 

### October University for Modern Sciences and Art

### Faculty of Computer Science

### Graduation Project Title: Deepfake Detection: Unmasking the Digital Impostors

### Supervisor: Dr. Wael Sersy

### Name: Ibrahim Mohamed Ezzat

### ID: 21196

### November 7, 2022

### Abstract

**Contents**

1. Introduction 6
   1. [Introduction 7](#_TOC_250031)
   2. [Problem statement 8](#_TOC_250030)
   3. [Objective 8](#_TOC_250029)
   4. [Motivation 8](#_TOC_250028)
   5. [Thesis layout 8](#_TOC_250027)
2. Background and Literature Review 9
   1. [Background 10](#_TOC_250026)
      1. [Machine learning 10](#_TOC_250025)
      2. [Deep learning 11](#_TOC_250024)
      3. [Transfer learning 11](#_TOC_250023)
   2. [Previous Work 11](#_TOC_250022)
      1. [Research 1 11](#_TOC_250021)
      2. [Research 2 11](#_TOC_250020)
3. Material and Methods 12
   1. [Materials 13](#_TOC_250019)
      1. [Data 13](#_TOC_250018)
      2. [Tools 14](#_TOC_250017)
      3. [Environment 14](#_TOC_250016)
   2. [Methods 15](#_TOC_250015)
      1. [System architecture Overview 15](#_TOC_250014)
4. System Implementation 16
   1. [System Development 17](#_TOC_250013)
   2. [System Structure 18](#_TOC_250012)
      1. [System architecture 18](#_TOC_250011)
      2. [TensorBoard 19](#_TOC_250010)
   3. [System Running 19](#_TOC_250009)
5. Results and Evaluation 20
   1. [Testing Methodology 21](#_TOC_250008)
   2. [Results 21](#_TOC_250007)
      1. [Limitations 21](#_TOC_250006)
   3. [Evaluation 22](#_TOC_250005)
      1. [Accuracy Evaluation 22](#_TOC_250004)
      2. [Time performance 22](#_TOC_250003)
6. Conclusion and Future Work 23
   1. [Conclusion 24](#_TOC_250002)
   2. [Problems 24](#_TOC_250001)
   3. [Future Work 24](#_TOC_250000)

References 25

**List of Figures**

2.1 Example of image 10

**List of Tables**

2.1 Table 1 Caption 11

**Chapter 1**

**Introduction**

# Introduction

This graduation project centers on the development of a web application dedicated to identifying deepfake content, a growing concern in the era of AI-generated deceptive media.

**Definition and Scope:**

Deepfakes refer to AI-generated multimedia, raising concerns about digital manipulation. The project's scope includes implementing advanced algorithms, machine learning, and computer vision for accurate detection

**Current Situation:**

****

**Figure 1.1**

The prevalence of deepfakes in social media and online platforms has surged, posing a significant challenge to content authenticity. As shown in Figure 1, instances of misleading content have become increasingly sophisticated.

**Evaluation and Gap Identification:**

The current situation underscores the urgency for effective deepfake detection tools. This project aims to offer a comprehensive and efficient web application for proactive identification and mitigation of deepfake content.Top of Form

# Problem statement

The problem in this area is that a lot of fake videos and pictures are spreading widely, making it hard to trust what we see online. As technology gets better at making these fake images and videos, there's a growing risk of people using them to spread lies, shape how others think, and make it difficult for us to trust what we see. The tools we have right now (later when the project is finished) spot these fake media often can't keep up with the newer, more advanced fake content. So, it's really important to find better and faster ways to identify and stop these fake images and videos. This is crucial for making sure that what we see online is truthful and to prevent the harmful effects of dishonest media.

# Objective

# Introducing a user-friendly web app that uses advanced algorithms and a high-quality dataset to accurately detect and evaluate the authenticity of media, including photos, videos, and audio. Tailored for non-technical users like journalists and social media platforms, the tool provides a simple interface with detailed authenticity percentages, empowering users to identify and report potential deepfakes across digital platforms.

# Motivation

Motivation for Others:

The significance of the proposed research on deepfake detection lies in its pivotal role in countering the rising tide of manipulated digital content. As deepfake technology becomes more sophisticated, there is a critical need for advanced tools to ensure the reliability of visual media, protecting individuals and society from the potential harms of deceptive information.

Motivation for the Researcher(me):

Engaging in research on deepfake detection is personally compelling as it represents a proactive contribution to the ongoing battle against misinformation and digital manipulation.

# Thesis layout

In this thesis, the first chapter will provide an introduction about the project and its aim. Then, the second chapter will provide a literature review and a background of the previous work in the same area of research

**Chapter 2**

**Background and Literature Review**

# Background

Figure 2.1: Example of image

## Machine learning

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Model | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Ref 1 Row 1 |  |  | test | test |  |  |  |  |
| Ref 1 Row 2 |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

Table 2.1: Table 1 Caption

## Deep learning

## Transfer learning

# Previous Work

## Research 1

A Visual Analytic Approach to Facilitate the Proctoring of Online Exams-2021 [1]

#### Strategy and structure

#### Data

#### Method evaluation

#### Results Evaluation

## Research 2

Massive Open Online Proctor: Protecting the Credibility of MOOCs certificates [2]

#### Strategy and structure

#### Data

#### Method evaluation

#### Results Evaluation

**Chapter 3**

**Material and Methods**

# Materials

## Data

## Tools

* + - * Python: high-level open source language based on C programming language commonly used for AI, machine learning, data analysis, automation of tasks.
      * Anaconda: is an efficient software platform mainly for python AI and machine learning development, which is useful to create separate python environment for every application which contains its own versions of libraries and different packages or even python version.
      * keras: is an open source library written in python that act as an interface for Tensorflow and artificial neural network.
      * Google colab: it is a google project that allow anyone to execute python with give specs.
      * Thinkgear: it is a tool that runs on background to direct data from EEG headset from serial port to an open network socket.
      * open-cv: it is a computer vision library developed by intel that is useful for model execution for machine learning, controlling webcam and input photos or videos to python

## Environment

* + - * CPU — Intel Core i7 9th Generation processor.
      * RAM — 16 GB
      * GPU - NVIDIA GeForce RTX 2060
      * Operating System — Ubuntu

# Methods

## System architecture Overview

**Chapter 4**

**System Implementation**

# System Development

#### Idea

#### Data Collection and preparation

#### Models

#### Modification of CNN model

# System Structure

## System architecture

## TensorBoard

In this section a data flow and graph represent each implemented model

# System Running

**Chapter 5**

**Results and Evaluation**

# Testing Methodology

# Results

## Limitations

# Evaluation

## Accuracy Evaluation

## Time performance

**Chapter 6**

**Conclusion and Future Work**

# Conclusion

# Problems

# Future Work

**Bibliography**

1. H. Li, M. Xu, Y. Wang, H. Wei, and H. Qu, “A visual analytics approach to facilitate the proctoring of online exams,” *Proceedings of the 2021 CHI Con- ference on Human Factors in Computing Systems*, May 2021. [Online]. Available: <http://dx.doi.org/10.1145/3411764.3445294>
2. X. Li, K.-m. Chang, Y. Yuan, and A. Hauptmann, “Massive open online proctor: Protecting the credibility of moocs certificates,” in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, ser. CSCW ’15. New York, NY, USA: Association for Computing Machinery, 2015, p. 1129–1137. [Online]. Available: https://doi.org/10.1145/2675133.2675245