tasks mostly contain processing the new data acquired in the first part of the week, and also further developing the thesis report. The next scheduled meeting, Friday 25.04.2022, has been re-defined as an individual work meeting. Each group member is working on their assigned task.

Summary

A finalized dataset task issuer-update, and stable draft deliverable clarification meeting.

40 Stable draft meeting

02.05.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Hamza has covered a large amount of the State of the Art part of the thesis report. This part will undoubtedly be one of the most in-depth parts of the report, and also the largest. Good progress.
- Milosz has developed results using both internal and external datasets - the internal dataset, with depth, shows positive results when compared to other public datasets.
- Kristian updated further parts of depth development, and also the technical specifications of the mobile depth application.

Action Items

- Define the work week. With the impending 02.05 stable draft submission, we need to fully focus on stabilizing the thesis report further. The plans defined in this meeting, will cover the rest of the work week, up until the submission deadline.

Highlights and Key Decisions

- Hamza and Kristian will continue with the thesis report.
- Milosz will continue to develop and analyze results, and eventually add this to the report when "finalized" for stable draft delivery.

Agreements

- For the remaining days of the week, the work will be conducted in a work-from-home environment. This works best for the work that is ahead, based on previous experiences. Each group member now has their own tasks, and will continue with these up until Wednesday of this week (04.03). Constant communication and individual progress updates will happen on the Discord-platform.
- The Thursday-meeting (05.05), with stable draft delivery, will happen on-campus.

Summary

A short work definition-meeting. Here we defined what lies ahead in the next few days, in terms of work that has to be done.

41 Results and conclusion discussion meeting

04.05.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Milosz has developed thorough, and semi-conclusive, results using the depth data collected last week. The usage of depth in conjunction with normal RGB data leads to better attack detection with the data we have on hand.
- Hamza and Kristian have continued to write the thesis report, and it is coming along nicely. The main sections missing are technical design (which Milosz has expressed desire to write), results, and conclusive notes.

Action Items

- Discuss the presentation of results. Which results should be shown off to define the point of the report.
- Discuss the structure of the conclusion and abstract of the report.

Highlights and Key Decisions

- Gained some more conclusiveness to the presentation of results. We are now in agreement of what to show off, and how to discuss it.
- Drew up how to conclude the project in the report.

Agreements

- Continue extensive report writing, and have a stable draft ready by the end of the day.
- Keep constant contact within Discord, if there is anything that is prone to discussion.

Summary

Discussion meeting of certain aspects of the thesis report. Came to agreement on a number of things regarding individual report parts.

42 Stable Draft Delivery

05.05.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

Supervisor

Kiran Raja - kiran.raja@ntnu.no

Additional Participants

Erik Guoqiang Li - gl@mobai.bio

What has happened between last meeting and now?

- Finalized a stable draft of the report. This will be presented to the supervisor and task-issuer of the project.
- Visualized the results. Need more feedback on this, and hence it could be interpreted as unfinished.
- The conclusion of the report is still unwritten, as it needs more discussion and contemplation in order to be written.

Action Items

- Show off the stable draft of the report.
- Give the task-issuer a deadline for constructive criticism - Wednesday 11th of May.

Highlights and Key Decisions

- The main task-issuer representative for the project, whom we wanted feedback from the most, did not show up to this meeting. We sent out an e-mail to him, and expect him to give feedback within the set timeframe.
- Got feedback on the results-section of the report, and more viewpoints on how the results should be displayed. This needs to be further expanded upon in the following days/week.

Agreements

- The work this week has been quite extensive, so the following day (friday) will be used as a break-day, to reduce the probability of burnout amongst the group members.

Summary

The stable draft of the report and software was handed in this day. We are currently awaiting feedback from the task-issuer.

43 Development Phase 3: Summary

05.05.2022

Phase Goals

- Gathering results from the package functions
- Completed the TrueDepth-dataset and tested depth-based functions properly.
- Finalized the report to a stable draft state within the set deadline: 5th of May.
- Finalized the package to a stable/complete state within the given deadline: 5th of May.
- Both the report and package has been submitted to task-issuer and is awaiting concrete feedback.

Week 16: 18.04-24.04

Goals

- The report has been further developed. This is a constantly evolving report, with respective individuals of the group having their assigned tasks.
- Developed results for the package.
- Planned for a final display of results and utility of the package.

Week 17: 25.04-01.05

Goals

- The TrueDepth-dataset was completed this week, but took a lot longer than anticipated. This whole week, Kristian and Milosz did nothing but data-collection.
- Further tests were ran with the newfound data. These results are going to be shown off in the "stable draft" delivery.

Week 18: 02.05-08.05

Goals

- Finalized the thesis report for approval by task issuer on Thursday 05.05. This counts as a "stable draft" of the report, and only serves as an opportunity for the task-issuer to give us valuable feedback.
- Finalized the program itself for approval by the same date as the report. The same thing as mentioned above, with the task-issuer, also applies to the package and other data.
- We needed to give the task-issuer time to get back to us with feedback, so there was not a lot left to do this week. The third development phase concludes, and we now move right into the finalization phase of the project. This phase is exclusively for report-work, and finalizing every deliverable that exists for the project.

Finalization Phase

44 Report Results and Conclusion Discussion

09.05.2022

Participants

Group Members

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Lots of results have been visualized. New comments on the results, and discussion, has been added.
- The task-issuer has provided some feedback on the report.

Action Items

- Discuss the results, and how to conclude the thesis in a proper manner.
- Discuss and fix items the task-issuer has mentioned that could be improved.

Highlights and Key Decisions

- Hamza did not show up for the meeting, and we were therefore unable to get his thoughts on the results, and how to conclude the report. Kristian and Milosz discussed, and agree on the elements that need to be included in the conclusion.

Agreements

- Hamza needs to give his thoughts on the conclusion. A new meeting will be scheduled, and will happen shortly. This will be after the task-issuer feedback has been gathered.
- We need to tidy up the references, and find a way to make LaTeX actually display the references correctly.
- The next few meetings will only consist of thesis report writing.

Summary

A report-forward meeting, focusing on result-display and discussion-elements of the thesis report.

45 Discussing the Thesis Conclusion

12.05.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Thesis report progress has been great over the last few days. Now multiple parts of the report can be considered to be done.

Action Items

- Discuss the results and what implications they have on the conclusion.
- Draft both the conclusion and the abstract.

Highlights and Key Decisions

- Reached an agreement on the conclusion, and a draft of both the conclusion and the abstract has been created.

Agreements

- Continue individual work on parts of the report, and keep contact within Discord.

Summary

A shorter meeting, discussing the conclusive remarks and abstract of the thesis report.

46 Report Discussion with Supervisor

16.05.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

Supervisor

Kiran Raja - kiran.raja@ntnu.no

What has happened between last meeting and now?

- Even further progress has been made on the report. Now most parts are considered to be done.

Action Items

- Go through the entire report with our Supervisor.
- Note feedback from supervisor and work out issues mentioned in this meeting.

Highlights and Key Decisions

- Supervisor has mentioned some specific subsections, within the introduction, results, and organization chapters of the report, that can be updated with new information gathered from result analysis. These have been marked and commented in the document and will be inspected further in the coming days.
- He also mentioned a few errors within the structure of the report, organization and development process should go AFTER the conclusion.

Agreements

- Work further on individual parts, and there will be another physical meeting on wednesday of this week. Wednesday and thursday will focus entirely on finalizing the thesis report.

Summary

A supervision meeting consisting of report-writing and feedback.

47 Finalizing Thesis for Quality Assurance

18.05.2022

Participants

Group Members

Hamza Azim - hamzaa@stud.ntnu.no

Milosz Antoni Wudarczyk - miloszaw@stud.ntnu.no

Kristian Amundsen Øhman-Norén - kristaoh@stud.ntnu.no

What has happened between last meeting and now?

- Most of the conclusion was written by Kristian yesterday.
- Other members of the group took a day off, considering the day yesterday was Norway's Constitution Day.

Action Items

- Finish individual tasks assigned before tomorrow. Tomorrow is the day Kristian will focus on assuring continuity and quality for the entire report. The rest of the report will be concluded and handed in tomorrow.

Highlights and Key Decisions

- All group members now have set tasks, and is working in parallel with each other to ensure the report is ready for QA by the end of the day.

Agreements

- By the end of the day, all parts of the report, excluding the conclusion and abstract, need to be fully finished. The day following this one will only consist of quality assurance.
- Milosz will also prepare dataset and software for delivery (.zip).
- Tomorrow will be the last day of work on the project, and is considered a work session, as it will exclusively contain QA measures and other minor items to finalize the report. This will be the last meeting schedule included in the thesis report.

Summary

A final discussion meeting. The thesis report is scheduled for delivery one day before the deadline, which is tomorrow. This is the final meeting of the project.

G Timetables

Hamza

Day	Date	Time St	Time En	Hours	What has been done?	Sources
Monday	17.01.2022	12:00	14:00	02:00		
Tuesday	18.01.2022			00:00		
Wednesday	19.01.2022	12:00	15:30	03:30		
Thursday	20.01.2022			00:00		
Friday	21.01.2022	12:00	16:00	04:00		
Saturday	22.01.2022	12:00	14:00	02:00	Learning PyCharm + Python + OpenCV	https://tryhackme.com/c/omgpythontobasics
Sunday	23.01.2022			00:00		
Monday	24.01.2022	12:00	14:00	02:00	Startup Group Meeting + Creation of Discord Server for internal digital communication	
Tuesday	25.01.2022			00:00		
Wednesday	26.01.2022	10:00	13:30	03:30	Creation of group contract and project plan in Overleaf + Collaboration agreement modifications	
Thursday	27.01.2022			00:00		
Friday	28.01.2022	14:00	18:00	04:00	Meeting with supervisor and task giver, and a group collaboration session afterwards to discuss new information on the task	
Saturday	29.01.2022	06:00	10:00	04:00	Familiarising myself with and learning python on tryhackme.	
Sunday	30.01.2022	14:00	16:00	02:00	Reading up on some different python packages, and how they are made up.	
Monday	31.01.2022	10:00	14:45	04:45	Meeting with the group. Planning the week to come, finalising the project plan and the group contract. Worked mostly on group contract and beginning GANTT diagram.	
Tuesday	01.02.2022			00:00		
Wednesday	02.02.2022			00:00		
Thursday	03.02.2022	10:00	16:30	06:30	Meeting with mobai, more work on project plan, cleaning up language, creating risk analysis, learning more about opencv	
Friday	04.02.2022	10:00	14:00	04:00	Meeting with the team. Worked on researching facial recognition spoofing etc, worked with team to create a pitch for the high level use case to present to mobai on thursday.	
Saturday	05.02.2022			00:00		
Sunday	06.02.2022			00:00		
Monday	07.02.2022	11:00	17:00	06:00	Meeting with kiran, Learning about different ways that images can be processed, and getting a clearer understanding of python.	
Tuesday	08.02.2022	16:00	20:00	04:00	Learning PyCharm + Python + OpenCV	https://opencv.org/
Wednesday	09.02.2022			00:00		
Thursday	10.02.2022	12:00	15:00	03:00	meeting	
Friday	11.02.2022	11:00	14:45	03:45	meeting	
Saturday	12.02.2022			00:00		
Sunday	13.02.2022			00:00		
Monday	14.02.2022	10:00	14:30	04:30		
Tuesday	15.02.2022			00:00		
Wednesday	16.02.2022			00:00		
Thursday	17.02.2022	11:00	14:00	03:00		
Friday	18.02.2022	11:00	14:00	03:00		
Saturday	19.02.2022			00:00		
Sunday	20.02.2022			00:00		
Monday	21.02.2022	11:00	14:40	03:40		
Tuesday	22.02.2022	13:00	14:00	01:00	eye gaze research	
Wednesday	23.02.2022	11:20	16:10	04:50	working on eye gaze research and beginning to write code.	
Thursday	24.02.2022	11:00	15:30	04:30	Meeting with mobai. They elaborated on us needing to learn to extract depth data from ios. Continuing work on eye gaze after.	
Friday	25.02.2022	11:00	15:00	04:00		
Saturday	26.02.2022			00:00		
Sunday	27.02.2022			00:00		
Monday	28.02.2022	11:00	15:30	04:30	working with media pipe, implementing the example code from website-m	
Tuesday	01.03.2022			00:00		
Wednesday	02.03.2022			00:00		
Thursday	03.03.2022	11:00	14:00	03:00	Meeting with mobai. Kiran was not present. Got some help from hareesh about what to do, how to continue, etc.	
Friday	04.03.2022	11:00	14:45	03:45	Finalising meeting notes from previous notes and reflecting on the meetings so far.	
Saturday	05.03.2022			00:00		
Sunday	06.03.2022			00:00		
Monday	07.03.2022	11:00	14:00	03:00	Working with writing out the requirements and such with kristian, and looking at what we hope to and expect to achieve in the coming phase. Ad to leave early for a meeting, but this was fine as kristian and milosz had to work on their physics homework for the n	
Tuesday	08.03.2022	20:00	22:15	02:15	processing the data that we received from mobai.	
Wednesday	09.03.2022			00:00		
Thursday	10.03.2022	12:00	18:30	06:30	Meeting with mobai. Had a productive meeting meeting planning future interactions.	
Friday	11.03.2022	11:00	16:00	05:00	Meeting with the group. Working to find datasets since mobai is not giving any to us.	
Saturday	12.03.2022	19:00	00:00	05:00	reading literature given by Kiran on friday, taking notes to be able to recall it quickly when writing and to make it so other group members dont have to read through all of it.	
Sunday	13.03.2022	18:00	20:00	02:00	same as last. working on a review of state of the art paper.	
Monday	14.03.2022	11:00	13:45	02:45		
Tuesday	15.03.2022			00:00		
Wednesday	16.03.2022			00:00		
Thursday	17.03.2022	11:00	18:00	07:00	Meeting with mobai at their office. Demo. Lots of progress in understanding the requirements of this project.	
Friday	18.03.2022	11:00	14:00	03:00		
Saturday	19.03.2022			00:00		

Hamza

Sunday	20.03.2022	16:00	20:00	04:00	Reading a new doc on state of the art. Seems to have a lot of relevant information but at the same time seems to be impossible to understand.	
Monday	21.03.2022	12:30	16:00	03:30		
Tuesday	22.03.2022			00:00		
Wednesday	23.03.2022			00:00		
Thursday	24.03.2022	11:00	19:00	08:00	Expanding internal dataset and writing report and systemising sources.	
Friday	25.03.2022	11:00	17:00	06:00	Dataset expansion & reading	
Saturday	26.03.2022			00:00		
Sunday	27.03.2022			00:00		
Monday	28.03.2022			00:00		
Tuesday	29.03.2022	12:00	13:30	01:30		
Wednesday	30.03.2022	20:00	23:00	03:00		
Thursday	31.03.2022	10:00	15:00	05:00		
Friday	01.04.2022	11:00	15:00	04:00		
Saturday	02.04.2022			00:00		
Sunday	03.04.2022			00:00		
Monday	04.04.2022	11:15	17:15	06:00	Meeting with kiran then fixed the repo to convert video files into individual frames.	
Tuesday	05.04.2022	17:00	23:30	06:30	reading and writing the SOTA section for further details in the future for writing in the technologies chapter	
Wednesday	06.04.2022	19:30	23:15	03:45	Reading ComPaper3 to get a better overview of the timeline of the development of PAD since 2004. Hoping to get some mad writing done tomorrow.	
Thursday	07.04.2022	11:00	16:00	05:00	Meeting with kiran and hareesh. Kiran clarified a lot of things. Namely my tasks hereforth. I will need to create a timeline of PAD development.	
Friday	08.04.2022	00:00	04:00	04:00	citing sources	
Saturday	09.04.2022			00:00		
Sunday	10.04.2022	00:00	01:00	01:00	Writing more on the technologies part of the report.	
Monday	11.04.2022	00:00	02:00	02:00	Writing more on the technologies part of the report.	
Tuesday	12.04.2022	16:00	20:00	04:00	Writing more on the technologies part of the report.	
Wednesday	13.04.2022	12:00	20:00	08:00	Writing more on the technologies part of the report.	
Thursday	14.04.2022			00:00		
Friday	15.04.2022			00:00		
Saturday	16.04.2022			00:00		
Sunday	17.04.2022			00:00		
Monday	18.04.2022			00:00		
Tuesday	19.04.2022			00:00		
Wednesday	20.04.2022	08:00	12:00	04:00	report writing. Continuing on SOTA.	
Thursday	21.04.2022	11:00	16:00	05:00		
Friday	22.04.2022	11:00	14:00	03:00		
Saturday	23.04.2022			00:00		
Sunday	24.04.2022			00:00		
Monday	25.04.2022	11:00	14:00	03:00		
Tuesday	26.04.2022			00:00		
Wednesday	27.04.2022			00:00		
Thursday	28.04.2022	11:00	17:00	06:00	Further writing in different areas of the report. Clarified language. Elaborated in chapter SOTA	
Friday	29.04.2022	01:00	12:00	11:00	Report writing	
Saturday	30.04.2022	14:00	17:00	03:00	Report writing	
Sunday	01.05.2022	16:00	23:20	07:20	Report writing and a lot of reading today in addition to the things that kiran recently sent to me. Change of pace.	
Monday	02.05.2022	12:00	21:00	09:00	a lot of reading today. Why do prestatations attack! What is the point of detecting them? Who is bona? Why is he hide?	
Tuesday	03.05.2022	11:00	23:00	12:00	Wrote about PVMAD and its origins and clarified a lot of the language throughout the thesis.	
Wednesday	04.05.2022	12:30	00:00	11:30	General report writing. Elaborated a lot of areas and went into detail where deemed necessary and left some comments and suggestions for change for the others.	
Thursday	05.05.2022	11:00	15:30	04:30	Delivery of first draft. Feedback received from both gojuang and kiran. Tomorrow will be a rest day.	
Friday	06.05.2022			00:00		
Saturday	07.05.2022	15:20	17:30	02:10	working on the changes needed in chapter 1	
Sunday	08.05.2022			00:00		
Monday	09.05.2022	00:00	06:10	06:10	Worked with making all sources functional in JabRef. Great tool. Worked wonders.	
Tuesday	10.05.2022	18:00	21:30	03:30	Worked on improving chapter one. A lot had to be updated.	
Wednesday	11.05.2022	01:30	16:30	15:00	Rewrote chapter 1. Gave feedback on chapter 6 and read the entire report and added many tasks to the new trello board i made to share with the group to keep track of necessary changes. Spoke to hareesh and GQ about their thoughts on the thesis. Elaborated	
Thursday	12.05.2022	08:00	16:45	08:45	Finished the glossary and cited all the sources for it. Read more papers to add more to SOTA. Added the kiran paper.	
Friday	13.05.2022	17:00	19:30	02:30	rewrite some of chapter one. Will continue later. Will share with the group and ask for feedback when done.	
Saturday	14.05.2022	01:00	08:40	07:40	rewrote chapter one, added to chapter 3. Fixed some stuff according to feedback.	
Sunday	15.05.2022	15:00	20:40	05:40		
Monday	16.05.2022	13:00	17:10	04:10	Meeting with Kiran. Got a lot of help about how we should restructure and rewrite some of the parts of the report. Very productive.	
Tuesday	17.05.2022			00:00		
Wednesday	18.05.2022	13:00	23:00	10:00	Cleaned up much of the report. Lots of small compilation errors within the sources that had to be fixed. Created a draft for the abstract. Looked over the conclusion, had a meeting with kiran. Added the extra pages at the beginning of each chapter. This part did	
Thursday	19.05.2022	11:45	00:00	12:15		
Friday	20.05.2022	00:00	04:20	04:20	Finishing touches on the entire thesis. So many small things came up. Fixed a lot of language to make it academic. Worked together with the boys. Great night. Great thesis. Good job.	
	TOTAL			372:00		

Milosz

Day	Date	Time Start	Time End	Hours	What has been done?	Sources
Mon	17.01.2022	12:00	14:00	02:00	Startup Group Meeting + Creation of Discord Server for internal digital communication	
Tue	18.01.2022			00:00		
Wed	19.01.2022			00:00		
Thu	20.01.2022			00:00		
Fri	21.01.2022	14:00	18:00	04:00	Meeting with supervisor and task giver, and a group collaboration session afterwards to discuss new information on the task	
Sat	22.01.2022			00:00		
Sun	23.01.2022			00:00		
Mon	24.01.2022	11:00	16:15	05:15	Working on Gantt diagram, Group contract & Project plan	
Tue	25.01.2022			00:00		
Wed	26.01.2022			00:00		
Thu	27.01.2022	10:00	16:30	06:30	Gantt diagram, Group contract & Project plan, Task Issuer meeting	
Fri	28.01.2022	10:00	12:00	02:00	Gantt diagram, Group contract & Project plan, finalize	
Sat	29.01.2022			00:00		
Sun	30.01.2022			00:00		
Mon	31.01.2022	10:00	16:00	06:00	Package / Program Design	
Tue	01.02.2022			00:00		
Wed	02.02.2022			00:00		
Thu	03.02.2022	10:00	16:00	06:00	Package / Program Design & Logic Flow	
Fri	04.02.2022	10:00	14:00	04:00	Package / Program Design & Logic Flow	
Sat	05.02.2022			00:00		
Sun	06.02.2022	18:00	20:00	02:00	Working on a program prototype using OpenCV	
Mon	07.02.2022	10:00	17:00	07:00	Improving the prototype & meeting with project advisor to discuss the details of our package	
Tue	08.02.2022			00:00		
Wed	09.02.2022			00:00		
Thu	10.02.2022	11:00	17:00	06:00	Worked on implementing test data generation into the package	
Fri	11.02.2022	10:00	14:00	04:00	Worked generating the data set	
Sat	12.02.2022			00:00		
Sun	13.02.2022	18:00	21:00	03:00	Worked on the packages detection functions: Micro Movements	
Mon	14.02.2022	10:00	16:00	06:00	Trying out the micro movement implementation	
Tue	15.02.2022			00:00		
Wed	16.02.2022			00:00		
Thu	17.02.2022	10:00	14:00	04:00	Working on github repository & meeting with supervisor, improving micromovement detection function	
Fri	18.02.2022	11:00	17:00	06:00	Working on github repository readme & processing of test images for micromovements	
Sat	19.02.2022	19:00	22:00	03:00	Processing of test images for micromovements to determine accuracy & voodoo constants	
Sun	20.02.2022			00:00		
Mon	21.02.2022	12:00	15:00	03:00	Splitting of tasks & research, looking at the results of micro movement detection on test datasets & voodoo constants	
Tue	22.02.2022			00:00		
Wed	23.02.2022			00:00		
Thu	24.02.2022	11:00	15:30	04:30	Meeting with Mobai, working on depth detection & project rapport	
Fri	25.02.2022	11:00	16:00	05:00	Working with depth detection	
Sat	26.02.2022			00:00		
Sun	27.02.2022	18:00	22:00	04:00	Depth detection brainstorming: how could we process depth data to accomplish detection?	
Mon	28.02.2022	11:00	16:00	05:00	Worked on writing notes and things to include in the rapport	
Tue	01.03.2022			00:00		
Wed	02.03.2022	14:00	16:00	02:00	Report-writing class w/ Frode Haug	
Thu	03.03.2022	11:00	15:00	04:00	Preparation of iOS application demo for the Supervision meeting Further work on the package function (depth) and iOS Depth Capture application	
Fri	04.03.2022	11:00	14:30	03:30	End of development phase I, reflection on work done so far during phase I	
Sat	05.03.2022			00:00		
Sun	06.03.2022	18:00	23:00	05:00	Attempted optimization on micro movement detection	
Mon	07.03.2022	11:00	16:00	05:00	Development phase II planning, testing dataset against new optimization on micro movement detection, had a meeting with Kiran where he explained error- and determinant-calculations for attack detection	
Tue	08.03.2022			00:00		
Wed	09.03.2022			00:00		
Thu	10.03.2022	11:00	18:00	07:00	Discussion surrounding report work and motivation, impromptu meeting with the supervisor regarding this	
Fri	11.03.2022	11:00	18:00	07:00	Voicing our concerns to Mobai, work with supervisor on EER graphs	
Sat	12.03.2022			00:00		
Sun	13.03.2022			00:00		
Mon	14.03.2022	22:00	01:00	03:00	Talk with Mobai on Teams chat regarding our work, suggestions, etc. + own researching time	
Tue	15.03.2022			00:00		
Wed	16.03.2022			00:00		
Thu	17.03.2022	11:00	15:00	04:00	Physical meeting with Mobai, showcase of what Mobai is doing, question time, datasets + folders of pictures	
Fri	18.03.2022	11:00	15:00	04:00	Further work on the repo, peeking into depth histograms and equalization	
Sat	19.03.2022			00:00		
Sun	20.03.2022			00:00		

Milosz

Mon	21.03.2022			00:00	
Tue	22.03.2022			00:00	
Wed	23.03.2022			00:00	
Thu	24.03.2022	11:00	18:00	07:00	Meeting with Mobai, making of an internal bonafide & PA depth data set
Fri	25.03.2022	11:00	16:00	05:00	Worked on processing the data from the various datasets given through our package
Sat	26.03.2022			00:00	
Sun	27.03.2022	21:00	01:00	04:00	Worked on restructuring the package repo and processing data
Mon	28.03.2022	11:00	15:00	04:00	Processing data from the datasets given through our package methods
Tue	29.03.2022			00:00	
Wed	30.03.2022			00:00	
Thu	31.03.2022	18:00	21:00	03:00	Working on producing EER graphs for the depth mask method
Fri	01.04.2022	18:00	22:00	04:00	Working on getting PW_MAD implementation up and running
Sat	02.04.2022			00:00	
Sun	03.04.2022	18:30	01:00	06:30	Further work on PW_MAD package Processing OULU dataset to fit PW_MAD model input
Mon	04.04.2022			00:00	
Tue	05.04.2022			00:00	
Wed	06.04.2022			00:00	
Thu	07.04.2022			00:00	
Fri	08.04.2022			00:00	
Sat	09.04.2022			00:00	
Sun	10.04.2022			00:00	
Mon	11.04.2022	21:00	23:00	02:00	
Tue	12.04.2022			00:00	
Wed	13.04.2022			00:00	
Thu	14.04.2022			00:00	
Fri	15.04.2022			00:00	
Sat	16.04.2022			00:00	
Sun	17.04.2022			00:00	
Mon	18.04.2022			00:00	
Tue	19.04.2022			00:00	
Wed	20.04.2022			00:00	
Thu	21.04.2022	09:30	23:00	13:30	Making / Splitting datasets, processing data, training models, creating EER models
Fri	22.04.2022	12:30	17:00	04:30	Training more models, creating EER models
Sat	23.04.2022	20:30	00:00	03:30	Splitting data, creating datasets, training RGB & Depth models
Sun	24.04.2022			00:00	
Mon	25.04.2022	11:00	16:30	05:30	Gathering RGB & Depth data for the KMH dataset
Tue	26.04.2022	11:00	19:00	08:00	Gathering RGB & Depth data for the KMH dataset
Wed	27.04.2022	10:30	18:00	07:30	Gathering RGB & Depth data for the KMH dataset
Thu	28.04.2022	12:00	20:00	08:00	Processing the KMH dataset
Fri	29.04.2022	17:30	22:30	05:00	Splitting KMH dataset, Cleaning up repositories
Sat	30.04.2022	16:00	22:30	06:30	Cleaning up repositories, Preparing functions for RGB-D data, Preparing model for RGB-D data
Sun	01.05.2022	17:00	01:00	08:00	Training RGB and Depth models, Performing analysis on the first results
Mon	02.05.2022	11:00	18:30	07:30	Training RGB-D models, Performing analysis on results and cross-analysis on previous model's results (RGB, Depth), Writing in report (Design & Implementation), producing graphs
Tue	03.05.2022	12:00	23:30	11:30	Writing further in the report, producing graphs
Wed	04.05.2022	12:00	23:30	11:30	Writing further in the report, producing graphs
Thu	05.05.2022	12:00	03:00	15:00	Finishing up the design & implementation section in the report, producing more graphs
Fri	06.05.2022			00:00	
Sat	07.05.2022	18:00	22:00	04:00	Added models and wrote in the report, outlining the important details to be featured in the results and conclusion sections
Sun	08.05.2022			00:00	
Mon	09.05.2022	21:00	02:30	05:30	Worked on writing in the report and finishing up the result's section
Tue	10.05.2022	22:00	04:30	06:30	Worked on rewriting the results section as well as producing up to date models
Wed	11.05.2022			00:00	
Thu	12.05.2022	14:30	20:00	05:30	Graphing resulting ROC curve information into tables
Fri	13.05.2022	19:00	00:00	05:00	Writing section 5 & 6 in the report, producing figures and illustrations for related section's
Sat	14.05.2022	23:00	01:00	02:00	Creating tables for section 6
Sun	15.05.2022	22:00	23:00	01:00	Creating figures for section 6
Mon	16.05.2022			00:00	
Tue	17.05.2022	23:00	03:30	04:30	Restructuring and writing in section 4, 5 and 6
Wed	18.05.2022	12:30	02:30	14:00	Finishing up the report, producing tables and graphs, polishing the repositories, updating the figures
Thu	19.05.2022	11:00	00:00	13:00	Finishing up the report, producing tables and graphs, polishing the repositories, updating the figures
Fri	20.05.2022	00:00	04:20	04:20	
Sat	TOTAL			359:05	
Sun					

Kristan

Day	Date	Time Start	Time End	Hours	What has been done?	Sources
Mon	17.01.2022	12:00	14:00	02:00	Startup Group Meeting + Creation of Discord Server for internal digital communication	
Tue	18.01.2022			00:00		
Wed	19.01.2022	10:00	13:30	03:30	Creation of group contract and project plan in Overleaf + Collaboration agreement modifications	
Thu	20.01.2022			00:00		
Fri	21.01.2022	14:00	18:00	04:00	Meeting with supervisor and task giver, and a group collaboration session afterwards to discuss new information on the task	
Sat	22.01.2022	11:00	14:00	03:00	Familiarizing myself with Python, and setting the PyCharm IDE up to work properly with project files. Created Timetables for all group members	https://hr.puckles.com/group/pythonbasics
Sun	23.01.2022	12:00	14:30	02:30	Looked further into different open source Python-packages that could be used to solve the task at hand. Noted discussion points for these packages to discuss during the next meeting	
Mon	24.01.2022	10:00	16:30	06:30	Further development of Group Contract and Project Plan, creation of Gantt-diagram.	
Tue	25.01.2022			00:00		
Wed	26.01.2022			00:00		
Thu	27.01.2022	10:00	16:00	06:00	Meeting with supervisor and task giver to clarify issues we had since last meeting Group collaboration session afterwards, where we worked on finishing up the Project Plan	
Fri	28.01.2022			00:00		
Sat	29.01.2022			00:00		
Sun	30.01.2022	08:30	10:00	01:30	Finalizing and delivering contracts and plans due at the end of January	
Mon	31.01.2022	10:00	14:00	04:00	Initial High-Level Design model created. Discussions on different aspects of features.	
Tue	01.02.2022			00:00		
Wed	02.02.2022			00:00		
Thu	03.02.2022	10:00	14:00	04:00	Finalizing the design-document, and ready it for task-giver approval.	
Fri	04.02.2022	12:00	15:00	03:00	Meeting with supervisor to give thoughts on the design document and	
Sat	05.02.2022			00:00		
Sun	06.02.2022			00:00		
Mon	07.02.2022	10:00	17:00	07:00	Experimenting with OpenCV-libraries, to see how python and images truly interact with each other. Enlightening meeting on the project topic. The supervisor presented known and well-tested methods of presentation attack detection.	
Tue	08.02.2022			00:00		
Wed	09.02.2022			00:00		
Thu	10.02.2022	11:00	17:00	06:00	Start of the dataset creation using the developed tool. All group members create their own dataset after given specifications. If something goes wrong, or anyone needs help processing the dataset, this will be covered in the following meeting.	
Fri	11.02.2022	10:00	14:00	04:00	Completing the datasets for all members (4 x 60 Frames per group member, processed with DeepV2 Foreground/Background Algorithm)	
Sat	12.02.2022			00:00		
Sun	13.02.2022			00:00		
Mon	14.02.2022	10:00	16:00	06:00	Exploring the datasets, and similarity-calculation between each frame of each dataset. How do they vary? And how are they similar for the different behaviors? Wrote and updated the meeting summaries and other related documents to be up-to-date and up-to-standard.	
Tue	15.02.2022			00:00		
Wed	16.02.2022			00:00		
Thu	17.02.2022	10:00	15:00	05:00	Update-meeting with task-issuer Downloading and preparing new dataset, gathered from task-issuer	
Fri	18.02.2022	11:00	15:00	04:00	Discussed and agreed on ways of optimizing the current function. Needs further testing (to be done over the weekend).	
Sat	19.02.2022			00:00		
Sun	20.02.2022			00:00		
Mon	21.02.2022	12:00	17:30	05:30	Splitting of tasks. Assigned task: Research on depth-sensing. Have worked on this for this period. In addition, we discussed test-results generated through the weekend. Created skeleton of the main-report for the Thesis itself.	
Tue	22.02.2022	14:30	17:30	03:00	Finishing up the skeleton of the main-report. It is now fully prepared and compiled in Overleaf!	
Wed	23.02.2022	10:00	11:00	01:00	Fixed some formatting issues in Overleaf, and added an example on how to cite sources in the main report. Updated meeting summaries.	
Thu	24.02.2022	11:30	17:00	05:30	Task-issuer meeting + Further research on iPhone development and deployment. Gained access to Task-issuer Apple Developer Platform and explored opportunities on depth-detection.	
Fri	25.02.2022	10:00	17:30	07:30	Apple Developer Platform - solving issue with Guoqiang and Martin from Mobai Group meeting: Wrapping up the week, and Dev Phase 1. Further exploring individual tasks, for me, iPhone deployment and depth-data	
Sat	26.02.2022			00:00		
Sun	27.02.2022			00:00		
Mon	28.02.2022	10:30	16:00	05:30	Developing the depth-translation function. Working on documents for both meeting summaries.	
Tue	01.03.2022	14:00	16:00	02:00	Looking deeper into Swift syntax (for iOS development) and developing a more user-friendly GUI for the depth-capture application	
Wed	02.03.2022	14:00	16:00	02:00	Report-writing class w/ Frode Haug	
Thu	03.03.2022	10:00	17:00	07:00	Preparation of iOS application demo for the Supervision meeting Further work on the package function (depth) and iOS Depth Capture application	
Fri	04.03.2022	11:00	14:30	03:30	Wrapping up Development Phase 1 + Testing. Wrote Dev Phase 1 reflection notes.	
Sat	05.03.2022			00:00		
Sun	06.03.2022			00:00		
Mon	07.03.2022	11:00	16:00	05:00	Planning Phase 2 of Development. Wrote High-level Phase plan. Meeting with Supervisor - Development Updates and Introduction to error- and determinant-calculations for attack detection	
Tue	08.03.2022			00:00		
Wed	09.03.2022			00:00		
Thu	10.03.2022	11:00	18:30	07:30	Analyzing results from the optimized micromovement function. +Vast discussion about project motivation in relation to task-issuer and supervisor. Urgent meeting with supervisor	
Fri	11.03.2022	11:00	16:00	05:00	Discussing the collaboration-issues, and helping Mobai with the mobile application. Correspondence with Guoqiang - and further development on the depth-translation function	
Sat	12.03.2022			00:00		
Sun	13.03.2022			00:00		
Mon	14.03.2022			00:00		
Tue	15.03.2022	16:00	18:00	02:00	Depth-data for internal dataset - creation and formatting	
Wed	16.03.2022			00:00		

Kristan

Thu	17.03.2022	11:00	17:00	06:00	Task-issuer physical introduction. Introduction to the products they aim to deliver.
Fri	18.03.2022	11:00	15:00	04:00	Individual research on state of the art of presentation attack detection
Sat	19.03.2022			00:00	Further work on the state of the art section of the project report. Individual work on research.
Sun	20.03.2022			00:00	
Mon	21.03.2022	09:30	10:45	01:15	Organizational aspects, including updating the meeting reports so they are up to date.
Tue	22.03.2022			00:00	
Wed	23.03.2022			00:00	
Thu	24.03.2022	11:00	19:15	08:15	Internal Depth Dataset - Expansion (1.5GB of files, 90 recordings).
Fri	25.03.2022	11:15	16:00	04:45	All files compiled and named appropriately - uploaded to file sharing service
Sat	26.03.2022			00:00	Further report writing
Sun	27.03.2022			00:00	
Mon	28.03.2022	11:00	15:30	04:30	Report writing
Tue	29.03.2022			00:00	
Wed	30.03.2022			00:00	
Thu	31.03.2022	10:00	15:00	05:00	Task-issuer update
Fri	01.04.2022	11:30	15:00	03:30	Further updates on report structure, and appending data to the depth-dataset
Sat	02.04.2022			00:00	Report writing
Sun	03.04.2022			00:00	
Mon	04.04.2022	11:00	16:30	05:30	Meeting with supervisor
Tue	05.04.2022	11:30	16:00	04:30	Report writing + Diagram Creation (Project Structure)
Wed	06.04.2022			00:00	Report Writing - More on Development Process
Thu	07.04.2022	11:00	16:30	05:30	Report structuring and writing
Fri	08.04.2022	11:00	16:00	05:00	Writing - Report: Development Process + Development Phase 2 Summary
Sat	09.04.2022			00:00	
Sun	10.04.2022			00:00	
Mon	11.04.2022			00:00	
Tue	12.04.2022			00:00	
Wed	13.04.2022	11:30	16:00	04:30	Report writing - finishing depth-function development process + appending comments to other parts of the report
Thu	14.04.2022			00:00	
Fri	15.04.2022			00:00	
Sat	16.04.2022			00:00	
Sun	17.04.2022			00:00	
Mon	18.04.2022			00:00	
Tue	19.04.2022			00:00	
Wed	20.04.2022			00:00	
Thu	21.04.2022	11:00	16:30	05:30	Easter break Summary - Planning for Development Phase 3 - Individual writing on report
Fri	22.04.2022	10:00	16:30	06:30	Updating meeting documents
Sat	23.04.2022			00:00	Individual report work - reworking Discussion section - scattering into multiple branches of discussion for each section of the report
Sun	24.04.2022			00:00	
Mon	25.04.2022	11:00	17:30	06:30	Further expansion of dataset: 12 new subjects for bonafide - 48 new entries to the dataset
Tue	26.04.2022	11:00	19:00	08:00	Mapping subjects, re-labelling the bonafide part of the dataset based on subject - compiling and uploading for further use
Wed	27.04.2022	10:30	18:00	07:30	More dataset expansion - aiming for 50 unique bonafide subjects by wednesday. Added attack-attempt for each current existing subject for straight paper attack (42)
Thu	28.04.2022	11:00	16:00	05:00	Finalizing the dataset - 50 unique individuals in bonafide - and additionally paper attacks (both straight and curved), and display attacks of all 50 subjects
Fri	29.04.2022	11:00	16:30	05:30	Showing off the "final" dataset to task issuer.
Sat	30.04.2022			00:00	Further report writing
Sun	01.05.2022			00:00	
Mon	02.05.2022	12:00	18:00	06:00	Report work - iOS DepthCapture application - Technical Design
Tue	03.05.2022	11:00	16:30	05:30	Report work - stabilizing most already-written parts of the report
Wed	04.05.2022	11:00	21:00	10:00	Group Meeting - Discussing the final results and conclusion
Thu	05.05.2022	09:30	13:30	08:00	Report work - finalizing the stable draft document - for delivery to task-issuer tomorrow
Fri	06.05.2022			00:00	Further finalizing stable draft document + formatting appendices + creating project presentation
Sat	07.05.2022			00:00	
Sun	08.05.2022			00:00	
Mon	09.05.2022	10:30	17:30	07:00	Report writing - adding missing content in various sections - re-structuring
Tue	10.05.2022	11:00	16:00	05:00	Updating report further - implementing the new reference-file compiled by Hamza - labelling and fixing referrals within the various sections of the report
Wed	11.05.2022	10:00	16:30	06:30	Updating the meeting-documents so they are fully up to date.
Thu	12.05.2022	11:00	17:00	06:00	Report - wrote discussion elements that were not present. Fixed figure visibility issues
Fri	13.05.2022	09:30	17:00	07:30	Meeting - discussed the conclusion of the thesis, while also looking at the results.
Sat	14.05.2022			00:00	Writing more on discussion in the reports, some restructuring
Sun	15.05.2022	12:00	16:30	04:30	Defining the Abstract - draft version. Finishing the discussion
Mon	16.05.2022	10:00	22:30	12:30	Re-structuring the report. Writing conclusion, finishing up overseeing and correcting previously unfinished parts
Tue	17.05.2022	11:00	17:30	06:30	Writing conclusion to report - updating (and writing) sections task-issuer mentioned that should be included
Wed	18.05.2022	11:00	20:00	09:00	Work on finalizing the meeting documents, and fixing feedback on the thesis once again.
Thu	19.05.2022	11:00	00:00	13:00	Finalizing thesis report aspects, and quality-assuring the thesis.
Fri	20.05.2022	00:00	04:20	04:20	Quality Assurance and final delivery.
TOTAL					352:45

H Depth Data Collection: Protocol

Depth Data Collection Protocol

The subject will participate in 4 separate recordings with varying lighting and background conditions with set protocol behaviors

1. Usual behavior: Full focus on phone, normal behavior simulating attempt at authenticating oneself with the use of FaceID.
2. Semi-distracted behavior: Semi focus on phone, behavior trying to authenticate oneself but whilst a distraction is occurring, such as a conversation with a person.
3. Distracted behavior: No focus on phone, face completed to the side or varying a lot, similar situation as if a “over the shoulder” attack is occurring
4. Varied video: Varied focus on phone, varied lighting & background conditions.

I Depth Data Collection: Consent Form

Consent form data collection for

Improving and evaluating Facial Verification Algorithms on Various Cameras

This is an inquiry about participation in evaluating and improving the Mobai computer vision offerings. This specific data collection is conducted on an Apple iOS mobile system.

Purpose of the data collection

The main purpose of the data collection is to evaluate and improve our Mobai computer vision offerings, such as our face verification algorithms.

Responsible data processing organization

*Mobai AS (Org nr 922 935 815) is the organisation responsible.
CEO of Mobai AS: Brage Strand (brage@mobai.bio).*

Participation is voluntary

Participation in the data collection is voluntary. If you chose to participate, you can withdraw your consent at any time without giving a reason, and then all personal data of you will then be deleted.

Your personal privacy – how we will store and use your personal data

We will only use your personal data for the purpose(s) specified in this information letter. We will process your personal data confidentially and in accordance with data protection legislation (the General Data Protection Regulation and Personal Data Act).

- *Only personal from Mobai will have the access to your data.*
- *Your facial data (in the format of a video) will be anonymized with a random ID number as file name, no other personal data will be directly linked to this video file.*
- *The video of you will be used to evaluate, test, improve and create new algorithms.*
- *Mobai will never share or sell any of your data*

Your rights

So long as you can be identified in the collected data, you have the right to:

- access the personal data that is being processed about you
- request that your personal data is deleted
- request that incorrect personal data about you is corrected/rectified
- receive a copy of your personal data (data portability), and
- send a complaint to the Data Protection Officer or The Norwegian Data Protection Authority regarding the processing of your personal data

What gives us the right to process your personal data?

We will process your personal data based on your consent.

Where can I find out more?

If you have questions about the data collection, or want to exercise your rights, contact: *Mobai CEO: Brage Strand, by email: (brage@mobai.bio) or by telephone + 47 40 49 04 11.*

J Development Process: Micro-Movements

The first task we started working on in the entire project, was detection of micro-movements between background and foreground of a subject. A lot of research went into this function, and after a series of attempts and thorough testing, we decided to solve it using background segmentation. The foreground of the image in this method was detected using a pre-trained deep-learning algorithm, deeplab_v3. This algorithm is based on simple pre-defined detection algorithms, with the main goal being isolation of foreground objects ([60]).

The development process itself started with making some simple functions for each part of the overarching micro-movements-module. These functions based themselves on theory in regards to micro movements, pixel comparison for euclidean distance, image pre-processing & standardization (outline detection via deeplab_v3, resizing), and more. This series of functions are described in greater detail at [*CHAPTER 2.???*].

In the beginning, the usage of the deeplab_v3 algorithm for outline detection indicated lackluster performance. The upside, however, was that the function itself showed great results for the current datasets. We conducted a larger set of tests with an in-house specialized dataset received from the task-issuer. At this stage, it was found that results were quite accurate, but the performance was the key issue with this specific outline detection algorithm.

We tried to solve the performance-issues caused by the deep-learning algorithm in a multitude of ways. Some less successful than others. After a set of tests, the concluding measure that improved performance the most was a pre-processing procedure of the input-images. A series of tests of the developed micro-movement function was ran on the same images in different resolutions. It was found that drastically downscaling an image showed little to no effect on loss in terms of attack-detection result accuracy. Meanwhile, the function had near exponential growth in performance for each downscale-attempt. The optimal resolution, in terms of accuracy-to-performance ratio, was found through testing to be 144p.

After the results of the function utilizing deeplab_v3 had been fully analyzed, there seemed to still be some performance that was left to be desired. The function processed 5 consecutive frames in about 1.5 seconds, while keeping the attack detection accuracy we originally recorded. The group then started questioning if this type of method could be implemented in an entirely different, more performant, way. We then did some extensive research, and developed an alternative to the micromovements-function.

The method we developed to combat the performance even further utilized the MediaPipe-package for face detection. The MediaPipe-library is primarily built for handling face detection, and other object recognition, in a performant manner. This is to make the package able to work on camera live-feeds. The new function utilized this MediaPipe-package to create a bounding-box around the subjects face, and then some further processing on the created box. This processing is mainly related to the dilation-operation, where the bounding box was

enlarged to ensure most of the subject was covered. The micro-movements were then measured by the bounding box, instead of the outline created by the deeplab_v3 algorithm.

This solution improved the overall processing time by around 35%. The results this solution produced seemed to produce in some cases, but the overall results showed a decline in accuracy.

As a result of thorough analysis and testing of these developed functions, the group settled on using the original deeplab_v3 outline-detection approach of attack detection, with pre-processing measures that scales down the resolution of each image to allow for optimal execution speed to accuracy ratio.

K External Libraries & Dependencies

K.1 NumPy

NumPy is an open-source library primarily used within python-based environments. The primary goal of this library is to enable numerical computing with Python. It includes advanced mathematical functions, that are used in conjunction with image processing libraries to process pixel-values mathematically. ([61])

K.2 OpenCV

OpenCV (Open Source Computer Vision Library) is an open source computer vision and machine learning software library. The library has more than 2500 optimized algorithms, which include a comprehensive set of both classic and state-of-the-art computer vision and machine learning algorithms ([62]). This project primarily uses OpenCV as the go-to tool for opening and processing images within a Python-based environment.

K.3 PyTorch & torchvision

PyTorch

PyTorch (torch) is a Python package that enables Tensor computation (like NumPy) with strong GPU acceleration [63]. This is used to drastically improve the processing times per image frame with PAD-algorithms.

torchvision

The torchvision package consists of popular datasets, model architectures, and common image transformations for computer vision. TorchVision enables model architectures to work with computer vision tasks in Python [64].

K.4 MediaPipe

MediaPipe is a set of libraries that offers cross-platform, customizable machine learning solutions for human artifact detection in videos [65]. This project utilizes

the Face Detection-package of MediaPipe to create a bounding box to crop out faces within the PAD-process.

