Enhanced ATM security with the use of deep learning and image processing for facial recognition

Dr. Sara Ali[1], Mrs. Tasleem Sultana[2], Mrs. Matheen Sultana[3]

Professor[1], Assistant Professor[2,3]
Department of CSE
Global Institute of Engineering and Technology

Abstract:

It is possible to automatically identify or verify a person from a digital picture or a video frame using a face recognition system, which is a computer program. The proposed study demonstrates how to verify users in an ATM system using a facial recognition approach. There are two distinct kinds of comparisons used in facial recognition. Here, the system checks the user's claimed identity against their actual one and returns a yes/no answer; this is known as verification. Following this is identification, which entails the system comparing the supplied person to every other person in the database and providing a prioritized list of potential matches. The specific arrangement, shape, and pattern of a face's characteristics are studied by face recognition technologies. The majority of face recognition software uses Convolutional Neural Networks (CNNs), which is a pretty sophisticated piece of technology. People currently utilize automated teller machines quite a bit. However, customers may lose their ATM card or misplace their PIN since it is cumbersome to carry the card with them at all times. Users may find themselves in a predicament where they are unable to access their funds due to the ATM card being broken. Instead of PINs and ATM cards, our approach promotes the use of biometrics for authentication. Given that the integration of these biometrics yielded the most favorable results among the identification and verification methods, Face ID is given top attention in this regard. An concern that arises with the introduction of ATM machines is the possibility that unauthorized persons with valid authentication codes might access the devices. To ensure the security of the users, the photos taken in front of the ATM are compared to the ones already stored in the database.

I. Introduction

The proliferation of consumer-focused machinery in India is a direct result of the country's rapid technological development in recent decades. One such equipment that simplified banking for consumers is the automated teller machine (ATM). On the other hand, this augmentation increases the offender's chances of getting his "unauthentic" portion. A customer's account has traditionally been secured by requesting a combination of a physical access card and a PIN or other password. This strategy is vulnerable to fraud efforts due to a number of factors, including stolen cards, poorly selected or randomly allocated PINs, cards without encryption techniques, staff who have access to client account information that is not encrypted, and other points of failure. In this study, we provide a methodology for ATM security that integrates biometric authentication, PIN entry, and electronic face recognition. By implementing a system that requires the ATM to compare a customer's real-time facial picture with an image linked to their account number in a bank database, the potential harm caused by stolen PINs and cards is successfully mitigated. Full verification of a user is achieved when the PIN matches the account and the saved and live images match. Some systems can just look at the eyes, while others can scan the whole face (including the nose, ears, lips, and eyebrows). Also covered in this article is an ATM security model that allows users to withdraw funds without entering a PIN or card details.

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

Because our ATM system would only try to match two (and subsequently a handful of) separate photos, it would be pointless to search through a huge database of potential matching candidates. Pattern matching would essentially replace the procedure, and it wouldn't take long at all. Most examples might have minor differences explained with good illumination and powerful learning software. Also, if the live picture is a good match, it will be saved in the database. This way, if the original account image doesn't match, subsequent transactions may utilize a larger base to compare against, which will reduce the number of false negatives. If the PIN and picture don't match, the bank may still restrict transactions according to the terms agreed upon when the account was created, and they can save the picture for future reference. In addition to reducing the risk of bank workers obtaining client PINs for illegal purposes, this method would also make it harder for customers to consent to the low limit the bank has set for visually unverifiable transactions. Currently, the entire credit card issuing industry would need to be restructured in order to implement such a verification system for ATM credit card transactions. However, if this system were to produce positive results, such as a substantial decrease in fraud, it could inspire the industry to undergo this transformation. Finally, clients could be hesitant to have their pictures stored in a bank database, encrypted or not, because of privacy issues caused by potential hacking efforts or staff abuse. Having the picture stolen by an outsider would, perhaps, have much fewer serious repercussions than the account details itself. Also, it's not a huge stretch to assume that banks already have a database of client photos, even if they aren't labeled with account details, given that almost all ATMs record people doing transactions. 4.1 Background The first automated teller machines (ATMs) were offline, meaning that customers may manually withdraw funds from their accounts. Back then, there wasn't a network connecting the bank accounts to the ATM. As a result, banks initially very picky about who they allowed access to their ATMs. Only those with excellent credit histories who utilize credit cards (which were used before ATM cards) will be given them. Modern automated teller machines (ATMs) require users to input a numeric password known as a PIN (personal identification number), which may be altered in certain instances, and a plastic card with a magnetic stripe, which encodes the user's account number. As a security measure, most ATMs will keep the card if the PIN is input incorrectly many times in a row. This prevents unauthorized users from guessing the PIN.

III.SYSTEM ANALYSIS

1.1. 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.

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.

1.2. 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, ATM .

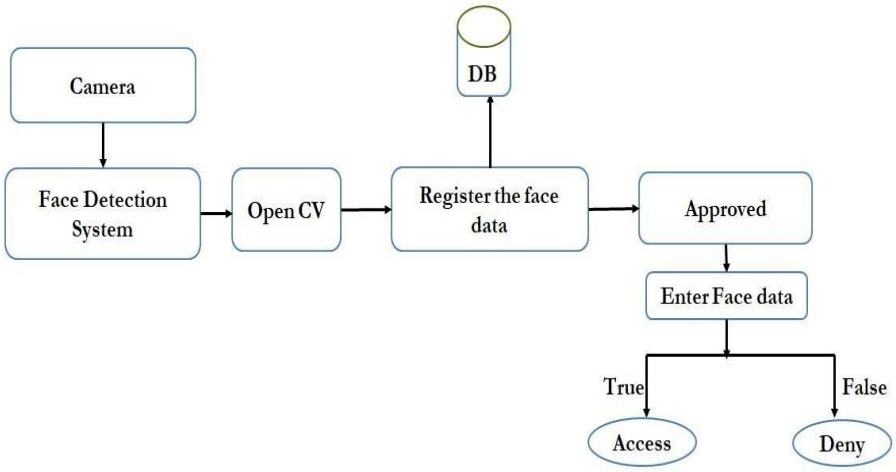
Here the facial image of the user is stored in the database at the time of registration. So if any user want to withdraw amount from their account then that user must scan their face at the camera present at the ATM. Here OpenCV module is used to capture the image of the user and compare it with the 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 gets identified. This in turn enhances the confidentiality of ATM.

IV.SYSTEM DESIGN

4.1 SYSTEM ARCHITECTURE

Below diagram depicts the whole system architecture.



4.1. System Architecture

V. SYSTEM IMPLEMENTATION

5.1. 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:

5.1.1 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.

5.1.2 Preprocessing:

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

5.1.3 Face detection:

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

5.1.4 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.

5.1.5 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).

5.1.6 Face recognition:

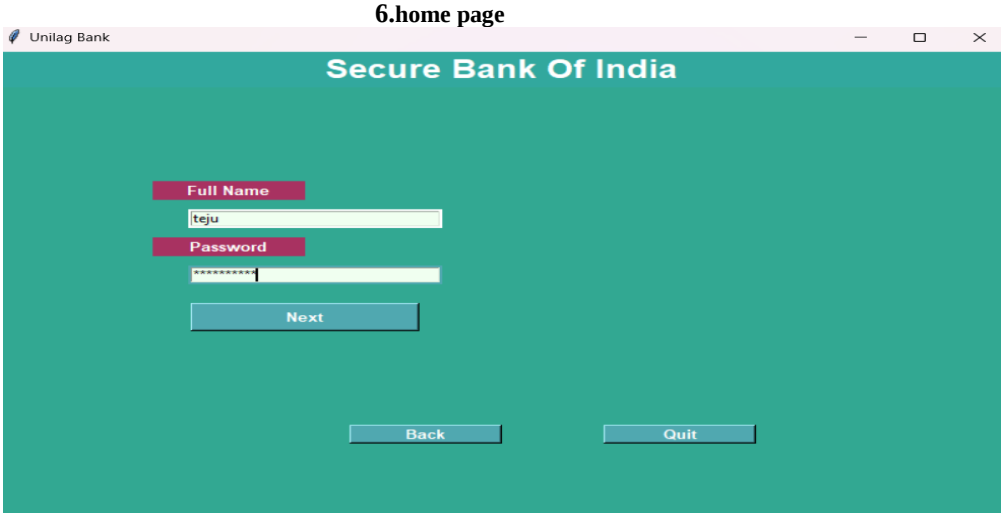
Compare the extracted features of the input face with the features of the faces in the training dataset using a distance metric, such as Euclidean distance or Cosine similarity, to find the closest match.

5.1.7 post-processing:

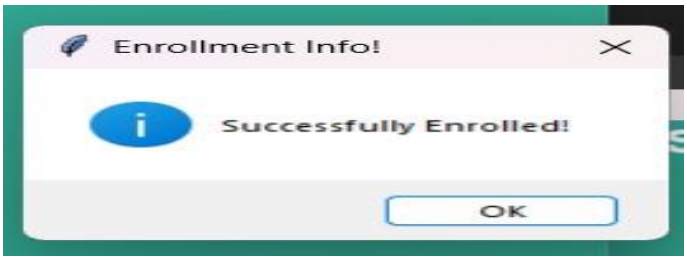
Apply post-processing techniques, such as thresholding or decision making based on majority voting, to refine the face recognition results.

VI. RESULTS

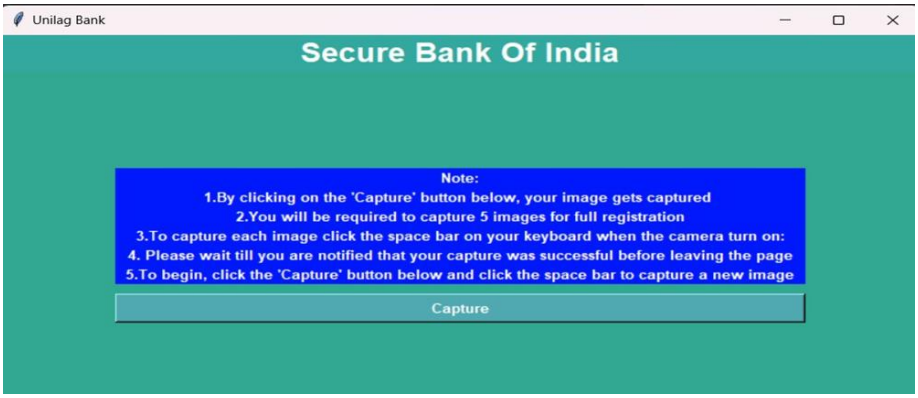
6.home page

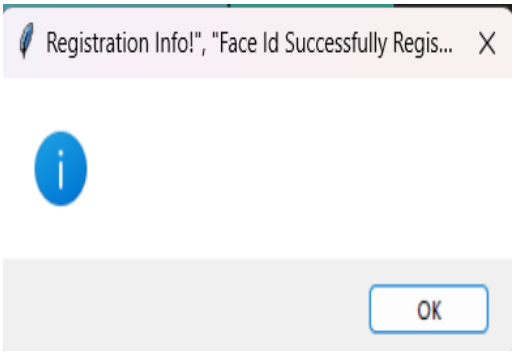


6.1 Login page



6.3 Enrollment





6.4 Image capture and register

6.5 After validation we can do money transactions

VII.CONCLUSION AND FUTURE WORK

We thus develop an ATM model that is more reliable in providing security by using facial recognition software. By keeping the time elapsed in the verification process to a negligible amount we even try to maintain the efficiency of this ATM system to a greater degree. 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.

REFERENCES :

1. 1. Anne, everyone. "Defy me with Triple DES." 21 Apr. 2002 ATM Marketplace.com.
2. 2. Mike Bone, Dr. James L. Wayman, and Duane Blackburn. "Facial Recognition Technology: A Review for Use in Drug Control" ONDCP International Symposium on Counterdrug Technology: Facial Recognition Vendor Evaluation. Counterdrug Technology Development Program Office, Department of Defense, June 2001.
3. Thirdly, Gross, Jianbo, and Cohn, Jeffrey F. are authors. "Face Recognition quarrels." This is the third workshop on computer vision empirical evaluation methods. Kauai: at the end of 2001.
4. In their paper titled "Local Feature Analysis: A General Statistical Theory for Object Representation," Penev and Atick discuss how to represent objects statistically. Volume 7, Issue 3, pages 477–500, 1996, Network: Computation in Neural Systems. A. Jay Wrolstad. "NCR To Install Microsoft's New Operating System in ATMs" CRMDaily. 202 November 29.