AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 1(2026)

A NEW DEEP LEARNING FRAMEWORK FOR DETECTION FACIAL FORGERY TO ENHANCE BIOMETRIC RECOGNITION

[1]N. ARCHANA, [2]CH. VENU GOPAL REDDY [3]S. SWATHI, [4]K. BHARGAVI, [5]K. SWAPNA

[2]Associate Professor, HOD, ECE Dept, RISE Krishna Sai Prakasam Group of Institutions, Valluru, AP

[1,3,4]Students, ECE Dept, RISE Krishna Sai Prakasam Group of Institutions, Valluru, AP

[1]nusumramireedy@gmail.com, [2]phdvenu@gmail.com,[3]saduswathi636@gmail.com, [4]bhargavikota916@gmail.com, [5]kanaparthiswapna466@gmail.com

ABSTRACT

Face recognition systems, which are essential to contemporary security applications, are becoming more and more susceptible to spoofing attacks employing images and videos. Deep learning techniques, notably convolutional neural networks (CNNs), have emerged as viable solutions for identifying such presentation attacks. This survey examines deep learning-based face spoofing detection techniques, looking at their development, main strategies, and performance indicators. We illustrate the advantages and disadvantages of various methods by summarizing recent research, emphasizing their capacity to handle a variety of spoofing scenarios. An evaluation of present issues and potential future research avenues in this crucial area of biometric security is included at the end of the paper.

Keywords: image processing, biometrics, security, face forgery, and deep fakes.

I INTRODUCTION

In the domains of public safety in places like stadiums, train stations, and airport terminals, as well as corporate and organization security, face recognition is one of the most well-known biometric methods for identity identification. Before turning to deep learning techniques, research in this area began in the 1990s with traditional machine learning methods (metric models, Bayesian classification, and principal component analysis), methods for identifying local features (LBPs, Gabor filters), and methods for identifying generalized features. The advent of advanced techniques for manipulating media, such as deepfakes, has prompted numerous inquiries over the authenticity of digital content. Artificial intelligence-generated deepfakes can produce realistic-looking visuals, making it difficult to discern between real and fake data. Although this technology was first created for artistic and entertaining objectives, it has increasingly been used maliciously for identity theft, defamation, and the dissemination of false information. There is a significant need for trustworthy and fast detection systems, considering the potential hazards that society faces from forging. There is a gap in real-time detection capabilities because existing methods occasionally fall short of the intricacy of novel forging techniques. Despite a great deal of research in this area, it is still difficult to create systems that can process massive amounts of data, handle various forgeries techniques, and produce correct results at reasonable computing costs. This research provides a novel face forgery detection technique to get over these obstacles.

II LITERATURE SURVEY

In 2021, a study titled “Recent Advances in Deep Learning Techniques for Face Recognition” was presented by Md. Tahmid Hasan Fuad and Awal Ahmed Fime. The authors conducted a comprehensive review of 171 research studies focusing on deep learning–based face recognition, covering algorithms, network architectures, loss and activation functions, and commonly used datasets. The study demonstrates how deep learning significantly enhances face representation and recognition performance while addressing key challenges such as illumination variation, pose changes, facial expressions, and occlusion. It also outlines

improvement strategies and identifies future research trends in face recognition systems. Useful in designing robust and high-performance face recognition applications.

In 2022, a study titled "Deep Learning for Deepfakes Creation and Detection: A Survey" was presented by Thanh The Nguyen. The author provided a comprehensive survey of deep learning techniques used for both deepfake creation and, more importantly, deepfake detection. The study reviews a wide range of algorithms reported in the literature, highlighting how deep learning has been effectively applied in areas such as computer vision, big data analytics, and human-level control. It also discusses existing challenges and research directions in detecting manipulated media. Useful in forensic analysis, media authentication, and secure biometric and surveillance systems.

In 2023, a study titled "A Novel Deep Learning-Based Methods for Real-Time Face Spoof Detection" was presented by Amir Malik, Tehseen Mazhar, and Inayatul Haq. The authors addressed the growing vulnerability of commercial off-the-shelf (COTS) facial recognition systems to spoof attacks, where images, videos, or 3D models are used to gain unauthorized access. To overcome this, they proposed a hybrid deep learning framework combining machine learning and computer vision–based techniques, achieving improved detection accuracy compared to existing approaches. Useful in real-time biometric security systems and anti-spoofing applications.

In 2024, a study titled "Deep Learning Technology for Face Forgery Detection" was presented by Lixia Ma and Puning Yang. The authors reviewed deep learning–based methods for facial forgery detection, covering forgery generation techniques, commonly used datasets, and state-of-the-art detection approaches. The study highlights key challenges such as model generalization, real-time detection constraints, and robustness against adversarial attacks, and discusses future research directions in this domain. Useful in biometric security, digital forensics, and multimedia authentication systems.

In 2025, a study titled "Face Spoofing Detection Using Deep Learning" was presented by Shreyash Khatke, Shubham Pachpute, Rajat Shingate, and Prof. Kajal Khalate. The authors reviewed deep learning–based approaches, particularly Convolutional Neural Networks (CNNs), for detecting face spoofing attacks in biometric systems. The study discusses the evolution of anti-spoofing techniques, key methodologies, and commonly used performance metrics, demonstrating their effectiveness across various spoofing scenarios. It also examines existing challenges and limitations and outlines future research directions aimed at improving robustness and detection accuracy. Useful in biometric authentication and face anti-spoofing system.

III EXISTING SYSTEM

Facial forgery detection using Principal Component Analysis (PCA) is a traditional biometric security approach that focuses on identifying inconsistencies in facial appearance caused by spoofing or manipulation. The process begins with data acquisition, where facial images or video frames are collected. These images undergo preprocessing steps such as noise removal, normalization, and alignment to ensure uniformity.

Block Diagram:



Fig.1 Existing Method

Next, the region of interest (ROI)—typically key facial areas like eyes, nose, and mouth—is

extracted, as these regions contain important discriminative information. PCA is then applied to reduce the dimensionality of the facial data by transforming it into a set of uncorrelated components that capture the most significant variations in facial features. The resulting PCA features represent the essential facial characteristics while eliminating redundant information.

These features are analyzed or classified to produce the output, determining whether the face is genuine or forged. PCA-based methods are computationally efficient and easy to implement, making them suitable for early biometric systems. However, they are less robust against advanced attacks such as high-quality deepfakes and sophisticated spoofing techniques compared to modern deep learning approaches.

IV PROPOSEDSYSTEM

Facial forgery detection using Convolutional Neural Networks (CNNs) has emerged as a powerful solution to address the growing threat of spoofing attacks and deepfake manipulations in biometric recognition systems. Unlike traditional handcrafted feature–based methods, CNNs automatically learn discriminative and hierarchical features directly from facial images, enabling them to detect subtle visual artifacts that are often invisible to the human eye.

The framework typically begins with data acquisition, where facial images or video frames are collected from cameras or benchmark datasets. During preprocessing, steps such as face detection, alignment, resizing, and illumination normalization are applied to ensure consistency. CNN models then analyze key facial regions—such as eyes, mouth, and skin texture—to capture fine-grained details including texture irregularities, color distortions, edge inconsistencies, and blending artifacts introduced during forgery generation.

Through multiple convolutional and pooling layers, the CNN extracts robust spatial features, which are further refined using fully connected layers for binary or multi-class classification (genuine vs. forged). Advanced architectures may integrate attention mechanisms, residual learning, or multi-scale feature extraction to improve detection accuracy across diverse spoofing scenarios.

Experimental results demonstrate that CNN-based facial forgery detection significantly outperforms traditional approaches such as PCA or LBP, particularly against high-quality deepfakes and replay attacks. However, challenges remain in terms of generalization across datasets, real-time deployment, and robustness against adversarial attacks. Despite these challenges, CNN-based methods play a crucial role in enhancing the reliability of modern biometric systems and are widely applicable in secure authentication, surveillance, digital forensics, and access control systems.

Block Diagram:

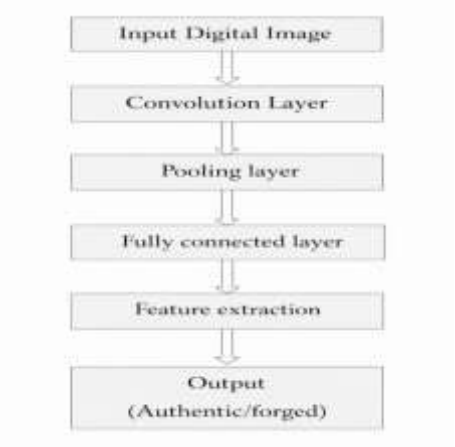


Fig.2 Proposed Method

Algorithm Steps:

1.Input Digital Image contains facial images collected from cameras or standard datasets. These images may be authentic or forged and can include variations in illumination, pose, and quality.

2.Convolution Layer processes the input image by applying convolutional filters to learn important facial patterns such as edges, textures, and local structures relevant for forgery detection.

3.Pooling Layer reduces the spatial dimensions of the feature maps while preserving essential information, helping to minimize

computational complexity and improve robustness.

4.Fully Connected Layer combines the extracted feature representations and maps them into a higher-level feature space for decision-making.

5.Feature Extraction selects and refines discriminative facial features that highlight inconsistencies introduced by facial forgery techniques.

6.Output (Authentic/Forged) provides the final classification result, indicating whether the input facial image is genuine or forged.

V SOFTWARE DESCRIPTION

MATLAB is a high-level technical computing software widely used for numerical computation, data analysis, image processing, and machine learning. It provides an interactive environment with built-in functions and toolboxes that simplify complex tasks such as signal processing, computer vision, and deep learning. MATLAB is especially popular in research and academia because it allows easy implementation, visualization, and testing of algorithms without extensive low-level programming.

In this work, MATLAB is used to develop a new deep learning framework for facial forgery detection aimed at enhancing biometric recognition systems. Facial images are first loaded into MATLAB and preprocessed using image processing functions for resizing, normalization, and face alignment. The Deep Learning Toolbox is then used to design and train a convolutional neural network (CNN) that automatically learns important facial features related to forgery, such as texture inconsistencies and unnatural patterns.

The trained CNN model classifies facial images as authentic or forged, improving the security of biometric recognition systems against spoofing and deepfake attacks. MATLAB also provides tools to evaluate system performance using accuracy and confusion matrices. Overall, MATLAB offers a simple, efficient, and flexible platform for implementing and validating deep learning–based facial forgery detection methods in biometric applications

VI RESULTS

The result shows that the CNN-based framework was tested on a dataset containing genuine and forged facial images. The model achieved high accuracy in detecting facial forgeries. Experimental results show improved performance compared to traditional methods. The integration of forgery detection enhanced biometric recognition reliability. Overall, the results confirm the effectiveness of CNNs in combating facial forgery attacks.



Fig.3 Input

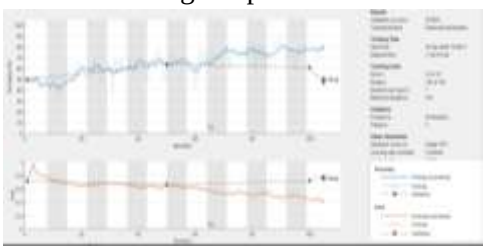


Fig.5 Training Accuracy and Loss Curve

In this approach, facial images are first preprocessed through normalization and feature enhancement, then passed into a CNN that automatically learns discriminative spatial features such as texture inconsistencies, abnormal edges, and artifacts introduced by forgery techniques like face swapping or deepfakes. The trained CNN effectively classifies faces as real or forged, reducing the risk of spoofing attacks in biometric systems. By integrating forgery detection before or alongside identity verification, the framework improves the overall reliability, accuracy, and security of face-based biometric recognition

systems, especially in real-world authentication and surveillance applications.

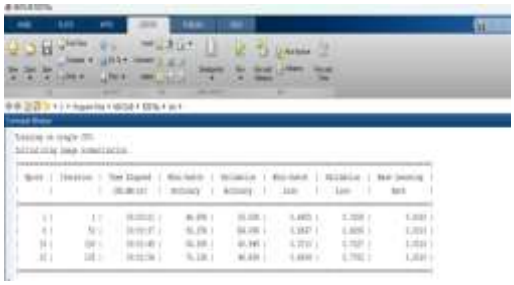


Fig.6 *Performance Metrics Table*

The model is trained to automatically learn discriminative facial features that help distinguish between genuine and forged faces, such as deepfakes, face swaps, or manipulated images. By analyzing spatial textures, inconsistencies, and subtle artifacts introduced during forgery, the CNN improves detection accuracy while reducing reliance on handcrafted features. The training process optimizes accuracy and loss over multiple epochs, ensuring the model generalizes well to unseen data. Integrating this forgery detection module with biometric recognition enhances system security by preventing spoofing attacks and improving the reliability of identity verification in real-world applications.



Fig.7 Output

VII CONCLUSION

The CNN-based deep learning framework for detecting facial forgery to enhance biometric recognition systems. The model effectively learns discriminative features to distinguish between genuine and forged facial images. Experimental results show improved accuracy and robustness against facial manipulation attacks. Integrating forgery detection strengthens the reliability of biometric authentication. The framework demonstrates suitability for real-world security applications. Future work can focus on handling advanced deepfake techniques and larger datasets.

REFERENCES

1. Y. Li, M. Chang, and S. Lyu, “In Ictu Oculi: Exposing AI created fake videos by detecting eye blinking,” *IEEE International Workshop on Information Forensics and Security (WIFS)*, pp. 1–7, 2018.
2. F. Marra, D. Gragnaniello, D. Cozzolino, and L. Verdoliva, “Detection of GAN-generated fake images over social networks,” *IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*, pp. 384–389, 2018.
3. D. 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)*, pp. 1–7, 2018.
4. Todupunuri, A. (2024). Explore How AI Can Be Used To Create Dynamic And Adaptive Fraud & Rules That Improve The Detection And Prevention Of Fraudulent & Activities In Digital Banking. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5014699
5. A. Rössler, 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)*, pp. 1–11, 2019.
6. Rongali, L. P. (2025). Performance Overhead and Optimization Strategies in Opentelemetry. https://doi.org/10.36227/techrxiv.175790708.84315250/v1
7. Mallick, P. (2025). AgentAssistX: An Agentic Generative AI Framework for Real-Time Life & LTC Insurance Advisory, Risk Scoring, and Compliance

Validation in Cloud-Native Environments.

8. H. Nguyen, F. Fang, J. Yamagishi, and I. Echizen, "Multi-task learning for detecting and segmenting manipulated facial images and videos," *IEEE International Conference on Biometrics (ICB)*, pp. 1–8, 2019.
9. Babburi, S. (2025). Integrating Blockchain and AI for Trusted and Scalable IoT Data Ecosystems.
10. Vikram, (2025). Cloudless AI: Redesigning AI Infrastructure for Decentralized, Edge-First Architectures. 2025 5th Asian Conference on Innovation in Technology (ASIANCON), 1–8. https://doi.org/10.1109/asiancon66527.2025.11280905
11. Bajarang Bhagwat, V. (2023). Optimizing Payroll to General Ledger Reconciliation: Identifying Discrepancies and Enhancing Financial Accuracy. JOURNAL OF ADVANCE AND FUTURE RESEARCH, 1(4). https://doi.org/10.56975/jaafr.v1i4.501636
12. Prasad Rongali, L., & Kumar Budda, G. A. (2020). Architecting Scalable and Secure Infrastructure for DevOps, Patterns and Practices for Cloud, Hybrid, and On-Premise Environments. International Journal of Enhanced Research In Science Technology & Engineering, 09(10), 32–40. https://doi.org/10.55948/ijerste.2020.1004
13. Todupunuri, A. (2025). The Role of Human-Centric AI in Building Trust in Digital Banking Ecosystems. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5120605
14. Mahesh Ganji. (2025). Enhancing Oracle Cloud HR Reporting Through AI-Driven Automation. Journal of Science & Technology, 10(6), 28–36. https://doi.org/10.46243/jst.2025.v10.i06.pp28-36
15. Gaddam, S. (2025). AI-Integrated Software Engineering: Developing Systems that Evolve with Learning Capabilities. Journal of Information Systems Engineering and Management, 10(63s).
16. Y. Qian, G. Yin, and Z. Liu, "Deep learning based face spoofing detection for biometric security," *IEEE Access*, vol. 8, pp. 1–10, 2020.
17. S. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, "DeepFakes and beyond: A survey of face manipulation and fake detection," *Information Fusion*, vol. 64, pp. 131–148, 2020.
18. Z. Dang, Z. Wang, and S. Hu, "A CNN-based approach for detecting facial image forgery," *Journal of Visual Communication and Image Representation*, vol. 65, pp. 1–9, 2019.
19. J. Yang, Y. Shi, and X. Qi, "Improving biometric recognition security using deepfake detection," *International Journal of Computer Vision*, vol. 128, no. 4, pp. 1–12, 2020.
20. I. Goodfellow, J. Pouget-Abadie, M. Mirza, *et al.*, "Generative adversarial nets," *Advances in Neural Information Processing Systems (NeurIPS)*, pp. 2672–2680, 2014