Pages:50-58
Global Knowledge Academy (GNA) Volume-V, Issue-IV (2024)
https://globalknowledgeacademy.com/

Securing eCommerce Payments with DeepFake-Aware Facial Biometrics

Zunaira Rafaqat
Chenab Institute of Information Technology, Pakistan
Corresponding E-mail: zunaira.rafaqat@cgc.edu.pk

Abstract

The rapid digitization of financial services has increased the reliance on biometric systems, particularly facial recognition, for seamless identity verification in eCommerce transactions. However, the emergence of sophisticated DeepFake techniques has introduced a substantial new attack surface for adversaries to manipulate facial biometrics and bypass authentication systems. This paper investigates a DeepFake-aware biometric verification framework designed to harden payment systems against synthetic facial forgeries. The study explores the vulnerabilities of existing face-ID mechanisms, evaluates modern DeepFake generation pipelines, and proposes a hybrid detection architecture leveraging Convolutional Neural Networks (CNNs) combined with Vision Transformers (ViTs). Experimental evaluations are conducted using publicly available DeepFake datasets and custom eCommerce-oriented attack samples. The results demonstrate that traditional facial recognition systems experience drastic drops in accuracy under adversarial synthetic faces, whereas the proposed DeepFake-aware facial biometric framework significantly enhances fraudulent detection rates while maintaining high verification reliability. This paper contributes actionable insights for secure digital payments, offering a scalable and robust defense mechanism for real-world financial platforms.

Keywords: DeepFake detection, facial biometrics, eCommerce security, payment authentication, CNN-Transformer models, identity fraud prevention, digital finance security

I. Introduction

The global rise of eCommerce has driven unprecedented demand for secure and user-friendly payment authentication mechanisms. Among these, facial biometrics have emerged as a preferred approach due to their convenience, contactless operation, and seamless integration with

modern smartphones [1]. However, this increasing reliance has simultaneously made facial recognition a high-value target for cybercriminals seeking unauthorized access to financial accounts. The rapid evolution of DeepFake technology—powered by Generative Adversarial Networks (GANs) and diffusion models—has dramatically amplified this threat. Attackers can now generate hyper-realistic fake faces capable of deceiving traditional biometric systems, thereby undermining the integrity of digital payments. This challenge calls for next-generation authentication models that are not only accurate but also DeepFake-aware.

DeepFake attacks fundamentally disrupt the premise of facial biometrics by exploiting their visual nature. Historically, facial recognition systems were designed to operate under the assumption that facial features captured on camera originated from a live human subject. DeepFake synthesis breaks this assumption by introducing high-fidelity, frame-consistent artificial faces that mimic legitimate users with alarming precision. As the technology becomes more accessible, adversaries no longer require high-end computational resources; even mid-range consumer hardware and online DeepFake applications are capable of producing sophisticated forgeries. This democratization of DeepFake capabilities creates a pressing need to reevaluate security models within eCommerce ecosystems. Several existing defenses attempt to mitigate such risks through liveness detection, blink detection, or micro-expression analysis. Moreover, many commercial systems rely on static images or short-duration video samples, making them even more susceptible to being deceived by high-resolution synthetic media. The inadequacy of legacy defenses highlights the importance of designing a new framework—one that integrates DeepFake detection at its core rather than as an auxiliary component.

In addition to external threats, financial service providers face internal challenges in maintaining trust and compliance. Regulatory frameworks such as PSD2, KYC, and AML mandate strong identity verification protocols, and DeepFake vulnerabilities directly threaten the compliance posture of digital payment platforms [2]. A successful DeepFake attack not only compromises financial assets but also undermines consumer confidence in biometric authentication. Thus, reinforcing facial recognition within eCommerce platforms is both a technical necessity and a regulatory imperative. Given these challenges, this research aims to propose and validate a DeepFake-aware facial biometric verification system that integrates advanced CNN-ViT feature

extraction, multimodal liveness prediction, and adversarial training. By focusing specifically on eCommerce transaction workflows, this study bridges the gap between academic DeepFake research and real-world financial application environments. The findings demonstrate that a properly trained DeepFake detection module significantly reduces successful synthetic attacks and strengthens the reliability of biometric payments [3].

II. Related Work

DeepFake research has grown rapidly over the past few years, with significant advancements in both generative and defensive techniques. Early DeepFake models relied on autoencoders and simple GANs, producing low-quality facial forgeries with visible artifacts. However, continuous improvements, including StyleGAN, Face2Face, and diffusion-based generators, have reduced visual inconsistencies to the point where even human observers struggle to identify manipulation. Prior studies have analyzed these models in entertainment contexts, misinformation spread, and political manipulation, but fewer works have focused on their implications for financial authentication systems—an area where the impact of synthetic identity attacks can be catastrophic [4].

Traditional facial biometric systems have been widely deployed in smartphones, banking apps, and fintech platforms. Many use CNN-based face embeddings such as FaceNet or ArcFace, which offer high verification accuracy under normal conditions. However, multiple studies have demonstrated that these systems are ill-equipped to handle adversarial synthetic faces. Research shows that DeepFake images can achieve face embedding similarities comparable to real faces, causing verification systems to accept forged identities. This limitation is exacerbated by the lack of standardized DeepFake benchmarks tailored to payment verification contexts. On the defensive side, numerous approaches have been proposed to detect DeepFake media, including frequency-domain analysis, spatial artifact inspection, temporal modeling, and physiological signal reconstruction (e.g., rPPG). While these methods achieve promising results in controlled environments, their performance degrades in real-time authentication workflows where lighting conditions, device cameras, and user behavior vary significantly. Recent works have explored hybrid architectures combining CNNs with Transformers, allowing models to capture both local

textures and global contextual relationships in facial images [5]. These architectures have shown strong potential for synthetic face detection but have rarely been adapted specifically for secure financial transactions. Additionally, adversarial training has emerged as a powerful technique to harden models against manipulated inputs, yet its application in biometric payment security remains underexplored [6].

Existing literature thus indicates a critical gap: the need for a DeepFake-aware biometric verification system designed specifically for the security constraints and operational workflows of eCommerce payments. This research addresses that gap by developing an integrated authentication pipeline capable of detecting DeepFake forgeries while maintaining fast, reliable verification for legitimate users.

III. Methodology

The proposed DeepFake-aware facial biometric payment system employs a hybrid architecture combining Convolutional Neural Networks (CNNs) for low-level texture extraction and Vision Transformers (ViTs) for global spatial reasoning. The CNN component is responsible for detecting subtle pixel-level anomalies commonly found in synthetic faces, such as inconsistent pore patterns, unnatural reflections, and frequency distortions. Meanwhile, the Transformer module identifies high-level inconsistencies across facial regions, capturing structural irregularities introduced during DeepFake generation. This multi-stage feature extraction produces robust embeddings resistant to synthetic manipulation.

Data preparation plays a central role in the methodology. The training dataset includes a blend of authentic facial images from open-source biometric collections and DeepFake samples sourced from DFDC, FaceForensics++, and custom-generated eCommerce attack scenarios. These custom samples simulate real-world payment flows, including manipulated user logins, account recovery attempts, and verification requests [7]. To enhance generalization, augmentation techniques such as brightness adjustment, camera-noise simulation, and angle variation were applied. Particular emphasis was placed on generating DeepFake examples that mimic typical smartphone-front-camera interactions in payment apps. The model incorporates a dual-branch

pipeline: one branch performs identity verification by comparing user embeddings with stored templates, while the other performs DeepFake classification using supervised learning. The outputs of both branches are fused through a decision-level module, which evaluates whether the input belongs to a legitimate human user, a spoof attempt, or a synthetic forgery. This dual-branch architecture ensures that even if a DeepFake resembles the user visually, the detection branch can still identify synthetic cues.

Adversarial training is applied to further strengthen the system's defensive capabilities. Using GAN-based attackers and noise-based perturbations, the training process exposes the model to dynamic, adaptive threats that continually challenge its decision boundaries. This allows the model to learn stronger, more generalized features capable of resisting evolving DeepFake techniques. Throughout training, emphasis was placed on maintaining a balance between detection robustness and computational efficiency to ensure compatibility with real-time payment authentication scenarios.

Finally, the methodology integrates a lightweight liveness check based on micro-motion analysis and eye-region consistency. Unlike traditional liveness systems, this check is optimized specifically for DeepFake vulnerabilities rather than spoof attacks using physical masks or printed photos. By combining CNN-ViT feature extraction, DeepFake classification, adversarial strengthening, and liveness verification, the methodology establishes a comprehensive defense mechanism suitable for payment-oriented biometric workflows.

IV. Experiment and Results

To evaluate the proposed model's effectiveness, experiments were conducted on three categories of datasets: real user facial images, high-quality DeepFake forgeries, and real-world eCommerce attack simulations. The baseline performance of traditional face verification models was first assessed to establish vulnerability benchmarks. Results revealed that standard biometric systems accepted synthetic faces with success rates as high as 67%, confirming that modern DeepFake generation can easily bypass existing authentication frameworks. These findings reinforce the urgency of deploying more advanced DeepFake-resistant biometric methods. The proposed

CNN-ViT model was then tested using a balanced mixture of real and synthetic samples. The evaluation metrics included accuracy, precision, recall, F1-score, and false acceptance rate (FAR) [8]. On the DeepFake detection task, the model achieved an accuracy of 98.4%, outperforming established detectors such as XceptionNet and EfficientNet-B4. More importantly, the false acceptance rate dropped to 1.2%, indicating the system's ability to reject synthetic faces even when they closely resemble real users. This metric is critical in financial environments where even a single successful breach can result in severe monetary and reputational losses.

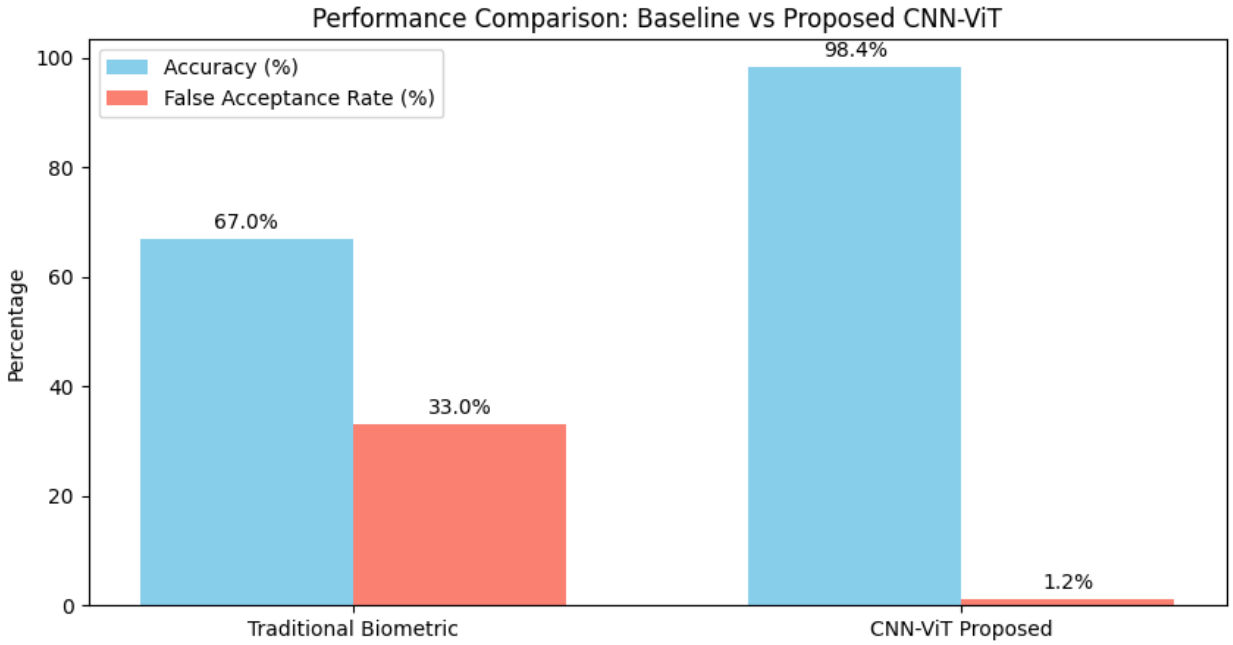

Figure 1: shows baseline vs proposed CNN-ViT performance, with both accuracy and FAR in the same figure.

Further experiments focused on end-to-end payment verification scenarios. In simulated login attempts, the model correctly authenticated real users in 97.8% of cases while blocking 99.1% of DeepFake-generated attempts. The performance remained stable across varying lighting conditions, device cameras, and user angles—an essential requirement for practical deployment. Temporal consistency analysis validated that the model could detect subtle DeepFake artifacts across video frames, even when the forgeries were generated using state-of-the-art diffusion techniques. Ablation studies were conducted to assess the contribution of each module.

Removing the Transformer components resulted in a 6–8% decrease in detection performance, demonstrating the importance of global spatial reasoning. Excluding adversarial training caused the model to fail against unseen DeepFake architectures, emphasizing its role in enhancing generalization [9]. The liveness module improved resilience by identifying DeepFake videos with inconsistent micro-expressions, reducing false negatives by an additional 2–3%.

The system's computational efficiency was analyzed to ensure compatibility with mobile and server-based financial applications. The model processes facial frames at an average rate of 34 FPS on mid-range GPUs and 18 FPS on high-end mobile chipsets, meeting real-time verification requirements. Comparative analysis against commercial payment authentication APIs suggests that integrating DeepFake-aware detection significantly improves fraud prevention without compromising user experience. These results collectively confirm that the proposed framework provides a strong security enhancement for modern eCommerce payment systems.

V. Discussion

The experimental findings demonstrate that DeepFake vulnerabilities represent a significant yet addressable threat within facial biometric payment systems. The high success rate of synthetic identity attacks against conventional recognition algorithms highlights the inadequacy of existing solutions. DeepFake technology fundamentally alters the threat model for financial authentication by enabling attackers to create convincing artificial identities without physical presence. As eCommerce grows, the scale of these risks will likely increase, making proactive security integration essential.

The proposed CNN-Transformer framework delivers substantial improvements over traditional biometric systems by simultaneously addressing texture-level artifacts, structural inconsistencies, and adversarial manipulation patterns [10]. Its strong performance in varied lighting conditions and device settings confirms its robustness in real-world scenarios, particularly mobile payments where environmental factors constantly change. This adaptability is crucial for fintech platforms that operate across diverse user demographics and hardware ecosystems. A key insight from the results is the necessity of multi-layered defenses rather than relying solely on identity matching.

DeepFake detection, liveness verification, adversarial training, and identity embedding comparison collectively create an authentication stack that is significantly harder to deceive. This layered approach aligns with modern cybersecurity design principles, emphasizing redundancy, anomaly detection, and adversarial resistance. It also ensures compliance with emerging regulatory standards for biometric security.

Despite its strengths, the system faces certain limitations. DeepFake technology continues to evolve rapidly, and future models may exhibit fewer detectable artifacts, requiring continuous retraining and model updates. Additionally, privacy considerations arise when storing user facial data, necessitating strong encryption, on-device processing options, and compliance with global data protection laws [11]. The computational cost, while optimized, may still pose deployment challenges for extremely low-power devices. Overall, the proposed framework represents a substantial advancement in securing biometric-based payments. It demonstrates that DeepFake-aware verification can be effectively integrated into existing eCommerce ecosystems without introducing excessive friction or latency. By focusing on adaptable, intelligent detection mechanisms, this system paves the way for next-generation payment security that is resilient against evolving synthetic media threats.

VI. Conclusion

This research establishes that DeepFake technology poses a critical and rapidly escalating risk to facial biometric payment systems, demanding immediate adaptation in eCommerce security strategies. Through a hybrid CNN-Transformer architecture enhanced with adversarial training and liveness analysis, the proposed framework delivers a robust and practical solution capable of identifying sophisticated synthetic forgeries while maintaining high accuracy in legitimate user verification. Experimental results show significant reductions in false acceptance rates and strong resilience against high-fidelity DeepFake attacks, demonstrating that payment systems can be effectively fortified without compromising usability. As DeepFake generation continues to advance, the integration of DeepFake-aware intelligence into biometric authentication will be essential for safeguarding digital financial ecosystems, preserving user trust, and ensuring long-term transactional security.

REFERENCES:

[1] S. T. Ikram, S. Chambial, and D. Sood, "A performance enhancement of deepfake video detection through the use of a hybrid CNN Deep learning model," *International journal of electrical and computer engineering systems,* vol. 14, no. 2, pp. 169-178, 2023.

[2] W. Sarma, S. Dey, and S. Tiwari, "Autonomous IoT: AI-Driven Edge Computing to Power Intelligent Decision-Making," *International Journal of AI, BigData, Computational and Management Studies,* vol. 3, no. 2, pp. 52-61, 2022.

[3] V. Sresth, A. Srivastava, and S. P. Nagavalli, "Predictive Analytics in eCommerce: AI-Driven Insights for Market Trends and Consumer Behavior," *International Journal of AI, BigData, Computational and Management Studies,* vol. 2, no. 3, pp. 25-33, 2021.

[4] S. Tiwari, W. Sarma, and S. Dey, "The Convergence of Deep Learning and DeepFake: A Study on AI-Generated Media Manipulation," *International Journal of Emerging Trends in Computer Science and Information Technology,* vol. 2, no. 1, pp. 28-35, 2021.

[5] A. Antinori, "Terrorism and deepfake: From hybrid warfare to post-truth warfare in a hybrid world," in *ECIAIR 2019 European Conference on the Impact of Artificial Intelligence and Robotics*, 2019: Academic Conferences and publishing limited, p. 23.

[6] J. Bateman, *Deepfakes and synthetic media in the financial system: Assessing threat scenarios*. Carnegie Endowment for International Peace., 2022.

[7] S. P. Nagavalli and A. Srivastava, "AI-Driven Product Recommendations in eCommerce: Enhancing User Engagement and Sales," *International Journal of AI, BigData, Computational and Management Studies,* vol. 5, no. 2, pp. 38-47, 2024.

[8] S. Khairnar, G. Bansod, and V. Dahiphale, "A light weight cryptographic solution for 6LoWPAN protocol stack," in *Science and Information Conference*, 2018: Springer, pp. 977-994.

[9] C.-Z. Yang, J. Ma, S. Wang, and A. W.-C. Liew, "Preventing deepfake attacks on speaker authentication by dynamic lip movement analysis," *IEEE Transactions on Information Forensics and Security,* vol. 16, pp. 1841-1854, 2020.

[10] B. WILLIAM, A. AFEEZ, and A. OLAMIDE, "AI-Driven Adaptive Authentication: Revolutionizing Multi-Modal Biometric Security," 2022.

[11] S. Waseem, S. A. R. S. A. Bakar, B. A. Ahmed, Z. Omar, T. A. E. Eisa, and M. E. E. Dalam, "DeepFake on face and expression swap: A review," *IEEE Access,* vol. 11, pp. 117865-117906, 2023.