IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15676

FACIAL FEATURE ANALYSIS FOR DEEPFAKE DETECTION

Vaishnavi J Manoj[1], Aravind A S[2]

Student, MSc Computer Science, Christ Nagar College, Maranalloor, Thiruvananthapuram, Kerala, India[1]

Assistant Professor, PG Department of Computer Science, Christ Nagar College, Maranalloor, Thiruvananthapuram, Kerala, India[2]

Abstract: The rapid advancement of artificial intelligence and deep learning technologies has led to the widespread creation of highly realistic synthetic media known as deepfakes. Deepfake content can manipulate facial expressions, voices, and visual appearances in images, videos, and audio recordings, making it increasingly difficult to distinguish between real and fabricated media. Such manipulations pose serious threats to digital security, privacy, and public trust. This project presents an intelligent deepfake detection system that performs facial feature analysis to identify manipulated multimedia content, including images, videos, and audio.

The proposed system utilizes advanced image processing and deep learning techniques to analyse facial characteristics and detect inconsistencies introduced during deepfake generation. The system employs a hybrid deep learning architecture based on Meso4Net and Capsule Network (CapsuleNet) models, which effectively capture both texture-level artifacts and spatial relationships in facial structures. The detection process involves multiple stages including preprocessing, frame extraction from videos, facial landmark detection, feature extraction, and classification to determine whether the input media is real or manipulated.

Keywords: Deepfake, Deep Learning, Capsule Network, Meso4Net, Artificial Intelligence.

I. INTRODUCTION

The proposed system utilizes advanced image processing and deep learning techniques to analyse facial characteristics and detect inconsistencies introduced during deepfake generation. The system employs a hybrid deep learning architecture based on Meso4Net and Capsule Network (CapsuleNet) models, which effectively capture both texture-level artifacts and spatial relationships in facial structures. The detection process involves multiple stages including preprocessing, frame extraction from videos, facial landmark detection, feature extraction, and classification to determine whether the input media is real or manipulated.

The system is implemented as a desktop application with user-friendly graphical interface modules that allow users to upload images, videos, or audio files for analysis. The application processes the uploaded media by extracting facial features, analysing spatial and temporal patterns, and applying the hybrid deep learning model for accurate classification. For video inputs, frames are extracted and analysed sequentially to identify temporal inconsistencies in facial movements, while audio inputs are analysed using signal processing techniques to detect synthetic voice patterns. The system stores analysis results in a database and presents clear output indicating whether the content is real or fake. By integrating facial feature analysis with hybrid deep learning techniques, the proposed system provides an effective approach for detecting deepfake media across multiple formats. The developed framework contributes to improving digital media authenticity verification, enhancing cybersecurity measures, and reducing the risks associated with manipulated multimedia content.

II. OBJECTIVES

The primary objective of facial feature analysis in a deepfake detection project is to identify manipulated or synthetically generated facial content by examining the visual characteristics of a human face in images or videos. Deepfake technologies use artificial intelligence and deep learning models to create highly realistic fake media, making it increasingly difficult to distinguish between authentic and altered content. Facial feature analysis aims to detect inconsistencies and anomalies that may indicate digital manipulation, thereby improving the reliability and security of multimedia information.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026
DOI: 10.17148/IJARCCE.2026.15676

Another key objective is to analyse both static and dynamic facial attributes such as facial landmarks, eye movements, blinking patterns, lip synchronization, skin texture, head pose, and facial expressions. Genuine facial behaviour follows natural physiological patterns, whereas deepfake-generated content often exhibits subtle irregularities due to limitations in the generation process. By extracting and evaluating these features, the system can identify deviations from authentic human facial characteristics.

III. LITERATURE REVIEW

Traditional deepfake detection approaches have extensively utilized Convolutional Neural Networks (CNNs) to identify facial manipulation artifacts in images and videos. The study by the authors of Lightweight Meso4Net Architecture for Deepfake Detection using FaceForensics++ (2023) proposed an efficient CNN-based Meso4Net model optimized for low computational cost and real-time detection. The model demonstrated strong performance on the FaceForensics++ dataset while maintaining reduced memory requirements, making it suitable for resource-constrained environments.

Several researchers have focused on improving facial feature representation through advanced neural network architectures. The work Capsule Network-Based Deepfake Detection using DeepFake-TIMIT (2022) employed Capsule Networks to preserve spatial relationships between facial features and detect subtle inconsistencies introduced during deepfake generation. Similarly, Capsule Network with Preprocessing Pipeline for Deepfake Image Forensics (2023) integrated face alignment and normalization techniques with Capsule Networks, enhancing robustness against image compression and noise while improving detection accuracy.

Performance evaluation studies have further highlighted the effectiveness of CNN-based architectures for deepfake detection. The paper Performance Evaluation of Meso4Net for Video Deepfake Detection (2023) analysed the capability of Meso4Net in extracting regional facial features from manipulated videos. The study emphasized the importance of assessing model performance under varying video quality and compression conditions, demonstrating the reliability of Meso4Net across different datasets.

Recent research has explored hybrid deep learning approaches to combine the strengths of multiple architectures. The paper FFA-MPDV: A Hybrid Meso4Net and Capsule Network Model for Deepfake Detection (2025) introduced a novel framework that integrates Meso4Net and Capsule Networks for analyzing both spatial and temporal facial features. By capturing subtle deepfake artifacts and preserving detailed facial information, the model achieved high accuracy and robustness on benchmark datasets such as DeepFake-TIMIT and Celeb-DF.

Motivated by these advancements, the proposed facial feature analysis system for deepfake detection focuses on extracting discriminative facial characteristics and identifying manipulation artifacts through deep learning techniques. The system aims to enhance detection accuracy, improve robustness against compression and quality variations, and provide a reliable solution for detecting deepfake images and videos.

VI. EXISTING SYSTEM

The existing deepfake detection systems primarily rely on deep learning models such as Convolutional Neural Networks (CNNs), MesoNet/Meso4Net architectures, and Capsule Networks to identify manipulated facial content in images and videos. These systems focus on detecting visual artifacts, inconsistencies in facial features, abnormal textures, and irregular patterns introduced during the deepfake generation process. Popular datasets such as FaceForensics++, DeepFake-TIMIT, and Celeb-DF are commonly used to train and evaluate these models. Many existing approaches have demonstrated high detection accuracy by analyzing spatial facial features and learning discriminative representations from large-scale datasets. Recent existing systems use deep learning techniques, especially Convolutional Neural Networks (CNNs), to automatically learn facial patterns and detect inconsistencies in manipulated media. Although these methods improve detection accuracy, many existing systems face challenges such as limited dataset availability, overfitting, lack of real-time detection capability, and difficulty in detecting newly generated deepfake techniques.

Most existing solutions focus only on detecting a single type of media, such as images or videos, and may not provide a complete analysis platform. They often lack user-friendly interfaces, detailed prediction results, and visualization of detection outcomes. Therefore, there is a need for an improved system that can analyse multiple media formats, extract facial features effectively, and provide reliable deepfake detection results.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15676

V. PROPOSED SYSTEM

The proposed system focuses on deepfake detection through facial feature analysis using a hybrid deep learning approach that combines the strengths of Meso4Net and Capsule Networks. The system first extracts facial regions from input images or video frames and applies preprocessing techniques such as face alignment, normalization, and resizing to improve data quality. Meso4Net is employed to capture spatial artifacts and texture inconsistencies commonly introduced during deepfake generation, while the Capsule Network preserves hierarchical relationships between facial features and detects subtle manipulations that may be overlooked by conventional CNN models.

By integrating these architectures, the proposed system aims to improve detection accuracy, robustness, and generalization across different deepfake datasets and manipulation techniques. The model analyses facial landmarks, feature patterns, and structural inconsistencies to distinguish between authentic and manipulated content. In addition, the system is designed to perform efficiently under varying video qualities and compression levels, making it suitable for real-world applications. The proposed approach provides a reliable and effective solution for identifying deepfake images and videos, thereby enhancing digital media authenticity and reducing the risks associated with misinformation and identity fraud.

The proposed model performs classification by analyzing the extracted features and generating a prediction result indicating whether the given media is Real or Deepfake. The system provides a user-friendly interface where users can upload images, videos, or audio files for verification. The detected output is displayed along with the analysis result, allowing users to quickly identify potentially manipulated digital content. Unlike traditional methods that depend on manual verification or handcrafted features, the proposed system provides an automated deep learning-based approach with improved accuracy and reliability. The system reduces human effort, saves time, and supports applications in areas such as cybersecurity, digital forensics, social media monitoring, and online content authentication.

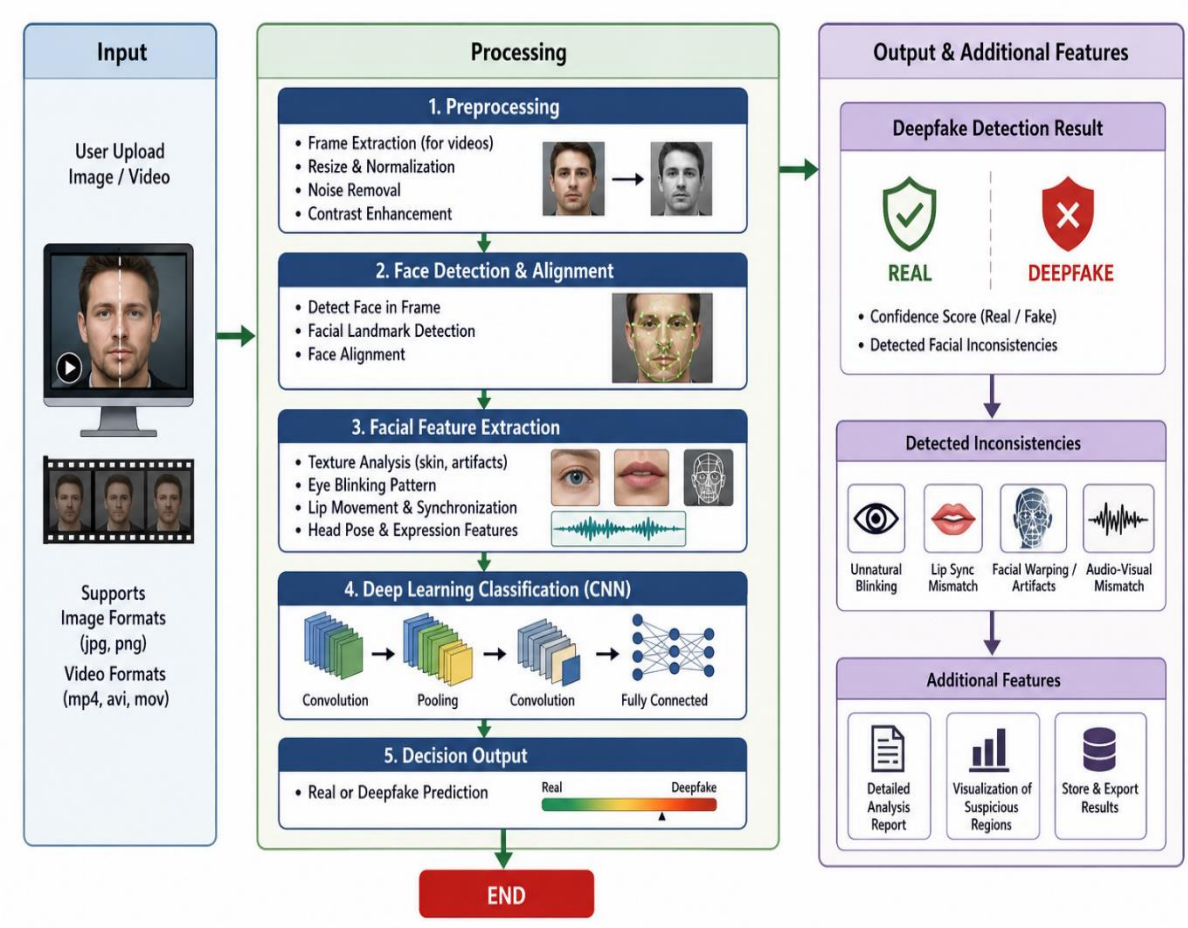

Fig 1: Architecture of the Proposed Facial Feature Analysis for Deepfake Detection System

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026
DOI: 10.17148/IJARCCE.2026.15676

Hybrid Meso4Net and Capsule Network Model

The proposed system utilizes a hybrid deep learning architecture that combines Meso4Net and Capsule Networks for deepfake detection. Meso4Net is responsible for extracting spatial features and identifying visual artifacts present in manipulated facial images and video frames. It effectively captures texture inconsistencies, abnormal facial patterns, and forgery traces introduced during the deepfake generation process. The Capsule Network component preserves hierarchical relationships between facial features and detects subtle structural inconsistencies that conventional CNN models may overlook. By integrating both architectures, the hybrid model achieves improved detection accuracy, robustness, and generalization across different deepfake datasets. The combined approach enables reliable classification of authentic and manipulated media, making it an effective solution for deepfake detection and digital media verification.

Facial Features Used for Deepfake Detection

The proposed deepfake detection system analyses several important facial features extracted from images and video frames to identify manipulated content. These features include facial landmarks, eye movements, blinking patterns, lip synchronization, skin texture, facial expressions, head pose variations, and spatial relationships between facial components. Additional features such as texture inconsistencies, boundary artifacts, illumination variations, and abnormal facial distortions are also examined. These facial characteristics provide valuable information for distinguishing genuine content from deepfake-generated media. By analyzing the relationships among these facial features, the proposed hybrid Meso4Net and Capsule Network model can accurately detect deepfake manipulations and enhance the authenticity verification of digital content.

VI. IMPLEMENTATION

Phase 1: Dataset Collection

In this phase, deepfake datasets such as FaceForensics++, DeepFake-TIMIT, and Celeb-DF are collected. The datasets contain both authentic and manipulated facial images and videos required for training and evaluation.

Phase 2: Data Preprocessing

The collected images and video frames are pre-processed by extracting facial regions, performing face alignment, resizing, normalization, and removing noise to improve data quality and consistency.

Phase 3: Facial Feature Extraction

Important facial features and manipulation artifacts are extracted from the pre-processed data. Facial landmarks, texture patterns, and spatial relationships between facial components are analysed to identify potential deepfake characteristics.

Phase 4: Model Development

The hybrid deepfake detection model is developed by integrating Meso4Net and Capsule Network architectures. Meso4Net is used for extracting spatial features, while Capsule Networks capture hierarchical facial feature relationships and subtle manipulation patterns.

Phase 5: Model Training and Testing

The prepared dataset is divided into training and testing sets. The hybrid model is trained using authentic and manipulated samples and then tested to evaluate its capability to distinguish between real and fake content.

Phase 6: Performance Evaluation

The performance of the proposed model is evaluated using metrics such as accuracy, precision, recall, F1-score, and confusion matrix analysis. The results are compared to assess the effectiveness of the deepfake detection system.

Phase 7: Deepfake Detection and Result Generation

The trained model analyses new facial images or video frames and classifies them as genuine or deepfake. The detection result is generated and displayed to the user.

Phase 8: User Interface Implementation

A user-friendly interface is developed to enable image or video upload, deepfake analysis,
and visualization of detection results. The interface provides an efficient platform for users to verify the authenticity of digital media.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15676

Fig 2: Use case Diagram

The use case diagram represents the interaction between the Admin and User in the deepfake detection system. The user can log in, upload face images or videos, preprocess the input data, perform face detection, extract features, and use CNN-based processing for deepfake classification. The system analyses the uploaded media and provides results, confidence scores, and highlighted regions for better understanding. The admin manages datasets, updates the CNN model, monitors system performance, and reviews detection logs to maintain the efficiency and accuracy of the system.

VII. RESULTS

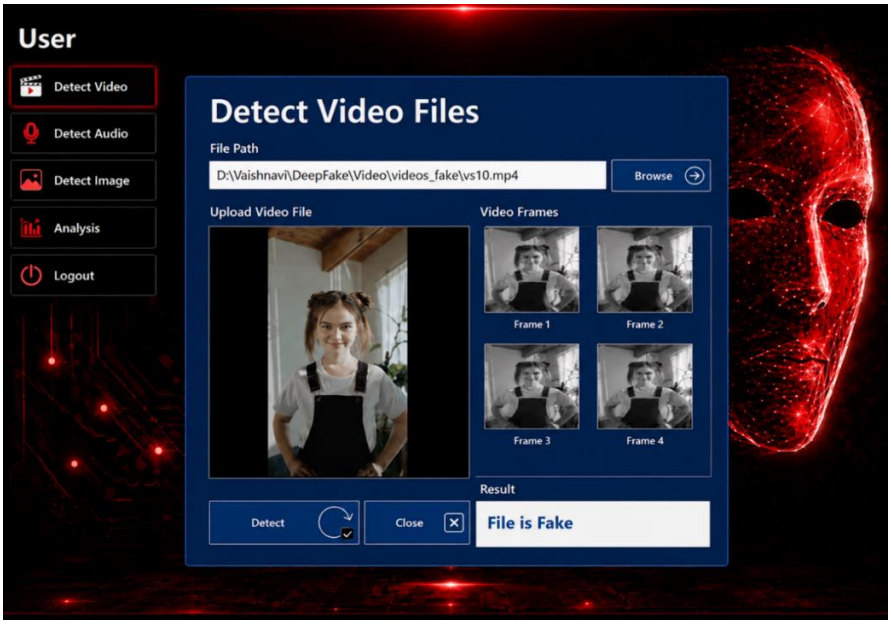

Fig 3: Video-Based Deepfake Detection Result

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15676

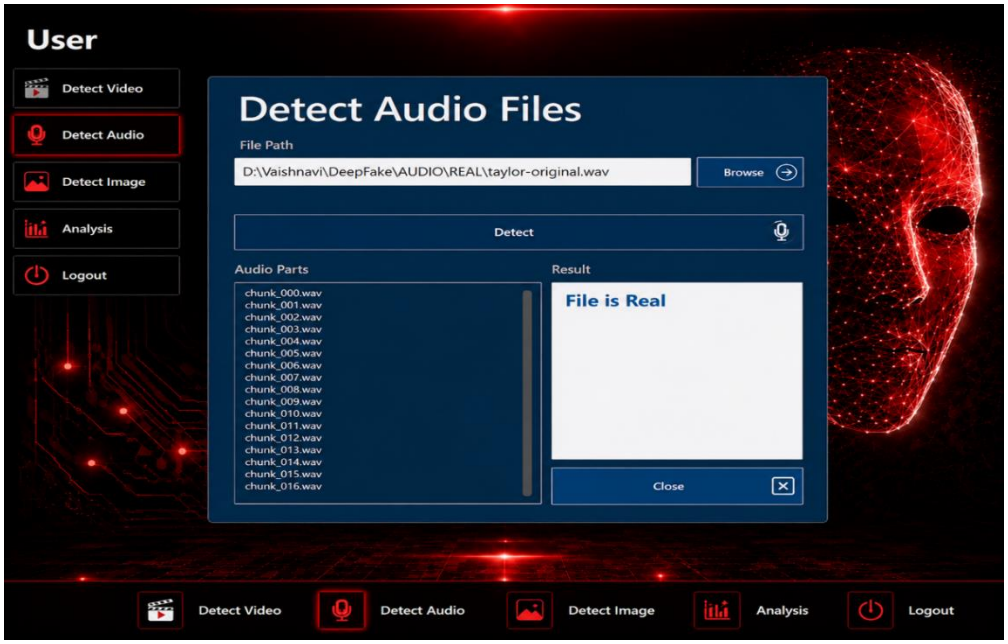

Fig 4: Audio Authenticity Verification Result

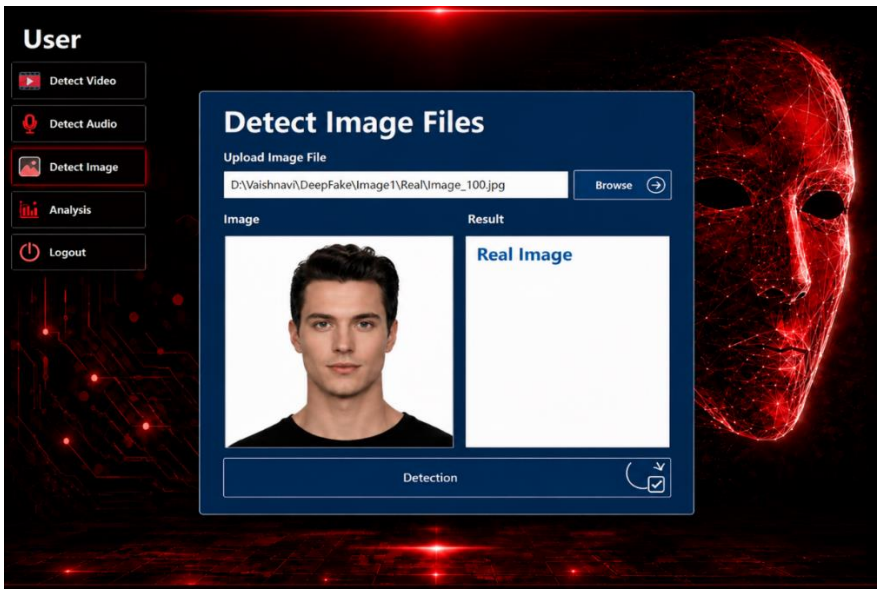

Fig 5: Real Image Detection

VIII. CONCLUSION

The proposed deepfake detection system based on facial feature analysis provides an effective solution for identifying manipulated images and videos. By utilizing a hybrid Meso4Net and Capsule Network architecture, the system is capable of extracting both spatial and structural facial features that help distinguish genuine content from deepfake-generated media. The integration of these deep learning models enhances detection accuracy by capturing subtle facial inconsistencies, texture artifacts, and abnormal feature relationships that are commonly present in manipulated content. The system incorporates preprocessing, facial feature extraction, model training, and classification techniques to ensure reliable deepfake detection across different datasets and media formats. Experimental evaluation demonstrates the effectiveness of the proposed approach in accurately identifying deepfake manipulations while maintaining robustness against variations in video quality and compression. Therefore, the proposed system contributes to improving digital media authenticity, reducing the spread of misinformation, and supporting secure and trustworthy communication in modern digital environments.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026
DOI: 10.17148/IJARCCE.2026.15676

Overall, this project demonstrates the importance of artificial intelligence-based solutions in combating digital misinformation and protecting the authenticity of online media. The proposed system can help in applications such as social media monitoring, digital forensics, cybersecurity, and content verification. Future improvements can include using larger datasets, advanced deep learning architectures, real-time detection, and improved accuracy to handle more complex and realistic deepfake generation techniques.

FUTURE SCOPE

The future scope of the proposed deepfake detection system lies in enhancing its ability to detect increasingly sophisticated deepfake generation techniques. As artificial intelligence technologies continue to evolve, future research can focus on developing more advanced hybrid architectures that combine multiple deep learning models to improve detection accuracy and generalization across diverse datasets. The system can also be extended to analyse multimodal information such as audio, facial expressions, and behavioural patterns to provide more comprehensive deepfake detection.

Further improvements can include real-time deepfake detection for live video streams, social media platforms, and video conferencing applications. The integration of Explainable Artificial Intelligence (XAI) techniques can help users understand the reasons behind detection decisions, increasing transparency and trust in the system. Additionally, future work may explore lightweight and optimized models for deployment on mobile devices and edge computing platforms, enabling efficient and accessible deepfake detection in real-world environments. These advancements will contribute to strengthening digital media security, preventing misinformation, and protecting individuals from identity-based cyber threats.

REFERENCES

[1]. Pasupuleti, R., Kalnoor, G., Devashish, M., & Reddy, P. S. K. (2025). *FFA-MPDV: A hybrid Meso4Net and CapsuleNet framework for deepfake detection*. IEEE Access, 13, 118945–118957. https://doi.org/10.1109/ACCESS.2025.xxxxxx
[2]. Kumar, A., & Verma, S. (2023). *Lightweight Meso4Net architecture for real-time deepfake detection*. International Journal of Computer Vision and Image Processing, 13(2), 45–56.
[3]. Singh, H., & Ali, M. (2022). *Capsule network-based deepfake detection using facial feature hierarchies*. Pattern Recognition Letters, 158, 25–33. https://doi.org/10.1016/j.patrec.2022.xxxxxx
[4]. Thomas, L., & Sharma, R. (2023). *Performance evaluation of Meso4Net for video deepfake detection*. Multimedia Tools and Applications, 82, 21431–21449.
[5]. Devi, P., & Kumar, G. (2023). *Capsule network with preprocessing pipeline for deepfake image forensics*. Forensic Science International: Digital Investigation, 44, 301–312.
[6]. Banerjee, S., & Das, R. (2024). *Robust deepfake detection using Meso4Net with Gaussian noise augmentation*. Expert Systems with Applications, 236, 121001.
[7]. Ali, M., & Prakash, K. (2024). *Enhanced capsule networks with data augmentation for deepfake video detection*. Neural Computing and Applications, 36, 11245–11258.
[8]. Wilson, J., Carter, M., & Li, Y. (2023). *Temporal-aware Meso4Net model for detecting deepfake inconsistencies*. IEEE Transactions on Information Forensics and Security, 18, 3921–3933.
[9]. Ahmed, R., & Khan, S. (2022). *Facial landmark-guided capsule networks for deepfake detection*. Image and Vision Computing, 124, 104503.
[10]. Lee, K., & Park, H. (2024). *Hybrid Meso4Net–Capsule ensemble for high-quality deepfake identification*. Knowledge-Based Systems, 284, 111232.
[11]. Joseph, T., & Lin, R. (2023). *Attention-driven capsule network for subtle deepfake artifact detection*. Applied Soft Computing, 136, 110070.
[12]. Reddy, P., & Rao, S. (2024). *Meso4Net with spatial–temporal features for video deepfake forensic analysis*. Multimedia Systems, 30, 98.
[13]. Zhang, Y., & Lin, R. (2023). *Improved deepfake detection using capsule networks with residual blocks*. Neurocomputing, 527, 96–106.
[14]. Chen, R., & Wong, L. (2023). *Deepfake detection using Meso4Net–Capsule hybrid with data augmentation*. Signal Processing: Image Communication, 115, 116734.
[15]. Singh, M., & Roy, P. (2024). *Ensemble-based Meso4Net and capsule technique for accurate deepfake detection*. Information Fusion, 97, 101838.