Journal of Advances in Developmental Research (IJAIDR)

E-ISSN: 0976-4844 ● Website: www.ijaidr.com ● Email: editor@ijaidr.com

Face Verification Based Banking System

Vvalarmathi A[1], Renuka.R[2]

[1,2]Bsc. Computer Science, Jepiaar University

Abstract:
Python and the Flask framework were used to create the secure online banking application known as the Face Verification Based Banking System. By utilizing face recognition technology for biometric authentication, the system improves banking security. Passwords and PINs, which are susceptible to theft, hacking, and unauthorized access, are a major component of traditional banking systems. The suggested system adds facial recognition as an extra layer of authentication to get around these restrictions .Users can register their personal details with the system, and their faces are safely saved in a database. The system uses a camera to take a picture of the user's face during login, then uses OpenCV-based facial recognition techniques to compare it with stored facial data.

Keywords: Face Verification, Recognition of faces Biometric Verification, Security of Banking, Web-Base Program, OpenCV, Processing Images, Authentication of Users, Verification of Identity, Safe Login Procedure, Database administration, digital banking, camera integration, and feature extraction, Learning by Machine, Vision in Computers, Security of Data, Preventing Fraud.

1.INTRODUCTION

Banking systems have quickly developed into online platforms in the current digital era, providing users all over the world with convenience and accessibility. But this development has also raised the danger of identity theft, illegal access, and cyberattacks. Due to their vulnerability to hacking, phishing,
and social engineering attacks, traditional authentication techniques like passwords and PINs are no longer adequate to guarantee total security.
The Face Verification Based Banking System is presented as a safe and creative way to deal with these issues. To improve the security of online banking applications, this system incorporates facial recognition technology for biometric authentication.

2.LITERATURE REVIEW

The topic of biometric authentication has seen substantial development in recent years, with a special emphasis on facial recognition to improve banking security. Due to the widespread criticism of traditional authentication techniques like passwords and PINs for being susceptible to hackers, experts are now looking at more secure options.
Combining several biometric techniques has also been investigated. A multimodal solution that combines face and fingerprint recognition to offer more robust authentication was presented in an ATM security study. This method lowers the possibility of unwanted access while increasing accuracy. IJRASET Additional developments in real-time systems demonstrate that facial recognition can be effectively applied to online transactions. A real-time biometric system that replaces conventional password-based authentication was proposed by Dhivya et al.

3.PROBLEM STATEMENT

In modern digital banking systems, security is a major concern due to the increasing number of cyberattacks, identity thefts, and unauthorized access attempts. Traditional authentication methods such

as passwords and PINs are widely used but are vulnerable to hacking, phishing, and misuse. Users often create weak passwords or reuse them across multiple platforms, which further increases security risks.
It is challenging to confirm that the person gaining access to an account is the authorized user since existing banking systems lack strong identity verification procedures. The majority of current systems mostly rely on knowledge-based authentication techniques like PINs and passwords, which are readily guessed, stolen, or shared. Because unauthorized people can obtain access without being physically present, this poses a serious security risk.

Additionally, these systems are susceptible to fraud and impersonation as they do not instantly confirm the user's true identity. Attackers can take advantage of these flaws by using methods including social engineering, credential stuffing, and phishing. Sensitive financial data is thereby made public, raising the possibility of data breaches and financial loss.This creates opportunities for fraud and financial loss. Therefore, there is a need for a more secure, reliable, and user-friendly authentication system that can overcome the limitations of traditional methods and enhance banking security.

4.PROPOSED METHODOLOGY

4.1system design

The system is designed as a web-based application using Python and the Flask framework. It includes modules such as user registration, login authentication, facial verification, and banking operations. A database is used to store user details and facial data securely.

4.2 User Registration

New users are required to register by providing personal information such as name, account details, and contact information. During registration, the system captures multiple facial images using a webcam. These images are processed and stored in the database for future verification.

4.3 Image Preprocessing

The captured facial images are preprocessed to improve accuracy. This includes:
Converting images to grayscale
Resizing images to a standard format
Noise reduction and normalization
These steps help in improving the performance of the face recognition algorithm.

4.4 Face Detection and Feature Extraction

The system uses OpenCV to detect faces from the captured images. Techniques such as Haar Cascade or deep learning-based models are used to locate facial features. Important features are extracted and converted into numerical representations (feature vectors).

4.5 Face Recognition

During login, the system captures the user's live image and compares it with stored facial data. Recognition algorithms such as Local Binary Pattern Histogram (LBPH) or deep learning models are used to match facial features. If the similarity score meets the required threshold, the user is authenticated.

4.6Authentication Process

The system verifies both login credentials (username/password) and facial recognition results. Access to the banking system is granted only when both authentication steps are successfully completed, ensuring multi-level security.

4.7Database Management

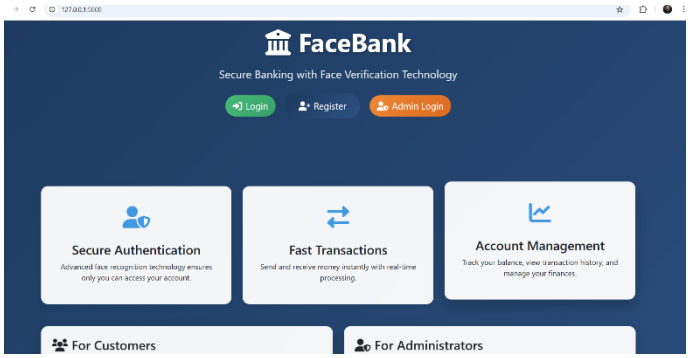
All user data, including facial images and account details, are securely stored in a database. Data encryption and secure storage practices are followed to protect sensitive information.

4.8 Banking Operations

Once authenticated, users can perform banking operations such as checking balance, transferring funds, and viewing transaction history within the secure environment.

4.9Security Measures
Additional security features are implemented, including:
Data encryption
Secure session management
Protection against spoofing attacks (basic level).

5.SYSTEM ARCHITECTURE
1. User Access
User opens the web application in browser
Home page shows:
1.Register 2.Login



2. Registration Workflow
Steps:
User clicks Register
Enters details:
Name
Account number
Other info
System activates webcam
Captures multiple face images
Face is detected using OpenCV
Images stored in dataset folder
User data saved in database
Output: User successfully registered

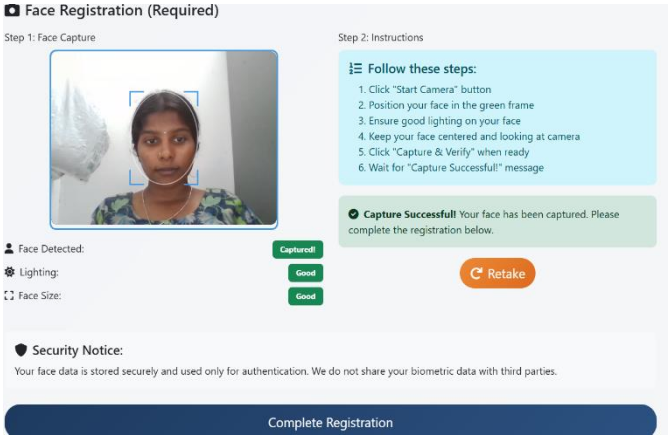
3. Login Workflow (Face Verification)
Steps:
User clicks Login
Webcam opens automatically
System captures live face
Face detection performed
Face converted into encoding
Compared with stored face data

6.IMPLEMENTATION OF MODULES
1. User Registration Module
The registration module allows new users to create an account and store their facial data.
Users enter details such as name, account number, email, and password

Password is securely hashed before storing in the database
OpenCV is used to capture multiple facial images via webcam
Images are stored in a dataset folder or database
All user details are saved and linked with facial data
Steps:
User fills registration form
System captures face images
Images are preprocessed and stored
User data is saved in database

2.Admin Module:
The admin module manages users and monitors system activity.
Admin logs in with secure credentials
Can view registered users and their details
Can monitor transactions and system logs
Has permission to add/remove users
Can update or delete user records if required
Steps:
Admin logs into system
Access admin dashboard
Manage users and data
Monitor system performance

3.User Login Module
The login module verifies user identity using both credentials and face recognition.
User enters username and password
System validates credentials from database
Webcam captures live facial image
OpenCV compares captured face with stored dataset
If both password and face match → access granted
Steps:
User enters login details
System checks username/password
Face is captured and processed
Face recognition is performed
If matched → user redirected to dashboard
If not matched → access denied
Unauthorized users were denied access when the facial data did not match, demonstrating the system's effectiveness in preventing intrusions.
Banking operations such as balance inquiry, fund transfer, and transaction history were executed smoothly after successful authentication.



7. CONCLUSION

The Face Verification Based Banking System provides a secure and efficient solution to the limitations of traditional authentication methods used in banking. By integrating facial recognition technology with a web-based application developed using Python and the Flask framework, the system enhances user authentication and reduces the risk of unauthorized access and identity fraud.

The use of biometric verification ensures that only authorized users can access their accounts, making the system more reliable than password-based security alone. The implementation of OpenCV for face detection and recognition demonstrates how computer vision techniques can be effectively applied in real-world banking applications.

Overall, the system improves security, user convenience, and trust in digital banking services. It highlights the potential of biometric technologies in modern financial systems and opens the path for further advancements, such as multi-factor authentication and improved anti-spoofing techniques. Future enhancements can focus on increasing accuracy, handling real-time challenges, and strengthening data privacy measures.

REFERENCES:

1. A. K. Jain, A. Ross, and S. Prabhakar, “An Introduction to Biometric Recognition,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, Jan. 2004.
2. R. Szeliski, Computer Vision: Algorithms and Applications, Springer, 2010.
3. G. Bradski and A. Kaehler, Learning OpenCV: Computer Vision with the OpenCV Library, O’Reilly Media, 2008.
4. P. Viola and M. Jones, “Rapid Object Detection using a Boosted Cascade of Simple Features,” in Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2001.
5. I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning, MIT Press, 2016.
6. OpenCV Documentation, “Face Recognition using OpenCV,” [Online]. Available: https://opencv.org/
7. Flask Documentation, “Flask Web Framework,” [Online]. Available: https://flask.palletsprojects.com/
8. S. Z. Li and A. K. Jain, Handbook of Face Recognition, Springer, 2011.