IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 12, Issue 2, March-April 2025

Impact Factor: 8.152

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 2, March-April 2025 ||

DOI:10.15680/IJARETY.2025.1202047

Enhancing ATM Security Through Biometric Face Recognition

Kunaparaju Venkata Jhansi Rani[1], Kalla Malavika[2], Mattey Prashanthi[3], Jonuboyina Siva Venkata Nagaraju[4], Ande Satyanarayana[5]

Associate Professor, Department of CSE, Eluru College of Engineering & Technology, Eluru, India[1]

B. Tech Student, Department of CSE, Eluru College of Engineering & Technology, Eluru, India[2,3,4,5]

ABSTRACT: Facial recognition systems are sophisticated computer applications designed to automatically identify or verify individuals using digital images or video frames. This paper proposes the integration of facial recognition technology as an authentication mechanism in Automated Teller Machines (ATMs). Facial recognition operates through two key processes: verification, which determines whether an individual matches the claimed identity, and identification, which ranks the individual against a database of faces. By leveraging convolutional neural networks (CNNs), this technology analyzes the unique structure, patterns, and positioning of facial features to ensure robust security.

The reliance on traditional ATM authentication methods such as physical cards and PIN codes has notable drawbacks. Users may misplace cards, forget PINs, or encounter damage to the cards, rendering access to funds challenging. To address these limitations, this study emphasizes biometrics, particularly facial recognition, as a superior alternative. By replacing cards and PINs with facial verification, the risk of unauthorized access by illegitimate users possessing valid credentials is minimized. Authentication is achieved by comparing the image captured at the ATM to those stored in a secure database, ensuring enhanced security and user convenience. This approach underscores the potential of biometrics in revolutionizing ATM systems for better accessibility and fraud prevention.

KEYWORDS: Face Recognition, Security, Biometric and ATM.

I. INTRODUCTION

The rise of technology in India has brought into force many types of equipment that aim at more customer satisfaction. ATM is one such machine which made money transactions easy for customers to bank. The other side of this improvement is the enhancement of the culprit's probability to get his 'unauthentic' share. Traditionally, security is handled by requiring the combination of a physical access card and a PIN or other password in order to access a customer's account. This model invites fraudulent attempts through stolen cards, badly-chosen or automatically assigned PINs, cards with little or no encryption schemes, employees with access to non-encrypted customer account information and other points of failure. Our paper proposes an automatic teller machine security model that would combine a physical access card, a PIN, and electronic facial recognition. By forcing the ATM to match a live image of a customer's face with an image stored in a bank database that is associated with the account number, the damage to be caused by stolen cards and PINs is effectively neutralized. Only when the PIN matches the account and the live image and stored image match would a user be considered fully verified. A system can examine just the eyes, or the eyes nose and mouth, or ears, nose, mouth and eyebrows, and so on. In this paper , we will also look into an automatic teller machine security model providing the customers a cardless, passwordfree way to get their money out of an ATM.

1.1 MOTIVATION

The motivation behind this study is to overcome the shortcomings of traditional ATM authentication methods, such as physical cards and PIN codes, which are vulnerable to loss, theft, and unauthorized access. Many users face challenges like forgetting PINs or misplacing cards, leading to inconvenience and security risks. By integrating facial recognition technology, this research aims to enhance ATM security and user convenience by leveraging biometrics for authentication. Convolutional neural networks (CNNs) enable precise facial verification, reducing the risk of fraud and unauthorized transactions. This approach underscores the potential of facial recognition to revolutionize banking security, offering a seamless Sand more secure alternative to conventional authentication methods.

1.2 PROBLEM DEFINITION

The problem addressed in this study is the vulnerability and inconvenience associated with traditional ATM authentication methods, which rely on physical cards and PIN codes. Users often face issues such as card loss, PIN theft, skimming attacks, and forgetting credentials, leading to security risks and access challenges. Fraudsters can exploit stolen cards and PINs to gain unauthorized access to bank accounts, posing a significant threat to financial security. Existing authentication systems lack robustness against such attacks, necessitating a more secure and user-friendly solution. This study proposes facial recognition technology as a biometric alternative to mitigate these risks by ensuring that only the rightful account holder can access ATM services, thereby enhancing security and convenience.

1.3 OBJECTIVE OF THE PROJECT

The objective of this study is to develop and integrate facial recognition technology as a secure and efficient authentication mechanism for Automated Teller Machines (ATMs). By replacing traditional card-based and PIN-based authentication with biometric verification, this approach aims to enhance security, reduce fraudulent activities, and improve user convenience. The study seeks to leverage convolutional neural networks (CNNs) to accurately analyze facial features, ensuring reliable identity verification. Additionally, it aims to eliminate risks associated with lost or stolen cards and forgotten PINs, providing a seamless and fraud-resistant banking experience. Ultimately, the goal is to modernize ATM security by implementing a robust, user-friendly biometric authentication system.

II. LITERATURE SURVEY

This chapter describes the research literature relevant to the primary aspects of this thesis. The core aspects of this thesis are deep learning applications to identify faces and classification techniques. Both these fields have received a lot of attention in the past years and there are a number of popular texts with relevant background material. As there is an enormous amount of literature available on both these aspects, these works can be described along several dimensions.

ATM SYSTEMS

Our ATM system would only attempt to match two (and later, a few) discrete images, searching through a large database of possible matching candidates would be unnecessary. The process would effectively become an exercise in pattern matching, which would not require a great deal of time. With appropriate lighting and robust learning software, slight variations could be accounted for in most cases. Further, a positive visual match would cause the live image to be stored in the database so that future transactions would have a broader base from which to compare if the original account image fails to provide a match – thereby decreasing false negatives. When a match is made with the PIN but not the images, the bank could limit transactions in a manner agreed upon by the customer when the account was opened, and could store the image of the user for later examination by bank officials. In regards to bank employees gaining access to customer PINs for use in fraudulent transactions, this system would likewise reduce that threat to exposure to the low limit imposed by the bank and agreed to by the customer on visually unverifiable transactions. In the case of credit card use at ATMs, such a verification system would not currently be feasible without creating an overhaul for the entire credit card issuing industry, but it is possible that positive results (read: significant fraud reduction) achieved by this system might motivate such an overhaul. The last consideration is that consumers may be wary of the privacy concerns raised by maintaining images of customers in a bank database, encrypted or otherwise, due to possible hacking attempts or employee misuse. However, one could argue that having the image compromised by a third party would have far less dire consequences than the account information itself. Furthermore, since nearly all ATMs videotape customers engaging in transactions, it is no broad leap to realize that banks already build an archive of their customer images, even if they are not necessarily grouped with account information. 4 HISTORY The first ATMs were off-line machines, meaning money was not automatically withdrawn from an account. The bank accounts were not (at that time) connected by a computer network to the ATM. Therefore, banks were at first very exclusive about who they gave ATM privileges to. Giving them only to credit card holders (credit cards were used before ATM cards) with good banking records. In modern ATMs, customers authenticate themselves by using a plastic card with a magnetic stripe, which encodes the customer's account number, and by entering a numeric passcode called a PIN (personal identification number), which in some cases may be changed using the machine. Typically, if the number is entered incorrectly several times in a row, most ATMs will retain the card as a security precaution to prevent an unauthorised user from working out the PIN by pure guesswork.

III. SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

Researchers also tried to use some other traditional methods like elastic graph matching, singular value decomposition for face recognition. Those methods were mostly tested on small data sets. Even in some cases the size of the data set was less than 100.

There are methods for detection purposes like PDA with an accuracy of 95.32 , REST with an accuracy of 93.4. Although these methods are used as detection algorithms, these methods have low accuracy to detect the faces.

3.1.1 DISADVANTAGES OF EXISTING SYSTEM

- Elastic Graph Matching can only be applied to objects with a common structure such as Faces in frontal pose, sharing a common set of landmarks like the tip of the nose.
- The Main disadvantage of Singular Value Decomposition is that it only makes use of a dataset.

3.2 PROPOSED SYSTEM

To overcome the disadvantage of existing system the proposed system came into the picture.The proposed system includes FACIAL IMAGE OF REGISTERED USER along with registered user,ATM card,PIN number,OTP,ATM .

Here the facial image of the user is stored in the database at the time of registration.So if any user want to withdraw amount from their account then that user must scan their face at the camera present at the ATM. Here OpenCV module is used to capture the image of the user and compare it with the registered image of the user.If both images are matched then the access will be granted else the access will be denied.

As we know that each and every person has unique iris,based on irises and other facial features the correct user get identified. This in turn enhances the confidentiality of ATM.

3.2.1 ADVANTAGES OF PROPOSED SYSTEM

- Enhanced Security – Facial recognition eliminates the risk of unauthorized access due to stolen cards or PIN theft, ensuring only the rightful user can access their account.
- Elimination of Card-Related Issues – Users no longer need to carry ATM cards, reducing the risks of card loss, damage, or skimming attacks.
- Fraud Prevention – The biometric-based system prevents identity fraud and unauthorized transactions, significantly reducing financial crimes like phishing and card cloning.
- User Convenience – Customers can access ATMs seamlessly without needing to remember PINs, making transactions faster and hassle-free.
- Non-Transferable Authentication – Unlike PINs, which can be shared or stolen, facial recognition ensures that authentication is strictly personal and non-transferable.
- Efficient Transaction Processing – Automated facial recognition speeds up the authentication process, reducing transaction time and improving overall efficiency.
- Reduced Maintenance Costs – The system minimizes reliance on physical cards and PIN reset services, lowering operational costs for banks.
- Integration with Other Security Features – Facial recognition can be combined with additional security layers like liveness detection and AI-driven fraud detection for even stronger protection.

3.3 MODULES

- DATA COLLECTION
- PREPROCESSING
- FACE DETECTION
- FACE ALIGNMENT
- FEATURE EXTRACTION
- FACE RECOGNITION
- POST PROCESSING

The face recognition process using OpenCV can be broken down into the following steps:

3.3.1 Data collection:

Collect a dataset of faces to be recognized, along with their corresponding labels. This dataset is used to train the face recognition model.

3.3.2 Preprocessing:
Preprocess the face images to standardize their size, orientation, and lighting conditions, as well as remove any noise or artifacts.

3.7.3 Face detection:
D3tect the faces in the input image using a face detection algorithm, such as Haar Cascades or HOG+SVM.

3.3.4 Face alignment:
Align the detected faces using landmarks or feature points, such as eyes, nose, and mouth, to ensure that they are in a consistent position and orientation.

3.3.5 Feature extraction:
Extract a set of discriminative features from the aligned face images, such as Local Binary Patterns (LBP), Histogram of Oriented Gradients (HOG), or Deep Convolutional Neural Networks (CNNs).

3.3.6 Face recognition:
Compare the extracted features of the input face with the features of the faces in the training dataset using a distance metric, such as Euclidean distance or Cosine similarity, to find the closest match.

3.3.7 Post-processing:
Apply post-processing techniques, such as thresholding or decision making based on majority voting, to refine the face recognition results.

IV. SYSTEMDESIGN

4.1 SYSTEM ARCHITECTURE

Below figure 1, depicts the whole system architecture of the work.

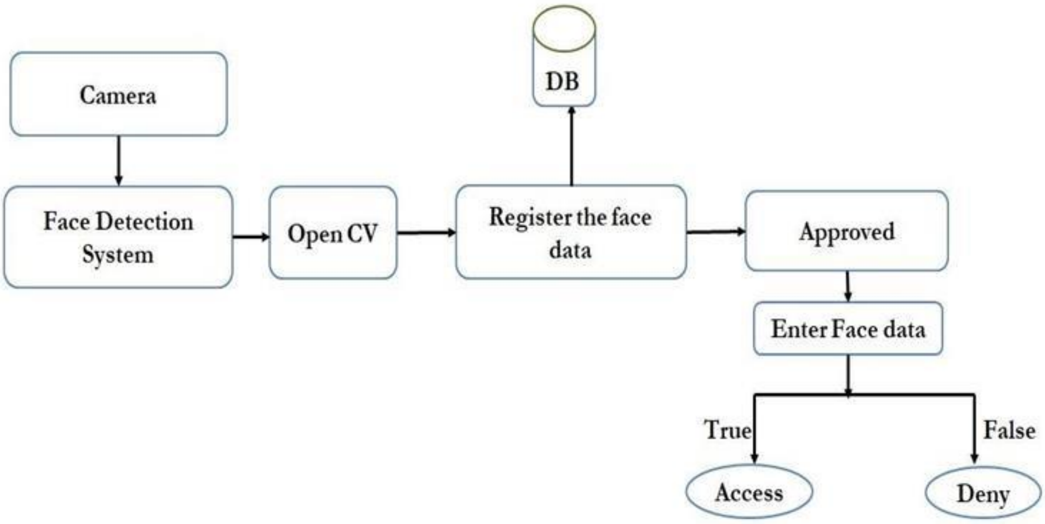


Fig 1: System Architecture

4.2 UML REPRESENTATION

GOALS:

1. Introduce Facial Recognition in ATMs – Clearly present the concept of integrating facial recognition as an authentication mechanism in Automated Teller Machines (ATMs).
2. Explain Key Processes – Outline the two main processes of facial recognition: verification (matching a claimed identity) and identification (comparing against a database).
3. Highlight the Role of CNNs – Emphasize how convolutional neural networks (CNNs) are used to analyze facial features for security.
4. Address Limitations of Traditional Methods – Explain the drawbacks of physical cards and PIN codes, such as loss, forgetfulness, or damage.
5. Justify Biometrics as a Superior Alternative – Argue that facial recognition reduces unauthorized access and enhances both security and convenience.
6. Describe the Authentication Process – Explain how ATM authentication is performed by comparing a captured

image with stored data.

7. Emphasize Security and Fraud Prevention – Highlight how biometric authentication improves accessibility and minimizes fraudulent activities.

4.3 ALGORITHMS

4.3.1 Convolutional Neural Netwoks

A Convolutional Neural Network (CNN) is a type of Deep Learning Neural Network architecture commonly used in Computer Vision. Computer vision is a field of Artificial Intelligence that enables a computer to understand and interpret the image or visual data.

When it comes to Machine Learning, Artificial Neural Networks perform really well. Neural Networks are used in various datasets like images, audio, and text. Different types of Neural Networks are used for different purposes, for example for predicting the sequence of words we use Recurrent Neural Netwoks more precisely an LSTM, similarly for image classification we use Convolution Neural networks. In this blog, we are going to build a basic building block for CNN.

Convolutional Neural Network (CNN) is the extended version of artificial neural networks (ANN) which is predominantly used to extract the feature from the grid-like matrix dataset. For example visual datasets like images or videos where data patterns play an extensive role.

4.3.2 CNN Architecture

Convolutional Neural Network consists of multiple layers like the input layer, Convolutional layer, Pooling layer, and fully connected layers.

The Convolutional layer applies filters to the input image to extract features, the Pooling layer downsamples the image to reduce computation, and the fully connected layer makes the final prediction. The network learns the optimal filters through backpropagation and gradient descent.

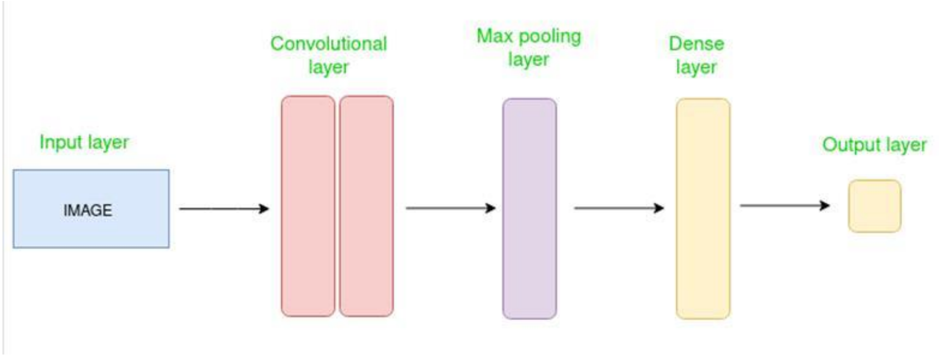


Fig 2: Simple CNN architecture

Layers Used to Build ConvNets

A complete Convolution Neural Networks architecture is also known as covnets. A covnets is a sequence of layers, and every layer transforms one volume to another through a differentiable function.

Types of layers: datasets

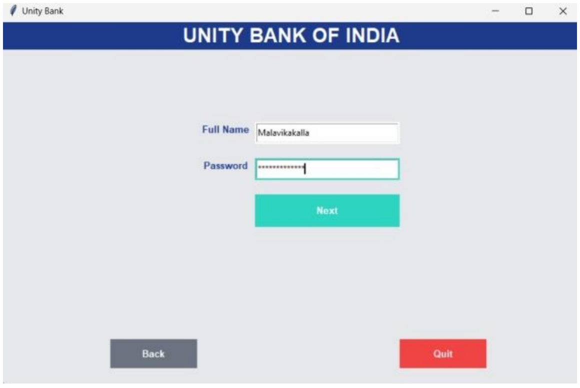
Let's take an example by running a covnets on of image of dimension 32 x 32 x 3.

- **Input Layers:** It's the layer in which we give input to our model. In CNN, Generally, the input will be an image or a sequence of images. This layer holds the raw input of the image with width 32, height 32, and depth 3.
- **Convolutional Layers:** This is the layer, which is used to extract the feature from the input dataset. It applies a set of learnable filters known as the kernels to the input images. The filters/kernels are smaller matrices usually 2×2, 3×3, or 5×5 shape. it slides over the input image data and computes the dot product between kernel weight and the corresponding input image patch. The output of this layer is referred as feature maps. Suppose we use a total of 12 filters for this layer we'll get an output volume of dimension 32 x 32 x 12.
- **Activation Layers:** By adding an activation function to the output of the preceding layer, activation layers add nonlinearity to the network. it will apply an element-wise activation function to the output of the convolution layer. Some common activation functions are **RELU**: max(0, x), **Tanh**, **Leaky RELU**, etc. The volume remains unchanged hence output volume will have dimensions 32 x 32 x 12.

- **Pooling Layer:** This layer is periodically inserted in the covnets and its main function is to reduce the size of volume which makes the computation fast reduces memory and also prevents overfitting. Two common types of pooling layers are **max pooling** and **average pooling**. If we use a max pool with 2 x 2 filters and stride 2, the resultant volume will be of dimension 16x16x12.
- **Flattening:** The resulting feature maps are flattened into a one-dimensional vector after the convolution and pooling layers so they can be passed into a completely linked layer for categorization or regression.
- **Fully Connected Layers:** It takes the input from the previous layer and computes the final classification or regression task.
- **Output Layer:** The output from the fully connected layers is then fed into a logistic function for classification tasks like sigmoid or softmax which converts the output of each class into the probability score of each class.

V. RESULTS

The following figures present the sequence of screenshots of the results.

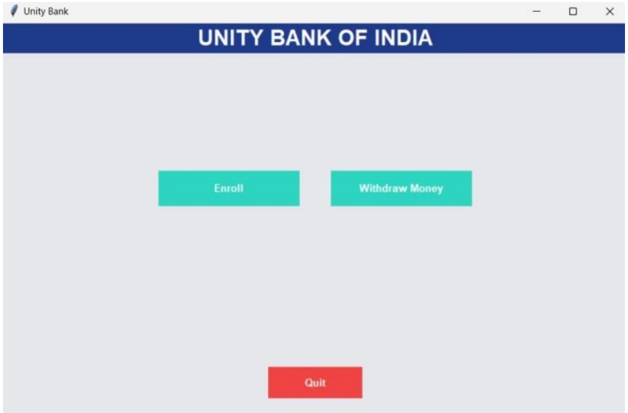


Full Name Malavikakalla

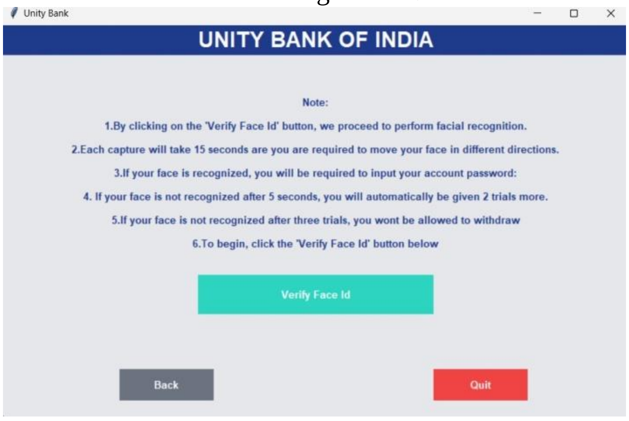
Password ••••••••••••

Enrollment

Face Id Registration.



Withdrawal of money



Note:

1.By clicking on the 'Verify Face Id' button, we proceed to perform facial recognition.

2.Each capture will take 15 seconds are you are required to move your face in different directions.

3.If your face is recognized, you will be required to input your account password:

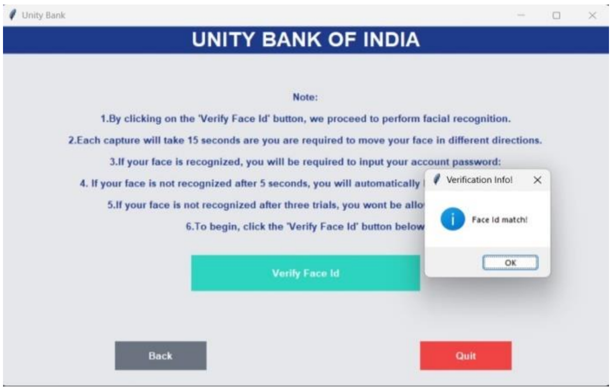
4. If your face is not recognized after 5 seconds, you will automatically be given 2 trials more.

5.If your face is not recognized after three trials, you wont be allowed to withdraw

6.To begin, click the 'Verify Face Id' button below

Face id verification

Face id verification



Note:

1.By clicking on the 'Verify Face Id' button, we proceed to perform facial recognition.

2.Each capture will take 15 seconds are you are required to move your face in different directions.

3.If your face is recognized, you will be required to input your account password:

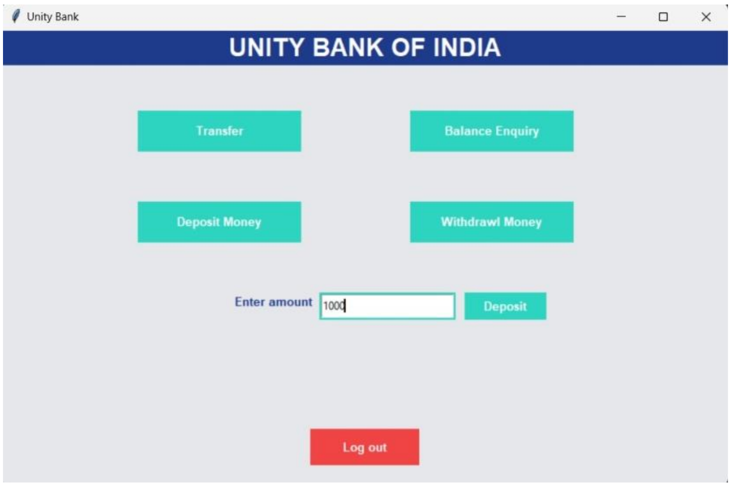
4. If your face is not recognized after 5 seconds, you will automatically

5.If your face is not recognized after three trials, you wont be allo

6.To begin, click the 'Verify Face Id' button below

Face Id match!

Face id verification success



Money withdraw success.

VI. CONCLUSIONS AND FUTURE WORK

6.1 CONCLUSIONS

The implementation of a facial recognition-based ATM system significantly enhances security and user convenience by eliminating the need for physical cards and PINs. Traditional ATM authentication methods are prone to risks such as card theft, skimming, PIN breaches, and fraud, making them vulnerable to unauthorized access. By leveraging facial recognition technology, this system ensures that only the rightful account holder can access their funds, reducing fraud and security threats. Additionally, the verification process is designed to be fast and efficient, ensuring minimal waiting time for users while maintaining high accuracy. A key advantage of this approach is that even if a user's image is compromised, the risk is significantly lower compared to losing direct access to their account credentials. Furthermore, since banks already archive ATM footage for security purposes, integrating facial recognition into authentication aligns with existing practices. Overall, this system has the potential to revolutionize ATM security, offering a seamless, fraud-resistant, and user-friendly banking experience.

6.2 FUTURE WORK

While facial recognition-based ATM authentication presents a promising advancement, further improvements can enhance its accuracy, security, and adaptability. Future developments can focus on improving recognition under challenging conditions, such as poor lighting, extreme facial angles, aging effects, and the use of accessories like masks or glasses. Integrating multi-factor authentication (MFA), such as combining facial recognition with fingerprint scanning, voice recognition, or behavioral biometrics, could further strengthen security. Another key area of enhancement is the use of AI-driven anti-spoofing techniques, which can detect and prevent fraudulent attempts using photos, videos, or 3D masks.

Additionally, exploring cloud-based biometric databases can improve scalability, efficiency, and real-time processing, enabling faster authentication across multiple ATM locations. Blockchain technology could also be considered for secure and tamper-proof storage of biometric data. Moreover, ensuring compliance with data privacy regulations such as GDPR and biometric security laws is crucial to gaining public trust and preventing biometric data breaches.

For widespread adoption, user education and awareness programs should be implemented to address privacy concerns and help users understand the security benefits of facial recognition. Future research can also explore cost-effective hardware solutions to make this technology affordable and accessible across different banking sectors worldwide. With continuous advancements, facial recognition-based ATMs can set a new benchmark for secure, convenient, and fraud-proof banking systems in the future.

REFERENCES

[1] All, Anne. "Triple DES dare you." ATM Marketplace.com. 19 Apr. 2002.

[2] Bone, Mike, Wayman, Dr. James L., and Blackburn, Duane. "Evaluating Facial Recognition

[3] Technology for Drug Control Applications." ONDCP International Counterdrug Technology Symposium: Facial Recognition Vendor Test. Department of Defense Counterdrug Technology Development Program Office, June 2001.

[4] Aragani, V.M.; Maroju, P.K. Future of Blue-Green Cities Emerging Trends and Innovations in ICloud Infrastructure. In Integrating Blue-Green Infrastructure into Urban Development; IGI Global: Hershey, PA, USA, 2024; pp. 223–244. [Google Scholar]

[5] Gross, Ralph, Shi, Jianbo, and Cohn, Jeffrey F. "Quo vadis Face Recognition." Third Workshop on Empirical Evaluation Methods in Computer Vision. Kauai: December 2001.

[6] Penev, Penio S., and Atick, Joseph J. "Local Feature Analysis: A General Statistical Theory for Object Representation." Network: Computation in Neural Systems, Vol. 7, No. 3, pp. 477-500,

[7] 1996. Wrolstad, Jay. "NCR To Deploy New Microsoft OS in ATMs." CRMDailyDotCom. 29 Nov. 2000.

IJARETY

INNO SPACE
SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर
NISCAIR

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com