



International Journal of Multidisciplinary and Scientific Emerging Research (IJMSERH)

Volume 14, Issue 3, July-September 2026

Impact Factor: 9.798



An Intelligent Deep Learning Framework for Automated DeepFake Detection

Nagajyothi Banda, Prof. Suthan R

M. Tech Student, Department of Computer Science and Engineering, Shridevi Institute of Engineering and Technology, Tumkur Karnataka, India

Assistant Professor, Department of Computer Science and Engineering, Shridevi Institute of Engineering and Technology, Tumkur Karnataka, India

ABSTRACT: Deep fakes are artificial intelligence-generated images, films, or audio recordings that mimic real people's words or actions. Humans are finding it more and more challenging to recognize modified information as deep fake technology advances. This raises significant issues with cyber security, fraud, disinformation, and privacy abuses. Therefore, it is now crucial to create efficient techniques for automatically identifying deep fakes. The goal of this project is to employ deep learning techniques for automated deepfake identification.

KEYWORDS: Deepfake Detection , Deep Learning , Convolutional Neural Networks (CNNs) , Artificial Intelligence (AI) , Digital Media Authentication , Cybersecurity

I. INTRODUCTION

The rapid advancement of artificial intelligence, increased access to digital tools, and extensive use of social media have led to an unprecedented rise in synthetic media production. Architectures to detect anomalies in facial patterns, textures, movements, and frequency-level features. Such models can identify subtle irregularities that are typically invisible to the naked eye. The system analyzes image or video inputs, extracts meaningful characteristics through computer learning techniques, and compares them with learned representations of authentic and manipulated media. Once the system identifies manipulation cues, it classifies the content accordingly.

This automated process ensures faster identification, reduces false judgments, and improves overall detection accuracy. By integrating machine learning with intelligent feature analysis, the suggested methodology for detecting deep fakes provides a scalable, reliable, and sustainable solution suitable for social platforms, educational institutions, workplaces, and public digital environments.

This project aims to create and carry out a Deep fake Machine learning-based detection system to automatically identify and classify manipulated media, including images and videos. The system reduces the requirement for manual verification using deep learning models in conjunction with the ability to identify subtle inconsistencies introduced during synthetic content generation.

By analyzing characteristics that are frequently imperceptible to the human eye, the system increases precision and reliability in detecting manipulated content.

Through advanced Feature extraction and categorization methods, the system categorizes media as real or fake based on learned representations of authentic and manipulated samples. The main goal is to create an efficient, scalable, and user-friendly detection mechanism suitable for real-world environments, supporting digital security, reducing misinformation, and promoting trust in online communication platforms. Deepfake technology uses advanced Artificial Intelligence (AI) and Deep Learning techniques to create highly realistic fake images.

SCOPE

The scope of this project includes the development, testing, and evaluation of an automated deep fake machine learning-based detecting system algorithms ability to evaluate temporal and geographical characteristics in multimedia content.

1. Application of cybersecurity:
2. Electronic Forensic.
3. Election and political security.
4. Journalisim and Media.
5. preventing Financial fraud.
6. Improvement of Biometric Authentication.
7. Security in health care and telemedicine.
8. Detects AI-generated fake images, videos, and audio automatically.
9. Identifies face-swapped and facial reenactment videos.
10. Detects manipulated images by analyzing visual artifacts and inconsistencies.
11. Recognizes synthetic or cloned voices in audio recordings.
12. Uses deep learning models such as CNNs, RNNs, LSTMs, and Vision Transformers (ViTs) for accurate detection.
13. Supports real-time deepfake detection in video conferencing and live streaming.
14. Helps social media platforms identify and remove fake or misleading content.
15. Assists in combating misinformation, fake news, and online propaganda.
16. Strengthens cybersecurity by detecting identity spoofing and impersonation attacks.
17. Supports digital forensics by verifying the authenticity of multimedia evidence.
18. Enhances biometric security systems such as facial recognition and voice authentication.
19. Assists law enforcement agencies in investigating cybercrimes involving manipulated media.
20. Protects political, financial, and corporate sectors from deepfake-based fraud.
21. Enables multimodal detection by analyzing video, audio, and text together.
22. Improves detection accuracy through continuous training on large and diverse datasets.
23. Supports deployment on cloud, mobile, and edge computing platforms.
24. Integrates Explainable AI (XAI) to make detection results more transparent and interpretable.
25. Can be combined with blockchain and digital watermarking for media authentication.
26. Continuously adapts to new and evolving deepfake generation techniques.
27. Contributes to maintaining trust, security, and authenticity in digital communication and online media

Objective

- **To develop an automated deepfake detection system** capable of accurately classifying facial images as real or fake.
- **To preprocess the input images** by converting them to grayscale and resizing them to a uniform size for consistent feature extraction..
- **To extract frequency-domain features** from images using the **Fast Fourier Transform (FFT)** and **Azimuthal Averaging** to identify hidden artifacts introduced by deepfake generation.
- **To provide a reliable and efficient solution** for deepfake image detection that can support applications in digital forensics, cybersecurity, media authentication, and social media content verification.

Problem statement

- The rapid advancement of **Artificial Intelligence (AI)** and **Deep Learning** has enabled the creation of highly realistic deepfake images that are difficult to distinguish from genuine images.
- Deepfake content poses serious challenges, including misinformation, identity theft, fraud, and manipulation of digital media, making reliable detection increasingly important..
- Traditional visual inspection and conventional image analysis techniques are often insufficient for detecting advanced deepfake images due to their high level of realism.
- There is a need for an automated deepfake detection system that can analyze hidden frequency-domain features using **Fast Fourier Transform (FFT)** and **Azimuthal Averaging** to identify image

II. LITERATURE SURVEY

1. Passos et al. (2024) – A Review of Deep Learning-Based Approaches for Deepfake Content Detection.
2. Abbas & Taeihagh (2024) – Unmasking Deepfakes: A Systematic Review of Deepfake Detection and Generation Techniques Using Artificial Intelligence

3. Pei et al. (2024) – Deepfake Generation and Detection: A Benchmark and Survey.
4. Mirsky & Lee (2021) – The Creation and Detection of Deepfakes: A Survey.
5. Tolosana et al. (2020) – DeepFakes and Beyond: A Survey of Face Manipulation and Fake Detection

III. PROPOSED METHODOLOGY

- ❖ Dataset Collection
- ❖ Image Processing
- ❖ FrequencyDomain Transformation
- ❖ Feature Extraction
- ❖ Feature Storage
- ❖ Dataset Preparation
- ❖ Performance Comparision
- ❖ Deepfake Image Detection

❖ Dataset Collection

Collect a dataset containing **Real** and **Deepfake** facial images. Organize the dataset into **Training** and **Testing** folders.

❖ Image Processing

Read the input images using OpenCV, Convert images into grayscale, Resize all images to **256 × 256 pixels**, Remove corrupted or invalid images.

❖ Frequency Domain

Apply the Fast Fourier Transform (FFT) to convert images from the spatial domain to the frequency domain. Generate the **Magnitude Spectrum** of each image.

❖ Feature Extraction.

Apply Azimuthal Averaging(extract frequency based features) on the magnitude spectrum .

Extract the Power Spectral Density (image details are distributed) feature vector. Convert each image into a fixed-length feature vector .

❖ Feature Storage

Save the extracted feature vectors using a Pickle (.pkl) file. This reduces feature extraction time during future executions.

❖ Dataset Preparation

Prepare the feature matrix (X) and labels (y). Split the dataset into **90% training** and **10% testing** using stratified sampling.

❖ Performance Comparison

Compare the performance of all classifiers. Select the model with the highest accuracy score.

Deepfake Image Detection

Predicts whether the input image is:.

1. Real Image.
2. Deepfake Image

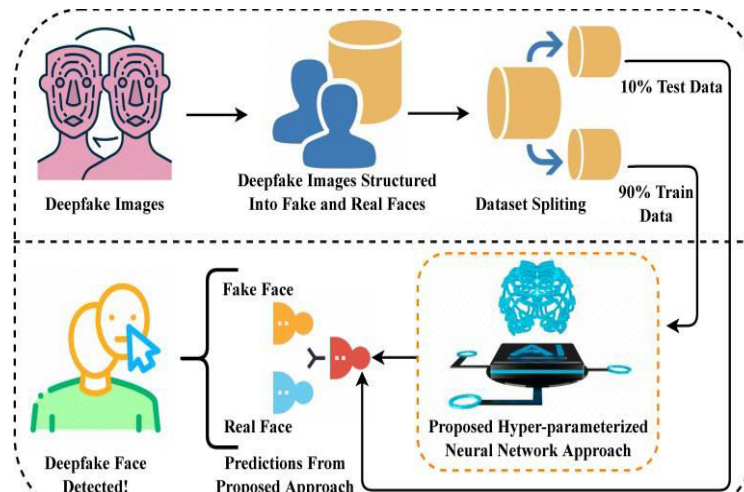


Fig.1.DeepFake Image Detection

Formulas for Deep fake detection

1. Cosine Similarity: $\text{Cos}(\theta) = (\mathbf{A} \cdot \mathbf{B}) / (\|\mathbf{A}\| \|\mathbf{B}\|)$

- **Cosine Similarity** measures the similarity between two facial feature vectors (embeddings) extracted by a deep learning model.
- **A** represents the feature vector of the original face, and **B** represents the feature vector of the suspected face.
- The similarity score ranges from **-1 to 1**, where a value close to **1** indicates highly similar facial features.
- In automated deepfake detection, a low cosine similarity score indicates differences between the embeddings, helping identify

2. Binary Accuracy: $\text{Accuracy} = (\text{TP} + \text{TN}) / (\text{TP} + \text{TN} + \text{FP} + \text{FN})$

- **Binary Accuracy** measures the percentage of correctly classified images or videos by the deep learning model.
- **TP (True Positive)** represents deepfake images correctly identified as deepfakes, while **TN (True Negative)** represents real images correctly identified as real.
- **FP (False Positive)** occurs when a real image is incorrectly classified as a deepfake, and **FN (False Negative)** occurs when a deepfake is incorrectly classified as real.
- A higher binary accuracy value indicates that the deep learning model is more effective at distinguishing between authentic and manipulated (deepfake) images or videos.

IV. OUTPUT SNAPSHOT

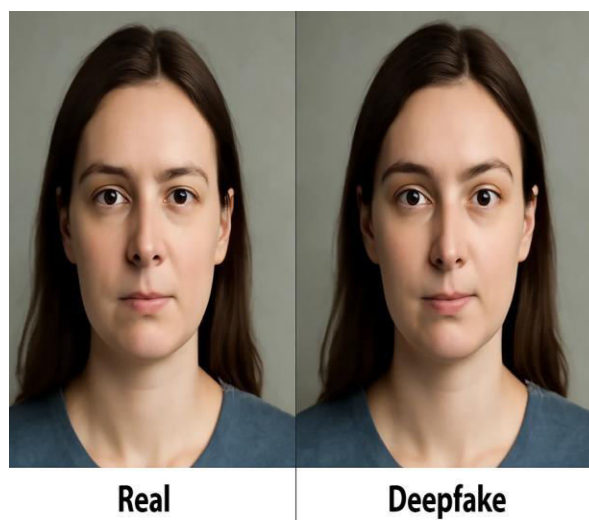


Fig.1.1.Detection of Real and Deepfake image



Fig.1.2.Face Deepfake Detection

V. CONCLUSION

- The project successfully develops an **automated deepfake detection system** for classifying images as real or fake using frequency-based analysis and machine learning techniques.
- The proposed system reduces dependence on manual inspection by providing an automated method for identifying AI-generated fake images.
- The developed framework provides a foundation for building advanced deepfake detection systems capable of handling evolving AI-generated content.
- The proposed approach provides an efficient and practical solution for applications such as digital forensics, cybersecurity, media verification, and online content authentication.
- The proposed methodology can be extended in the future for deepfake video detection and real-time multimedia authentication systems.

VI. FUTURE WORK

- ❖ The existing system can be enhanced by implementing advanced deep learning architectures such as **Convolutional Neural Networks (CNNs)**.
- ❖ The model can be optimized and deployed for real-time applications such as live video calls, online meetings, and social media platforms..
- ❖ Future work can include training the model on larger and more diverse datasets containing different deepfake generation methods, image qualities, and real-world conditions..
- ❖ Future models can be designed with continuous learning capabilities to adapt to newly emerging deepfake generation techniques and maintain detection performance over time.
- ❖ Develop a desktop, mobile, or web-based application with a simple interface, allowing users to upload images and receive instant deepfake detection results.

REFERENCES

- [1]A. Rössler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies and M. Nießner, “FaceForensics++: Acquiring the ability to recognize modified faces videos,” Proc. IEEE/CVF Int. Conf. Computer Vision (ICCV), 2019.
- [2] D. Afchar, V. Nozick, J. Yamagishi and I. Echizen, “MesoNet: A compact facial video forgery detection network,” Proc. IEEE Int. Workshop on Information Forensics and Security (WIFS), 2018
- [3] P. Korshunov and S. Marcel, “Deepfakes: a new threat to face recognition? Assessment and detection,”

arXiv:1812.08685, 2018.

[4] P. Nowakowski and T. Pamula, “Deep learning–based image classification for detecting manipulated video content 2020.

[5] T.J.Shengetal., “AI-driven real-time monitoring using deep learning and cloud connectivity,” IEEE Access, 2020.

[6] B. Dolhansky et al., “The Deepfake Detection Challenge (DFDC) Dataset,” Proc. IEEE/CVF Conf. Pattern Recognition and Computer Vision Pattern Recognition and Computer Vision (CVPR), 2020.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



International Journal of Multidisciplinary and Scientific Emerging Research (IJMSE RH)

Impact Factor: 9.274