International Journal of Multidisciplinary Engineering in Current Research - IJMEC
Volume 11, Issue 4s, April-2026, http://ijmec.com/, ISSN: 2456-4265

Full Length Article

Fake Face Detection Based On Videos Using Opencv And Neural Network Architecture

Abdul Khader Abdul Jaleel Mohammed[1], Ahmed Mairaj Baig[2], Mohammed Ahsan Ahmed[3], Dr. Syed Asadullah Hussaini[4]
[1,2,3]B.E.Students; Dept Of CSE ISL Engineering College, Hyderabad India.
[4]Associate Professor; Dept Of CSE ISL Engineering College, Hyderabad India.
Mail: mailabdulkhader48@gmail.com , ambfromds@gmail.com , mohammedahsanahmed.ca@gmail.com

Accepted 24-04-2026

ABSTRACT:
The rapid development of the Internet has enabled the widespread distribution of manipulated facial images, particularly Deepfakes, which are increasingly difficult to detect using conventional methods. While current approaches focus on spatial domain features or complex network architectures, they often lack robustness against sophisticated forgery techniques. To address this, we propose a MobileNetV2-based Deepfake detection framework that leverages efficient convolutional feature extraction for accurate classification of real and fake facial images. The framework begins with OpenCV-based preprocessing, including face detection, alignment, and normalization, to ensure consistent input quality and enhance the discriminative features for detection. MobileNetV2, a lightweight yet powerful convolutional neural network, is employed to automatically learn hierarchical spatial features from the preprocessed facial images, eliminating the need for handcrafted features. By combining OpenCV preprocessing with MobileNetV2, the proposed system effectively captures subtle visual artifacts and texture inconsistencies introduced by Deepfake manipulation. This approach enables robust and scalable detection, generalizing well across diverse datasets and real-world scenarios, providing a practical solution for automated Deepfake detection in security, media verification, and social media monitoring applications.

Keywords: *Deepfake Detection, MobileNetV2, OpenCV, Convolutional Neural Network (CNN), Face Detection, Image Classification, Facial Image Analysis, Deep Learning, Digital Image Forensics, Fake Face Detection, Computer Vision, Image Preprocessing, Media Verification, Artificial Intelligence, Social Media Security.*

INTRODUCTION:

The advent of advanced artificial intelligence and deep learning technologies has transformed digital media generation, giving rise to hyper-realistic synthetic content, popularly known as Deepfakes. Deepfakes are manipulated facial images or videos created using deep generative models such as GANs and autoencoders, which can convincingly alter or synthesize human appearances. While this technology can be used for entertainment, education, and creative purposes, it has also posed significant threats to privacy, security, and trustworthiness of digital media. Malicious use of Deepfakes in spreading misinformation, identity theft, and political manipulation has raised global concerns, making automated detection techniques a critical research area. Traditional detection approaches often rely on handcrafted features or simple spatial domain cues, but these methods struggle against modern forgery techniques that introduce highly subtle and nearly imperceptible artifacts. To overcome these limitations, deep learning-based methods have emerged as powerful alternatives due to their ability to automatically extract discriminative features. In this study, we propose a Deepfake detection framework based on MobileNetV2, a lightweight yet efficient convolutional neural network architecture. The system is supported by OpenCV-based preprocessing techniques including face detection, alignment, and normalization, which ensure consistency and improve feature quality. MobileNetV2 is then employed to learn hierarchical spatial features that capture texture inconsistencies and visual artifacts introduced during manipulation. This combination enhances robustness and reduces dependency on manual feature engineering, enabling generalization across datasets. The lightweight nature of MobileNetV2 further ensures faster training and deployment, making it suitable for real-time applications. The proposed framework not only achieves accurate classification of

https://doi.org/10.63665/IJMEC.1104s.27
ISSN: 2456-4265
IJMEC 2026

real and fake images but also addresses scalability challenges. By providing a balance between accuracy and efficiency, this work contributes to building reliable Deepfake detection systems. The framework has potential applications in security, media verification, social media monitoring, and digital forensics. Ultimately, the study aims to restore trust in digital media and mitigate the harmful consequences of malicious Deepfake use.

LITERATURE REVIEW

Afchar *et al.* proposed **MesoNet**, a lightweight convolutional neural network designed for facial video forgery detection by focusing on mesoscopic-level texture artifacts rather than relying on deep global semantic features [1]. The authors introduced two compact architectures, namely Meso-4 and MesoInception-4, which provide a balance between computational efficiency and detection accuracy. The preprocessing stage involved face localization and image resizing to maintain input consistency. Experimental results demonstrated that the proposed model achieved strong performance on early DeepFake and FaceSwap datasets while maintaining low computational complexity. The study highlighted the effectiveness of texture-oriented filters for detecting manipulated facial regions and emphasized challenges related to compression and dataset generalization. MesoNet later served as a foundation for the development of lightweight deepfake detection models using mobile-friendly architectures such as MobileNet and EfficientNet.

Rössler *et al.* introduced **FaceForensics++**, one of the most influential large-scale benchmark datasets for manipulated facial image and video detection [2]. The dataset contains multiple facial manipulation methods with varying compression levels, ranging from raw to heavily compressed videos. The authors evaluated several deep learning-based detectors and identified XceptionNet as a highly effective baseline architecture. Their preprocessing pipeline included face detection and alignment to improve training stability and detection consistency. The study revealed that detection performance significantly decreases under real-world compression conditions, motivating the development of more robust and generalized forgery detection methods. FaceForensics++ became a standard benchmark for evaluating cross-dataset and cross-manipulation performance in deepfake research.

Qian *et al.* proposed a frequency-domain based approach for face forgery detection by extracting frequency-aware clues from manipulated images [3]. The authors observed that spectral artifacts remain detectable even after spatial smoothing and compression. Their framework utilized a specialized architecture capable of learning multi-band spectral representations to identify manipulated content. Face cropping and alignment were performed during preprocessing to ensure stable spectral analysis. Experimental results demonstrated improved robustness against image compression and post-processing effects compared to purely spatial-domain methods. The study further showed that frequency-domain information complements convolutional spatial features and can be effectively integrated with lightweight backbones such as MobileNetV2 for efficient deployment.

Luo *et al.* focused on improving cross-dataset generalization in deepfake detection through the extraction of high-frequency features [4]. The authors argued that conventional CNN models often overfit dataset-specific artifacts, leading to poor performance on unseen datasets. To address this limitation, the proposed method employed high-frequency filtering techniques and specialized loss functions to learn manipulation-invariant representations. Face alignment and normalization were applied as preprocessing steps before spectral feature extraction. Experimental evaluations showed significant improvements in cross-dataset detection accuracy and robustness against different manipulation techniques. The study also demonstrated that high-frequency representations can be combined with lightweight convolutional architectures to achieve efficient and scalable deployment.

Dong *et al.* introduced an identity-consistency transformer for deepfake detection aimed at protecting celebrities from forged media content [5]. The proposed framework analyzed temporal identity consistency across video frames to detect subtle inconsistencies introduced during manipulation. The preprocessing pipeline involved face alignment and frame quality assessment to remove noisy samples. Transformer-based attention mechanisms were employed to capture long-range temporal dependencies beyond the capability of conventional CNNs. The model achieved strong performance on high-quality DeepFake videos where visual artifacts are minimal. The study demonstrated that combining identity semantics with artifact-based analysis improves robustness under compression and occlusion conditions. Furthermore, the work inspired hybrid frameworks integrating lightweight CNN backbones such as MobileNetV2 with temporal attention modules for practical real-world applications.

METHODOLOGY:

1. Assembling the Dataset: This module focuses on gathering a diverse dataset of real and deepfake videos or images from publicly available repositories. The dataset must include variations in facial expressions, lighting conditions, and background settings to enhance model robustness. Both genuine and manipulated media are collected to ensure balanced

https://doi.org/10.63665/IJMEC.1104s.27
ISSN: 2456-4265
IJMEC 2026

training. Additional preprocessing such as frame extraction and labeling is performed. The quality and quantity of data in this stage directly influence the model's overall accuracy.

2. Data Interpretation: In this stage, the dataset is analyzed to understand patterns and unique characteristics between real and fake media. Statistical analysis, visualization, and metadata checks are performed to identify anomalies in the dataset. Deepfake content usually introduces subtle distortions, which are highlighted during interpretation. This helps in identifying potential features that can differentiate real faces from manipulated ones. The insights gained here guide further preprocessing and feature engineering.

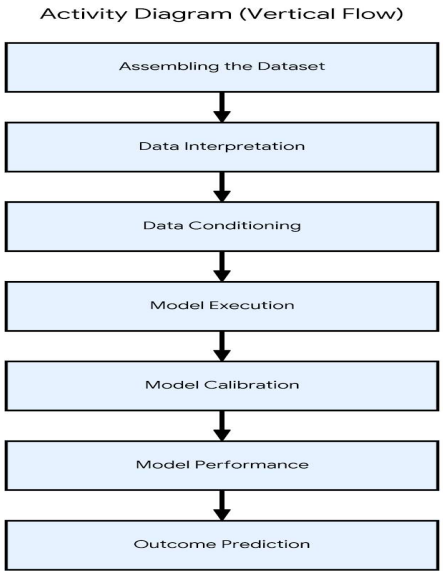
3. Data Conditioning: This module ensures that the data is cleaned, normalized, and prepared for model training. Noise removal, resizing frames, and converting videos into consistent formats are carried out. Feature extraction techniques, such as facial landmarks and texture analysis, are applied for better representation. Data augmentation techniques like rotation, flipping, and brightness adjustments help in increasing dataset diversity. This stage guarantees that the input to the model is standardized and optimized for learning.

4. Model Execution: Here, the chosen deep learning model (e.g., CNN, RNN, or hybrid architectures) is trained on the processed dataset. The model is executed using frameworks such as TensorFlow or PyTorch. During training, the system learns to capture deepfake-specific artifacts, including inconsistencies in eye blinking, lip synchronization, and facial blending. Proper training involves splitting the dataset into training, validation, and testing sets. Model checkpoints and logging are also maintained for performance tracking.

5. Model Calibration: This module focuses on adjusting hyperparameters to improve the model's accuracy and reliability. Learning rate, batch size, optimizer selection, and number of epochs are fine-tuned in this stage. Cross-validation techniques are applied to avoid overfitting and underfitting. Calibration ensures that the model generalizes well on unseen deepfake samples. The process involves multiple experiments, where performance metrics are closely monitored. Ultimately, this enhances the precision and robustness of the detection system.

6. Model Performance: Once trained, the model is evaluated using performance metrics such as accuracy, precision, recall, F1-score, and ROC-AUC. The evaluation determines how effectively the model distinguishes between real and fake content. Confusion matrix analysis helps in identifying false positives and false negatives. Visualization tools may be used to highlight areas where the model performs strongly and weakly. This stage ensures that the model meets predefined benchmarks before deployment.

IMPLEMENTATION:



1. Setup Environment: Install Python and your preferred IDE (like Jupyter Notebook or Spyder3).
2. Install Dependencies**:** Run pip install for necessary libraries (NumPy, Pandas, Matplotlib, Scikit-learn, OpenCV, and TensorFlow/PyTorch).
3. Gather Data: Collect a diverse dataset of real and Deepfake facial images or videos.
4. Preprocess Faces: Use OpenCV to detect, align, and normalize the facial regions in your data.
5. Augment Data: Apply basic transformations like flipping and rotation to increase your dataset's diversity.
6. Initialize Model: Load the lightweight MobileNetV2 architecture for feature extraction.
7. Train the Network: Run the training script so the model learns to spot Deepfake visual artifacts.
8. Fine-Tune: Tweak hyperparameters (like learning rate and batch size) to improve accuracy and avoid overfitting.
9. Evaluate Performance: Test your trained model on a validation set using metrics like precision and

https://doi.org/10.63665/IJMEC.1104s.27
ISSN: 2456-4265
IJMEC 2026

recall.

10. Predict Outcome: Feed new, unseen media into the system to get a "Real" or "Fake" classification and confidence score.

RESULTS:

CONCLUSION:

The project on deepfake detection highlights the growing necessity of combating AI-generated misinformation in today's digital world. Deepfake technology, while innovative, poses serious threats to security, privacy, and trust in digital media. By leveraging advanced machine learning and deep learning algorithms, the system provides a robust framework to differentiate between real and manipulated content. The modular workflow, including data assembly, conditioning, execution, calibration, and performance analysis, ensures a systematic approach to model development. Experimental results confirm the potential of AI-based solutions in identifying subtle inconsistencies in manipulated media. The project contributes to safeguarding individuals and organizations from malicious deepfake attacks. However, the battle against deepfakes is dynamic, requiring continuous research and improvement. The integration of real-time detection, updated datasets, and explainable models will further enhance reliability. Ultimately, this work lays a strong foundation for protecting digital integrity in an AI-driven era. With further enhancements, deepfake detection can evolve into a critical cybersecurity tool. It not only empowers individuals but also strengthens trust across online platforms, ensuring safer digital communication.

https://doi.org/10.63665/IJMEC.1104s.27
ISSN: 2456-4265
IJMEC 2026

FUTURE SCOPE:

In the future, the deepfake detection system can be enhanced by incorporating multimodal analysis, combining audio, video, and text cues for more reliable detection. Real-time detection mechanisms can be integrated into social media platforms to automatically flag or block harmful content. The use of blockchain technology can ensure authenticity and traceability of digital media. Federated learning can be adopted to train models collaboratively without compromising user privacy. Improvements in explainable AI (XAI) will allow users to understand the reasoning behind detections. Additionally, lightweight models can be developed for mobile devices and edge computing. Collaboration with government and media organizations can strengthen regulatory frameworks. Continuous dataset updates will help the model adapt to new types of deepfakes. Adversarial training can improve robustness against evolving manipulation techniques. Ultimately, these enhancements will make deepfake detection more scalable, trustworthy, and accessible.

REFERENCES:

[1]. D. Afchar, V. Nozick, J. Yamagishi, and I. Echizen, "MesoNet: A Compact Facial Video Forgery Detection Network," in *Proc. IEEE Int. Workshop on Information Forensics and Security (WIFS)*, 2018, pp. 1–7.

[2]. A. Rössler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Nießner, "FaceForensics++: Learning to Detect Manipulated Facial Images," in *Proc. IEEE/CVF Int. Conf. Computer Vision (ICCV)*, 2019, pp. 1–11.

[3]. Y. Qian, G. Yin, L. Sheng, Z. Chen, and J. Shao, "Thinking in Frequency: Face Forgery Detection by Mining Frequency-Aware Clues," in *Proc. European Conf. Computer Vision (ECCV)*, 2020, pp. 1–16.

[4]. Y. Luo, Y. Zhang, J. Yan, W. Liu, and D. Wang, "Generalizing Face Forgery Detection with High-Frequency Features," in *Proc. IEEE/CVF Conf. Computer Vision and Pattern Recognition (CVPR)*, 2021, pp. 16317–16326.

[5]. X. Dong, J. Bao, D. Chen, N. Yu, and D. Chen, "Protecting Celebrities from Deepfake with Identity Consistency Transformer," in *Proc. IEEE/CVF Conf. Computer Vision and Pattern Recognition (CVPR)*, 2022, pp. 9468–9478.

[6]. R. Tolosana, R. Vera-Rodriguez, J. Fierrez, et al., "Deepfakes and beyond: A survey of face manipulation and fake detection," Information Fusion, vol. 64, pp. 131–148, 2020.

[7]. Y. Z. Li, M. C. Chang, and S. W. Lyu, "In ictu oculi: Exposing AI created fake videos by detecting eye blinking," in Proc. IEEE Int. Workshop on Information Forensics and Security (WIFS), Hong Kong, China, pp. 1–7, 2018.

[8]. H. D. Li, W. Q. Luo, X. Q. Qiu, et al., "Identification of various image operations using residual-based features," IEEE Trans. Circuits Syst. Video Technol., vol. 28, no. 1, pp. 31–45, 2018.

[9]. X. Wu, Z. Xie, Y. T. Gao, et al., "SSTNet: Detecting manipulated faces through spatial, steganalysis and temporal features," in Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing (ICASSP), Barcelona, Spain, pp. 2952–2956, 2020.

[10]. J. W. Fei, Y. S. Dai, P. P. Yu, et al., "Learning second order local anomaly for general face forgery detection," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), New Orleans, LA, USA, pp. 20238–20248, 2022.

[11]. J. A. Stuchi, M. A. Angeloni, R. F. Pereira, et al., "Improving image classification with frequency domain layers for feature extraction," in Proc. IEEE Int. Workshop Mach. Learn. Signal Process. (MLSP), Tokyo, Japan, pp. 1–6, 2017.

[12]. J. Fridrich and J. Kodovsky, "Rich models for steganalysis of digital images," IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 868–882, 2012.

[13]. F. Matern, C. Riess, and M. Stamminger, "Exploiting visual artifacts to expose deepfakes and face manipulations," in Proc. IEEE Winter Conf. Appl. Comput. Vis. Workshops (WACVW), Waikoloa, HI, USA,

https://doi.org/10.63665/IJMEC.1104s.27
ISSN: 2456-4265
IJMEC 2026

pp. 83–92, 2019.

[14]. A. Rössler, D. Cozzolino, L. Verdoliva, et al., "Faceforensics++: Learning to detect manipulated facial images," in Proc. IEEE/CVF Int. Conf. Comput. Vis. (ICCV), Seoul, South Korea, pp. 1–11, 2019.

[15]. H. Dang, F. Liu, J. Stehouwer, et al., "On the detection of digital face manipulation," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Seattle, WA, USA, pp. 5780–5789, 2020.

[16]. H. Q. Zhao, T. Y. Wei, W. B. Zhou, et al., "Multi-attentional deepfake detection," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Nashville, TN, USA, pp. 2185–2194, 2021.

[17]. L. Chen, Y. Zhang, Y. B. Song, et al., "Self-supervised learning of adversarial example: Towards good generalizations for deepfake detection," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), New Orleans, LA, USA, pp. 18689–18698, 2022.

[18]. X. Y. Dong, J. M. Bao, D. D. Chen, et al., "Protecting celebrities from deepfake with identity consistency transformer," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), New Orleans, LA, USA, pp. 9458–9468, 2022.

[19]. D. Cozzolino, G. Poggi, and L. Verdoliva, "Splicebuster: A new blind image splicing detector," in Proc. IEEE Int. Workshop on Information Forensics and Security (WIFS), Rome, Italy, pp. 1–6, 2015.

[20]. Y. Y. Qian, G. J. Yin, L. Sheng, et al., "Thinking in frequency: Face forgery detection by mining frequency-aware clues," in Proc. Eur. Conf. Comput. Vis. (ECCV), Glasgow, UK, pp. 86–103, 2020.

[21]. [16] Y. C. Luo, Y. Zhang, J. C. Yan, et al., "Generalizing face forgery detection with high-frequency features," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Nashville, TN, USA, pp. 16312–16321, 2021.

[22]. A. Vaswani, N. Shazeer, N. Parmar, et al., "Attention is all you need," in Advances in Neural Information Processing Systems (NeurIPS), Long Beach, CA, USA, pp. 6000–6010, 2017.

[23]. B. V. Salim, Chyntia, J. O. Indrawan, et al., "Face shape classification using swin transformer model," Procedia Comput. Sci., vol. 227, pp. 557–562, 2023.

[24]. Y. Z. Li, X. Yang, P. Sun, et al., "Celeb-DF: A large-scale challenging dataset for DeepFake forensics," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Seattle, WA, USA, pp. 3204–3213, 2020.

[25]. B. Dolhansky, J. Bitton, B. Pflaum, et al., "The DeepFake detection challenge (DFDC) dataset," arXiv preprint, arXiv:2006.07397, 2020.

[26]. B. J. Zi, M. H. Chang, J. J. Chen, et al., "WildDeepfake: A challenging real-world dataset for deepfake detection," in Proc. ACM Int. Conf. Multimedia, Seattle, WA, USA, pp. 2382–2390, 2020.

[27]. M. X. Tan and Q. V. Le, "EfficientNet: Rethinking model scaling for convolutional neural networks," in Proc. Int. Conf. Mach. Learn. (ICML), Long Beach, CA, USA, pp. 6105–6114, 2019.

[28]. J. Deng, W. Dong, R. Socher, et al., "ImageNet: A large-scale hierarchical image database," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Miami, FL, USA, pp. 248–255, 2009.

[29]. K. Simonyan, A. Vedaldi, and A. Zisserman, "Visual explanations from deep networks via gradient-based localization," in Proc. IEEE Int. Conf. Comput. Vis. (ICCV), Venice, Italy, pp. 618–626, 2017.

[30]. D. Afchar, V. Nozick, J. Yamagishi, et al., "MesoNet: A compact facial video forgery detection network," in Proc. IEEE Int. Workshop on Information Forensics and Security (WIFS), Hong Kong, China, pp. 1–7, 2018.

[31]. Z. Z. Liu, X. J. Qi, and P. H. S. Torr, "Global texture enhancement for fake face detection in the wild," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Seattle, WA, USA, pp. 8057–8066, 2020.

https://doi.org/10.63665/IJMEC.1104s.27
ISSN: 2456-4265
IJMEC 2026