BANK LOCKER SECURITY SYSTEM

SUBMITTED BY

1.Vaishnavi Chourasiya B150453022
2.Virashree Jadhav B150453051
3.Srushti Karpe B150453058

UNDER THE GUIDANCE OF

Dr. Ms. M. A. Dudhedia (Internal Guide)

IN PARTIAL FULFILMENT OF
B.E. (ELECTRONICS & TELECOMMUNICATION) SAVITRIBAI PHULE PUNE UNIVERSITY 2021-2022

MARATHWADA MITRA MANDAL'S COLLEGE OF ENGINEERING, PUNE- 52
DEPARTMENT OF ELECTRONICS AND TELECOMMUNICATION

MARATHWADA MITRA MANDAL'S

COLLEGE OF ENGINEERING, PUNE

CERTIFICATE

This is to certify that the project report entitles

"BANK LOCKER SECURITY SYSTEM"

Submitted by

1. Vaishnavi Chourasiya B150453022
2. Virashree Jadhav B150453051
3. Srushti Karpe B150453058

is bonafide work carried out by them under the supervision of **Dr. Ms. M. A. Dudhedia** and it isapproved for the partial fulfilment of requirement of Savitribai Phule Pune University for award of the degree of Bachelor of Engineering (Electronics and Telecommunication).

This seminar report has not been earlier submitted to any other Institute or University for the award of any degree or diploma.

Dr. Ms. M. A. Dudhedia	**Dr. G. S. Gawande**	**Dr. V. N. Gohokar**
Project Guide	Head of Department	Principal of
Department of E&TC	Department of E&TC	MMCOE

Place **:** Pune
Date **:**

ACKNOWLEDGEMENT

"Ability and ambition alone are not enough for success. Many able persons have failed to achieve anything worthwhile because of lack of guidance and direction. Success of any project depends greatly on the support, guidance and encouragement received from the guide." We have been fortunate to have more than one pillar of strength in our humble effort to make this project successful.

It gives us a great pleasure in presenting the report on Bank Locker Security System using Face & Liveness Detection. We would like to express our special thanks of gratitude to our guide, **Dr. Ms. M. A. Dudhedia** for her resourceful & able guidance which lead to timely completion of this seminar report. It was really her insight and obsession for innovative ideas that motivated us to consider our idea seriously.

We managed to learn quite few things from her which will definitely help us in the future. We sincerely thank her for this kind co-operation and extreme patience that she has shown.

We are very thankful to **Dr. G. S. Gawande**, Head of Department and **Dr. Ms. P. S. Sawant,** previous Head of Department for providing all the necessary facilities and support.

We would also like to thank the entire teaching and non-teaching staff of E&TC Department, who extended their kind co-operation. Last but not the least; we would like to thank our family and friends for their constant support

Vaishnavi Chourasiya
Virashree Jadhav
Srushti Karpe

ABSTRACT

Ensuring the security of transactions is currently one of the biggest challenges facing banking systems. The use of biometric authentication of users attracts huge sums of money from banks around the world due to their convenience and acceptance. Especially in offline environments, where face images from ID documents are matched to digital selfies. In fact, comparisons of selfies with ids have also been used in some broader programs these days, such as automatic immigration control. The great difficulty of such a process lies in limiting the differences between comparative facial images given their different origins. Propose a novel architecture for cross-domain matching problem based on deep features extracted by two well referenced Convolutional Neural Networks(CNN). The results obtained from the data collected, called Face Bank, with more than 93% accuracy, indicate the strength of the proposed face-to-face comparison problem and its inclusion in real banking security systems.

INDEX

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

In today's modern world, security plays an important role. Every person has precious accessories like gold, jewellery or cash. It is not enough to have these accessories, but security of this is very important, for this purpose we keep them in bank lockers. Still we often hear or read in newspaper that some fake person has access the locker of another person and have stolen money. In order to overcome this type of frauds, authentication of the person who wants to use the locker is very important.

1.2 OVERVIEW

Although the recognition performance of biometric system is nowadays quite satisfactory for most applications, much work is still necessary to allow convenient, secure and privacy-friendly systems to be designed. In face recognition, the usual attack methods may be classified into several categories.

The idea of classifying is based on what verification proof is provide to face verification system, such as a stolen photo, stolen face photos, recorded video, 3D face models with the abilities of blinking and lip moving, 3D face models with various expressions and so on. The idea of classifying is based on what verification proof is provide to face verification system, such as a stolen photo, stolen face photos, recorded video, 3D face models with the abilities of blinking and lip moving, 3D face models with various expressions and so on.

Proposed a method of live face detection to resist the attack using aphotograph on what verification proof is provide to Face verification system, such as a stolen photo, stolen face photos, recorded video, 3D face models with the abilities of blinking and lip moving, 3D face models with various expressions and so on.

The algorithm is based on analysis of movement of facial components, especially eyes, in sequential images. Generally in sequential face images there are very little variations in shape of face and facial components. But eyes have much larger variation in shape because we always blink and move the pupils unconsciously. So we detect eyes in sequential face images and compare the shape of each eye region to decide whether input face is a real face or a photograph.

1.3 MOTIVATION

Liveliness detection has been a very active research topic in fingerprint recognition and iris recognition communities in recent years. But in face recognition, approaches are very much limited to deal with this problem. Liveliness is the act of differentiating the feature space into live and non-living. Imposters will try to introduce a large number of spoofed biometrics into system. With the help of liveliness detection, the performance of a biometric system will improve. It is an important and challenging issue which determines the trustworthiness of biometric system security against spoofing.

1.4 PROBLEM DEFINITION AND OBJECTIVES

1.4.1 Problem Definition

The general public has immense need for security measures against spoof attack. Biometrics is the fastest growing segment of such security industry. Some of the familiar techniques for identification are facial recognition, fingerprint recognition, handwriting verification, hand geometry, retinal and iris scanner. Among these techniques, the one which has developed rapidly in recent years is face recognition technology In general, face recognition algorithms are not able to differentiate live face from not live face which is a major security issue. It is an easy way to spoof face recognition systems by facial pictures such as portrait photograph. In order to guard against such spoofing, a secure system needs liveliness detection.

1.4.2 Objectives

- To study existing bank locker's method.
- To design the system architecture for proposed system.
- To analyze and evaluate the design module.

1.5 PROJECT SCOPE AND LIMITATIONS

1.5.1 Project Scope

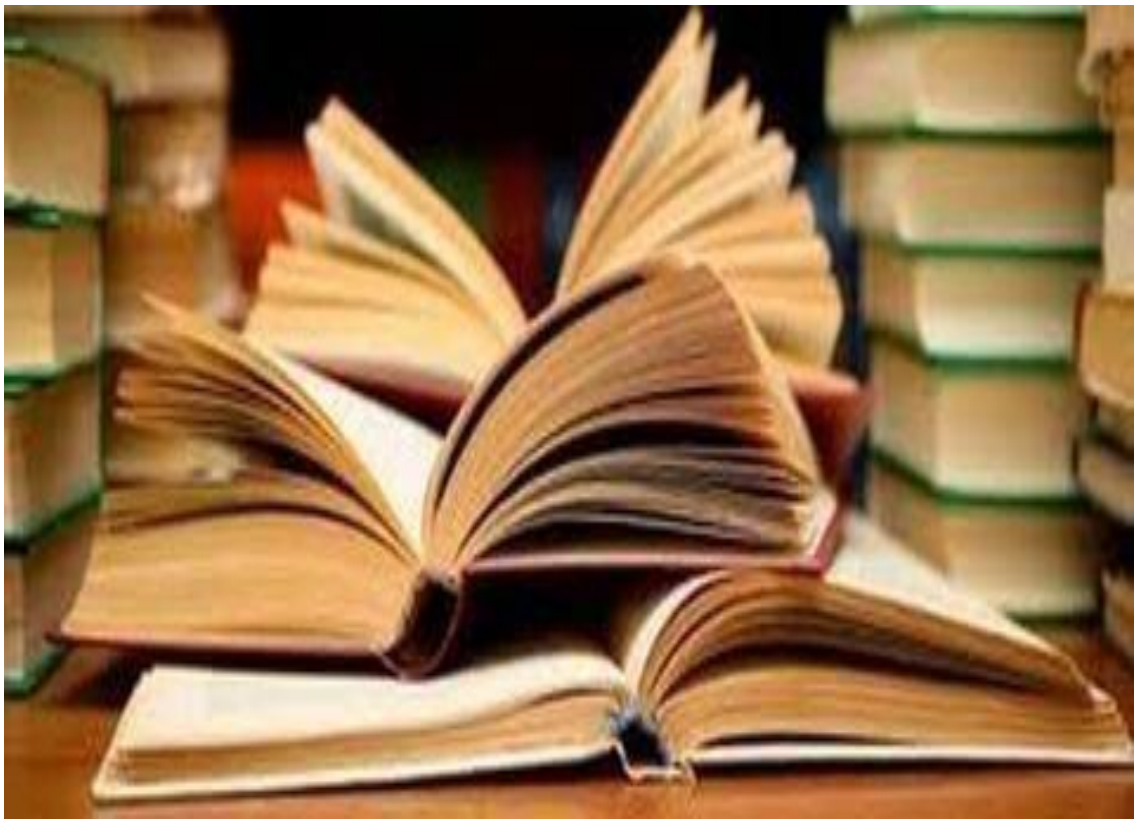
1. To give a clear pathway for future development of more secured, user friendly and efficient approaches for face liveliness detection
2. Face liveliness detection which helps understanding different spoof attacks scenarios and their relation to the developed solutions.

1.5.2 Project Limitations

If the number of user increases, we need to increase database of user which will affects in system, so system become slower.

CHAPTER 2

LITERATURE SURVEY



2.1 LITERATURE SURVEY

Gang Pan et al.[1] gift a spoofing against photograph in face recognition exploitation real time physiological property detection exploitation spontaneous eye blinking. This methodology needs solely a generic camera no different hardware to avoid spoofing attack in nonintrusive manner. Eye blinking is physical method that in a flash opens and closes lids Again and once more in an exceedingly} very minute. Generic camera captures fifteen frames per seconds, it provides 2 frames of faces that used as clue against spoofing attack. 2 captured frames in sequence are thought about as freelance. HMM produces options from finite state set. Typical blinking activity exploitation HMM feature finds spoofing attack.

Anjos et al. [2] planned how supported foreground or background motion correlation for checking physiological property of user. This methodology classified in motion detection. This methodology works on correlation between head rotation of user and its background. To go looking out correlation author uses fine grained motion direction. Optical flow is used to hunt out the direction of motion. This approach is easy method however need multiple frames to check physiological property, thus user ought to be co-operative. Face physiological property detection [3] has been planned to reinforce the dependability and security of face recognition system. The faux faces ar distinguished from the 000 ones exploitation totally different classification techniques. During this paper, we tend to propose one image-based faux face detection methodology supported frequency and texture analyses for discriminating 2-D paper masks from the live faces.

For the frequency analysis, we have got applied power spectrum primarily based methodology [4] that exploits not solely the low frequency info however conjointly the info residing among the high frequency regions. Moreover, wide used native Binary Pattern (LBP) [5]. In face recognition, the quality attack strategies may even be classified into many classes. The idea of classifying depends on what verification proof is give to face verification system, sort of a purloined picture, purloined face photos, recorded video, 3D face models with the abilities of blinking and lip moving, 3D face models with numerous expressions and so on [6]. The most goal of this paper is to vogue and implement a bank locker security system supported RFID and GSM technology which could be organized in bank, secured offices and homes. Throughout this method solely authentic person is recovered cash from bank locker. The RFID reader reads the id range from passive tag and send to the microcontroller, if the id range is valid then microcontroller send the SMS request to the documented person mobile range, for the primary countersign to open the bank locker, if the person send the countersign to the microcontroller, which may verify the passwords entered by the key board and received from documented mobile. If these 2 passwords are matched the locker are opened otherwise it's going to be stay in bolted position[7].

Initially pattern flow unit of measurement collected as datasets and maintained in bank agent server. The machine includes a camera to capture the pattern flow of user and sent for method choices of the logic were compared and user where recognized. Additionally to the authentication of user there's another system to spot the user before that RFID little indefinite quantity checking is required.

Image method is used and information data input device identification is required for an additional level of security. In future bank can implement this sort of authentication chance for banking and from this project shows that everyone the bank accounts is accessed whereas not practice cards

through this face recognition with efficiency and safely [8]. Access system forms a vital important} link during a} terribly very security chain. The Fingerprint associated identification based security system given here is AN access system that enables exclusively authorized persons to access a restricted house.

Implemented a locker security system supported fingerprint, identification and technology containing door lockup system which might activate, proof and validate the user and unlock the door in real time for locker secure[9]. They says perhaps the foremost very important application of correct personal identification is securing restricted access systems from malicious attacks. Among all the presently utilized biometric techniques, fingerprint identification systems have received the foremostattention due to the long history of fingerprints and their intensive use in forensics. This paper deals with the difficulty of selection of associate optimum formula for fingerprint matching thus on voguea system that matches required specifications in performance and accuracy[10].

CHAPTER 3

SYSTEM SCHEMATIC AND SPECIFICATIONS

3 SYSTEM DESIGN

3.1 SYSTEM ARCHITECTURE

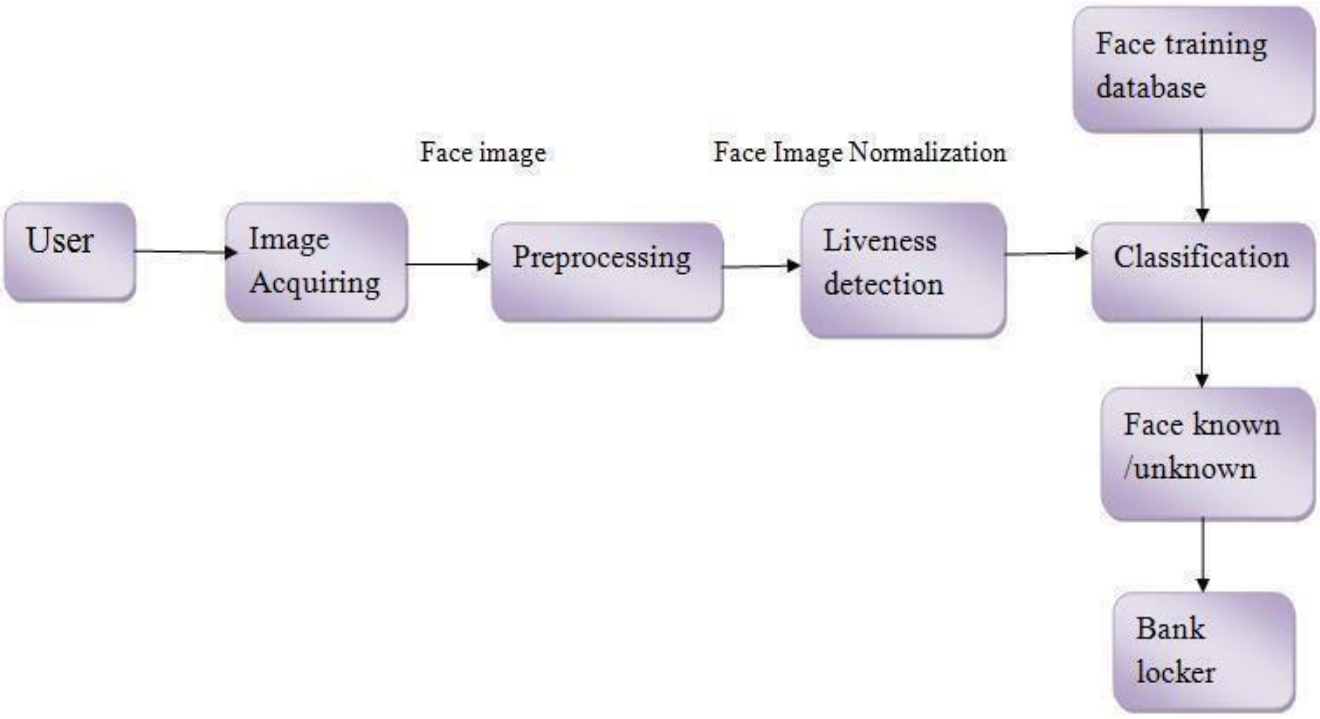


Fig No. 1. System Architecture

The block diagram indicates eye-blink detection & face recognition Based on LBPH algorithm. The algorithm works in real time through a webcam and displays the human's name. The program runs as follows**:**

1. **Image acquisition:** The general purpose here is to convert the view image (real world data) into a series of numerical data that can be converted later on a computer.
2. **Face Detection:** Here the algorithm focuses on finding the front face of person. It is like getting a picture where the person's picture is slowly matched. Any change in facial features on the website will disable the matching process.
3. **Face Recognition:** It is a computer program that uses an algorithm to detect and detect faces in an image. These are many algorithms used for face recognition but many programs use eye recognition for face detection. In this case sensory networks can be trained to see the user's face.
4**. Liveliness Detection:** Face detection Biometrics refers to the use of computer vision technology to detect the harmless presence of a live user, instead of representations such as a photo, video or mass
5. **Access Control:** It is a data protection system that enables organizations to control who is authorized to access business and resource data.

3.2 MATHEMATICAL MODEL

Let S be the list of modules or the functionalities of the system.

Thus, S is a set:
S= {Image Capturing and identification, Display of ads, Image matching}

If D is a device it will perform functionalities on U: User
D: f1(Image Capturing and identification)->A

A=Attributes (gender, age, clothes, etc).

F2 (Display of ads)->Displaying the ads according to the customer.

F3(Image matching)->Checking presence of customer in the mall.

3.2.1 Model 1

Algorithm for Image capturing and identification –

F1: Process the captured Image and identify attributes in the image.

Algorithm: capture image, identify attributes

Input: image

Output: Attributes in image

C={wi}Where C is the dataset of objects and human images(wi).

Steps:
Capture Images of customers. Store the customers image
Processing the captured image
Matching the image with the images in the dataset

3.2.2 Model 2

Algorithm for displaying of ads

F2 sends the ads to the display device

Algorithm: Sending image

Input: Attributes from captured image

Output: Ads to display device

Steps:
Fetch the ads

Display the ads for different person in regular interval

3.2.3 Model 3

Algorithm for image matching

Input: Captured Image at entry and exit point.

Output: Delete the captured image of entry point.

Steps:

Capture image at exit point.

Matching the image with the images of entry point.

Delete the matching image from both the Camera storage.

3.3 UML (Unified Modeling Language) Diagram:

3.3.1 Sequence Diagram

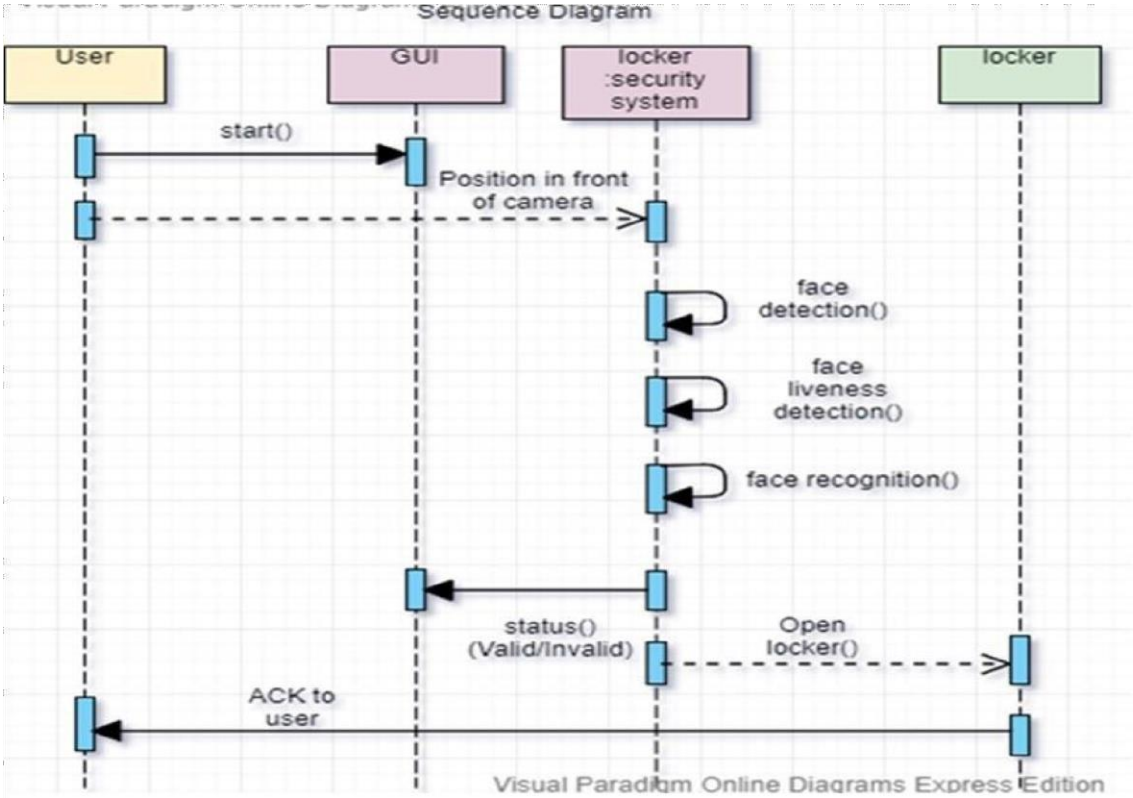


Fig no. 2. UML Diagram

3.3.2 User case Diagram

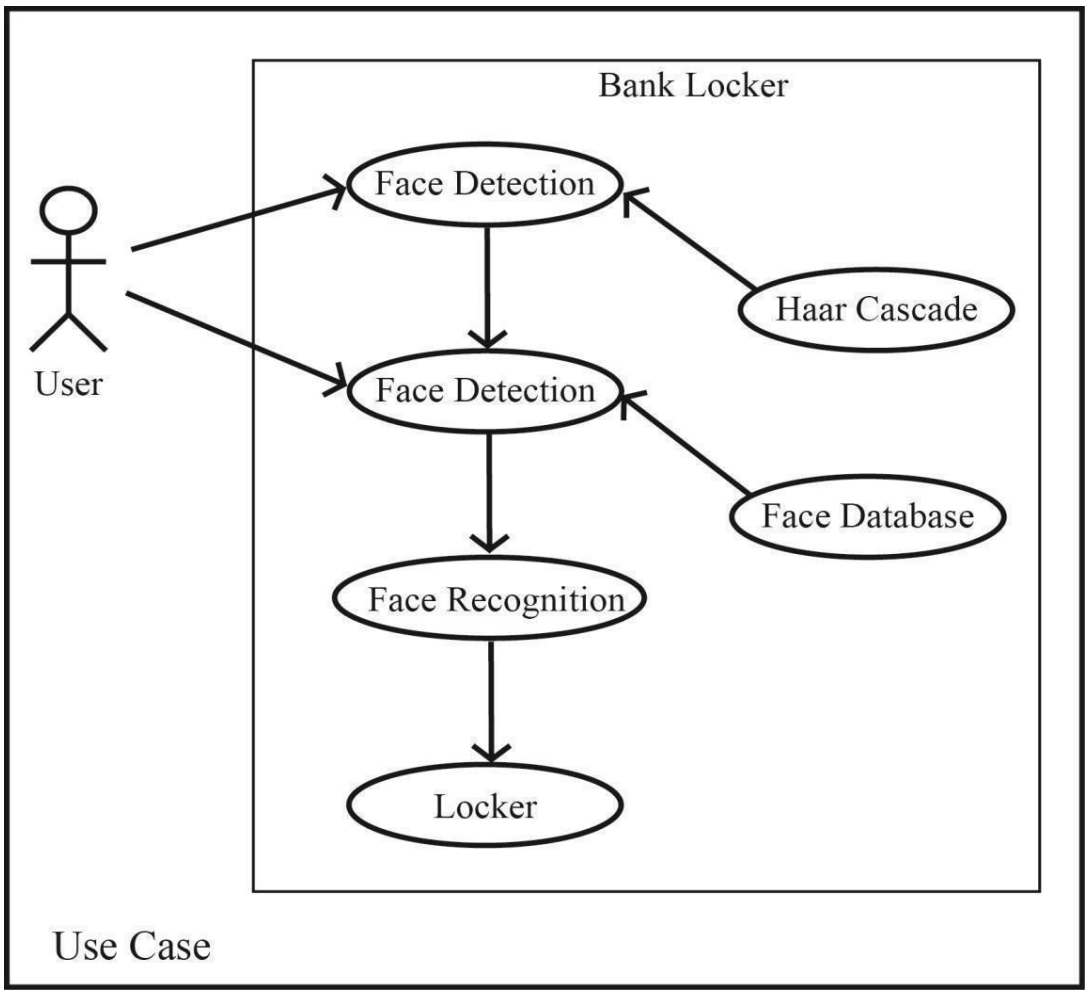


Fig no. 3. User Case Diagram

3.3.3 Class Diagram

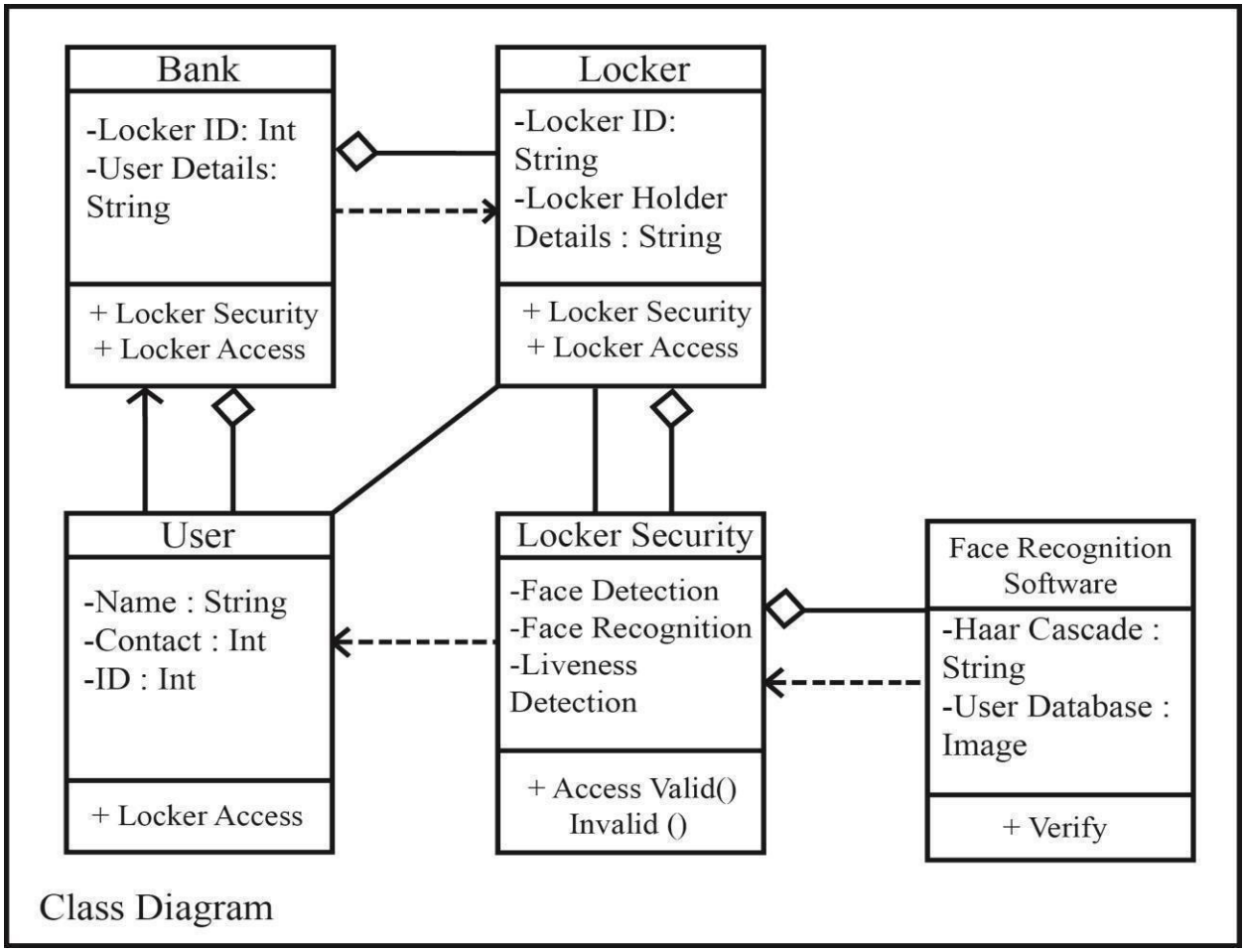


Fig no. 4. Class Diagram

CHAPTER 4

SOFTWARE AND HARDWARE REQUIREMENTS

4 SOFTWARE AND HARDWARE

4.1 SOFTWARE AND HARDWARE REQUIREMENTS

This project is divided into three modules Model 1, Model 2, Model 3.

Model 1 deals detection of face, face reorganization using camera and creating database of user's face.

Model 2 deals with liveliness detection of user can be achieved by eye blinking detection algorithm

Model 3 include access control achieved based on face & liveliness Detection.

4.2 FUNCTIONAL REQUIREMENTS

4.2.1 System Feature 1

In this system first action is face is detected using web camera. Then the camera will be interfaced to locker which will be controlled by python interface. Facial Landmarks can be used to detect Face of person.

4.2.2 System Features 2

In this system the second action is face recognition and liveness detection. Neural Network can be trained to recognize faces of user. Eye blink detection algorithm can be used to detect liveliness.

4.2.3 System Feature 3

In this system the final action is to give access to user for bank locker. It is based on user database this information goes through classification if face is known then give bank access to user. If user face is unknown based on data base it will decide either give bank access to user. Finally access control is achieved based on face & liveliness Detection.

4.3 EXTERNAL INTERFACE REQUIREMENTS

4.3.1 User Interface

In this system user interface will be a webpage where user can access bank locker by using HTML, CSS a webpage is designed.

4.3.2 Hardware Interface

Hardware interfaces are camera of used for face detection.

4.3.3 Software Interface

Implementation is done using python programming language with the help of machine learning algorithm.
Webpage is developed using html, CSS, JavaScript.

4.3.4 Communication Interface

Communication between camera and monitor is done by machine learning. In this project first face detection is done using camera then some pre-processing techniques face is recognized then based on data base user will meet bank locker access.

4.4 NON-FUNCTIONAL REQUIREMENTS

4.4.1 Performance Requirements

System should detect user's face.

Image should be capture within 2secs.
System should process the capture image using desktop

System should recognize person face based on database.

System should detect liveness of any person.

According system requirement use algorithm.

4.4.2 Safety Requirements

There will be no harm done by our project to anybody so there is no need to take Safety Requirements.

4.4.3 Security Requirements

There is no need of security in our system, as it is totally working offline, and there are no chances of hacking customer information.

4.4.4 Software Quality Attributes

Reliable: This system is reliable to work under any condition.
Maintainability: It is easy to update the code according to the future requirements.

Usability: This model is totally user friendly, as customer is going to interact with camera and monitor.

Flexible: This model is flexible to modify, we can increase number of user data base.

4.5 SYSTEM REQUIREMENTS

4.5.1 Software Requirements

Visual Studio Code

Arduino IDE

Python IDLE

4.5.2 Hardware Requirements

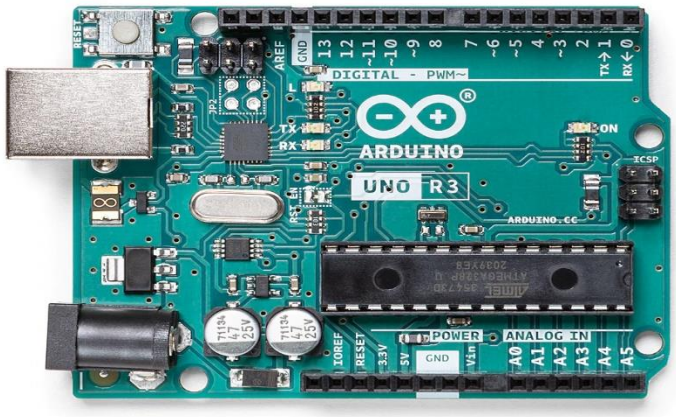
Arduino UNO

Servo Motor SG90

Laptop

4.6 HARDWARE AND SPECIFICATIONS

4.6.1 ARDUINO UNO



Arduino Uno is a microcontroller board based on the ATmega328p (datasheet). It has14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator (CSTCE16M0V53-R0), a USB connection, a power jack, an ICSP header and a reset button.

- Microcontroller: ATmega328P
- Operating Voltage: 5V
- Input Voltage (recommended): 7-12V
- Inout Voltage (limit): 6-20V
- DC Current per I/O Pin: 20 mA
- DC current for 3.3V Pin: 50 mA
- Flash Memory: 32 KB (ATmega328P)
- SRAM: 2 KB (ATmega328P)
- EEPROM: 1 KB (ATmega328P)
- Clock Speed: 16 MHz
- LED_BUILTIN: 13
- Length: 68.6 mm Width: 58.4 mm Weight: 25 g

4.6.2 SERVO MOTOR (SG90)

The servo motor is used in robotics to activate movements, giving the arm to its precise angle. The Servo motor is used to start, move and stop conveyor belts carrying the product along with many stages.

- Torque: 2.0kg/cm(4.8V), 2.2kg/cm(6V)
- Speed: 0.09s/60°(4.8V), 0.08s/60°(6V)
- Rotate angle: 180°
- Operating voltage: 4.8 ~ 6V
- Gear: plastic
- Dead band: 7us
- Weight: 10.5g
- Dimension: 22.8mm × 12.2mm × 28.5mm

CHAPTER 5

PROJECT IMPLEMENTATION

5 PROJECT IMPLEMENTATIONS

5.1 OVERVIEW OF PROJECT MODULES

5.1.1 Model 1

Algorithm for Image capturing and identification –

F1: Process the captured Image and identify attributes in the image.

Algorithm: capture image, identify attributes

Input: image

Output: Attributes in image

C={wi}Where C is the dataset of objects and human images(wi).

Steps:
Capture Images of customers.

Store the customers image

Processing the captured image

Matching the image with the images in the dataset

5.1.2 Model 2

Algorithm for displaying of ads

Algorithm: Sending image

Input: Attributes from captured image

Output: Ads to display device

Steps:

Fetch the ads

Display the ads for different person in regular interval

5.1.3 Model 3

Algorithm for image matching

Input: Captured Image at entry and exit point.

Output: Delete the captured image of entry point.

Steps:

Capture image at exit point.

Matching the image with the images of entry point.

Delete the matching image from both the Camera storage.

5.2 TOOLS AND TECHNOLOGIES USED

Tools: - Arduino

UNO

Servo Motor

Technologies: -

CNN

OpenCV

Image matching algorithm

Python

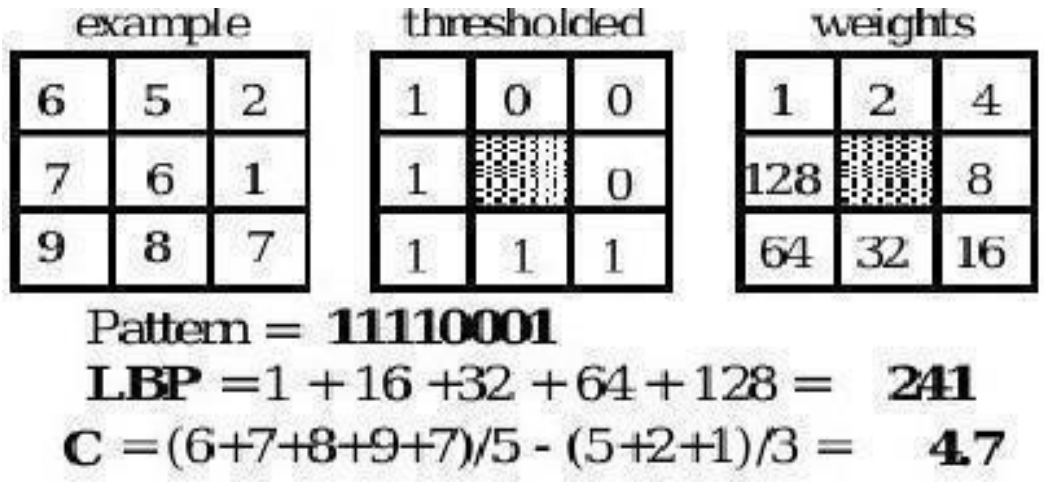
HTML

CSS

5.3 ALGORITHM DETAILS

5.3.1 CNN Algorithm

- It is used to determine the local features in the face.
- It works by using basic LBP operator. in a matrix originally of size 3×3, the values are compared by the value of the centre pixel, then binary pattern code is produced. The LBP code is obtained by converting the binary code into decimal one



- **LBP Histograms (Local Binary Pattern)-**

Each pixel of an image is labeled with an LBP code . First it will divide the image to several blocks. Then it will start calculating the LBP histogram for each block after that it will combine every LBP histogram for that image then you will get all the LBP histograms into one vector. Flowchart of LPBH –

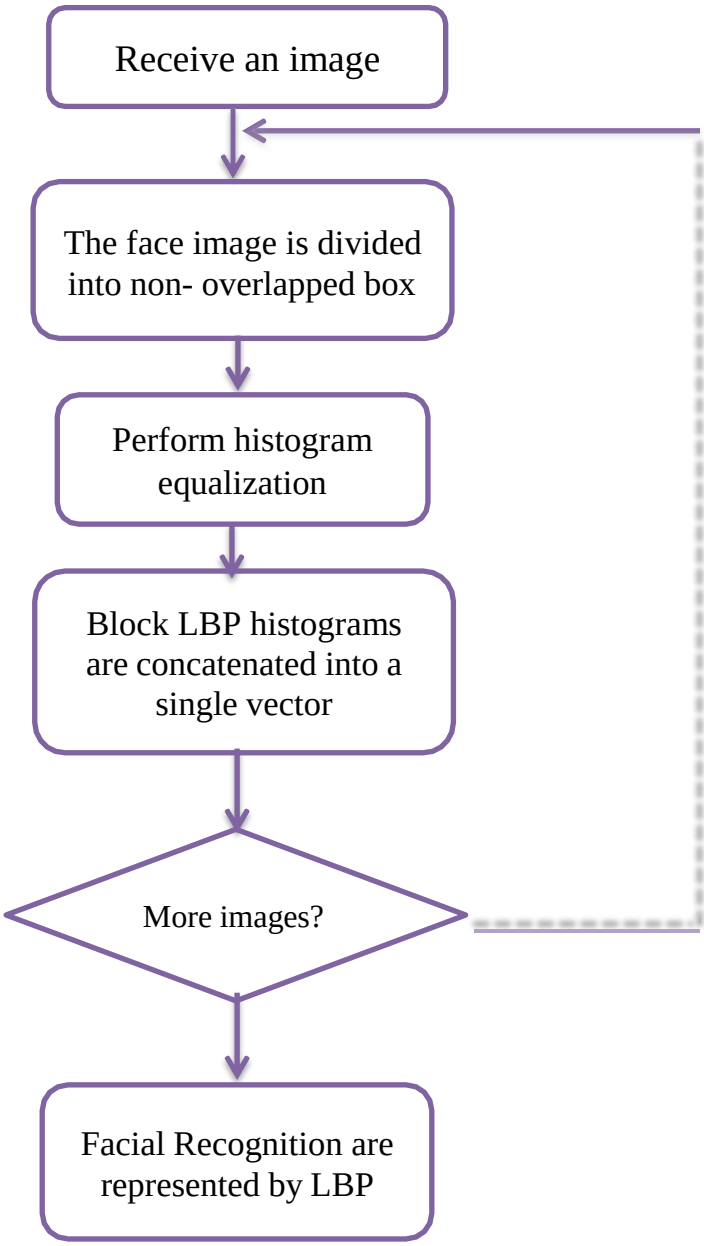


Fig no. 5. Flowchart of LPBH

1. Capture an image then store it.
2. The process will divide the image to several blocks.
3. Histograms will be calculated for each block, then a histograms will be concentrate into a single vector.

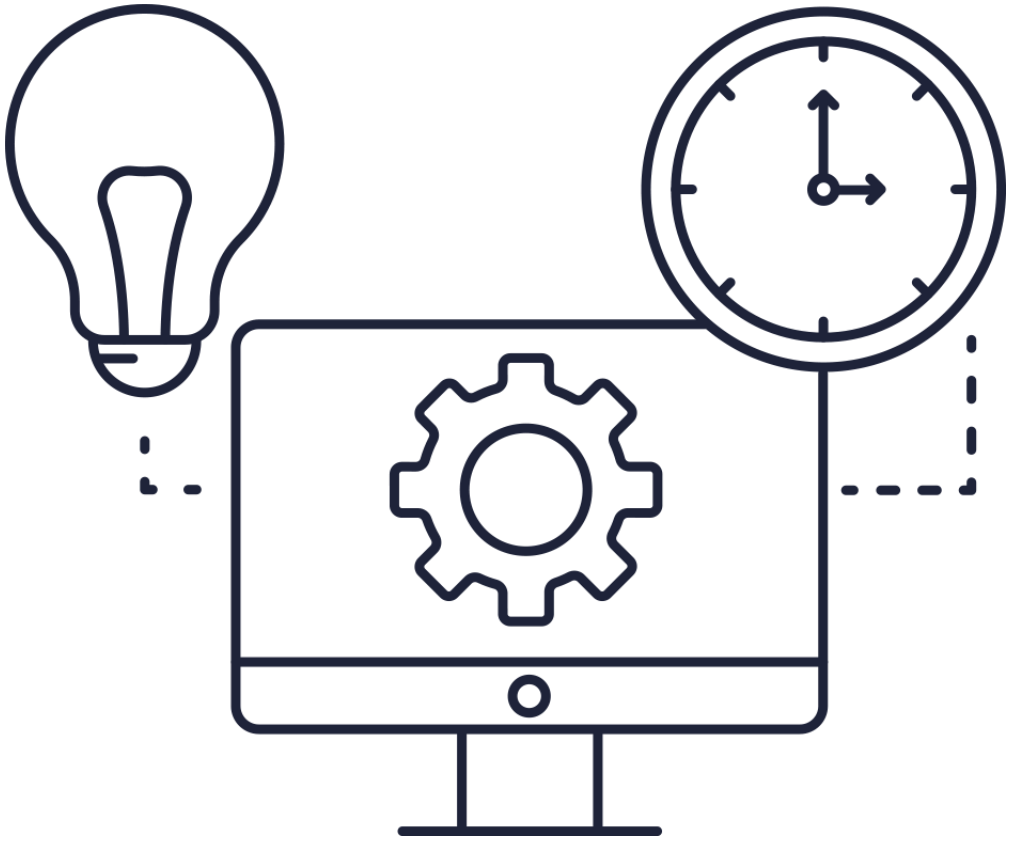
4. As a result, the facial recognition is represented by LBP and the shape of the face is obtained by concentration of different local histograms.

5.3.2 Modules

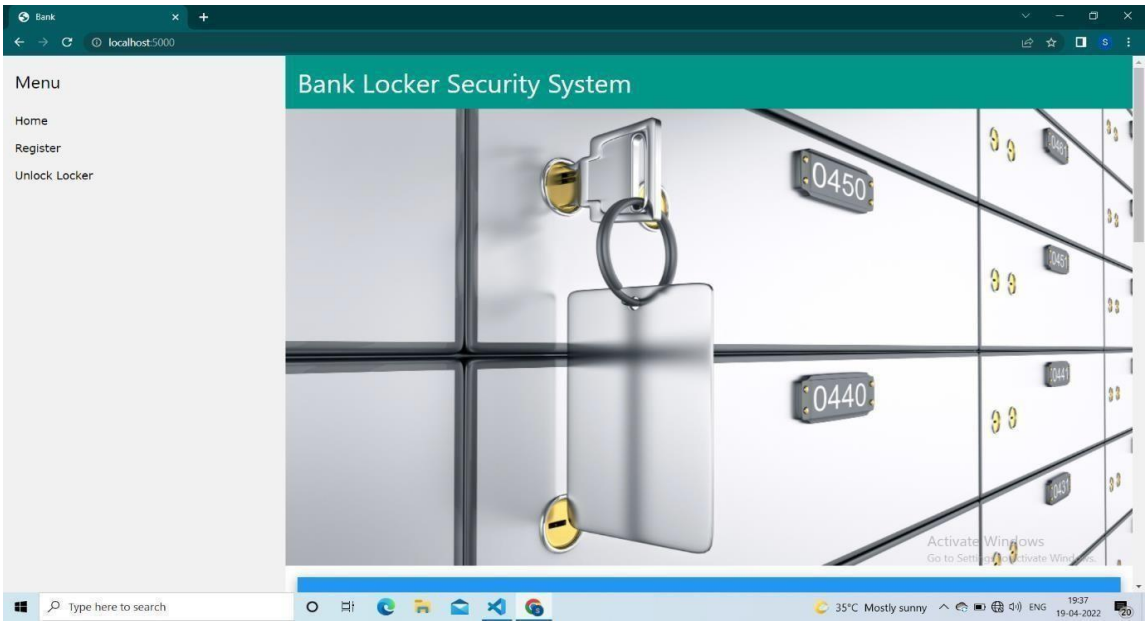
- **Image Acquisition:**
  The camera will be interfaced to locker which will be controlled by python interface
- **Face Detection:**
  Facial Landmarks can be used to detect Face of person
- **Face Recognition:**
  Neural Network can be trained to recognize faces of user
- **Liveliness Detection:**
  Eye blink detection algorithm can be used to detect liveliness
- **Access Control:**
  Finally access control is achieved based on face & liveliness Detection.

CHAPTER 6

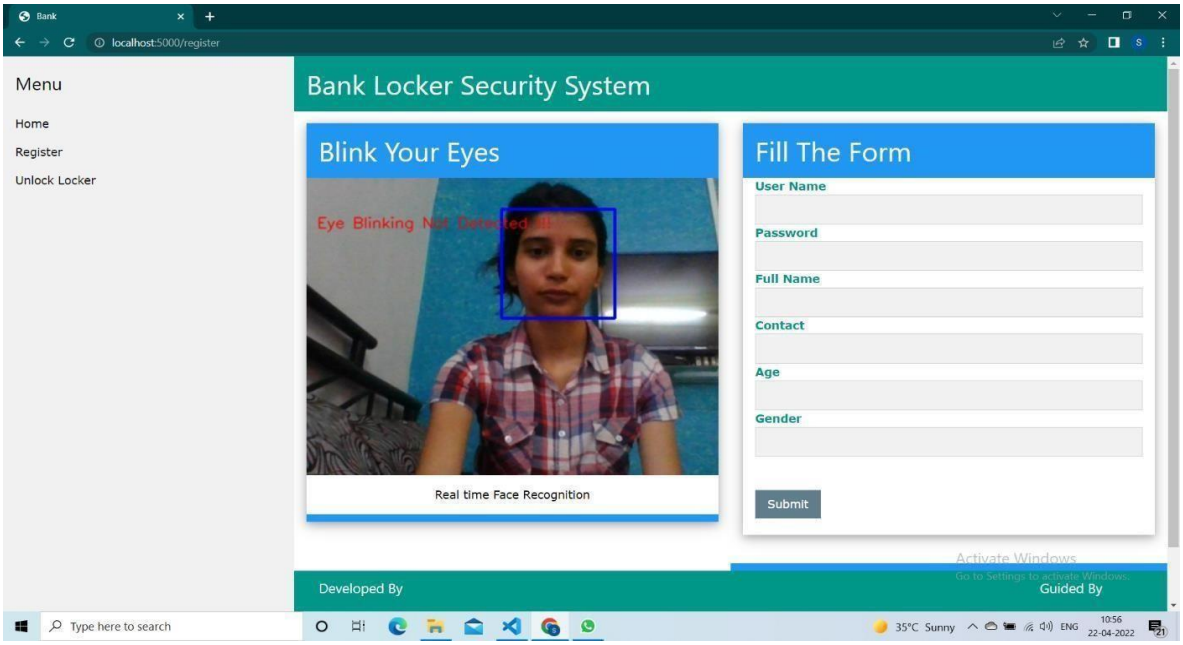
RESULTS



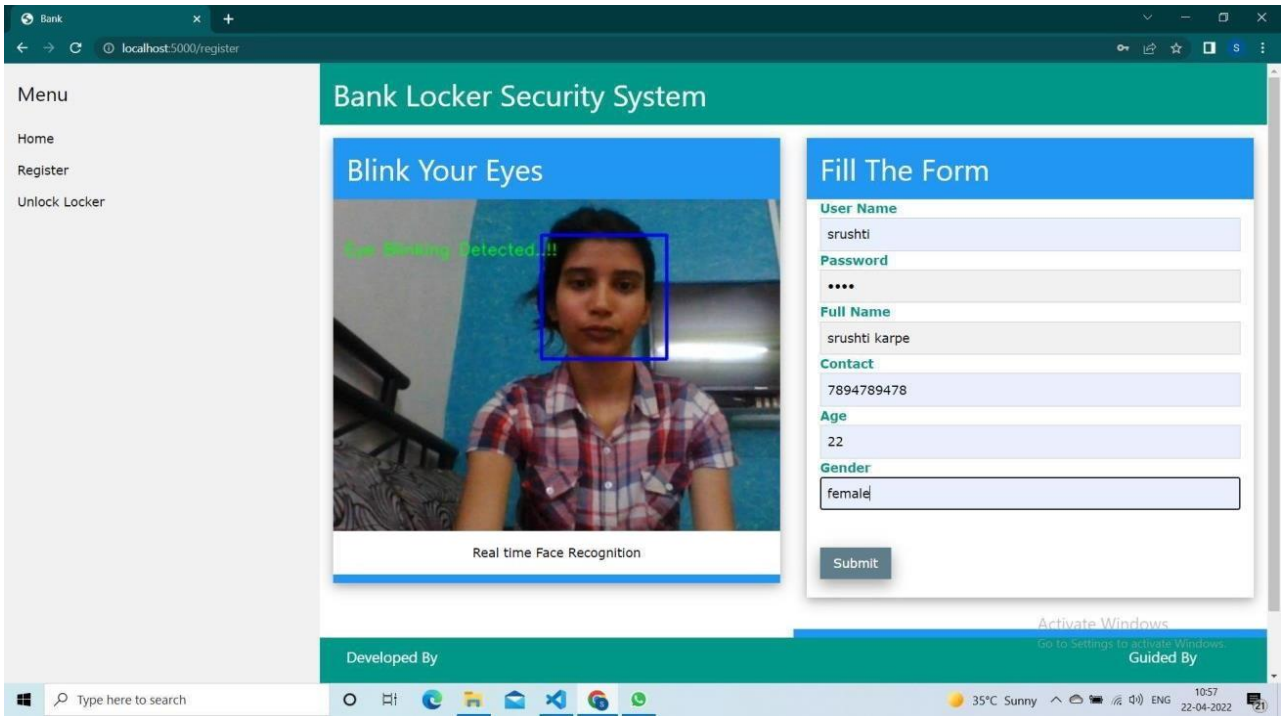
6 RESULTS



This is the dashboard of the Bank Locker Security System.



This is the registration page, where user have to register their personal information and submit the registration form.



While registration when the user blinks the eyes and submits the form, the registration is completed and his/her picture gets stored in the database.

After successful face recognition and liveliness detection access to the locker is granted.

CHAPTER 7

CONCLUSION AND FUTURE SCOPE

7 CONCLUSIONS

7.1 CONCLUSIONS

The system proposed is a machine learning based face detection-recognition and liveness detection for bank locker. In this project user will use bank locker by using face detection and liveness technique. This face detected locker is much better than traditional locker because it does not require any traditional key to unlock the locker. It is highly reliable system to ensure the security of our valuables.

7.2 FUTURE SCOPE

1. The System can be implemented in embedded processors such as Arduino UNO.
2. Additional Securities can be used such as fingerprint recognition.
3. The System can be further extended to other banking services.

7.3 APPLICATION

1. It can be used in attendance system in school or college.
2. Home security.
3. ATM security.

7.4 MERITS

1. System used for locker security.
2. Security against vulnerabilities such as spoofing, tampering, masquerade attack etc.
3. There is no retention of the template or image.
4. Improved authentication, security assurance. Maintaining Privacy and secrecy.
5. It can be implemented in large scale application and public domain with required authorization.

7.5 DEMERITS

1. The present system is less efficient in many ways.
2. The records of the customers accessing the vaults maybe lost or ruined by some external source.
3. Similarly a customer's fingerprint can be easily forged.
4. The existing system can also allow the intruders to break in easily due to it's pure security mechanism.

8 SCHEDULE

September:

- Searching for project ideas
- Finalizing the domain
- Shortlisting project topics

October & November:

- Approval of the topic
- Collected basic information related to the project
- Studying the Research Papers
- Preparing Dataset
- Training the model

December & January:

- Capturing image using OpenCV library
- Connecting camera and trained model
- Submission of Synopsis
- Submission of initial Report & PPT

February & March:

- Use of image matching algorithm
- Implementation of Software
- Developing user-interface

April:

- Implementation of Hardware
- Testing the entire model
- Final Project Report Submission

REFERENCES

[1] Sumit Sidana "Recommendation systems for online advertising",Computers and Society [cs.CY],2019

[2] T.Thiraviyam "ARTIFICIAL INTELLIGENCE MARKETING",International Journal of Recent Research Aspects,2018

[3] Daniel S´aez Trigueros "Face Recognition: From Traditional to Deep Learning Methods" ,arXiv,2018

[4] Jinesh Mehta, Eshaan Ramnani, and Sanjay Singh "Face Detection and Tagging usingDeep Learning",

International Conference on Computer, Communication, and Signal Processing(ICCCSP),2018.

[5] Srikar Appalaraju,Vineet Chaoji "Image similarity using Deep CNN and Curriculum Learning",arXiv,2017

[6] Manik Sharma, J Anuradha, H K Manne and G S C Kashyap "Facial detection using deep learning",IOP Conference Series: Materials Science and Engineering,2017

[7] Onkar Ghate, Gurunath Chavan, Krutika Dongare, Snehal Mangale "BlueTech: ABluetooth based Advertisement System for Mall",International Journal of Innovative Research in Computer and Communication Engineering,2017

[8] Daniel Fleder and Kartik Hosanagar "Recommender Systems and their Impact on Sales Diversity",EC'07 - Proceedings of the Eighth Annual Conference on ElectronicCommerce,2017.

[9] Liu, Shuangsag Fang, Yuehui Zhao, Peng Wang, Jun Zhang "Implementation of Training

Convolutional Neural Networks"arXiv,2016

[10] S. Muthuselvi and P. Prabhu "DIGITAL IMAGE PROCESSING TECHNIQUES – A SURVEY" International Multidisciplinary Research Journal,2016