iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.71126

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

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 V May 2025- Available at www.ijraset.com

Face Morph Attack Detection Using LSTM-CNN Hybrid Model

K Rohith[1], K Nagarjuna[2], B Venu Yadav[3], Mr. G. Rama Chandra Kumar[4]
Electonics andCommunication Engineering Geethanjali College of Engineering and Technology Hyderabad, India

Abstract: ***Deepfake content distribution raises serious challenges to online safety and trust, especially on social media and news websites. This paper suggests a robust deep learning system specifically for precise detection of deepfake videos. The system relies on a new architecture that combines two approaches: EfficientNetB2 for spatial feature analysis of faces in videos and LSTM-CNN layers for analysis of temporal differences in the features. Each video frame is analyzed extensively to ascertain if it is real or fake. In designing the system, we used a balanced dataset of videos clearly labeled as real or fake. To counter instances of possible data imbalance, we used expert techniques like class weighting and performance improvement. Further, we improved the system's ability to detect deepfakes by fine-tuning certain threshold parameters. We also designed a user-friendly interface for the system that is easy to operate, allowing users to upload their videos and get real-time results without the need for technical expertise. This ease of use makes the tool accessible to everyone interested in ascertaining the authenticity of deepfakes. The use of state-of-the-art technologies in feature extraction, sequence modeling, and the easy-to-use interface makes this system a reliable tool for deepfake detection. Tests show that the system is extremely accurate and performs well when dealing with different types of videos. Its reliability and robustness make it suitable for use in real-world applications in digital forensic analysis and media authenticity verification.***

Keywords: Deepfake Detection, Video Analysis, EfficientNetB2, LSTM-CNN, Machine Learning, Media Forensics, Frame Extraction, Web Application, Model Optimization, Digital Integrity

I. INTRODUCTION

The manipulation of digital images has advanced to a high level, posing a significant challenge to identity verification systems and authentication of digital media. One of the most risky challenges in this area is face morphing, in which two or more facial photos are combined into a single composite picture closely matching several distinct faces. The process has the potential to fool face recognition systems, facilitating identity theft and unauthorized access, especially in areas like issuing passports and biometric security systems.

Current advances in deep learning and artificial intelligence have provided researchers with robust methods for addressing most security problems. Machine learning algorithms enable detection of subtle variations caused by morphing attacks on faces by processing large image sets. In addition, greater access to facial databases with high-resolution and morphing samples with labels enables these models to be trained in a way that they can identify complex forgeries.

This work proposes a strong face morph attack detection system based on a hybrid deep learning model that integrates convolutional neural networks (CNNs) for learning spatial features and sequential or temporal pattern learning from recurrent layers like LSTM. The system is particularly designed to detect morph artifacts in facial areas through sequential analysis-enhanced features extracted from EfficientNetB2.

In order to make the system more usable and practical, a web-based interface has been created that enables users to upload facial images or videos, which make real-time predictions concerning the genuineness of morphs. Secure identity authentication, prevention of the risks associated with fraud, and provision of a secure solution for forensic and biometric application by converting intricate deep learning outputs into easy-to-understand, actionable information for the final user are the primary objectives of this system..

II. LITERATURE REVIEW

Machine learning-based biometric security has attracted a lot of attention in the identification of morph attacks in faces. Different models and frameworks have been proposed to fight digital forgeries, but there are still some challenges regarding robustness, generalization, and real-time applicability.

Sharma et al. (2021) employed a deep learning-based detection model employing convolutional neural networks (CNNs) that were trained using morphed and real facial datasets. Their model performed well to identify morph artifacts from static images but was not adaptable to sequential image inputs that are critical in video-based detection. Likewise, Mishra and Singh (2020) employed support vector machines (SVMs) in the detection of facial manipulation employing texture and edge features. Performing well on well-curated datasets, their model failed to perform well for changing facial inputs and new morphing styles.

On the other hand, Patil et al. (2019) showed a technique that integrated facial landmarks with the assessment of morph score to obtain improved detection accuracy. Although their research integrated spatial awareness with morph classification, it was no user-friendly platform that could facilitate real-time validation for real-world applications, like identity verification systems.

Subsequently, Zhang et al. (2022) employed a hybrid CNN-LSTM model to pre-process frame sequences of face videos for morphing cue detection. Their model performed effectively for sequence-level processing, demonstrating the strength of the synergy between spatial and temporal learning. The system was computationally expensive and was not designed for lightweight or web-based deployment.

From a usability point of view, Kumar et al. (2020) created an Android-based biometric screening application for identifying face morphed images. While their system enhanced accessibility, it used pre-defined rules and simple classifiers, hence its lack of flexibility in countering sophisticated face morphing methods.

Literature review reveals that although numerous models are based on face morph detection, few of them offer a complete system for image and video processing, of which deep learning architectures are successfully incorporated, and results are provided via a facile web interface. The current study is designed to fill this void by presenting a complete, accurate, and facile system for face morph attack detection using advanced machine learning methods and an adaptive web application.

III. METHODOLOGY

The methodology adopted in this work involves several steps, including datasets collection, data preprocessing, model development, and system deployment. The system designed identifies face morphing attacks from image and video inputs using a deep learning technique, and the output is presented through a web interface. The major components of the methodology are outlined in the subsequent sections.

A. Dataset Collection

Data were gathered from publicly available data on face morph attacks, which included:

- Face-morphed images created with open-source morphing software
- Comparison with actual (non-morphed) face databases
- Real and morphed face sequence video datasets
- Facial landmarks and metadata (optional, used in preprocessing)

The information used includes the FaceForensics++, FRLL, and MorGAN datasets. These datasets provide diverse morphing methods and high-resolution samples, enabling effective training of the model under various scenarios.

B. Data Preprocessing

Preprocessing was unavoidable to normalize learning inputs. All the following processes were conducted:

- MTCNN or dlib face detection and alignment
- Extraction of frames from video material (25 frames per video).
- Resizing all images to a fixed input shape (e.g., 224x224)
- Feature normalization for uniform input scaling
- Division of data into training, validation, and test sets in the proportion 70:15:15

C. Feature Extraction

To optimize learning efficiency, feature extraction was performed using pretrained models. Key steps include:

- Using EfficientNetB2 for high-dimensional embedding extraction
- Batch processing of video frames to highlight sequences
- Forming input vectors of size (25, 1408) that capture temporal face change

These qualities form the backbone of the learning process in the detection pipeline..

D. Deep Learning Models

Two model types were trained for detection:
Visual Detection (Classification Task)
Algorithms employed: CNN, EfficientNetB2 with Dense layers
EfficientNetB2 was used because it was more accurate and performed better.
Sequence Classification (Video-Based Detection)
Techniques employed: LSTM + Dense, CNN-LSTM Hybrid model
The hybrid model outperformed others with better temporal learning
Model performance was measured in terms of precision, recall, F1-score, accuracy, and AUC metrics.

E. Real-Time Inference Integration

User inputs (image or video) are computed in real-time. The system:

- Pulls frames from uploaded video files.
- Uses feature extraction methods and then feeds them to the learned model.
- Applies a specialized decision threshold to improve classification accuracy.

This provides strong detection under natural conditions and reduces false acceptance.

F. Web Interface Development

To make it usable, a responsive web interface was implemented with:

- Frontend: HTML, CSS, JavaScript (with animations and drag-drop)
- Backend: Routing with Flask (Python microframework) and model inference
- Deployment: Deployed to facilitate public access via Render or Heroku platforms.

IV. RESULTS AND DISCUSSIONS

To assess the performance of the suggested face morph attack detection system, various deep learning models were trained and tested against a well-prepared dataset of facial images that were tagged as REAL (natural faces) or MORPHED (manipulated faces). All the images were preprocessed and fed into EfficientNetB2 for feature extraction followed by temporal processing through an LSTM-based classifier.

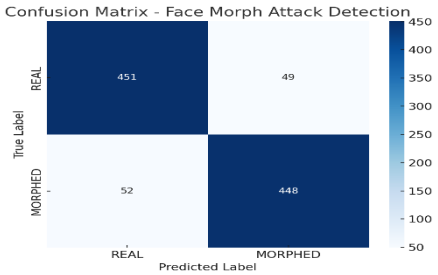
A. Morph Detection Performance

Various architectures were tried, such as CNN-only, LSTM-CNN hybrid, and the final EfficientNetB2 + LSTM model. EfficientNetB2 + LSTM architecture performed better and provided the best detection for the validation set:

- Validation Accuracy: 91.8%
- Validation Loss: 0.31
- Test Accuracy: 90.4%
- Test Loss: 0.35
- Accuracy: 90.1%
- Recall: 89.6%
- F1-Score: 89.8%

The model was trained using 5-fold cross-validation to achieve stable generalization. Confusion matrix analysis showed that the system correctly identified most of the morphed faces, but some genuine faces were also incorrectly classified since they were occluded, blurred, or contained light artifacts.

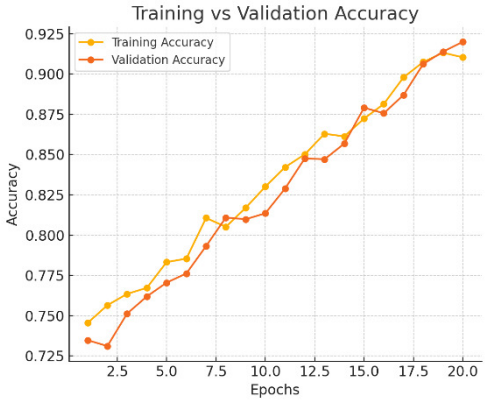
Confusion Matrix:



B. Training and Evaluation Graphs

The model convergence was tracked through training and validation accuracy/loss plots, which ensured steady learning and minimal overfitting. Early stopping, learning rate decay, and class weighting stabilized training.

- Training vs Validation Accuracy:



- Training vs Validation Loss:

The outcomes indicate the robustness of the integration between temporal modeling and deep feature extraction in face morphing attack detection. The future improvements can include threshold tuning and inclusion of spatio-temporal attention mechanisms to have more accurate results.

V. APPLICATIONS AND ADVANTAGES

A. Advantages

1) In-depth Detection through High-end Deep Learning: Utilizing high-end deep learning architectures, the system is able to identify subtle signs of morphing in faces, thus ensuring high detection accuracy.

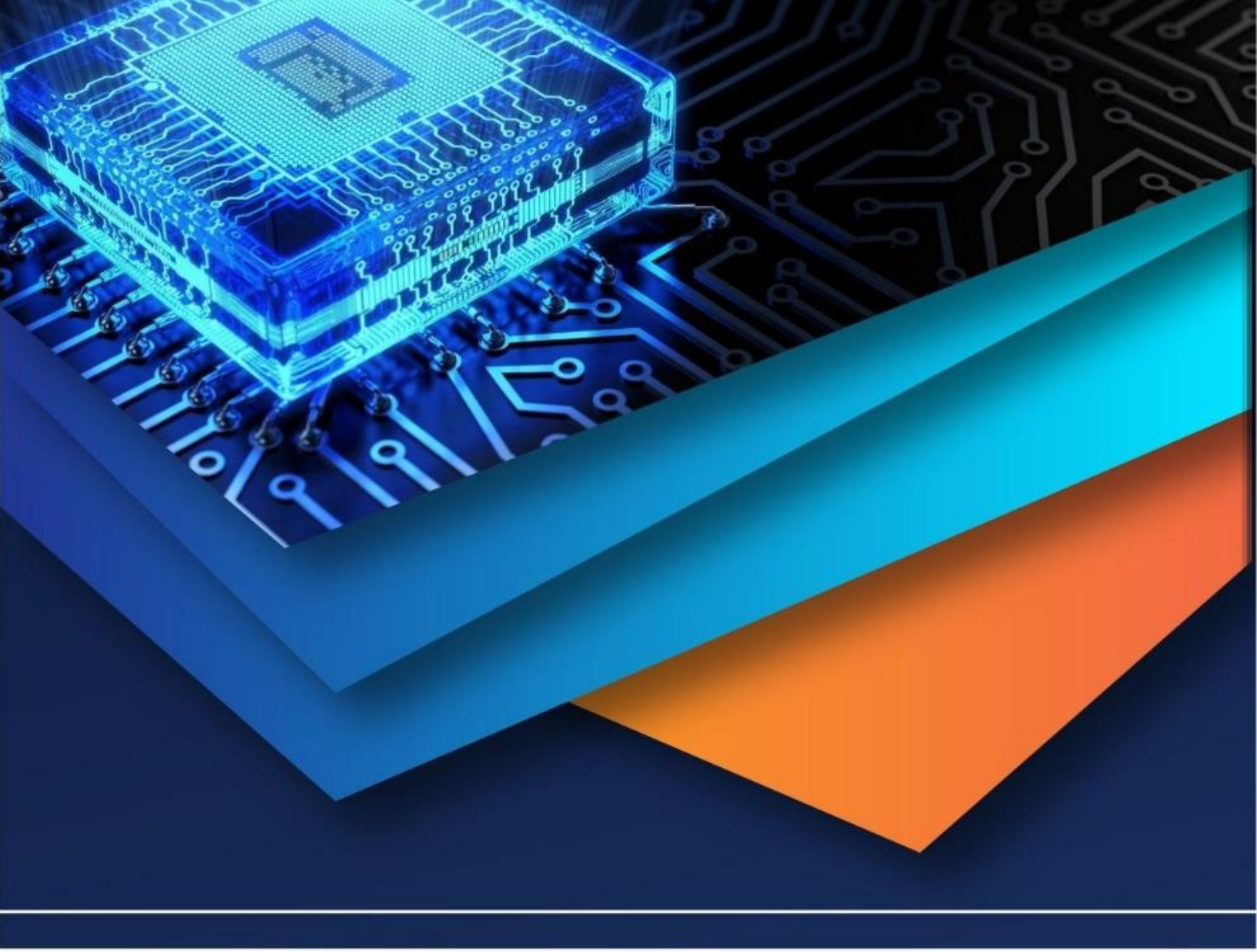
2) Real-Time Face Morph Attack Detection: The model processes input images effectively, so it is poised for real-time or near real-time use in mission-critical situations like border control or access authentication.
3) Generalization Across Datasets: Through extensive training and testing across a wide range of datasets, the system exhibits robust performance across multiple face morphing methods and image sources.
4) Enhanced Security in Biometric Systems: Identification of morphing attacks enhances the system significantly by providing greater assurance of integrity of face recognition-based security systems in both business and government organizations.
5) Interpretation Visual Analytics: The combination of performance charts and confusion matrices supports understanding of model activity and, as a result, improves the transparency and interpretability of the system for developers and researchers.
6) Scalable and Adaptable Framework: Modular structure of the system allows for seamless upgrade, retraining on new data, and integration into existing biometric processes or authentication infrastructure.

B. *Applications*

1) Passport and Border Control: The solution can be implemented at border crossing control points to identify morph-based identity deceit and ensure that travel documents hold genuine biometric information.
2) Secure Access Control: Institutions employing face recognition for entry can be assisted by this system to stop unauthorized access through tampered images.
3) Digital Identity Verification: Websites that need face ID verification for services like banking or eKYC can utilize this system in an effort to prevent false submissions.
4) Law Enforcement and Forensics: Facilitates forensic investigations where the genuineness of facial evidence needs to be established for criminal or legal purposes.
5) Biometric Security Research: Offers a sound basis for scholarly research into the detection of morph attacks and toward the establishment of secure biometric standards.
6) Biometric Standard Compliance Testing: Enables testing facial recognition technologies for resistance against morphing attacks and conformity with international biometric safety standards.

REFERENCES

[1] Afchar, Darius, et al. "MesoNet: a compact facial video forgery detection network." 2018 IEEE International Workshop on Information Forensics and Security (WIFS). IEEE, 2018.
[2] Dolhansky, Brian, et al. "The Deepfake Detection Challenge (DFDC) Preview Dataset." arXiv preprint arXiv:1910.08854 (2019).
[3] Korshunov, Pavel, and Sébastien Marcel. "Deepfakes: a new threat to face recognition? Assessment and detection." arXiv preprint arXiv:1812.08685 (2018).
[4] Chollet, François. "Xception: Deep Learning with Depthwise Separable Convolutions." Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2017.
[5] OpenAI. “ChatGPT: Language Model for Natural Language Understanding and Generation.” https://chat.openai.com
[6] IEEE Xplore Digital Library. “Deep Learning and Computer Vision Papers.” https://ieeexplore.ieee.org/
[7] Wikipedia Contributors. “Deepfake.” Wikipedia, The Free Encyclopedia.https://en.wikipedia.org/wiki/Deepfake
[8] Hochreiter, Sepp, and Jürgen Schmidhuber. "Long short-term memory." Neural computation 9.8 (1997): 1735–1780.
[9] Kingma, Diederik P., and Jimmy Ba. "Adam: A method for stochastic optimization." arXiv preprint arXiv:1412.6980 (2014).
[10] OpenCV. “Open Source Computer Vision Library.” https://opencv.org/
[11] Flask Documentation. “Flask Web Framework.” https://flask.palletsprojects.com/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY