Journal of Science, Computing and Engineering Research (JSCER)
Volume-9, Issue-3, March 2026.
DOI: *https://doi.org/10.46379/jscer.2024.0709*

FAKE FACE DETECTION (DEEPFAKE VS REAL FACE)

[1]J.R.Arun Kumar, [2]Gopal Sharma, [3]Guddu, [4]Saloni, [5]Sneha

[1]Professor, Department of CSE, Modern Institute of Technology and Research Centre, Alwar, Rajasthan, India.

[2,3,4,5]UG Student, Department of AI&DS, Modern Institute of Technology and Research Centre, Alwar, Rajasthan, India.

Article Information

Received : 25 March 2026
Revised : 25 March 2026
Accepted : 26 March 2026
Published : 28 March 2026

Correspomding Author:

Gopal Sharma

***Abstract*—** The aim of this project is to detect fake or synthetic human faces using deep learning technology to ensure digital trust and security.With the rapid rise of AI-generated deepfakes, fake human faces have become a serious concern for privacy, identity verification, and online authenticity. Therefore, early and accurate detection of such manipulated images is essential to prevent their misuse. This project employs a Convolutional Neural Network (CNN) model trained on the RVF10K dataset, which contains real and fake human face images. The CNN automatically learns distinctive facial patterns and features to accurately classify images as real or fake.

The proposed model specifically works on human faces and rejects non-human images during detection.This system can be effectively utilized in social media verification, cybersecurity, and forensic investigations, providing a reliable tool to maintain the authenticity of human digital content and strengthen protection against AI-based facial forgeries.

Keywords: Convolutional Neural Network (CNN), Deep Learning, Fake Face Detection, Image Preprocessing, Streamlit

Citation: J.R.Arun Kumar, Gopal Sharma, Guddu, Saloni, Sneha, "FAKE FACE DETECTION", Journal of Science, Computing and Engineering Research, 9(3), MAR 2026.

I. INTRODUCTION

In the modern digital era, the rapid advancement of artificial intelligence and deep learning has revolutionized the creation and manipulation of digital media. One of the most alarming outcomes of this advancement is the generation of AI-synthesized human faces, commonly known as deepfakes. These synthetic faces are often indistinguishable from real human images and are being increasingly used in identity fraud, misinformation, cybercrimes, and social media manipulation. Such misuse poses a serious threat to digital trust, privacy, and online authenticity.

Traditional methods of fake image detection rely on manual inspection, expert evaluation, or metadata analysis, which are time-consuming, error-prone, and ineffective against modern AI-generated faces. As deepfake technology continues to evolve, there is a growing need for automated and intelligent systems capable of accurately identifying fake human faces.

In this context, artificial intelligence and deep learning provide powerful tools to address these challenges. Specifically, convolutional neural networks (CNNs) have shown remarkable capability in analyzing and classifying image data. By leveraging CNN architectures, the proposed system can automatically extract important facial features and distinguish between real and AI-generated human faces with high accuracy.

This project presents a fake face detection system that employs a CNN-based model trained on the RVF10K dataset, containing both real and fake human face images. The model analyzes facial patterns, texture details, and inconsistencies to detect 7 manipulated or AI-generated faces. Furthermore, the system is integrated with a Streamlit user interface, enabling users to upload or capture images and instantly receive predictions with confidence scores. Multi-leveled equations and graphics, are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

II. PROBLEM STATEMENT

The growing advancement of artificial intelligence and deepfake generation technologies has led to the creation of highly realistic synthetic human faces that are almost indistinguishable from real ones. These AI-generated fake faces are increasingly being misused for unethical purposes such as

identity fraud, misinformation, cybercrimes, and social media manipulation. This has created serious concerns regarding digital trust, privacy, and the authenticity of online identities. Traditional methods of fake image detection rely on manual observation and metadata analysis, which are slow, inaccurate, and incapable of handling modern deepfake technologies. As a result, users and organizations remain vulnerable to AI based facial manipulations that can easily deceive human vision and conventional detection systems. To address this problem, there is a need for an automated and intelligent system that can accurately detect and classify fake human faces using advanced deep learning models. This project proposes a Convolutional Neural Network (CNN)-based approach to identify whether an image of a human face is real or AI-generated. The system focuses on analyzing texture inconsistencies, facial patterns, and pixel-level distortions that are not visible to the human eye.

III. PROPOSED MODEL

The proposed Fake Face Detection system is designed using deep learning and computer vision techniques to classify human face images as real or fake. The system follows a structured pipeline that includes image acquisition, preprocessing, CNN-based prediction, and result generation:

A. Image Acquisition

The process begins when the user uploads or captures an image through the Streamlit-based user interface. The uploaded image is treated as input for further processing. The system accepts common image formats such as JPG, PNG, and JPEG.

B. Face Detection

Before processing, the system checks whether the uploaded image contains a human face. This step is performed using the MTCNN (Multi-task Cascaded Convolutional Neural Network) algorithm. If no face is detected, the system displays an error message and requests the user to upload a valid image.

C. Image Preprocessing

Once the face is detected, the image undergoes preprocessing steps to improve model performance:

- Resizing image to 128×128 pixels
- Normalizing pixel values between 0 and 1
- Converting image into NumPy array
- Face cropping for better feature extraction

These steps ensure uniformity and enhance model accuracy.

D. CNN Based Feature Extraction

The preprocessed image is passed into the Convolutional Neural Network (CNN) model. The CNN automatically extracts important facial features such as:

- Texture patterns
- Facial distortions
- Pixel inconsistencies
- Lighting variations

These features help differentiate real faces from fake faces.

E. Classification Layer

After feature extraction, the fully connected layers classify the image into two categories:

- Real Face
- Fake Face

The Softmax activation function is used to generate prediction probabilities.

F. Result Generation

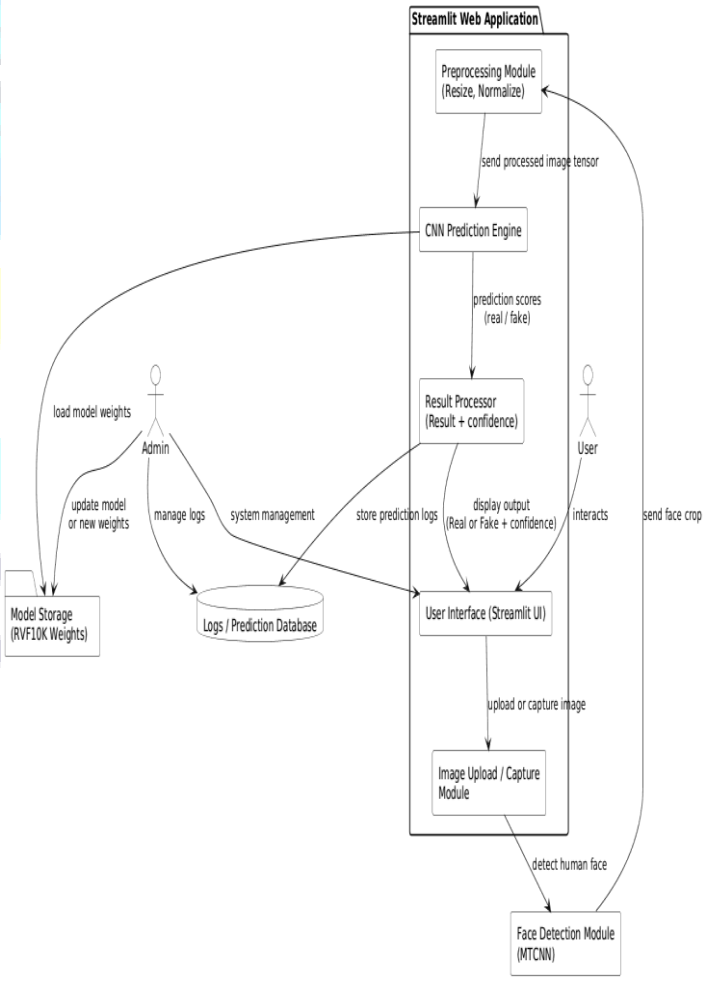
The model produces the final prediction along with a confidence score. The output is displayed on the Streamlit interface showing:

- Prediction Result (Real / Fake)
- Confidence Score
- Uploaded Image

This makes the system user-friendly and easy to interpret.

Component Diagram:

The Component Diagram illustrates the structural relationship among the software components.



IV. TECH STACK

The successful implementation of this system depends on a well-structured technology stack designed for performance, flexibility, and scalability. The stack is divided into four layers: frontend, backend, AI/ML, and supporting tools.

A. Frontend Technologies

These are used to build the graphical user interface that allows users to upload or capture images and view prediction results.

• **Streamlit** – For developing an interactive and responsive user interface.

B. Backend Technologies

These handle image validation, communication between the user interface and the AI model, and result generation.

• **Python** – The primary programming language used for backend logic and AI model integration.

C. AI/ML Technologies

These form the core of the fake face detection functionality. • TensorFlow / Keras –For building and training the Convolutional Neural Network (CNN) model.

• **OpenCV** –For image reading, resizing, color conversion, and face detection tasks.

• **MTCNN** – For detecting human faces and ensuring valid input images.

• NumPy & Pandas – For handling image arrays and managing dataset structures.

• **Scikit-learn** – For preprocessing, evaluation metrics, and class weight balancing.

D. Other Tools and Libraries

• **Jupyter Notebook** – For model experimentation, analysis, and performance tracking.

• **Matplotlib / Seaborn** – For plotting accuracy and loss graphs during model training.

• **Git / GitHub** – For version control and code management.

• **Google Colab** – For cloud-based training and testing of deep learning models.

V. RESULT SCREENSHOTS

The proposed Fake Face Detection system was successfully implemented using a Convolutional Neural Network (CNN). The model demonstrated strong performance in distinguishing real and fake human faces. During training, the model achieved an accuracy of over 95%, while validation accuracy reached around 85–90%, indicating good generalization. The system was tested using multiple real and fake images, and predictions were generated with high confidence scores. In several test cases, the model detected fake faces with confidence levels above 99%.

The Streamlit-based user interface enabled users to upload or capture images easily. The system processed the input image, detected human faces using MTCNN, and performed classification in real time. The output displayed the predicted result along with the confidence score. The system showed fast response time and reliable performance. Overall, the results demonstrate that the proposed CNN-based model effectively detects fake faces and can be used in cybersecurity, identity verification, and social media authentication.

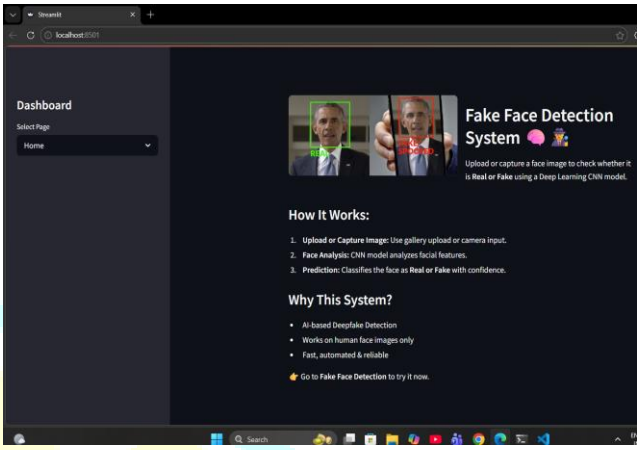


Fig. 1. Home page

Fig. 2. Output page

VI. CONCLUSION

The Fake Face Detection System developed in this project successfully demonstrates the potential of deep learning and computer vision in identifying AI-generated (fake) human faces. By leveraging Convolutional Neural Networks (CNN), the system is able to automatically extract and learn complex facial patterns, textures, and inconsistencies that distinguish real faces from synthetic ones. The use of preprocessing techniques such as normalization, resizing, and face detection using MTCNN further improves the model's accuracy and robustness. The Streamlit-based user interface allows users to upload or capture images and receive instant predictions along with confidence scores, making the system interactive and easy to use. The model trained on the RVF10K dataset performs effectively in real-world scenarios, showing promising results in detecting manipulated or fake human faces. This project provides a reliable and efficient solution that can be integrated

into various domains such as social media verification, digital forensics, and cybersecurity. It helps in promoting digital trust and safeguarding users against identity fraud and misinformation caused by AI-generated content.

REFERENCES

[1] He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep Residual Learning for Image Recognition. IEEE Conference on Computer Vision and Pattern Recognition (CVPR).

[2] Zhang, K., Zhang, Z., Li, Z., & Qiao, Y. (2016). Joint Face Detection and Alignment using Multi-task Cascaded Convolutional Networks (MTCNN). IEEE Signal Processing Letters.

[3] Simonyan, K., & Zisserman, A. (2015). Very Deep Convolutional Networks for Large-Scale Image Recognition. arXiv preprint arXiv:1409.1556.

[4] Rossler, A., et al. (2019). FaceForensics++: Learning to Detect Manipulated Facial Images. IEEE International Conference on Computer Vision (ICCV).

[5] Dolhansky, B., et al. (2020). The DeepFake Detection Challenge (DFDC) Dataset. arXiv preprint arXiv:2006.07397.

[6] Jiang, L., et al. (2020). DeeperForensics-1.0: A Large-Scale Dataset for Real-World Face Forgery Detection. CVPR.

[7] TensorFlow Documentation. (2024). TensorFlow: An End-to-End Open Source Machine Learning Platform.

[8] OpenCV Documentation. (2024). Open Source Computer Vision Library.

[9] Kaggle. (2024). RVF10K Dataset – Real and Fake Face Images.