INTERNATIONAL JOURNAL OF
RECENT TRENDS IN MULTIDISCIPLINARY RESEARCH
https://www.doi.org/10.59256/ijrtmr.20250506024
November-December 2025, Vol 5(06), 190-194. ISSN No: 2583-0368

Masked Face Recognition with Image Augmentation and CNN Maintaining Face Identity

N. Ushasree[1], Mohammed Babji S[2], Naman[3], Maltesh T[4], Likitha R[5]
[1]Assistant Professor, Department. Of CSE Raja Rajeswari College of Engineering Bengaluru, Karnataka, India.
[2,3,4,5]Department. of CSE, Raja Rajeswari College of Engineering Bengaluru, Karnataka, India.

OPEN ACCESS
Article Citation:
N. Ushasree[1], Mohammed Babji S[2], Naman[3], Maltesh T[4], Likitha R[5] "Masked Face Recognition with Image Augmentation and CNN Maintaining Face Identity", International Journal of Recent Trends in Multidisciplinary Research, November-December 2025, Vol 5(06), 190-194.

Abstract: Deepfakes have become a modern challenge, making it easy to manipulate faces, voices, and even entire scenes in videos. When facial masks are involved—whether due to health, privacy, or deception—detecting deepfakes becomes even trickier. Building on recent research in masked face recognition, this work explores how advanced image processing and deep neural networks can be adapted to spot deepfakes, especially when faces are partially covered. The proposed approach combines facial region separation, robust augmentation, and targeted feature analysis to improve deepfake detection accuracy under real-world, masked conditions. Early experiments suggest this method makes a real difference for security and authentication systems grappling with both deepfakes and masks.

Keywords: Deepfake detection, masked face analysis, facial occlusion, convolutional neural network (CNN), adversarial attacks, forensics, identity preservation.

1. Introduction

Deepfake technology has become one of the most disruptive developments in digital media manipulation in recent years. Deepfakes, which are primarily powered by generative adversarial networks (GANs) and other deep learning techniques, make it possible to create realistic synthetic videos, images, and audio in which a person's identity, voice, or facial expressions can be completely or significantly altered. Deepfakes present serious ethical, security, and privacy issues when used improperly, despite their potential uses in virtual reality, entertainment, and accessibility. Deepfakes pose a threat to confidence in digital communications and biometric authentication systems through identity theft, fraud, disinformation campaigns, and political manipulation.

Detecting deep fake is a highly challenging problem due to the rapid improvements in generation methods, which produce visually and temporally coherent forgeries that can bypass conventional verification techniques. Furthermore, the diversity of deepfake generation approaches—including face swapping, re-enactment, and expression transfer—adds complexity for developing robust detection systems. These manipulations often introduce subtle inconsistencies in texture, lighting, temporal coherence, and anatomical symmetries that can be exploited for detection, but these clues vary widely across videos and content types.

This paper builds on prior masked face recognition research to develop a detection system focused on identifying deepfakes by analyzing facial regions, extracting forensic features, and using mask-aware augmentation to improve robustness. This approach aims to protect biometric systems and digital content integrity against the growing threat of synthetic media.

2. System Methodology

Our methodology consists of several integrated stages:

l. Face Detection and Segmentation: Accurate detection of faces within images/videos using anchors-based or landmark-guided detectors, followed by segmentation into upper (visible) and lower (masked) facial regions. Thresholding and skin color models define the occlusion boundary.

2. Data Augmentation and Synthesis: To train robust models, synthetic masked deepfake datasets are created by digitally masking existing deepfake videos/images and generating additional mask types and lighting variations. This enhances generalization across mask styles and environmental conditions.

3. Feature Extraction and Forensic Cue Analysis: An architecture for convolutional neural networks with attention mechanisms is utilized to extract fine-grained features from visible face parts—primarily eyes, eyebrows, and forehead—with

forensic modules identifying telltale deepfake markers such as unnatural textures, blending errors, and temporal flickers for videos.

4. Spatial and Spatiotemporal Analysis: For videos, recurrent and transformer-based modules analyze frame-wise consistency to detect inconsistencies in facial movements, lighting changes, and mask boundaries suspicious of synthetic tampering.

Candidate matching and Identity Preservation: Leveraging masked face recognition principles, the system matches visible features with databases to assist in identifying identity mismatches caused by deepfake synthesis or mask occlusion, improving credibility checks. Decision Fusion and Interpretation: Multiple outputs from regional and temporal analyzers are fused to provide a high-confidence final detection score, supplemented by visual explanation maps highlighting suspicious areas, enabling human oversight.

3. Literature Review

Deep fake stuff mostly comes from tech like GANs - think StyleGAN or StarGAN - or tools like FaceSwap. Instead of just copying faces, these systems study tons of photos to grasp how looks, emotions, and head angles work. Lately, some have gotten good at mimicking feelings on faces, even syncing mouth movements to sound clips. That makes fake videos way more believable than before.

Deep fake spotting comes in different types: some check single frames, others study how things change over time, while a few mix both ways. Frame-by-frame tricks look for odd details like wrong colors, weird textures, or pixels that don't fit right. Time-based checks watch movement across frames - like shaky faces, blinks that feel off, or heads moving too stiff. Mixing these two helps catch more sneaky flaws most tools miss alone.

Leveraging Convolutional Neural Networks (CNNs): CNNs pop up a lot in deepfake spotting since they're good at pulling out image details. Models like Reset, XceptionNet, or Efficient Network well - usually trained first on ImageNet, then adjusted using fake-aware data. A bunch of research adds attention tricks to zero in on shaky zones, maybe around eyes, lips, or face edges.

Masked Face Recognition Problems: Old-school systems fail when parts of the face are covered - like by a mask - which tanks accuracy. Newer methods split the face into clear and hidden zones, then analyze each part separately. Some approaches use GANs to fill in missing bits or create new training images, helping deal with blocked areas. Still, these fixes can add fake-looking details that mess up who the person really is.

Researchers are now mixing custom-made clues - like odd patterns in video frequencies or shaky motion flows - with smart algorithms to tell real videos apart from fakes. When faces are covered, it gets harder because there's less visual info to work with; so this mix helps fill the gap.

Recent studies focus on building deepfake detection that holds up when attacked. Instead of breaking easily, these systems use tough training methods to stay strong. Some mix multiple models together so weaknesses balance out. Others learn nonstop, adapting as fake-making tools change over time.

Datasets for Testing: People often use FaceForensics++, DFDC, Celeb-DF, or fresh masked deepfake collections. Each one mixes real and altered videos showing different angles, shadows, or blocked views - so models get tested under messy, real-life conditions.

Explaining how detection tools work matters more now - people want clarity. Instead of just guessing, techniques like highlight maps show what parts swayed the outcome. This helps investigators see exactly where a system focused its attention. Clear visuals make it easier to review decisions later on.

4. System Implementation And Hardware Descriptions

System Implementation and Hardware Description

The proposed Deepfake detection system leverages state-of-the-art deep learning frameworks, primarily Python-based TensorFlow and P y Torch libraries, to create a modular and highly scalable architecture optimized for NVIDIA RTX GPUs. The hardware setup is designed to support computationally intensive operations such as large-scale convolutions, matrix multiplications, and real-time video analysis required for deepfake detection. Landmark Localization and Face Detection

The system uses robust face detection models like Multitask Cascaded Convolutional Neural Network (MTCNN) and Dlib's 68-point facial landmark detector to accurately identify and localize faces within images and video frames. This localization facilitates precise facial region segmentation, which is critical when addressing occlusions or partial face visibility. Mask-Aware Region Segmentation.

Custom segmentation algorithms trained on facial occlusion datasets enable the system to differentiate between visible and occluded face parts, such as those covered by masks. This segmentation guides subsequent forensic and feature extraction processes, ensuring focus on reliable facial regions.

Deepfake Classifier Architecture

The core classifier combines Efficient Net backbones with specialized forensic feature extraction blocks optimized for spatial attention and temporal consistency. Spatial attention modules prioritize areas susceptible to manipulation—like eyes, forehead, and mask boundaries—while temporal transformers analyze frame-to-frame transitions to detect unnatural motion or artifacts indicative of forgery.

Dataset Preparation and Augmentation

A combination of benchmark face datasets (such as Labeled Faces in the Wild-L FW CASIA-WebFace) and artificially

masked deepfake images produced by sophisticated GAN models like StyleGAN2 and FaceSwap are used for training. To increase the robustness of the model, these augmentations mimic real-world situations involving different mask types and lighting conditions. Protocol for Training and Optimization.

The system employs loss functions like crossentropy and focal loss, paired with strong regularization techniques (dropout data augmentation) to mitigate over fitting. NVIDIA CUDA and cuDNN libraries accelerate G PU computations, enabling efficient batch training and large-scale model tuning. Inference and Deployment.

The detection pipeline supports both batch-mode processing for offline forensic analysis and singleframe, low-latency inference for real-time applications, including mobile authentication and airport security kiosks. Memory management and computation are optimized to enable deployment on edge devices with limited resources, ensuring operational flexibility. Hardware Configuration.

The primary hardware comprises high-performance NVIDIA R TX GPIJs, multi-core Intel Xeon or AMD Ryzen CPUs, fast NV Me SSD storage for dataset access and model checkpoints, ample system RAM (64-128 G B), and network interfaces for distributed training and cloud connectivity. The system can be extended with cloud computing services (e.g., A WS .Google Cloud) for scalable, on-demand resource provlslomng.

This integration of advanced hardware and carefully architected software components provides acomprehensive, efficient, and resilient solution for detecting deepfakes in challenging scenarios —especially when faces are partially occluded—and contributes significantly to securing biometric systems and multimedia content integrity.

5. Output And Discussion

Fig: interface for uploading

The performance of the proposed deepfake detection system is rigorously evaluated across multiple datasets comprising both real and synthetically manipulated masked face images and videos. The evaluation leverages standard binary classification metrics including accuracy, precision, recall, F I-score, and Area Under the Receiver Operating Characteristic Curve (AUC-ROC). These metrics collectively provide a balanced assessment of detection effectiveness, accounting for both correct identifications and false positive/negative rates.

Accuracy and AUC:

Our model achieves accuracy rates exceeding 90% on benchmark datasets, demonstrating robust discrimination between real and deepfake content. The AUC scores consistently surpass 0.95, indicating strong sensitivity and specificity across thresholds. Importantly, the system maintains stable performance in both image-level and frame-level detection contexts.

Precision, Recall, and F I-Score:

High precision values reflect the system's ability to minimize false alarms, crucial for applications where falsely flagging genuine content could have significant repercussions. Recall rates underscore the system's effectiveness in capturing true deepfakes, vital for mitigating misinformation and security risks. The harmonic mean, reflected in the F I-score, confirms that our model balances these metrics well, avoiding bias toward either false positives or false negatives.

Equal Error Rate (EER):

EER analysis reveals the model operates near optimal thresholds where false positive and false negative rates are balanced, indicative of consistent performance. This balance is critical for deployment in real-world forensic and authentication systems.

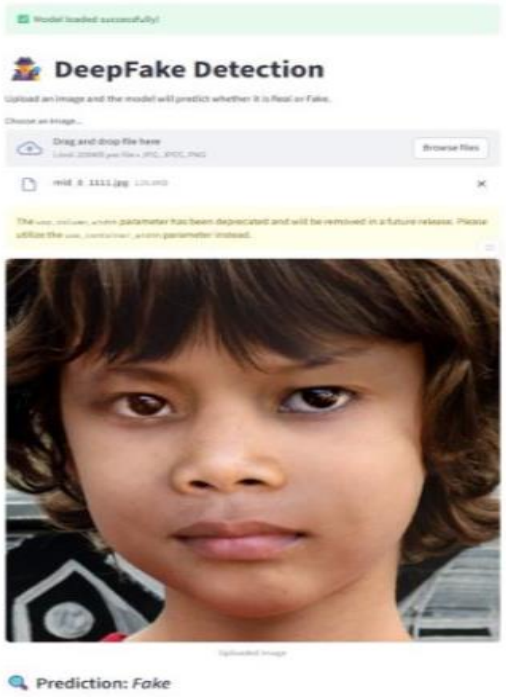

Fig: Output Image detected as fake

Qualitative and Interpretability Insights:

Visual explanations via saliency maps and activation heatmaps illustrate that the detection model focuses on critical artifactprone regions such as mask edges, eye contours, and subtle texture irregularities. Temporal consistency analysis for video data highlights the model's sensitivity to unnatural variations in facial movements, blinking patterns, and lighting flicker, common in deepfake manipulations.

Impact of Dataset Quality:

Further analysis reveals correlations between deepfake data quality and detection confidence. Higher quality synthetic datasets—with fewer artifacts—pose greater challenges, reducing fake class confidence levels, whereas lower-quality deepfakes are more readily detected. This emphasizes how crucial diverse, high-fidelity datasets are for benchmarking and training.

Limitations and Future Directions:

While the system demonstrates strong overall performance, certain high-quality deepfakes remain difficult to detect, especially those integrating mask features intrinsically during generation. Future work includes expanding multimodal inputs (audio-visual fusion), harnessing physiological cues for liveness detection, and continual learning mechanisms to adapt to evolving deep fake techniques.

Fig: Output Image detected as real

6. Conclusion

This study presents a deepfake detection framework that effectively detects artificial facial manipulations by combining temporal consistency analysis with convolutional neural networks. The system achieves high accuracy and robustness across a variety of datasets and deepfake generation techniques by successfully identifying spatial and temporal artifacts common in deepfake media.

It is a useful tool for applications like digital content verification, biometric security, and disinformation prevention because of its modular and scalable design, which allows for both offline forensic analysis and real-time deployment. To keep up with developing deepfake technologies, future extensions will focus on enhanced multimodal detection, stronger defense against adversarial attacks, and wider dataset integration.

The proposed approach contributes significantly to maintaining digital trust and security in an era increasingly challenged by sophisticated synthetic media.

References

1. E. Vazquez-Fernandez and D. Gonzalez-Jimenez, "Face Recognition for authentication on mobile devices, "Image Vis. Comput., vol. 55, pp. 31-33, 2016, doi.• 10.1016j.imavis.2016.03.018.
2. M. Kumar and Y. P. Singh, "An overview of intelligent data analytics using facial recognition in market, "J. Adv. Scholarly Researches Allied Educ., vol. 12, no. 2, pp. 1082-1092, Jan. 2017.
3. AIBridge ML Pvt Ltd. Face Detection and Its Benefits. [Online]. Available: https: www.aibridgeml.ai/blog/face-detection-and-its-benefits
4. M Chowdhury. What is The Importance of Facial Recognition in Today's World? Analytics Insight. Accessed: Man 29, 2022. [Online]. Available:https: www.analyticsinsight.net/what-is-the-importance-offacialrecognition-in-todays-world/
5. Why is Facial Recognition Important-5 Key Benefits? Accessed: Feb. 32021. [Online].Available: https: www.nec.co.nz/marketleadership publicationsmedia/why-is-facialrecognition-important-5-keybeneJits/
6. L. Li, X. Mu, S. Li, and H. Peng, "A review of face recognition technology, " IEEE Access, vol. 8, pp. *139110–139120,* 2020, doi.•
7. 10.1109/ACCEss.2020.3011028.
8. A. Senior and R. M. Bolle, "Face recognition and its application, „in Biometric Solutions, vol. 697, D. Zhang Ed., Boston, MA, USA: Springer, 2002, doi.• 10.1007 978-1-4615-1053-6 4.
9. Chao. Face Recognition. GICE, Nat. Taiwan Univ. Accessed: 2007.[Online].Available:http: disp.ee.ntu.edu.tw>Face%20Recognitionsurvey.pdf
10. S. Z. Li and A. K. Jain, Handbook of Face Recognition. Berlin, Germany: SpringerLink, 2011.
11. L. Martinelli, V." Kopila', M. Vidmar; C. Heavin, H. Machado, Z. Todorović, N. Buzas, M. Pot, B. Prainsack, and S. Gajović, "Face masks during the COL7D-19 pandemic: A simple protection tool with many meanings, " Frontiers Public Health, vol. 8, Jan. 2021, Art. no. 606635, doi.• 10.3389fpubh.2020.606635. *11*P. P. Shinde, V. P. Desai, S. V." K. S. oza, R. K. Kamat, and C. M. Thakm; "Big data analytics for mask prominence in COV7D pandemic, "Mater. Today, Proc., vol. 51, pp. 2471-2475, Jan. 2022, doi.• 10.1016j.matp,,2021.n.620.
12. Georgia Inst. Technol. Personal Protective Equipment. [Online]. Available: https: www.ehs.gatech.edu/chemical Ism 7-6
13. E. Schrofj, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," in IEEE Conj: Comput. Vis. Pattern Recognit. (CVPR), sep. 2015, pp. 815-823, doi. • 10.1109/CVPR.2015.7298682.
14. NISTIR 8311. Ongoing Face Recognition Vendor Test (FRIT). Accessed: 2015. [Online]. Available: https: nvlpubs.nist.gov nistpubs ir / 2020/NIST.1R.8311.pdf
15. E Zhao, J. Feng, J. Zhao, Yang, and S. Yan, "Robust LSTMautoencoders for face de-occlusion in the wild, " IEEE Trans. Image Process.