# A PROJECT REPORT

on

# "DEEPFAKE DETECTION"

# Submitted to KIIT Deemed to be University

# In Partial Fulfilment of the Requirement for the Award of

# BACHELOR'S DEGREE IN COMPUTER SCIENCE ENGINEERING

# BY

Kunal Kishore	21051060
Priyanshu Gupta	2105393
Sanskar Shukla	21051247
Riya Singh	21052783
Siddhant Kumar	21052970

UNDER THE GUIDANCE OF Prof. Sujoy Dutta



SCHOOL OF COMPUTER ENGINEERING
KALINGA INSTITUTE OF INDUSTRIAL TECHNOLOGY
BHUBANESWAR, ODISHA - 751024
April 2024

# KIIT Deemed to be University

School of Computer Engineering Bhubaneswar, ODISHA 751024



# **CERTIFICATE**

This is certify that the project entitled

# "DEEPFAKE DETECTION"

# submitted by

Kunal Kishore	21051060
Priyanshu Gupta	2105393
Sanskar Shukla	21051247
Riya Singh	21052783
Siddhant Kumar	21052970

is a record of bonafide work carried out by them, in the partial fulfilment of the requirement for the award of Degree of Bachelor of Engineering (Computer Science & Engineering OR Information Technology) at KIIT Deemed to be university, Bhubaneswar. This work is done during year 2023-2024, under our guidance.

Date: 07/04/2024

Prof. Sujoy Dutta Project Guide

# Acknowledgements

We are profoundly grateful to **Prof. Sujoy Dutta** of KIIT Deemed to be Unive rsity for his expert guidance and continuous encouragement throughout to see t hat this project meets its target from its commencement to completion. We also extend our thanks to the university, for giving us this opportunity to apply our knowledge and creativity in creating and developing this project.

Kunal Kishore Priyanshu Gupta Sanskar Shukla Riya Singh Siddhant Kumar

# **ABSTRACT**

Deepfake technology has become a major problem in recent years due to its ability to deceive and manipulate people by creating fake videos. As technology is used, more in-depth findings are needed to reduce the risks it poses to various areas such as politics, journalism and personal privacy. This research paper aims to investigate the role of artificial intelligence (AI) in deep search to tackle this problem and present new solutions for the same.

This research uses the power of artificial intelligence technology (specifically deep learning algorithms) to create a system that can truly distinguish real and manipulated media.

Preliminary results show that AI-based deep sensing performance and detection accuracy have increased significantly compared to traditional methods. The plan should address problems arising from the development of technology. Additionally, this research paper discusses the limitations of the current framework and suggests avenues for further development, such as the incorporation of artificial intelligence techniques such as differential communication (GAN) and tracking systems.

In summary, this research paper enables participation in deep research by using the power of artificial intelligence to create a strong foundation. Through the use of deep learning algorithms and comprehensive data, the proposed approach should provide insight and reduce the risks associated with these rapid updates.

**Keywords:** deepfake detection, artificial intelligence, deep learning algorithms, dataset evaluation future development.

# Contents

1	Intro	duction		1
2	Dog	o Cono	onto/Litorotura Daviovy	2
2	2.1		epts/ Literature Review hture Review	2
	2.2		nine Learning and Data Analysis	2
	2.3		eling Techniques	3
	2.4		lusion	3
	2.4	Conci	tusion	3
3	Prob	lem Sta	tement / Requirement Specifications	4
	3.1	Projec	ct Planning	4
	3.2	Proje	ect Analysis (SRS)	4
	3.3	Syste	m Design	5
		3.3.1	Design Constraints	5
		3.3.2	System Architecture	5
4	_	ementat		6
	4.1	Metho		6
	4.2	Trainir	-	6
	4.3	Testing		7
	4.4	Result	Analysis	7
5	Stand	dard Ad	onted	9
	5.1		Standards	9
	5.2		g Standards	10
	5.3		g Standards	10
6	Conc	lusion a	and Future Scope	12
	6.1	Conclu	ision	12
	6.2	Future	Scope	12
F	Refere	nces		14
1	101010	11005		17
Inc	lividu	al Conti	ribution	15
Pla	ıgiaris	m Repo	ort	20

# Introduction

The growth of deepfakes in today's digital age has raised serious concerns about the control and fraud of multimedia content. Deepfakes are electronic devices created using artificial intelligence (AI) technology that can undermine credibility, reveal misinformation, and have serious consequences for many locations. As deepfake technology continues to evolve, effective detection methods are urgently needed to prevent its effects. This research paper explores the role of artificial intelligence in deep search and offers new methods to address gaps in existing systems.

As artificial intelligence increases, facial recognition becomes easier and allows the creation of fake videos that are difficult to recognize the difference between actual and manipulated content. These hoaxes can be used to manipulate public opinion, insult people, and even influence the political landscape. As many events in recent years have shown, the potential for violence and destruction is real. Therefore, a strong and reliable deepfake detection system needs to be developed to avoid the disadvantages of this technology.

To solve this challenge, our aim is to use the power of artificial intelligence, especially in deep learning, to create effective and accurate results in deeper searches. By analyzing images and body movements in videos, our aim is to distinguish between real and fake content, thus reducing the risks associated with deepfake communication. We will build on existing research and use the latest advances in artificial intelligence to improve the detection capabilities of deep search engines and improve their overall performance.

Although several in-depth research methods have been proposed, they are often lacking in many aspects. Subtle and well-crafted deepfakes can be difficult to detect with current techniques, which can lead to false positives. Additionally, many methods require large amounts of resources, making them impractical for content monitoring in large-scale applications. Deep dives are currently underway into the importance of our research in providing better and more effective solutions.

# Basic Concepts/ Literature Review

Deepfake technology involves the creation of synthetic media using AI and machine learning algorithms, posing risks of misinformation and manipulation. Detecting deepfakes is crucial for preserving media integrity and trust. Detection methods include forensic analysis and machine learning algorithms, but they face challenges such as adversarial attacks. Ethical concerns revolve around the potential misuse of deepfakes, prompting efforts in policy-making and public awareness.

### 2.1 Literature Review

Deepfake technology has rapidly emerged as a significant societal concern due to its potential for misinformation and manipulation. Deepfakes, which involve the synthesis of realistic but fabricated audio, video, or images using artificial intelligence (AI) and machine learning algorithms, pose serious threats to the integrity of digital media and public trust. The literature review encompasses various aspects of deepfake technology, including its evolution, detection methods, ethical implications, and future directions.

# 2.2 Machine Learning and Data Analysis

Machine learning plays a central role in deepfake detection, as it enables algorithms to learn patterns and features indicative of manipulation from labeled datasets. Supervised learning approaches, such as CNNs, are commonly used for deepfake detection tasks, where models are trained on a dataset containing both real and fake media samples. Feature extraction techniques, such as facial landmarks detection or optical flow analysis, are employed to extract relevant information from the media input, which is then fed into the model for classification.

Data analysis is crucial for preprocessing and understanding the characteristics of the dataset used for training and testing. Exploratory data analysis (EDA) techniques, such as data visualization and statistical analysis, are employed to gain insights into the distribution of data, identify potential biases or anomalies, and inform preprocessing decisions. Moreover, techniques such as data augmentation may be applied to augment the training dataset and improve the generalization capability of the model.

# 2.3 Modeling Techniques

Modeling techniques in deepfake detection encompass a wide range of approaches, from traditional machine learning algorithms to deep learning architectures. Commonly used models include CNNs, recurrent neural networks (RNNs), and their variants, which are tailored to handle spatial and temporal dependencies in media data. Ensemble methods, such as bagging and boosting, may be employed to combine multiple weak classifiers into a stronger ensemble model, enhancing overall detection performance.

Model evaluation is essential for assessing the performance of deepfake detection models and comparing different approaches. Standard evaluation metrics, such as accuracy, precision, recall, and F1-score, are commonly used to quantify the model's performance on binary classification tasks. Additionally, techniques such as cross-validation and holdout validation are employed to estimate the generalization performance of the model on unseen data and mitigate overfitting.

#### 2.4 Conclusion

The literature review provides a comprehensive overview of deepfake technology, including its evolution, detection methods, ethical implications, and future directions. Deepfakes pose serious threats to the integrity of digital media and public trust, highlighting the importance of developing robust detection methods and mitigation strategies. Future research efforts should focus on addressing existing challenges and advancing interdisciplinary collaborations to safeguard against the harmful effects of deepfake technology.

# Problem Statement / Requirement Specifications

The problem statement for this project revolves around the urgent need to develop effective solutions for detecting and mitigating deepfake media. With the rise of deepfake technology, there is a significant risk of misinformation, manipulation, and privacy breaches in various domains, including journalism, politics, and entertainment.

# 3.1 Project Planning

The project planning phase involves defining the scope, objectives, and timeline for the deepfake detection project. Key activities include:

**Scope Definition:** Clearly define the boundaries and objectives of the project, including the types of deepfake media to be detected and the target platforms for deployment.

**Resource Allocation:** Identify the human and technological resources required for project execution, including personnel, software tools, and hardware infrastructure.

**Timeline Development:** Create a detailed project schedule outlining the sequence of tasks, milestones, and deadlines for each phase of development. Risk Assessment: Identify potential risks and challenges that may impact project delivery, such as data privacy concerns, technical constraints, or regulatory requirements.

# 3.2 Project Analysis

The Software Requirements Specification (SRS) document outlines the functional and non-functional requirements for the deepfake detection system. Key components include:

**Functional Requirements:** Specify the system's capabilities and functionalities, such as media ingestion, feature extraction, model training, and real-time detection.

**Non-functional Requirements:** Define quality attributes such as performance, scalability, reliability, and security, ensuring that the system meets or exceeds industry standards.

**Use Cases:** Document detailed use cases illustrating how users interact with the system to perform various tasks, such as uploading media files, initiating detection scans, and reviewing detection results.

# 3.3 System Design

# 3.3.1 Design Constraints

Design constraints refer to limitations or restrictions that must be considered during the system design phase. Key constraints for the deepfake detection system may include:

**Computational Resources:** Availability of computational resources, including processing power, memory, and storage, may impose constraints on the design and implementation of detection algorithms.

**Data Privacy Regulations:** Compliance with data privacy regulations, such as GDPR or HIPAA, may restrict the collection, storage, and processing of sensitive user data.

**Real-time Processing:** The need for real-time detection may impose constraints on the efficiency and responsiveness of the detection algorithms and system architecture.

# 3.3.2 System Architecture (UML)

The system architecture defines the overall structure and components of the deepfake detection system. It may be represented using UML diagrams or block diagrams to illustrate the relationships between different modules and subsystems, including:

**Data Ingestion:** Module responsible for collecting media content from various sources, such as social media platforms, news websites, and user uploads.

**Preprocessing:** Module for preprocessing media content, including tasks such as data cleaning, normalization, and feature extraction.

Model Training: Module for training deep learning models using labeled datasets of real and fake media samples.

**Real-time Detection:** Module for deploying trained models to perform real-time detection of deepfake media, including online streaming and batch processing capabilities.

**User Interface:** Module for providing a user-friendly interface for interacting with the system, including options for uploading media files, initiating detection scans, and reviewing detection results.

# **Implementation**

The implementation phase of the deepfake detection project involves translating the proposed methodology into executable code, training detection models, conducting testing, and analyzing the results.

# 4.1 Methodology

The methodology employed for deepfake detection combines both traditional computer vision techniques and state-of-the-art deep learning algorithms. The process involves the following steps:

**Data Collection:** Acquire a diverse dataset containing both real and fake media samples, including images, videos, and audio recordings. The dataset should cover a wide range of deepfake manipulation techniques and variations to ensure robust model training.

**Preprocessing:** Preprocess the raw media data to prepare it for training, including tasks such as resizing images, normalizing pixel values, and extracting relevant features. Techniques such as data augmentation may be applied to augment the training dataset and improve model generalization.

**Feature Extraction:** Extract meaningful features from the preprocessed media data to capture distinguishing characteristics of deepfake manipulations. Common features may include facial landmarks, temporal dynamics, and artifact patterns introduced during manipulation..

**Training Strategy:** Train the selected models using the labeled dataset of real and fake media samples. Employ techniques such as transfer learning and finetuning to leverage pre-trained models and adapt them to the specific characteristics of the deepfake detection task.

# 4.2 Training

The training phase involves optimizing the selected deep learning models to accurately distinguish between real and fake media samples. Key steps in the training process include:

**Model Initialization:** Initialize the parameters of the selected deep learning architectures using appropriate initialization techniques.

**Loss Function Selection:** Choose a suitable loss function to quantify the difference between predicted and ground truth labels. Common loss functions for binary classification tasks include binary cross-entropy and hinge loss.

**Optimization Algorithm:** Select an optimization algorithm to minimize the chosen loss function and update the model parameters iteratively. Popular optimization algorithms include stochastic gradient descent (SGD), Adam, and RMSprop.

**Hyperparameter Tuning:** Fine-tune the hyperparameters of the deep learning models, including learning rate, batch size, and regularization parameters, to optimize model performance and convergence speed.

# 4.3 Testing

The testing phase involves evaluating the trained deepfake detection models on an independent dataset to assess their performance and generalization capabilities. Key steps in the testing process include:

**Evaluation Metrics:** Calculate performance metrics such as accuracy, precision, recall, and F1-score to measure the effectiveness of the detection models in correctly identifying real and fake media samples.

**Cross-Validation:** Employ techniques such as k-fold cross-validation to assess the robustness of the trained models and mitigate overfitting.

**Adversarial Testing:** Conduct adversarial testing to evaluate the resilience of the detection models against adversarial attacks designed to evade detection algorithms.

# 4.4 Result Analysis

The result analysis phase involves interpreting the performance metrics obtained during testing and drawing conclusions about the effectiveness of the deepfake detection models. Key aspects of result analysis include:

Performance Comparison: Compare the performance of different detection models using evaluation metrics to identify the most effective approach for deepfake detection. **Generalization:** Assess the generalization capabilities of the trained models across different datasets and manipulation techniques to determine their applicability in real-world scenarios.

**Future Directions:** Based on the result analysis, propose recommendations for future research and development efforts to enhance the effectiveness and robustness of deepfake detection methods.

```
1/1 [=======] - 0s 198ms/step
Predicted likelihood: 0.7237
Actual label: 1
1/1 [======] - 0s 30ms/step
```

Correct prediction: True



# Standards Adopted

# **5.1 Design Standards**

**Modularity:** Design the system with modular components that encapsulate specific functionality. Modularity promotes code reusability, ease of maintenance, and scalability. Adhering to modular design principles allows developers to add, remove, or modify components without affecting other parts of the system.

**Layered Architecture:** Organize the system into layers, each responsible for a specific aspect of functionality. Common architectural layers include presentation, business logic, and data access layers. Layered architecture promotes separation of concerns, making the system easier to understand, test, and maintain.

Loose Coupling: Minimize dependencies between system components to reduce the impact of changes and improve flexibility. Use interfaces and dependency injection to decouple components and promote modularization. Loose coupling enables easier integration with external systems and facilitates unit testing.

**High Cohesion:** Ensure that each module or component has a single, well-defined responsibility. High cohesion within modules makes the system easier to understand and maintain, as each module focuses on a specific task or functionality. Avoid modules that are overly complex or have multiple unrelated responsibilities.

**Scalability:** Design the system to accommodate growth in data volume, user traffic, and feature complexity. Use scalable architecture patterns such as microservices or distributed computing to handle increased workload. Scalable design ensures that the system can adapt to changing requirements and handle larger workloads without performance degradation.

**Documentation:** Document the design decisions, architecture, and implementation details of the system to facilitate understanding, collaboration, and maintenance. Provide comprehensive documentation for developers, administrators, and end-users to ensure that all stakeholders have access to necessary information. Clear and up-to-date documentation reduces misunderstandings and accelerates onboarding of new team members.

# **5.2 Coding Standards**

**Coding Style:** The code should be written in a modular and reusable way to ensure code reusability and maintainability.

**Documentation:** The documentation of the code should be clear and concise, and comments should also be included within the code to explain certain statements and docstrings should be created for functions and classes.

Use of Libraries: Python libraries like TensorFlow, PyTorch, OpenCV, and scikit-learn should be used to leverage the existing functionalities and optimize the code's performance.

**Error Handling:** Implementation of error handlers should be done to handle exceptions and errors that may occur during the execution of the code.

**Testing:** Unit tests should be created to verify that the code is functional and for checking whether the predictive model created is operating as intended or not. School of Computer Engineering, KIIT, BBSR 16 Predicting shelf life of fruits

**Version Control:** Keeping track of changes, working together with the team members, and preserving the record of the project should be done using control systems, such as Git.

**Code Review:** The code should be reviewed to make sure it is well-written and follows the coding guidelines. Along with this, feedback should be taken after review for any changes to be done.

# **5.3 Testing Standards**

**Experiment Tracking:** Experiment tracking is the process used for systematically organizing and managing machine learning experiments, which includes parameters, metrics, and results, using tools such as MLflow or Neptune. These technologies help to provide a single platform that records the experiment details, which makes it easier to reproduce, collaborate, and compare several model iterations. To increase model accuracy and generalization, the researchers can easily and efficiently track the model performance over time, spot the patterns, and make datadriven decisions by keeping a clear record of experiments.

**TensorBoard :** TensorBoard is offered by TensorFlow. It is a visualization tool used for examining and tracking deep learning models. It provides tools, which can be used for monitoring training progress, analyzing model performance, and displaying model graphs. Users are able to analyze the model behavior in an insightful manner by visualizing metrics like accuracy, loss curves, and other performance indicators. It makes it possible to visualize the data flow across the computational graph, making it easier to troubleshoot and optimize models. Summary Writer: TensorBoard is used to show the appropriate information that is logged during model training in TensorFlow's

**Summary Writer:** tool. Various metrics, including gradients, activations, loss values, and accuracy, can be recorded by users to monitor the model's behavior and performance over time. Researchers can better understand the training process, spot possible problems, and make decisions for enhancing the model's performance by using the Summary Writer.

# Conclusion and Future Scope

## 6.1 Conclusion

In conclusion, adhering to design standards is crucial for the successful development of a deepfake detection system. By following established principles such as modularity, layered architecture, loose coupling, and high cohesion, developers can create a system that is robust, maintainable, and scalable. These design standards promote code reusability, ease of maintenance, and flexibility, enabling developers to adapt to changing requirements and handle increasing complexity.

Furthermore, integrating security measures into the design of the system is essential for protecting against threats such as data breaches and unauthorized access. By following secure coding practices and adhering to security standards, developers can mitigate security risks and safeguard sensitive information. Effective error handling mechanisms and comprehensive documentation are also critical aspects of system design. Robust error handling ensures that the system can gracefully handle unexpected situations, while clear documentation facilitates understanding, collaboration, and maintenance.

In essence, design standards serve as guiding principles for creating a deepfake detection system that is reliable, secure, and user-friendly. By incorporating these standards into the development process, developers can build a system that meets the needs of users and stakeholders while minimizing risks and vulnerabilities associated with deepfake technology.

# **6.2 Future Scope**

The future scope of the deepfake detection project is promising, with several avenues for further research, development, and enhancement. Here are some potential directions for future exploration:

**Advanced Detection Techniques:** Continued research into advanced detection techniques, such as leveraging reinforcement learning, graph neural networks, or attention mechanisms, could improve the accuracy and robustness of deepfake detection models. Exploring novel feature extraction methods and fusion strategies may also enhance detection capabilities across different media modalities.

Adversarial Defense Mechanisms: Developing effective adversarial defense mechanisms to counteract sophisticated adversarial attacks aimed at evading detection algorithms is essential. Research into adversarial training techniques, robust optimization strategies, and adversarial data augmentation may help improve the resilience of deepfake detection models against adversarial manipulation.

**Real-time Detection Systems:** Developing real-time deepfake detection systems capable of identifying and flagging suspicious media content as it emerges online is crucial for combating the rapid spread of deepfake misinformation. Research into efficient streaming algorithms, edge computing solutions, and parallel processing techniques may enable scalable and responsive real-time detection capabilities.

**Deployment and Integration:** Integrating deepfake detection systems into existing platforms and services, such as social media platforms, news websites, and multimedia archives, could help mitigate the spread of deepfake misinformation at scale. Developing user-friendly APIs, SDKs, and plugins for seamless integration with third-party applications may facilitate widespread adoption of deepfake detection technology.

**Privacy-Preserving Solutions:** Designing privacy-preserving deepfake detection solutions that prioritize user privacy and data protection is critical. Research into secure and decentralized architectures, differential privacy techniques, and federated learning approaches may enable deepfake detection without compromising user privacy or exposing sensitive information.

**Education and Awareness:** Increasing public awareness and understanding of deepfake technology and its potential risks is essential for building resilience against deepfake manipulation. Educational initiatives, awareness campaigns, and interactive tools for detecting and debunking deepfakes may empower individuals to critically evaluate media content and mitigate the impact of deepfake misinformation.

# References

- [1] DeepFake detection Paper with Code https://paperswithcode.com/task/deepfake-detection
- [2] Md Shohel Rana, Mohammad Nur Nobi, Beddhu Murali, Andrew H. Sung "A Systematic Literature Review IEEE"

https://ieeexplore.ieee.org/document/9721302

[3] Arash Heidari, Nima Jafari Navimipour, Hasan Dag, Mehmet Unal "Deepfake detection using deep learning methods"

https://wires.onlinelibrary.wiley.com/doi/full/10.1002/widm.1520

[4] Jia Wen Seow , Mei Kuan Lim , Raphaël C.W. Phan , Joseph K. Liu "A comprehensive overview of Deepfake: Generation, detection, datasets, and opportunities" <a href="https://www.sciencedirect.com/science/article/pii/S0925231222012334">https://www.sciencedirect.com/science/article/pii/S0925231222012334</a>

#### **DEEPFAKE DETECTION**

## KUNAL KISHORE 21051060

#### **Abstract:**

The aim of the project is to develop a robust deepfake detection system using machine learning techniques to mitigate the spread of manipulated media content. The objective is to design and implement an effective solution capable of accurately identifying deepfake images, videos, and audio recordings, thus enhancing media integrity and trustworthiness in the digital landscape.

## **Individual contribution and findings:**

The individual contribution to the project involved researching and implementing machine learning algorithms for deepfake detection, conducting experiments, and analyzing results. The findings revealed the effectiveness of the proposed detection methods in accurately identifying manipulated media content, contributing to the advancement of deepfake detection technology. An IEEE file of the project was created to document the research, methodology, results, and conclusions following IEEE standards for conference proceedings or journal publications.

# **Individual contribution to project report preparation:**

Contributed to Chapter 3: Problem Statement/Requirement Specifications; the Project Planning that included the steps for model creation, project analysis, and system design, where design constraints were described and the block diagram of the code was made.

### **Individual contribution for project presentation and demonstration:**

The individual provided substantial assistance in crafting the introduction and abstraction parts of the project presentation. During the demonstration, they effectively communicated the project's abstract concepts. Their contribution played a pivotal role in setting the stage for the presentation and facilitating comprehension of the project's goals and significance.

Full Signature of Supervisor:	Full signature of the student:

#### **DEEPFAKE DETECTION**

## PRIYANSHU GUPTA 2105393

#### **Abstract:**

The aim of the project is to develop a robust deepfake detection system using machine learning techniques to mitigate the spread of manipulated media content. The objective is to design and implement an effective solution capable of accurately identifying deepfake images, videos, and audio recordings, thus enhancing media integrity and trustworthiness in the digital landscape.

## **Individual contribution and findings:**

Prepared the collected data for testing and training. Used Python script to import the downloaded images into a singular folder to compress all the images; these compressed images were further saved in another folder for easier access. Also, used another Python script to split the final data into two datasets, which were used for training and testing. At last, loaded all the finalized data on GitHub and also imported them to Colab Notebook.

# **Individual contribution to project report preparation:**

Contributed to Chapter 1: Introduction, giving an overview of the problem statement at hand and the solution provided, and Chapter 2: Basic Concepts/Literature Review of the project report by providing details about the machine learning, deep learning and data analysis techniques used.

## **Individual contribution for project presentation and demonstration:**

The individual made significant contributions to the project presentation by focusing on the objective and methodology sections. They meticulously outlined the project's goals, defining clear objectives and explaining the chosen methodologies. During the demonstration, they elucidated the steps involved in the project's execution, providing a comprehensive overview of the methodology used.

Full Signature of Supervisor:	Full signature of the student:
••••••	

#### **DEEPFAKE DETECTION**

## SANSKAR SHUKLA 21051247

#### **Abstract:**

The aim of the project is to develop a robust deepfake detection system using machine learning techniques to mitigate the spread of manipulated media content. The objective is to design and implement an effective solution capable of accurately identifying deepfake images, videos, and audio recordings, thus enhancing media integrity and trustworthiness in the digital landscape.

## **Individual contribution and findings:**

The individual made significant contributions to the project by conducting a comprehensive review of existing literature on deepfake detection techniques and methodologies. Additionally, they provided valuable insights and guidance during the coding phase of the project, contributing to the implementation of machine learning algorithms for deepfake detection. The findings of the review paper highlighted key trends, challenges, and advancements in deepfake detection, offering valuable insights for researchers and practitioners in the field.

## **Individual contribution to project report preparation:**

Contributed to Chapter 4: Implementation, the methodology used, training and testing of the model, and result analysis of the entire model, and Chapter 6: Conclusion and Future Scope, along with proofreading of the entire report.

## **Individual contribution for project presentation and demonstration:**

The individual contributed to the project presentation by highlighting the libraries used in the development process. They provided valuable insights into the selection and utilization of relevant libraries, explaining their importance in implementing specific functionalities. During the demonstration, they showcased the integration of these libraries, demonstrating their role in enhancing the project's capabilities.

Full Signature of Supervisor:	Full signature of the student:

#### **DEEPFAKE DETECTION**

RIYA SINGH 21052783

#### **Abstract:**

The aim of the project is to develop a robust deepfake detection system using machine learning techniques to mitigate the spread of manipulated media content. The objective is to design and implement an effective solution capable of accurately identifying deepfake images, videos, and audio recordings, thus enhancing media integrity and trustworthiness in the digital landscape.

## **Individual contribution and findings:**

The individual played a pivotal role in crafting a review paper on deepfake detection techniques, consolidating existing literature and synthesizing key findings. Their contribution provided a comprehensive overview of the state-of-the-art methods, challenges, and advancements in the field. By analyzing and synthesizing the research landscape, the review paper shed light on effective strategies for mitigating the spread of manipulated media content, offering valuable insights for future research and development efforts.

## **Individual contribution to project report preparation:**

Contributed to Chapter 5: Standards Adopted; the Design Standards that were used for the actual project to be developed, the Coding Standards that were adopted for the coding process, and the Testing Standards used during the testing of the model using the collected data.

## **Individual contribution for project presentation and demonstration:**

The individual made a substantial contribution to the project presentation by explaining the layers used by Keras, a deep learning library. They elucidated the architecture of the neural network model, detailing the various layers utilized for feature extraction and classification. During the demonstration, they demonstrated the functionality of each layer, showcasing how they contribute to the overall performance of the model.

Full Signature of Supervisor:	Full signature of the student:

#### **DEEPFAKE DETECTION**

## SIDDHANT KUMAR 21052970

#### **Abstract:**

The aim of the project is to develop a robust deepfake detection system using machine learning techniques to mitigate the spread of manipulated media content. The objective is to design and implement an effective solution capable of accurately identifying deepfake images, videos, and audio recordings, thus enhancing media integrity and trustworthiness in the digital landscape.

# **Individual contribution and findings:**

The respected individual made a substantial contribution by creating an IEEE-standard file for the project, ensuring compliance with rigorous academic standards. Additionally, they provided valuable assistance in the coding phase, offering insights and support to the team. Their efforts culminated in a well-documented project report adhering to IEEE guidelines, showcasing the research findings and coding contributions effectively.

# Individual contribution to project report preparation:

Contributed towards writing the Abstract along with formatting and Chapter 6: Conclusion and Future Scope, along with proofreading of the entire report.

# Individual contribution for project presentation and demonstration:

The individual played a crucial role in the project presentation by focusing on result analysis and conclusion sections. They meticulously analyzed the outcomes of the project. During the demonstration, they effectively communicated the significance of the results, highlighting key findings and implications for future work.

Full signature of the student:

# TURNITIN PLAGIARISM REPORT

# DEEPFAKE DETECTION

ORIGIN	LITY REPORT		
	7% 13% INTERNET SOUR	2% PUBLICATIONS	10% STUDENT PAPERS
PRIMAR	/ SOURCES		
1	www.worldleadersh	nipacademy.live	5%
2	Submitted to KIIT U	niversity	2%
3	www.coursehero.co	om	2%
4	kdd.isti.cnr.it Internet Source		1%
5	mdpi-res.com Internet Source		1%
6	Submitted to Manch University Student Paper	nester Metropolit	tan 1 %
7	Submitted to Interc	ollege	1%
8	arxiv.org Internet Source		<1%
9	www.trendytechjou	rnals.com	<1%

10	dblp.dagstuhl.de Internet Source	<1%
11	Submitted to Birla Institute of Technology and Science Pilani Student Paper	<1%
12	Parvataneni Rajendra Kumar, S. Meenakshi, S. Shalini, S. Rukmani Devi, S. Boopathi. "chapter 1 Soil Quality Prediction in Context Learning Approaches Using Deep Learning and Blockchain for Smart Agriculture", IGI Global, 2023 Publication	<1%
13	accentsjournals.org Internet Source	<1%
14	Submitted to Auckland Institute of Studies Student Paper	<1%
15	Submitted to University of Adelaide Student Paper	<1%
16	www.ijert.org Internet Source	<1%
17	Submitted to Fakultet elektrotehnike i računarstva / Faculty of Electrical Engineering and Computing Student Paper	<1%
18	www.powtoon.com Internet Source	<1%

19	Submitted to Oregon State University Student Paper	<1%
20	Submitted to University of Wales Institute, Cardiff Student Paper	<1%
21	www.jetir.org Internet Source	<1%
22	www.onlinesciencepublishing.com Internet Source	<1%
23	Yizhe Zhu, Chunhui Zhang, Jialin Gao, Xin Sun, Zihan Rui, Xi Zhou. "High-compressed deepfake video detection with contrastive spatiotemporal distillation", Neurocomputing, 2023 Publication	<1%
24	Submitted to Washington State University System Student Paper	<1%
25	pure.rug.nl Internet Source	<1%
26	tudr.thapar.edu:8080 Internet Source	<1%
27	www.ijnrd.org Internet Source	<1%
28	Submitted to Dulwich College Singapore Student Paper	<1%

29	Submitted to University of Sydney Student Paper	<1%
30	moam.info Internet Source	<1%
31	www.ijraset.com Internet Source	<1%
32	www.irjmets.com Internet Source	<1%
33	Rami Mubarak, Tariq Alsboui, Omar Alshaikh, Isa Inuwa-Dute, Saad Khan, Simon Parkinson. "A Survey on the Detection and Impacts of Deepfakes in Visual, Audio, and Textual Formats", IEEE Access, 2023	<1%