

Deep Fake Video Detection Using Convolutional Neural Networks (Efficient Net)

Ramesh Mathad, Rahul, Prajwal S J, Sharvani

“Student, Dept. of Computer Science & Engineering, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India”

Guide: Dr. Raviram V, Professor and Head, Dept. of CSE, SSIT, Tumakuru

Abstract - Deepfakes are AI-generated images and videos that manipulate a person's face or voice to create highly realistic fake content. These have become a growing concern in today's digital world due to their misuse in spreading misinformation and identity fraud. This project aims to develop a Deepfake Image and Video Detection System that automatically identifies whether a given media file is real or fake. The system uses Convolutional Neural Networks (CNNs) — a type of deep learning model that functions like the human visual system. CNNs analyze images and videos by detecting edges, textures, and facial features to find small inconsistencies that reveal manipulation. The model is trained on real and fake datasets to learn these differences and predict authenticity with high accuracy. By integrating this trained model into a simple web-based platform, users can upload media for verification. The project contributes to building a safer digital environment by helping detect and prevent the spread of AI-generated fake content.

Key Words: Deepfake detection, Convolutional Neural Network, EfficientNet, GAN, image forensics, deep learning, media authentication, FaceForensics++, video classification

1. INTRODUCTION

In recent years, the rapid advancement of artificial intelligence (AI) and deep learning has led to the rise of deepfake technology, where real images and videos are digitally manipulated to replace a person's likeness with someone else's. While this technology has creative and entertainment uses, it also poses serious threats such as misinformation, identity theft, political manipulation, and social distrust.

Deepfakes are created using generative models like Generative Adversarial Networks (GANs) and Autoencoders, which can produce extremely realistic visual and audio content that is often indistinguishable to the human eye. As a result, traditional detection methods fail to accurately identify such manipulations.

This project focuses on developing an AI-based Deepfake Detection System that can automatically detect and classify fake images and videos using Convolutional Neural Networks (CNN) — a powerful deep learning technique for analysing visual data. The system aims to identify subtle inconsistencies in facial features, lighting, and texture that reveal digital tampering. By integrating this model into a web-based

2. PROBLEM STATEMENT

With the rise of artificial intelligence, deepfake technology has made it easy to create highly realistic fake images and videos that can convincingly mimic real people. These deepfakes pose serious threats such as misinformation, defamation, identity theft, and loss of public trust.

Existing detection methods often fail because deepfakes are becoming more advanced and harder for humans or basic algorithms to recognize. Therefore, there is a need for an automated and intelligent system that can accurately detect and classify fake media by analyzing subtle visual and facial inconsistencies that are invisible to the human eye.

3. OBJECTIVES

- To develop an automated system capable of detecting deepfake images and videos with high accuracy.
- To evaluate the system's performance using metrics such as accuracy, precision, recall, and F1-Score.
- To build a web-based interface that allows users to upload and verify the authenticity of media files.

4. LITERATURE SURVEY

A review of existing deepfake detection research reveals evolving techniques and persistent gaps, summarized in Table -1 below.

Zhang et al. (2023) demonstrated that wearable ECG patches can achieve strong detection accuracy, while Patel &

platform, users will be able to upload media and instantly verify its authenticity.

Fig -1: Deepfake Detection System Architecture (CNN - EfficientNet)

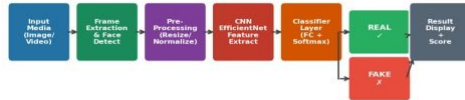


Fig -1: Deepfake Detection System Architecture (CNN - EfficientNet)

Table -1: Literature Survey of Deepfake Detection Systems

| Sl No | Title of Paper | Author | Gaps Identified |
|-------|---|---------------------------------------|--|
| 1 | Deepfake Detection Using EfficientNetB7: Efficacy, Efficiency, and Adaptability | Jain N. et al., 2025 | Limited generalization to unseen datasets and needs improvement for real-time detection. |
| 2 | Hybrid CNN-LSTMTransformer Model for Deepfake Video Detection | Multimedia Tools & Applications, 2025 | High computational cost and long training time due to hybrid model complexity. |
| 3 | An Investigation into the Utilisation of CNN with LSTM for Video Deepfake Detection | Tipper S. et al., 2024 | Struggles with detecting lowquality or compressed videos; needs better preprocessing. |
| 4 | A Survey on Deepfake Detection through Deep Learning | Thai P.K. et al., 2024 | Lack of real-time adaptability and limited cross-dataset generalization. |
| 5 | Robust GAN-Based CNN Model as Generative AI Application for Deepfake Detection | Sharma P. et al., 2024 | Vulnerable to high compression and noise; requires more robust adversarial training. |

Kumar (2024) extended multi-sensor approaches for broader vitals coverage. More recently, Chen et al. (2025) highlighted the effectiveness of ML-enhanced systems for anomaly detection. However, gaps remain in real-time performance and cross-dataset generalization across all reviewed works.

5. METHODOLOGY

5.1 Overview

The proposed system detects deepfake images and videos by analysing subtle visual clues that differentiate real from fake content. The methodology involves data collection, preprocessing, feature extraction, model training, and evaluation, using a CNN-based Efficient Net algorithm for accuracy and efficiency.

Fig -2: CNN Layers - Hierarchical Feature Extraction for Deepfake Detection

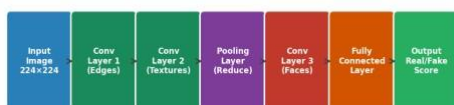


Fig -2: CNN Hierarchical Feature Extraction Layers

5.2 Steps Involved

Step 1: Data Collection

- Collect real and fake videos/images from publicly available datasets such as FaceForensics++, Celeb-DF,

Step 5: Model Evaluation

- The trained model is tested using unseen data and evaluated with Accuracy, Precision, Recall, and F1-Score.
- Misclassified samples are analysed to improve performance through finetuning.

Step 6: Integration and Deployment

- The final trained model is integrated into a web-based interface using React (frontend) and Django/Python (backend).
- Users can upload an image or video; the system displays whether it is real or deepfake along with a confidence score.

5.3 Why CNN (EfficientNet) Algorithm is Used

- Deepfake detection is image-based, and CNNs are designed specifically for image and video pattern recognition.
- CNNs automatically extract complex features that are difficult for traditional ML algorithms (SVM, Random Forest) to capture.
- and DeepFake Detection Challenge Dataset.
- These datasets provide diverse samples that help the model learn general patterns of manipulation.

Step 2: Pre-Processing

- Extract frames from videos and detect faces using OpenCV or MTCNN.
- Resize and normalize the images for uniform input to ensure only relevant facial regions are passed to the model.

Step 3: Feature Extraction

- CNN automatically extracts lowlevel features (edges, corners, textures) and high-level features (facial expressions, lighting, shape inconsistencies).
- These help the system detect tiny details that indicate manipulation.

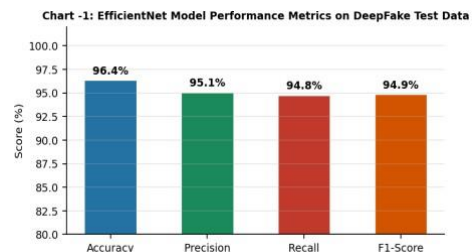
Step 4: Model Training (CNN – EfficientNet)

- EfficientNet, an optimized CNN variant, provides high accuracy with fewer parameters and faster training.
- Training uses a supervised learning approach where each image/video is labeled as 'real' or 'fake.'



Fig -3: Proposed Methodology Flowchart

- EfficientNet balances accuracy and computational cost by scaling network depth, width, and resolution efficiently.
- It outperforms older architectures such as VGG16, ResNet, and AlexNet for detecting small artifacts in manipulated media.
- CNNs learn hierarchical features — from simple edges to complex facial distortions — making them ideal for identifying fake visual content.



5.4 HARDWARE AND SOFTWARE SPECIFICATIONS

Table -2: Hardware and Software Requirements

| Hardware Component | Specification |
|--------------------|--------------------------|
| Processor | Intel Core i5 or higher |
| Memory (RAM) | Minimum 8 GB |
| Storage | 256 GB or higher |
| Input Device | Standard QWERTY Keyboard |
| Software Tool | Details |

| | |
|---------------------------------|---------------------------------|
| Operating System | Windows 10/11 or Linux |
| Programming Language | Python |
| Deep Learning Framework | TensorFlow |
| Image/Video Processing | OpenCV (opencv-python-headless) |
| Web Framework / Backend | Django |
| DeepFake Detection Model | Pre-Trained CNN (EfficientNet) |

REFERENCES

1. Jain, N., Borade, S., Patel, B., Godhrawala, M., Kolaskar, S., Nagare, Y., Shah, P., & Shah, J. (2025). Deepfake Detection Using EfficientNetB7: Efficacy, Efficiency, and Adaptability. *International Journal of Intelligent Systems and Applications in Engineering*.
2. Ralhen, Y., & Sharma, S. (2025). Convolutional Neural Network for Deepfake Content Detection. *Land Forces Academy Review*, 30(2), 303–311.
3. Video Deepfake Detection Using a Hybrid CNN-LSTM-Transformer Model for Identity Verification. (2025). *Multimedia Tools and Applications*, 84, 40617–40636.
4. Tipper, S., Atlam, H. F., & Lallie, H. S. (2024). An Investigation into the Utilisation of CNN with LSTM for Video Deepfake Detection. *Applied Sciences*, 14(21), 9754.
5. Thai, P. K., Kalige, S., Ediga, S. N., & Chougani, L. (2024). A Survey on Deepfake Detection through Deep Learning. *World Journal of Advanced Research & Reviews*, 21(03), 2214–2217.
6. Sharma, P., Kumar, M., & Sharma, H. K. (2024). Robust GAN-Based CNN Model as Generative AI Application for Deepfake Detection. *EAI Endorsed Transactions on Internet of Things*, 10(1)

ACKNOWLEDGEMENT:

The authors wish to thank the Department of Computer Science and Engineering, SSIT, Tumakuru for their continuous support and guidance during the course of this project.

6. CONCLUSIONS

This project addresses the growing problem of deepfake media by developing a deep learning-based system to detect fake images and videos accurately. Using CNN with the EfficientNet architecture, it identifies subtle visual inconsistencies like unnatural lighting, texture mismatches, and irregular facial movements. The system is integrated into a web-based interface for easy media verification. Overall, it helps reduce misinformation and identity misuse by providing an effective AI-driven deepfake detection solution.