Journal of Science and Technology
ISSN: 2456-5660 Volume 8, Issue 04 (April -2023)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2023.v8.i04.pp46 - 52*

Deep Learning and image processing based ATM security and identifying the face

Mr. M. RAJA KUMAR, [1],Medavarapu Tejaswi [2],Kurukuri Haritha [3],Mothukuri Sunil [4],Vundavalli Sri Navya [5],Kolli Navadeep [6]
ASSOCIATE PROFESSOR
DEPT OF COMPUTER SCIENCE AND ENGINEERING
PRAGATI ENGINEERING COLLEGE(A),SURAMPALEM(EAST GODAVARI)A.P,INDIA

To Cite this Article
Mr. M. RAJA KUMAR, ,Medavarapu Tejaswi ,Kurukuri Haritha ,Mothukuri Sunil ,Vundavalli Sri Navya ,Kolli Navadeep **Deep Learning and image processing based ATM security and identifying the face** ” *Journal of Science and Technology, Vol. 08, Issue 04,-April 2023, pp46-52*

Article Info
Received: 19-02-2023 Revised: 2-03-2023 Accepted: 22-03-2023 Published: 16-04-2023

Abstract:

A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. Proposed paper uses face recognition technique for verification in ATM system. For face recognition, there are two types of comparisons. The first is verification, this is where the system compares the given individual with who that individual says they are and gives a yes or no decision. The next one is identification this is where the system compares the given individual to all the other individuals in the database and gives a ranked list of matches. Face recognition technology analyzes the unique shape, pattern and positioning of the facial features. Face recognition is very complex technology and is largely software based using Convolutional Neural network (CNN). Automated Teller Machines are widely used nowadays by people. But It’s hard to carry their ATM card everywhere, people may forget to have their ATM card or forget their PIN number. The ATM card may get damaged and users can have a situation where they can’t get access to their money. In our proposal, use of biometrics for authentication instead of PIN and ATM card is encouraged. Here, The Face ID is preferred to high priority, as the combination of these biometrics proved to be the best among the identification and verification techniques. The implementation of ATM machines comes with the issue of being accessed by illegitimate users with valid authentication code. The users are verified by comparing the image taken in front of the ATM machine, to the images which are present in the database.

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, password- free way to get their money out of an ATM.

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 unauthorized user from working out the PIN by pure guesswork.

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 .

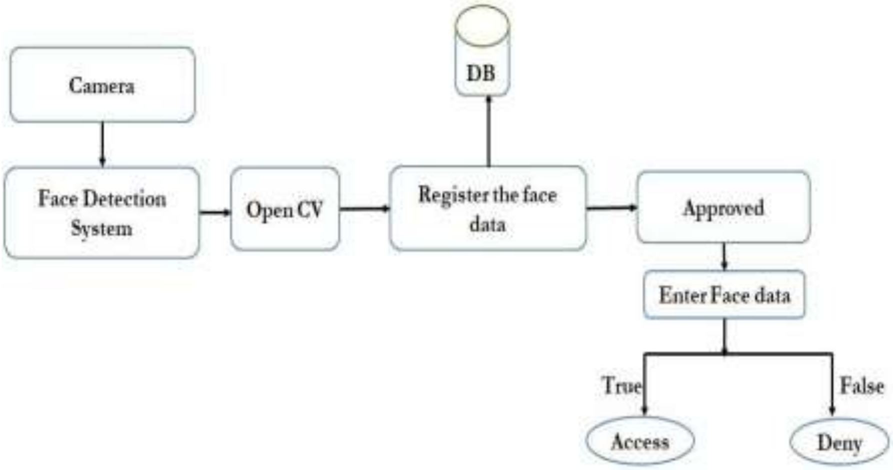
Here the facial image of the user is stored in the database at the time of registration. So if any user want to withdraw amount from their account then that user must scan their face at the camera present at the ATM. Here OpenCV module is used to capture the image of the user and compare it with the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

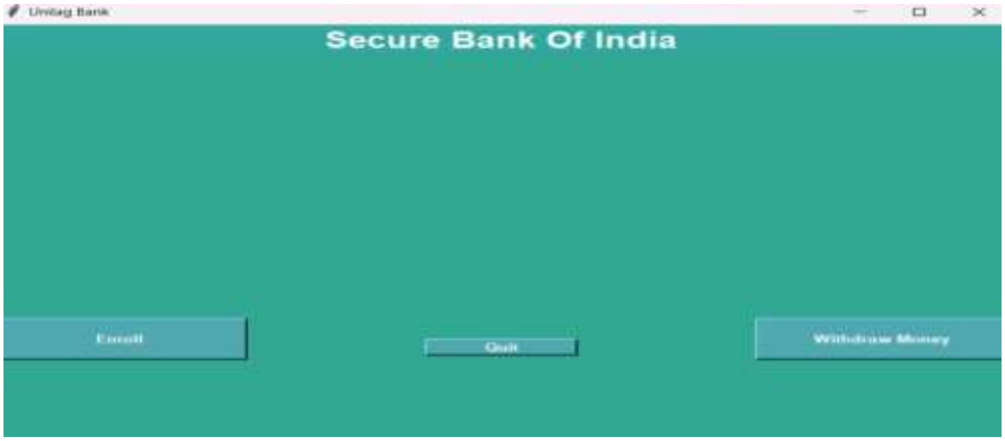
5.1.6 Face recognition:

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.

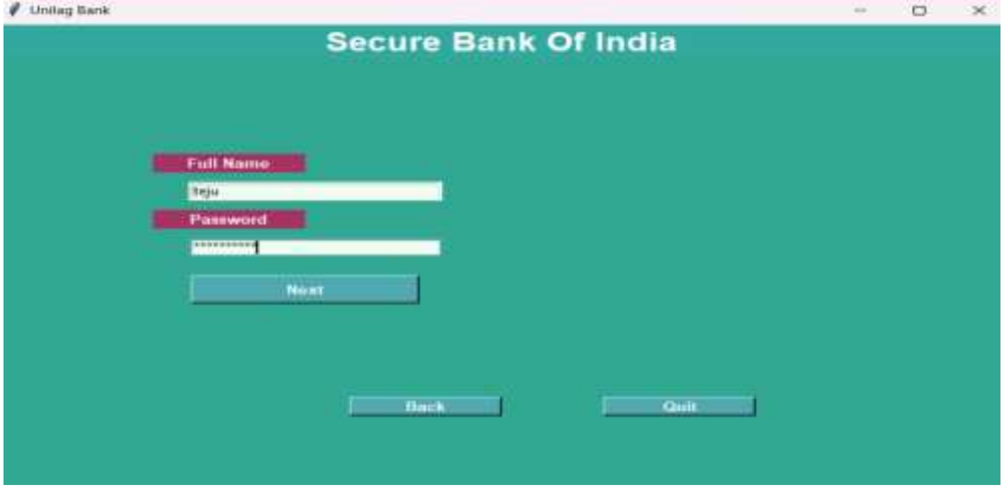
5.1.7 post-processing:

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

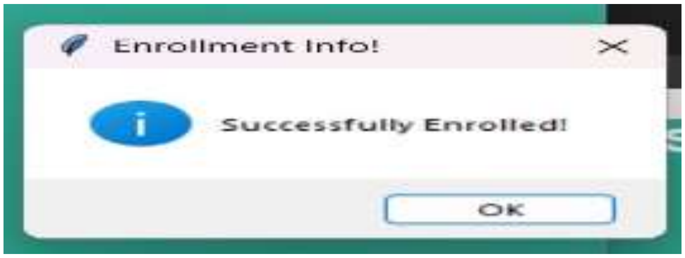
VI. RESULTS



6 home page



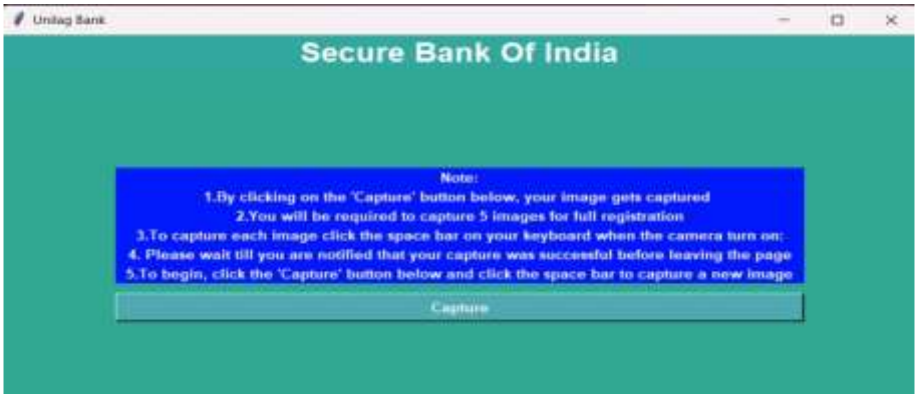
6.1 Login page



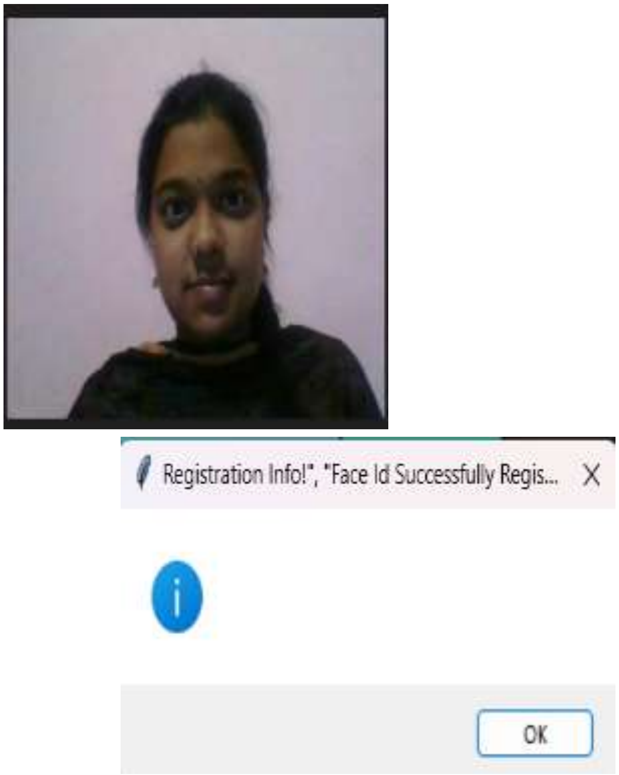
Enrollment Info!

Successfully Enrolled!

6.3 Enrollment

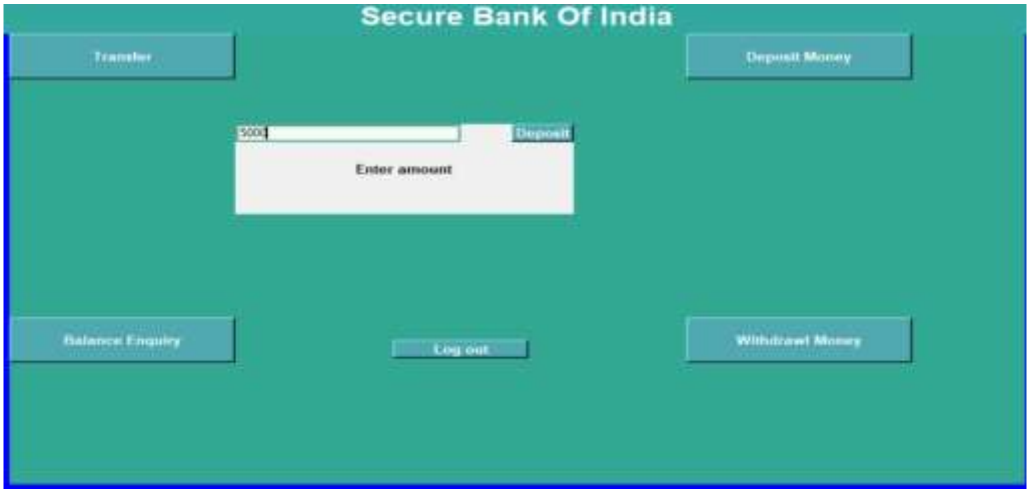


Note:
1.By clicking on the 'Capture' button below, your image gets captured
2.You will be required to capture 5 images for full registration
3.To capture each image click the space bar on your keyboard when the camera turn on:
4. Please wait till you are notified that your capture was successful before leaving the page
5.To begin, click the 'Capture' button below and click the space bar to capture a new image



Registration Info!", "Face Id Successfully Regis...

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. 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 Technology for Drug Control Applications.” ONDCP International Counterdrug Technology Symposium: Facial Recognition Vendor Test. Department of Defense Counterdrug Technology Development Program Office, June 2001.
3. Gross, Ralph, Shi, Jianbo, and Cohn, Jeffrey F. “Quo vadis Face Recognition.” Third Workshop on Empirical Evaluation Methods in Computer Vision. Kauai: December 2001.
4. 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, 1996. Wrolstad, Jay. “NCR To Deploy New Microsoft OS in ATMs.” CRMDailyDotCom. 29 Nov. 200