iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: XII Month of publication: December 2025

DOI: https://doi.org/10.22214/ijraset.2025.76034

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XII Dec 2025- Available at www.ijraset.com

Identification of Fake Faces Using Deep Learning

Dr.Vidyarani HJ, Mrs, Divya S, Mohammed Sameer, Mohammed Armaan, Puneeth SN, Vishal Gowda T R
Computer Science And Business System, DrAit Bengaluru, India

Abstract: The increasing computational power has signifi- cantly enhanced the capabilities of deep learning algorithms, making it easier to generate hyper-realistic fake facial imagesand videos, commonly known as deepfakes. These manipulated media are often linked to harmful scenarios such as political propaganda,identitytheft,blackmail,andthespreadofmisinfor- mation. Thisworkpresentsanoveldeeplearning-basedapproach foridentifyingAI-generatedfakefaces.Ourmethodcombinesthe strengths ofResNeXtConvolutionalNeuralNetworks(CNNs) to extract frame-level features and Long Short-Term Memory (LSTM)-basedRecurrentNeuralNetworks(RNNs)forsequential temporal analysis, enabling accurate classification of fake versus real faces. To ensure robust performance, the model was trained and evaluated on a large, diverse dataset that includes Face-Forensics++, the Deepfake Detection Challenge, and Celeb-DF. The results demonstrate that our simple yet effective approach achieves high accuracy in detecting fake faces, showcasing its potential for combating the misuse of deepfake technology while paving the way for further advancements in this field.

Index Terms: Component, formatting, style, styling, insert

I. INTRODUCTION

The primary goal of this project is to develop an effective systemforidentifyingfakefacesgeneratedusingdeepfake technology.Thisisachievedby leveraging advanceddeep learning architectures specifically designed for analyzing and classifying facial images and videos as real or fake.

The approach integrates ResNeXt Convolutional Neural Networks(CNNs)toextractintricateandhighdimensional features from individual frames of video content.

Additionally, Long Short- Term Memory (LSTM)-based Recurrent Neural Networks (RNNs) are employed to analyze temporal data, capturing sequential patterns and contextual information within video sequences. This combination of CNNs and RNNs ensures robust performance in detecting subtle manipulations that might otherwise go unnoticed. To enhance the real-world applicability and effectivenessofthemodel,adiverseand comprehensive dataset was curated for training. This datasetincludesFaceForensics++,theDeepfakeDetection Challenge dataset, and Celeb-DF, which collectively provide a wide range of real and fake content. By combining these datasets, the system is trained to generalize across different scenarios and adapt to unseen fake generation techniques, ensuring its reliabilityagainst evolvingdeepfakemethods.Thefinalsystemisintegratedinto a user-friendly application, allowing users to upload videos foranalysis.Theapplicationprocessestheinputandgenerates a detailed report, indicating whether the video containsfake facesandprovidingaconfidencescore.This practical solution bridges advanced technology and usability, making deepfake detection accessible to a broad audience.

II. LITERATURE SURVEY

Researchindeepfakedetectionhasseensignificantadvance- ments, with several studies contributing valuable insights into identifying fake faces using deep learning methods.

Ahmed H. Khalifa *et al.* [1] proposed a framework named DSLRFN(DualScaleLocalReceptiveFieldNetwork)intheir study, *"Convolutional Neural Network Based on Diverse Ga- borFilters for Deepfake Recognition."* Thismethod leverages Gabor filters to extract spatial-spectral features, enhancing deepfakeimagerecognition.However,thecomplexityofthese filters makes interpreting the learned features challenging.

Eunji Kim and Sungzoon Cho [2] introduced a hybrid approach in *"Exposing Fake Faces Through DNN Combining ContentandTraceFeatureExtractors."*Thisframeworkcom- bines content and trace feature extraction using Convolutional Neural Networks (CNNs) to detect manipulations in facial media, such as DeepFake and Face2Face. While effective, the study focuses primarilyon experimental evaluations and lacks detailed exploration of feature interpretability.

Sani M. Abdullahi *et al.* [3], in their work *"DeepFake Detection for Human Face Images and Videos,"* explored various techniques for detectingfake faces in both imagesand videos. Their study highlights the use of deep neural networks,includingcapsulenetworksandadversarialmethods, to improve detection accuracy.

However, these methods are computationally intensive, which poses challenges for real- time applications.

S. Agarwal *et al.* [4] employed Long Short-Term Memory (LSTM) networks in their study, *"Detecting Deepfake Videos UsingRecurrentNeuralNetworks,"*forsequentialanalysis of video frames. By leveraging temporal inconsistencies in deepfake videos, this approach achieves improved accuracyfor dynamic content but requires substantial computational resources for frame-level processing.

YuezunLi,Ming-ChingChang,andSiweiLyu[5]proposed a novel approach to detect AI-generated fakevideos by focus- ingonabnormaleyeblinkingpatterns.Theirmethodleverages theabsenceorirregularityofeyeblinksinsyntheticvideos to identify deepfakes effectively. This approach provided a unique angle for exposing AI-generated manipulations.

Li, Y., *et al.* [6] introduced Celeb-DF, a high-qualitydataset for deepfake forensics, addressing limitations in ex- isting datasets. Their work emphasized the dataset's realism and diversity, making it a valuable resource for training and evaluating deepfake detection models.

Deng Pan *et al.* [7] explored deepfake detection using deep learning techniques, presenting a framework that combines Convolutional NeuralNetworks (CNNs) forfeatureextraction withclassifiersforeffectiveidentification.Theirworkdemon- strated improved performance on benchmark datasets.

AsadMalik*etal.*[8]proposedadeepfakedetectionsystem focusingonhumanfaceimagesandvideos,utilizingadvanced deep neural network architectures. Their approach achieved competitiveaccuracyandrobustness,addressingchallengesin real-time application scenarios.

Md. Shohel Rana *et al.* [9] investigated machine learning algorithms for deepfake detection, evaluating models such as Support Vector Machines (SVM) and Random Forests. Their study highlighted the potential of traditional machine learning methods alongside deep learning approaches.

NishikaKhatri*etal.*[10]conductedacomparativestudy of deepfake detection using various deep-learning models, analyzing performance metrics such as accuracy and scala- bility. Their findings provided insights into the strengths and limitations of different architectures for deepfake detection.

Video processing and denoising are critical areas of re- search, particularly in applications involving video surveil- lance, broadcasting, and multimedia communication. Signif- icant contributions in this domain have focused on motion detection and noise reduction techniques, as outlined below:

Reeja, S. R., and Dr. N. P. Kavya [11], in their paper *"Motion Detection for Video Denoising–The State of Art and the Challenges,"* reviewed the methodologies employed in motion detection for video denoising. The authors highlighted the importance of motion estimation in improving the quality of noisy video sequences. They explored various techniques, including block-matching algorithms and optical flow, em- phasizing their strengths and limitations. However, the study pointed out challenges such as computational complexity, scalability to higher resolutions, and sensitivity to varying noise levels. This paper served as a foundational work for understanding the interplay between motion detection and noise reduction.

In a related study, Reeja, S. R., and Dr. N. P. Kavya [12] proposedadetailedanalysisofnoisereductiontechniques in video sequences in their work *"Noise Reduction in Video*

Sequences: The State of Art and the Technique for Motion Detection." The authors examined different noise models and theirimpactonvideoquality.Theyproposedmotiondetection as a key strategy to isolate dynamic areas in video frames, enablingtargetednoisereduction. Thepaperprovidedinsights into techniques like temporal averaging,Kalman filtering,and wavelet-based methods. The authors also identified open challenges, such as balancing denoising performance with computationalefficiencyandpreservingthestructuralintegrity of the video.

These studies collectively highlight advancements in deep- fakedetectionandvideoprocessingusingdeeplearning,while addressing challenges such as interpretability, scalability, and computational feasibility for real-world applications.

III. METHODOLOGY

This project leverages advanced deep learning architectures to detect fake facial media with high accuracy. The method- ology consists of the following key components:

A. Data Collection and Preprocessing

The systemis trained onpublicly availabledatasets,includ- ingFaceForensics++,DeepfakeDetectionChallenge(DFDC), and Celeb-DF, ensuring diversity and robustness against var- ious manipulation techniques. Preprocessing involves split- ting videos into frames, detecting and cropping faces using OpenCV, and resizing the frames to 112×112pixels.

These steps minimize noise and emphasize facial features critical for detection.

Usingthesedatasetsensuresthatthemodelistrainedon a wide variety of scenarios and manipulation methods, which enhances its generalization ability.

Preprocessing is an essential step in preparing data for machinelearningmodels.Itfocusesonimprovingdataquality by reducing noise and ensuring the input is suitable for the model.

1) SplittingVideosintoFrames

Why: Videos contain temporal data, but deepfake detec- tion often relies on individual frames to analyze facial details. Splitting videos into frames makes it easier to process and analyze each frame separately.

2) DetectingandCroppingFacesUsingOpenCV

Why:Facesarethekeyareastofocusonfordeepfakede- tection because manipulation often affects facial regions. OpenCV provides efficient methods for face detection and cropping, suchasHaar cascades, DNN(Deep Neural Networks), or other pre-trained models.

3) ResizingFrames

Why: Resizing frames to a consistent size (e.g., 112 × 112 pixels) standardizes input dimensions for the model. This minimizes variations in image sizes, which could lead to inconsistencies in feature extraction and reduces computational overhead.

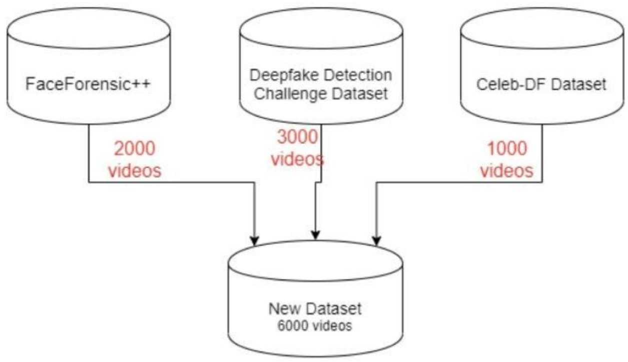


Fig.1.Dataset.

B. ModelArchitecture

The detection system integrates ResNeXt Convolutional Neural Networks (CNNs) for feature extraction and Long Short-Term Memory (LSTM) networks for temporal analysis. ResNeXtcapturesspatialinconsistenciesinindividualframes, while LSTM identifies temporal anomalies across sequential frames, enabling robust detection of manipulations.

C. ResNeXtConvolutionalNeuralNetworks (CNNs)

Purpose: ResNeXt is a powerful CNN architecture that excels in capturing spatial features, especially spatial incon- sistencies within individual frames.

KeyFeatures:-FeatureExtraction:ResNeXtisdesigned to efficiently extract features from images by using parallel pathways with different filter sizes, which allows it to capture a wide range of spatial details.

- Handling Manipulations: In deepfake detection, manip- ulated frames often exhibit inconsistencies (e.g., unnatural facial expressions, blurring artifacts, or inconsistencies inskin texture). ResNeXt helps identify these inconsistencies by analyzing the visual features across multiple layers.

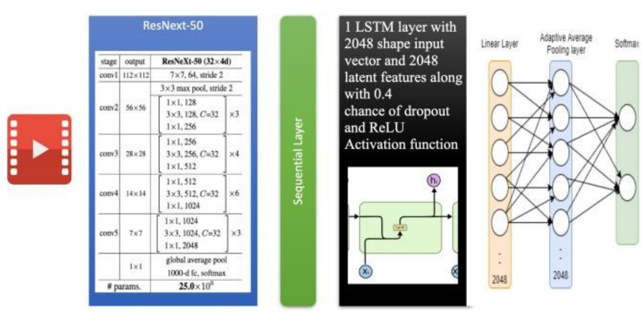


Fig.2.ModelArchitecture

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XII Dec 2025- Available at www.ijraset.com

D. LongShort-Term Memory(LSTM)Networks

Purpose: LSTM networks are specifically designed to han- dle sequential data, which is critical for deepfake detection in videoswheremanipulationtechniquesofteninvolvealterations across multiple frames.

Key Features: - Temporal Analysis: LSTMs process se- quences of frames, identifying patterns and changes overtime, such as unnatural transitions or inconsistencies in facial motion.

-RobustDetection:Byexaminingtemporalpatterns,LSTM networks can differentiate between natural variations and ma- nipulations, such as smoothly transitioning facial expressions versus abrupt or unrealistic changes.

Hereisthesystemarchitecture:

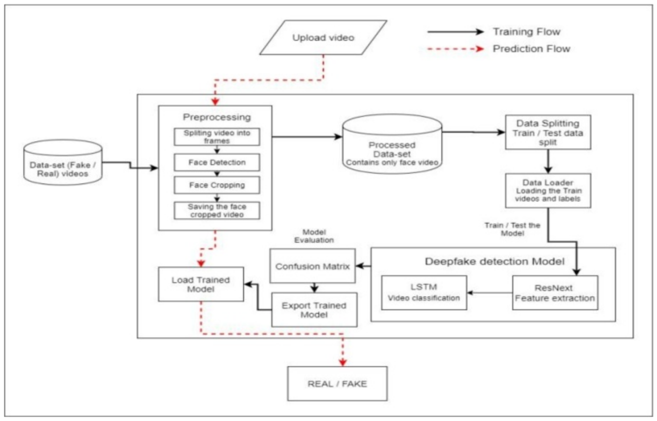


Fig.3.SystemArchitecture

E. Training andOptimization

The preprocessed data is divided into training, validation, and testing subsets in a 70 : 15 : 15 ratio. The model is optimized using cross-entropy loss and the Adam optimizer. Hyperparameter tuning is conducted to refine the learningrate, batch size, and number of epochs. Data augmentation techniques, including random rotations and flips, are appliedto enhance generalization.

F. Evaluation

The model is evaluated using metrics such as accuracy, precision,recall,andF1-score.Aconfusionmatrixisused to visualize performance and identify areas for improvement. Generalizationisvalidatedonunseendatasets,ensuringadapt- ability to diverse deepfake techniques.

G. Implementation Tools

The system utilizes PyTorch for model development, OpenCV for video processing, and Google Cloud Platform (GCP) for high-performance training. These tools streamline the pipeline from preprocessing to real-time detection.

H. OutputandUserInterface

Thefinalsystemintegratesaweb-basedinterfacebuiltusing DjangoandHTML/CSS,allowinguserstouploadvideos for analysis. The system provides a classification (real orfake) with a confidence score, ensuring accessibility for non- technical users.

This methodology effectively combines preprocessing, spa- tial and temporal feature extraction, and real-time application, resulting in a robust and scalable deepfake detection system.

IV. ANALYSIS

A. Solution Requirement

Weanalyzedtheproblemstatementandfoundthefeasibility of the solution to the problem. We referred to different research papers as mentioned in Section 3.3. After checking the feasibility of the problem statement, the next step was dataset gathering and analysis.

Weanalyzedthedatasetusingdifferenttrainingapproaches, such as negatively or positively trained models (i.e., training the model with only fake or real videos). However, we found thatthisapproachmayleadtotheadditionofextrabiasin the model, resulting in inaccurate predictions. After extensive research,weconcluded thatbalanced trainingofthealgorithm is the best way to avoid bias and variance, thereby achieving good accuracy.

B. SolutionConstraints

Weanalyzedthesolutionintermsof:

- Cost
- Speedofprocessing
- Requirements
- Levelofexpertise
- Availabilityof equipment

C. ParametersIdentified

Thefollowingparameterswereidentifiedfordetecting inconsistencies in deepfake videos:

- Blinkingofeyes
- Teethenhancement
- Biggerdistancebetweeneyes
- Moustaches
- Doubleedges(eyes,ears,nose)
- Irissegmentation
- Wrinklesontheface
- Inconsistentheadpose
- Faceangle
- Skintone
- Facialexpressions
- Lighting
- Differentposes
- Doublechins
- Hairstyle
- Highercheekbones

D. StepsinTestingWorkflow

1) UserVideo:Theuseruploadsavideoforanalysis. The system ensures the uploaded file is valid, typically checking the file format (e.g., .mp4, .avi) and size limits. The video is queued for preprocessing to extract frames and detect features.
2) Preprocessing:

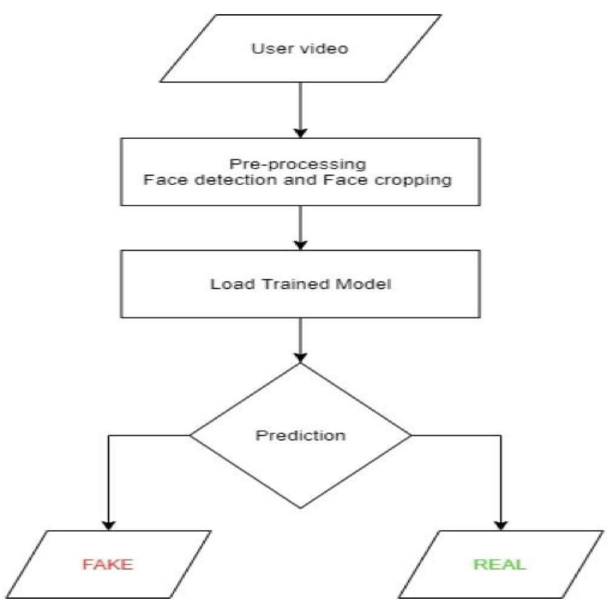


Fig.4.Processflow.

- The video is split into individual frames. This step converts the temporal video data into sequential images.
- Faces are detected in each frame using tools like OpenCV, ensuring only relevant regions (faces) are analyzed.
- The detected faces are cropped and resized to a uniform size (e.g., 112 × 112 pixels) to standardize the input for the deep learning model.

3) Load TrainingModel:
- The pre-trained deepfake detection model (combin- ingResNeXt and LSTM) is loaded.
- The ResNeXt component processes each frame to extractspatialfeatures, whiletheLSTMcomponent analyzes sequential patterns across frames.

4) Prediction:
- Theprocessedframesarepassedthroughthemodel.
- The ResNeXt extracts visual features, such as ar- tifacts, inconsistencies, or manipulations in facial regions.
- The LSTM evaluates temporal patterns, looking for irregularities in motion, expressions, or transitions acrossframes.
- The final output is a binary classification (e.g., Realor Fake) or a confidence score indicating the likelihood of the video being a deepfake.

V. RESULTS

The proposed deepfake detection system was thoroughly evaluated, showcasing itsefficiency and accuracy in detecting manipulated videos. Below are the key results and observa- tions:

A. Model Accuracy

Thetrainedmodeldemonstratedsignificantaccuracyacross multiple datasets and configurations:
- FaceForensics++Dataset:Achieved97.76%accuracy with 100-frame sequences.
- CombinedDataset(Celeb-DF+FaceForensics++):Achieved93.97%accuracywith100-framesequences.
- CustomDataset:Accuracyvariedfrom84.21%(10- frame sequences) to 89.34% (40-frame sequences).

B. Evaluation Metrics

Theperformanceofthemodelwasmeasuredusingstandard metrics:
- Precision:Thesystemeffectivelyminimizedfalseposi- tives.
- Recall:Demonstratedahighrecallrate,accuratelyde- tecting fake videos.
- F1-Score:Maintainedastrongbalancebetweenprecision and recall.

C. ConfusionMatrixAnalysis

Theconfusionmatrixindicated:
- Hightruepositiveratesfordeepfakevideos.
- Minimalfalsenegatives,ensuringreliabledetectionof fake content.

D. OutputVisualization

Thesystemprovidedclearoutputsforuser-uploadedvideos:
- RealVideos:Correctlyclassifiedwithhighconfidence.
- Fake Videos:Detected withdetailed confidencescores, ensuring transparency.

E. Model Efficiency

Thesystemprocessedvideosat10framespersecond, bal- ancingreal-timeperformancewithcomputationalefficiency.

F. Real-World Testing

The model performed effectively on real-world videos sourced from platforms like YouTube, ensuring generalizabil- ity across various scenarios.

G. UserInterfaceEvaluation

The developed web application was intuitive and user- friendly, allowing users to upload videos for analysis and receive classification results with confidence scores.

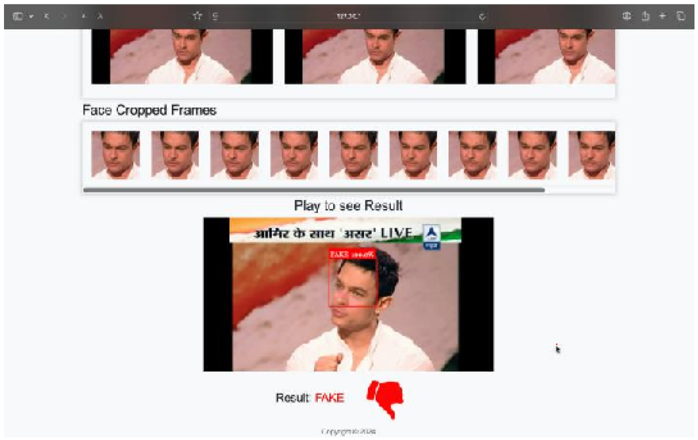


Fig.5.DetectionResult:FAKE.

H. Conclusion

The resultsdemonstrate the robustnessand reliability of the system, providing a scalable solution for real-time deepfake detection.

VI. CONCLUSION AND FUTURE SCOPE

A. Conclusion

Theprojectfocusesonthedevelopmentandimplementation of a highly effective ”Deepfake Detection System” to address the growing challenge of identifying manipulated media. The systemleveragesadvancedtechnologies,includingdeeplearn- ing frameworks, computer vision, and neural networks, to ac- curately detectfakefacesin videoswithreal-timecapabilities. Its objective is to provide a robust solution for distinguishing between real and fake faces, enabling practical applications in fieldssuchasmediaverification,security,anddigitalforensics.

System’sCoreFeatures:

1) PreprocessingPipeline:Thesystemintegratesa comprehensive preprocessing pipeline involving video splitting, face detection, and frame resizing to ensure that only relevant facial features are analyzed during detection.
2) Model Architecture: Combines convolutional neu- ral networks (CNNs) and long short-term memory (LSTM) networks to capture both spatial and tem- poral features essential for deepfake detection.
3) Real-Time Detection: Optimized for real-time de- tection, making it suitable for practical applications in live media verification and security contexts.

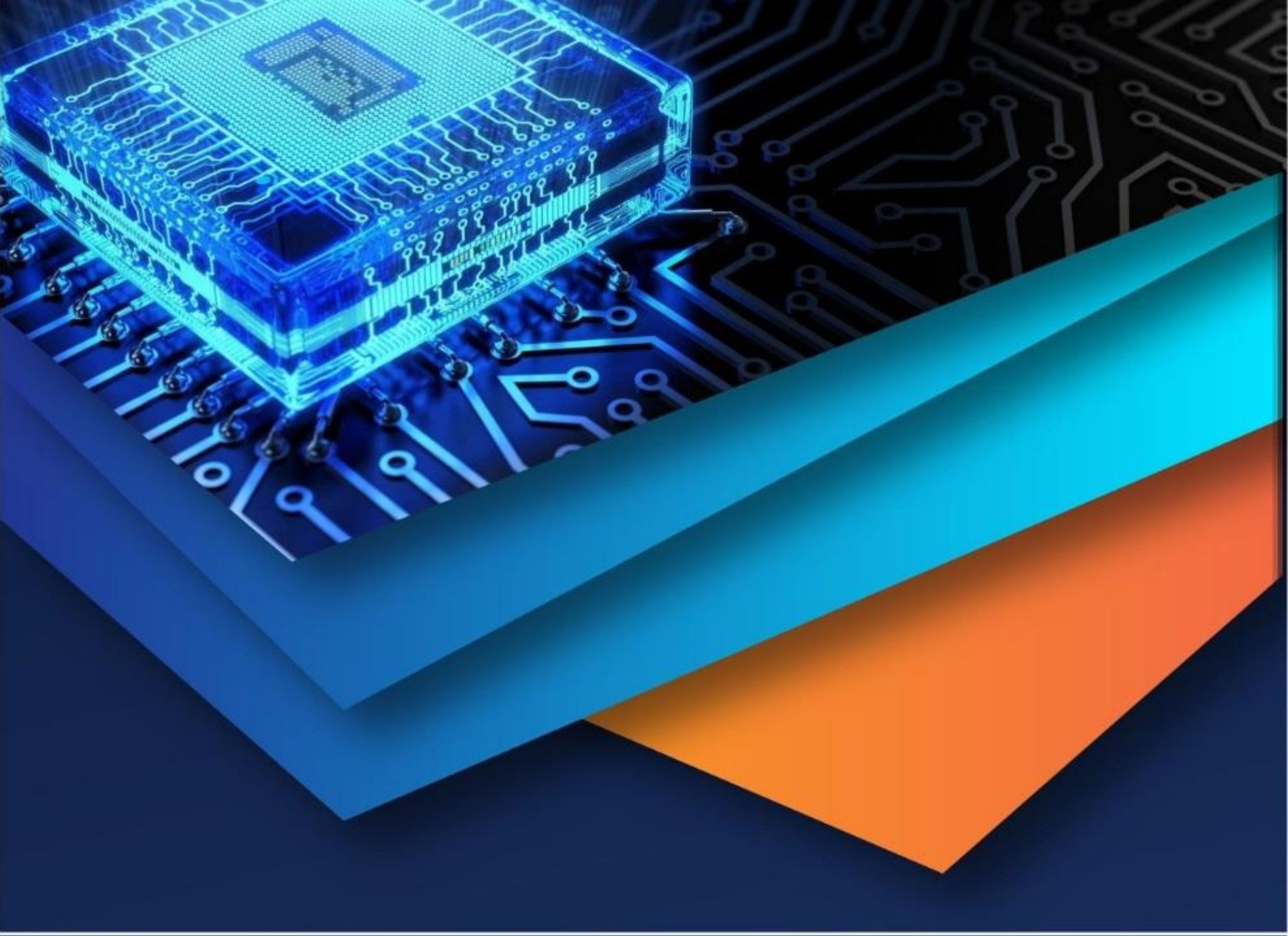
B. Future Scope

1) Improved Detection Accuracy: Further development of the model by incorporating advanced architectures like transformers or hybrid models will help address more sophisticated deepfake techniques, enhancing detection accuracy.
2) Scalability and Real-Time Performance: Optimizing the system to handle larger video streams, such as those used in live broadcasts or security surveillance, is crucial for future advancements to ensure adaptability for real- time, large-scale video analysis.
3) Cross-Domain Detection:Expanding thesystem’scapa- bilitytodetectdeepfakesinotherformsofmedia,suchas audio and text, would provide a comprehensive solution for multimedia deepfake detection.
4) User-Friendly Interface: Enhancing the user interface (UI) to improve ease of use and accessibility for non- technical users will broaden the system’s applicability across various industries, including media, law enforce- ment, and social media platforms.
5) Adversarial Robustness: Developing strategies to train the model with adversarial examples will strengthen its ability to withstand future deepfake generation methods that attempt to bypass detection.

This projectprovides astrongfoundationforcombating the misuse of deepfake technology and offers a scalable solutionforreal-worldapplications,pavingthewayforfurther innovations in this domain.

REFERENCES

[1] A. H. Khalifa et al., “Convolutional neural network based on diversegabor filters for deepfake recognition,” 2022.
[2] E.KimandS.Cho,“Exposingfakefacesthroughdnncombiningcontentand trace feature extractors,” 2021.
[3] S. M. Abdullahi et al., “Deepfake detection for human face images andvideos,”2022.
[4] S. Agarwal et al., “Detecting deepfake videos using recurrent neuralnetworks,”2021.
[5] Zhang et al., “Deepfake detection via temporal and spatial features,”2022.
[6] Liu et al., “Attention mechanisms in deepfake detection: A noveltransformer-based approach,” 2023.
[7] Y. Li, M.-C. Chang, and S. Lyu, “Exposing ai created fake videos bydetecting eye blinking,”arXiv, vol. arXiv:1806.02877v2, 2018.
[8] Y. Li et al., “Celeb-df: A new dataset for deepfake forensics,” arXivPreprint, vol. arXiv:1909.12962, 2019.
[9] D. Pan, L. Sun, R. Wang, X. Zhang, and R. O. Sinnott, “Deepfakedetection through deep learning,” 2020.
[10] A. Malik,M.Kuribayashi, S.M. Abdullahi,and A. N. Khan, “Deepfakedetection for human face images and videos,” 2022.
[11] M. S. Rana, B. Murali, and A. H. Sung, “Deepfake detection usingmachine learning algorithms,” 2022.
[12] N. Khatri, V. Borar, and R. Garg, “A comparative study: Deepfakedetection using deep-learning,” 2023.
[13] S. R. Reeja and N. P. Kavya, “Motion detection for video denoising–the state of art and the challenges,” International Journal of ComputerEngineering Technology (IJCET), vol. 3, no. 2, pp. 518–525, 2012.
[14] “Noise reduction in video sequences: The state of art and thetechnique for motion detection,” International Journal of ComputerApplications, vol. 58, no. 8, pp. 31–36, Nov 2012.



10.22214/IJRASET

INDEX COPERNICUS
45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL
IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY