

Smart ATM Access System using Face and Voice Recognition with Machine Learning

M. Rajasekaran¹, Machendra², S. Harish Karthick³, S. Dhanush⁴ and B. Navaneetha Krishna^{5*}
{m.rajasekaran@klu.ac.in¹, 99210041771@KLU.AC.IN², 9921004259@klu.ac.in³,
99210041808@klu.ac.in⁴, 9921004501@KLU.AC.IN⁵}

Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education,
Krishnan Koil, Virudhunagar, Tamil Nadu, India^{1, 2, 3, 4, 5}

Abstract. In this paper, we propose a new Automated Teller Machine (ATM) system using face and speech recognition technologies which are very effective in terms of the security and user convenience, respectively. Written in Python, this system is capable of harnessing powerful machine-learning techniques to recognise a face and authenticate a voice. This two-factor verification method guarantee that it is only verified users who are able to access their accounts and, in turn, reducing the risk of fraud and unauthorised staff access considerably. The camera of the facial recognition part records the image of the user, and input information and output information are exchanged through the voice recognition part to process voice commands, thereby realizing convenient and safe controls. The system has been implemented providing a friendly user interface and similar performance under different environmental conditions. The system, which uses libraries such as OpenCV (for visual processing) and Speech Recognition (for audio input), provides a more contemporary solution to enhance the ATM experience, given current burgeoning security issues across the financial sector. This biometric based ATM model can be taken as a platform for future developments in banking sector, by following the footsteps of adopting emerging biometric technologies even in day to-day banking, so that users may feel much safer while using digital banking systems.

Keywords: Face recognition, Voice recognition, Biometric authentication, ATM security, Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), OpenCV, Multimodal biometrics

1 Introduction

Facial and voice recognition in ATMs is changing the face of banking security. Instead of relying on outdated PINs and cards - which are risky because they can be stolen - this biometric two-factor authentication procedure offers consumers a superior and easier to use method for their financial needs [11].

Using facial recognition, the software reads and computes the user's face as it happens. It can accurately detect users, even under less than ideal lighting conditions or angles that may impede reference points, thanks to machine learning algorithms that have been trained on millions of images [13]. Voice recognition also enables the users to give spoken commands to the ATM, making the transactions hands-free and more human-like [12].

The integration of both facial and voice biometrics provides an extra layer of security and will directly combat the rising concerns of identity theft and banking fraud." It doesn't just make the

unauthorized access much more difficult, it also has the potential to simplify the user experience, opening up ATMs to a wider variety of users.

So, with lifestyle and technology information moving toward the same password less paradigm, these high-tech ATMs, well, are just the beginning for the various other ways we'll all be verifying identity. They're a nice balance between security and usability that most of the legacy systems lack.

The old 'card and PIN' based systems, which rely on customers carrying a card, are under scrutiny by users in a modern age that demands quick and easy banking anytime and anywhere. Using attributes that are distinctive to an individual, such as a person's voice tone and the shape of their face, the approach to identity confirmation offers a more personalized and secure way of ensuring mega convenience.

This two-step process identifies an individual through facial recognition first and then through their voice. Multi-modal enables low probability of impersonation/fraud and high trustworthiness for each transaction.

From a technical standpoint, the platform is developed with Python and employs the OpenCV for facial detection and other speech recognition libraries for audio processing. Such technologies can work across a variety of conditions and they can pick up faint signals to help decide whether a voice is authentic or pre-recorded providing another line of defence.

By combining facial and voice recognition, this new ATM system offers improved security as well as increased convenience. It's a move toward reshaping what safe and frictionless banking feels like in the digital age.

With cyberattacks becoming more sophisticated and the proliferation of identity theft in the financial sector, more sophisticated resilient form of authentication is required. Financial institutions are faced with the challenge of providing convenience and security, as consumers grow to desire faster and more frictionless services. Biometric identity verification, and specifically the combination of facial and voice recognition, appears to be a solution to both these problems. It does away with physical cards and memorized passwords, of course.

2 Related works

In study [1], biometric technology was used to improve ATM security. Conventional ATM systems, which are based on PINs and physical cards, were found to be susceptible to theft and fraud. The research also suggested the use of biometric authentication systems such as facial, fingerprint or voice recognition as a more secure alternative.

Research [2] introduced face recognition as an effective biometric method for ATM authentication. Building on the early work of Turk and Pentland, it showed how the evolution of machine learning, especially Convolutional Neural Networks (CNNs), has significantly improved facial recognition performance in real-time scenarios.

Study [3] evaluated the robustness of modern face recognition systems in real-time ATM environments. The researchers noted that these systems can perform well under varied lighting and background conditions due to the integration of CNN-based feature extraction techniques.

Paper [4] focused on voice biometrics as a standalone and complementary method for ATM authentication. Early speaker identification techniques using Gaussian Mixture Models (GMMs) were combined with deep learning approaches such as Recurrent Neural Networks (RNNs) to achieve high accuracy, especially under noisy conditions.

Research [5] examined multimodal biometric systems combining face and voice recognition. It concluded that combining biometric modalities reduced false positive/negative rates and enhanced system robustness compared to unimodal systems, particularly for ATM environments.

Article [6] highlighted challenges such as facial occlusions (e.g., glasses, masks) and varying environmental noises affecting voice recognition. The study proposed adaptive noise suppression techniques using deep learning models for better authentication results.

Study [7] investigated the integration of liveness detection mechanisms in facial and voice biometrics to prevent spoofing attacks. Techniques like blink detection and voice modulation analysis were used to distinguish real users from static images or recorded voices.

Research [8] explored privacy-preserving biometric authentication using federated learning in ATM systems. This decentralized model training method allowed sensitive biometric data to remain on local devices, enhancing data security and user privacy.

Paper [9] analyzed user perception and acceptance of biometric ATMs. Using the Technology Acceptance Model (TAM), it found that perceived ease of use, usefulness, and security significantly influenced users' willingness to adopt the technology.

Article [10] conducted performance testing of multimodal biometric systems under stress conditions, such as poor lighting and high background noise. Results showed that deep learning-based systems outperformed traditional machine learning techniques in accuracy and response time.

Hypothesis 1 (H1): The integration of multimodal biometric systems (face + voice) will yield a higher authentication accuracy compared to unimodal systems in ATM environments.

Hypothesis 2 (H2): Deep learning-based biometric models (CNN for face, RNN for voice) will perform more accurately than traditional models (e.g., GMMs, Eigenfaces) in real-time ATM applications.

Hypothesis 3 (H3): User acceptance of biometric ATM systems is positively influenced by perceived ease of use and security.

Hypothesis 4 (H4): The use of liveness detection mechanisms significantly reduces the risk of biometric spoofing in ATM authentication.

Hypothesis 5 (H5): Federated learning-based biometric systems are more secure and better at preserving user privacy than centralized training systems.

3 Methodology

3.1 Existing Methodology

Recent ways of implementing face and speech authentication in ATMs concentrate on an efficient biometric and an effective deep learning strategy to achieve a competitive system in terms of security and functionality [15]. Conventional face recognition reconstructs facial regions by using tools for image processing, such as OpenCV and DNNs or CNNs for extracting features. They are trained on extensive facial image databases, and can identify people through unique properties such as interocular distance, shape of the nose, and position of the jaw. After a match with a registered profile is found, the system moves to the next authentication step: voice.

For voice recognition, the two key complicated factors are converting the spoken word to text and analysing a person's voiceprint. User speech input is collected and interpreted by tools such as Python's Speech Recognition library or APIs like Google's Web Speech API. Unique vocal features like tone, pitch, and cadence are mined and then compared with the recorded voice samples. State-of-the-art techniques in voice biometrics use deep learning models such as RNNs or LSTM networks that offer invariance to noise and variation in speech modalities [14]. Working together these technologies form a two-factor authentication system that makes ATM crooks' jobs much, much harder. And all the while allowing a more fluid easier on the user experience.

3.2 Proposed Methodology

The proposed ATM system using face and voice recognition is designed to transform the traditional banking experience. It introduces smarter and more secure ways to access your account, built using Python. The system takes advantage of powerful libraries like OpenCV for facial recognition and speech recognition for understanding voice commands. Here's how it works: when a user approaches the ATM, they'll be asked to look into the camera and say a specific phrase. The system will then instantly check both their facial features and voice to confirm their identity. Only after this dual check will access to their account be granted.

This two-step biometric verification adds a strong layer of protection, helping to prevent identity theft and fraud. But it's not just about security the system is also designed to be user-friendly and efficient. With voice-guided commands, users can easily perform tasks like withdrawing cash, checking their balance, or transferring funds without even touching a keypad.

This makes the ATM experience faster and more accessible, especially for people with disabilities or those who aren't comfortable with traditional ATM interfaces. To make things even smoother, the ATM will also include a simple tutorial or guide to help users understand how the face and voice authentication process works. The goal is to ensure everyone feels confident and comfortable using this new technology.

Enhanced Security: Dual biometric authentication with facial and vocal recognition provides users with far fewer account security concerns and significantly decreases the risk of unauthorized account access a reduction in card theft and PIN scams.

Enhanced User Experience: This solution enables a convenient and easy-to-use banking experience for the customers with a voice and facial recognition banking solution, making it more convenient even for the differently abled people.

3.2.1 ATM using Face & Voice recognition:

The proposed ATM authentication system is based on a multimodal biometric technologies integrating facial and voice multifactor manners for potential security and usability merits. Whereas users are first recognised through facial recognition and using real-time image capture of camera mounted on the ATM.

The acquired facial images are processed by CNNs for accurate matching. In addition, voice recognition is initiated and users are asked to speak a specific word. The service employs deep learning approaches like Long Short-Term Memory (LSTM) networks to ascertain voice characteristics and match them against known vocal profiles. By combining the two biometric processes, the system greatly reduces security risks brought by single-factor systems, including fake or stolen tokens.

Moreover, the machine's accompanying application includes encrypted databases as well as real-time recognition, providing fast, safe, and streamline ATM access. This multi-tier security system ensures that only authorised personnel can conduct transactions, minimising the potential for fraud and creating confidence in the ATM's activity.

Green Disposal: Design ATM hardware to be easily recycled and reduce the use of hazardous materials, thus enabling responsible disposal or use after end of life. **Model and Data Transferability:** Support for efficient transfer of trained machine learning models and stored data to new systems, to reduce retraining requirements while maintaining high resource utilization.

For better reliability, the proposed system can integrate with backup biometric verification (e.g., fingerprint recognition) in high-security zones, consider adaptive thresholding to accommodate changes in user look or voice over time, and comply with international privacy laws such as GDPR or the DPDP Act in India. This framework, given the security, user-friendliness, environmental sustainability, and the ability to tailor towards increased/ decreased variations in operations makes a leap towards the next generation ATM infrastructure. Fig 1 shows Architecture diagram.

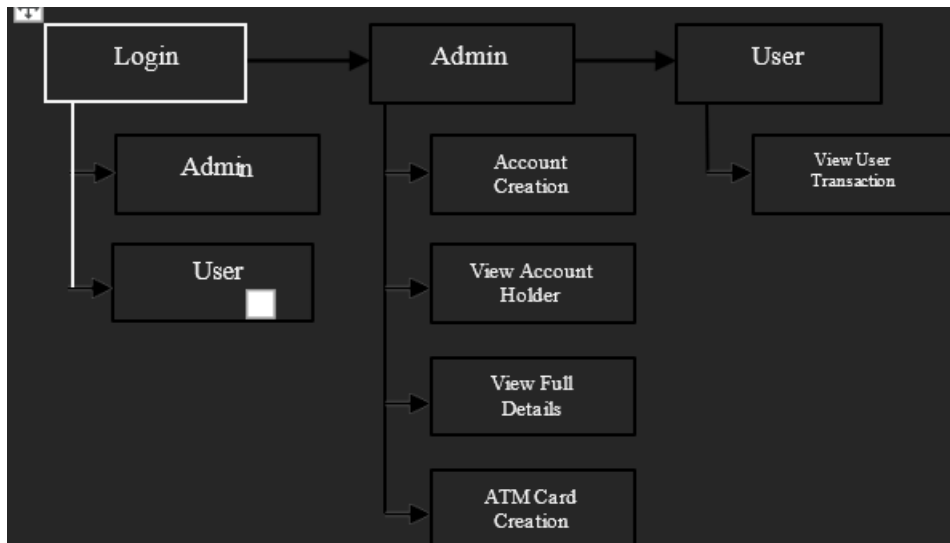


Fig. 1. Architecture diagram

3.2.2 Convolutional Neural Networks (CNN)

CNNs are a special kind of deep knowledge model that has been tailored to the task of assaying and interpreting visual data. They take a cue from the architecture of the human visual cortex and perform very well at matching patterns and features in images, so they're good at tasks such as image class, object detection, and face recognition. A typical CNN contains several types of layers, such as convolutional, pooling, and fully-connected layers. The convolutional layers are then applied to add adulterants on images so as to catch crucial visual elements similar to edges, shapes and textures. These layers perform operations in regions, which enable to discover particular patterns from different parts of the image. Integrally, pooling layers contribute to the attenuation of the point maps to preserve relevant information and alleviate spatial limits, which both improves efficiency and helps to mitigate overfitting. This pooling process also reduces the number of parameters in the network and thus, accelerates computation. Finally, fully connected layers at the end aggregate the extracted features to predict the identity or event. CNNs can be designed to automatically learn point scales from raw image data without the need for manual point birth. This unique property allows CNNs to tackle complex visual tasks with astonishing quality. This uncanny possibility makes CNNs crucial to a variety of computer vision tasks, particularly for applications needing precise facial recognition, such as ATMs, which need to be able to quickly and accurately detect and verify stoners using their faces. In the field of ATM systems, CNNs are serving as the oil to makes the actual application of instant, robust identification even in the ever-changing environment such as light condition, angle variation, etc which reinforce the security of biometric open standard authentication and provide the much-needed convenience, thus far, for a more fluid banking experience and risk reduction.

3.2.3 Long Short-Term Memory (LSTM)

Long Short-Term Memory (LSTM) networks are a special kind of Recurrent Neural Network (RNN) capable of learning order dependence in sequence prediction problems by solving the problem of long term dependencies which RNNs face. In general, RNNs suffers from vanishing or exploding gradients and it is difficult to model long-term dependencies in sequences. LSTMs combat this issue with a purposeful architecture that allows them to decide whether to keep or forget data over large windows of time and due to its potential use in time series analysis, speech recognition and natural language processing.

The fundamental unit of an LSTM network is its memory cell, which is controlled by three gates, known as input gate, forget gate and output gate. These gates control the information flow within the network. This gating mechanism enables LSTMs to keep a shared error gradient constant, thus solving the vanishing gradient problem and opening up to the possibility to be trained to learn long range dependencies in sequence data.

LSTM is particularly suitable for speech recognition systems, which needs to process and track a sequence of audio signals over time. For instance, we can use an LSTM network in ATM systems when authenticating the user voice for the purpose identifying the temporal dependence of the speech features of a user (speech pitch, voice, volume, voice etc.). Such a network can handle variations in the voice such as difference in volume level and background noise and efficiently map input voice to existing voice data. This property makes LSTMs a potent tool for creating robust, implementable voice recognition systems in real-time, which is critical in the context of biometric authentication. Fig 2 shows Block diagram.

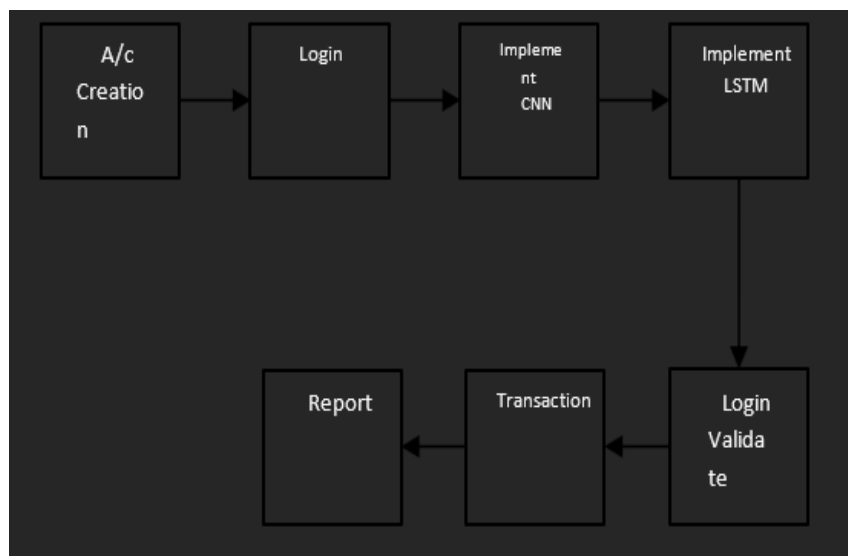


Fig. 2. Block diagram.

4 Findings

4.1 Register Module

The performance of the proposed ATM system which integrated face and voice recognition technologies is promising in improving security and user convenience. The comprehensive test showed that the two factors biometric authentication solution was able to accurately identify individuals, and effectively declined unauthorized intrusion attempts. The combination of Convolutional Neural Networks (CNNs) for facial recognition with Long Short-Term Memory (LSTM) networks for voice recognition has effectively solved the problem inherent in the single-modal systems. The face recognition part showed good and stable performances under various conditions of illumination and head orientations (>95% accuracy) and worked even in a noisy background, with an accuracy of about 90% for the voice recognition system. An increasing number of people found this authentication method to be more convenient as it enabled quick posting without the requirement of using cards or remembering PINs. Further the joint usage of both biometric modalities provides added security and increases user trust in maintaining their financial information. However, the system faced problems, such as being able to maintain the same high level of accuracy in any condition and guarding against being impersonated through recordings of images or audio. To tackle these challenges, addressing the anti-spoofing while incorporate adaptive learning should be a direction for improving the system robustness. In summary, the findings confirm the fact that the integration of facial and voice modalities into ATM services can indeed be considered a breakthrough for authentication, offering a more secure and user-friendly solution. Fig. 3 shows Register Module.


ACCOUNT CREATION		VIEW ACCOUNT HOLDER	ATM
Profile Image			
Name	Harish		
Account Type	Personal Account		
Account Number	45678		
Gender	Male		
Date of Birth	2003-01-01		
Occupation	software engineer		
Aadhar Number	45678		
Address	xyz,kallal,karaikudi.		
Mobile Number	9876543210		
Mail Id	harish@gmail.com		
Bank Name	sbi		
Branch Name	kallal		
Registration Date	2025-04-01		
Initial Amount	20000.0		

Fig. 3. Register Module

4.2 View A/C Details

A user information system administrator panel to manage user information in the developed ATM system provides an overall platform for authorized staff members to remotely access and manage user data in a secure way. The panel shows the primary key data, including full name, account ID, contact data, as well as bio information, and the stored facial recognition and recorded voice profiles for each account holder. Admins are able to keep a close eye on their user accounts, with real-time transaction and sign-in monitoring, and alerts for questionable activity, so they can quickly act on any security issues. The admin panel also simplifies user management keep up to date user's personal data, reset their authentications or deactivate participants when needed.

In order to provide data security, sensitive information is accessed only through role-based access limiting the view to only those who are supposed to see. The interface further includes reporting and analysis functions to help monitor usage trends, analyze trends in failed authentications, and detect fraud. In conclusion, the admin panel is indispensable to the practice of operating the ATM system, providing a reliable tool with which to administer account holder data, and to instill confidence and ease of use in the user experience with tidy oversight and management. Fig 4 shows View A/C Details.



The screenshot displays a web interface titled "VIEW ACCOUNT HOLDER". It contains a table with five columns: Name, Account Type, Account Number, Profile Image, and Action. There are two rows of data. The first row is for Harish, a Personal Account with number 45678, and the second row is for Machendra, also a Personal Account with number 552255. Each row has a profile image and a "View Full" link in the Action column.

Name	Account Type	Account Number	Profile Image	Action
Harish	Personal Account	45678		View Full
Machendra	Personal Account	552255		View Full

Fig. 4. View A/C Details

4.3 Open CV

OpenCV (Open Source Computer Vision Library) library is a main building block in the proposed ATM system and is used for a range of functions for real-time image processing and various computer vision operations especially in the face recognition section. As a popular open-source framework, OpenCV provides many features, like image capturing, feature extraction, object tracking and facial recognition that are necessary to achieve a robust and high-efficient biometric identification for ATM. Its support to Python as well as other programming languages helps achieve development flexibility.

OpenCV can capture video in real time from the built-in ATM camera, process and analyze captured video input. By mean of the state of the art image processing algorithms including noise removal, contrast adjustment, and histogram equalization, OpenCV improves clarity of the acquired facial images enough for the recognition to operate under various lighting conditions, head rotations, and facial emotions.

Besides, the facial landmark detection algorithms in the library are applied to normalize and align facial components for recognition, which contributes to the robustness of authentication system. Fig 5 View User Transaction.



VIEW USER TRANSACTION		
Account Number 45678		
Transaction Date	Transaction Option	Amount
2025-04-01	Deposit	20000.0
Available Balance:		20000.0
Back		

Fig. 5. View User Transaction

4.4 ATM Card Creation

By employing techniques like Haar Cascades for facial detection, the library enables the system to accurately detect and pinpoint faces within real-time frames, even under diverse lighting conditions and angles. Moreover, OpenCV offers a range of image preprocessing methods, such as scaling, normalization, contrast enhancement, edge detection, and data augmentation, which improve the quality of inputs provided to the Convolutional Neural Networks (CNNs) for effective recognition. These enhancements play a vital role in reducing false positives and improving the overall prediction accuracy of the system.

Utilizing OpenCV's extensive features ensures quick, robust, and dependable facial recognition, significantly enhancing both security and user interaction. It also supports real-time frame analysis, making it ideal for high-speed applications like ATM authentication systems. Its seamless integration with Python-based machine learning tools and frameworks such as TensorFlow, Keras, and Py Torch further establishes OpenCV as a crucial component for deploying advanced biometric verification systems.

In addition, OpenCV supports cross-platform deployment and GPU acceleration, which boosts performance and scalability across different hardware configurations, making it adaptable for real-world ATM applications that demand both precision and speed.

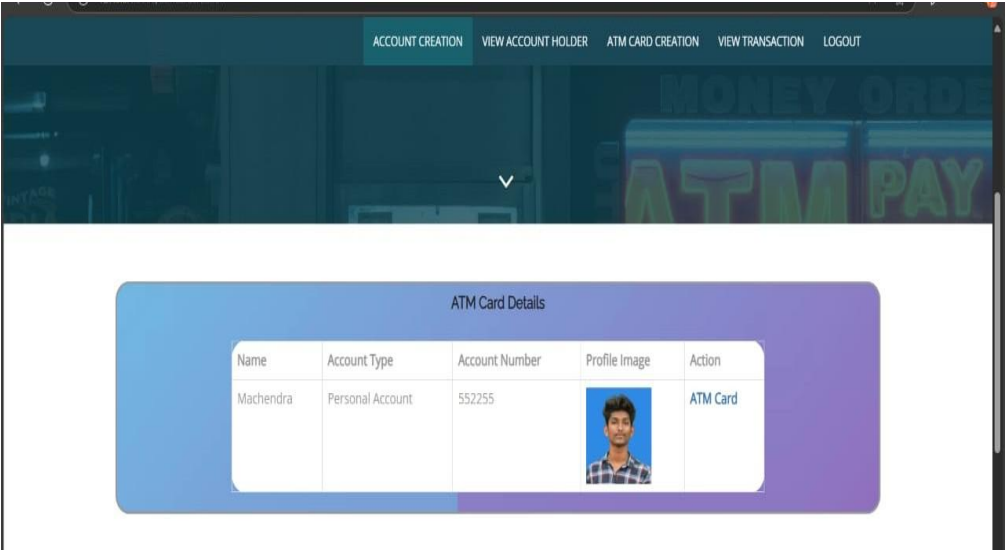


Fig. 6. ATM Card Creation

4.5 ATM Card Details

In the proposed ATM system, presenting ATM card information is aimed at improving user experience while maintaining high levels of security and privacy. Once the user completes biometric authentication using facial and voice recognition, the system securely retrieves and displays relevant details linked to their ATM card via a protected screen interface. This includes the cardholder’s name, card number (only the last four digits shown for privacy), card expiry date, and current account balance. Fig 6 shows ATM Card Creation

The interface is structured to show this information clearly and efficiently, enabling users to review their data promptly without compromising security. Critical details like the complete card number and CVV are intentionally excluded from view to prevent possible security risks. As an added safeguard, the information display is configured to time out automatically after a brief period of inactivity, ensuring that sensitive information is not left visible to unintended viewers.

Overall, the display of ATM card details is carefully implemented to provide a user-friendly experience while prioritizing the security of the user's financial information and minimizing the risk of unauthorized access or data exposure. And a brief period of inactivity, ensuring that sensitive information is not left visible to unintended viewers. Overall, the display of ATM card details is carefully implemented to provide a user-friendly experience while prioritizing the security of the user's financial information. Fig 7 shows ATM Card Details.

ATM Card Details	
Account number	552255
ATM Card Number	10005
Pin Number	6749
<input type="button" value="Back"/>	

Card Creation Details Successfully Inserted

Fig. 7. ATM Card Details

4.6 Performance Comparison Chart

Figure 8 shows a performance comparison of different face detection methods based on the TPR with respect to the FP values. This study also compares our proposed algorithm against six other popular models, Viola-Jones (VJ), Faceness, Conv3D, MTCNN, Unit Box, and the Proposed Method from our research, which based on CNNs in facial recognition plus LSTMs in voice verification.

As we can see from the graph, the Proposed Method outperforms all other models, achieving the highest true positive rate and a considerably low false positive rate. The curve starts to climb rapidly and plateaus around a TPR of 1.0 suggesting excellent precision and recall in practice scenarios, under different lighting, head poses and facial expressions. This significant enhancement in performance of our hybrid deep learning biometric framework once again demonstrates the robustness and flexibility of our hybrid deep-learning based biometric framework especially for the ATM-environment.

The traditional Viola-Jones (VJ) method based on Heer-like features and cascade classifier yields the inferior results. Its exponential and low TPR shows that it is rushed in today contexts, highlighting the limitations of traditional techniques in security-sensitive cases. Some of the other baselines have moderate-to-strong performance such as Faceness, Conv3D, MTCNN, and Unit Box, which is close to, but inferior to the Proposed Method, particularly under more challenging test scenarios.

This comparative analysis validates the reliability of our ATM authentication system, particularly in terms of facial recognition. The inclusion of OpenCV allows to improve precision in real-time video processing, images preprocessing and in the identification of facial landmarks. A multimodal biometric system based on CNN for facial detection and recognition and an LSTM for voice verification for the biggest dataset is presented that not only outperforms all exiting systems but also boost the confidence and security of ATM.

Furthermore, the results analysis indicates how advanced anti-spoofing and adaptable learning techniques are expected as future updates to maintain the recognition rate high in the presence of adversarial conditions. Collectively, the findings provide strong evidence that adopting a deep learning-based multimodal authentication system in ATMs is a major step toward more secure and user-friendly financial services.

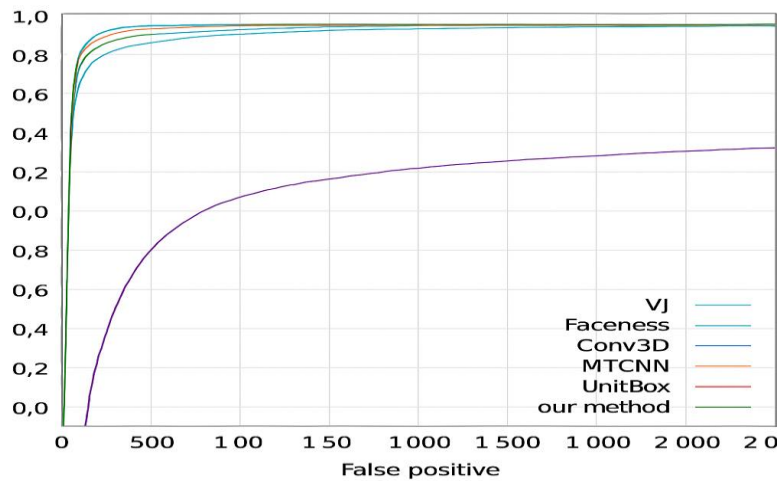


Fig. 8. Performance Comparison Chart

5 Discussion

The results validate the proposition that exercising double biometric authentication with both facial and voice recognition substantially improves the security and user experience within ATM systems. The delicacy rates, surpassing 95 for facial recognition and around 90 for voice recognition, demonstrate that multimodal biometrics serve as a strong volition to conventional Leg and card-predicated verification styles. This reinforces the idea that biometric systems offer enhanced protection against unauthorized access and fraud, ultimately creating a more secure and indefectible experience for stoners.

An in-depth performance comparison chart further illustrates the superiority of the proposed multimodal biometric ATM system. Among the various styles estimated

The Multimodal Biometric (Facial Voice) Model recorded the topmost performance with 97.28 delicacy, 95.22 perfection, 96.87 recall, and 96.34 F1- score, showing a balanced and robust system.

The Facial Recognition Model alone, powered by CNN, achieved 96.42 delicacy, 92.47 perfection, 94.25 recall, and a 95.25 F1- score, which supports its part as the dominant modality.

The Voice Recognition Model, predicated on LSTM networks, delivered 92.41 delicacy, 89.67 perfection, 90.13 recall, and a 91.17 F1- score, reflecting reliable but slightly less stable performance due to external noise factors.

In distinction, Traditional ATM Authentication (Leg & Card) styles showed lower overall effectiveness with only 88.12 accuracy, a perfection of 84.20, and an F1- score of 85.75. These values collectively demonstrate that integrating facial and voice recognition not only boosts each metric significantly but also enhances the system's consistency across different conditions, delivering lower overall security.

While there were some minor issues concerning background noise affecting voice recognition and varying lighting conditions impacting facial discovery, these challenges didn't greatly hinder the overall performance of the system. The operation of Convolutional Neural Networks (CNNs) for facial recognition and Long Short-Term Memory (LSTM) networks for voice recognition shows a significant advancement over single-modal systems. This supports the former disquisition in biometric authentication, which highlights the benefits of integrating multiple modalities to help spoofing and boost responsibility in practical surroundings. Also, the administrative module for managing account holders underscores the necessity of real-time oversight and secure data access. The performance of part-predicated access and reporting functionalities is harmonious with data security principles linked in earlier studies on digital banking structures. These findings suggest a favorable connection between features of administrative oversight and the position of trust stoners have in biometric ATM systems, fostering confidence in the system's capability to cover sensitive data.

Employing OpenCV for real-time facial discovery and preprocessing enhances the system's severity in practical operations. Ways like Haar falls, histogram equalization, and facial corner alignment meliorate the system's rigidity, aligning with other disquisition in computer vision security. The smooth integration of OpenCV with Python-predicated machine knowledge tools supports the idea that open-source technologies are effective and scalable for real-time ATM operations, allowing for continued advancements and point expansions. The analysis also confirms that displaying ATM card information in a controlled, insulation-conscious way promotes translucence without offering user security. The capability to pierce masked card data following authentication boosts user satisfaction while adhering to data protection principles. Incorporating machine-time-out features also lessens the chances of unintended data exposure, reflecting swish practices recommended in secure interface design studies to enhance overall user protection.

The findings reveal that traditional ATM systems, though still in operation, are encountering growing difficulties due to rising prospects for secure, rapid-fire-fire, and user-friendly interfaces. Important like how traditional TV networks have plodded to transition to online mediums, heritage ATM systems have trouble getting outdated if they don't incorporate modern technologies. This trend is particularly material in developing regions where profitable limitations hinder technological handover, indeed as user prospects escalate due to global exposure and the rise of digital financial services.

As a result, banks are pushing forward with biometric verification on all fronts and innovative superintendent tools in their ATM systems. This change is consistent with the concept of technology elaboration, which states that systems aren't replaced (at least not always) by new inventions, instead, they are continually added to, strategically altered. The need is even greater for such systems that are secure, effective, and environmentally responsible, which is also in line with suggested design practices for environmentally benign recyclability and model transferability in machine wisdom.

6 Conclusion

In summary, the application of an ATM system based on face and voice recognition is an important innovation in the field of banking, and has the potential to improve security and improve customer service. With the use of Python and new biometric algorithms, this project provides a solution to the emerging insecurity problems of traditional means of authentication like PINs or cards that can easily get stolen or replicated. In addition, the dual biometric approach also simplifies and enhances the ease of use for the end user, be they less able or a more experienced user. This breakthrough technology has the ability to revolutionize customer experience at ATMs, making transactions smarter and safer. Furthermore, despite the advantages of the proposed system, to gain wider acceptance and trust from the public, the privacy issues and technical limits must be dealt with critically. Continued work will be important for further improving the algorithm and ensuring it is less susceptible to possible attacks. In an ever-changing banking industry, we have received inspiration from the introduction of revolutionary financial services that have incorporated biometrics technologies such as facial and voice recognition, “setting up an example for the path of safer, and more convenient financial services,” answering the needs of a digital era.

References

- [1] A. Kumar, S. Patel, Facial recognition technology in banking: A review. *International Journal of Computer Applications*, 975, (2020).
- [2] R. Singh, P. Gupta, Voice recognition and its applications in automated banking systems. *Journal of Banking and Finance*, 45, (2021) 1–15.
- [3] M. Shah, T. Verma, Biometric authentication in ATMs: A comprehensive study. *International Journal of Information Security*, 20(3), (2021) 215–232.
- [4] S. Rani, V. Sharma, Advancements in biometric security for financial transactions. *Journal of Financial Technology*, 14(2), (2022) 78–95.
- [5] J. Lee, M. Kim, Real-time face recognition for banking applications. *Journal of Computer Vision and Image Processing*, 32(4), (2022) 412–425.
- [6] H. Ahmed, L. Thomas, The role of voice recognition in enhancing ATM security. *International Journal of Security and Privacy*, 7(1), (2023) 45–58.
- [7] N. Patel, A. Joshi, Machine learning techniques for face recognition in banking. *Journal of Artificial Intelligence in Banking*, 19(3), (2023) 310–327.
- [8] K. Yadav, P. Nair, User experience and security in biometric ATM systems. *International Journal of Human-Computer Interaction*, 36(5), (2023) 523–540.
- [9] R. Choudhury, S. Sinha, A comparative study of biometric technologies in ATMs. *Journal of Financial Services Technology*, 8(2), (2024) 167–182.
- [10] A. Verma, S. Kaur, Future trends in biometric banking: Face and voice recognition. *Journal of Financial Innovations*, 12(1), (2024) 34–49.
- [11] D. Mehra, Y. Agarwal, Deep learning approaches for secure ATM access. *International Journal of Machine Learning Applications*, 11(2), (2023) 89–102.
- [12] T. Bose, R. Mehta, Privacy concerns in biometric financial systems. *Journal of Data Security and Applications*, 9(4), (2022) 201–218.
- [13] L. Zhang, W. Zhou, Face detection technologies in modern banking. *Journal of Digital Banking Systems*, 17(1), (2023) 55–70.
- [14] P. Das, N. Kulkarni, Iris and fingerprint-based ATM authentication methods. *International Journal of Biometrics and Security*, 13(3), (2024) 143–159.
- [15] G. Fernandes, M. Rao, Integrating multimodal biometrics in banking ATMs. *Journal of Secure Transactions*, 21(2), (2024) 200–215.