CLASSIFICATION OF REAL AND FAKE HUMAN FACES USING DEEP LEARNING FOR DATA SECURITY

WAN MUHAMMAD AZIM BIN WAN SUHAIZAL

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

[CLASSIFICATION OF REAL AND FAKE HUMAN FACES USING DEEP LEARNING FOR DATA SECURITY]

[WAN MUHAMMAD AZIM BIN WAN SUHAIZAL]

This report is submitted in partial fulfillment of the requirements for the Bachelor of [Computer Science (Computer Security)] with Honours.

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2024

DECLARATION

I hereby declare that this project report entitled

Classification of real and fake human faces
using deep learning for data security

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : [WAN MUHAMMAD AZIM BIN WAN SUHAIZAL] Date : 31/8/2024

I hereby declare that I have read this project report and found

this project report is sufficient in term of the scope and quality for the award of Bachelor of [Computer Science (Software Development)] with Honours.

SUPERVISOR: _____ Date : 31/8/2024

([DR. ZAHEERA ZAINAL ABIDIN])

DEDICATION

To my beloved parents, I like to extend my thanks to my father and mother who always support me despite of many obstacles in life. I would like to express my gratitude and appreciation to them because they have given me a lot of encouragement and keep praying for successful future. This work hard is for my parents, and I want to make them happy.

To my fellow friends, thank you for being there for me throughout the entire bachelor program and their cooperation while conducting the research. I would like to express my gratitude to my supervisor for encouraging and believing in me to complete this research.

ACKNOWLEDGEMENTS

All praise is due to the All-Mighty Allah SWT, who has granted me the faith, strength, and abilities to comprehend, study, and complete this research. Peace and prayers be upon our most beloved Prophet Muhammad S.A.W., the most beautiful soul whose sayings, actions, and stories have profoundly inspired me to believe that there are no limits to what I can accomplish when fully committed to achieving something with Allah on my side.

I also revere the assistance and direction of my supervisor, DR. Zaheera Binti Zainal Abidin, for his guidance, encouragement, and patience in preparing this research. I am fortunate to have had such wonderful, loving, and supportive parents, who provided me with a home education while I was growing up and paid for my education until I graduated. They have been my pillar of fortitude, and to this day, they want to be the first to congratulate me on even the smallest of my accomplishments. To my colleagues who assisted in the arduous process of gathering data and preparing this research. May Allah bless you all for your perseverance and altruism. I would also like to thank my beloved parents who have supported and motivated me throughout my project.

ABSTRACT

The classification of real and fake human faces using deep learning has become increasingly critical for enhancing data security in various applications. This research focuses on developing robust deep learning models capable of accurately distinguishing between authentic and synthetic facial images. Leveraging techniques such as convolutional neural networks (CNNs) and advanced image processing algorithms, the study addresses the challenge of detecting sophisticated manipulations like deepfakes. A comprehensive dataset comprising diverse facial expressions, lighting conditions, and ethnicities is utilized for training and evaluating the models, ensuring their generalizability and reliability across different scenarios. The methodology includes image preprocessing, feature extraction, and model training using Google's Teachable Machine, facilitating intuitive model development and iteration. The effectiveness of the proposed approach is demonstrated through experimental evaluations, highlighting its potential to mitigate risks associated with fake media content and bolster data security measures. This research contributes to advancing the field of deep learning for facial recognition and underscores its role in safeguarding authenticity and trust in digital environments.

TABLE OF CONTENTS

Table of Contents

DECLARATION……ii

DEDICATION……iii

ACKNOWLEDGMENTS…… iv

ABSTRACT……v

TABLE OF CONTENTS……vi

LISTOFTABLES……x

LIST OF FIGURES……xi

CHAPTER 1:INTRODUCTION……1

1.1 Introduction……1
1.2 Problem Statements……3
1.3 Project questions……3
1.4 Project objective……..4
1.5 Project scope……4
1.6 Project contribution……5
1.7 Report organization……6
1.7.1 Introduction…… ..6
1.7.2 Literature review……6
1.7.3 Project Methodology……7
1.7.4 Analysis and Design……..7
1.7.5 Implementation……7
1.7.6 Testing……...7
1.7.7 Project Conclusion……7
1.8 Conclusion……8

CHAPTER 2 :LITERATURE REVIEW……..9

2.1 Introduction……9

2.2 Deep Learning……11

2.2.1 Convolutional Neural Network (CNN)……11

2.2.1.1 Convolution Layer……12

2.2.1.2 Pooling Layer……13

2.2.1.3 Rectified Linear Unit Layer (ReLU) ……14

2.2.1.4 Dropout Layer……...14

2.2.1.5 Batch Normalization Layer……...15

2.2.1.6 Fully Connected Layer (FC) ……..15

2.2.1.7 SoftMax……..16

2.2.1.8 Backpropagation……16

2.2.1.9 Adam optimization……17

2.3 Real and Fake face detection technique process……17

2.3.1 Dataset……..18

2.3.2 Data Collection……..19

2.3.3 Input Image……20

2.3.4 Image Preprocessing……..21

2.3.5 Real and Fake image detection and extraction. ……21

2.3.6 Image Segmentation……..22

2.3.7 Morphological Operation……...22

2.3.8 Output of the process image……...23

2.3.9 Data storage and integration……...23

2.4 Critical Review……...24

2.4.1 Comparative studied on Classification of real and fake human faces. ……..24

2.5 Critical Literature Review……..26

2.6.1 Combination between Convolutional Neural Network with Teachable Machine…….26

2.6.2 Combination between region Based Convolutional Neural Network with Teachable Machine……27

2.6 Challenge and Future Directions……28
2.6.1 Hybrid Approaches Combining Multiple Techniques. ……..28
2.6.2 Advancements in Deep Learning and AI...…….29
2.7 Conclusion...……...29
CHAPTER 3 :METHODOLOGY ……...30
3.1 Introduction……30
3.2 Methodology……..30
3.2.1 Previous Research……..32
3.2.2 Information Gathering……32
3.2.3 Define Scope……..32
3.2.4 Design and implementation. ……32
3.2.5 Testing and evaluation model.……...33
3.2.6 Documentation……..33
3.3 Project Flowchart……..34
3.4 Project Milestones.……35
3.5 Requirement Analysis.……..39
3.6 Software Requirements.……39
3.7 Hardware requirements.……40
3.8 Conclusion.……40
CHAPTER 4 :ANALYSIS AND DESIGN ……..41
4.1 Introduction……...41
4.2 Problem Analysis……...41
4.3 Project Requirement Analysis……....42
4.3.1 Dataset……...43
4.3.2 Technique Selection……...44
4.3.3 Image Extraction……...46

4.3.4 Image recognition and Training……47

4.3.5 Output……48

4.3.6 Software Requirement……...49

4.3.6.1 Google Teachable Machine……49

4.3.6.2 Phyton……50

4.4 Project Design……51

4.5 Proposed Method……...52

4.6 Conclusion……54

CHAPTER 5 :IMPLEMENTATION ……..55

5.1 Introduction……55

5.2 Process Module……..56

5.3 Teachable Machine……..57

5.3.1 Input ……57

5.3.2 Image Preprocessing ……59

5.3.3 Image Extraction……...60

5.3.4 Model Training and Evaluation……61

5.3.5 Output……62

5.4 Region Based Convolutional Neural Network ……63

5.4.1 Input ……64

5.4.2 Image Preprocessing ……...65

5.4.3 Image Extraction……..65

5.4.4 Model Training and Evaluation……...66

5.4.5 Output……...67

5.5 Conclusion ……...68

CHAPTER 6 : TESTING……69

6.1 Introduction……...69

6.2 Result Comparison……69

6.2.1 Result Comparison Average ……71

6.3 Discussion……71

6.4 Summary……...72

CHAPTER 7 : CONCLUSION……73

7.1 Introduction……73

7.2 Project Summary……73

7.3 Project Constraint……...74

7.4 Project Limitation ……..75

7.5 Future Work……75

7.6 Project Contribution……75

7.7 Conclusion……..76

REFERENCES ……77

LIST OF TABLES

Table 1.1 Summary of Problem Statement 1

Table 1.2 Summary of Project Questions 2

Table 1.3 Summary of Project Objective 4

Table 1.4 Summary of Project Contribution 5

Table 2.4.1 Comparative Studied On Classification of Real and Fake human faces 24

Table 3.4.1 Project Milestone 33

Table 3.4.2 Project Gantt Chart 34

Table 3.6 Software Requirement for the project 35

Table 3.7 Hardware Requirements 36

Table 4.3.2: Characteristic of deep learning 41

LIST OF FIGURES

Figure 2.1 Taxonomy of Project Background 10

Figure 3.2 Framework of the methodology model 31

Figure 3.3 Project Flowchat 34

Figure 4.3 Project Workflow 42

Figure 4.3.1.1 Example of real human face 43

Figure 4.3.1.2 Example of fake human face 43

Figure 4.3.3 Image Extraction 46

Figure 4.3.4 Image recognition and training 47

Figure 4.3.6.1 Teachable Machine 49

Figure 4.3.6.2 Python Library 50

Figure 4.4 Project Design 51

CHAPTER 1: INTRODUCTION

1.1 Introduction

Artificial intelligence and machine learning are used to make deepfakes, which are synthetic media in which a person's likeness is substituted for another people in an image or video. This technology creates extremely realistic but fake content using deep learning algorithms, specifically Generative Adversarial Networks (GANs). The procedure entails gathering copious amounts of data on the subject, training a model to imitate their movements and facial features, switching faces in video frames, and then post-processing to add further realism. Deepfakes are useful for study, education, and entertainment, but they also raise serious ethical and security issues because they can be abused to distribute false information.

Deepfakes pose serious issues, such as the dissemination of false information and fake news that has the power to sway public opinion and erode confidence in the media. Through the creation of unlicensed explicit content, they represent a serious threat to privacy, causing victims' grief and harm to their reputations. Due to their ability to access private data, deepfakes are also utilized for fraud and impersonation, which presents security risks. Because deepfake intricacies are difficult for present laws to address, making accountability more difficult, legal and ethical issues arise. The widespread occurrence of deepfakes undermines confidence in digital media, leading to doubts about authentic material and affecting sectors that depend on visual authenticity. Significant worries also include the psychological damage done to victims and the financial strain industries face in ensuring the validity of material. Deepfakes can also be used as a weapon for social and political manipulation, which has the potential to destabilize societies and affect political outcomes. To reduce these risks, strong detection technologies, sound legal frameworks, and public awareness campaigns are essential.

The goal of the proposed research is to use deep learning to examine the design and implementation of classification of real and fake human faces using deep learning. This project will require in depth investigation of the real and fake human faces.

The research will concentrate on determining the benefits and drawbacks of the current systems and recommending fresh approaches to get around drawbacks and boost the system's precision and effectiveness. A prototype system will be created, implemented, tested, and evaluated as part of the project to guarantee the system's accuracy and dependability under real-world circumstances.

The goal of my research on the classification of real and fake human faces using deep learning was to create a deep learning model that could reliably and extremely accurately differentiate between real and fake facial photos. Better classification performance was expected by utilizing state-of-the-art methods and a wide dataset that included different face expressions, lighting conditions, and ethnicities. It was anticipated that the model would not only identify complex synthetic faces, such as deepfakes, but would also be able to generalize well in many contexts, guaranteeing its usefulness. The model's interpretability and efficiency were also intended to be improved, making it easier to integrate into real-time applications and advancing the field of deep learning for image analysis.

1.2 Problem Statement (PS)

Deep learning, a subset of machine learning in artificial intelligence, is a powerful tool that enables networks to learn from unstructured or unlabelled data without explicit supervision. This technology has gained significant attention in recent years due to its remarkable performance in various applications, including image and speech recognition, natural language processing, and game playing.

One of the most exciting applications of deep learning is in the field of face detection and recognition. With the increasing use of profile images on social media platforms, deep learning techniques have become essential for detecting and recognizing faces in images. These techniques can distinguish between real and fake faces, providing a crucial layer of security for data protection.

Table 1.1: Summary of Problem Statement

PS	**Problem Statement**
PS_1	Human face is difficult to be identified either real or fake in digital format.

1.3 Project Question (PQ)

The current project question is the identification of Fake Faces using machine learning techniques. To address the problem statement, the project question needs to be formed.

Table 1.2: Summary of Project Questions.

PS	**PQ**	**Project Question**
PS_1	PQ_1	What are the characteristics of a fake picture?
PS_2	PQ_2	What is the algorithm to differentiate between real and fake faces?
PS_3	PQ_3	How to increase rate to classify fake face?

1.4 Project Objective (PO)

The project objectives are a critical element of final year project that outline the specific goals and milestones throughout the duration of the project. By achieving these objectives, the initiative intends to contribute to the advancement of deep learning-based classification of real and fake human faces.

Table 1.3: Summary of Project Objectives.

PS	PQ	PO	Project Objective
PS_1	PQ_1	PO_1	To study the authentic and synthetic face images using datasets.
PS_2	PQ_2	PO_2	To analyse the authentic and synthetic face image accuracy based on several techniques
PS_3	PQ_3	PO_3	To propose a suitable technique for determining the authentic versus synthetic face images

1.5 Project Scope

I. To study the authentic and synthetic face images using datasets.

II. To analyse the authentic and synthetic face image accuracy based on several techniques.

III. To propose a suitable technique for determining the authentic versus synthetic face images.

1.6 Project Contribution (PC)

The project has contributed to several topics outlined in this section, derived from the stated questions and objectives as presented in table 1.2 and table 1.3. Table 1.4 presents a concise overview of the scientific contribution.

Table 1.4: Summary of Project Contribution.

PS	**PQ**	**PO**	**PC**	**Project Contribution**
PS_1	PQ_1	PO_1	PC_1	A comparison of image in classification between real and fake human faces.
		PO_2	PC_2	Accuracy performance between real and fake.
		PO_3	PC_3	A new technique of classification of real and fake human faces.

1.7 Report Organization

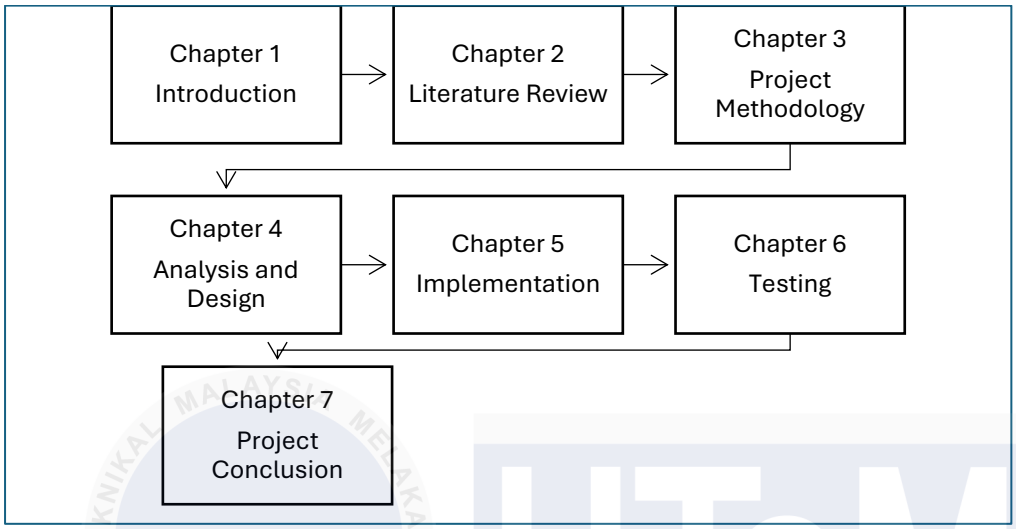


Figure 1.7: Report Organization

The visual representation in Figure 1.1 illustrates the necessary component to present the project under study comprehensively. These components include the introduction, literature review, methodology, design, implementation, testing and analysis, and project conclusion. The contents of each chapter will be discussed in subsequent subchapter.

1.7.1 Introduction

This chapter provides an overview of the project, including its background, problem statement, project questions, project objectives, project scopes, project contribution and the significance of using machine learning to detect real and fake human faces using deep learning for data security. It provides context for the remainder of the report.

1.7.2 Literature Review

This chapter will examine prior research, journal articles, conference. presentations, and other pertinent works for the project to justify its necessity. The chapter begins with a taxonomy diagram that will be used to examine the labelling, defining, and classification of the project framework. This chapter will provide reviews of significant project components, such as detection techniques, detection features, and datasets, to justify how the selected components could be adapted to the proposed solution. After this chapter, an overall analysis will be presented as the culmination of the literature reviews.

1.7.3 Project Methodology

This chapter justifies the methodology, and procedures used to complete the project. To contextualize the introduced process, this chapter discusses the methods for eliminating work-related tasks. The task must include four stages to achieve the project's objective. The use of this phrase encourages the completion and management of these responsibilities. It is founded on a basic framework and a comprehensive structure.

1.7.4 Analysis and Design

This chapter discusses the analysis and design of a classification of real and fake human faces using deep learning for data security. It comprises the system problem Analysis, requirement analysis, Data requirement, Functional and Non-functional requirement, others requirement, high-level design and Detailed design. The project's design decisions and considerations are elaborately described.

1.7.5 Implementation

This chapter concentrates on classification of real and fake human faces actual implementation. It discusses implementation-related tools, technologies, and programming languages. The chapter also discusses incorporating deep-learning models, data processing protocols, and other necessary system components.

1.7.6 Testing

This chapter describes the testing procedure and evaluation of the developed system. It contains the testing methodology, performance metrics, and results from testing the system against multiple datasets. The efficacy of the system and the analysis of the results are discussed about the project's objectives.

1.7.7 Project Conclusion

The concluding chapter offers an overview of the complete project. It discusses the accomplishments, constraints, and obstacles encountered throughout the endeavour. The chapter concludes with critical findings, recommendations for future improvements, and the

project's overall significance in the context of classification of real and fake human faces using deep learning for data security.

1.8 Conclusion

The introduction addresses the problem statement regarding the difficulties in detecting and recognizing real and fake human faces. The project aims to answer the question regarding real and fake human faces. This topic also discusses the objective to study algorithm and deep learning to improve security that related to real and fake human faces. Collecting a representative dataset, analysing the best features for differentiation, and developing a deep learning model comprise the project's scope. The project contributions Evaluating the effectiveness of the deep learning model in enhancing data security, developing a novel deep learning model for real and fake face detection that can improve data security, Exploring explainable AI techniques for facial manipulation detection.

Chapter 2: Literature Review

2.1 Introduction

A brief synopsis of the next literature review is given in the opening section, along with an outline of the chapters' thematic organization. The review will go over the foundations of deep learning and face recognition, explore the history and ramifications of deepfake technology, look at how it affects data security in different industries, review conventional and deep learning-based face classification techniques, investigate deep learning models specifically designed for face classification, point out flaws and limitations in current approaches, look at recent developments and potential directions for future research, and end with a summary of the project's main conclusions. Using deep learning for data security, this methodical methodology guarantees an exhaustive investigation of the classification of actual and false faces. The taxonomy of the project background is displayed in Figure 2.1.

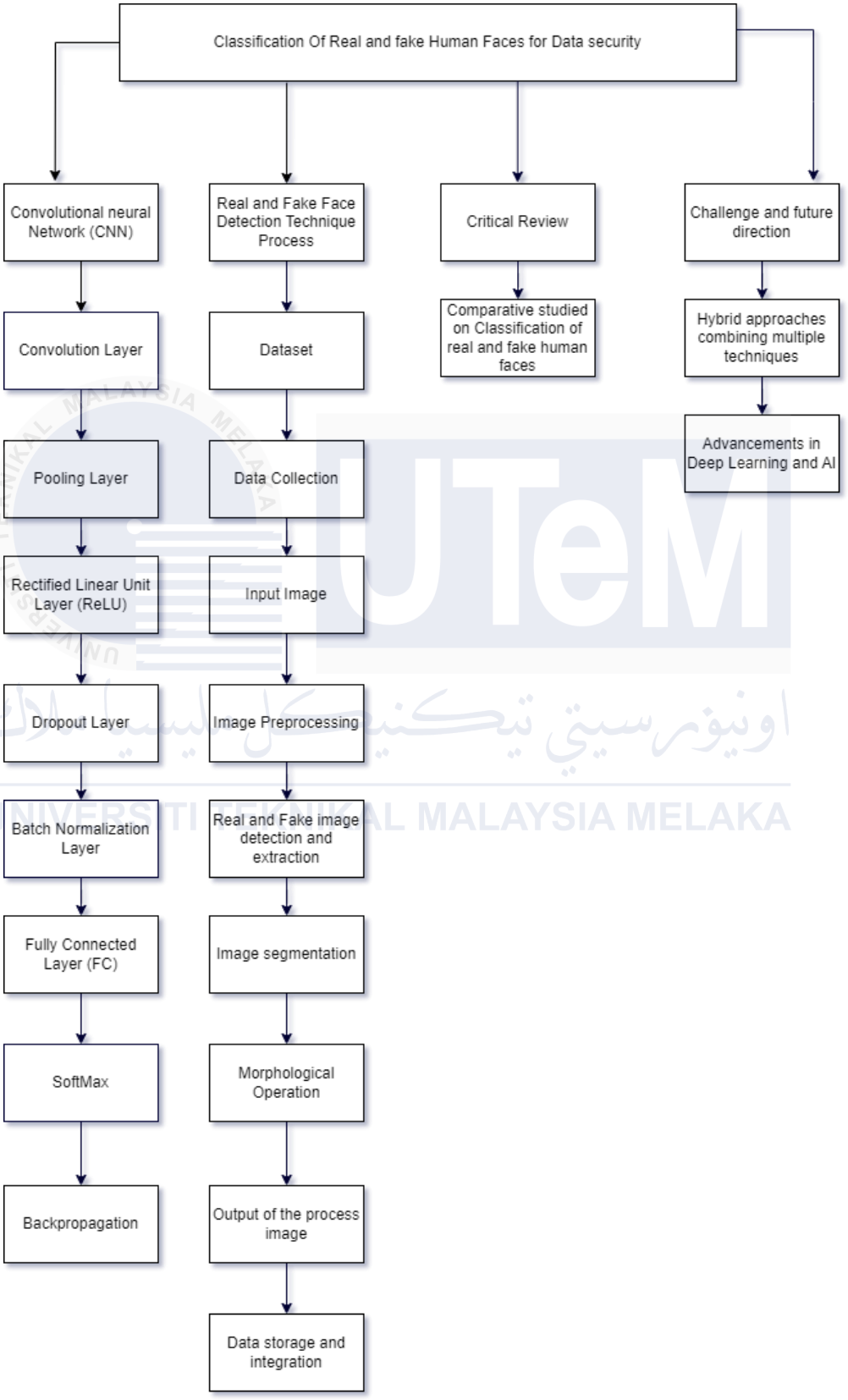


Figure 2.1: Taxonomy of Project Background.

2.2 Deep Learning

In the project "Classification of Real and Fake Human Faces Using Deep Learning for Data Security," deep learning is instrumental in developing advanced algorithms to differentiate between authentic and manipulated facial images. Utilizing Convolutional Neural Networks (CNN), these algorithms are trained on large datasets to learn distinctive features, enabling accurate classification of real and fake faces. Deep learning's ability to analyse complex visual data enhances the project's effectiveness in safeguarding data integrity and trust against potential threats. (Ranjan et al., 2018)

Convolutional Neural Networks (CNN) are highly effective in image recognition, classification, and object detection tasks due to their ability to automatically learn hierarchical representations of features from raw pixel values. They have revolutionized various fields, including computer vision, medical image analysis, and autonomous driving, and continue to be a cornerstone of deep learning research and applications. (Rohan, 2018) (Wu et al., 2017) (Chen, 2020)

2.2.1 Convolutional Neural Network (CNN)

Convolutional neural Network were initially proposed by LeCun (2010). In image categorization, CNN have done better than conventional computer vision techniques. (Krizhevsky et al., 2012) Neural network has at least one layer that uses a convolution operation rather than matrix multiplication. One of the primary areas for picture categorization and recognition is this one. According to theory, to train and evaluate deep learning CNN models, each input image is passed through several convolution layers that include polling, fully connected layers (FC), filters (Kernels), and the SoftMax function to classify objects with probabilistic values between 0 and 1. (Senan et al., 2020)

2.2.1.1 Convolution layer

The convolutional layer is a crucial component of convolutional neural networks. It applies filters to the input image, extracting relevant features such as edges, textures, and shapes. These extracted features play a vital role in determining whether a human face is real or fake, as certain patterns and details may differ between the two. Deep learning methods, specifically convolutional neural networks, have revolutionized the field of image classification (Wan et al., 2022). Their approach is based on three steps: First, convolutional neural networks are used to extract the features from VGG_Faces (Al-Eidan et al., 2020). After that, the result of the feature map is used to train the LSTM, which is a type of recurrent neural network (Zhao et al., 2018). The combination of convolutional neural networks and Long Short-Term Memory models allows for accurate classification of real and fake human faces, making it a powerful tool for data security (Al-Eidan et al., 2020). Therefore, by utilizing a combination of convolutional neural networks and Long Short-Term Memory models, it becomes possible to accurately classify real and fake human faces for data security purposes. Therefore, by utilizing a combination of convolutional neural networks and Long Short-Term Memory models, it becomes possible to accurately classify real and fake human faces for data security purposes, ensuring the integrity and authenticity of human identities in various applications (Brown et al., 1995).

2.2.1.2 Pooling Layer

The pooling layer is another important component of convolutional neural networks (Wan et al., 2022). It helps to down sample the feature maps extracted by the convolutional layer, reducing their spatial dimensions while retaining the most important information. This down sampling process allows for more efficient computation and helps in capturing the most salient features of the input image. By applying pooling layers in the convolutional neural network, relevant information is retained while reducing the spatial dimensions (Srinivas et al., 2016). This helps in improving computational efficiency and capturing the essential features of human faces, enabling more accurate classification of real and fake identities for data security purposes. Therefore, by utilizing a combination of convolutional neural networks and Long Short-Term Memory models, it becomes possible to accurately classify real and fake human faces for data security purposes, thus ensuring the integrity and authenticity of human identities in various applications. To address the challenges of processing time and storage memory, various methods have been proposed. One approach is to use pre-trained models like VGG_Faces for feature extraction, followed by training a Long Short-Term Memory model on the extracted features (Zhao et al., 2018). This approach allows for faster processing of a relatively small training set while also reducing the storage memory required for the features. Therefore, the combination of pre-trained models and Long Short-Term Memory models enables efficient and accurate classification of real and fake human faces for data security purposes, contributing to enhanced data protection and safeguarding against fraudulent activities.

2.2.1.3 Rectified Linear Unit Layer (ReLU)

The Rectified Linear Unit layer is commonly used in convolutional neural networks as an activation function (He et al., 2016). It introduces non-linearity to the network and helps in capturing complex patterns and features of human faces. By applying ReLU activation function in the convolutional neural network, the network becomes more capable of classifying real and fake human faces accurately by capturing intricate details and distinguishing characteristics (Wu et al., 2023). In addition, the ReLU layer addresses the incompatibility between element-wise addition and ReLU activation by introducing weighted residual networks (He et al., 2016). This allows for effective and efficient combination of residuals from different layers, contributing to the overall performance and accuracy of the network. Therefore, by utilizing convolutional neural networks with ReLU activation function and weighted residual networks, it is possible to accurately classify real and fake human faces for data security purposes, ensuring the integrity and authenticity of identities in various applications.

2.2.1.4 Dropout Layer

The dropout layer is a commonly used technique for preventing overfitting in deep learning models, including convolutional neural networks. It randomly selects a subset of the neurons in a layer and sets their outputs to zero during the training process. (Trevor, 2023) This helps in reducing the interdependencies between neurons and promotes the generalization ability of the network, making it less prone to overfitting. By incorporating dropout layers in the convolutional neural network, overfitting can be mitigated, leading to improved accuracy and generalization capabilities in classifying real and fake human faces.(Salakhutdinov, 2014)(SalakhutdinovRuslan, 2014)(Krizhevsky et al., 2012) Therefore, by incorporating techniques such as dropout layers and weighted residual networks in convolutional neural networks with ReLU activation function, the accuracy and generalization capabilities of the network can be enhanced, enabling more reliable classification of real and fake human faces for data security purposes (He et al., 2016).

2.2.1.5 Batch Normalization Layer

The batch normalization layer is another commonly used technique in deep learning models, including convolutional neural networks. By incorporating batch normalization layers in the network, the inputs to each layer are normalized, which helps in stabilizing and accelerating the training process (Zhang et al., 2020). This normalization technique reduces the internal covariate shift, making the network more robust and less sensitive to variations in input data. By utilizing batch normalization layers in the convolutional neural network architecture, the classification of real and fake human faces can be further enhanced. Moreover, the use of batch normalization layers helps in reducing the training time and improving the accuracy of classification by stabilizing the network during training and making it less sensitive to variations in input data. Therefore, by utilizing techniques such as dropout layers and batch normalization layers in convolutional neural networks with ReLU activation function, the accuracy, generalization capabilities.

2.2.1.6 Fully Connected Layer (FC)

The fully connected layer is a crucial component in deep learning models, including convolutional neural networks (Wang et al., 2021). It is typically located at the end of the network and serves as a classifier, mapping the extracted features to specific classes or categories. In the case of classifying real and fake human faces, the fully connected layer would receive the input from the previous layers and perform the final classification based on the learned features. Therefore, by incorporating fully connected layers in the convolutional neural network architecture, the network can learn and make predictions about whether a given human face is real or fake with high accuracy.

2.2.1.7 SoftMax

The SoftMax layer is commonly used as the final layer in deep learning models, including convolutional neural networks, for classification tasks (Stoian et al., 2019). It performs the task of assigning class probabilities to the input data. In the context of classifying real and fake human faces, the SoftMax layer would assign probabilities to each class, indicating the likelihood of a human face being real or fake (Zhou et al., 2022). By utilizing the SoftMax layer at the end of the convolutional neural network architecture for classifying real and fake human faces, it can obtain probability distributions over the two classes, indicating the likelihood of a given human face being real or fake. Therefore, by utilizing techniques such as dropout layers, batch normalization layers, fully connected layers, and a SoftMalayer in the convolutional neural network architecture, it can achieve high accuracy in classifying real and fake human faces while reducing training time and improving generalization capabilities.

2.2.1.8 Backpropagation

Backpropagation is a crucial algorithm used in training convolutional neural networks. It is used to compute the gradients of the loss function with respect to the network's parameters, allowing for the optimization of these parameters through gradient descent. By utilizing backpropagation during the training process of the convolutional neural network for classifying real and fake human faces, the network can effectively adjust its weights and biases to minimize the loss function and improve its ability to accurately classify real and fake human faces (Wang et al., 2021). Therefore, by incorporating fully connected layers, softmax layer, and utilizing backpropagation in the convolutional neural network architecture, it can achieve high accuracy in classifying real and fake human faces, while also optimizing the network's parameters and reducing the loss function during training (Zhou et al., 2022).

2.2.1.9 Adam optimization

Adam optimization is a popular algorithm used to optimize the parameters of a neural network during training (Wang et al., 2021). By utilizing Adam optimization in the training process of the convolutional neural network for classifying real and fake human faces, it can effectively update the network's weights based on the gradient of the loss function, leading to faster convergence and improved accuracy in classifying real and fake human faces (Yu et al., 2023). Furthermore, the use of Adam optimization helps in minimizing the loss function and adjusting the network's parameters, ultimately leading to improved accuracy in classifying real and fake human faces. By incorporating techniques such as dropout layers, batch normalization layers, fully connected layers, and a softmax layer in the convolutional neural network architecture, along with applying Adam optimization during training, it can achieve even higher accuracy in classifying real and fake human faces.

2.3 Real and Fake face detection technique process.

The process of the fake face detection technique involves several steps. First, the input image of a face is fed into the pre-trained convolutional neural network model. The model performs a series of convolutional and pooling operations to extract relevant features from the input image. These features are then passed through fully connected layers and a SoftMax layer to classify the input image as either real or fake (Stoian et al., 2019). By leveraging the power of deep learning, specifically convolutional neural networks, it can develop a robust system for classifying real and fake human faces using advanced techniques such as feature fusion networks, bounding box regression loss functions, and confidence loss functions to improve accuracy and reduce false detections (Yu et al., 2023). Therefore, our research focuses on utilizing convolutional neural networks to accurately classify real and fake human faces.

2.3.1 Dataset

To train and evaluate the fake face detection technique, a comprehensive and diverse dataset is necessary (Stoian et al., 2019). This dataset should consist of a wide range of real human faces as well as a significant number of fake or manipulated faces (Joshi et al., 2020). To address this, a dataset was collected that includes real human faces from various sources such as social media profiles, celebrity images, and stock photo platforms. To augment the dataset with fake faces, various techniques such as deepfake generation, photo manipulation, and digital compositing were employed (Le et al., 2022). With the collected dataset, a balanced distribution of real and fake face images was ensured to avoid bias. In recent years, deep learning technology has made significant advancements in computer vision research, allowing for the development of robust algorithms capable of accurately classifying real and fake human faces (Yu et al., 2023). By leveraging the power of convolutional neural networks and utilizing techniques such as feature fusion networks, bounding box regression loss functions, and confidence loss functions, a highly accurate model for distinguishing between real and fake human faces can be created.

2.3.2 Data Collection

Various sources, including social media profiles, celebrity photos, and stock photo platforms, were used to gather the data required for training and assessing the model. These sources made sure that the dataset was varied and included both artificially created and actual human faces. A comprehensive dataset representing a wide range of real and fake human faces was gathered based on these sources. The model can be evaluated and trained to distinguish between real and fake human faces with accuracy by using a broad dataset that includes real human faces taken from stock picture sites, celebrity photographs, and social media profiles. A convolutional neural network model may be trained to reliably and robustly distinguish between real and fake human faces using the gathered comprehensive dataset, enhancing data security and reducing the hazards associated with deepfake technology (TEMİR, 2020). Deep learning technology has advanced computer vision research significantly in recent years, enabling the creation of reliable algorithms that can distinguish between real and fake human faces with accuracy (Yu et al., 2023). Training a diversified dataset and utilizing deep learning algorithms can yield a highly accurate model for distinguishing between real and artificial human faces.

2.3.3 Input Image

A convolutional neural network model may be trained to reliably and robustly distinguish between real and fake human faces using the gathered comprehensive dataset, enhancing data security and reducing the hazards associated with deepfake technology (TEMİR, 2020). Deep learning technology has advanced computer vision research significantly in recent years, enabling the creation of reliable algorithms that can distinguish between real and fake human faces with accuracy (Yu et al., 2023). Training a diversified dataset and utilizing deep learning algorithms can yield a highly accurate model for distinguishing between real and artificial human faces. The Multi-Task Cascaded Convolutional Neural Network for face detection, a diverse dataset of real and fake human faces sourced from various sources, including social media profiles, celebrity images, and stock photo platforms, and the power of deep learning algorithms are combined to create a model that effectively analyses and classifies real and fake human faces, improving data security and thwarting the risks associated with deepfake technology. Three methods are proposed to reduce the likelihood of missed and false detections and increase the accuracy of the model: a confidence loss function to boost the model's confidence in its predictions, a bounding box regression loss function to optimize the localization of facial features, and a feature fusion network to combine multiple sources of information (Yu et al., 2023).

.

2.3.4 Image Preprocessing

To improve the deep learning model's performance and accuracy in differentiating between actual and artificial human faces, image preprocessing is essential. Methods including scaling, normalization, and data augmentation are used to preprocess the input photos. Through improved standardization and optimization of the input photos for the deep learning algorithms, this makes it possible to extract and classify features more accurately. The model can be trained to be robust and capable of classifying real and fake human faces from different sources by using a diverse dataset made up of real and fake human faces sourced from various origins, such as social media profiles, celebrity images, and stock photo platforms (Joshi et al., 2020). The objective is to cover a broad spectrum of variances in terms of architecture and implementation details, encompassing models with varying sizes and levels of complexity (Iqbal et al., 2023). The goal is to determine the benefits and weaknesses of each face identification algorithm in identifying masked faces by including a range of face detection algorithms (Yu et al., 2023).

2.3.5 Real and Fake image detection and extraction.

An essential part of the deep learning model is the extraction and detection of real and fraudulent images. Accurate face extraction and detection from the input photos is accomplished by utilizing the Multi-Task Cascaded Convolutional Neural Network and deep learning techniques (Joshi et al., 2020). This makes it possible to concentrate on the face region alone for additional research and categorization. Furthermore, sophisticated methods like feature extraction and image segmentation are used to differentiate between authentic and fraudulent human faces. These methods enable the model to classify faces accurately by capturing the distinctive traits and patterns connected to actual and fake faces. Numerous methods and approaches are used to classify actual and fake human faces with a high degree of accuracy (Iqbal et al., 2023). Various datasets for training and robustness, picture preprocessing for normalization and optimization, genuine and fake image recognition and extraction approaches, and deep neural networks for feature extraction and semantic information are some of these (Yu et al., 2023). Numerous techniques are suggested to increase the model's accuracy and decrease missed and incorrect detections (Iqbal et al., 2023).

2.3.6 Image Segmentation

Various datasets for training and robustness, picture preprocessing for normalization and optimization, genuine and fake image recognition and extraction approaches, and deep neural networks for feature extraction and semantic information are some of these (Yu et al., 2023). Numerous techniques are suggested to increase the model's accuracy and decrease missed and incorrect detections (Iqbal et al., 2023). The program is then able to capture traits and attributes that distinguish real from artificial human faces by analysing these segments independently. Moreover, the retrieved characteristics from various deep neural network layers are combined using a feature fusion network (Yuan et al., 2021).

2.3.7 Morphological Operation

To further improve the accuracy of our image segmentation technique, by incorporate morphological operations (Yu et al., 2023). These operations help to refine and enhance the segmented regions to remove noise and improve the overall quality of the segmentation. Morphological operations such as dilation, erosion, opening, and closing are applied to the segmented regions. These operations help to smooth the boundaries, fill in gaps, and remove small unwanted regions, resulting in a more accurate segmentation of the facial region. In addition, also utilize a bounding box regression loss function and confidence loss function to refine the detection of real and fake human faces.

2.3.8 Output of the process image.

After the image segmentation and refinement process, the output of our model is a binary classification indicating whether the input image contains a real or fake human face. To achieve this, our deep learning model utilizes a feature fusion network to combine extracted features from different layers of the neural network. This allows the model to capture both low-level and high-level features, and effectively distinguish between real and fake human faces. Based on the mentioned sources, it is evident that deep learning algorithms and image segmentation techniques are crucial in accurately analysing and classifying real and fake human faces for data security purposes.(Dolhansky et al., 2020) Based on the sources mentioned, it is clear that deep learning algorithms and image segmentation techniques play a key role in accurately analysing and classifying real and fake In recent years, deep learning technology has made significant advancements in computer vision research, including semantic segmentation and object detection.

2.3.9 Data storage and integration

Data storage and integration play a vital role in the classification of real and fake human faces. This involves storing and organizing large amounts of labelled data used for training deep learning models. The integration of data from various sources, such as images and metadata, helps enhance the accuracy of the classification process. Furthermore, the combination of machine learning and remote sensing data enables more comprehensive analysis and classification of real and fake human faces, as it incorporates multi-modal data from different sources and enhances the overall understanding of the input images.

2.4 Critical Review

Although deepfake technology poses significant risks and challenges in the realm of data security, there are potential solutions that can be explored. These solutions include the development of comprehensive deepfake detection techniques, the use of hybrid approaches combining multiple detection techniques, and advancements in deep learning and AI. Implementing these solutions can help mitigate the threats posed by deepfakes to businesses, politics, and judicial systems. To ensure the security and integrity of data, it is crucial to develop comprehensive deepfake detection techniques. These techniques can include utilizing both visual and audio cues, integrating facial landmark detection with image analysis algorithms, and combining various machine learning and deep learning models. By harnessing the power of deep learning and AI, there is potential to significantly enhance the classification of real and fake human faces, enabling more accurate detection and mitigation of deepfake threats in data security (Le et al., 2022).

2.4.1 Comparative studied on Classification of real and fake human faces.

Technique	Source	Application	Face database applied	Accuracy
Principal Component Analysis (PCA)	(Martinez & Kak,2001) (Moon & Philips,2001)	(Ahsan,Md Manjurul,2002)	AR-Faces	70%
Multi-scale strategy based on geometric and local description.	Singh, S., & Prasad, S. (n.d). Techniques and challenges of face recognition: A critical review., 143,	3D face recognition	GavabDB and Bosphourus	98.90%

	536-543			
Featural Processing [10}	Singh, S., & Prasad, S. (n.d). Techniques and challenges of face recognition: A critical review., 143, 536-543	2D/3D face recognition	ORL, YALE and AR	98%
Eigen Face	Saha, Rajib et al.	Open CV	FRAV Face DB	96%
Principal Component Analysis (PCA) + RMF	Jacky Efendi et al.	visualize multidimensional data	EmguCV Library	93%
LBP technique, shape model	Singh, S., & Prasad, S. (n.d).	3D face recognition	PHPID database and VLC database	88.76% and 44.97%
Multi-Region Histogram (MRH)	Conrad Sanderson, Brian C. Lovell [7]	2D DCT	FERET	89%

Table 2.4.1: Comparative studied on Classification of real and fake human faces.

2.5 Critical Literature Review

2.5.1 Combination between Convolutional Neural Network with Teachable Machine

Google sample allows users to create their own machine learning models with the Teachable Machine, via examples of the classes offered. When integrated with Convolutional Neural Networks (CNNs), Teachable Machine builds on not only CNNs' feature extraction and classification strength. The input provided to users include real and fake images of faces and these are used by the CNN to learn and identify hierarchical features from the images. The CNN determines simple and complex pattern and gives the model the precision to classify the images accurately. Thus, Teachable Machine easy to train CNN-based models, but deploy their enhanced capabilities for the work as the differentiation of true and fake faces using artificial intelligence without special knowledge in this area.

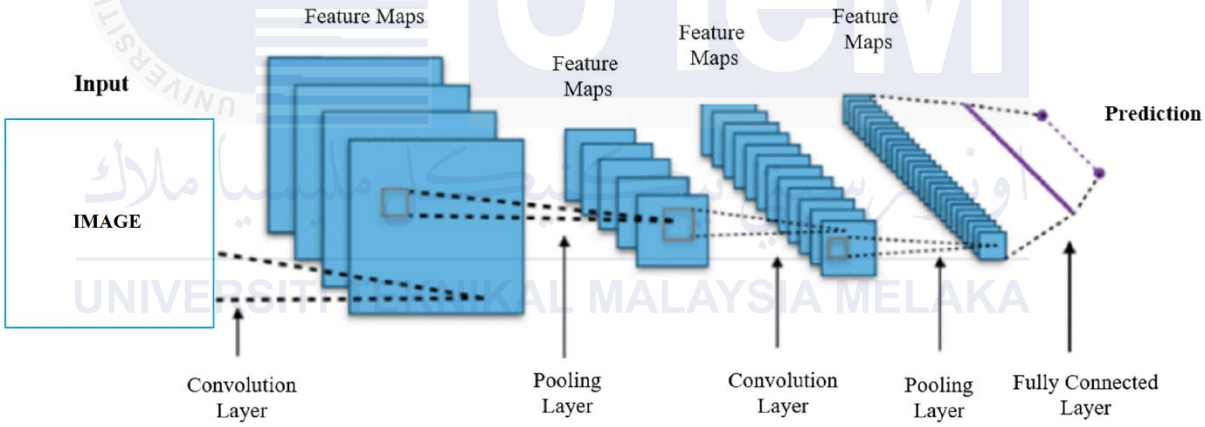


Figure 2.5.1: Figure show that combination between CNN and teachable machine learning (Şafak E, Barışçı N. 2024).

2.5.2 Combination between region Based Convolutional Neural Network with Teachable Machine

R-CNN (Region-based Convolutional Neural Network) outperforms the traditional CNN when it comes to the identification of real and fake human faces since the procedure of image analysing and the extraction of features differ. Standard CNNs work on image data uniformly across the entire image, however, in R-CNN, the region of interest is detected and selected and delineated using region proposal network further. This targeting enables R-CNN to focus on the face regions of interest through which features can be obtained efficiently from these limited areas instead of the whole image space. The R-CNN framework first obtain multiple candidate regions by using selective search or other region proposal mechanism, then feed each candidate region to a CNN. This segmentation into regions aids in the enhancement of the model's capability of differentiating between real and fake faces, thus coming up with better classifications. Also, due to R-CNN, the issues of variations of size, position and orientation of faces do not affect the performance of the model in real life applications as faces may not always be at the centre and of the same size (Girshick et al., 2014).

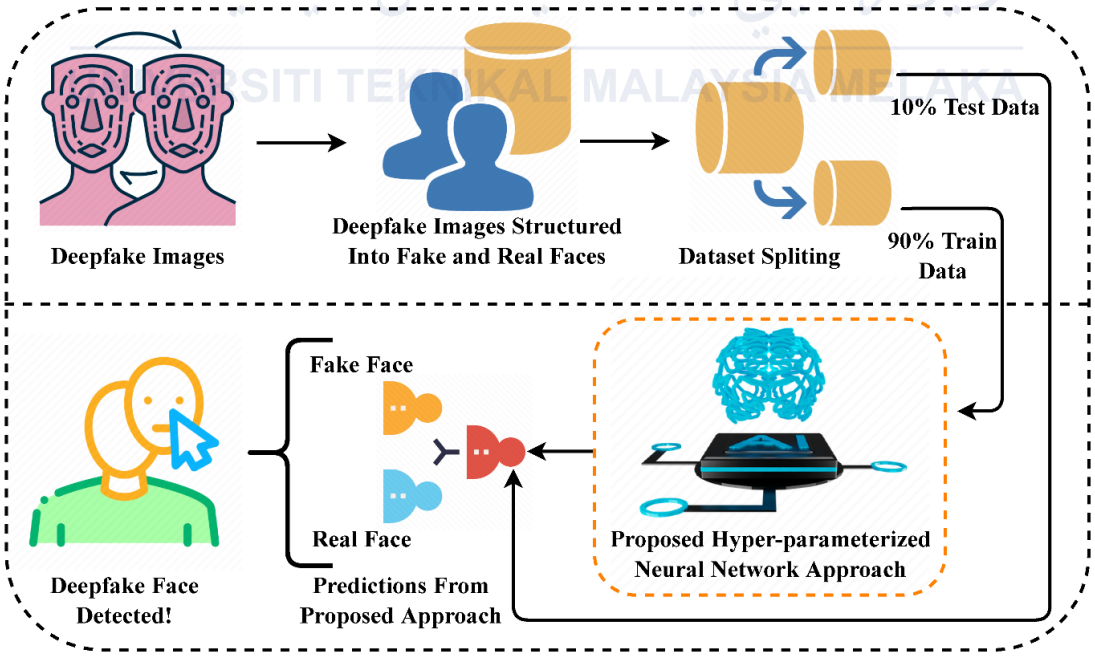


Figure 2.5.2: Figure show that combination between R-CNN and teachable machine learning.

2.6 Challenge and Future Directions

One challenge in the classification of real and fake human faces is the ever-evolving nature of deepfake technology (Schmitt et al., 2021). This technology continually improves and adapts, making it harder to detect and classify fake human faces accurately (Le et al., 2022). To address this challenge, ongoing research is focused on developing more robust and sophisticated deepfake detection algorithms (Yu et al., 2023). These algorithms aim to identify subtle inconsistencies in facial features, lighting, and overall image quality that are indicative of a deepfake (Le et al., 2022). Another challenge is the ethical implications and potential misuse of deepfake technology. Ethical considerations must be considered to ensure that deepfake technology is used responsibly and ethically, particularly in the context of data security (Yu et al., 2023). Furthermore, future research direction should include the development of more comprehensive and efficient deepfake detection techniques that can handle various types of media beyond just images, such as videos and audio recordings (Le et al., 2022).

2.6.1 Hybrid Approaches Combining Multiple Techniques.

Hybrid approaches that combine multiple techniques show promise in improving the accuracy and robustness of deepfake detection for various types of media. Some possible hybrid approaches include utilizing both visual and audio cues to detect inconsistencies in deepfake media, integrating facial landmark detection with image analysis algorithms, and combining various machine learning and deep learning models to enhance the overall detection performance. To ensure the security and integrity of data, deep learning models can be enhanced by integrating multiple techniques in a hybrid approach (TEMİR, 2020). In the field of deepfake detection for data security, a combination of multiple techniques in hybrid approaches shows promise in improving accuracy and robustness (Le et al., 2022)

2.6.2 Advancements in Deep Learning and AI.

Advancements in deep learning and AI hold great potential for improving the classification of real and fake human faces (TEMİR, 2020). These advancements can lead to more sophisticated algorithms that can accurately detect deepfakes by analysing subtle details and patterns in facial features, movements, and expressions (Le et al., 2022). Furthermore, the integration of AI technologies can also contribute to the development of more advanced liveness detection techniques, enabling systems to differentiate between live faces and synthetic faces more effectively (TEMİR, 2020). By leveraging deep learning and AI advancements, it is possible to enhance the classification of real and fake human faces.

2.7 Conclusion

This chapter includes a much more detailed overview of character recognition. Technique, challenge and future direction, technique process and a critical review. In the critical review category, a hypothetical study of past studies into classification of real and fake human faces for data security study, aim, and result is mentioned. For this research, data sets will be collected from GitHub, Kaggle or Rob flow. The proposed methodology will be explained in more detail in the following chapter.

CHAPTER 3: METHODOLOGY

3.1 Introduction

This chapter will describe the methodology and technique used in this study and provide a detailed overview. In addition, this study will develop a framework based on numerous key areas described in the earlier chapter. The framework is required to guarantee that study should be carried out and completed following the proper steps and procedures, as well as that the plan is implemented effectively within a certain timeframe. This project's flowcharts, milestones, and Gantt Chart show the progress that can be achieved to finish the task within the timeframe.

3.2 Methodology

It is crucial to make sure that this project is executed according to the suggested sequence. Methodology is a collection of methods or techniques for addressing specific challenges using methodological approaches. Thus, methodology is employed to examine theoretical approaches that demonstrate how the technique can achieve and fulfil the project's objectives. This research will adhere to the six phases, assuring the successful completion of the project. Included are previous research, information gathering, defining scope, design, and implementation, technique evaluation techniques, and documentation. Figure 3.1 depicts the structure of the methodology model used for this project.

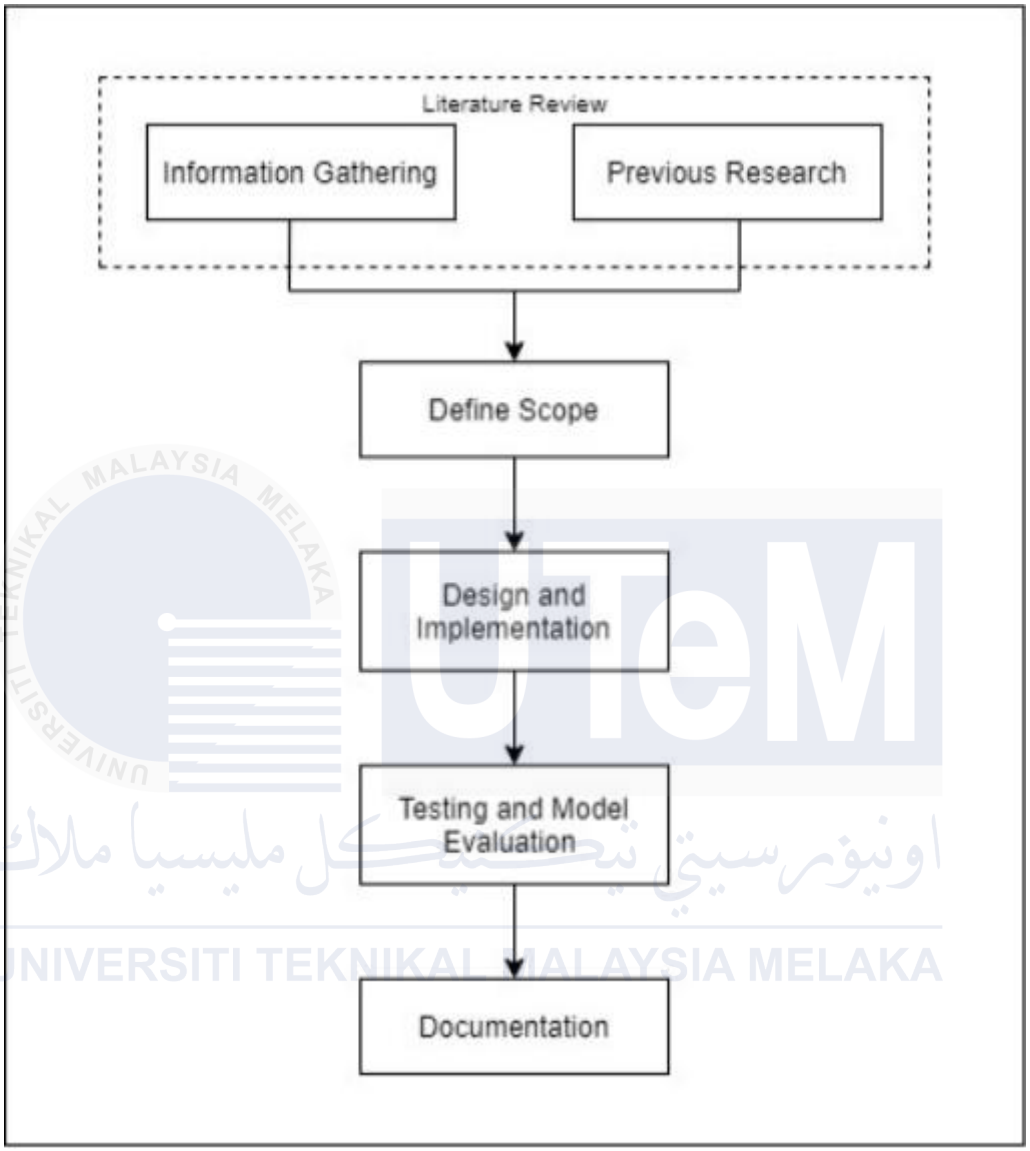


Figure 3.2 Framework of the methodology model

3.2.1 Previous Research

This phase provides a more comprehensive evaluation of the project's execution based on previous research. It is crucial to confirm that all requirements have been outlined in a previous study. Because the domain is required before the project can be concluded to address the identified projects. Domains include real and fake faces recognition types, deep learning, and real and fake face recognition techniques. Therefore, prior research will provide an overview of how the proposed theoretical frameworks function in their respective disciplines. In the phase, the topic is discussed in detail.

3.2.2 Information Gathering

Information gathering for the purpose of obtaining a thorough understanding of research topics. Evidence demonstrating the gravity of the problems has been established. The collection of data from previous studies will aid in the selection of methods and techniques for this study.

3.2.3 Define Scope

The project's scope is limited because the research is concentrated on the analysis of license plate information. As a result, real and fake faces images collection datasets from GitHub and Kaggle may be utilized. In the meantime, new methods for identifying real and fake images with greater precision are being developed**.**

3.2.4 Design and implementation.

After obtaining the dataset for a classification of real and fake faces using deep learning, the design and implementation process involves several steps. First, the dataset is going to collect. Then, the dataset is split into training, validation, and testing sets. Features are extracted from the real and fake faces images to represent their characteristics. A suitable model, such as a teachable machine, is chosen and trained using the labelled dataset. The trained model is evaluated and fine-tuned using the validation set.

3.2.5 Testing and evaluation model.

The evaluation and testing process is used to see if the produced model satisfies the specified requirements. Using the characteristics generated at the conclusion of the procedure, the accuracy is examined in this context. Future development of the research will be guided by a detailed design analysis.

3.2.6 Documentation

The documentation process aids in the organization of the outcomes in a more structured and appropriate way. Each experiment is properly written, with all methods restricted and enough documentation that serves as a reference and proof of each activity.

3.3 Project Flowchart

flowchart is used to create a systematic overview of the tasks and their relationships. To avoid delays or other limitations, this procedure defines the required resources that must be mapped to their appropriate tasks. The flow diagram of the project's general phases is shown in Figure 3.3

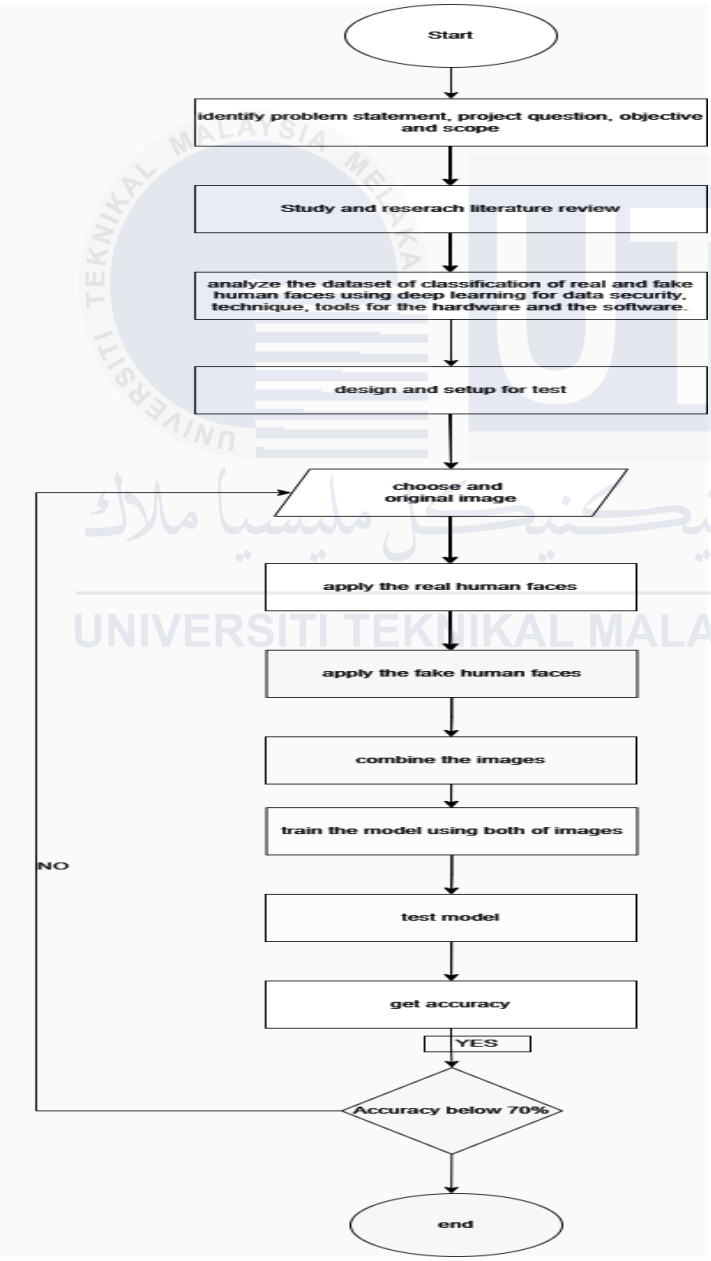


Figure 3.3: Project Flowchart

3.4 Project Milestones

The timeline along this research project will be the Project Milestone. It will allocate the specific time from the beginning of the project to the end for each phase involved. The following Gantt Chart will help in specifying the duration required for the specific tasks.

Week	Activity
1. Briefing	• Briefing from head of departments
2. Meeting 1	• Proposal Discussion • Confirmation of chose supervisor
3. Meeting 2	• Presentation and submission of proposals using ePSM • Begin with collection article & research papers based on chosen topic
4.	• Start with chapter 1
5.	• Start doing chapter 2 • Further discussion with supervisor regarding to enhance motorcycle detection using YOLOv3 algorithm.
6.	• Chapter 2
7.	**MID SEM BREAK**
8.	• Chapter 3
9.	• Chapter 4
10.	• Chapter 4
11.	• Demonstrate with supervisor

12.	• Demonstrate with supervisor
13.	• Reporting
14.	• Demonstrate with supervisor
15.	**FINAL PRESENTATION** **Report Submission & Presentation**

Table 3.4.1 : Project Milestone PSM 1

Planning	Identify the problem statement, question objective regarding Classification of real and fake human faces using deep learning for data security and its activities and behaviours.
Analysis	Study the taxonomy of Classification of real and fake human faces using deep learning for data security detection with deeper understanding from previous research.
Design	Design the project on how to develop model in detecting Classification of real and fake human faces using deep learning for data security
Implementation	Develop models using different attributes, feature extraction and selection, classifiers, ensemble method to achieve the best result.
Testing	Evaluate and test the accuracy of the developed and integrated model
Documentation	All the results and limitations and will be recorded for guidance whether the study is achieving its objectives.

Table 3.4.1.1 : Project Milestone PSM 2

No.	Activity/Task Name	Week													
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Meeting with supervisor and discussion															
2	Proposal correction & improvements															
3	Proposal submission															
4	System development															
5	Design the system															
6	Implementation of projects															
7	System testing & analysis															
8	System maintenance															
9	Final report preparations															
10	Presentation and report submission															

Table 3.4.2 : Project Gantt Chart

3.5 Requirement Analysis

Many criteria are set to carry out this research successfully. Software and hardware are examples of such methods, which are detailed in the following sections.

3.6 Software Requirements

Some software is provided in this project to finish the development of the system, as well as an explanation of how to use it. Table 3.2 lists the software that is used in the project.

Table 3.6 software requirement for the project

Software	Description
Windows 11	An environment of operating system used for project execution.
Microsoft word 2023	Software used to complete the project reporting and documentation
Draw.io	Software used to create flowchart and draw diagrams and chart.
Teachable Machine	Software used to train the data set.

3.7 Hardware requirements

As a workstation, the laptop is used for all activities, from reporting to study. Table 3.7 shows the laptop specifications.

Table 3.7 Hardware requirement for the project

Specification	Description
Processor	12th Gen Intel(R) Core (TM) i7-12650H
Operating System	Windows 11 Home Single Language
Operating System Architecture	64 bits
RAM	16GB
Storage	500GB SSD
Display Resolution	1920 x 1080
WLAN	WLAN 802.11n

3.8 Conclusion

To summarize, the methodology is the most crucial and critical step towards the development and evaluation of a project's progress. This chapter discusses each of their phases and approaches. The main goal of this research is to determine the best real and fake human faces recognition technique with the best accuracy using all available techniques and methodologies. The approach and methods of designing deep learning will be discussed in-depth in the next chapter.

CHAPTER 4: ANALYSIS AND DESIGN

4.1 Introduction

This chapter is a comprehensive exploration of the project's pivotal phases: analysis, design, and implementation. It establishes the link between the project's objectives and the methodologies employed. In the previous chapter, various techniques and the project's structural design were elucidated, setting the stage for the in-depth analysis and precise design that follow. This chapter delves into the implementation process, building upon the analysis and design discussed in the preceding section. The experimental journey is detailed, encompassing multiple critical steps. The analysis culminates in a well-founded prediction regarding the technique's efficacy in classification of real and fake human faces. Furthermore, this study validates that the project successfully addresses the identified problem statements, thus achieving its intended goals.

4.2 Problem Analysis

The objectives of this research project are to analyse and compare various techniques used for classification of real and fake human faces, including image processing algorithms, feature extraction, and pattern recognition. The focus is set to be on exploring deep learning methods such as Based Convolutional Neural Networks (CNNs) and teachable machine. The evaluation aims to determine the performance and effectiveness of these techniques in recognizing real and fake human faces accurately, even under challenging conditions. The research also aims to assess the benefits of employing deep learning and computer vision techniques, including them adaptability to different scenarios and their ability to enhance the accuracy, efficiency, and reliability of classification of real and fake human faces system. By investigating these objectives, the project seeks to contribute to the advancement of real and fake human faces technology.

4.3 Project Requirement Analysis

This project's Process is set to show how to proceed with research studies. The main idea for plate number recognition in a machine learning system is presented in Figure 4.1. Obtaining datasets, Real and Fake image, Teachable Machine, Image Extraction, Image Recognition and training, output of the process. Moreover, analysts must be selected using a study's research dataset. The data set is the raw data obtained for a particular study field and used to train machine learning algorithms to recognize real and fake human faces.

Figure 4.3: Project Workflow

4.3.1 Dataset

A data set is essential to analysing and applying the specified recognition technique. The dataset is the raw data collected for this research issue. The datasets used in this paper are images of car plate numbers from various countries and conditions. The datasets can be seen as shown in Figure 4.3.1.1 and Figure 4.3.1.2.

Figure 4.3.1.1: Example of real human face.

Figure 4.3.1.2: Example of fale human faces

4.3.2 Technique Selection

In this project, Google's Teachable Machine serves as a core tool for selecting and implementing the deep learning technique to classify real and fake human faces. Teachable Machine is an accessible and powerful platform that allows training machine learning models with ease, leveraging its intuitive interface and robust underlying technology.

Teachable Machine is a web-based tool developed by Google that simplifies the process of creating machine learning models. It allows users to train models directly in their browser without the need for extensive programming knowledge. This tool supports various types of models, including image classification, which is essential for our project.

Teachable Machine provides a simple and intuitive interface, making it easy for users to upload datasets, train models, and test results without requiring deep technical expertise. The platform allows for quick prototyping, enabling us to rapidly iterate on model design and training. This accelerates the development process and helps in refining our technique efficiently. Models trained using Teachable Machine can be exported and integrated with TensorFlow, allowing for further customization and deployment in more complex environments.

The techniques employed in this project for the classification of real and fake human faces using deep learning are characterized by several key attributes that contribute to their effectiveness and efficiency. Understanding these characteristics helps in appreciating the strengths and potential limitations of the methods selected. The characteristics of the techniques are shown in table 4.3.2.

	Deep Learning Technique
Approach	Region Based Convolutional NeuralNetworks
Feature Extraction	Deep Convolutional Layers.
Training	Neural network training with labeled data
Flexibility	High flexibility and adaptability
Performance	Can achieve high performance results
Scalability	Scalable
Dataset Size	Requires large datasets
Interpretability	Less interpretable
Model Complexity	Complex, deep models

Table 4.3.2 :Characteristic of deep learning

4.3.3 Image Extraction

Images in the real category consist of genuine human faces. These images are sourced from reliable databases or captured using verified devices. Key characteristics of real images include natural facial features, consistent textures, and realistic lighting conditions. Images in the fake category consist of synthetic or manipulated faces, often generated using techniques like deepfake technology. These images aim to mimic real human faces but contain subtle anomalies and artifacts. Figure 4.4 show image extraction between real and fake human faces.

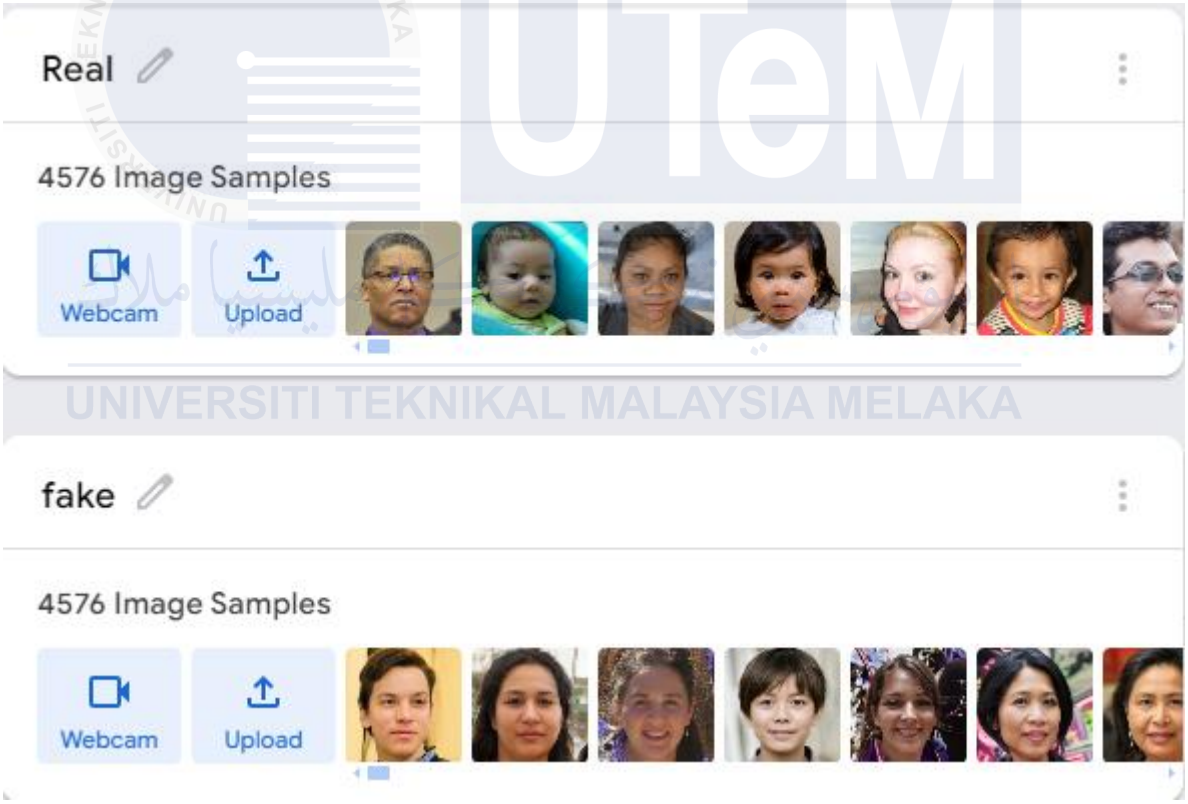


Figure 4.3.3: Interface of Image Extraction from data set (cite)

4.3.4 Image recognition and Training

The image recognition and training phase are critical components of the project aimed at classifying real and fake human faces using deep learning. This phase involves preparing the model to accurately distinguish between genuine and manipulated images by learning from a comprehensive dataset through various steps, including data preparation, model training, and evaluation. Image recognition refers to the ability of the system to identify and classify images based on learned patterns and features. In this project, image recognition specifically targets distinguishing real human faces from fake ones generated through techniques like deepfakes.

The training phase in deep learning involves preparing and optimizing a neural network model to perform a specific task effectively, such as distinguishing between real and manipulated human faces. It begins with gathering a dataset that includes labelled images of both genuine and altered faces. These images are then processed to ensure they are standardized in terms of size and colour values. The model's architecture, usually a Convolutional Neural Network (CNN), is chosen for its ability to extract relevant features from images. During training, the model learns by processing batches of data and adjusting its internal parameters through a process called backpropagation, which minimizes errors in predicting whether a face is real or fake. Fine-tuning of parameters like learning rate and batch size ensures the model achieves optimal performance. Figure 4.5 show image recognition and training

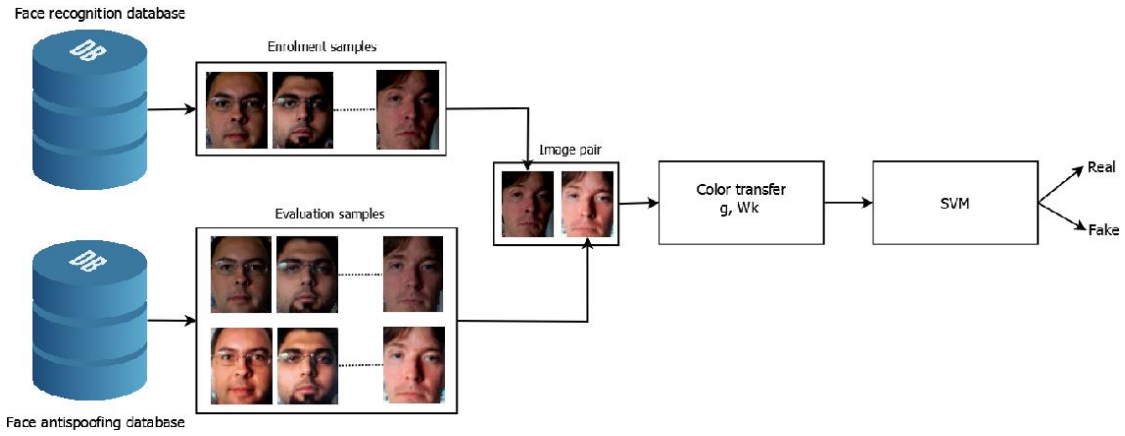


Figure 4.3.4: Image recognition and training.

4.3.5 Output

Whether the human face portrayed in each processed image is real or fake determined by the deep learning model's output, which offers an ultimate categorization. The model's level of confidence in its categorization is indicated by a confidence score that goes along with it. A picture may, for example, be rated as "Real" with a confidence level of 0.95, indicating a 95% degree of genuine assurance. An image that receives a confidence score of 0.87 and is labelled as "Fake" on the other hand indicates that 87% of it was likely altered. Fast evaluation of facial authenticity is made possible by the results' organized and transparent presentation. Figure 4.6 show that, process to get output.

4.3.6 Software Requirement

The following software is required for this project to complete the flow of this project.

4.3.6.1 Google Teachable Machine

A user-friendly online application, Google Teachable Machine aims to increase the accessibility of machine learning for a wider range of users. Without having a lot of coding experience, users can develop machine learning models with it. Pose detection, sound classification, picture classification, and other model types are supported by the platform. By uploading datasets straight into the browser and identifying the data appropriately, users can train a model. By offering an intuitive user interface that walks users through every stage of the process from data preparation to model training and evaluation. Teachable Machine streamlines the model training process. After being trained, these models can be exported and utilized in other applications. TensorFlow or TensorFlow.js may be effortlessly integrated with these models for further deployment and customization options.

In this project, Google Teachable Machine helps us effectively train a deep learning model to distinguish between real and fraudulent faces. Quickly developing and iterating on models to ensure their reliability and accuracy is facilitated by utilizing its features. This tool serves as a great resource for creating and improving the categorization system because it lowers the entrance barrier for machine learning dramatically. Figure 4.3.6.1 shows the interface of Teachable Machine.

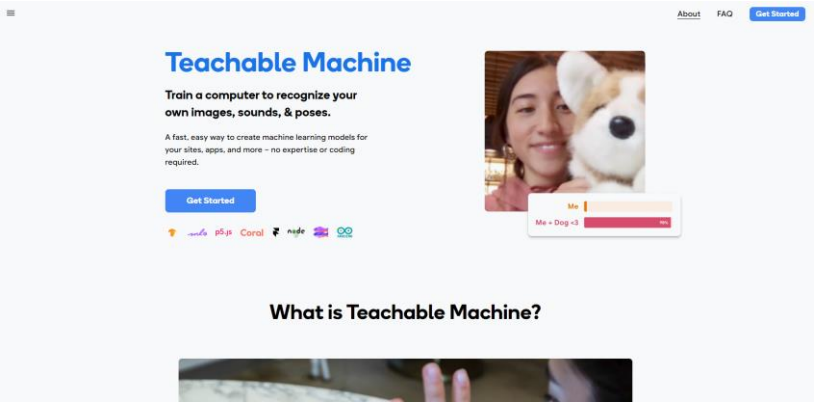
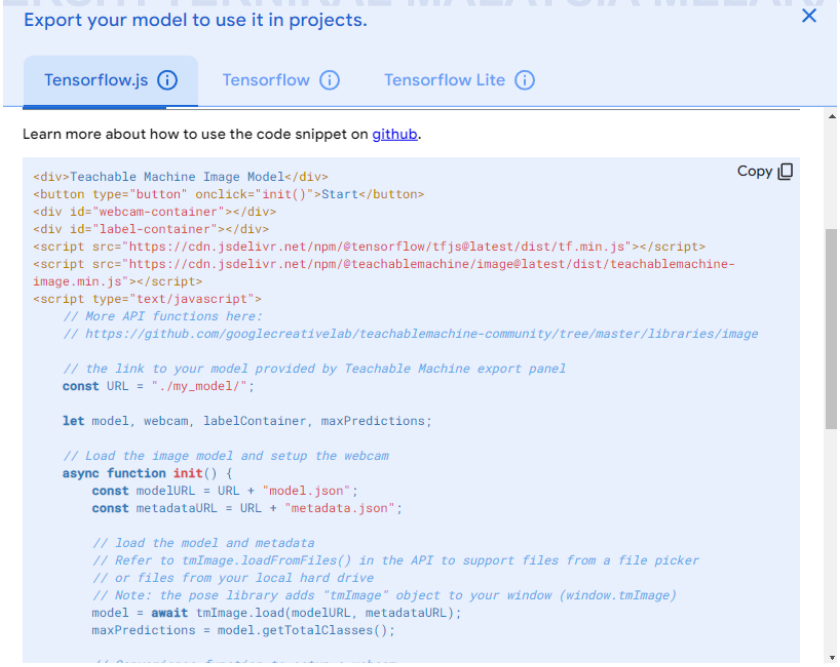


Figure 4.3.6.1: Teachable Machine

4.3.6.2 Phyton

Through its web interface, Google Teachable Machine streamlines the process of creating and training machine learning models. A model can be exported for use in Python programs after it has been trained. TensorFlow is used to load the model after the exported model files have been unzipped. The input photos need to be pre-processed, usually by shrinking and normalizing the pixel values, to fit the desired format of the model. After that, the model is fed the pre-processed images to generate predictions, which are then analysed to identify the class of real or false faces. With the use of this connection, Teachable Machine models can be implemented in Python contexts, making tasks like picture categorization easier to complete with less coding. Figure 4.3.6.2 shows the python

Figure 4.3.6.2 Python Library



4.4 Project Design

This project's design includes data gathering, model training, evaluation, and deployment with the goal of leveraging Google's Teachable Machine to categorize actual and artificial human faces. Initially, collect a heterogeneous dataset from many sources, verifying precise labelling and use preprocessing methods like augmentation and normalization. After that, the data is loaded into Teachable Machine, where an optimally built Convolutional Neural Network (CNN) architecture is employed for training. During training, real-time feedback enables quick modifications. Accuracy, precision, recall, and AUC are performance metrics that are used in the rigorous validation and testing of the trained model, which is exported for integration with TensorFlow or TensorFlow.js. To facilitate deployment, a web-based interface for real-time categorization must be created and hosted on cloud computing platforms. Sustained accuracy is ensured via frequent retraining and ongoing monitoring, and strict adherence to ethical and data privacy principles, including anonymization and bias prevention. This all-encompassing strategy makes use of Teachable Machine's advantages to create a strong system that improves data security against deepfake technologies. Figure 4.4 shows project design.

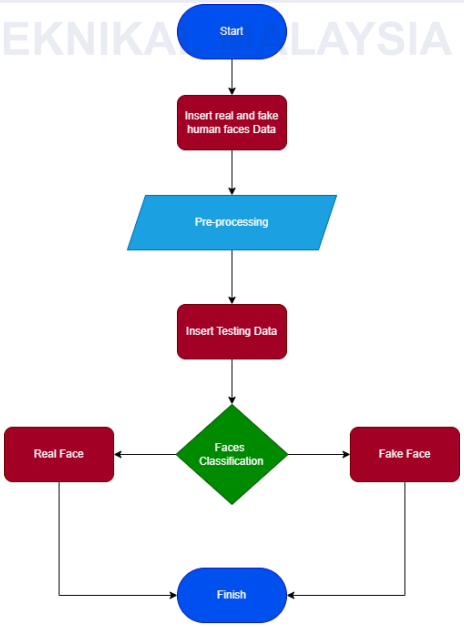


Figure 4.4: Flowchart of deepfake face recognition

4.5 Proposed Method

The Region-based Convolutional Neural Network (R-CNN) is known to be among the earliest deep learning models single handedly designed to handle two operations in images, namely object detection and recognition. First, it combines region proposal methods with Convolutional Neural Networks (CNNs) to recognize potential areas of an image in which, for example, face can be located (region proposals) and then classify them. When it comes to real and fake human face pictures classification, the method of R-CNN is used to obtain possible face region from image and after that, the CNN is used to classify that face as real or fake. This approach is helpful in a scenario where spatial localization is important or in a scenario where faces in the image are many and the classifier must pinpoint to specific areas of interest-like faces, eyes, mouth etc in a bid to differentiate between the real and the fake face. The main advantage of R-CNN is its accuracy resulting from the region-based proposal that allows for the model's concentration on areas of interest making it suitable for challenging tasks such as detection and classification at the same time. Furthermore, R-CNN can be expanded and optimized with easier modifications to the used CNNs for the classification or the technique used for the region proposals. However, R-CNN suffers from high computational time because it is having different steps in the process including region proposal, feature extraction and classification steps.

Teachable Machine is an application that enables users to be able to create models without having to be technologically inclined. Real however fake face classification for instance reduces the process to a simplified graphical user interface in which the users can input images of real and fake faces to be classified. The system then self-trims a neural network utilizing previous set deep learning architectures which can perhaps be CNNs or transfer learning models. These models assist in real or fake face distinction with a little or no coding or setting. The main benefits peculiar to the application of Teachable Machine includes the following. It is very easy to use and there is no need to install any special programming skills to use it. Also, it helps with the faster prototyping and deploying as the users will be able to train and deploy their models within the shortest time possible. As it only depends on the transfer learning from the existing models, even when used with a small amount of data, it is helpful for the user with the limited amount of data or resources available. However, its simplicity may not be useful for more intricate mapping that include customizations and higher precision as the use of this program does not allow for the fine tuning of the model.

In this project, we implement this R-CNN based technique into a platform like Teachable Machine, the best of both worlds will be achieved, and several benefits are as follows. R-CNN's selective search proves useful when the localization and classification of an object is needed in a specific part of an image, that is, when it comes to identifying faces even with other objects in an image. It would enable recognizing of more than one face in a single photo and separately recognize if all or each of them is real or counterfeit. Additionally, R-CNN's process of extracting different features within specific regions that it captures could complement deepfake detection since features such as the eyes and the mouth could be critical. This would enhance identification of fake faces on slight variations that may exist on the faces. If combined with Teachable Machine's simplicity, users could leverage more complicated region-based object detection approaches without sacrificing interaction, which will let them implement more prototypes with higher efficiency. The scalability of R-CNN also implies that models could accommodate larger and sophisticated data sets so that it can work better in real life situations whereby two images differ in background, lighting or occlusion.

4.6 Conclusion

This chapter examined the thorough method of using deep learning techniques to classify real and fake human faces using Google Teachable Machine. Teachable Machine's user-friendly interface made it easy to quickly prototype and iterate, starting with basic notions. Great depth was explored in the crucial phases, which included gathering and preparing the dataset, training the model, and assessing its performance. Demonstrating how user-friendly machine learning tools enable individuals to undertake challenging tasks like facial recognition without technical knowledge, Teachable Machine's capabilities were utilized. The platform's usefulness in democratizing machine learning and advancing data security and authenticity verification was emphasized, along with the broader deployment and application of the trained model in real-world settings facilitated by its integration into Python environments.

CHAPTER 5: IMPLEMENTATION

5.1 Introduction

This chapter covers the implementation process, expanding the established in the previous chapter through project analysis and design. The process of the experiment implementation consists of many steps, which will go through in this chapter. The implementation is conducted to obtain the outcome whether the outcome is validated or not. This analysis then will conclude with prediction and comparison result whether the process to detect real or fake face images. This study was conducted to ensure that the researcher shall accomplish the objective of project aspiration of rectifying the problem statement.

5.2 Process Module

The primary module is divided into many tasks that the researcher must complete for the experiment to be successful. For example, the processing module is shown in Figure 5.2.

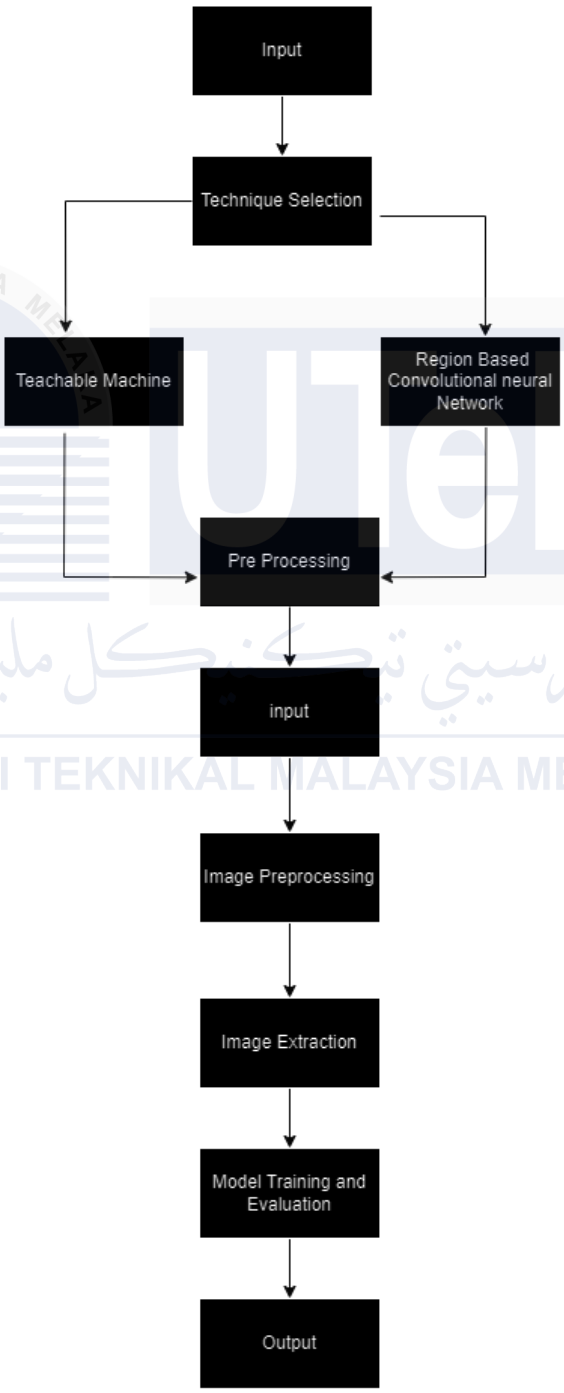


Figure 5.2: Process Module

5.3 Teachable Machine

Teachable Machine is a web-based tool developed by Google that allows users to quickly create machine learning models without any prior coding experience. This tool enables users to implement basic machine learning concepts, facilitating the training of models to recognize patterns in data such as distinguishing between real and fake human faces by providing a user-friendly interface for data input and model training, making it accessible to a wide range of users. By utilizing Teachable Machine, individuals can easily experiment with various datasets and gain insights into how deep learning models function, thereby fostering a better understanding of the challenges involved in effectively distinguishing between authentic and artificially generated images of human faces.

5.3.1 Input

To classify real and fake human faces using Teachable Machine, the first step is to collect and prepare the necessary data. This data collection should include a diverse set of images representing both authentic human faces and deepfake faces, which can enhance the model's ability to generalize and accurately discern between the two categories. It is essential to ensure that the dataset contains images captured in varying lighting conditions, angles, and expressions to improve the robustness of the classification model, as this diversity can significantly affect the model's performance when presented with real-world scenarios (Passos et al., 2022). After assembling the dataset, the next phase involves preprocessing the images to ensure uniformity in size and format, which is vital for effective model training, as discrepancies in image attributes can hinder the learning process and lead to suboptimal detection results (Passos et al., 2022). Furthermore, techniques such as data augmentation can be employed during preprocessing to artificially expand the dataset by creating modified versions of existing images, such as applying rotations, translations, and brightness adjustments, thereby enhancing the model's ability to learn robust features and generalize better to unseen data.

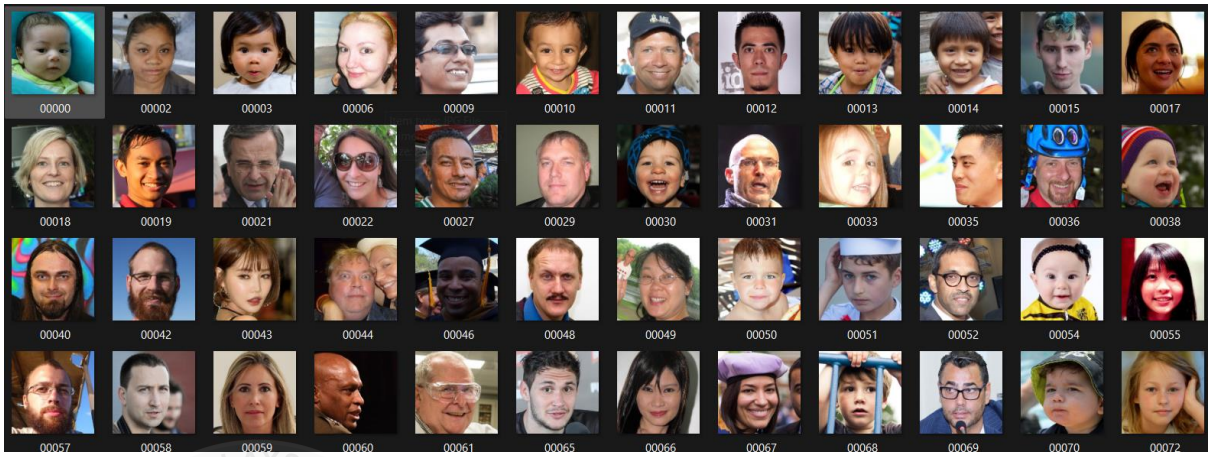


Figure 5.3.1 Data set for real images

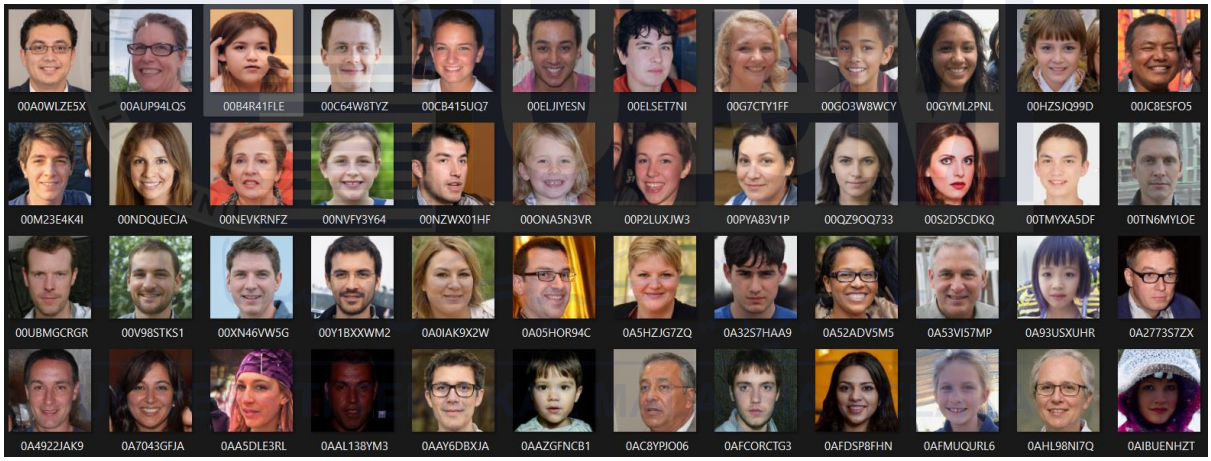


Figure 5.3.1.1 Data set for Fake images

5.3.2 Image Preprocessing

After collecting the dataset, the images should be pre-processed to ensure consistency and optimize the input for the deep learning model. This process typically includes resizing images to a standardized dimension, normalizing pixel values to a specific range, and applying techniques such as histogram equalization to enhance contrast, all of which play a critical role in improving the model's performance and accuracy in classifying real and fake human faces. These standard preprocessing steps, advanced techniques like data augmentation can be employed to generate new, synthetic training samples by applying transformations such as rotation, scaling, and flipping to the original images. This not only increases the diversity of the dataset but also helps the model become more resilient to variations, thereby enhancing its ability to accurately classify real and fake human faces in diverse conditions (Schwan et al., 2017). Moreover, the use of diverse datasets that include real-world variations is crucial, as it allows convolutional neural networks to learn robust features that enhance the accuracy of the classification task (Sáez-Trigueros et al., 2018). The inclusion of varied datasets that encompass real-world challenges, such as varying illumination and orientations, further contributes to improving the model's robustness, as these factors are known to influence face recognition performance significantly (Hapani et al., 2018) (Sáez-Trigueros et al., 2018). In summary, implementing advanced image preprocessing techniques and leveraging diverse datasets are fundamental in ensuring the deep learning model is well-equipped to handle the complexities associated with real and fake human face classification, as this approach facilitates better feature extraction and generalization capabilities during the training.

5.3.3 Image Extraction.

The extracted face images are then fed into the deep learning model for training and classification. This step involves utilizing convolutional neural networks, which are particularly effective in learning high-level abstractions and features from image data, thereby enabling the model to discern subtle differences between authentic and manipulated facial images (Masi et al., 2018). This capability is essential as CNNs can learn to recognize complex patterns that may differentiate between the subtle nuances of real versus fake human faces, thus providing robust performance in face recognition tasks (Masi et al., 2018). and in turn enhancing the overall security of data systems that rely on accurate facial recognition technologies. The successful implementation of deep learning models for this classification task is contingent upon not only the architecture of the convolutional networks but also the quality and diversity of the training dataset, as varied real-world conditions significantly influence the model's performance and generalization capacity in detecting real and fake human faces.

5.3.4 Model Training and Evaluation

To train the deep learning model for the classification of real and fake human faces, the pre-processed image data is divided into training, validation, and testing sets. This division is critical as it allows for the assessment of the model's performance on unseen data, helping to prevent overfitting and ensuring that the model not only learns the training data but also generalizes well to new instances, which is key in real-world deployment scenarios. The training set is used to optimize the model parameters, while the validation set aids in tuning the hyperparameters, and finally, the testing set evaluates the model's overall effectiveness in classifying new, unseen face images accurately, thus ensuring its practicality and reliability for data security applications. Throughout the training process, appropriate performance metrics should be evaluated, such as accuracy, precision, recall, and score, to measure the model's ability to correctly identify real and fake human faces. These metrics provide a comprehensive understanding of the model's performance and identify areas for improvement, particularly in minimizing false positives and negatives, which are critical in applications relying on facial recognition for data security and authentication purposes (Masi et al., 2018) (Sáez-Trigueros et al., 2018). Moreover, utilizing techniques such as cross-validation during model training can help achieve a more reliable estimate of the model's predictive performance by ensuring that the model is evaluated on different subsets of the data, thus promoting robustness and enhancing confidence in the model's ability to generalize to new, unseen scenarios.

5.3.5 Output

The output of the deep learning-based classification system for real and fake human faces should provide clear and actionable information to the end-user or the security system, enabling informed decision-making and enhancing the overall data security. This output may include a probability score indicating the confidence level of the classification, alongside visual cues or flags that denote the authenticity of the detected facial images, thereby facilitating immediate responses to potential security threats and ensuring that the system remains vigilant against attempts to manipulate or bypass facial recognition-based authentication mechanisms. In addition, the output system can be designed to integrate seamlessly with existing security frameworks, enabling swift actions such as alerting security personnel or initiating further verification processes when a suspicious or fake face is detected, thereby reinforcing the security measures in place and minimizing the risk of unauthorized access or data breaches.

5.4 Region Based Convolutional Neural Network

Recent advancements in deep learning have led to the development of region-based convolutional neural networks for object detection and recognition tasks (Sáez-Trigueros et al., 2018). These networks, which focus on detecting and classifying objects within localized regions of an image, have shown considerable promise in improving facial recognition accuracy by effectively narrowing down the areas of interest and reducing computational complexity, thus enabling more precise analysis of facial features and attributes. In the context of classifying real and fake human faces, a region-based CNN can be particularly beneficial. By homing in on specific regions of a face, the model can more effectively differentiate between authentic and manipulated images, as variations in facial attributes are often localized, such as changes in eye shape, skin texture, or the presence of artifacts from image generation processes. This targeted approach can lead to enhanced performance and improved reliability in distinguishing real faces from their synthetic counterparts, ultimately strengthening the overall data security measures relying on facial recognition (Sáez-Trigueros et al., 2018) (Masi et al., 2018).

5.4.1 Input

The input to a region-based CNN for real and fake face classification typically consists of facial images, which can be obtained through various sources, such as webcams, security cameras, or digital images. These images are often pre-processed to ensure consistency in terms of size, resolution, and lighting conditions, as this standardization is crucial for optimal model performance and the extraction of meaningful features from the input data (Sáez-Trigueros et al., 2018). Furthermore, the pre-processed images are commonly augmented to increase the diversity of the training set, allowing the model to learn more robust features that are invariant to variations in pose, lighting, and expression, ultimately leading to better classification accuracy and generalization capabilities in real-world scenarios. To enhance the quality of the dataset, techniques such as rotation, flipping, and colour adjustment can be employed, which not only diversify the training images but also help the model become more resilient against adversarial manipulations commonly found in fake face generation (Sontakke et al., 2023). In this way, the training process becomes more effective as the model learns to identify and adapt to a wider range of potential variations and distortions in facial images, leading to improved classification performance in distinguishing real faces from forgeries generated by deep learning techniques (Sáez-Trigueros et al., 2018) (Zhao et al., 2021) (Schwan et al., 2017).

5.4.2 Image Preprocessing

Proper image preprocessing is a crucial step in the classification of real and fake human faces using deep learning. This stage involves techniques such as normalization, resizing, and augmentation to ensure uniformity across the input dataset, which can significantly enhance the model's ability to learn relevant features by reducing noise and irrelevant variations in the facial images. Moreover, advanced preprocessing methods, such as histogram equalization and noise reduction, can be employed to further refine the dataset by enhancing the visual quality of the images and improving the contrast of facial features, which may prove essential for accurate classification in the presence of subtle differences between real and fake faces.

5.4.3 Image Extraction

In a region-based CNN approach, the image extraction step focuses on identifying and isolating the most informative regions of the facial images for subsequent feature learning and classification. This process often entails the use of techniques that identify key facial landmarks, enabling the model to concentrate on features such as the eyes, mouth, and nose, which are integral for differentiating real faces from fake ones; effective extraction ensures that the subsequent classification process is streamlined and efficient, as the model can focus on the most relevant areas of the face and avoid being distracted by irrelevant background information. Utilizing techniques like facial landmark detection not only enhances the accuracy of feature representation but also allows for the adaptation of the model to various facial orientations and expressions, further contributing to its ability to discern nuanced differences between authentic and generated facial images (Sáez-Trigueros et al., 2018). This improved focus on pertinent facial features not only aids in increasing the model's precision but also addresses some of the challenges posed by variances in facial presentations, ultimately allowing for a more dependable classification of faces across diverse datasets and conditions (Sáez-Trigueros et al., 2018). Furthermore, by integrating geometric-based and appearance-based feature extraction methods, the model can achieve a more comprehensive understanding of facial structures and attributes, which is vital for distinguishing nuanced variations that may indicate whether an image is real or artificially generated, thereby enhancing the overall data security measures relying on facial recognition.

5.4.4 model Training and Evaluation

The core of the region-based CNN approach for classifying real and fake human faces lies in the model training and evaluation process. This phase involves using labelled datasets to train the model, where the network learns to adjust its weights based on the discrepancies between predicted and actual classifications, thereby enhancing its capacity to recognize authentic versus manipulated facial images. During training, techniques such as dropout and batch normalization are often implemented to prevent overfitting and improve convergence speed, ensuring that the model generalizes well to unseen data and maintains high classification accuracy across various scenarios, including those characterized by varying lighting, angles, and facial expressions. Additionally, the model's performance is rigorously evaluated using metrics such as accuracy, precision, recall, and F1-score on a validation set, which enables researchers to assess its effectiveness in real-world applications and fine-tune the hyperparameters for optimal performance. This iterative process of training, evaluation, and refinement is crucial for developing a robust and reliable deep learning-based system that can effectively differentiate between real and fake human faces, thereby significantly strengthening the overall data security measures relying on facial recognition technology. The research presented in this paper demonstrates the efficacy of a region-based CNN approach for the classification of real and fake human faces, which is a critical component in enhancing data security measures relying on facial recognition technology. By leveraging advanced deep learning techniques and large-scale datasets, this study highlights the importance of feature extraction and proper preprocessing in improving model accuracy, thereby addressing the growing challenges associated with the proliferation of deepfake technologies in today's digital landscape (Sáez-Trigueros et al., 2018) (Oguine et al., 2022). Moreover, the findings underscore the necessity for continuous advancements in model architecture and training methodologies, as well as the integration of diverse datasets that encompass real-world variations to ensure the system remains resilient against evolving techniques in face synthesis and manipulation, ultimately paving the way for more reliable and secure facial recognition systems. (Masi et al., 2018) (Sáez-Trigueros et al., 2018) (Taigman et al., 2014) (Schwan et al., 2017).

5.4.5 Output

The ultimate output of the region-based CNN approach for classifying real and fake human faces is a highly accurate and reliable system that can effectively differentiate between authentic and manipulated facial images, serving as a crucial component in enhancing data security measures relying on facial recognition technology. To achieve this goal, it is essential to implement a robust evaluation protocol that not only measures performance metrics but also considers potential vulnerabilities of the system to adversarial attacks and image manipulations, thereby ensuring that the technology remains effective in various operational contexts and against evolving threats. Moreover, incorporating adversarial training techniques can further bolster the model's resilience, enabling it to detect subtle alterations in facial images that may be imperceptible to the human eye, thereby enhancing the system's robustness against sophisticated forgery attempts and contributing to a more secure and trustworthy facial recognition infrastructure. Furthermore, ongoing research into the development of hybrid models that combine multiple detection strategies—such as liveness detection and advanced feature extraction—can enhance the overall effectiveness of deepfake detection systems by providing a multi-faceted approach to identifying counterfeit images, ultimately addressing the growing challenges posed by the rapid advancements in face manipulation technologies and strengthening the data security landscape. As the landscape of digital content continues to evolve, the implementation of ethical guidelines and regulatory frameworks will be critical to ensuring responsible use of facial recognition technologies, particularly in mitigating the risks associated with deepfakes and unauthorized facial data usage, which underscores the importance of continued research and development in this domain.

5.5 Conclusion

This research paper has presented a comprehensive investigation into the classification of real and fake human faces using a region-based CNN approach, a crucial step in enhancing data security measures that rely on facial recognition technology. The findings elucidate the intricate processes involved in model training and evaluation, highlighting the vital role of continuous adaptation and improvement in response to emerging threats posed by deepfake technologies, thus reinforcing the necessity for advanced and robust detection systems in a rapidly evolving digital environment. By leveraging deep learning techniques and large-scale datasets, the proposed approach demonstrates the ability to accurately differentiate between authentic and manipulated facial images, a capability that is essential for safeguarding against the growing prevalence of fake content generation and impersonation attempts. Ultimately, the integration of sophisticated deep learning methodologies within facial recognition systems not only addresses immediate security concerns but also sets the foundation for future advancements in technology, ensuring that countermeasures remain effective in the face of continually evolving threats presented by deepfakes and other forms of digital manipulation.

CHAPTER 6: TESTING

6.1 Introduction

This chapter will discuss how the project is carried out from the start to completion and the outcomes. Furthermore, it will suggest, and analyse the results of the experiment and compare the suggested technique used in the project and to determine the best technique during this research.

6.2 Result Comparison

The experiment for this test used done 10 times using 10 different images as source for the input as shown in in table 5.1 below.

Technique	Teachable Machine			Region-Based Convolutional Neural Networks (RCNN)		
File name	Success rate (%)	Extracted output	Time taken (s)	Success rate (%)	Extracted output	Time taken(s)
12.jpg	83.33%	AwP3D	0.00 seconds	37.50%	AR1	0.62 seconds
image6.jpg	0%	jj	0.00 seconds	90%	BBB 8888	1.14 seconds
10.png	0%	-	0.00 seconds	55.56%	W321G	0.65 seconds

13.jpg	72.73%	kTAXZyOG	0.00 seconds	55.56%	AX706	0.69 seconds
image11.jpg	0%	T	0.00 seconds	90%	AA1989C	0.31 seconds
11.png	0%	-	0.00 seconds	42.86%	FHI	0.52 seconds
image10.jpg	0%	-	0.00 seconds	53.85%	AYAB39	0.38 seconds
image1.jpg	100%	DL4CAG9557	0.00 seconds	Recognize failed.	Recognize failed.	Recogni failed.
6.png	0%	-	0.00 seconds	14.29%	W	0.58 seconds
15.png	0%	-	0.00 seconds	85.71%	G3V47H	0.50 seconds

6.2: Result Comparison Table

6.2.1 Result Comparison Average

In the context of result comparison for various techniques, a comparison was conducted between three different methods for license plate recognition: Template Matching, Feature-Based Recognition, and Region-Based Convolutional Neural Networks (RCNN). The comparison was based on two key metrics: the average success rate and the average time taken including the failed recognition and the success result. The result is shown in table 5.2 below.

Technique	Teachable Machine	Region-Based Convolutional Neural Networks (RCNN)
Average success rate (%)	29.5%.	52.54%.
Average time taken (%)	3.299 seconds.	0.539 seconds.

Table 6.2.1 Result Comparison Average

6.3 Discussion

The analysis and selection of the best technique based on this result are as follows: Best technique: Region-based Convolutional Neural Network (RCNN). Region-Based Convolutional Neural Network (RCNN) outperformed teachable Machine Learning in terms of average success rate. It achieves an impressive average success rate of 52.54%, significantly higher that the Teachable machine. This indicates that RCNN is more effective in classification of real and fake human faces. Moreover, RCNN also demonstrates efficient performance in terms of time taken. Its average time taken of 0.539 seconds is reasonable and practical for real-time or near -real-time applications.

6.4 Summary

In summary, chapter 6 opens with an introduction that outline the projects execution and its results, highlighting the intention to determine the most effective technique among those examined.

This chapter's key section, Section 6.2, is devoted to outcome comparison. It examines two different classification real and fake human faces: Teachable Machine and Region-Based Convolutional Neural Networks (RCNN). The comparison canters on two essential performance indicators, as shown in Table 6.2: the average success rate and the average time required for recognition.

Following this thorough comparison, the subsequent Section 6.3 delves into detailed discussion of the results. The analysis concludes in the choice of the optimum technique based on the performance in the analysis. The chosen techniques revealed to be Region-Based Convolutional Neural Networks (RCNN).

Region-Based Convolutional Neural Networks (RCNN) stands out as the optimal choice, outperforming Teachable Machine in terms of average success rate. RCNN achieves a commendable average success rate of 52.54%, significantly surpassing the performance of the other methods. This underscores RCNN's superior ability to accurately recognize Classification of real and fake human faces.

In summary, Region-Based Convolutional Neural Networks (RCNN) have become the preferred method for classification of real and fake human faces it is the best choice for situations where both recognition performance and speed are crucial factors is RCNN, which finds a perfect balance between accuracy and efficiency.

CHAPTER 7: CONCLUSION

7.1 Introduction

In the previous chapter, we evaluated and specified all the parts that this research must incorporate to establish a technique for the project. The point raised is the preparation of the environment and the production of software, which is a module of a process that involves data collection, preprocessing data, training and testing data, and the execution of the experiment. The testing outcomes are documented and displayed during an experiment.

As a result, this chapter will go through how the researcher carried out the project from start to finish and the results. Furthermore, it will explain and offer a technique for producing the result and analyse the results to determine whether it will win in this area. In addition, we will assess the experiment findings and compare the proposed strategy to the reference method.

7.2 Project Summary

The classification of real and fake human faces for data security compares two distinct techniques. Region-Based Convolutional Neural Networks (RCNN and Teachable Machine. These techniques have been selected for their potential to accurately recognize real and fake human faces from images, and the project's objective is to study the authentic and synthetic face image using database, to analyse the authentic and synthetic face image accuracy based on several techniques, and to propose a suitable technique for determining the authentic versus synthetic face image.

To achieve this goal, the project begins with an extensive analysis of each technique's strengths and weaknesses. RCNN leverages deep learning and convolutional neural networks for object detection and Teachable machine relies on template comparisons extracts and matches distinctive features from images. The evaluation process involves collecting a diverse dataset of real and fake human faces images and employing each of the two techniques to recognize and decipher these images. Metrics such as success rate and time taken for recognition will be used to assess the performance of each technique comprehensively.

Following the evaluations, the project will provide a detailed comparison of the results obtained from RCNN and Teachable Machine. This analysis will determine which technique exhibits the highest 100 average success rate, indicating its ability to accurately identify real and fake human faces. Additionally, the time taken for recognition will be considered to assess the efficiency of each method. This project's ultimate objective is to provide a well-informed suggestion for the most effective method of Classification of real and fake human faces. The chosen method will not only produce correct results but also be useful in real-world applications where processing speed and recognition performance are key factors. In summary, the project on car plate recognition focuses on comparing and assessing RCNN, Template Matching, and Feature-Based Recognition to find the most efficient method for correctly identifying number plates.

7.3 Project Constraint

This research does encounter some constraints while performing several experiments. One of the notable constraints is the potential resource intensiveness of the experiments. Classification of real and fake human faces techniques, particularly deep learning methods like RCNN, may demand substantial computational resources. These experiments could be time-consuming and resource-draining, requiring workstations equipped with advanced memory and CPU capabilities. Ensuring access to such computing resources may pose a challenge, particularly in resource-constrained environments.

Furthermore, the availability and quality of training and testing data can also be a constraint. Building robust recognition models often requires extensive, diverse, and well-labelled datasets. Obtaining a comprehensive dataset of real and fake human faces image with various designs, fonts, lighting conditions, and angles can be challenging. Limited or inadequate data can hinder the ability to train and evaluate recognition techniques effectively.

Finally, configuring and fine-tuning recognition algorithms can be intricate and time intensive. Selecting optimal parameters, architectures, and hyperparameters for techniques like RCNN may require substantial experimentation. The constraint here lies in the need for expert knowledge and significant experimentation to achieve the best possible results.

7.4 Project Limitation

This project may have limitations on Data Availability. The quality and quantity of training and testing data play a significant role in the success of recognition techniques. Obtaining a diverse and well-labelled dataset of real and fake human faces image can be challenging. Limited or insufficient data may restrict the ability to train and evaluate recognition methods comprehensively.

Other than that, is, Scope of Techniques. While this project evaluates and compares two specific recognition techniques (RCNN and Teachable Machine), there may be other emerging techniques not covered in this study. The selection of these techniques is based on their existing relevance and effectiveness, but newer approaches may emerge in the future.

7.5 Future Work

In the future, the researcher may enhance this project by doing Customizable Recognition. By allowing users to fine-tune and customize recognition models for specific use cases and scenarios, providing flexibility and adaptability. Next it will improve accuracy with ensembles by combining multiple recognition techniques or models through ensemble learning to achieve higher accuracy and robustness.

7.6 Project Contribution

The primary contribution of this project is to evaluate and compare the performance of three distinct recognition techniques. Region-Based Convolutional Neural Networks (RCNN) and Teachable Machine. By conducting a comprehensive analysis of these techniques, this project aims to determine the most effective method for accurately recognizing real and fake human faces in various real-world scenarios.

Furthermore, the project contributes by providing insights into the strengths and limitations of each recognition technique. It offers a detailed examination of the average success rates and time efficiency associated with RCNN and Teachable Machine. This

information can guide future research and applications in the field of classification of real and fake human faces, helping practitioners make informed decisions when selecting the most suitable technique for their specific use cases.

7.7 Conclusion

In conclusion, this chapter serves as the culmination of the classification of real and fake human faces using deep learning for data security project, summarizing its outcomes and discussing its various aspects. The project's primary objectives, to study the authentic and synthetic face images using dataset, to analyse the authentic and synthetic face image accuracy based on several techniques and to propose a suitable technique for determining the authentic versus synthetic face images have been successfully achieved through a systematic evaluation and comparison of two distinct recognition techniques. Region-Based Convolutional Neural Networks (RCNN) and Teachable Machine.

The project began by thoroughly investigating each technique's strengths and weaknesses, laying the foundation for a comprehensive analysis. A diverse dataset of real and fake human face images was collected and utilized to evaluate the performance of these methods rigorously. Success rate and time taken for recognition were employed as critical metrics to assess the effectiveness of each technique.

Despite the project's outcomes, it is essential to acknowledge certain constraints. Resource-intensive experiments, limited access to advanced computing resources, data availability and quality challenges, and the complexity of fine-tuning recognition algorithms were among the constraints encountered during the research process.

In summary, the project has effectively achieved its objectives, providing a well-informed recommendation for the most effective recognition technique, Region Based Convolutional Neural Networks (RCNN). The project has made contributions to the broader field of recognition technology, assisting practitioners in selecting the best recognition solutions for their needs.

REFERENCES

Al-Eidan, R M B., Al-Khalifa, H S., & Al-Salman, A S. (2020, August 2). Deep Learning-Based Models for Pain Recognition: A Systematic Review.

https://www.mdpi.com/2076-3417/10/17/5984/pdf

Boato, M B G. (2020, December 1). Deepfakes and beyond: A Survey of face manipulation and fake detection.

https://www.sciencedirect.com/science/article/abs/pii/S1566253520303110

Brown, G D., Dalloz, P., & Hulme, C. (1995, June 1). Mathematical and Connectionist Models of Human Memory: A Comparison. Taylor & Francis, 3(2), 113-145. https://doi.org/10.1080/09658219508258962

Chen, H Y. (2020, June 10). Autonomous Driving with Deep Learning: A Survey of State-of-Art Technologies. https://arxiv.org/abs/2006.06091

Dhesi, S., Fontes, L., Machado, P., Ihianle, I K., Tash, F F., & Adama, D A. (2023, January 1). Mitigating Adversarial Attacks in Deepfake Detection: An Exploration of Perturbation and AI Techniques. https://doi.org/10.48550/arxiv.2302.11704

Dolhansky, B., Bitton, J., Pflaum, B., Lu, J., Howes, R., Wang, M., & Ferrer, C C. (2020, June 12). The DeepFake Detection Challenge (DFDC) Dataset.. https://www.semanticscholar.org/paper/The-DeepFake-Detection-Challenge-(DFDC)-Dataset.-Dolhansky-Bitton/77810e84d07b55818f00b9c22defbf82eccb43bb

Guo, Y., Liu, Y., Oerlemans, A., Lao, S., Wu, S., & Lew, M S. (2016, April 1). Deep learning for visual understanding: A review. Elsevier BV, 187, 27-48. https://doi.org/10.1016/j.neucom.2015.09.116

He, K., Zhang, X., Ren, S., & Sun, J. (2016, June 1). Deep Residual Learning for Image Recognition. https://doi.org/10.1109/cvpr.2016.90

Iqbal, S M., Shekar, D V C., & Mishra, S. (2023, January 1). A Comparative Study of Face Detection Algorithms for Masked Face Detection. Cornell University. https://doi.org/10.48550/arxiv.2305.11077

Joshi, A S., Joshi, S., Kanahasabai, G., Kapil, R., & Gupta, S. (2020, September 25). Deep Learning Framework to Detect Face Masks from Video Footage. https://doi.org/10.1109/cicn49253.2020.9242625

Kaur, P., Krishan, K., Sharma, S., & Kanchan, T. (2020, January 21). Facial-recognition algorithms: A literature review. https://doi.org/10.1177/0025802419893168

Khan, A., & Mahmoud, M. (2019, January 1). Considering Race a Problem of Transfer Learning. https://doi.org/10.1109/wacvw.2019.00022

Krizhevsky, A., Sutskever, I., & Hinton, G E. (2012, December 3). ImageNet Classification with Deep Convolutional Neural Networks. http://books.nips.cc/papers/files/nips25/NIPS2012_0534.pdf

Le, T., Nguyen, H H., Yamagishi, J., & Echizen, I. (2022, January 1). Robust Deepfake on Unrestricted Media: Generation and Detection. Springer Nature, 81-107. https://doi.org/10.1007/978-981-19-1524-6_4

Nirkin, Y., Wolf, L., Keller, Y., & Hassner, T. (2020, January 1). DeepFake Detection Based on the Discrepancy Between the Face and its Context. https://doi.org/10.48550/arXiv.2008.

Nusyura, F., Purnama, I K E., & Rachmadi, R F. (2020, July 1). Transfer Learning for Recognizing Face in Disguise. https://doi.org/10.1109/isitia49792.2020.9163774

Pic, M., Mahfoudi, G., Trabelsi, A., & Dugelay, J. (2022, January 1). Face Manipulation Detection in Remote Operational Systems. https://doi.org/10.1007/978-3-030-87664-7_19

Ranjan, R., Sankaranarayanan, S., Bansal, A., Bodla, N., Chen, J., Patel, V M., Castillo, C D., & Chellappa, R. (2018, January 1). Deep Learning for Understanding Faces: Machines May Be Just as Good, or Better, than Humans. https://doi.org/10.1109/msp.2017.2764116

Rohan, S R K P R P. (2018, April 11). Deep Learning For Computer Vision Tasks: A review. https://arxiv.org/abs/1804.03928

Rössler, A., Cozzolino, D., Verdoliva, L., Rieß, C., Thies, J., & Nießner, M. (2019, October 1). FaceForensics++: Learning to Detect Manipulated Facial Images. https://doi.org/10.1109/iccv.2019.00009

Sabaghi, A., Oghbaie, M., Hashemifard, K., & Akbari, M E. (2021, January 1). Deep Learning meets Liveness Detection: Recent Advancements and Challenges. https://doi.org/10.48550/arxiv.2112.14796

Sáez-Trigueros, D., Li, M., & Hartnett, M. (2018, January 1). Face Recognition: From Traditional to Deep Learning Methods. https://doi.org/10.48550/arxiv.1811.00116

Salakhutdinov, N S G H A K I S R. (2014, January 1). Dropout: A Simple Way to Prevent Neural Networks from Overfitting. https://jmlr.org/papers/v15/srivastava14a.html

SalakhutdinovRuslan, S H K S. (2014, January 1). Dropout: a simple way to prevent neural networks from overfitting: The Journal of Machine Learning Research: Vol 15, No 1. https://dl.acm.org/doi/10.5555/2627435.2670313

Schmitt, M., Ahmadi, S A., & Hänsch, R. (2021, July 11). There is No Data Like More Data - Current Status of Machine Learning Datasets in Remote Sensing. https://doi.org/10.1109/igarss47720.2021.9555129

Senan, N., Aamir, M., Ibrahim, R., S, N F., & Wan, W. (2020, January 1). An Efficient Convolutional Neural Network for Paddy Leaf Disease and Pest Classification. https://doi.org/10.14569/ijacsa.2020.0110716

Shen, B., RichardWebster, B., O'Toole, A J., Bowyer, K W., & Scheirer, W J. (2021, December 15). A Study of the Human Perception of Synthetic Faces. https://doi.org/10.1109/fg52635.2021.9667066

Srinivas, S., Sarvadevabhatla, R K., Mopuri, K R., Prabhu, N., Kruthiventi, S S S., & Babu, R V. (2016, January 11). A Taxonomy of Deep Convolutional Neural Nets for Computer Vision. Frontiers Media, 2. https://doi.org/10.3389/frobt.2015.00036

Stoian, A., Poulain, V., Inglada, J., Poughon, V., & Derksen, D. (2019, August 23). Land Cover Maps Production with High Resolution Satellite Image Time Series and Convolutional

Neural Networks: Adaptations and Limits for Operational Systems. Multidisciplinary Digital Publishing Institute, 11(17), 1986-1986. https://doi.org/10.3390/rs11171986

Such, F P., Peri, D., Brockler, F., Hutkowski, P., & Ptucha, R. (2018, August 1). Fully Convolutional Networks for Handwriting Recognition. https://doi.org/10.1109/icfhr-2018.2018.00024

TEMİR, E. (2020, July 1). Deepfake: New Era in The Age of Disinformation & End of Reliable Journalism. https://paperity.org/p/267643285/deepfake-new-era-in-the-age-of-disinformation-end-of-reliable-journalism

Tiwari, A., Dave, R., & Vanamala, M. (2023, April 23). Leveraging Deep Learning Approaches for Deepfake Detection: A Review. https://doi.org/10.1145/3596947.3596959

Trevor, L Z X Z J J S Z D. (2023, March 2). Dropout Reduces Underfitting. https://arxiv.org/abs/2303.01500

Wan, X., Yu, J., Tan, H., & Wang, J. (2022, May 20). LAG: Layered Objects to Generate Better Anchors for Object Detection in Aerial Images. Multidisciplinary Digital Publishing Institute, 22(10), 3891-3891. https://doi.org/10.3390/s22103891

Wang, G., Guo, Z., Wan, X., & Zheng, X. (2021, June 1). Study on Image Classification Algorithm Based on Improved DenseNet. IOP Publishing, 1952(2), 022011-022011. https://doi.org/10.1088/1742-6596/1952/2/022011

Wu, Q., Liu, Y., Li, Q., Jin, S., & Li, F. (2017, October 1). The application of deep learning in computer vision. https://doi.org/10.1109/cac.2017.8243952

Wu, S., Wang, J., Liu, L., Chen, D., Lu, H., Xu, C., Hao, R., Zhao, L., & Wang, Q. (2023, August 9). Enhanced YOLOv5 Object Detection Algorithm for Accurate Detection of Adult Rhynchophorus ferrugineus. Multidisciplinary Digital Publishing Institute, 14(8), 698-698. https://doi.org/10.3390/insects14080698

Yu, J., Zhang, X., Wu, T., Pan, H., & Zhang, W. (2023, May 10). A Face Detection and Standardized Mask-Wearing Recognition Algorithm. Multidisciplinary Digital Publishing Institute, 23(10), 4612-4612. https://doi.org/10.3390/s23104612

Yuan, Q., Shafri, H Z M., Alias, A H., & Hashim, S J. (2021, June 24). Multiscale Semantic Feature Optimization and Fusion Network for Building Extraction Using High-Resolution Aerial Images and LiDAR Data. Multidisciplinary Digital Publishing Institute, 13(13), 2473-2473. https://doi.org/10.3390/rs13132473

Zhang, Z., Wu, C., Coleman, S., & Kerr, D. (2020, August 5). DENSE-INception U-net. https://www.sciencedirect.com/science/article/pii/S0169260719307904

Zhao, Z., Zheng, P., Xu, S., & Wu, X. (2018, January 1). Object Detection with Deep Learning: A Review. Cornell University. https://doi.org/10.48550/arxiv.1807.05511

Zhou, T., XinYu, Y., Lu, H., Zheng, X., Qiu, S., & Liu, Y. (2022, April 25). Dense Convolutional Network and Its Application in Medical Image Analysis. Hindawi Publishing Corporation, 2022, 1-22. https://doi.org/10.1155/2022/2384830