Anti Deepfake Examiner

Final Year Project

Session 2020-2023

A project submitted in partial fulfillment of the degree of

BS in Artificial Intelligence

Department of Software Engineering

Faculty of Computer Science & Information Technology

The Superior University, Lahore

Fall 2023

Type (Nature of project)	[✓] **D**evelopment [ ] **R**esearch [ ] **R**&**D**
Area of specialization	Artificial Intelligence (Machine Learning & Deepfake)
BSAI-FYP-S23-004	

Project Group Members

Sr.#	Reg. #	Student Name	Email ID	*Signature
(I)	BAIM-F19-007	Abdullah Maroof	baim-f19-007@superior.edu.pk	
(ii)	BAIM-S20-006	Abubakar Siddique	baim-s20-006@superior.edu.pk	
(iii)	BAIM-S20-009	Muhammad Zubair Ali	baim-s20-009@superior.edu.pk	

*The candidates confirm that the work submitted is their own and appropriate credit has been given where reference has been made to work of others

Plagiarism Free Certificate

This is to certify that, I Abdullah Maroof S/D of Maroof Hussain, group leader of FYP under registration no BSAI-FYP-S23-004 at Software Engineering Department, The Superior University, Lahore. I declare that my FYP report is checked by my supervisor.

Date: Name of Group Leader: Abdullah Maroof Signature: _____

Name of Supervisor: Mr. Nagesh Kumar

Designation: Lecturer

Signature: _____

HoD: Dr. Tehreem Masood

Signature: _____

Project Report

Anti Deepfake Examiner

Change Record

Author(s)	Version	Date	Notes	Supervisor's Signature
Abdullah Maroof	1.0		Original Draft	
Mr. Nagesh Kumar (Supervisor) & Abdullah Maroof	1.1		Project title & document changes	
Evaluators (Ms. Tayyaba Farhat & Mr. Tayyab Khushi) & Abdullah Maroof	2.0		Few changes in idea according to feedback of evaluators	
Abubakkar Siddique	2.1		Additions in the document	
Zubair Ali	2.2		Modifications in the dataset chapter of document	
Mr. Nagesh Kumar (Supervisor) & Abdullah Maroof	2.3		Addition of Diagrams & Tables	
Evaluators (Mr. Tayyab Khushi & Ms. Asma Abubakkar) & Abubakkar Siddique	3.0		Project title changes & modification in the document	
Dr. Tehreem Masood (HOD) & Abdullah Maroof	3.1		Project title changes	
Mr. Abdullah Maroof & Zubair Ali	4.0		Addition of Chapters & Modification of document	

APPROVAL

PROJECT SUPERVISOR

Comments: _____

_____

Name:_____

Date:_____ Signature:_____

PROJECT MANAGER

Comments: _____

_____

Date:_____ Signature:_____

HEAD OF THE DEPARTMENT

Comments: _____

_____

Date:_____ Signature:_____

Dedication

*"We are dedicating this project to our **Parents** & **Teachers** who are giving their best for our better education"*

Acknowledgements

We have taken efforts in this project. However, it would not have been possible without the kind support and help of **Sir Nagesh Kumar (Supervisor)**. We would like to extend our sincere thanks to him.

We are highly indebted to our Evaluators & Teachers for their guidance & constant supervision as well as providing necessary information regarding the project and for their support in completing the project.

Executive Summary

Anti Deepfake Examiner is a Deepfake Detection System of Images. This project is aimed to bring enhancement in the field of Artificial Intelligence. Now-a-days, Deepfake technology is used for the negative purposes in the society which is leading towards the fake information and this false information is making a huge impact on our society. Our Project seeks to address this growing concern by leveraging different Machine Learning models to identify and expose deepfake images.

Our primary objective of our project is that you don't need to train the model on specific person's images to identify the image. By focusing on features such as facial landmarks, optical flow, texture analysis and noise patterns. Our project aims to identify anomalies and inconsistencies that are indicative of deepfake manipulation.

To achieve our objective, we are using a dataset which is already provide on kaggle with the name of **Deepfake and Real Images Dataset**. This dataset is consist of **190,335 images** of labeled data. Dataset contains images of common people and all images are different from each image. It will help us to identify real & fake images without the need of training on specific person images.

To achieve best results, we had applied different **CNN & Keras Applications** like **VGG16**, **RESNET50**, **DENSENET201** & **InceptionV3**. We had generated positive results with our project.

In conclusion, Anti Deepfake Examiner will bring innovation in the Artificial Intelligence field because existing systems are working through generalization and GAN.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Chapter 1: Introduction

Anti Deepfake Examiner is based on developing an innovative Deepfake Detection System. As deepfake technology continuous to advance, manipulated videos, images & audios are becoming significant threat to our society. Our project aims to create a solution that detects deepfakes based on feature analysis, eliminating the need for specific person training. By applying Machine Learning Algorithms and Diverse Feature Sets, this system will identify outliers and inconsistencies of deepfake manipulation. This innovative approach ensures adaptability and scalability, enabling detection of new and emerging deepfake techniques.

1.1 Background

Deepfake is an emerging technology of Artificial Intelligence which growing rapidly in our society for the negative purposes. Every day, we are watching different news, images & videos on social media platforms & news channels which are seem to be real but most of them are deepfaked which is leading our society to false information. It is becoming a big problem in our society. Deepfaked images, videos & audios are spread everywhere like a real news & there are many paid software are available online which allows people to make deepfake images, videos & audios. There are different paid deepfake detection system are available on internet but you need diverse amount of pictures & videos of a specific person to detection the fakeness of it. You can get diverse amount of data of a celebrity or a politician but to collect diverse amount of data of a common person is difficult. This is the main reason behind our project. We came-up with an idea to introduce a system which will work through feature analysis and without the need of training the model on a specific person images.

1.2 Motivations and Challenges

The **Motivation** behind the Anti Deepfake Examiner derived from the need to stop or slow down the negative aspects of deepfake technology. Deepfakes have the potential to make people trust in fake images, videos & audios which is causing significant harm to our society. By developing an advanced Deepfake Detection System, it will safeguard the integrity of digital content and protect against the manipulation of images. It will promote accountability in the digital era. The motivation also lies in the desire to empower individuals, organizations and platforms with a reliable tool to identify and expose the deepfake manipulation.

We have to face a **Challenge** while developing our project. It required an efficient system which have a Good GPU, RAM & Advanced Processors. New technologies & fully equipped system was caused a huge amount to buy it.

1.3 Goals and Objectives

Goals of our project are as follow:

- Implementation of feature-based analysis techniques.
- Overcome the problem of generalization.
- Ensure the real-time deepfake detection.
- Trust of the society on digital media.
- Reduce the deepfake manipulation.

Objectives of our project are as follow:

- Implement efficient algorithms and optimizations to enable real-time processing.
- Develop a reliable tool to identify and expose deepfake images.
- Train the system on diverse datasets to extract a wide range of subjects, backgrounds and scenarios.

1.4 Literature Review/Existing Solutions

After study different research papers which are based on deepfake detection & its techniques, deepfake detection has been an active area of research with numerous studies proposing various techniques & methodologies [4]. These all papers are downloaded from IEEE Xplore, IEEE Access & Google Research which are published in different Conferences all over the world.

During the study of research papers, mostly researchers are using common dataset like FaceForensics++, DFDC & UADFV [1] [3] [4] [5] [6] [8]. Algorithms are mostly used such as GAN, CNN & RNN [4]. Different researchers like Chintha, Guera and Daniel came-up to a conclusion that most of system are working on generalization [4].

Jixin Zhang, Ke Chen from School of Computer Science, Hubei University of Technology, China proposed their research on deepfake detection through feature extraction by using gray scale images [2].

Krishnakripa Jayakumar - Department of Computing, Informatics Institute of Technology, affiliated to University of Westminster, UK Colombo, Sri Lanka had proposed a model which will also explain on which basis trained model or system has answered that the video or image is deepfake or not [3]. It brings innovation in the generalization deepfake systems research.

There are different existing systems in the market which are detecting through different techniques like Face X-ray, Head Pose, Eye Blinking, Spatiotemporal features with LSTM, Intra-frame and temporal inconsistencies & Automatic Face Weighting [4] [6].

Y. Patel worked to remove the generalization with CNN Models but in the end, he used GAN with Customized CNN model. He used combination of 5 Dataset which are already available and related to celebrities [7].

M. S. Rana, M. N. Nobi, B. Murali and A. H. Sung provided a complete details of all deepfake detection systems and papers published from 2012 – 2022. They came to a conclusion that results varies with the dataset and mostly are using GAN and customized dataset and models to achieve Optimal Accuracy [8].

1.5 Gap Analysis

After studying different research papers & analyzing different existing system for deepfake detection, we had analysis following gaps:

- Generalization
- Computational Complexity
- Limited Availability of Diverse and Realistic Datasets
- Transferability to New Domains

  [3] [4] [8]

In FYP Project, we are aimed to overcome the first-three gaps of existing systems.

1.6 Proposed Solution

After studying the existing systems & researcher papers, we are came-up with an innovative idea of deepfake detection. The proposed solution combines advanced feature-based analysis techniques, real-time processing capabilities, and adaptability to emerging deepfake techniques. We are developing a deepfake detection system which is fully based on feature analysis and no need to train the model on specific person images. This system allows to identify outliers & discrepancies in deepfake images. The system will extract and analyzes various features like facial landmarks, optical flow, texture patterns, noise inconsistencies and many more. By comparing these features between real and fake images, it can be easy to identify irregularities that indicates the presence of deepfake. It will allow real-time deepfake detection. It will also increase the efficiency of the detection. This system implements different Keras Applications like VGG16, RESNET50, DENSENET201 and InceptionV3 which allow us to get a better accuracy & performance of the system.

This Project's solution aims to contribute to the fight against deepfake manipulation by providing a reliable, adaptable, and efficient results. By combining advanced feature analysis and real-time processing, our project seeks to safeguard the integrity of visual media, protect against the spread of misinformation, and promote a more trustworthy digital environment.

1.7 Project Plan

This Project aims to develop a deepfake detection system based on advanced feature analysis techniques, to ensure the best outcomes. For this purpose, a well-structured plan is essential. Here is a comprehensive project plan:

1.7.1 Work Breakdown Structure

- **Problem Analysis & Idea:** A complete study of deepfake detection systems and research papers. Identify the problems and gaps. Determine the solutions of these problems and gaps. Choosing the best & innovative idea which will bring advancement in Artificial Intelligence Field.
- **Project Definition & Scope**: Clearly define the goals, objectives, and scope of the Project. Identify the target platforms, application scenarios and intended users for the project. Determine the key features and functionalities that the system should possess, such as real-time processing, adaptability, and transparency.
- **Data Collection**: Collect a diverse dataset of both real and deepfake images. Ensure the dataset represents a wide range of subjects, scenarios, manipulation techniques, and variations.
- **Front-End Design**: Designed the front-end of the system with the help of Python Library Tkinter and Keras Application will be implemented as a backend of it. Designed an attractive design which allow users to interact with it easily.
- **Data Preprocessing & Feature Extraction**: Preprocess the dataset by performing necessary data cleaning, normalization, and augmentation techniques. Implement feature extraction algorithms to extract relevant visual features from the dataset, such as facial landmarks, optical flow, texture patterns, and noise inconsistencies.
- **Model Training & Validation**: Design and implement Keras Applications such as VGG16, RESNET50, DENSENET201 and InceptionV3, to learn discriminative features from the extracted data. Train the models using the preprocessed dataset. Validate the trained models using evaluation metrics and benchmark datasets to assess their performance, accuracy, and robustness.

- **Testing & Evaluation**: Conducting different test on the system to validate its functionality, performance, and detection accuracy. Evaluate the models by applying it on test data. Calculate Test Accuracy, F1 Score, Confusion Matrix, Precision and Recall.
- **Documentation**: Document the entire development process, including methodologies, algorithms, implementation details, and system architecture. Prepare comprehensive reports, including the project's objectives, findings, challenges encountered, and recommendations for future improvements.

1.7.2 Roles & Responsibility Matrix

In the Roles & Responsibility Matrix, we had described the team member's names, their roles and responsibilities. For this purpose, we make a table for the explanation.

Name	Role	Responsibility
Abdullah Maroof	Project Manager/ Developer	Overall project Management, Project Implementation & Documentation.
Abu Bakar Siddque	Data Scientist/ Developer	Data Collection, Data Analysis & Preprocessing and Project Development.
Zubair Ali	Frontend Designer	Project Designing & User Interface Design.

Table 1: Roles & Responsibili y Marix

1.7.3 Gantt Chart

Gantt Chart is defined as the yearly plan of the project development. We had make the Gantt chart in which we defined our yearly plan of our FYP Project. We had explained our every month activities of FYP project in the following Gantt chart:

Figure 1: Gantt Chart Diagram

1.8 Report Outline

Report Outline contains the following:

- **Introduction:** It will include the background of deepfake technology, motivation for developing, objectives and goals, scope and limitation of the project.
- **Literature Review:** It will include overview of deepfake detection techniques, existing solutions and their strengths & weaknesses, key research papers and study in the field, evaluation matrices and benchmark datasets.

- **Methodology:** It will include data collection and preprocessing, feature analysis techniques, deep learning models and algorithms, model training and optimization strategies, real-time processing implementation.
- **System Design and Implementation:** It will include architecture and components of the project, user interface design and functionalities, integration with target platforms or applications, technical details of system development and implementation.
- **Validation and Evaluation:** It will include performance evaluation metrics and methodologies, evaluation of the project on benchmark datasets, comparative analysis with existing deepfake detection solutions, testing and validation results, including detection accuracy and efficiency.
- **Conclusion:** It will include summary of the project's objectives and achievements, contributions to the field of deepfake detection, significance of the project in addressing deepfake threats.
- **References:** It will include list of research papers, articles and sources where we get help in our project & documentation.

1.9 Empathy Map

An empathy map is a visual tool used to understand and empathize with users' behaviors, thoughts, and emotions, aiding in the development of user-centric solutions. We had analyzed the problem of normal people related to deepfake and then identify the solution through empathy map.

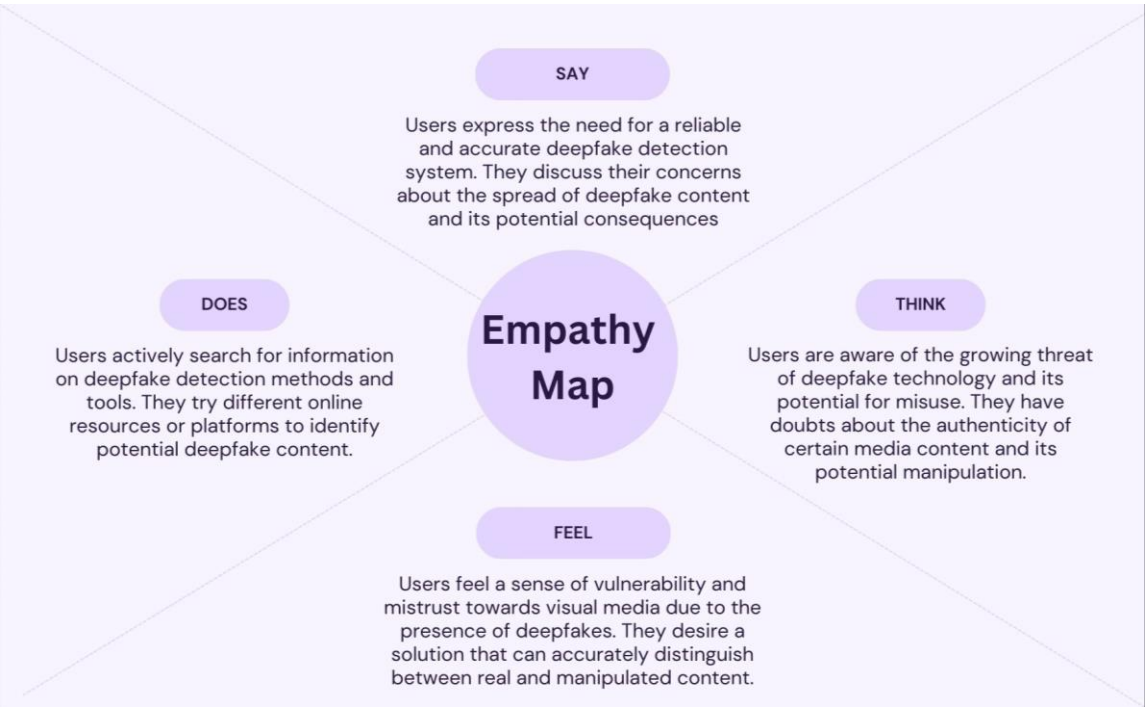

Figure 2: Empathy Map Diagram

Chapter 2

Data Collection

2 Data Collection

2.1 Introduction

2.1.1 Sources of Data

Images Dataset: Deepfake and Real Images Dataset

Author: Manjil Karki

Website: Kaggle

URL: https://www.kaggle.com/datasets/manjilkarki/deepfake-and-real-images

2.1.2 Access the Data

The dataset used for this project was sourced from Kaggle. To obtain the dataset, a Kaggle account was created, and the dataset was downloaded from the provided link. The dataset consists of a collection of deepfake and real images, which will be used for training and evaluation in the project.

2.2 Data preparation

The data preparation process for the project involved the following steps using the dataset obtained from the provided link:

- Downloading the dataset of real and fake images from the provided links.
- Analysis of the data to check the structure, size and the distribution of the data.
- Data Preprocessing of the dataset includes the resizing of the images and converting them to a standardized format.
- Optimizing the model by running more epochs on the dataset.

2.3 Data Storage

The dataset obtained from the provided link was stored and organized as follows:

- Dataset is downloaded from the kaggle and stored on a local storage (SSD). It is placed in the folder which is used for Project Data.
- Dataset is separately organized in three folders containing training, testing & validation data. Each folder contains two sub-folders (Real & Fake).
- Each image was assigned a unique name for the proper identification.

Chapter 3

Data Preprocessing

3 Data Preprocessing

In data preprocessing of the dataset, we just simply resize the images according to the need of our training models. We also perform rescaling, zoom range, shear range, rotation range, horizontal & vertical flip and width & height shift range according to the need of training models. Dataset is already divided into training and validation. All the images are already labeled.

3.1 Description of the data cleaning process

There was no need to apply cleaning process on the dataset because images are already classified and there is no outlier in it.

3.2 Identification of data issues:

We identified no issue within the dataset but while doing data exploration process, we faced a system issue while loading whole dataset for exploratory data analysis. I performed EDA on a same part of dataset. We had used 4002 images from the training dataset for EDA.

3.3 Handling of missing values:

This Dataset is consist of Images and all the images are labeled and classified. There is no issue of missing values.

3.4 Data type conversion:

We didn't convert the type of dataset but resized the images according to the need of model by using Keras Preprocessing technique. We convert the testing data in Numpy array to predict the result for the image.

3.5 Data normalization:

Before putting our dataset for the training, we normalized the images according to the need of Machine Learning Algorithms. We performed resizing, rescaling, zoom range, shear range, rotation range, horizontal & vertical flip and width & height shift range on the images.

3.6 Conclusion:

In the conclusion of this chapter, we must say that Data Preprocessing is an important part for the training of model and getting best outcomes. It was little difficult to apply different preprocessing on different models. By doing it, we came-up with better results.

Chapter 4

Data Exploration

4 Data Exploration

In Data Exploration Analysis, we had analysis the dataset. We used different python libraries such as OS, CV2, Numpy, Matplotlib and Tqdm. We had performed EDA on a part of a dataset because our system providing us a lot of issues while loading the whole dataset for the analysis. We check Basic Information of Dataset which includes size.

4.1 Description of Dataset

The project utilizes the datasets sourced from the kaggle. The dataset comprises more than 190,335 images, consisting of both fake and real. The dataset includes a diverse range of subjects, backgrounds and conditions to ensure its effectiveness in training and evaluating the project. Each file in the dataset is labeled and divided into training, testing and validation. This labeling allows for supervised learning approaches to be employed during the model development phase. The dataset is balanced, meaning that an equal number of real and fake images are present, which helps prevent bias and ensures fair evaluation of the deepfake detection system's performance.

Description of Dataset			
SR	**FOLDERS**	**REAL IMAGES (Subfolder)**	**FAKE IMAGES (Subfolder)**
1	Training (140,002 Images)	70,001	70,001
2	Validation (39,428 Images)	19,787	19,641
3	Testing (10,905 Images)	5,413	5,492

Table 2: Description of Dataset

4.2 Descriptive statistics

In descriptive statistics, we had find tendency & dispersion and visualize them on a plot.

Statistics Table

We had performed mathematical calculation on our dataset. EDA were showing errors when we are performing analysis on the full dataset, so we take sample size of 4002 images to perform different kind of analyses. In Descriptive Statistics, we find mean, median, standard deviation & variance (dispersion).

Descriptive Statistics (Sample Size 4002 Images)		
SR	**Statistics**	**Average Result**
1	**Mean**	101.11537013068987
2	**Median**	93.33333333333333
3	**Standard Deviation**	67.33551158972055
4	**Variance**	4545.091790491668

Table 3: Descriptive Statistics

Tendency

In Tendency, we calculated the mean and median. Average mean is 101.11537013068987 and average median is 93.33333333333333. We visualized the mean and median which is shown in the figure.

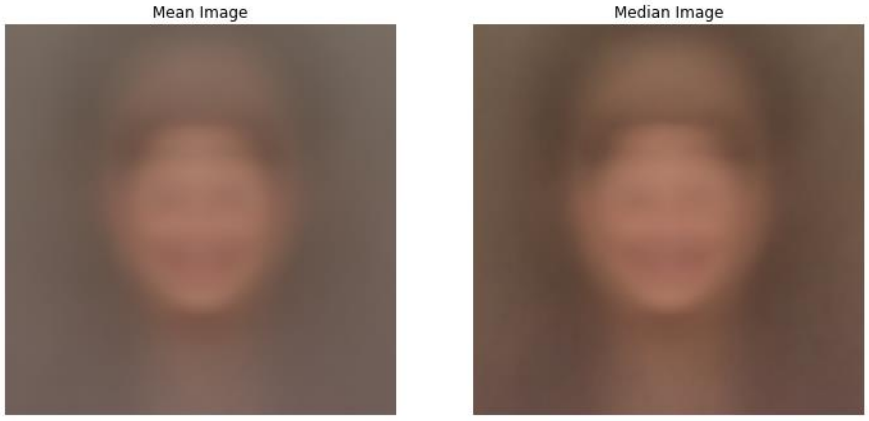

Figure 3: Tendency Visualization

Dispersion

In Dispersion, we calculated the variance. Average variance is 4545.091790491668. We visualized the variance which is shown in the figure.

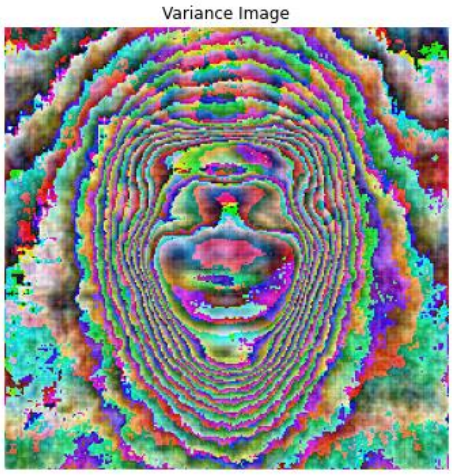

Figure 4: Dispersion Visualization

4.3 Visualizations

We have visualized by our dataset and results are as follow:

Visualizing Dataset Images

We had displayed random samples from our dataset and all the samples are labeled with fake and real images which are as follows:

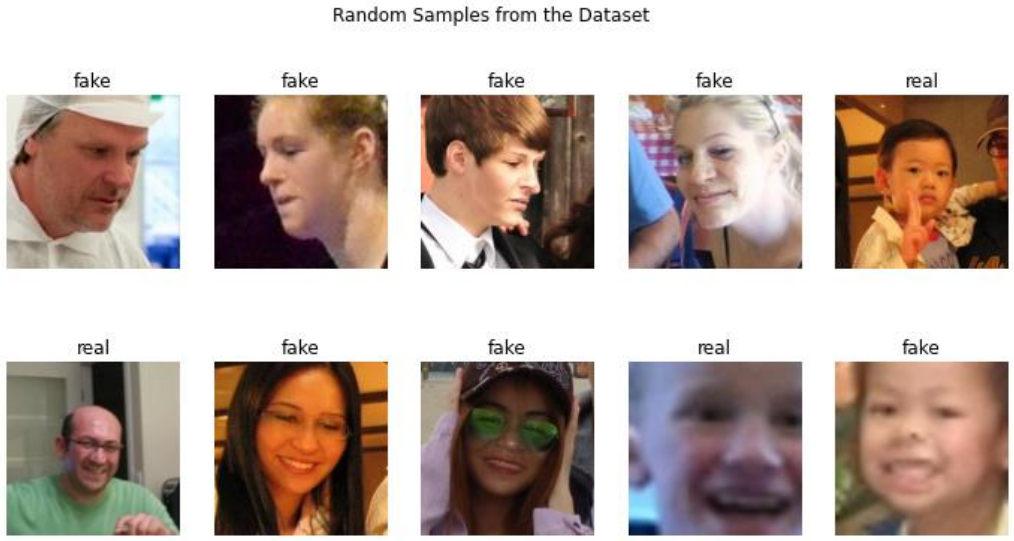

Figure 5: Random Samples Visualization

Visualizing Dataset in RGB Scheme

We had visualized the color distribution of the dataset by using histogram plot of Matplotlib Library (Used for the visualization through graphs and plots). We displayed the distribution of RGB Color in separate plots.

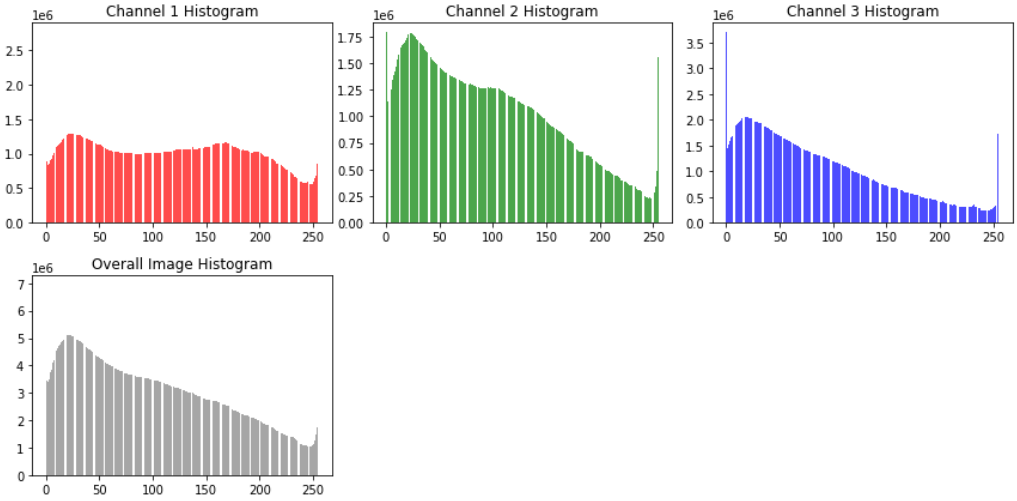

Figure 6: Dataset RGB Histogram Plot

4.4 Data Correlation

To check the correlation of the data, we first resize the images to (50, 50). We were having memory allocation issues so we resize the images and visualize the dataset correlation. The average result is 0.2354100473216279. Visualization of data correlation is as follows:

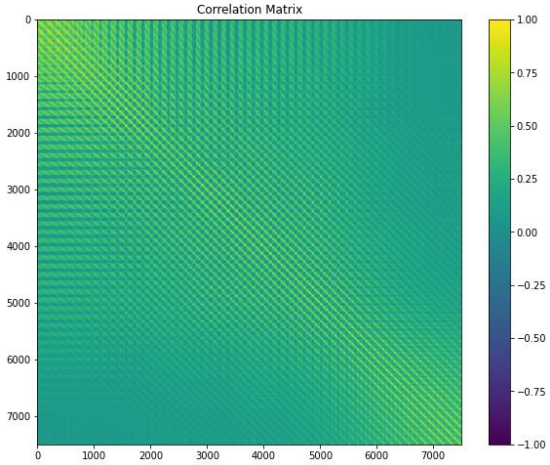

Figure 7: Correlation Matrix

Chapter 5
Purposed Approach

- **Dataset Collection:** We will collect a diverse dataset comprising both real and fake images. Ensure the dataset covers a wide range of Subjects, Scenarios, and Manipulation Techniques.
- **Dataset Analysis:** We will implement different analysis techniques to analyze the dataset. We will implement Exploratory Data Analysis techniques such as Size Analysis, Statistics Information, Color Scheme Analysis, Correlation Analysis and many more.
- **Data Preprocessing:** Before putting our dataset in the training model, we will preprocess the dataset. We will resize, zoom-in, flipping, rotation and shifting.
- **Machine Learning Model Selection & Implementation:** We will check for Keras Applications which will suits best and provide maximum best results. Keras Applications will help us in extracting features from the images and doing training on them. We are going to use VGG16, DENSENET201, RESNET50 and InceptionV3.
- **Model Evaluation:** We will evaluate the trained models on our testing dataset and established evaluation metrics. Measure the detection accuracy, precision, recall, and F1 score to assess the model's performance.
- **Graphical User Interface:** We will develop a user-friendly interface for users to interact with the system. Design an intuitive dashboard that allows users to upload and analyze images easily.
- **Documentation**: We will document the entire approach, including methodologies, algorithms, and implementation details. Prepare comprehensive reports summarizing the project's objectives, findings, and challenges.

By following this proposed approach, the Project aims to develop an effective and reliable deepfake detection system that can accurately identify manipulated images, restore trust in visual media, and contribute to the ongoing efforts in combating deepfake threats.

Project Development Diagram

In the project development diagram, we had displayed the whole process of our project development which includes data collection, preprocessing, model selection, training, evaluation, data analysis and GUI designing.

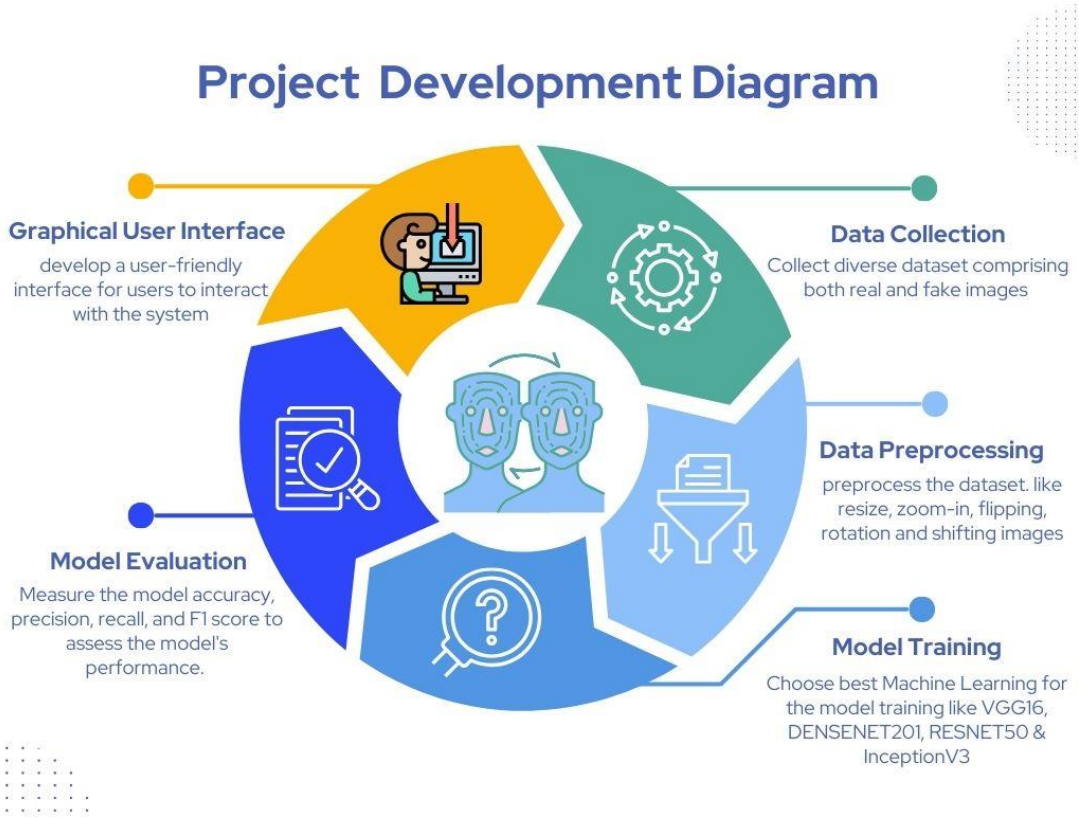

Figure 8: Project Development Diagram

Architectural Diagram

In the architectural diagram, we had displayed the working process of our project which includes the process of user interaction with our system which includes Graphic User Interface (Main Page, About Team Page & Deepfake Detection Portal Page).

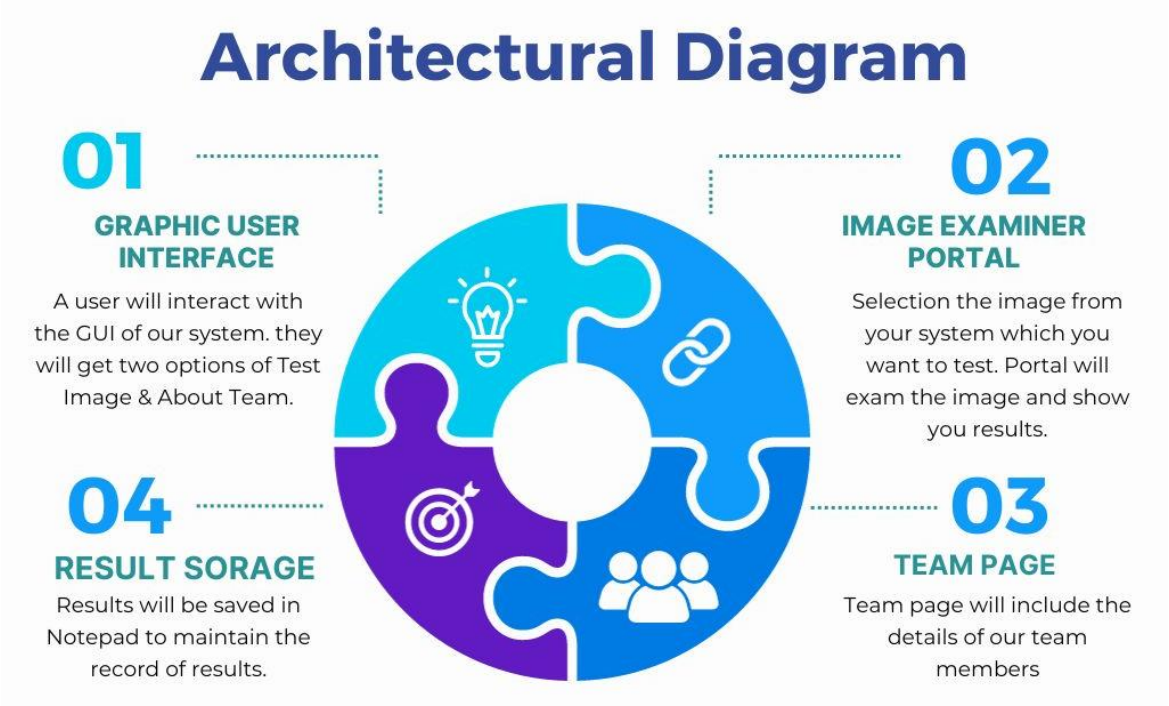

Figure 9: Architectural Diagram

Chapter 6
Implementation

6.1 Tools and Technologies

We had used Python Language for our project. We used different libraries of python like Numpy, Sclkit-Image, Matplotlib, OS, CV2, Tkinter, Tensorflow, Keras, Pyttsx3 and many more. We implement our project by using Jupyter Notebook through Anaconda Environment.

6.2 Data Collection & Feature Engineering

We had studied different dataset for our project because we required a dataset which consist of common people images. We ensured the dataset represents a wide range of subjects, scenarios, manipulation techniques, and variations. Before putting our dataset into training, we apply Data Generator from Keras Preprocessing method to resize, scale-up, flip and zoom the images.

6.3 Model Selection and Training

After studying different deepfake detectors and measuring our system specification, we used CNN model as known as Keras Application. We selected and trained dataset on VGG16, DENSENET201, RESNET50 and InceptionV3. We evaluated the results and came to a conclusion with best results with DENSENET50.

6.4 Evaluation Metrics

We had evaluated all the models. F1 Score, Recall, Precision and AUC-ROC Charts are as follows and each evaluation metrics chart is separately defined:

F1 Score Result

The F1 score in AI is a metric that combines precision and recall into a single value, providing a balance between the two measures for evaluating classification models. In the following graph, RESNET50 has the best F1 Score and after that VGG16 has the second best F1 Score. InceptionV3 has worst F1 Score in all of the models.

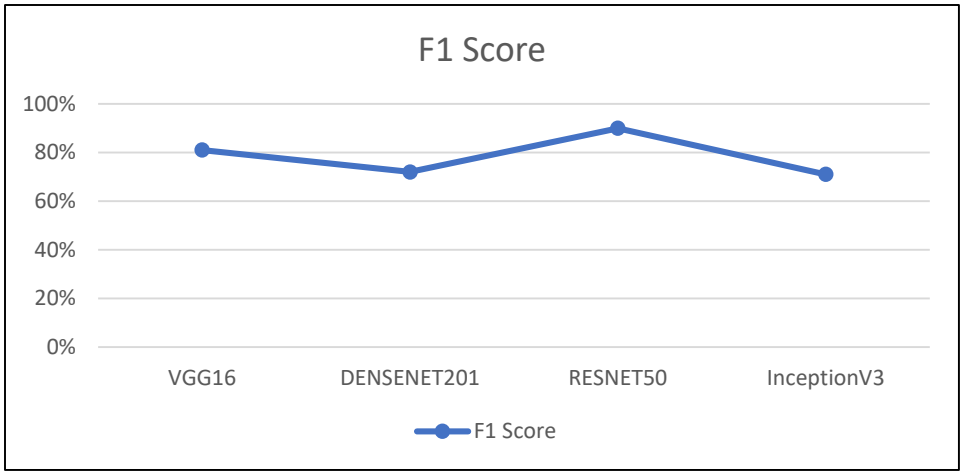

Figure 10: F1 Score Evaluation Chart

AUC ROC Score Result

The AUC ROC (Area Under the Receiver Operating Characteristic Curve) score in AI measures the ability of a classification model to distinguish between classes, summarizing the model's performance across various thresholds. In the following graph, RESNET50 has the best AUC ROC score and after that VGG16 has the second best AUC ROC score. InceptionV3 has worst AUC ROC score in all of the models.

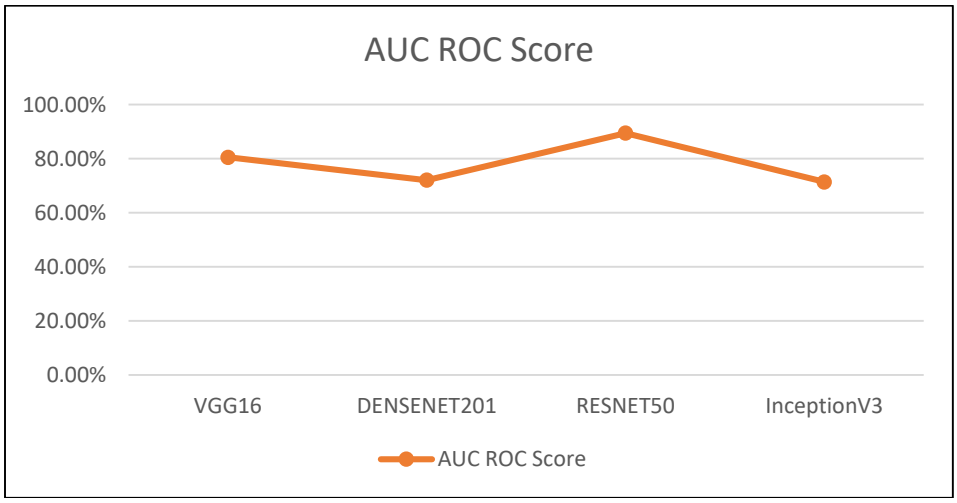

Figure 11: AUC ROC Score Evaluation Chart

Precision Result

Precision is the measure of the accuracy of the positive predictions made by a model among all positive predictions and is calculated as the ratio of true positives to the sum of true positives

and false positives. In the following graph, RESNET50 has the best precision and after that VGG16 has the second best precision. InceptionV3 has worst precision in all of the models.

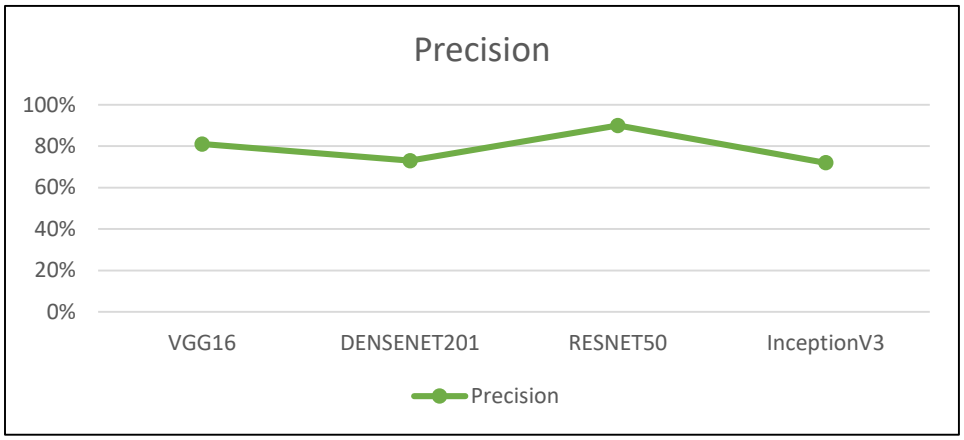

Figure 12: Precision Evaluation Chart

Recall Result

Recall measures the ability of a model to identify all relevant instances from the dataset and is calculated as the ratio of true positives to the sum of true positives and false negatives. In the following graph, RESNET50 has the best recall and after that VGG16 has the second best recall. InceptionV3 has worst recall in all of the models.

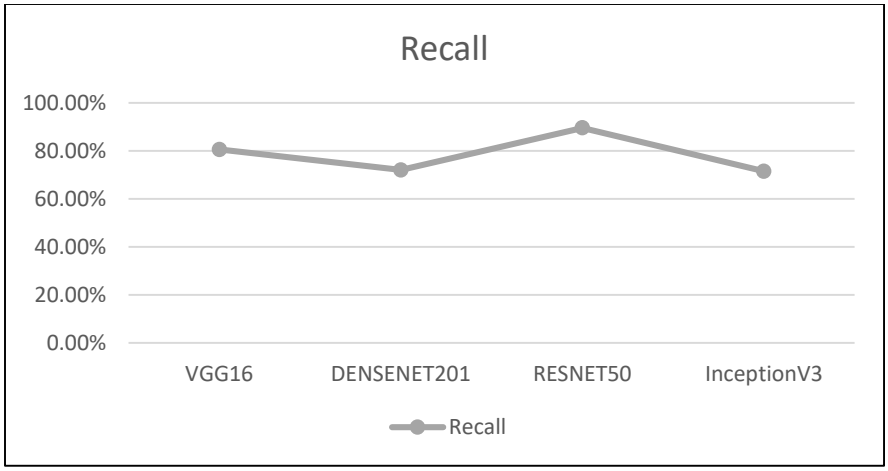

Figure 13: Recall Evaluation Chart

6.5 Experimental Design

Experimental design is defined as the Project Development Design. It will include the dataset used, the experimental setup, and the performance measures used to evaluate the model. Steps are as follows:

- Step-1: We studied and collect a data which was rarely used in any deepfake detection system. This Dataset was a diverse dataset which included common people with a wide range of subjects, scenarios, manipulation techniques, and variations. Dataset was already divided into training, validation and testing data with two labeled classes fake and real.
- Step-2: We had reprocessed the dataset according to the need of model which included resizing, zooming, flipping, rotation and shifting. We used Keras Preprocessing function for it which is Data Generator.
- Step-3: After studding current models and deepfake detection systems, most of them had used GAN models or customized designed CNN models for the detection. Most of them are working on the term of Generalization or Celebrity Data. We had four CNN which are also known as Keras Applications. We used VGG16, RESNET50, DENSENET201 and InceptionV3 to train the model. We saved them in .h5.
- Step-4: After training the models, we evaluate them by performing different evaluation metrics. We also tested the whole testing dataset and calculated the accuracies. We also developed Confusion Matrix of each model to check the percentage of right and wrong results. We had evaluated F1 Score, Precision, Recall and AUC-ROC Accuracy. RESNET50 provided the best results.
- Step-5: After the evaluations and choosing the best model for the project, we design Graphic User Interface which includes three pages (MAIN Page, About Page and Testing Page).

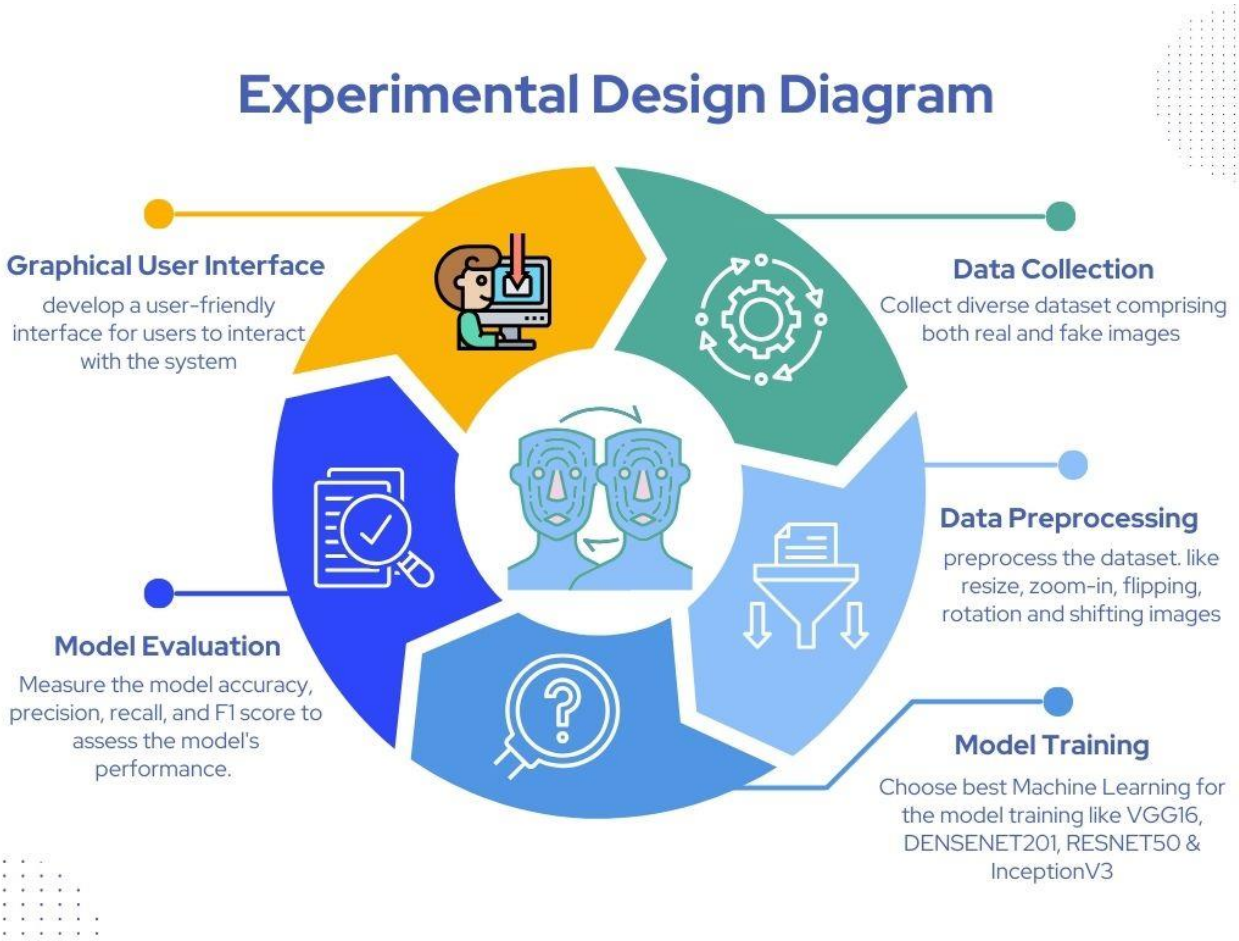

Figure 15: Experimental Design Diagram

Chapter 7

Results and Analysis

7 Results and Analysis

In this chapter of Results and Analysis, we have presented the results and evaluations obtained from the proposed approaches which we mentioned in the Chapter 6. This chapter includes interpretation of results in the light of goals and objectives which we stated in Chapter 1. The analysis is based on the evaluation metrics described in Chapter 6.4. It includes Charts, Confusion Matrices and Graphs to present the results in an easy understandable format.

7.1 Performance Metrics

We had evaluated all the models. We calculated the F1 Score, Recall, Precision and AUC-ROC Chart and results are as follows:

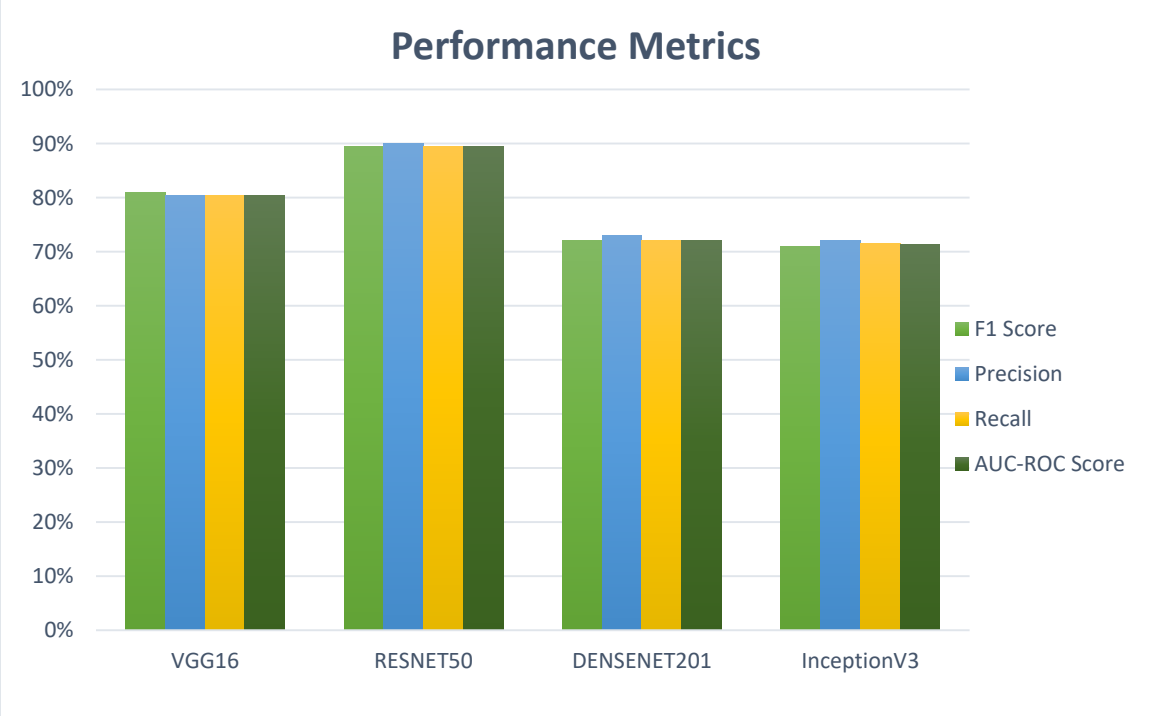

Figure 16: Performance Metrics Chart

7.2 Comparison of Confusion Matrices:

We had evaluated all the trained models with testing data and came-up with best results of RESNET50. Confusion Matrices of all models are as follows:

VGG16

We had displayed the confusion matrix of VGG16 Model performance on the test dataset. It showed that the model predicted 4687 deepfake images correct & 805 deepfake images wrong and 4094 real images correct & 1319 real images wrong. It is also displayed in the following figure:

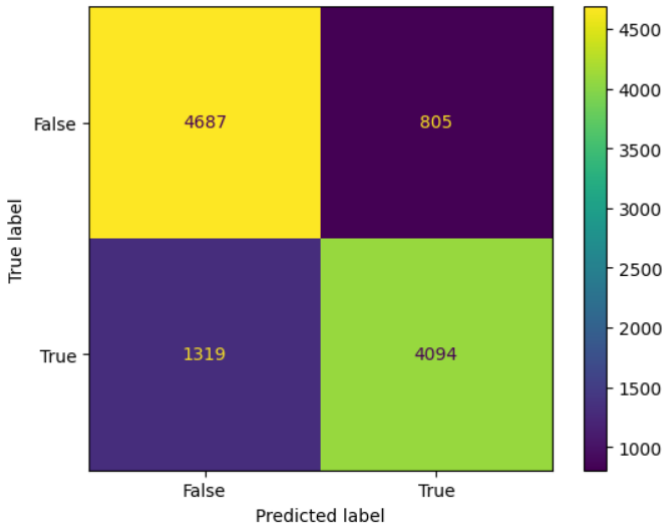

Figure 17: VGG16 Confusion Matrix

DENSENET201

We had displayed the confusion matrix of DENSENET201 Model performance on the test dataset. It showed that the model predicted 4498 deepfake images correct & 994 deepfake images wrong and 3367 real images correct & 2046 real images wrong. It is also displayed in the following figure:

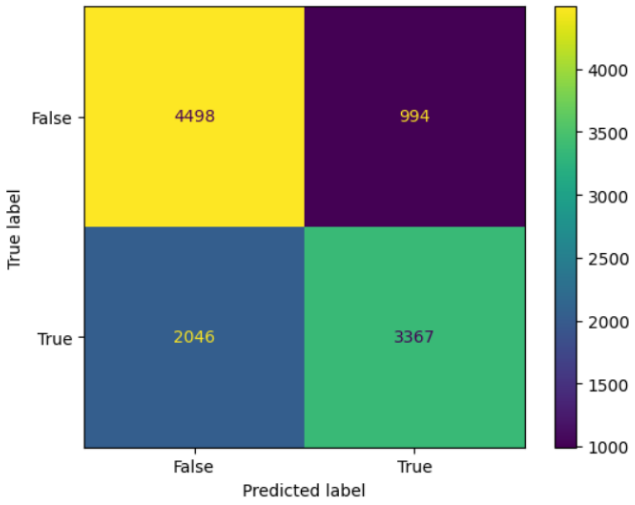

Figure 18: DENSENET201 Confusion Matrix

RESNET50

We had displayed the confusion matrix of RESNET50 Model performance on the test dataset. It showed that the model predicted 5141 deepfake images correct & 351 deepfake images wrong and 4616 real images correct & 797 real images wrong. It is also displayed in the following figure:

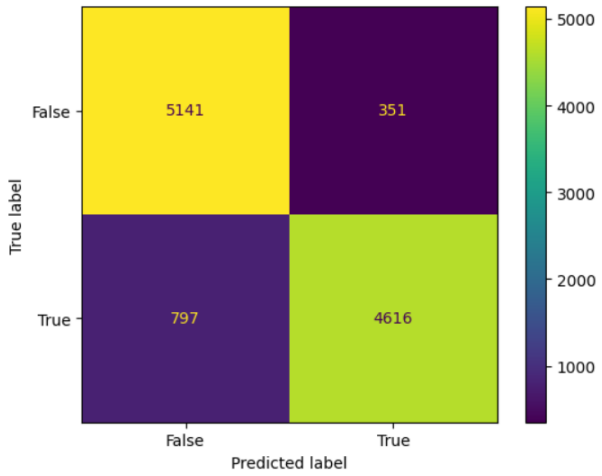

Figure 19: RESNET50 Confusion Matrix

InceptionV3

We had displayed the confusion matrix of VGG16 Model performance on the test dataset. It showed that the model predicted 3491 deepfake images correct & 2001 deepfake images wrong and 4289 real images correct & 1124 real images wrong. It is also displayed in the following figure:

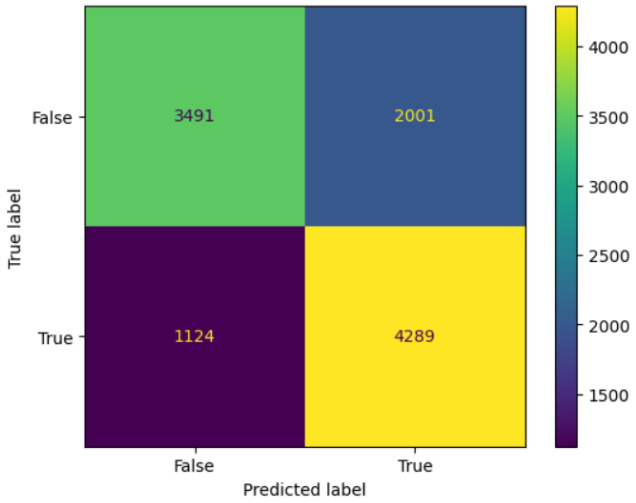

Figure 20: InceptionV3 Confusion Matrix

In this section, the results obtained from the proposed approach are compared by the Confusion Matrices of each approach. The comparison should clearly show the improvement in performance achieved by the proposed approach. RESNET50 showed the best results.

7.3 Interpretation of Results

In this section, the results obtained from the experimentation are analyzed and interpreted in detail. You can see the training and testing results of each proposed approach in the following chart:

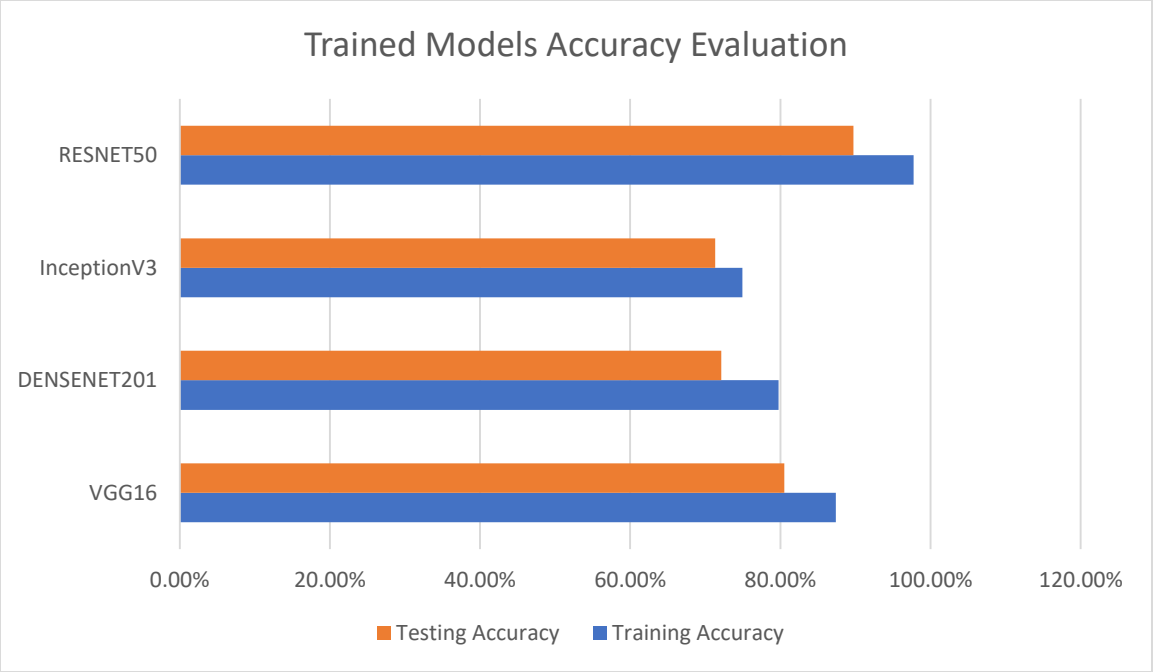

Figure 21: Training Models Accuracy Evaluation Chart

7.4 Graphical User Interface

Anti Deepfake Examiner GUI is consist of three tabs. GUI of the system is designed by the Tkinter Library of Python Langauge which is used for making graphical user interface. We had also used PIL Library in our GUI which is used for the images. System GUI tabs are as follows:

Main Tab GUI

The Main Tab GUI consist of three sections. First section is the header which contains title and quotation. Second section is consist of icon image, definition of deepfake, brief description of system and two buttons (About Tab & Deepfake Examiner Portal Tab). Third section is the Footer which contains the copyright statement.

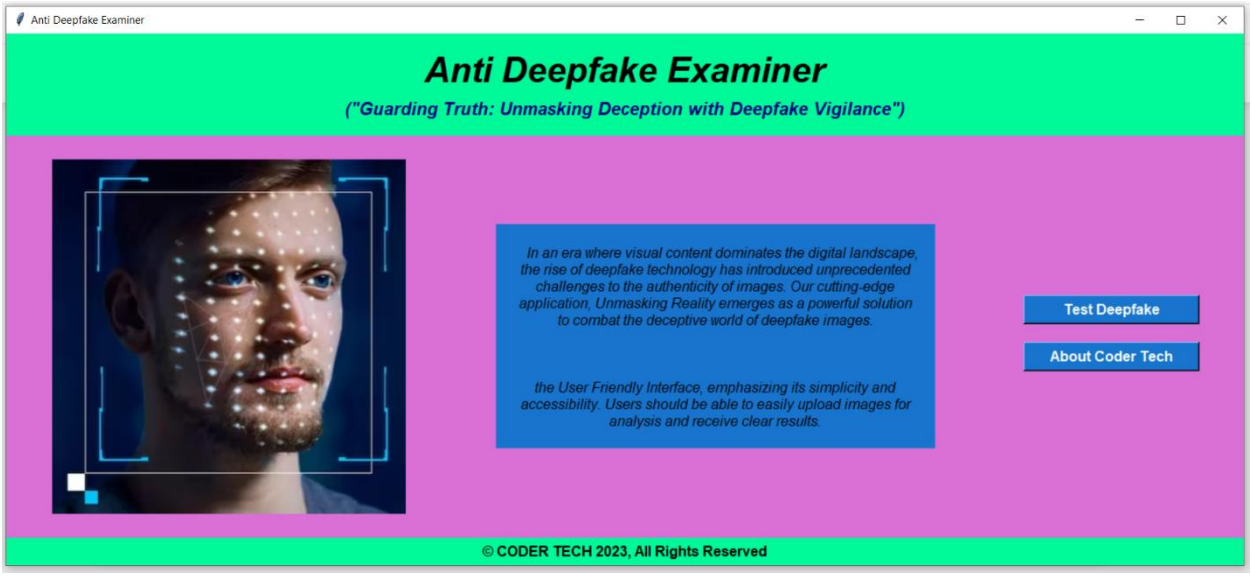

Figure 22: System Main Tab GUI

About Tab GUI

The About Tab GUI consist of three sections. First section is the header which contains title and quotation. Second section is consist of tab title and team members' image & button which tell the details of the member and open his LinkedIn profile. Third section is the Footer which contains the copyright statement.

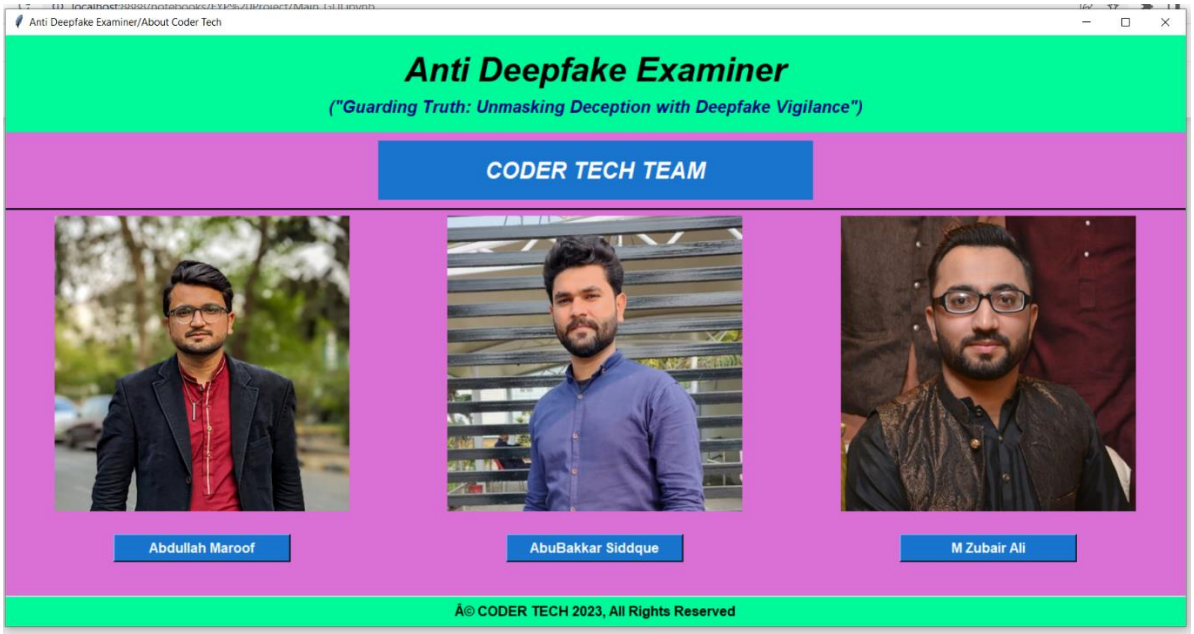

Figure 23: System About Tab GUI

Deepfake Examiner Portal Tab GUI

The Deepfake Examiner Portal Tab GUI consist of three sections. First section is the header which contains title and quotation. Second section is consist of tab title, icon image, upload image button for the testing, test image button will test the uploaded image & give the result as fake or real image, entry bar which shows the address of the image and image label shows the uploaded image. Third section is the Footer which contains the copyright statement.

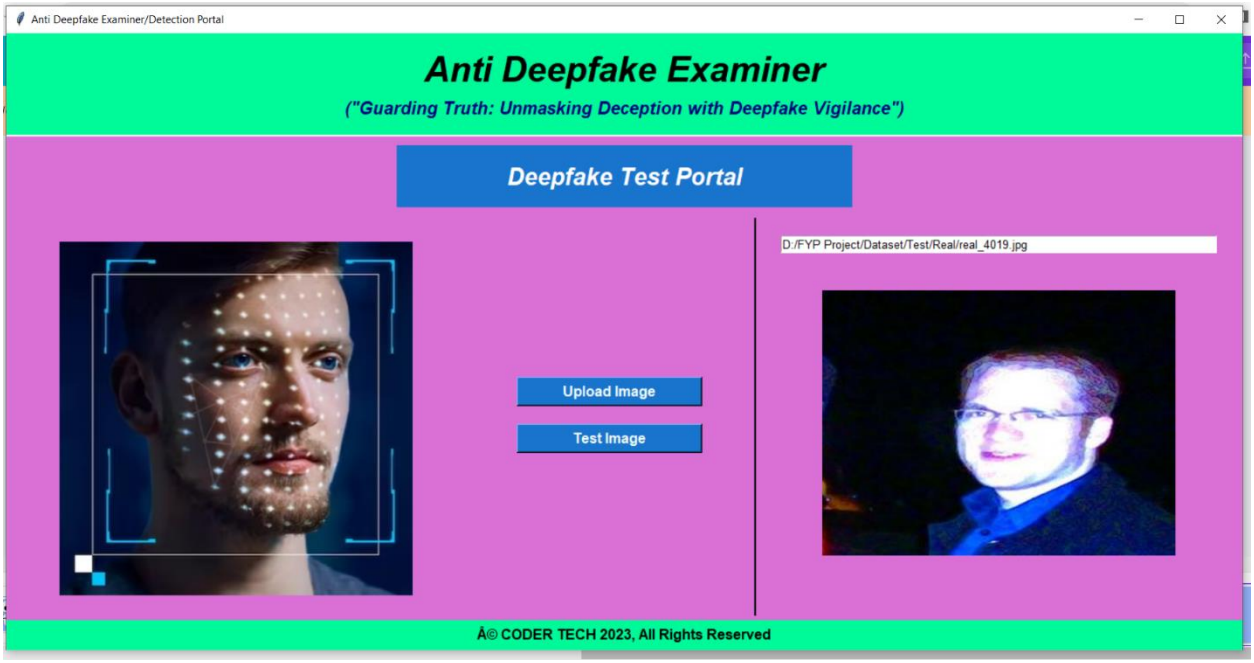

Figure 24: Deepfake Examiner Portal Tab GUI

7.5 Ethical Considerations

In this session of Ethical Considerations, This chapter is consideration ethics in our FYP Project. As a Developers, we keep the Code of Conduct of ACM/IEEE Software Engineering while studying and developing the FYP Project. We had used an open-source Dataset of Images for the project. It was available on Kaggle for further developments with it. We had studied all the kaggle notebooks which are present there and we tried to implement other CNN Models to get more accuracy. Our results which are mentioned in the Document are totally real and identify by our implementations. All the graphs or tables or

diagrams which are used in the project, they are available in our in our codes. Our goal is to ensure that the results obtained are accurate and can be replicated in future studies.

7.6 Conclusion

In this section, we had concluded the whole document to provide a clear understanding of our FYP Project. We are doing our FYP in Deepfake Detection System of Images. According to our studies, Most of the models are working on Generalization specially which are using CNN models. We are using the CNN models but we are not using fully customizing CNN Models to obtain best results. We had used a dataset of real and fake images which is fully authentic dataset and sourced from kaggle. There is limited working with this dataset till right now, according to our study. This dataset is consist of diverse images of real people. We obtained optimal results. We used VGG16, DENSENET201, RESNET50 and InceptionV3. We get the best training and testing outcomes with RESNET50. We had objectified to get results of a specific person without training system on their images.

References

References

[1] N. Khatri, V. Borar and R. Garg, "A Comparative Study: Deepfake Detection Using Deep-learning," 2023 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2023, pp. 1-5, doi: 10.1109/Confluence56041.2023.10048888.

[2] J. Zhang, K. Cheng, G. Sovernigo and X. Lin, "A Heterogeneous Feature Ensemble Learning based Deepfake Detection Method," ICC 2022 - IEEE International Conference on Communications, Seoul, Korea, Republic of, 2022, pp. 2084-2089, doi: 10.1109/ICC45855.2022.9838630.

[3] K. Jayakumar and N. Skandhakumar, "A Visually Interpretable Forensic Deepfake Detection Tool Using Anchors," 2022 7th International Conference on Information Technology Research (ICITR), Moratuwa, Sri Lanka, 2022, pp. 1-6, doi: 10.1109/ICITR57877.2022.9993294.

[4] J. John and B. V. Sherif, "Comparative Analysis on Different DeepFake Detection Methods and Semi Supervised GAN Architecture for DeepFake Detection," 2022 Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Dharan, Nepal, 2022, pp. 516-521, doi: 10.1109/I-SMAC55078.2022.9987265.

[5] S. S. Chauhan, N. Jain, S. C. Pandey and A. Chabaque, "Deepfake Detection in Videos and Picture: Analysis of Deep Learning Models and Dataset," 2022 IEEE International Conference on Data Science and Information System (ICDSIS), Hassan, India, 2022, pp. 1-5, doi: 10.1109/ICDSIS55133.2022.9915885.

[6] D. Stephen and T. Mantoro, "Usage of Convolutional Neural Network for Deepfake Video Detection with Face-Swapping Technique," 2022 5th International Conference of Computer and Informatics Engineering (IC2IE), Jakarta, Indonesia, 2022, pp. 22-28, doi: 10.1109/IC2IE56416.2022.9970025.

[7] Y. Patel et al., "An Improved Dense CNN Architecture for Deepfake Image Detection," in IEEE Access, vol. 11, pp. 22081-22095, 2023, doi: 10.1109/ACCESS.2023.3251417.

[8] M. S. Rana, M. N. Nobi, B. Murali and A. H. Sung, "Deepfake Detection: A Systematic Literature Review," in IEEE Access, vol. 10, pp. 25494-25513, 2022, doi: 10.1109/ACCESS.2022.3154404.