

# **THIRD GENERATION ATM MACHINES USING COMPUTER VISION TECHNIQUES**

Submitted in partial fulfillment of the requirements for  
the award of  
Bachelor of Engineering degree in Computer Science and Engineering  
by

**CHOLAVETI SAI NAVEEN (Reg.No.37110160)**

**DEVARAPALLI RAMU (Reg.NO.37110183)**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING  
SCHOOL OF COMPUTING**

## **SATHYABAMA**

**INSTITUTE OF SCIENCE AND TECHNOLOGY  
(DEEMED TO BE UNIVERSITY)**

**Accredited with Grade "A" by NAAC  
JEPPIAAR NAGAR, RAJIV GANDHI  
SALAI, CHENNAI – 600 119**

**MARCH - 2021**



# **SATHYABAMA**

INSTITUTE OF SCIENCE AND TECHNOLOGY  
(DEEMED TO BE UNIVERSITY)

Accredited with "A" grade by NAAC  
Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai – 600 119

[www.sathyabama.ac.in](http://www.sathyabama.ac.in)



## **DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

### **BONAFIDE CERTIFICATE**

This is to certify that this project report is the bonafide work of **CHOLAVETI SAI NAVEEN (Reg. No. 36110160), DEVARAPALLI RAMU (Reg.No 37110183)** who carried out the project entitled "**THIRD GENERATION ATM MACHINES USING COMPUTER VISION TECHNIQUES**" under my supervision from **August 2020 to March 2021**.

**Internal Guide**  
**Mr.A.Yovan Felix, M.E.,(Ph.d)**

**Head of the Department**

---

Submitted for Viva voce Examination held on \_\_\_\_\_

**Internal Examiner**

**External Examiner**

## **DECLARATION**

I **DEVARAPALLI RAMU (Reg.NO 37110183)** hereby declare that the Project Report entitled "**THIRD GENERATION ATM MACHINE USING COMPUTER VISION TECHQUNIES**" is done by me under the guidance of **Mr. A.YOVAN FELIX, M.E.**, Department of Computer Science and Engineering at Sathyabama Institute of Science and Technology is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering.

**DATE:**

**PLACE: CHENNAI**

**SIGNATURE OF THE CANDIDATE**

## ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala, M.E., Ph.D., Dean**, School of Computing, **Dr. S. Vigneswari, M.E., Ph.D., and Dr. L. Lakshmanan, M.E., Ph.D., Heads of the Department** of Computer Science and Engineering for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Mrs. A.YOVAN FELIX, M.E., Assistant Professor**, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

## **ABSTRACT**

Facial recognition is a technique which uses the facial features to recognize the face. Although it is the most useful and necessary feature it is not fully developed. For the improvement and upgrading this facial recognition computer vision technique are the most suitable option. This concept deals with the development and safety of the users of the atm machines. The use of current software and the methods will lead to great development of the security systems in the present era. To prevent the losses and also to ensure the security there should be an improvement of the systems which are used right now. The proposed system can be used as perfect facial recognition software which deals with all kinds of situations and ensures that the losses are kept to minimum these are the minimum requirements of the current living situations. This deals with the identification of face of the user. This also deals with the security measures which should be taken in case of something unnatural or someone other than the user is trying to access the data. The help of computer vision techniques helps very much in the development of the project.

# TABLE OF CONTENTS

|                    |                                        |                 |
|--------------------|----------------------------------------|-----------------|
|                    | <b>ABSTRACT</b>                        | <b>v</b>        |
|                    | <b>LIST OF FIGURES</b>                 | <b>viii</b>     |
| <b>CHAPTER No.</b> | <b>TITLE</b>                           | <b>PAGE No.</b> |
| <b>1.</b>          | <b>INTRODUCTION</b>                    | <b>1</b>        |
|                    | 1.1 ATM SYSTEMS                        | 1               |
|                    | 1.2 HISTORY OF ATM                     | 2               |
|                    | 1.3 REQUIREMENTS AND INSTALLATION      | 3               |
|                    | 1.4 MANAGING PACKAGES                  | 3               |
| <b>2.</b>          | <b>LITERATURE REVIEW</b>               | <b>4</b>        |
| <b>3.</b>          | <b>AIM AND SCOPE</b>                   | <b>7</b>        |
|                    | 3.1 AIM OF PROJECT                     | 7               |
|                    | 3.2 <i>SCOPE OF PROJECT</i>            | 7               |
|                    | 3.2.1 OBJEVITIVE OF PROJECT            | 8               |
|                    | 3.3 <i>DISADVANTAGES</i>               | 8               |
| <b>4.</b>          | <b>SYSTEM DESIGN &amp; METHODOLOGY</b> | <b>9</b>        |
|                    | 4.1 EXISTING SYSTEM                    | 9               |
|                    | 4.1.1 GEOMETRICAL APPROACH             | 9               |
|                    | 4.1.2 PICTORIAL APPROACH               | 10              |
|                    | 4.2 DIADVANTAGES OF EXISTING SYSTEM    | 10              |
|                    | 4.3 PROPOSED SYSTEM                    | 11              |
|                    | 4.3.1 RELIABILITY                      | 11              |
|                    | 4.3.2 SECURITY                         | 12              |
|                    | 4.4 FACIAL RECOGNITION                 | 13              |
|                    | 4.5 FLOW CHARTS                        | 14              |
|                    | 4.6 ADVANTAGES OF PROPOSED SYSTEM      | 15              |
|                    | 4.7 REQUIREMENT SPECIFICATION          | 16              |
|                    | 4.8 MODULES                            | 16              |
| <b>5.</b>          | <b>RESULTS AND DISCUSSION</b>          | <b>19</b>       |
|                    | <b>5.1 SCREENSHOTS</b>                 | <b>19</b>       |



|           |                                   |           |
|-----------|-----------------------------------|-----------|
| <b>6.</b> | <b>CONCLUSION AND FUTURE WORK</b> | <b>24</b> |
|           | 6.1 CONCLUSION                    | 24        |
|           | 6.2 FUTURE WORK                   | 24        |
|           | <b>REFERENCES</b>                 | <b>25</b> |

## **APPENDIX**

|                          |    |
|--------------------------|----|
| A. PAPER ACCEPTANCE MAIL |    |
| B. PLAGIARISM REPORT     |    |
| C. JOURNAL PAPER         | 26 |
| D. SOURCE CODE           | 33 |

## LIST OF FIGURES

| FIGURE No. | FIGURE NAME                   | PAGE No. |
|------------|-------------------------------|----------|
| 4.1.1      | PICTORIAL APPROACH            | 10       |
| 4.5.1      | PROPOSED SYSTEM FLOW<br>CHART | 15       |
| 4.5.2      | BLOCK DIAGRAM                 | 15       |
| 5.1        | USER INTERFACE                | 20       |
| 5.2        | LOG-IN PAGE                   | 21       |
| 5.3        | REGISTRATION FORM             | 22       |
| 5.4        | FACE REGISTRATION             | 23       |
| 5.5        | TRANSCATIONS PAGE             | 24       |

# CHAPTER 1

## 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. Just step up to the camera while your eye is scanned. The iris -- the colored part of the eye the camera will be checking -- is unique to every person, more so than fingerprints.

### 1.1 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.

## **1.2 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..

## 1.3 Requirements and Installation

The most convenient way of installing the Python requirements for this tutorial is by using the Anaconda scientific Python distribution. Anaconda is a collection of the most commonly used Python packages preconfigured and ready to use.

Approximately 150 scientific packages are included in the Anaconda installation.

Install the version of Anaconda for your operating system.

All Python software described here is available for Windows, Linux, and Macintosh. All code samples presented in this tutorial were tested under Ubuntu Linux 14.04 using Python 2.7. Some code examples may not work on Windows without slight modification (e.g. file paths in Windows use \ and not / as in UNIX type systems).

The main software used in a typical Python machine learning pipeline can consist of almost any combination of the following tools:

1. NumPy, for matrix and vector manipulation
2. Pandas for time series and R-like DataFrame data structures
3. The 2D plotting library matplotlib
4. SciKit-Learn as a source for many machine learning algorithms and utilities
5. Keras for neural networks and deep learning

## 1.4 Managing Packages

Anaconda comes with its own built in package manager, known as Conda. Using the conda command from the terminal, you can download, update, and delete Python packages. Conda takes care of all dependencies and ensures that packages are preconfigured to work with all other packages you may have installed.

Keeping your Python distribution up to date and well maintained is essential in this fast moving field. However, Anaconda makes it particularly easy to manage and keep your scientific stack up to date. Once Anaconda is installed you can manage your Python distribution, and all the scientific

packages installed by Anaconda using the conda application from the command line. To list all packages currently installed, use conda list. This will output all packages and their version numbers. Updating all Anaconda packages in your system is performed using the conda update -all command. Conda itself can be updated using the conda update conda command, while Python can be updated using the conda update python command. To search for packages, use the search parameter, e.g. conda search stats where stats is the name or partial name of the package you are searching for.

## **CHAPTER 2**

### **LITERATURE REVIEW**

**TITLE:** The FERET evaluation methodology for face-recognition algorithms

**YEAR:** 2010

**AUTHOR:** P. Jonathon Phillips Syed A. Rizvi Hyeonjoon Moon

**ABSTRACT:**

Two of the most critical requirements in support of producing reliable face-recognition systems are a large database of facial images and a testing procedure to evaluate systems. The Face Recognition Technology (FERET) program has addressed both issues through the FERET database of facial images and the establishment of the FERET tests. To date, 14,126 images from 1,199 individuals are included in the FERET database, which is divided into development and sequestered portions of the database. In September 1996, the FERET program administered the third in a series of FERET face-recognition tests. The primary objectives of the third test were to

- 1) assess the state of the art,
- 2) identify future areas of research, and
- 3) measure algorithm performance.

**TITLE:** Face recognition for smart environments

**YEAR:** 2014

**AUTHOR:** Alex Pentland Tanzeem Choudhury

**ABSTRACT:**

Smart environments, wearable computers, and ubiquitous computing in general are the coming “fourth generation” of computing and information technology. But that technology will be a stillbirth without new interfaces for interaction, minus a keyboard or mouse. To win wide consumer acceptance, these interactions must be friendly and personalized; the next generation interfaces must recognize people in their immediate environment and, at a minimum, know who they are. In this article, the authors discuss face

recognition technology, how it works, problems to be overcome, current technologies, and future developments and possible applications. Twenty years ago, the problem of face recognition was considered among the most difficult in artificial intelligence and computer vision. Today, however, there are several companies that sell commercial face recognition software that is capable of high-accuracy recognition with databases of more than 1,000 people. The authors describe the face recognition technology used, explaining the algorithms for face recognition as well as novel applications, such as behavior monitoring that assesses emotions based on facial expression.

**TITLE:** Iris Recognition System using canny edge detection for Biometric Identification

**YEAR:** 2015

**AUTHOR:** Chouhan Bhawna Shailja Shukla

**ABSTRACT:**

Biometric system provides automatic identification of an individual based on a unique feature or characteristic possessed by the individual. Iris recognition is regarded as the most reliable and accurate biometric identification system available. Most commercial iris recognition systems use patented algorithms developed by Daugman, and these algorithms are able to produce perfect recognition rates. Especially it focuses on image segmentation and feature extraction for iris recognition process. The performance of iris recognition system highly depends on edge detection. The Canny Edge Detector is one of the most commonly used image processing tools, detecting edges in a very robust manner. For instance, even an effective feature extraction method would not be able to obtain useful information from an iris image that is not segmented properly. This paper presents a straightforward approach for segmenting the iris patterns. The used method determines an automated global threshold and the pupil center. Experiments are performed using iris images obtained from CASIA database (Institute of Automation, Chinese Academy of Sciences) and Matlab application for its easy and efficient tools in image manipulation.

**TITLE:** Face detection attendance system

**YEAR:** 2016

**AUTHOR:** Kaneez Bhatti Laraib Mughal Faheem Khuawar

**ABSTRACT:**

To maintain the attendance record with day to day activities is a challenging task.

The conventional method of calling name of each student is time consuming and there is always a chance of proxy attendance. The following system is based on face recognition to maintain the attendance record of students. The daily attendance of students is recorded subject wise which is stored already by the administrator. As the time for corresponding subject arrives the system automatically starts taking snaps and then apply face detection and recognition technique to the given image and the recognize students are marked as present and their attendance update with corresponding time and subject id. We have used deep learning techniques to develop this system, histogram of oriented gradient method is used to detect faces in images and deep learning method is used to compute and compare feature facial of students to recognize them. Our system is capable to identify multiple faces in real time.

**TITLE:** Facial recognition using EIGEN faces

**YEAR:** 2018

**AUTHOR:** Hafizur Rahman Abhijit Bhowmik Md. Saef Ullah Miah

**ABSTRACT:**

In this article, a face recognition system using the Principal Component Analysis (PCA) algorithm was implemented. The algorithm is based on an eigenfaces approach which represents a PCA method in which a small set of significant features are used to describe the variation between face images. Experimental results for different numbers of eigenfaces are shown to verify the viability of the proposed method

## **CHAPTER 3**

### **AIM AND SCOPE**

#### **3.1 AIM OF THE PROJECT:**

Automated teller machines (ATMs) are well known devices typically used by individuals to carry out a variety of personal and business financial transactions and/or banking functions. ATMs have become very popular with the general public for their availability and general user friendliness. ATMs are now found in many locations having a regular or high volume of consumer traffic. For example, ATMs are typically found in restaurants, supermarkets, Convenience stores, malls, schools, gas stations, hotels, work locations, banking centers, airports, entertainment establishments, transportation facilities and a myriad of other locations. ATMs are typically available to consumers on a continuous basis such that consumers have the ability to carry out their ATM financial transactions and/or banking functions at any time of the day and on any day of the week. The study is focused on Design and Implementation of Face Detection based ATM Security System using object detection concept. The system is implemented on the credit card size Raspberry Pi board with extended capability of open source Computer Vision (OpenCV) software which is used for Image processing operation. High level security mechanism is provided by the consecutive actions such as initially system captures the human face and check whether the human face is detected properly or not. If the face is not detected properly, it warns the

user to adjust him/her properly to detect the face. Still the face is not detected properly the system will lock the door of the ATM cabin for security purpose.

### **3.2 SCOPE OF THE PROJECT:**

The main purpose of the project is to assure the safety of the people who are using ATM machines. The number of people using the ATM machines has been increasing in a rapid rate. As the number of people using Increasing the number of crimes and fraud activities are also been increasing at a very noticeable rate. Thus we have come forward with a more appealing and more secure process through which we can feel more secure while using the ATMs. Thus the software and the hardware are much reliable for this purpose. These may take time to be implemented all across the world but once when the installation is done world will be a better place with less number of fraud activities across the globe.

#### **3.2.1 OBJECTIVE OF THE PROJECT**

- The objective of this project is to show how sentimental analysis can help improve the user experience over a social network or system interface.
- The learning algorithm will learn what our emotions are from statistical data then perform sentiment analysis.
- Our main objective is also maintain accuracy in the final result.
- The main goal of such a sentiment analysis is to discover how the audience perceives the television show. The Twitter data that is collected will be classified into two categories; positive or negative. An analysis will then be performed on the classified data to investigate what percentage of the audience sample falls into each category.
- Particular emphasis is placed on evaluating different machine learning algorithms for the task of twitter sentiment analysis.

### **3.4 DISADVANTAGES OF SYSTEM:**

- The picture quality isn't exactly great.

- If there is less light close to the ATM then the nature of the picture can alter and this may prompt some bogus approvals.
- The edge of the camera or the picture sensor must be in an ideal position or, in all likelihood it may cause a few mistakes.

## **CHAPTER 4**

### **SYSTEM DESIGN AND METHODOLOGY**

#### **4.1 EXISTING SYSTEM:**

Face attestation moves from the resulting that machine began to wind up being continuously "canny" and had the improvement of fill in, right or help the nonattendance of human cutoff points and assets. The subject of face insistence is as old as PC vision and both thinking about the sensible centrality of the point and hypothetical energy from mental science. Face attestation isn't the essential framework for seeing others. Without a doubt, even people between one another use assets so as to recall that others. Machines have a logically wide area for attestation purposes, which use thinks, for example, fingerprints, or iris checks. Despite the way that these strategies for ID can be powerfully definite face attestation has dependably stays an important purpose of union of research as a result of its non meddling nature and it is individuals' fundamental strategy for individual unmistakable affirmation. Since the beginning of that field of advancement two standard strategy apologies are

followed

- Geometrical approach
- Pictorial approach

#### 4.1.1 Geometrical approach

The geometrical strategy uses the spatial arrangement of facial features. This infers the rule geometrical the association is set up, the specialist keeps features of the face, for instance, and the eyes, nose and mouth are first found and subsequently faces are assembled dependent on various geometrical partitions and edges between features. Of course, the pictorial technique uses designs to see facial features. This pictorial strategy uses the formats of the critical facial features and entire face to perform affirmation on frontal points of view on faces. Countless the endeavors relied upon these two systems have some fundamental extensions, communication in the situations where there occurs a slight malfunction which handle different stances establishments. Beside these two techniques the other late organization in the process but the instant recovery after some time based philosophies, which structure formats from the image point, and the crucial fragment assessment approach, which can be examined as a flawed design approach.

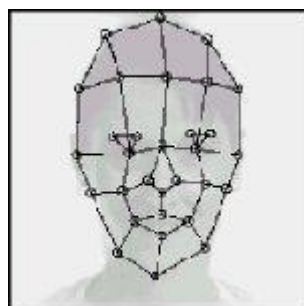


Figure 4.1.1 Pictorial and Geometric approaches

#### 4.1.2 Pictorial approach

The pictorial and highlight geometry approaches has been applied to faces at different posture and appearance is appeared in the figure 2.1 After geometrical approach or pictorial

methodology techniques, different strategies like Eigen faces, Principal positive Component the specialist reacts with CONNACK message.

When Analysis, and strategies that procedure pictures in blend with neural systems. In the representative acknowledgment stage and the following the information is looked at against all present representative chose model perspectives on every individual. To look at the contribution of the specific in the specific model view, the face is first geometrically lined up with the aid of model view which helps in identifying. A relative change is applied to the contribution to bring the facial highlights naturally situated by the framework into correspondence with similar highlights on the model. A method dependent on the optical stream in middle of the situation which might be the changed info and the model is utilized to make up for any staying little change between the two. Layouts from the model are then contrasted and the picture utilizing standardized connection. Both the given mode and information pictures are pre-handled with a differential administrators.

## **4.2 DISADVANTAGES OF EXISTING SYSTEM:**

- The picture quality isn't exactly great.
- If there is less light close to the ATM then the nature of the picture can alter and this may prompt some bogus approvals.
- The edge of the camera or the picture sensor must be in an ideal position or, in all likelihood it may cause a few mistake

## **4.3 PROPOSED SYSTEM:**

**Computer vision** is an interdisciplinary scientific field that deals with how computers can gain high-level understanding from digital images or videos. From the perspective of engineering, it seeks to understand and automate tasks that the human visual

system can do. Computer vision tasks include methods for acquiring, processing, analyzing and understanding digital images, and extraction of high-dimensional data from the real world in order to produce numerical or symbolic information, e.g. in the forms of decisions. Understanding in this context means the transformation of visual images (the input of the retina) into descriptions of the world that make sense to thought processes and can elicit appropriate action. This image understanding can be seen as the disentangling of symbolic information from image data using models constructed with the aid of geometry, physics, statistics, and learning theory. In existing system, face attestation only happens. But in our proposed system, we have computer vision techniques for the face recognition process. Instead of using ATM card, the users face will be captured and recognized and verified for the transaction process. FRS is an application that mechanically identifies a person from a digital image or a video outline from a video source. One of the behaviors to do this method is by matching chosen facial features from a facial database and the image.

#### **4.3.1 RELIABILITY**

ATMs are generally reliable, but if they do go wrong customers will be left without cash until the following morning or whenever they can get to the bank during opening hours. Of course, not all errors are to the detriment of customers; there have been cases of machines giving out money without debiting the account, or giving out higher value notes as a result of incorrect denomination of banknote being loaded in the money cassettes. Errors that can occur may be mechanical (such as card transport mechanisms; keypads; hard disk failures); software (such as operating system; device driver; application); communications; or purely down to operator error.

#### **4.3.2 SECURITY**

Early ATM security focused on making the ATMs invulnerable to physical attack;

they were effectively safes with dispenser mechanisms. ATMs are placed not only near banks, but also in locations such as malls, grocery stores, and restaurants. The other side of this improvement is the enhancement of the culprit's probability to get his 'unauthentic' share.

ATMs are a quick and convenient way to get cash. They are also public and visible, so it pays to be careful when you're making transactions. Follow these general tips for your personal safety.

**Stay alert.** If an ATM is housed in an enclosed area, shut the entry door completely behind you. If you drive up to an ATM, keep your car doors locked and an eye on your surroundings. If you feel uneasy or sense something may be wrong while you're at an ATM, particularly at night or when you're alone, leave the area.

**Keep you PIN confidential.** Memorize your Personal Identification Number (PIN); don't write it on your card or leave it in your wallet or purse. Keep your number to yourself. Never provide your PIN over the telephone, even if a caller identifies himself as a bank employee or police officer. Neither person would call you to obtain your number.

**Conduct transactions in private.** Stay squarely in front of the ATM when completing your transaction so people waiting behind you won't have an opportunity to see your PIN being entered or to view any account information. Similarly, fill out your deposit/withdrawal slips privately.

**Don't flash your cash.** If you must count your money, do it at the ATM, and place your cash into your wallet or purse before stepping away. Avoid making excessively large withdrawals. If you think you're being followed as you leave the ATM, go to a public area near other people and, if necessary, ask for help.

**Save receipt.** Your ATM receipts provide a record of your transactions that you can later reconcile with your monthly bank statement. If you notice any discrepancies on your statement, contact your bank as soon as possible. Leaving receipts at an ATM can also let others know how much money you've withdrawn and how much you have in your account.

**Guard your card.** Don't lend your card or provide your PIN to others, or discuss your bank account with friendly strangers. If your card is lost or stolen, contact your bank immediately.

**Immediately report any crime to the police.** Contact the Department Of Public Security or your local police station for more personal safety information.

#### **4.4 FACIAL RECOGNITION:**

The main issues faced in developing such a model are keeping the time elapsed in the verification process to a negligible amount, allowing for an appropriate level of variation in a customer's face when compared to the database image, and that credit cards which can be used at ATMs to withdraw funds are generally issued by institutions that do not have in-person contact with the customer, and hence no opportunity to acquire a photo.

Because the 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.

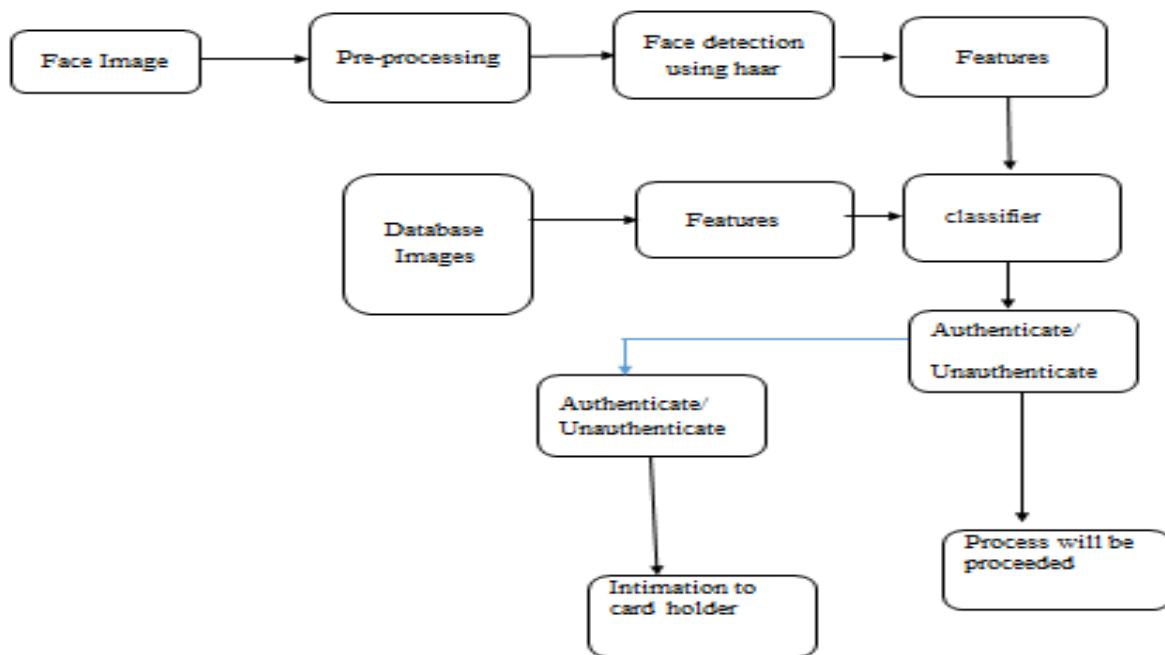
When a match is made with the PIN but not the images, the bank could limit transactions in a manner agreed upon by the customer when the account was opened, and could store the image of the user for later examination by bank officials. In regards to bank employees gaining access to customer PINs for 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

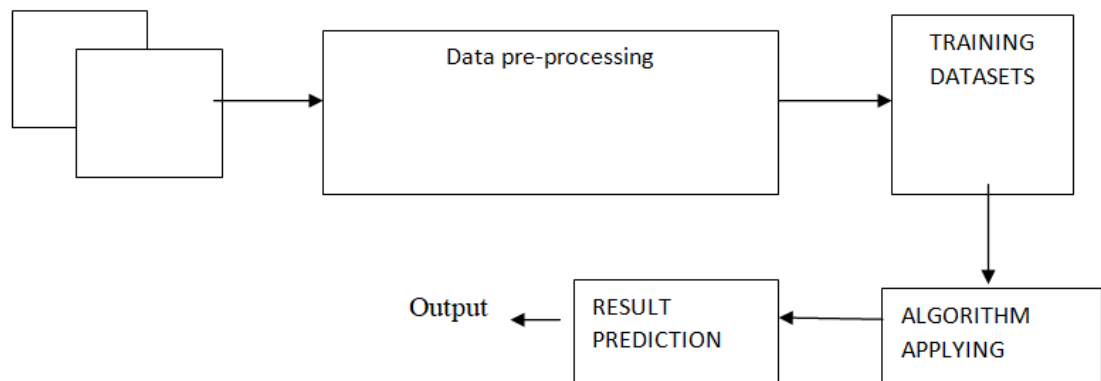
possible that positive results (read: significant fraud reduction) achieved by this system might motivate such an overhaul.

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.

## **4.5 FLOW CHARTS:**



#### 4.5.1 PROPOSED SYSTEM FLOW CHART



#### 4.5.2 SIMPLE BLOCK DIAGRAM FOR UNDERSTANDING

#### 4.6 ADVANTAGES OF PROPOSED SYSTEM:

1. **Enhanced security:** As for personal use, facial recognition can be used as a security

tool for locking personal devices and for personal surveillance cameras.

**2. Faster processing:** The process of recognizing a face takes a second or less — and this is incredibly beneficial for the companies. Considering that facial recognition in ATM systems is almost instant, it grants a quick and efficient verification of a person. In addition, it's hard to fool this technology so this is another bonus.

**3. Seamless integration:** The facial recognition technology is quite easily integrated so it's a perfect choice. It does not require spending additional money on its integration and most facial recognition solutions are compatible with the majority of security software.

**4. Automation of identification:** Before, security guards had to perform manual identification of a person that took too much time and did not boast high accuracy. But today, facial recognition is completely independent in the identification process and not only takes seconds but is also incredibly accurate

## **4.7 REQUIREMENT SPECIFICATION:**

### **HARDWARE REQUIREMENTS:**

PROCESSOR : Intel I5  
RAM : 4GB MIN

### **SOFTWARE REQUIREMENTS:**

PYTHON IDE : Anaconda Jupyter Notebook IDE .  
PROGRAMMING LANGUAGE : Python

## **4.8 MODULES:**

### **4.8.1 Dataset preparation and preprocessing:**

Data is the foundation for any machine learning project. The second stage of project implementation is complex and involves data collection, selection, preprocessing, and transformation. Each of these phases can be split into several steps.

#### **Data collection:-**

It's time for a data analyst to pick up the baton and lead the way to machine learning implementation. The job of a data analyst is to find ways and sources of collecting relevant and comprehensive data, interpreting it, and analyzing results with the help of statistical techniques.

The type of data depends on what you want to predict.

There is no exact answer to the question “How much data is needed?” because each machine learning problem is unique. In turn, the number of attributes data scientists will use when building a predictive model depends on the attributes' predictive value.

‘The more, the better’ approach is reasonable for this phase. Some data scientists suggest considering that less than one-third of collected data may be useful. It's difficult to estimate which part of the data will provide the most accurate results until the model training begins. That's why it's important to collect and store all data — internal and open, structured and unstructured.

The tools for collecting internal data depend on the industry and business infrastructure. For example, those who run an online-only business and want to launch a personalization campaign can try out such web analytic tools as Mixpanel, Hotjar, CrazyEgg, well-known Google analytics, etc. A web log file, in addition, can be a good source of internal data. It stores data about users and their online behavior: time and length of visit, viewed pages or objects, and location.

Companies can also complement their own data with publicly available datasets. For instance, Kaggle, Github contributors, AWS provide free datasets for analysis.

#### **Data preprocessing:-**

The purpose of preprocessing is to convert raw data into a form that fits machine learning. Structured and clean data allows a data scientist to get more precise results from an applied machine learning model. The technique includes data formatting, cleaning, and

sampling.

**Data formatting:** - The importance of data formatting grows when data is acquired from various sources by different people. The first task for a data scientist is to standardize record formats. A specialist checks whether variables representing each attribute are recorded in the same way. Titles of products and services, prices, date formats, and addresses are examples of variables. The principle of data consistency also applies to attributes represented by numeric ranges.

**Data cleaning:** - This set of procedures allows for removing noise and fixing inconsistencies in data. A data scientist can fill in missing data using imputation techniques, e.g. substituting missing values with mean attributes. A specialist also detects outliers — observations that deviate significantly from the rest of distribution. If an outlier indicates erroneous data, a data scientist deletes or corrects them if possible. This stage also includes removing incomplete and useless data objects.

**Data anonymization:** - Sometimes a data scientist must anonymize or exclude attributes representing sensitive information (i.e. when working with healthcare and banking data).

**Data sampling:** - Big datasets require more time and computational power for analysis. If a dataset is too large, applying data sampling is the way to go. A data scientist uses this technique to select a smaller but representative data sample to build and run models much faster, and at the same time to produce accurate outcomes.

#### **4.8.2 Data splitting:-**

A dataset used for machine learning should be partitioned into three subsets — training, test, and validation sets.

**Training set:** - A data scientist uses a training set to train a model and define its optimal parameters — parameters it has to learn from data.

**Test set:** - A test set is needed for an evaluation of the trained model and its capability for generalization. The latter means a model's ability to identify patterns in new unseen data after having been trained over a training data. It's crucial to use different subsets for training and testing to avoid model over fitting, which is the incapacity for generalization we mentioned above.

### 4.8.3 Modeling:-

During this stage, a *data scientist* trains numerous models to define which one of them provides the most accurate predictions.

#### **Model training:-**

It's time to train the model with this limited number of images. fast.ai offers many architectures to use which makes it very easy to use transfer learning.

We can create a convolutional neural network (CNN) model using the pre-trained models that work for most of the applications/datasets.

We are going to use ResNet architecture, as it is both fast and accurate for many datasets and problems. The 18 in the resnet18 represents the number of layers in the neural network.

We also pass the metric to measure the quality of the model's predictions using the validation set from the dataloader. We are using error\_rate which tells us how frequently the model is making incorrect predictions.

The fine\_tune method is analogous to the fit() method in other ML libraries. Now, to train the model, we need to specify the number of times (epochs) we want to train the model on each image.

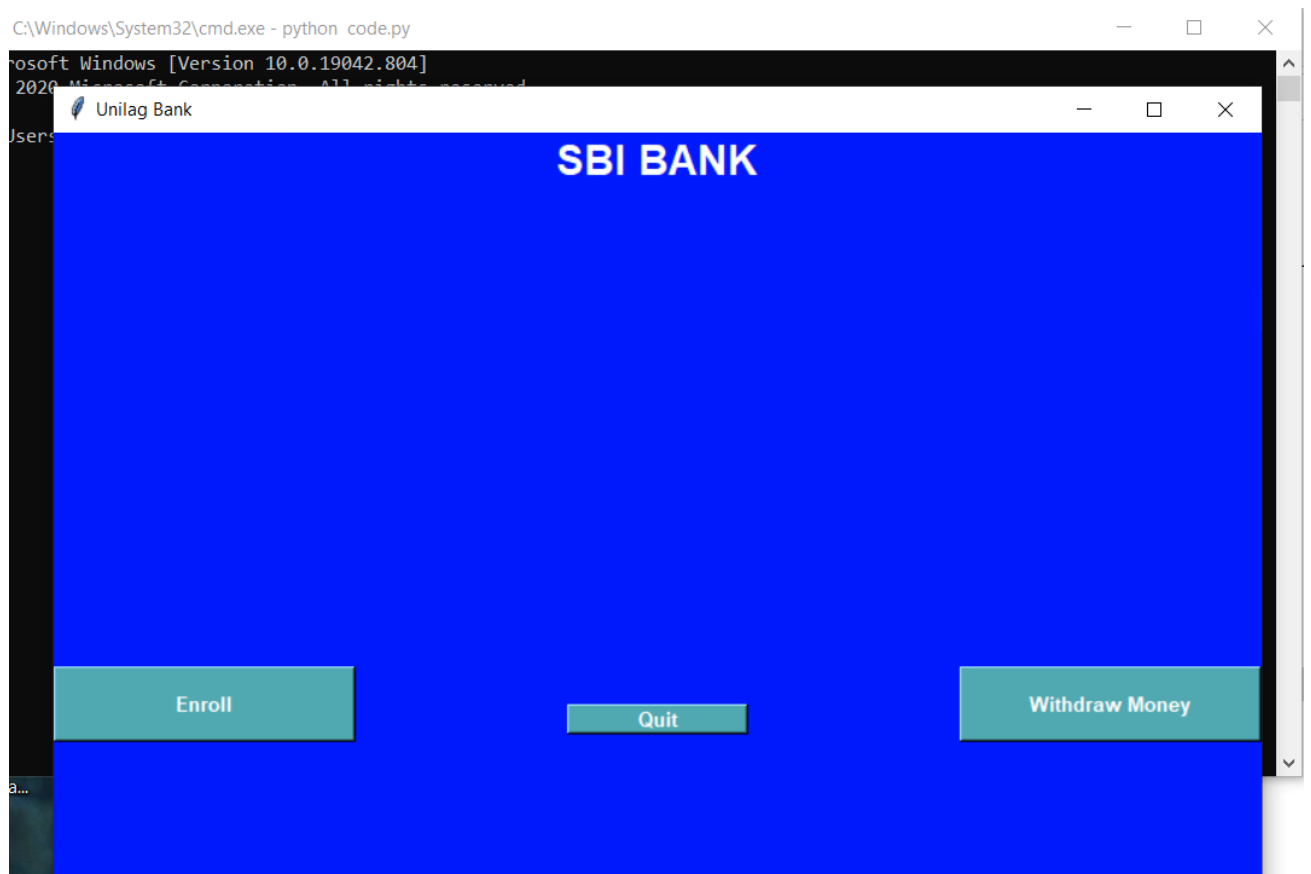
## CHAPTER 5

### RESULTS AND DISCUSSION

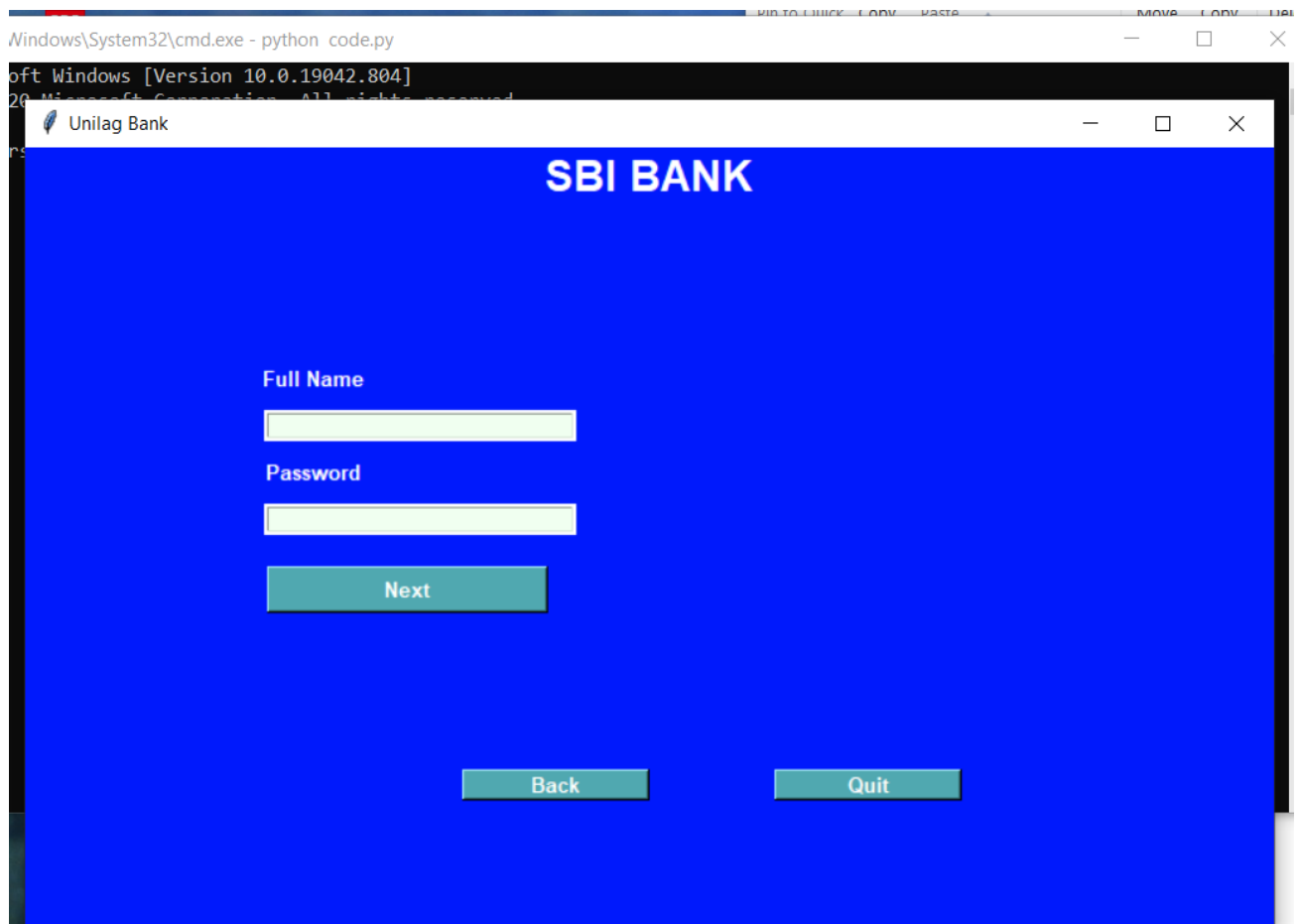
#### SCREENSHOTS:



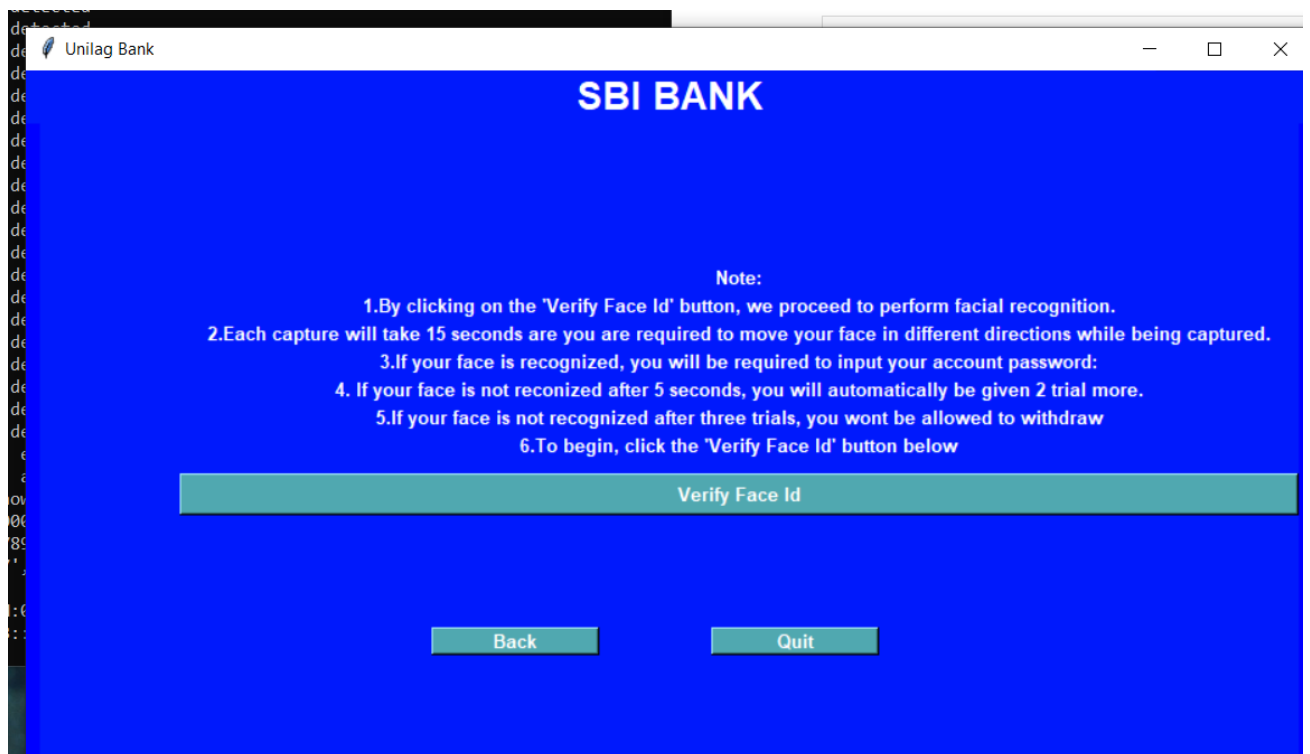
**5.1. USER INTERFACE TO BEGIN TRANSCATIONS.**



5.2 LOGIN AND SIGN UP PAGE.



### 5.3 ENTERING DETAILS FOR SIGN UP



## 5.4 REGISTERING FACE .



## 5.5 TRANSCATIONS OF ATM AFTER LOGIN .

## **CHAPTER 6**

### **CONCUSION AND FUTURE WORK**

#### **6.1 CONCLUSION:**

Face recognition technology has come a long way in the last twenty years. Today, machines are able to automatically verify identity information for secure transactions, for surveillance and security tasks, and for access control to buildings. Prototype system for automatic Helmet Detection, face detection and face recognition are successfully implemented and tested. The system is smart in the way that if the person tries to cover his face, it gives warning message for proper detection of face. If face is not recognized, then OTP is sent to authorize person.

#### **6.2 FUTURE WORK:**

System can be further improved by developing better algorithm for faster face recognition. 3D Models can be used to identify or verify another 3D image from database. The 3Dmodel is more reliable, better, effective and accurate than 2D.

This is proved to be better than the current running safety And security measures taken

The decrease in the time requirements change the whole process into a great success. the system is provided with highly developed sensors and software which make it even more accurate and dependable. With the increase in the use of the ATM machines there will be a great need of the security to be developed from day to day. We need to keep up with the society and should increase the security. These methods will help in obtaining a secure future.

## **REFERENCES**

- [1] K. Bavithra Devi, S Mohamed Roomi “Deep Learn Helmets-Enhancing Security at ATMs” 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)
- [2] Arunkumar V “ATM Security Using Face Recognition”, International Journal of Current Engineering and Scientific Research (IJCESR) IN 2018.
- [3] Swedha. K, Tanuja Dubey “Analysis of Web Authentication methods using Amazon Web Services” 9th International Conference on Computing, Communication and Networking Technologies-2018
- [4] Jignesh J. Patoliya “Face Detection based ATM Security System using Embedded Linux Platform”, published in 2nd International Conference for Convergence in Technology (I2CT) 2017.

[5] Neel Ramakant Borkar, Sonia Kuwelkar “Real-Time Implementation of Face Recognition System” IEEE 2017 International Conference on Computing Methodologies and Communication (ICCMC)

[6] Musab Coskun, Aysegul Ucar, Ozal, Yakup Demir “Face Recognition Based on Convolutional Neural Network” published in 2017 IEEE.

[7] Sambarta Ray “An Intelligent Vision System for monitoring Security and Surveillance of ATM”, published in IEEE INDICON in 2015.

## **THIRD GENERATION ATM USING COMPUTER VISION TECHNIQUES**

**C.SAI NAVEEN**

B.E, Computer Science and Engineering  
Sathyabama Institute Of Science And  
Technology Chennai, India.

**D.RAMU**

B.E ,Computer Science and  
Engineering Sathyabama Institute Of  
Science And Technology  
Chennai, India.

**A. Yoven Felix**

Associate Professor, Computer Science  
and Engineering Sathyabama Institute Of  
Science And Technology  
Chennai,India.

**Abstract**— Facial recognition is a technique which uses the facial features to recognize the face. Although it is the most useful and necessary

feature it is not fully developed. For the improvement and upgrading this facial recognition computer vision techniques are the most suitable

option. This concept deals with the development and safety of the users of the atm machines. The use of current software and the methods will lead to great development of the security systems in the present era. To prevent the losses and also to ensure the security there should be an improvement of the systems which are used right now. The proposed system can be used as perfect facial recognition software which deals with all kinds of situations and ensures that the losses are kept to minimum these are the minimum requirements of the current living situations. This deals with the identification of face of the user. This also deals with the security measures which should be taken in case of something unnatural or someone other than the user is trying to access the data. The help of computer vision techniques helps very much in the development of the project.

**Key Words:** python, camera, min 4gb ram.

## 1. INTRODUCTION

Face Recognition is an application to naturally distinguish an individual in the wake of contrasting and a database of pictures. A test picture is taken with the assistance of a camera from a still source or video outline, and in the wake of representing different conceivable face appearance varieties, is contrasted and the database pictures for character. Analysis have an extraordinary enthusiasm for this field for its applications in different spaces. One of the business utilizations of the face acknowledgement frameworks could be begin with little essential login applications and prompting the improvement of a high security get to control framework, secure biometric based exchange or exceptionally verified observation framework A information and procedure

acclaimed affirm or check the character of an individual or totally security requirements.2 confirmation could be a framework wherever in 2 or a great deal of different elements zone until wont to exhibit the people exploitation higher than issue is ordinarily alluded to as "Solid Confirmation". The technique for numerous responses to challenge inquiries similarly you as recovers 'something you have' or 'something you are' is taken into thought multifaceted.

## 2.LITERATURE REVIEW

Iris Recognition System using canny edge detection for Biometric Identification By Bhavana Chohan Shailaja shulka.

This cannot work well when the gradient is not strong enough.

The FERET evaluation methodology for face-recognition algorithms By P.J Philips, H.moon, S.A.Rizvi, P.J.Rauss –the system can not differentiate between the similar faces.

Face recognition for smart environments By A.Pentland, T.Choudary- They require users to position their bodies then pause for a second to "declare" themselves.

Face detention attendance system By Prof T.Venkat narayan Rao - Difficult to maintain and repair. System is ineffective if there is no power supply.

Facial recognition using EIGEN faces By M.A.Turk, A.P.Pentland -Only gray scale image can be detected. A noisy image can reduce the efficiency

## 3.EXISTING SYSTEM

Face attestation moves from the resulting that machine began to wind up being continuously "canny" and had the improvement of fill in, right or help the nonattendance of human cutoff points and assets.

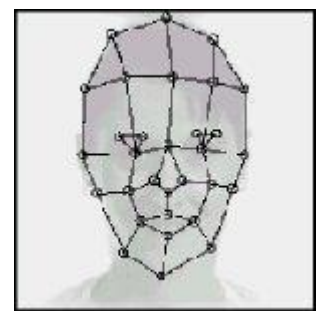
The subject of face insistence is as old as PC visio

n and both thinking about the sensible centrality of the point and hypothetical energy from mental science. Face attestation isn't the essential framework for seeing others. Without a doubt, even people between one another use assets so as to recall that others. Machines have a logically wide area for attestation purposes, which use thinks, for example, fingerprints, or iris checks. Despite the way that these strategies for ID can be powerfully definite face attestation has dependably stays an important purpose of union of research as a result of its non meddling nature and it is individuals' fundamental strategy for individual unmistakable affirmation. Since the beginning of that field of advancement two standard strategy apologies are followed

- Geometrical approach
- Pictorial approach

The geometrical strategy uses the spatial arrangement of facial features. This infers the rule geometrical the association is set up, the specialist keeps features of the face, for instance, and the eyes, nose and mouth are first found and subsequently faces are assembled dependent on various geometrical partitions and edges between features. Of course, the pictorial technique uses designs to see facial features. This pictorial strategy uses the formats of the critical facial features and entire face to perform affirmation on frontal points of view on faces. Countless the endeavors relied upon these two systems have some fundamental

extensions, communication in the situations where there occurs a slight malfunction which handle different stances establishments. Beside these two techniques the other late organization in the process but the instant recovery after some time based philosophies, which structure formats from the image point, and the crucial fragment assessment approach, which can be examined as a flawed design approach.



Pictorial and Geometric approaches

#### DISADVANTAGES OF EXISTING SYSTEM

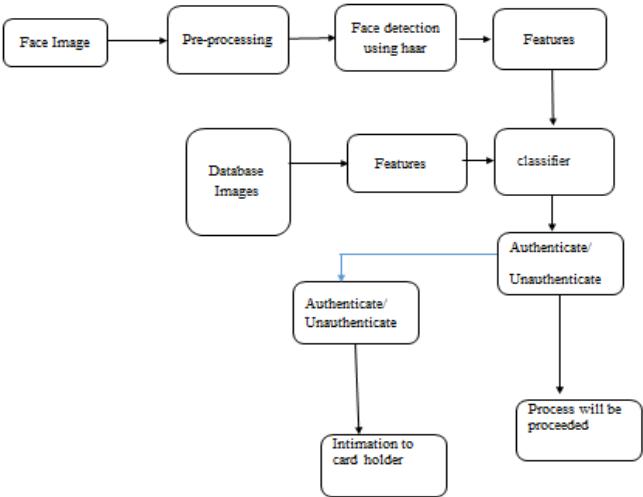
- The picture quality isn't exactly great.
- If there is less light close to the ATM then the nature of the picture can alter and this may prompt some bogus approvals.

The edge of the camera or the picture sensor must be in an ideal position or, in all likelihood it may cause a few mistakes

#### 4.PROPOSED SYSTEM

Computer vision tasks include methods for acquiring, processing, analyzing and understanding digital images, and extraction of high-dimensional data from the real world in order to produce numerical or symbolic information, e.g. in the forms of

decisions. Understanding in this context means the transformation of visual images (the input of the retina) into descriptions of the world that make sense to thought processes and can elicit appropriate action. This image understanding can be seen as the disentangling of symbolic information from image data using models constructed with the aid of geometry, physics, statistics, and learning theory. In existing system, face attestation only happens. But in our proposed system, we have computer vision techniques for the face recognition process. Instead of using ATM card, the users face will be captured and recognized and verified for the transaction process. FRS is an application that mechanically identifies a person from a digital image or a video outline from a video source. One of the behaviors to do this method is by matching chosen facial features from a facial database and the image.



Flow chart of proposed system

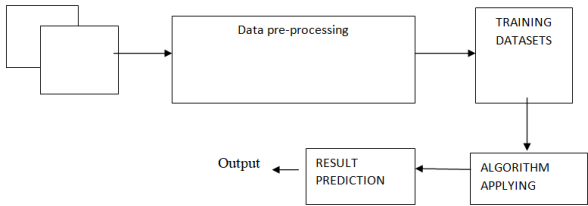
ADVANTAGES OF PROPOSED SYSTEM:

**1.Enhanced security:** As for personal use, facial recognition can be used as a security tool for locking personal devices and personal surveillance cameras.

**2. Faster processing:** The process of recognizing a face takes a second or less — and this is incredibly beneficial for the companies. Considering that facial recognition in ATM systems is almost instant, it grants a quick and efficient verification of a person. In addition, it's hard to fool this technology so this is another bonus.

**3. Seamless integration:** The facial recognition technology is quite easily integrated so it's a perfect choice. It does not require spending additional money on its integration and most facial recognition solutions are compatible with the majority of security software.

**4. Automation of identification:** Before, security guards had to perform manual identification of a person that took too much time and did not boast high accuracy. But today, facial recognition is completely independent in the identification process and not only takes seconds but is also incredibly accurate.



## SYSTEM ARCHITECTURE

### 5.METHODOLOGY

#### Data splitting:-

A dataset used for machine learning should be partitioned into three subsets — training, test, and validation sets.

**Training set:** - A data scientist uses a training set to train a model and define its optimal parameters — parameters it has to learn from data.

**Test set:** - A test set is needed for an evaluation of the trained model and its capability for generalization. The latter means a model's ability to identify patterns in new unseen data after having been trained over a training data. It's crucial to use different subsets for training and testing to avoid model over fitting, which is the incapacity for generalization we mentioned above.

#### Modeling:-

During this stage, a *data scientist* trains numerous models to define which one of them provides the most accurate predictions.

#### Model training:-

It's time to train the model with this limited number of images. fast.ai offers many architectures to use

which makes it very easy to use transfer learning.

We can create a convolutional neural network (CNN) model using the pre-trained models that work for most of the applications/datasets.

We are going to use ResNet architecture, as it is both fast and accurate for many datasets and problems. The 18 in the resnet18 represents the number of layers in the neural network.

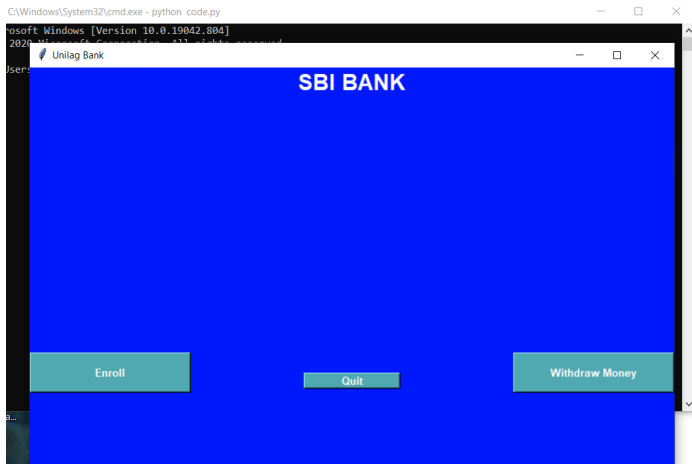
We also pass the metric to measure the quality of the model's predictions using the validation set from the dataloader. We are using `error_rate` which tells us how frequently the model is making incorrect predictions.

The `fine_tune` method is analogous to the `fit()` method in other ML libraries. Now, to train the model, we need to specify the number of times (epochs) we want to train the model on each image.

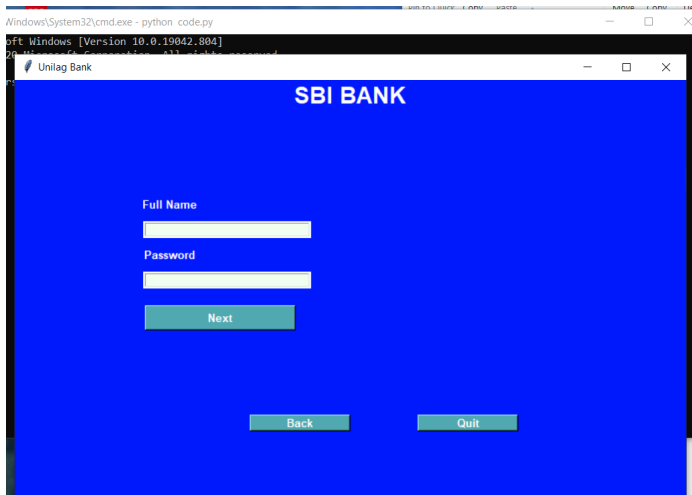
### 6.RESULTS.



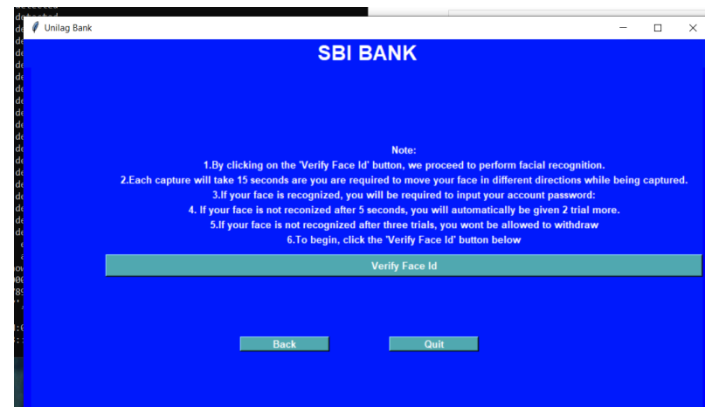
i) **USER INTERFACE TO BEGIN TRANSCATIONS**



## ii) LOGIN OR SIGNUP PAGE



## iii) DETAILS TO SIGNUP FOR TRANSCATIONS



## iv) ENROLLING THE FACE USING THE SIGNUP.



## v) TRANSCATIONS INTERFACE OF ATM

## 7.CONCLUSION AND FUTURE WORK.

### CONCLUSION:

Face recognition technology has come a long way in the last twenty years. Today, machines are able to automatically verify identity information for secure transactions, for surveillance and security tasks, and for access control to buildings. Prototype system for automatic Helmet Detection, face detection and face recognition

are successfully implemented and tested. The system is smart in the way that if the person tries to cover his face, it gives warning message for proper detection of face. If face is not recognized, then OTP is sent to authorize person.

#### **FUTURE SCOPE :**

System can be further improved by developing better algorithm for faster face recognition.

3D Models can be used to identify or verify another 3D image from database. The 3Dmodel is more reliable, better, effective and accurate than 2D

#### **8.REFERENCES:**

- [1] K. Bavithra Devi, S Mohamed Roomi "Deep Learn Helmets-Enhancing Security at ATMs" 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)
- [2] Arunkumar V "ATM Security Using Face Recognition", International Journal of Current Engineering and Scientific Research (IJCESR) IN 2018.
- [3] Swedha. K, Tanuja Dubey "Analysis of Web Authentication methods using Amazon Web Services" 9th International Conference on Computing, Communication and Networking Technologies-2018
- [4] Jignesh J. Patoliya "Face Detection based ATM Security System using Embedded Linux Platform", published in 2nd International Conference for Convergence in Technology (I2CT) 2017.
- [5] Neel Ramakant Borkar, Sonia Kuwelkar "Real-Time Implementation of Face Recognition System" IEEE 2017 International Conference on Computing Methodologies and Communication (ICCMC)
- [6] Musab Coskun, Aysegul Ucar, Ozal, Yakup Demir "Face Recognition Based on Convolutional Neural Network" published in 2017 IEEE.
- [7] Sambarta Ray "An Intelligent Vision System for monitoring Security and Surveillance of ATM", published in IEEE INDICON in 2015.
- [8] Mohsin Karovaliya, Saifali karedia "Enhanced security for ATM machine with OTP and facial recognition features" (2015).
- [9] 9 T. Suganya "Securing ATM by Image Processing- Facial Recognition Authentication" International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882. Volume 4, Issue 8, August 2015



