Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 03 Issue: 12 | Dec-2025
ISSN (O) 3107-6696

Enhanced Banking Security System Using AI Based Facial Recognition With Anti-Spoofing

Anusha Chandrahas Raykar[1], Mr. Ajith G L[2]

[1] MCA Student, PES Institute of Technology and Management, Shivamogga, Karnataka, India.
[2] Assistant Professor, MCA PES Institute of Technology and Management, Shivamogga, Karnataka, India.

Abstract - The need for reliable and safe methods of user verification has grown as digital banking continues to grow. Passwords PINs and one-time codes are examples of older techniques that are no longer as trustworthy. They are more susceptible to unauthorized access because they can be stolen hacked or misused through phishing attacks. To get around these limitations the current work provides an improved banking security system with anti-spoofing and AI-based facial recognition. Deep learning technology is used in this system to identify a persons face and it also uses small real-time signals like blinking and skin texture to determine if the person is truly alive. A CNN model analyzes a persons facial features and compares them to user information that is safely kept in the system. It is difficult for someone to trick the system with printed photos mobile displays or masks because of the integrated anti-spoofing feature. In general this configuration makes online transactions safer and gives users greater confidence in their digital banking.

Keywords: CNN, facial recognition, AI, liveness detection, anti-spoofing, secure banking.

Introduction

People can now manage their money with very little effort thanks to the rapid growth of online banking via mobile apps and websites. Although this convenience has fundamentally altered the way we handle our money it has also made additional security issues possible. Password theft phishing scams and illegal access have all increased in frequency. Passwords PINs and OTPs are examples of older verification techniques that are gradually losing their reliability due to their ease of theft guessing and misuse. Because AI-powered facial recognition relies on an individuals distinctive biometric features which are much more difficult to falsify it is beginning to be perceived as a safer alternative due to these problems. However pre-recorded videos printed images and realistic masks can still fool even the most advanced face recognition systems. The suggested system combines cutting-edge anti-spoofing techniques with AI-based facial recognition to address these flaws. While liveness checks—such as blink detection texture analysis and depth checking—ensure that the user is a real person in front of the camera deep learning models like CNNs assist in highlighting significant facial features. The system greatly lowers the likelihood of unwanted access and improves overall banking security by combining facial recognition with robust anti-spoofing techniques. Additionally it makes the verification process quicker touchless and simpler for users.

2. Literature Review

Their approach still had many practical issues because it was unable to distinguish between a real face and a fake one and performed poorly when the lighting changed. Therefore even though it appeared to be adequate for real-time use it was actually insufficiently powerful for scenarios requiring high security. Ahmed Ali Muttasher and Rasha developed a face-based payment method in a different study to do away with the need for credit cards or passwords. Basically they wanted to make things easy and quick for the user. However since no anti-spoofing protection was added identity theft and replay attacks—a major problem in financial systems—could still fool the system. In a similar vein Patil and Jain proposed a technique that involved comparing a persons live face recorded by a camera with the face printed on a credit card. Although it did assist in verifying whether the real cardholder was completing the transaction the systems dependability was seriously compromised when someone used realistic masks or repeated video clips. A CNN-based facial recognition system that performed better in lighting and head angle changes was later introduced by Zhang and Kim. Although their findings were encouraging they also noted that without additional liveness checks CNN is still unable to distinguish between real and fake faces.

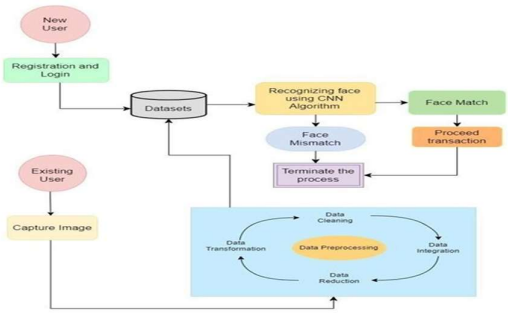
3. Methodology

The proposed Enhanced Banking Security System combines stronger anti-spoofing checks with AI-based face recognition to provide a more reliable method of user verification without slowing down operations. The system immediately uses the devices camera to take a live photo or brief video when someone tries to open the banking app. After that the image is cleaned up during the pre-processing stage which involves

adjusting the lighting eliminating excess noise and retaining only the subjects face for analysis. The CNN model then takes over and examines the processed image identifying the key facial features and converting them into numerical values for later comparison. Simultaneously the anti-spoofing component examines features such as blinking skin texture patterns depth information and subtle natural movements to determine whether the subject is truly real. This helps ensure that the user isnt attempting to trick the system by using a mask a recorded video or a printed picture. The system transmits the facial features to the banks secure encrypted database for comparison with the stored user profiles only after the anti-spoofing check verifies the face is authentic. The system either permits the user to enter or denies the attempt based on the match score and the liveness outcome. The user can perform standard banking operations such as checking their balance or completing transactions once access has been granted. To be extra cautious the system may even request another brief facial check for more delicate actions. Every users data is handled for a brief period of time and is securely encrypted to prevent any personal information from leaking or being exposed.

4. System Design

Every component of the Enhanced Banking Security System from the camera to the backend is configured in a layered fashion to ensure seamless operation. The camera records what it sees the preprocessing unit cleans it up the facial recognition model analyzes it the anti-spoofing component verifies that it is authentic and the banking backend determines whether to grant the user access. It all begins when the camera takes a picture or a quick video while the user interacts with the app. In order to prepare it for the AI model the raw image is immediately put through preprocessing which includes tasks like face detection lighting correction frame adjustment and even conversion to grayscale. After the image has been cleaned up CNN extracts the deeper facial features required to produce a personalized embedding for the user. In order to ensure that the user is not wearing a mask a printed photo or a replayed video the anti-spoofing module simultaneously examines the same input for indicators of genuine liveness such as blinking skin-texture patterns slight movement variations or depth cues. The authentication controller is then notified of both results. This unit verifies the liveness score and compares the newly created facial embedding with the safely stored one in the banks encrypted database. The user can proceed with standard banking operations such as checking their balance transferring funds or approving transactions if everything appears to be in order and the face is verified to be real. However the system immediately prevents access and flags the session for security review if anything appears suspicious such as spoofing attempts or mismatched IDs. To ensure that all biometric data is kept safe throughout the process the backend is also constructed with secure API gateways encrypted communication channels and appropriate logging. All things considered the configuration offers users a safe reliable and user-friendly login experience.



5. Mathematical Formula

1.Face Encoding

The input image is converted into a numerical feature vector (embedding) using a pretrained deep learning model (CNN or FaceNet):

F_E = \text{Model}(I)

Where:

: Input face image

: 128-D or 512-D face embedding generated by the model

2.Face Matching

To verify identity, similarity is measured between live face embedding and stored database embedding using Euclidean distance:

D = \sqrt{\sum_{i=1}^{n} (F_{E_i}^{live} - F_{E_i}^{stored})^2}

Decision Rule:

D < T \Rightarrow \text{Same Person}

D \ge T \Rightarrow \text{Different Person}

Where:

: Live face embedding

: Registered user embedding

: Threshold value

3.Anti-Spoofing Score

The anti-spoofing model predicts whether the input image is real or fake using a softmax classifier:

S = \text{Model}_{AS}(I)

P(real) = \frac{e^{S_{real}}}{e^{S_{real}} + e^{S_{fake}}}

Where:

: Raw output scores from the anti-spoofing model

: Probability that the face is live (not spoofed)

4.Softmax Activation

Softmax is used to convert raw model outputs into probabilities:

P(c_i|I) = \frac{\exp(z_i)}{\sum_{j} \exp(z_j)}

Where:

Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 03 Issue: 12 | Dec-2025
ISSN (O) 3107-6696

: Score for class (real / fake)
: Probability of class

5.Cross Entropy Loss

The model is trained using cross-entropy loss to ensure correct classification:

L_{CE} = -\log(P(c_{true}|I))

Where:
: Correct label (real or fake)
: Predicted probability for the correct class

6.Final Authentication Decision

D < T

Liveness Condition:

P(real) \ge L

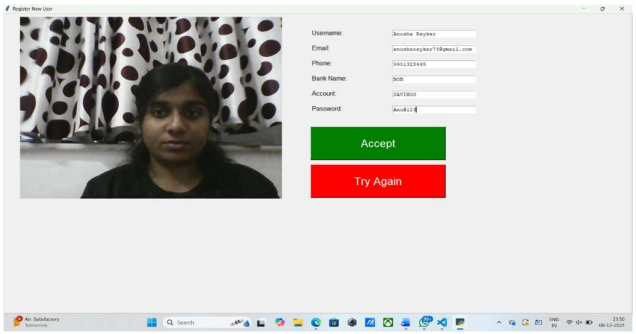
Combined Decision:

\text{Authenticate} =
\begin{cases}
\text{True}, & \text{if } D < T \ \text{and } P(real) \ge L \\
\text{False}, & \text{otherwise}
\end{cases}

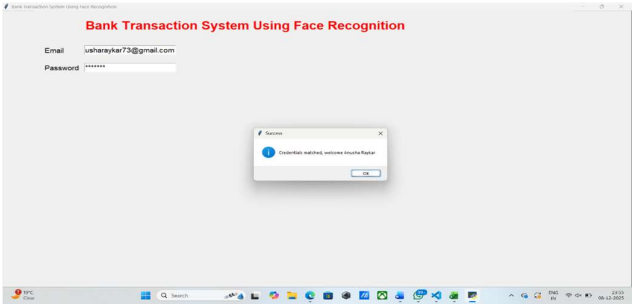
Where:
: Minimum liveness probability threshold

5. Results

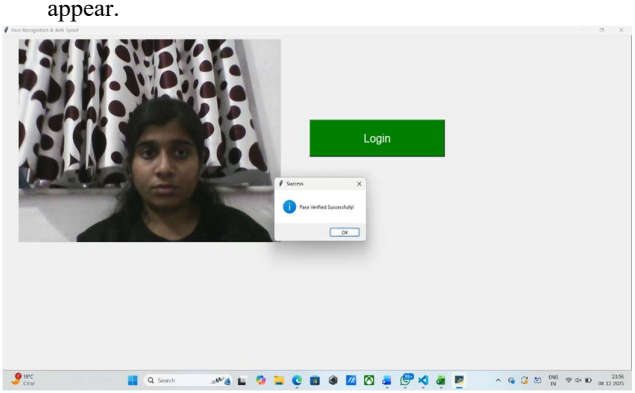
Figure 1 displays the account holder's registration page by taking a webcam picture of their face and entering their registration information, which will be saved in CSV files once they click the "accept" button.



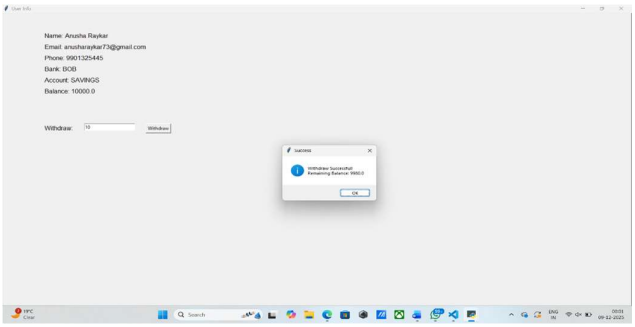
- The gateway page seen in Figure 2 is where the account holder enters their email address and password to match the information they entered during registration. displays a pop-up notification confirming the user's entered email address and password.



- By taking a picture of the account holder's face and comparing it to the image of the registered user, Figure 3 depicts the login page. The confirmation notice will then appear.



- The payment detail portal, which the account holder can access by entering the necessary amount, is seen in Figure 4. The user's bank data are also shown on the page.



- Figure 5 illustrates how the payment is confirmed by sending a message to the user's email.

Conclusion

By utilizing AI-based face recognition and anti-spoofing checks the Enhanced Banking Security System provides a reliable and modern response to the growing security concerns in online banking. To ensure that only a real present person can access sensitive banking features it combines deep-learning facial recognition with robust liveness tests such as blink detection texture checking and depth sensing. The results of the experiments demonstrated that the suggested system is much more secure and useful than more traditional techniques like passwords or OTPs. It improves accuracy more successfully thwarts spoofing attempts and provides users with a seamless and simple experience. All things considered the system reduces the likelihood of identity theft improves transaction security and satisfies the increasing demand for convenient and safe online banking. In summary this work demonstrates how combining cutting-edge anti-spoofing techniques with AI-driven facial recognition can greatly enhance banking authentication and pave the way for future more secure biometric applications.

Future Enhancement

By incorporating additional biometric features like voice recognition or fingerprint scanning this banking systems security could be further enhanced in the future. To make it more difficult for attackers to fool the system it may also incorporate sophisticated checks to identify phony or altered videos. Better cameras like those with 3D or infrared sensors might make it easier for the system to distinguish between a real person and a picture or video. This model could be used in ATMs as well as mobile banking apps enabling quicker and easier logins. All bank branches could benefit from cloud support which could offer fast updates and secure data storage. All things considered these enhancements would make the system more precise safe and user-friendly.

References

[1] AI-Driven Facial Recognition for Secure Banking Transactions International Computer Applications Journal vol. No twelve. pp. 3. 2022 45–52 A. Kumar R. Desai and S. Patel.

[2]. Journal of Intelligent Security Systems, vol. 10, no. 2, pp. 101–110, 2023; P. Sharma, M. Nair, and K. Iyer, "Liveness Detection Techniques for Anti-Spoofing in Facial Authentication Systems."

[3] CNN-Based Face Recognition for Financial Security Applications, International Journal of Emerging Technology and Advanced Engineering, vol. 14, no. 6, 2024; R. Bhat and S. Kulkarni.

[4] Journal of Applied Machine Learning, vol. 8, no. 1, pp. 33–41, 2023; L. Thomas and G. Prakash, "Presentation Attack Detection for Real-Time Face Authentication."

[5] AI and Security Review, vol. 5, no. 4, pp. 90–99, 2024; A. Gupta and N. Singh, "Enhanced Anti-Spoofing Methods Using Deep Learning for Banking Systems."

[6] Smart Computing and Information Technology Journal, vol. 7, no. 2, pp. 56–64, 2023; M. Patel, S. Jadhav, and V. More, "Improving ATM Security through Facial Recognition and Liveness Detection."

[7]. "Deep Learning Methods for Robust Facial Feature Extraction," arXiv preprint, arXiv:2302.14567, 2023, Y. Li, P. Savarese, and S. C. Hoi.

[8] International Research Journal of Modern Computing, vol. 9, no. 1, pp. 12–18, 2024; S. Mehta and R. Verma, "AI-Based Authentication Models for Fraud Prevention in Digital Banking."

[9] Pattern Recognition Letters, vol. 19, no. 3, pp. 72–80, 2022; J. Park and H. Kim, "Eye-Blink and Motion-Based Liveness Detection for Secure Face Recognition."

[10] International Journal of Advanced Computer Science, vol. 15, no. 2, pp. 84–92, 2024. K. Rao and M. Banerjee, "AI-Based Face Recognition Systems for Banking Security: A Comprehensive Review."