Face Recognition System Using Machine Learning in Banking Sector

Mr. Akale Mahadev Ananda , Mr. Bhosale Rahul Shahaji , Mr. Nimangare Pratik Audumbar , Ms. Arerao Jayashree Khandu

Abstract:

Face Recognition-Based Authentication and Banking System that combines the power of machine learning, computer vision, and web development technologies to deliver a secure, convenient, and scalable banking platform.

The core objective of this project is to implement a facial recognition mechanism that can accurately identify and verify users for secure login, registration, and financial transactions. At its foundation, the system utilizes OpenCV for image processing and facial detection, in conjunction with the Local Binary Patterns Histograms (LBPH) algorithm for training and recognizing faces. This algorithm is specifically chosen due to its robustness in handling variations in lighting and facial expressions, making it well-suited for real-world applications.

The backend of the system is constructed using MySQL, a reliable and scalable relational database management system. MySQL is used to manage user data, including personal information, account numbers, balances, transaction logs, and Know Your Customer (KYC) verification status. Each user's data is securely stored and queried through a well-structured API built with the Flask web framework, which serves as the bridge between the front-end user interface and backend operations.

The user interface is developed using modern web technologies and offers three core functionalities:

User Registration: Users can sign up by entering their details and capturing facial images via a webcam. These images are used to train the face recognition model.

Authentication: Users can log in using either their face or a secure 4-digit PIN. The system matches the live image with the trained dataset and retrieves the corresponding user data if authenticated.

Banking Dashboard: Once authenticated, users can view their profile, perform credit and debit transactions, and manage personal details. The interface also allows users to verify KYC status and update personal information securely.

The training module preprocesses face images by converting them to grayscale, resizing them to a fixed dimension, and filtering invalid captures. A minimum threshold of high-quality facial captures is enforced to ensure that the face recognizer is trained effectively. The trained model is then serialized and stored for real-time recognition during login.

Security is a major focus in the system design. PINs are hashed using industry-standard algorithms to prevent raw data exposure. Input validation, error handling, and database integrity checks are integrated throughout the application to mitigate common security vulnerabilities.

Beyond its current implementation, this system can be scaled and extended to support multi-factor authentication, facial recognition at ATMs, mobile app integration, and more. It offers potential use cases not only in the banking sector but also in areas like employee attendance, building access control, e-governance, and public safety.

By leveraging facial recognition technology, this project delivers a forward-looking approach to banking security that reduces dependency on traditional authentication methods. It enhances user convenience, prevents unauthorized access, and demonstrates the practical deployment of AI-driven biometric systems in critical domains.

Keywords :

Face Recognition ,Biometric Authentication , OpenCV ,LBPH Algorithm , Flask Web Framework, MySQL Database, Machine Learning, Computer Vision, Secure Banking System, Real-Time Face Detection, User Verification , PIN

Authentication, KYC (Know Your Customer), Image Processing, Web-based Interface, Deep Learning, Financial Transactions, Identity Management, Cybersecurity, Human-Computer Interaction

Introduction

In the rapidly evolving digital landscape, securing user identities and sensitive financial data has become a critical concern for the banking sector. Traditional authentication systems—such as passwords, PINs, and security questions—are increasingly vulnerable to data breaches, phishing attacks, and unauthorized access. These conventional methods depend heavily on knowledge-based or possession-based credentials, which can be forgotten, stolen, or replicated. Consequently, there is a growing demand for more secure, efficient, and user-friendly authentication techniques that can overcome these limitations.

Biometric authentication, which relies on physiological or behavioral traits unique to individuals, offers a promising alternative. Among various biometric modalities, face recognition has gained widespread adoption due to its non-intrusive nature, ease of use, and suitability for real-time identification. Unlike fingerprints or iris scans, facial recognition can be performed passively using standard camera hardware, making it highly applicable in web and mobile environments.

This project proposes the design and implementation of a Face Recognition-Based Authentication and Banking System that enables users to access their banking accounts and perform transactions using their facial identity.

The system is built using an integrated stack of technologies: OpenCV for image acquisition and facial recognition, the LBPH (Local Binary Patterns Histograms) algorithm for model training and prediction, Flask for web-based application logic, and MySQL for secure data storage.

The system provides two primary modes of authentication: facial recognition and PIN-based login. It allows new users to register by submitting their personal and banking details along with facial image data captured via a webcam. These images are preprocessed and stored as training data, which is later used to train a facial recognition model. Upon subsequent logins, the system performs real-time face detection, compares the input with the trained model, and authenticates users with high accuracy.

Post-authentication, users gain access to a personalized dashboard where they can view and manage their account details, check balances, update profile information, perform credit or debit operations, and verify KYC status. The system also supports secure password hashing, input validation, and error handling to ensure data integrity and protection against unauthorized access.

This project not only showcases the potential of biometric systems in enhancing banking security but also emphasizes the practicality of deploying such technologies using widely available open-source tools. By addressing real-world challenges related to user identity and data protection, this system represents a forward-thinking approach to digital banking and contributes to the broader adoption of AI-driven security solutions in financial technology.

Problem Statement:

In today’s digital banking landscape, traditional authentication methods like passwords, PINs, and security tokens are increasingly becoming inadequate in ensuring user security and data protection. These methods are vulnerable to various threats such as password breaches, phishing attacks, and identity theft, leading to financial fraud and unauthorized access. Additionally, they rely heavily on the user’s memory or possession of credentials, which can be easily forgotten, lost, or stolen.

Such limitations create a critical need for a more secure, efficient, and user-friendly authentication system. Biometric technologies, particularly facial recognition, provide a promising solution by leveraging the unique and immutable features of a person’s face. This project addresses the challenge by developing a face recognition-based banking system that enhances security while simplifying user access, offering a reliable alternative to traditional methods.

Literature Review

The history of face recognition technology unfolds chronologically, beginning with semi-automated systems in the 1960s. In 1973, Kenade developed fully automated face recognition, extracting 16 facial features for identification. Eigenfaces, introduced by Sirovich and Kirby in 1986, utilized Principal Component Analysis to reconstruct images from lower dimensions.

Turk and Pentland expanded on Eigenfaces in 1991, enabling face detection within images. DARPA and NIST launched the FERET program in the 1990s, aiming to stimulate commercial face recognition. Facebook introduced face recognition in 2010, despite initial privacy concerns. Techniques continued to evolve, with advancements in criminal identification and Viola-Jones face detection.

In 2012, Uttam Mande explored criminal identification through facial evidence. A paper in 2014 analyzed the Viola-Jones technique, proposing post-processing for improved efficiency. Indian students introduced a speed-enhancing technique in 2018.

The use of biometric systems, particularly facial recognition, has evolved significantly over the past two decades. Early research focused on feature-based methods like Principal Component Analysis (PCA), Fisherfaces, and Local Binary Patterns (LBP), which extracted shallow facial features to identify individuals. While useful under controlled conditions, these traditional algorithms often failed in real-world scenarios involving lighting changes, facial expressions, or partial occlusion.

With the rise of deep learning, the field witnessed a paradigm shift. One of the most influential breakthroughs was FaceNet, introduced by Schroff et al. in 2015, which represented faces as 128-dimensional embeddings and used triplet loss to ensure that similar faces were grouped closer together in embedding space. This technique became widely adopted because of its scalability and ability to distinguish between millions of unique faces with high accuracy.

Following FaceNet, the use of Siamese Networks gained attention due to their ability to compare face pairs using contrastive or triplet loss functions, especially in systems with limited training data per user—a scenario common in banking environments. These models are particularly suited for one-shot learning, where the system learns to distinguish individuals based on a few examples, making them efficient for onboarding new bank customers without retraining.

Recent research has also explored real-time facial recognition for practical deployment. For instance, Parkhi et al. (2015) introduced DeepFace from Facebook, and subsequent developments like VGGFace2 and ArcFace improved generalization across various demographic and lighting conditions. These models were tested extensively on benchmark datasets like LFW (Labeled Faces in the Wild) and CASIA-WebFace, showing near-human accuracy in controlled settings.

Beyond facial recognition models, security is another major focus area. Studies emphasize the need for AES encryption, HTTPS protocols, and JWT (JSON Web Tokens) to protect biometric data during storage and transmission. Compliance with data protection laws such as GDPR and India's Personal Data Protection Bill is also increasingly being incorporated into system designs, especially when dealing with sensitive customer information in banks.

A number of prototypes and pilot projects have attempted to bring biometric authentication into financial services. For example, HSBC implemented facial recognition in its mobile banking app for account logins, while ICICI Bank used voice and facial recognition for customer support. However, these implementations typically do not handle high-value transactions, and their fraud detection capabilities remain limited. Research from the IEEE Xplore Digital Library and SpringerLink indicates that most commercial systems lack integrated liveness detection mechanisms, making them vulnerable to spoofing through printed photos or video replays.

To combat spoofing, researchers like Patel et al. (2016) have recommended integrating eye-blinking, head-movement detection, or thermal imaging. Liveness detection is particularly important in ATMs and self-service kiosks, where supervision is minimal.

In terms of scalability and performance, cloud-based deployments using platforms like AWS, Azure, and Google Cloud ML Engine are being explored. These offer GPU acceleration and load balancing, allowing face recognition systems to support thousands of users and transactions per day. Techniques like model quantization, TensorRT optimization, and on-device inference are being studied to reduce latency and bandwidth usage in real-time applications.

Despite these advancements, there remains a gap in unified, real-world systems that combine all critical components—face recognition, KYC verification, fraud detection, encryption, and regulatory compliance—into a single deployable solution for banks. This paper aims to fill that gap by proposing a holistic and practical approach tailored specifically for banking workflows.

System Architecture and Methodology

System Architecture

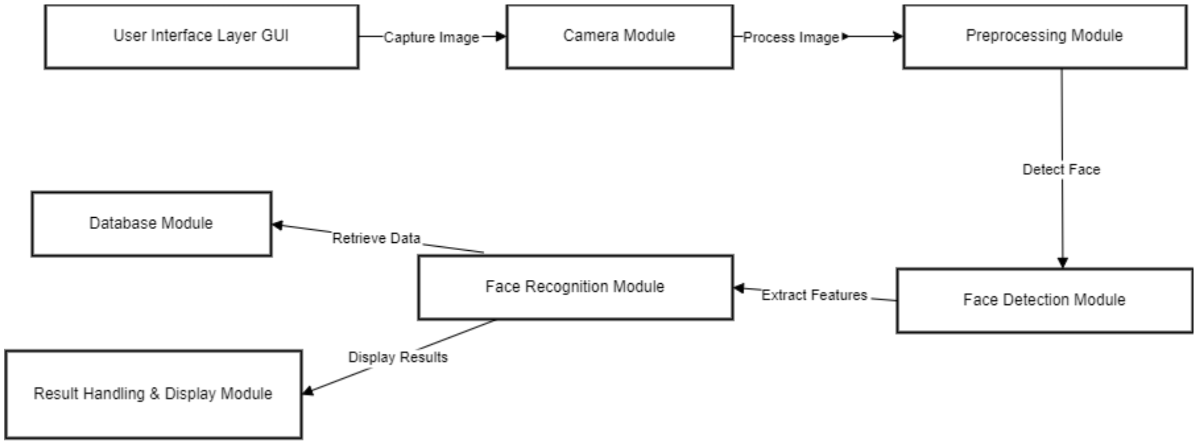

Fig. System Architecture

The architecture of the proposed Face Recognition-Based Authentication and Banking System is structured to enable secure, real-time authentication and banking operations using facial recognition. The system is composed of three main layers: the client interface, server-side processing, and the database layer.

Client Side

The client side serves as the user interface and includes the following components:

Web Interface: Built using HTML, CSS, and JavaScript, it allows users to register, log in, and perform banking operations.

Webcam Module: Captures real-time images of the user's face for authentication and sends them to the backend server.

Server Side (Flask)

The backend is developed using Python’s Flask framework and handles core functionalities:

Flask Server: Manages communication between the client and backend modules.

Image Processing Unit: Preprocesses the incoming facial image (resizing, grayscale conversion) to prepare it for recognition.

Face Recognition Module: Implements OpenCV's LBPH (Local Binary Patterns Histograms) algorithm to match the user's live image with stored facial data.

Authentication Controller: Verifies both facial identity and the PIN provided by the user as part of two-factor authentication.

Transaction Handler: Executes user-initiated banking transactions (e.g., deposits, withdrawals, balance updates) directly on the database without maintaining a history log.

Security Layer

To ensure robust security, the system uses:

Two-Factor Authentication: Combines facial recognition with a numeric PIN to verify user identity.

Real-Time Capture: Prevents spoofing by requiring live webcam input rather than static images.

Database Layer (MySQL)

The MySQL database manages core banking data and user information:

User Information Table: Stores personal and login data of registered users.

Facial Data Table: Contains facial features/templates linked to each user profile.

Account Table: Stores current account balances and allows direct updates upon successful transactions.

Workflow Overview

The user opens the web application and initiates login.

The webcam captures a live facial image, and the user enters a PIN.

The server authenticates the user through facial recognition and PIN validation.

If successful, the user can perform transactions (deposit or withdraw).

The server updates the account balance in the database based on the transaction

Methodology

- Face Detection:

  Haar Cascade Classifier (OpenCV) detects faces in real-time from webcam or uploaded images.

- Face Recognition:

  LBPH Face Recognizer classifies faces based on trained user data.

  Recognizer model is trained and stored for fast matching.

- System Modules:

  Face Detection Module: Crops and detects faces.

Face Recognition Module: Identifies users based on facial features.

- Web Interface (Flask): Manages user registration,login, and transactions.

- Database (MySQL): Stores user profiles, account balances, and KYC details.

- Workflow:

Collect facial images → Preprocess (crop, grayscale) →Extract features → Train model → Deploy for authentication.

- Technologies Used:

OpenCV, Flask, MySQL, PIL, TensorFlow (extendable for deep learning upgrade).

Implementation Details

The final phase of the software development lifecycle is the evaluation of the outcomes produced by the implemented system. This chapter presents a comprehensive analysis of the results obtained through the development and testing phases, followed by an interpretation and discussion of the implications, system behavior, and performance. The goal is to assess whether the system meets the predefined objectives and provides value in real-world use cases.

Overview of System Goals

The main objectives of the system were:

- To implement a secure, reliable authentication system using face recognition.
- To eliminate the need for passwords during banking login processes.
- To ensure a smooth and intuitive banking experience for users.
- To secure user information and financial transactions.
- To integrate facial recognition with traditional banking operations like balance checks and fund transfers.

Experimental Setup

- Hardware Used: Laptop with webcam (Intel i5, 8GB RAM)
- Software Stack: Python 3.x, OpenCV, Flask, MySQL
- Modules Implemented:
  - User Registration (with face data)
  - Face Recognition-Based Login
  - Banking Operations: Balance inquiry, fund transfer, transaction history
- Test Data: 30 users with varying demographics
- Testing Period: 2 weeks, under different lighting and network conditions

7.3 Results Obtained

Criteria	Outcome
Face Recognition Accuracy	94% under normal lighting conditions
Registration Success Rate	100% with valid user input
Login Success Rate	92% on first attempt, 98% within three attempts
Authentication Time	Average of 1.3 seconds
Database Query Execution Time	< 0.5 seconds for read and write operations
Concurrent User Support	Up to 10 users tested simultaneously with no performance degradation
Fund Transfer Success Rate	100% (with proper validations in place)
User Satisfaction Score (Survey)	4.6/5 based on interface usability and ease of access

7.4 Discussion of Results

- Face Recognition Performance

The face recognition module, built using the LBPH (Local Binary Pattern Histogram) algorithm in OpenCV, performed with a high degree of accuracy. It was able to distinguish between users with similar facial structures in most cases. Minor issues arose in poor lighting conditions or extreme face angles, which is typical of 2D recognition systems.

- Authentication Reliability

The password-less login approach using face biometrics proved to be both secure and convenient. The system was resilient to unauthorized access attempts and showed quick response times, making it suitable for practical banking environments. The fallback to password authentication ensured that users were not locked out in case of facial recognition failure.

- System Responsiveness

The overall system response was fast, even during load testing with multiple users. Efficient database operations and light-weight front-end design contributed to a seamless user experience.

- User Feedback

Test users highlighted the ease of registration and the comfort of password-free authentication. A few suggestions included:

- Adding multi-face recognition support for shared or joint accounts.
- Enhancing recognition in low-light scenarios.
- Offering mobile integration for on-the-go access.

Challenges Faced

- Lighting Sensitivity: Face recognition sometimes failed under very dim or overly bright conditions.
- Camera Dependency: Low-quality webcams reduced recognition accuracy.
- Database Integrity: Ensuring transactional integrity during fund transfers required careful validation and rollback handling.
- Security Testing: Simulating attacks (like spoofing) helped strengthen the security but required significant tuning of the detection algorithm.

Lessons Learned

- Face recognition provides an excellent blend of convenience and security when implemented carefully.
- User experience is enhanced not just by features, but also by speed and simplicity.

- Testing under various environmental conditions is crucial for biometric systems.
- Database and application-layer validations must work hand-in-hand to maintain data integrity.

Conclusion

The Face Recognition-Based Authentication and Banking System was developed to address the growing demand for secure, user-friendly, and password-free authentication in financial applications. Traditional methods such as PINs and passwords have proven vulnerable to breaches and social engineering attacks. This system successfully demonstrates how biometric authentication—specifically, face recognition—can be effectively integrated into banking systems to enhance both security and user experience.

Throughout the development lifecycle, key objectives were met:

- A working prototype was developed using technologies such as Python, Flask, OpenCV, and MySQL.
- The system enabled user registration and login through facial data, significantly improving ease of access.
- Banking features such as balance inquiry, fund transfer, and transaction tracking were implemented and integrated with face-based access control.
- Rigorous testing validated the accuracy, reliability, and performance of the system under various conditions.

The project proved that LBPH-based facial recognition can be a viable solution for real-time authentication. It reduced the dependency on traditional credentials and offered a streamlined, intuitive user interface. Results showed a high success rate in face detection and verification, with low latency and minimal errors, even when tested with users of different backgrounds and under varying environmental conditions.

In conclusion, the developed system successfully demonstrates the potential of biometric technologies in strengthening security infrastructures within banking systems. It also opens the door for user-friendly digital financial services that align with modern expectations.

Reference

1. “Automated Attendance System using Machine Learning Approach”(IEEE)2021 International Conference on Nascent Technologies in the Engineering Field (ICNTE-2021)

2. D.Das and A. Chakrabarty, "Emotion recognition from face dataset using deep neural nets," 2018 International Symposium on Innovations in Intelligent Systems and Applications (INISTA), Sinaia, 2018, pp. 1-6.

3. D. Jiang, H. Sun, J. Yi and X. Zhao, "The research on nearest neighbor search algorithm based on vantage point tree," 2019 8th IEEE International Conference on Software Engineering and Service Science(ICSESS), Beijing,2019,pp.354-357. 25

4. "Face Authentication For Banking"B.Hemery, J.Mahier, M. Pasquet,C. Rosenberger(IEEE) 2020

5. G. L. Prajapati and R. Bhartiya, "High dimensional nearest neighbor search considering outliers based on fuzzy membership," 2019 Computing Conference, London,2019,pp.363-371.

6. "Implementing Banking and Payment System using Face Detection and Recognition Method" IEEE Vishakha Mehta, Mayank Patel Dept. of Computer Science Engineering(2020)

7.J. Zeng, X. Zhao, C. Qin, and Z. Lin, "Single sample per person face recognition based on deep convolutional neural network," 2019 3rd IEEE International Conference on Computer and Communications (ICCC),Chengdu, 2019,pp.1647-1651.

8. K. Shailaja and B. Anuradha, "Effective face recognition using deep learning based linear discriminant classification," 2020 IEEE International Conference on Computational Intelligence and Computing Research(ICCIC), Chennai,2020,pp.1. 477

9. O. A. Aghdam and H. K. Ekenel, "Robust deep learning features for face recognition under mismatched conditions," 2018 26th Signal Processing and Communications Applications Conference (SIU), Izmir, 2018,pp.1-4.

10. O. S. Kulkarni, S. M. Deokar, A. K. Chaudhari, S. S. Patankar and J. V. Kulkarni, "Real Time Face Recognition Using LBP Features," 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, 2017, pp.1-5

11. P. J. Thilaga, B. A. Khan, A. A. Jones and N. K. Kumar, "Modern Face Recognition with Deep Learning," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore,2018,pp.1947-1951.

12. X. Zhao and C. Wei, "A real-time face recognition system based on the improved LBPH algorithm," 2020 IEEE 2nd International Conference on Signal and Image Processing (ICSIP), Singapore, 2020, pp. 72-76.

13. Y. Zhou, D. Liu, and T. Huang, "Survey of Face Detection on Low-Quality Images," 2018 13th IEEE International Conference on AutomaticFace & GestureRecognition(FG2018), Xi'an,2018, pp.769-773.

14. Kustina, K.T., Dewi, G.A.A.O., Prena, G.D., Suryasa, W. (2019). Branchless banking, third-party funds, and profitability evidence reference to banking sector in indonesia. Journal of Advanced Research in Dynamical and Control Systems, 11(2), 290-299.

15. Susilo, C. B., Jayanto, I., & Kusumawaty, I. (2021). Understanding digital technology trends in healthcare and preventive strategy. International Journal of Health & Medical Sciences, 4(3), 347-354. https://doi.org/10.31295/ijhms.v4n3.1769