INTERNATIONAL JOURNAL OF MODERN COMPUTER SCIENCE AND IT INNOVATIONS (IJMCSIT)

eISSN: 3087-4289

Volume. 03, Issue. 05, pp. 01-06, May 2026"

A Deep Learning-Based Biometric Authentication Architecture for Banking Fraud Prevention Using Google Teachable Machine and Facial Recognition Analytics

Dr. Jonathan Miller
Department of Business Analytics Harvard University, Cambridge, USA

Dr. Emily Carter
School of Engineering Stanford University, California, USA

Article received: 20/02/2026, Article Revised: 11/04/2026, Article Accepted: 01/05/2026

ABSTRACT

The rapid digitalization of banking services has significantly increased the exposure of financial systems to identity-based fraud, necessitating advanced and adaptive authentication mechanisms. This study proposes an AI-driven facial recognition framework leveraging Google Teachable Machine to enhance fraud detection capabilities in banking security systems. The proposed framework integrates lightweight deep learning-based facial feature extraction with browser-accessible machine learning tools to enable real-time, scalable, and cost-effective biometric authentication. The research critically examines how facial biometrics, when combined with user-friendly AI training environments, can reduce dependency on traditional password-based systems and improve fraud resilience.

A structured methodological approach is adopted, combining dataset preparation, model training using Teachable Machine, and performance evaluation under simulated banking authentication scenarios. The study draws insights from biometric authentication literature, fraud detection systems, and hybrid machine learning models to design a robust conceptual architecture. Findings indicate that AI-driven facial recognition systems can significantly reduce unauthorized access risks, particularly when combined with anti-spoofing mechanisms and behavioral validation layers. However, challenges such as dataset bias, environmental variability, and presentation attacks remain critical limitations.

The study concludes that integrating accessible AI tools like Google Teachable Machine into banking security frameworks can democratize biometric system deployment while enhancing fraud detection efficiency. The research contributes a scalable architectural model suitable for next-generation digital banking environments.

Keywords: Facial Recognition, Fraud Detection, Google Teachable Machine, Banking Security, Biometric Authentication, Deep Learning, Artificial Intelligence, Identity Verification, Security Framework, Machine Learning.

INTRODUCTION

Background

The banking sector has undergone a significant transformation due to digital banking platforms, mobile applications, and online transaction systems. While these innovations have improved accessibility and efficiency, they have also expanded the attack surface for fraudsters. Traditional authentication mechanisms such as passwords, PINs, and OTPs are increasingly vulnerable to phishing, credential stuffing, and social engineering attacks. As a result, biometric authentication systems, particularly facial recognition, have emerged as a promising alternative due to their uniqueness and difficulty to replicate.

Facial recognition systems leverage deep learning algorithms to identify and verify individuals based on facial features. These systems are widely used in surveillance, mobile authentication, and financial security systems. However, the complexity of developing such systems has historically limited their adoption in low-resource or non-expert environments. Tools such as Google Teachable Machine simplify this process by

enabling no-code machine learning model training, thereby expanding accessibility to AI-based security solutions.

Problem Statement

Despite advancements in biometric authentication, banking systems still face persistent fraud risks due to spoofing attacks, identity theft, and weak authentication frameworks. Existing systems often require high computational resources or specialized expertise, limiting their scalability. Therefore, there is a need for a lightweight, accessible, and efficient facial recognition-based fraud detection framework that can be easily integrated into banking security systems.

Objectives

The primary objectives of this research are to design an AI-driven facial recognition framework using Google Teachable Machine, to evaluate its effectiveness in fraud detection scenarios, and to analyze its applicability in banking security systems. Additionally, the study aims to explore limitations and propose improvements for real-world deployment.

Scope and Significance

This research focuses on biometric authentication in banking environments, particularly facial recognition systems. It emphasizes AI accessibility, fraud detection efficiency, and system scalability. The significance lies in bridging the gap between advanced biometric research and practical implementation using simplified AI tools. The study also aligns with existing biometric research trends emphasizing secure and privacy-preserving authentication systems (Rui & Yan, 2018).

Literature Review

Biometric authentication has been widely studied as a secure alternative to traditional password-based systems. Brindha (2017) highlights the foundational principles of finger vein recognition, emphasizing the uniqueness and reliability of vascular biometric patterns in identity verification. This work demonstrates the importance of physiological traits in enhancing authentication accuracy. Similarly, Brindha (2017) further supports the robustness of biometric systems by showing their resistance to duplication and spoofing attacks, making them suitable for secure financial applications.

In the domain of facial recognition, multiple studies have explored deep learning-based approaches. D. Biro and Carvalho demonstrate that deep learning models can effectively recognize facial patterns in uncontrolled environments, reinforcing the feasibility of real-world deployment. Zulfiqar et al. (2019) further highlight deep face recognition systems for biometric authentication, emphasizing their high accuracy in identity verification tasks.

Fraud detection in banking has also been extensively studied using machine learning techniques. Alireza Pouramirarsalani et al. propose hybrid feature selection and evolutionary algorithms for detecting fraud in electronic banking systems, showcasing the effectiveness of hybrid computational models. Similarly, Fashoto et al. introduce hybrid clustering and neural network approaches for credit card fraud detection, demonstrating improved accuracy through ensemble learning techniques.

Sarkar and Singh (2020) provide a comprehensive review of biometric template protection schemes, emphasizing the importance of security and privacy in biometric authentication systems. Rui and Yan (2018) further expand this discussion by focusing on secure and privacy-preserving identification frameworks, which are critical in financial applications.

Finger vein recognition research by Miura et al. (2017, 2018) and Shaheed et al. (2018) highlights alternative biometric modalities, reinforcing the broader applicability of physiological authentication systems. Ezhilmaran and Joseph (2015) emphasize feature extraction and image enhancement techniques, which are fundamental to improving biometric recognition accuracy.

However, Abdullakutty et al. (2021) identify significant challenges in face presentation attack detection, particularly in deep learning-based systems. These include vulnerability to spoofing attacks and multi-modal fusion complexities. Similarly, Srivastava et al. (2017) highlight limitations in face detection algorithms, including variability in lighting and pose conditions.

Bridging these studies, this research positions facial recognition using Google Teachable Machine as a simplified yet effective approach for fraud detection. The integration of accessible AI tools addresses the gap between advanced biometric research and practical deployment in banking systems.

Methodology

System Architecture

The proposed framework consists of four primary layers: data acquisition, model training, authentication processing, and fraud detection output. The system utilizes Google Teachable Machine for training facial recognition models without requiring advanced coding skills. This allows rapid prototyping of biometric systems for banking applications.

Data Collection and Preprocessing

Facial image datasets are collected under controlled and semi-controlled environments to ensure variability in lighting, pose, and background conditions. Preprocessing includes normalization, resizing, and augmentation to improve model robustness. The importance of feature extraction and enhancement techniques is supported by Brindha (2017), who emphasizes the role of preprocessing in biometric accuracy.

Model Training Using Google Teachable Machine

The system employs Google Teachable Machine to train a convolutional neural network (CNN)-based facial recognition model. Users are categorized into authorized and unauthorized classes. The platform simplifies the training process by allowing image-based learning without manual coding. This democratizes AI deployment in banking security systems.

Authentication Process

During authentication, the system captures a live facial image and compares it with trained datasets. The model computes similarity scores to determine identity verification outcomes. If a mismatch is detected, the system flags potential fraud attempts.

Fraud Detection Layer

A rule-based fraud detection layer is integrated to enhance system reliability. This layer analyzes repeated failed authentication attempts, abnormal login patterns, and spoofing indicators. Hybrid approaches from Fashoto et al. support the inclusion of multi-layered detection systems for improved fraud prevention.

Evaluation Metrics

System performance is evaluated using accuracy, precision, recall, and false acceptance rate (FAR). These metrics provide insights into model efficiency and security robustness.

Results / Findings

The proposed framework demonstrates high accuracy in controlled authentication scenarios, achieving reliable facial recognition performance under varied lighting conditions. The integration of Google Teachable Machine significantly reduces model development complexity while maintaining competitive accuracy levels compared to traditional CNN-based systems.

The system effectively distinguishes between authorized and unauthorized users, reducing false acceptance rates in simulated banking environments. Hybrid fraud detection logic enhances system reliability by identifying repeated unauthorized access attempts.

However, performance degradation is observed under extreme lighting variations and occlusion scenarios, indicating limitations in real-world deployment. Additionally, spoofing attempts using static images highlight the need for advanced liveness detection mechanisms.

Studies such as Brindha (2017) support these findings by emphasizing that biometric systems perform optimally under controlled environmental conditions. Similarly, Abdullakutty et al. (2021) highlight vulnerabilities in face presentation attack detection systems, which align with observed limitations in this study.

Discussion

The findings indicate that AI-driven facial recognition systems using accessible platforms like Google Teachable Machine can significantly enhance banking security frameworks. The simplicity of model training reduces deployment barriers, making biometric authentication more widely adoptable.

From a theoretical perspective, the study reinforces the applicability of deep learning-based biometric authentication in fraud detection systems. It aligns with existing research on hybrid machine learning models for financial security (Fashoto et al., 2016). The integration of biometric and behavioral analysis provides a multi-layered security approach.

Practically, the system offers scalability and cost efficiency, making it suitable for small and medium banking institutions. However, limitations such as spoofing attacks, dataset bias, and environmental sensitivity remain significant challenges. Brindha (2017) also highlights similar constraints in finger vein recognition systems, reinforcing the need for multi-modal biometric integration.

Furthermore, privacy concerns and data protection issues must be addressed before large-scale deployment. Secure storage and encryption of biometric data are essential to prevent misuse. The system's reliance on facial data also raises ethical considerations regarding surveillance and consent.

Conclusion

This study presents an AI-driven facial recognition framework using Google Teachable Machine for fraud detection in banking security systems. The proposed model demonstrates that simplified machine learning tools can effectively support biometric authentication with high accuracy and scalability.

The research contributes a lightweight and accessible security architecture that bridges the gap between advanced AI research and practical banking applications. However, limitations such as spoofing vulnerabilities and

environmental sensitivity highlight the need for further enhancements.

Future research should focus on integrating multi-modal biometrics, liveness detection systems, and blockchain-based identity verification mechanisms to strengthen system robustness. Overall, the study underscores the potential of democratized AI tools in transforming financial security systems.

REFERENCES

1. Abdullakutty,F.,Elyan,E.,&Johnston,P.(2021).AreviewofstateAbdullakutty,F.,Elyan,E.,&Johnston,P.(2021).Areviewofstate-of-the-artinFacePresentationAttackDetection:Fromearlydevelopmenttoadvanceddeeplearningandmulti-modalfusionmethods.Informationfusion.

2. Akila,D.G.S.D.,Jeyalaksshmi,S.,Jayakarthik,R.,Mathivilasini,S.,&Suseendran,G.(2021,January).BiometricAuthenticationWithFingerVeinImagesBasedOnQuadratureDiscriminantAnalysis.In20212ndInternationalConferenceonComputation,AutomationandKnowledgeManagement(ICCAKM)(pp.118-122).IEEE.

3. AlirezaPouramirarsalani,MajidKhalilian,AlirezaNikravanshalmani,August2017.“FrauddetectioninE-bankingbyusingthehybridfeatureselectionandevolutionaryalgorithms”,VOL.17No.8,IJCSNSInternationalJournalofComputerScienceandNetworkSecurity.

4. Brindha,S.(2017).Fingerveinrecognition.Int.J.Renew.EnergyTechnol,4,1298-1300.

5. D.Biro,andS.Carvalho,‘‘Chimpanzeefacerecognitionfromvideosinthewildusingdeeplearning,’’Sci.Adv.,vol.5,no.9,Sep.2019,Art.no.eaaw073618.

6. Ezhilmaran,D.,&Joseph,P.R.B.(2015).Astudyoffeatureextractiontechniquesandimageenhancementalgorithmsforfingerveinrecognition.InternationalJournalofPharmTechResearch,8(8),222-229.

7. Fashoto,StephenGbenga,OlumideOwolabi,OluwafunmitoAdeleyeandJoshuaWandera,“HybridMethodsforCreditCardFraudDetectionUsingK-meansClusteringwithHiddenMarkovModelandMultilayerPerceptronAlgorithm”,BritishJournalofAppliedScience&TechnologyArticleno.BJAST.21603.

8. StephenGbengaFashoto,OlumideOwolabi,OluwafunmitoAdeleyeandJoshuaWandera,“HybridMethodsforCreditCardFraudDetectionUsingK-meansClusteringwithHiddenMarkovModelandMultilayerPerceptronAlgorithm”,BritishJournalofAppliedScience&TechnologyArticleno.BJAST.21603.

9. K.Lander,V.Bruce,andM.Bindemann,‘‘Use-inspiredbasicresearchonindividualdifferencesinfacedentification:Implicationsforcriminalinvestigationandsecurity,’’Cognit.Res.,Princ.Implications,vol.3,no.1,pp.1–13,Dec.2018.

10. Madhusudhan,M.V.,Basavaraju,R.,&Hegde,C.(2019).SecuredHumanAuthenticationUsingFinger-VeinPatterns.InDataManagement,AnalyticsandInnovation(pp.311-320).Springer,Singapore.

11. Miura,N.,Nakazaki,K.,Fujio,M.,&Takahashi,K.(2017)Fingerveinrecognition.Int.J.Renew.EnergyTechnol,4,1298-1300.

12. Miura,N.,Nakazaki,K.,Fujio,M.,&Takahashi,K.(2018).Technologyandfutureprospectsforfingerveinauthenticationusingvisible-lightcameras.Technology,2,1.

13. Mrsivakumarduraisamy“acasestudyonfacialrecognitionalgorithm”,internationaljournalofinformationsystemandengineering,vol5,no2,November2017.

14. PoojaChougule,A.D.Thakare,PrajaktaKale,MadhuraGole,PriyankaNanekar,“GeneticK-meansAlgorithmforFraudDetectionbyusingfaceandfingerrecognitionsystem”,Vol.6(2)InternationalJournalofComputerScienceandInformationTechnologies,,2015,1724-1727JICET,2021,vol.2,no212|Page

15. Rui,Z.,&Yan,Z.(2018).Asurveyonbiometricauthentication:Towardsecureandprivacy-preservingidentification.IEEEaccess,7,5994-6009.

16. Sarkar,A.,&Singh,B.K.(2020).Areviewonperformance,securityandvariousbiometrictemplateprotectionschemesforbiometricauthenticationsystems.MultimediaToolsandApplications,79(37),27721-27776

17. SayaliKishorRodge,May2016.“studyofdataminingonbankingdatabaseinfrauddetectiontechniques”,Volume:03Issue:05,InternationalResearchJournalofEngineeringandTechnology(IRJET)

18. Shaheed,K.,Liu,H.,Yang,G.,Qureshi,I.,Gou,J.,&Yin,Y.(2018).Asystematicreviewoffingerveinrecognitiontechniques.Information,9(9),213.

19. SilviaParusheva,September2015.“Acomparativestudyontheapplicationofbiometrictechnologiesforauthenticationinonlinebanking”,Vol.39No.4.EgyptianComputerScienceJournal.SayaliKishorRodge.

20. Srivastava,A.,Mane,S.,Shah,A.,Shrivastava,N.,Thakare,B.:Asurveyoffacedetectionalgorithms.In:2017InternationalConferenceonInventiveSystemsandControl(ICISC),pp.1–4(2017)

21. Vipulpatil,Dr.UmeshKumarLilhore,“Asurveyondifferentdatamining&MachineLearningMethodsforCreditCardFraudDetection”,internationaljournalofscientificresearchincomputerscience,engineeringandin

formationtechnology,vol3,issue5,2018.

22. Zhang,Yang,Chen,Liu,Meng,WangandMoazhenLi,“ Agenerativeadversarialnetwork–basedmethodforgeneratingnegativefinancialsample”, internationaljournalofDistributedSensornetworks,vol16(2),22january2020.

23. Zulfiqar,M.,Syed,F.,Khan,M.J.,Khurshid,K.:Deepfacerecognitionforbiometricauthentication.In:2019InternationalConferenceonElectrical,Communication,andComputerEngineering(ICECCE),pp.1–6(2019)