International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 10 | Oct – 2025 DOI: 10.55041/ISJEM05133
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

NoMask.AI – AI Vs Human Face Detection

Mrs.I.A.Jannathul Firthous[1], Laksha.K[2], Mawiyah.H[3], Rithika.K.P[4]

[1,2,3,4]Information Technology, Sri Shakthi Institute of Engineering and Technology

---

Abstract - This document expressions the rapid advancements in artificial intelligence have enabled the creation of hyper-realistic synthetic faces that are nearly indistinguishable from genuine human faces. While this represents a significant technological milestone, it also poses critical challenges related to digital ethics, identity verification, and online security. **NoMask.AI** addresses this growing concern by providing an intelligent solution capable of distinguishing between real and AI-generated faces. The system employs a refined **ResNet-18 convolutional neural network**, trained on diverse datasets containing both authentic and synthetic facial images. Using **OpenCV** for face detection and preprocessing, and **PyTorch** for deep learning model inference, NoMask.AI performs probability-based classification to determine facial authenticity. A user-friendly **Flask-based web interface**, designed with **HTML and CSS**, enables seamless interaction and real-time detection. By integrating deep learning with practical usability, NoMask.AI enhances trust and security in digital environments, offering a robust defense against AI-generated identity fraud.

Key Words: Artificial Intelligence, Deepfake Detection, ResNet-18, Convolutional Neural Network, OpenCV, Digital Security

1. INTRODUCTION

The emergence of artificial intelligence has enabled the creation of hyper-realistic synthetic faces that closely resemble real humans, leading to concerns about digital identity, security, and misinformation. To address these challenges, **NoMask.AI** is developed as an intelligent system capable of distinguishing real human faces from AI-generated ones. It utilizes a refined **ResNet-18 convolutional neural network** trained on datasets containing both real and synthetic faces, with **OpenCV** for facial detection and **PyTorch** for model inference. The system's **Flask-based web interface**, designed using **HTML and CSS**, ensures a simple and efficient user experience. By providing accurate and reliable face authenticity detection, NoMask.AI strengthens digital security and trust in online interactions.

2. REVIEW OF LITERATURE

The rapid advancement of artificial intelligence and deep learning has led to significant progress in both **synthetic face generation** and **deepfake detection**. Early studies focused on GAN-based models such as StyleGAN and DeepFake, which demonstrated the ability to create highly realistic facial images. To counter this, researchers explored **deep learning-based detection techniques**, primarily using CNN architectures like ResNet, XceptionNet, and VGG for feature extraction and classification. Benchmark datasets such as **FaceForensics++**, **DFDC**, and **Celeb-DF** have been instrumental in evaluating model performance and generalization. Recent works also investigate **frequency domain analysis**, **physiological signal detection**, and **multi-modal fusion** methods to improve robustness against evolving generative models. Despite these advances, challenges remain in real-time detection, dataset bias, and cross-domain generalization, motivating the development of efficient systems like **NoMask.AI** for reliable face authenticity verification.

2.1. Historical Context and Evolution

Facial recognition initially relied on traditional machine learning methods like PCA and LDA, which offered limited accuracy under varying conditions. The rise of **deep learning** and **Convolutional Neural Networks (CNNs)** transformed face analysis by enabling automatic feature extraction from large datasets. In 2014, **Generative Adversarial Networks (GANs)** introduced the ability to generate highly realistic synthetic faces, leading to the spread of **deepfakes** and related security concerns. As these synthetic techniques evolved, researchers began developing advanced detection systems using deep neural networks and hybrid models. Building on this evolution, **NoMask.AI** leverages modern CNN architectures to accurately distinguish real human faces from AI-generated ones in real time.

2.2. Deepfake Detection Using CNN Architectures

Convolutional Neural Networks (CNNs) play a vital role in deepfake detection by identifying subtle visual inconsistencies in facial images. Models such as **ResNet**, **XceptionNet**, and **VGGNet** effectively learn texture and spatial features that distinguish real faces from AI-generated ones. Using these principles, **NoMask.AI** employs a refined **ResNet-18** model to achieve accurate and real-time detection of synthetic faces.

2.3. Datasets for Deepfake Detection

The performance of deepfake detection models heavily depends on the quality and diversity of datasets used for training. Popular benchmark datasets such as **FaceForensics++**, **DeepFake Detection Challenge (DFDC)**, **Celeb-DF**, and **DF-TIMIT** provide large collections of both real and manipulated facial images or videos. These datasets include variations in lighting, pose, and compression levels, helping models learn generalized features for reliable detection. **NoMask.AI** utilizes such mixed datasets to train its **ResNet-18** model, ensuring robustness in distinguishing between real and AI-generated faces under different conditions.

2.4. Research Gaps and Motivation for NoMask.AI

Despite significant progress in deepfake detection, existing models often face limitations in **real-time performance, generalization across datasets, and ease of deployment**. Many approaches require high computational power or fail to maintain accuracy when exposed to new generative models and compression artifacts. Additionally, few systems offer

user-friendly interfaces that allow non-technical users to verify facial authenticity effectively. These gaps highlight the need for a lightweight, accurate, and accessible detection system. Motivated by this, **NoMask.AI** is developed as an efficient and practical solution using a refined **ResNet-18 CNN**, integrated with a simple **Flask-based web interface** to provide reliable real-time detection of AI-generated faces.

3. EXISTING SYSTEMS

Existing deepfake detection systems primarily rely on deep learning architectures such as **XceptionNet**, **VGGNet**, and **ResNet** for identifying manipulated or AI-generated faces. These models analyze spatial and temporal inconsistencies, texture differences, and pixel-level artifacts to classify images as real or fake. While effective in controlled environments, most of these systems require **high computational resources**, are **limited to offline processing**, and often lack **real-time detection capabilities**. Moreover, many existing solutions do not provide **user-friendly interfaces** for practical use, restricting accessibility to researchers and developers. These limitations emphasize the need for a lightweight, real-time, and easily deployable solution like **NoMask.AI**.

4. FIELD OF INVENTION

The present work relates to the field of **artificial intelligence**, specifically within the domains of **computer vision**, **deep learning**, and **facial image analysis**. It focuses on developing an intelligent system capable of distinguishing between **real human faces and AI-generated (synthetic) faces** in real time. The invention combines **convolutional neural networks (CNNs)** with **image processing techniques** using **OpenCV** and **PyTorch** frameworks to achieve high detection accuracy. Furthermore, it incorporates a **Flask-based web interface** designed with **HTML and CSS**, enabling seamless user interaction and real-time verification. This invention is particularly applicable to areas such as **digital forensics**, **cybersecurity**, **identity verification systems**, and **media authentication**, providing a robust solution against the growing threat of AI-generated facial content and deepfakes.

5. SCREENSHOTS

Fig -1: Human Image Detection

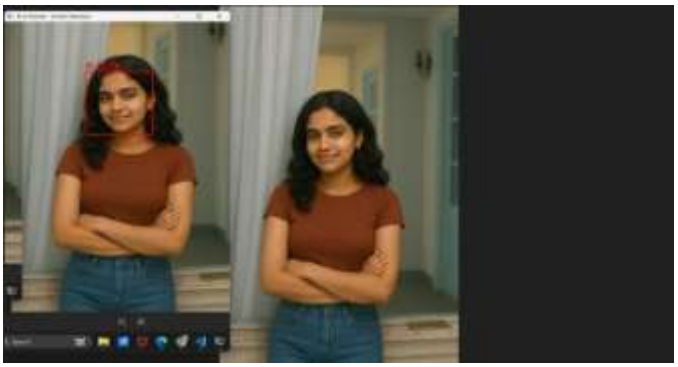

Fig -2: AI Image Detection

3. CONCLUSIONS

The emergence of AI-generated synthetic faces has raised serious concerns regarding digital identity, privacy, and security. To address these issues, **NoMask.AI** presents an effective solution capable of distinguishing between real and AI-generated faces using a refined **ResNet-18 convolutional neural network**. By integrating **OpenCV** for facial detection, **PyTorch** for model inference, and a **Flask-based web interface**, the system ensures accurate, efficient, and user-friendly real-time detection. The results demonstrate that deep learning models, when optimized and properly trained on diverse datasets, can reliably identify synthetic facial content. Overall, NoMask.AI contributes to enhancing **digital trust**, **cybersecurity**, and **identity verification** by offering a practical and scalable AI-driven face authentication system. Future work may include extending the model to video-based detection and improving robustness against emerging generative models.

ACKNOWLEDGEMENT

The authors would like to express their heartfelt gratitude to their **project guide** and **faculty members** of the **Department of Information Technology, Sri Shakthi Institute of Engineering and Technology**, for their continuous support, valuable guidance, and encouragement throughout the development of this project. The authors also extend sincere thanks to their **friends and peers** for their constructive feedback and collaboration during the research and implementation phases. Lastly, special appreciation goes to all those who contributed directly or indirectly to the successful completion of **NoMask.AI**, a project aimed at promoting safer and more secure digital interactions.

REFERENCES

1. I. Goodfellow, J. Pouget-Abadie, M. Mirza et al., “Generative Adversarial Nets,” Advances in Neural Information Processing Systems (NeurIPS), 2014.

2. T. Karras, S. Laine, and T. Aila, “A Style-Based Generator Architecture for Generative Adversarial Networks,” IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2019.

3. A. Rossler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Nießner, “FaceForensics++: Learning to Detect Manipulated Facial Images,” IEEE/CVF International Conference on Computer Vision (ICCV), 2019.

4. B. Dolhansky et al., “The DeepFake Detection Challenge (DFDC) Dataset,” arXiv preprint arXiv:2006.07397, 2020.

5. Y. Li, M.-C. Chang, and S. Lyu, “Celeb-DF: A Large-Scale Challenging Dataset for DeepFake Forensics,” IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2020.

6. F. Chollet, “Xception: Deep Learning with Depthwise Separable Convolutions,” IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2017.

7. K. He, X. Zhang, S. Ren, and J. Sun, “Deep Residual Learning for Image Recognition,” IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2016.

8. M. Afchar, V. Nozick, J. Yamagishi, and I. Echizen, “MesoNet: A Compact Facial Video Forgery Detection Network,” IEEE International Workshop on Information Forensics and Security (WIFS), 2018.

9. D. Güera and E. J. Delp, “Deepfake Video Detection Using Recurrent Neural Networks,” IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), 2018.

10. S. Agarwal et al., “Protecting World Leaders Against Deep Fakes,” IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2019.