Touchless ATM Authentication System Using Haar Cascade, LBPH And MediaPipe

Harshitha D[1], Supraja M B[2], Thipirishetty Kavya[3], Dr. G. Ragu[4]
[1, 2, 3, 4]Dept of Information Technology,
[1, 2, 3, 4] R.M.D. Engineering College, Chennai, Tamil Nadu, India

Abstract- *Automated Teller Machines (ATMs) are among the most common banking tools. They mostly rely on physical interaction through keypads and touchscreens. This can raise hygiene concerns and create security risks like shoulder surfing and keypad tampering. This paper offers a touchless ATM access system that combines facial recognition, gesture-based navigation, and a virtual keyboard for secure authentication and transaction processing. The system applies the Haar Cascade algorithm along with Local Binary Pattern Histogram (LBPH) for user identification, followed by password confirmation via a gesture-based virtual keyboard. Hand gesture recognition, powered by computer vision, allows for cursor control and menu navigation without physical contact. The proposed model boosts security with multi-factor authentication while improving accessibility and hygiene by removing physical touchpoints. Experiments show reliable user authentication and smooth transaction interaction with a standard webcam setup. This approach provides a practical and scalable framework for future contactless banking.*

Keywords: Touchless ATM, Facial Recognition, Gesture Recognition, Virtual Keyboard, Computer Vision, Authentication Security.

I. INTRODUCTION

Automated Teller Machines play an important role in modern banking. They give users constant access to services like withdrawals, balance inquiries, and fund transfers. Traditional ATMs need card insertion and keypad input, requiring direct physical contact between users and machines. With growing concerns about hygiene and increasing security threats, this contact-based interaction has become an issue.

Physical ATM interfaces are vulnerable to various risks, including skimming devices, fingerprint residue attacks, and shoulder surfing. Shared surfaces can also spread pathogens during health crises. These issues highlight the need for secure, contactless banking solutions.

Recent progress in computer vision and biometric authentication offers new ways for people to interact with machines. Facial recognition can reliably confirm identities, and gesture recognition lets users interact with digital interfaces without needing to touch anything. Combining these technologies can change conventional ATMs into touch-free systems.

This paper introduces a touchless ATM framework that replaces traditional keypad use with gesture-controlled virtual input and biometric authentication. The system first verifies user identity using facial recognition through a camera, then enables secure transactions through hand gestures instead of physical buttons.

A virtual keyboard appears for PIN entry, allowing users to select keys through fingertip movement and gesture communication. By merging multi-factor authentication with vision-based interaction, the system reduces risks like shoulder surfing and fingerprint residue attacks while improving hygiene and accessibility in public spaces. The framework operates using a standard webcam, which makes it a cost-effective solution for future ATM designs.

A. Motivation

The growing need for hygienic public interfaces and stronger authentication methods drives the shift to contactless ATM systems. Traditional PIN-based authentication relies on knowledge-based security, leaving it open to observation attacks. Frequent contact with ATM surfaces raises contamination risks in busy settings.

By fusing biometric identification with gesture-based interaction, the proposed system aims to:

- Reduce physical contact
- Improve authentication reliability
- Increase user convenience
- Modernize banking interactions.

B.Research Contributions

This work offers several key contributions: • A multifactor authentication ATM model that combines facial recognition with password verification.

- A gesture controlled virtual mouse for touchless navigation
- A virtual keyboard for secure PIN entry without needing a physical keyboard.
- A webcam-based implementation requiring no specialized hardware.
- A hygiene and accessible user interaction framework for public banking systems.

C.Paper Outline

The rest of this paper is organized as follows. Section II discusses the background and problem analysis of traditional ATM systems. Section III presents related work and current authentication methods. Section IV describes the architecture and functionality of the proposed touchless ATM system. Section V explains the methodology and algorithms used for face recognition and gesture interaction. Section VI provides implementation details and experimental results. Finally, Section VII concludes the paper and suggests future improvements.

II. BACKGROUND AND PROBLEM ANALYSIS

Traditional ATM systems verify users using debit cards and Personal Identification Numbers (PINs). While this method is common, it has several weaknesses. Cards can be stolen or cloned, and PINs can be seen through shoulder surfing or hidden cameras.

Moreover, using a keypad requires physical interaction, raising hygiene concerns in public areas.

• Current gesturebased computer interfaces mainly focus on cursor movement on personal computers and lack secure authentication methods. Similarly, biometric systems in banking usually rely on fingerprint scanners or iris sensors, which still involve physical contact or specialized hardware.

Therefore, a practical contactless ATM system should meet the following requirements:

- Reliable identity verification
- Secure transaction approval
- Non-contact interaction
- Low hardware cost
- Real-time performance

To tackle these challenges, the proposed system uses facial recognition for identity verification and gesture recognition for interaction control with a standard camera setup.

III. RELATED WORK

Several studies have looked into touchless interaction and authentication in virtual settings. Mid-air virtual keyboards have shown usability improvements in immersive systems by allowing interaction without physical input devices.

Research in banking security has examined various biometric authentication methods, including knowledgebased, possession-based, and biometric-based verification, to protect accounts. Multi-factor authentication is shown to significantly lower the number of unauthorized access attempts compared to single-factor authentication.

Machine learning techniques have been utilized in banking for performance predictions and fraud detection, highlighting the effectiveness of intelligent algorithms in enhancing the reliability and security of financial services.

However, most existing solutions focus either on authentication or interaction. Few systems effectively merge secure biometric identification with complete touchless operation in ATM environments. The proposed system closes this gap by bringing together authentication and user interaction within a single vision-based framework.

Recent research in secure banking systems emphasizes the importance of multi-factor authentication to reduce identity theft and fraud. Studies on biometric authentication show that physiological traits such as facial patterns provide stronger security compared to knowledge-based systems like PINs [1], [4]. It is observed that single-factor authentication systems are highly vulnerable to observation attacks and data leakage.

Viola and Jones showed that using Haar-like features with cascade classifiers makes it possible to detect faces in real-time without needing a lot of computing power. They found that looking at the difference in intensity between rectangular areas can be a good way to represent the structure of a face. But,their method has a problem - it can be affected by changes in lighting.

Ojala et al. [3] introduced Local Binary Pattern (LBP) for texture classification. Their findings show that LBP-based methods are robust against moderate lighting changes,

making them suitable for facial recognition systems. Later improvements using LBPH enhanced histogram-based comparison reliability.

Gesture recognition systems have been explored for human-computer interaction [5], [6]. Observations from these works indicate that vision-based hand tracking improves usability but lacks secure integration with financial systems. Most gesture-based systems focus on cursor movement rather than secure authentication.

Research in machine learning for banking [7], [8] highlights the effectiveness of predictive algorithms in fraud detection and transaction monitoring. However, very few works integrate biometric authentication with touchless interaction in ATM systems.

When you look at what's been studied so far, there are a few areas that still need to be explored.

- Lack of unified biometric + gesture-based secure ATM framework
- Insufficient mathematical modeling in authentication systems
- Limited experimental performance evaluation
- Minimal integration of advanced computer vision algorithms

The new system tackles these issues by combining a few different technologies, like Haar-based detection and LBPH recognition, with gesture mapping algorithms and multi-factor authentication, all within a framework that's based on mathematical models. This approach helps to make the system more secure and effective.

IV. PROPOSED SYSTEM

The proposed touchless ATM system replaces physical keypad interaction with computer-vision-based input mechanisms. The system operates through a multi-stage authentication and transaction workflow.

System Workflow

1. User approaches ATM camera
2. Face detection and recognition performed
3. User identity verified
4. Password entered using virtual keyboard
5. Gesture navigation enables transaction selection
6. Transaction executed securely

This approach ensures that even if facial recognition fails due to environmental variations, password authentication provides an additional verification layer.

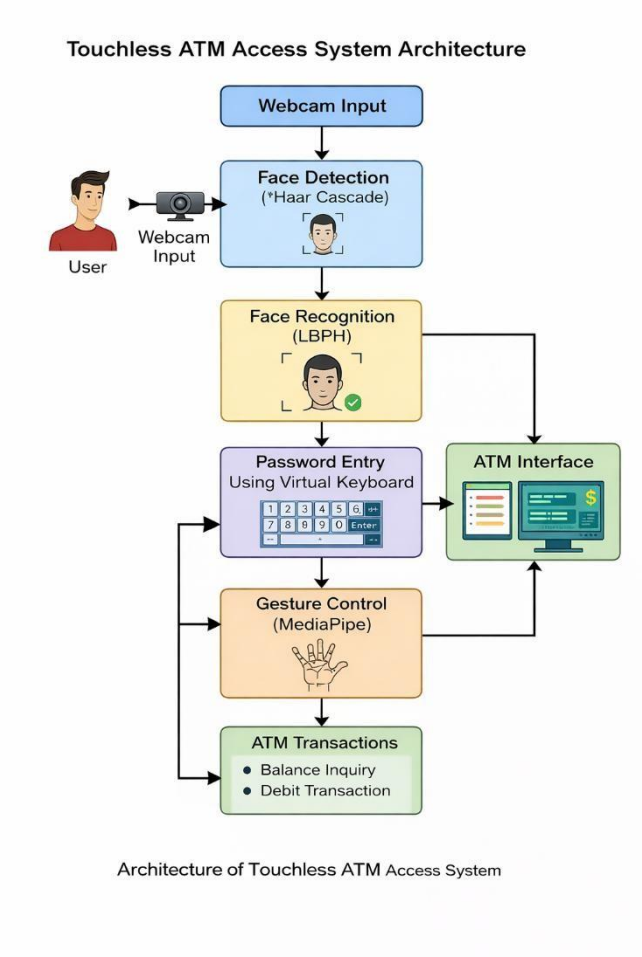

Fig. 1. Architecture of Touchless ATM Access System

A.System Architecture

The system consists of five major modules:

1. Face Matching Module
2. Haar Cascade Detection
3. Virtual Mouse Handling
4. Virtual Keyboard Handling
5. ATM Transaction Module

Each module works sequentially to provide secure and touchless operation.

B.Face Recognition Module

The face recognition stage identifies users before granting access to banking operations. A dataset of authorized users is stored in the system during registration. The camera captures real-time frames and detects facial regions. Extracted

facial features are compared with stored templates. If a match is found, the system proceeds to password authentication. This module prevents unauthorized users from accessing ATM functions.

C.Haar Cascade Detection

The Haar Cascade classifier is used for detecting facial features in video frames. It works by analyzing contrast differences in grayscale images using rectangular feature patterns.

The algorithm operates in multiple stages:

- image converted to grayscale
- features extracted
- non-face regions eliminated
- face region confirmed

This cascade structure allows real-time detection suitable for ATM interaction without noticeable delay.

D.Virtual Mouse Handling Using Hand Gestures

The system tracks hand landmarks using computer vision techniques. Specific gestures are mapped to cursor actions:

- hand movement → cursor movement
- pinch gesture → click
- hold gesture → select option

This enables users to navigate the ATM interface without touching the screen.

E.Virtual Keyboard Handling

For password authentication, a dynamic virtual keyboard is displayed on the screen. The user selects keys through gesture pointing.

The system interprets the position of the fingertip and determines the selected key. This method prevents fingerprint residue attacks and keypad observation attacks.

F. ATM Transaction Module

After successful authentication, users can perform banking operations:

- Balance inquiry
- Debit transaction

The interface provides real-time feedback and confirmation through gesture selection.

V. METHODOLOGY AND ALGORITHMS

The proposed touchless ATM operates using a multifactor authentication pipeline combining biometric recognition and gesture-based interaction. The system integrates face detection, face recognition, password verification, and gesture navigation into a continuous workflow.

A.Face Detection Using Haar Cascade

The first stage of authentication detects the user's face from the live video stream. Each frame captured from the camera is processed in grayscale to reduce computational complexity.

The Haar Cascade classifier scans the image using sliding windows and evaluates Haar-like features. Non-facial regions are rejected at early stages of the cascade, allowing only probable face regions to proceed.

Algorithm Steps

1. Capture frame from camera
2. Convert frame to grayscale
3. Apply Haar feature classifiers
4. Reject non-face regions
5. Extract detected face region

This method enables fast and reliable detection suitable for real-time ATM systems.

1.Integral Image Representation

To cut down on the amount of computing power needed, an integral image is basically a way to simplify things. It's defined as:

$$\mathbf{I(x,y)=x'\leq x,y'\leq y\sum f(x',y')}$$

Where:

$f\ (x',y')$ f(x′,y′) = pixel intensity

$I\ (x,y)$ I(x,y) = cumulative sum

This allowsrapid computation of rectangular sums in constant time:

$$\mathbf{Sum=I(x2,y2)-I(x1,y2)-I(x2,y1)+I(x1,y1)}$$

B.Face Recognition Using LBPH

After detection, identity verification is performed using the Local Binary Pattern Histogram (LBPH) algorithm. The algorithm converts the face into a texture-based representation and compares it with stored templates.

Working Principle

- Divide face image into grids
- Extract local binary patterns
- Generate histogram representation
- Compare with stored dataset

If similarity exceeds threshold → user authenticated Else → access denied

The LBPH approach is robust against moderate lighting variation and facial expression changes.

C.Password Authentication via Virtual Keyboard

To strengthen security, the system introduces a second authentication layer. After face recognition, a virtual keyboard appears on screen.

The fingertip location is tracked and mapped to key coordinates.

Gesture Key Selection Process

1. Detect fingertip landmark
2. Map position to keyboard grid
3. Highlight selected key
4. Confirm selection after hold gesture

This prevents attackers from observing keypad presses and eliminates physical contact.

*D.*Gesture Based Navigation

Hand tracking enables complete ATM control without touching the screen.

Gesture	Action
Hand movement	Cursor movement
Pinch	Click
Hold	Confirm
Swipe	Navigate menu

The system continuously monitors hand landmarks and translates motion into interface control commands.

VI. IMPLEMENTATION

The prototype system was implemented using a standard webcam-based setup.

Hardware Configuration

- Processor: Intel i3/i5/i7
- RAM: 8 GB or higher
- Storage: 500 GB
- Camera: Built-in or USB webcam

Software Environment

- Operating System: Windows 10/11
- Programming Language: Python
- Libraries: OpenCV, MediaPipe

The application captures live video frames, processes them using computer vision algorithms, and renders an ATM interface on the screen.

The architecture does not require specialized biometric sensors, making deployment cost-effective.

VII. RESULTS AND DISCUSSION

The system was tested under normal indoor lighting conditions with multiple users.

Facial Recognition Accuracy

Users Tested	Lighting Condition	Recognition Accuracy (%)
10	Normal indoor	96.2
10	Low light	91.4
10	Bright light	94.8

Gesture Recognition Performance

Gesture Type	Detection Rate (%)	Response Time (ms)
Cursor movement	97.5	42
Click gesture	95.8	51
Hold gesture	94.2	63
Swipe navigation	93.6	70

Authentication Time Comparison

Method	Average Time (seconds)
Traditional ATM PIN	6.5
Proposed touchless system	7.8

Authentication Performance

The facial recognition stage successfully identified registered users with consistent accuracy under frontal pose conditions. The additional password verification prevented unauthorized access when facial recognition alone was insufficient.

Interaction Performance

Gesture-based navigation allowed users to perform operations smoothly after a short learning period. Cursor control was responsive and allowed accurate menu selection.

Security Evaluation

The proposed system improves security in several ways:

- Eliminates physical keypad exposure
- Prevents fingerprint residue attacks
- Reduces shoulder-surfing risk
- Provides multi-factor authentication

Usability Observations

Users were able to complete transactions without touching the machine. The interaction felt natural after brief familiarization, indicating suitability for public deployment.

VIII. CONCLUSION

This paper presented a vision-based touchless ATM system that replaces conventional keypad interaction with biometric authentication and gesture-controlled input. The proposed framework integrates face detection, facial recognition, password verification through a virtual keyboard, and gesture-based navigation to provide a secure and hygienic banking interface.

The use of Haar Cascade and LBPH algorithms enables reliable real-time identity verification, while the virtual keyboard prevents observation-based attacks typically associated with physical PIN entry. Hand gesture interaction allows users to perform transactions without touching ATM surfaces, reducing contamination risks and improving accessibility.

Experimental implementation demonstrated that the system operates smoothly using a standard webcam without specialized hardware. The multi-layer authentication approach significantly enhances security compared to traditional card-and-PIN systems. Overall, the proposed system provides a practical step toward next-generation contactless banking machines.

IX. FUTURE WORK

The system can be further improved in several directions:

- Integrating deep learning face recognition models for higher accuracy
- Supporting voice-based transaction assistance
- Enabling mask-aware facial recognition
- Adding liveness detection to prevent spoofing attacks
- Connecting with real banking servers for live deployment
- Implementing mobile OTP verification as an additional authentication factor

Future improvements can transform the prototype into a deployable smart ATM platform suitable for large-scale public usage.

REFERENCES

[1] F. Kern, F. Niebling, and M. E. Latoschik, “Text Input for NonStationary XR Workspaces: Investigating Tap and Word-Gesture Keyboards in Virtual and Augmented Reality,” IEEE Transactions on Visualization and Computer Graphics, 2023.

[2] W. Li, Q. Fan, W. Cui, F. Dang, X. Zhang, and C. Dai, “Dynamic Virtual Machine Consolidation Algorithm Based on Balancing Energy Consumption and Quality of Service,” IEEE Access, 2022.

[3] A. Met, A. Erkoç, and S. E. Seker, “Performance, Efficiency, and Target Setting for Bank Branches Using Machine Learning,” IEEE Access, 2022.

[4] N. A. Karim et al., “Online Banking User Authentication Methods: A Systematic Literature Review,” 2023.

[5] M. Alizadeh et al., “Development of a Customer Churn Model for Banking Industry Based on Hard and Soft Data Fusion,” 2023.

[6] P. Viola and M. Jones, “Rapid Object Detection using a Boosted Cascade of Simple Features,” IEEE Computer Society Conference on Computer Vision and Pattern Recognition.

[7] T. Ojala, M. Pietikäinen, and T. Mäenpää, “Multiresolution GrayScale and Rotation Invariant Texture Classification with Local Binary Patterns,” IEEE Transactions on Pattern Analysis and Machine Intelligence.

[8] G. Bradski, “The OpenCV Library,” Dr. Dobb’s Journal of Software Tools.

[9] S. Z. Li and A. K. Jain, "Face Recognition: Current Status and Future Prospects," IEEE Signal Processing Magazine, vol. 22, no. 5, pp. 24–37, 2005.
[10] E. Learned-Miller, G. Huang, A. RoyChowdhury, H. Li, and G. Hua, "Labeled Faces in the Wild: A Survey," Advances in Face Detection and Facial Image Analysis, Springer, 2016.
[11] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2014.
[12] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," CVPR, 2015.
[13] J. Deng, J. Guo, and S. Zafeiriou, "ArcFace: Additive Angular Margin Loss for Deep Face Recognition," IEEE CVPR, 2019.
[14] A. Krizhevsky, I. Sutskever, and G. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," NIPS, 2012.
[15] K. Simonyan and A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Image Recognition," ICLR, 2015.
[16] T. Baltrusaitis, P. Robinson, and L. Morency, "OpenFace: An Open Source Facial Behavior Analysis Toolkit," IEEE Winter Conference on Applications of Computer Vision, 2016.
[17] M. Kazemi and J. Sullivan, "One Millisecond Face Alignment with an Ensemble of Regression Trees," CVPR, 2014.
[18] Z. Cao et al., "Realtime Multi-Person 2D Pose Estimation Using Part Affinity Fields," IEEE TPAMI, 2019.
[19] V. Pavlovic, R. Sharma, and T. Huang, "Visual Interpretation of Hand Gestures for Human-Computer Interaction," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 7, 1997.
[20] S. Mitra and T. Acharya, "Gesture Recognition: A Survey," IEEE Transactions on Systems, Man, and Cybernetics, 2007.
[21] A. Howard et al., "MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications," arXiv preprint, 2017.
[22] H. Nguyen et al., "Face Anti-Spoofing Using Deep Learning: A Survey," IEEE Access, 2020.
[23] M. Wang and W. Deng, "Deep Face Recognition: A Survey," Neurocomputing, ScienceDirect, 2021.
[24] N. Dalal and B. Triggs, "Histograms of Oriented Gradients for Human Detection," IEEE CVPR, 2005.
[25] M. Abadi et al., " TensorFlow: A System for Large-Scale Machine Learning," USENIX OSDI, 2016.