UNIVERSTIY OF APPLIED SCIENCES BERLIN

Detecting Deep Fakes in Video Communication

BACHELOR THESIS

International Degree Program Media and Computer Science

Department 4: Computer Science, Communication and Economics

BACHELOR OF SCIENCE

by

Liav Keren

First Supervisor: Prof. Dr. Sebastian Knorr

Secondary Supervisor: Hendrik Graupner

Submitted on:??????

Table of Contents

[ABSTRACT III](#_Toc168926644)

[LIST OF FIGURES III](#_Toc168926645)

[LIST OF TABLES III](#_Toc168926646)

[LIST OF ABBREVIATIONS III](#_Toc168926647)

[INTRODUCTION 1](#_Toc168926648)

[Background of the Study 1](#_Toc168926649)

[Problem Statement 1](#_Toc168926650)

[Research Objectives and Questions 1](#_Toc168926651)

[Scope 1](#_Toc168926652)

[Structure of the Thesis 2](#_Toc168926653)

[Literature Review 3](#_Toc168926654)

[Introduction 3](#_Toc168926655)

[Deep Fakes 3](#_Toc168926656)

[Biometrics 3](#_Toc168926657)

[Pupillometry 3](#_Toc168926658)

[Self-Recognition 3](#_Toc168926659)

[SOURCES 3](#_Toc168926660)

# ABSTRACT

# LIST OF FIGURES

# LIST OF TABLES

# LIST OF ABBREVIATIONS

# INTRODUCTION

## Background of the Study

On May 21 of this year, a meeting occurred between an employee of Arup Group Ltd.’s Hong Kong branch and multiple executives, including the Chief Finance Officer (CFO). In this meeting, the CFO requested the employee to transfer HK$ 4,000,000 (equivalent to around US$511,968 at the time of publication) to various accounts. Following a failed verification, the employee realized that she has been a victim of a phishing scam, whereby the CFO and all other executives attending the online meeting have been deep fake impersonations of said individuals [1]. The incident coincides with a rise of deep fake scams and its uses for political motivated attacks. Deep fake technology poses a security risk for individuals, companies and political entities. As the technology improves, it would be both easier for impersonators to create fakes from limited data, as well as it would become harder to detect them. The cost of deep fake scams is predicted to cost \_\_\_\_[FIND SOURCE]. With many scholars warning of the dangers of deep fakes to democracy [FIND SOURCE] and just this year, its uses have transformed the election landscape in India [SOURCE].

## Problem Statement

With Covid forcing many to work online, video calls have become integral to communication in government institutions. Deep fakes pose a security threat, whereby a person outside of the institution can impersonate a member of the government and collect classified information. As the deep fakes become more realistic, it will be harder to detect visual artifacts that indicate the use of deep fake masks. \_\_\_\_

## Research Objectives and Questions

This paper will propose a novel way of detecting deep fakes. Building on the previous research by Schwetlick at al. (2023), it will aim to improve the results using a field data collection method, longer data collection trials and improved data engineering methods. This paper will aim to compare the classification results of classes self, deep fake and not self with the results of the previous study. Considering various evaluation metrics for multi class classification.

In this paper the following questions will be answered:

Is it possible to detect deep fakes during video calls with models trained on pupillometry?

Is the model more reliable in detecting deep fakes in comparison with the work by Schwetlick et al (2023)?

## Scope

Using Gazepoint GP3 eye tracker device to measure various biometric data from eye dynamics, with the main objective of capturing pupil size changes. The study will focus on extracting valid eye pupil size changes during a specific measurement timeframe of 3000ms (as shown in (Schwetlick et al. 2023) [SOURCE HENRIK PAPER]), in which the subject will turn his gaze on the screen from a non-person-point towards either themselves or another person on the call. During the measurement timeframe in which the subject either gazes upon themselves or towards another participant in the video call, the subject must not blink.

Unlike the previous study (Schwetlick et al. 2023), this paper will only focus on pupil size changes and will not include microsaccadic dynamics, because of technological limitations of the eye tracker model. To measure microsaccadic dynamics, the eye tracker must at least capture 150Hz per frame [SOURCE]

The study will focus on three subjects, with data being captured over several hours through scheduled video calls during their working hours. This data capture will be conducted as field research. The measurements took place over the span of 3 weeks, between the 27th of May and the 14th of June.

For each subject, feature engineering will take place and will include extraction of statistical features (find another name) and a transformation (write it better). A series of traditional machine learning classifiers will use the data to classify between self, not self and deep fake for each subject.

## Structure of the Thesis

At first, an introduction to the field is done via a literature review, focusing on previous studies in the field of eye tracking, biometrics, deep fakes, pupillometry and a short summary of the paper (Schwetlick et al. 2023), as a comparison guide to this thesis. It follows this up with a deep explanation of the technology used for the research. There, the Gazepoint GP3 eye tracker device and its output will be introduced alongside the training client script used to calibrate and communicate with the eye tracker. Following this, a subsection on the trial setup explains the apps used in the trial, such as DeepFakeLab, Teams video conference app, OBS and their settings. The section Deep Fakes is a comprehensive explanation and analysis of deep fake inner workings, history and current solutions.

Methodology => training client , data, data preprocessing pipeline, feature engineering pipeline and classification models with subsections on each classifier

Results => evaluation metrics, classification results and deep comparison with previous study

Conclusion => evaluating the result of the study compared to previous study, what it means to the field of deep fake detection and further research

# Literature Review

## Introduction

This section gives an overview of the literature used for this thesis. These are divided into 4 sections. Deep fakes cover all the literature gathered and used in the field of deep fakes. These both explain the technology and history of deep fakes. Biometrics include all the work done in the field of using eyes as a biometric identifier both for authentication and beyond. Unlike the previous section, Pupillometry concerns itself specifically with the changes in pupil dimeter for cognitive recognition. Lastly, Self-Recognition provides an overview of the previous study (Schwetlick et al. 2023) in the field.

## Deep Fakes

G. Pei *et al.* (2024) provides us with a technical history of deefake solutions, the different routes of research that has been taking place since 2017, as well as the different categories of deepfakes. I. Perov etal(2024)showcases in the paper the technique used for this paper.

## Biometrics

Nugrahaningsih, Nahumi, & Porta (2014) were the first ones to explore pupil dynamics to images as an authentication method. F. Deravi and S. P. Guness (2011) explore the idea of gaze having a unique and individual pattern when exposed to images.

## Pupillometry

# Self-Recognition

# SOURCES

* L. Schwetlick, H. Graupner, O. Dimigen, and R. Engbert, “Face- and Self-Recognition Affect Pupil Size and Microsaccade Rate,” p. 21, Jun. 2023.
* G. Pei *et al.*, “Deepfake Generation and Detection: A Benchmark and Survey.” arXiv, May 16, 2024. Accessed: Jun. 15, 2024. [Online]. Available: <http://arxiv.org/abs/2403.17881>
* I. Perov *et al.*, “DeepFaceLab: Integrated, flexible and extensible face-swapping framework.” arXiv, Jun. 29, 2021. Accessed: Jun. 17, 2024. [Online]. Available: <http://arxiv.org/abs/2005.05535>
* Nugrahaningsih, Nahumi, and Marco Porta. “Pupil Size as a Biometric Trait.” Lecture notes in computer science, 2014, pp. 222–33. <https://doi.org/10.1007/978-3-319-13386-7_18>
* F. Deravi and S. P. Guness, “Gaze Trajectory as a Biometric Modality,” School of Engineering and Digital Arts, University of Kent, Canterbury, United Kingdom: University of Kent and African Leadership University, 2011