**VIVEKANAND EDUCATION SOCIETY’S INSTITUTE OF TECHNOLOGY**

**Department of Computer Engineering**

A logo of a book

AI-generated content may be incorrect.

Project Report on

Querencia: Encrypted Biometric authenticated ATM System.

### In partial fulfillment of the Fourth Year (Semester–VIII), Bachelor of Engineering (B.E.) Degree in Computer Engineering at the University of Mumbai

Academic Year 2021-2022

**CHAPTER 1: INTRODUCTION**

## **Introduction**

To address the problem of security in traditional ATM systems, fingerprint as a biometric authentication is implemented in very few banks, across the globe. Very few banks in the market have access to such systems. But the cases of fingerprint forgery is noticed, which is the drawback of such systems. To overcome this drawback, we aim to provide multiple layers of security into the systems which includes a two-step encrypted biometric authentication**.** Our project aims to improvise the existing systems by introducing new technologies. It ensures ease of access to the customers and a multi-layer secured system for transactions.

## **Motivation**

DCB Bank, a private sector bank introduced an Aadhaar based ATM in Madhya Pradesh in 2016, that accepts the customer’s Aadhaar number and fingerprint impression in addition to the usual debit card. Since then no further updates were published. Under Saudi Arabia’s Vision 2030, they aim to develop a biometric ATM prototype that is undergoing the testing phase.This technology is still new in India, also concerns like remembering Aadhar card numbers, fingerprint forgery exist. Hence, we aim to develop an ingenious solution that can utilize the current system and modify it to include fingerprint scan as well as iris scan along with PIN to allow any bank transaction. This will help to increase the security of the system greatly.

## **Problem Definition**

The traditional ATM (Automated Teller Machine) system employs ATM cards with PIN to grant access for transactions. This physical system has a great risk of violation of data from theft or alteration. In India, the concept of Biometric detection based system is not widespread. The biometric data is already recorded at the banks but not used extensively. We propose the solution to develop a two-step encrypted biometric authenticated ATM system. Combining these two technologies, we can develop seamless solutions for identity management and verification that keep the ID data safe in an encrypted distributed ledger system, thereby offering consumers complete control.

## **Existing Systems**

The current system asks the customer to enter the PIN only to gain access to his/her account. If the entered PIN is correct, the person gets authenticated and gets access to the bank account. It does not include any biometric verification process.

## **Lacuna of the Existing Systems**

The existing system is not very secure due to the use of only PIN for account access.With shoulder surfing, the attacker can manage to steal the ATM pin and if he steals the ATM card as well, he can empty the bank account immediately.

## **Relevance of the Project**

The current system asks the customer to enter the PIN only to gain access to his/her account. But with attacks like shoulder surfing, the attacker can easily observe the PIN and if he somehow manages to steal the ATM card, he can empty the bank account within seconds. Hence, we felt the need to enhance the security of this traditional ATM system and add 2 more layers of security to it using biometric authentication as the biometric characteristics of an individual cannot be stolen and duplicated. Also, due to such a smart and secure system, the banks would gain the trust of their customers, thereby impacting the business of the banks positively.

**CHAPTER 2: LITERATURE SURVEY**

1. **Brief Overview of Literature Survey**

**Fingerprint recognition:**

By referring to the papers based on fingerprint biometric authentication technique, we concluded that the most critical phase of this process is the post processing stage of biometric authentication called Minutiae matching to uniquely identify a fingerprint.

A minutiae matching is used to find out whether minutiae points of input fingerprint image and template fingerprint are from the same finger or not.

In fingerprint matching, we not only compare these two sets of minutiae points but also consider some problems like shifting of fingerprint, rotation of fingerprint etc.

The accuracy of our system will be dependent upon the FAR and FRR scores.

**False Acceptance Rate (FAR)**: the percentage of identification instances in which unauthorised persons are incorrectly accepted.

**False Rejection Rate (FRR)**: the percentage of identification instances in which authorised persons are incorrectly rejected.

**Iris recognition**:

Papers based on iris recognition system specify that in order to uniquely identify the iris patterns in a human eye, we need to focus on the techniques like:

**Image Acquisition**: Obtaining the eye image

**Segmentation**: To locate the iris region in image

**Normalisation**: To achieve invariance to iris size, position and different degree of iris dilation for matching different iris patterns at later stage.

**Feature Extraction & Matching**:To extract as many discriminating features as possible from the iris and result in an iris signature, or template, containing these features.

1. **Related Works**

## **Research papers**

### Overview of Fingerprint Recognition System:

*Ali, Mouad & Mahale, Vivek & Yannawar, Pravin & Gaikwad, Ashok. (2016). Overview of Fingerprint Recognition System. 10.1109/ICEEOT.2016.7754902. [2]*

* + - 1. Abstract of the research paper:

The paper throws light on the recent studies on the fingerprint recognition system and explains its conceptual as well as structural details including the four stages of fingerprint recognition process and the summaries of fingerprint databases along with their characteristics.

* + - 1. Inference drawn:

The paper gave an overview of the fingerprint recognition process. It highlighted the details of the fingerprint recognition step by step. Also, it discussed some techniques for fingerprint recognition and then finally the summary of fingerprint databases with some characteristics.

* + 1. SECURE & ENHANCED ATM WITH BIOMETRIC AUTHENTICATION: *a J, Bhuvaneshwari. (2019). SECURE & ENHANCED ATM WITH BIOMETRIC AUTHENTICATION. [3]*
       1. Abstract of the research paper:

It aims to eliminate the use of ATM cards completely and to ensure better security.In the proposed system, the idea of using Aadhar number as user ID and fingerprint as password instead of the PIN number is discussed. After biometric verification, the user will be allowed to proceed with the transaction. In case of three successive wrong attempts, the account will be blocked. The main motive is to replace the traditional insecure ATM transaction scheme using PIN which can be misused easily with a modern and a more secure biometric authentication scheme.

* + - 1. Inference drawn:

The proposed system is highly suitable for all kinds of banking applications and is highly reliable to deal reliably with security-related problems.

### Iris recognition techniques: A Literature Survey:

*Nithya, Alice & Lakshmi, C.. (2015). Iris recognition techniques: A Literature Survey. International Journal of Applied Engineering Research. 10. 32525-32546. [4]*

* + - 1. Abstract of the research paper:

This paper provides a timeline review of various iris recognition techniques, developed since 1993. It also talks about the iris recognition framework and iris databases.

* + - 1. Inference drawn:

Though the iris recognition techniques are now getting more sophisticated, there is more research to be carried out for implementing such robust methods in border security systems, access control systems, immigration checking systems, etc.

### Fingerprint Recognition Using Minutiae Score Matching

*Ravi, J. & K B, Raja & K R, Venugopal. (2010). Fingerprint Recognition Using Minutiae Score Matching. CoRR. abs/1001.4186. [5]*

1. Abstract of the research paper:

This paper discusses the fingerprint recognition methodology using minutiae score matching algorithm (FRMSM) and also the block filter method for fingerprint thinning.

1. Inference drawn:

The FRMSM method has shown better accuracy than the traditional FRFNN method.

### 2.1.5 Fingerprint minutiae extraction using deep learning:

*L. N. Darlow and B. Rosman, "Fingerprint minutiae extraction using deep learning," 2017 IEEE International Joint Conference on Biometrics (IJCB), 2017, pp. 22-30, doi: 10.1109/BTAS.2017.8272678. [6]*

1. Abstract of the research paper:

The paper proposes a deep neural network for minutiae extraction for formulating a post-processing procedure to determine precise minutiae locations. It also compares its performance with other minutiae extractors.

1. Inference drawn:

Profound neural networks still have the scope of modification and adaptability in order to improve the finger impression affirmation.

### 2.1.6 A review of iris recognition algorithms:

*Ng, Richard & Tay, Yong Haur & Mok, Kai. (2008). A review of iris recognition algorithms. Proceedings - International Symposium on Information Technology 2008, ITSim. 2. 1 - 7.10.1109/ITSIM.2008.4631656. [7]*

1. Abstract of the research paper:

This paper provides a summary of major iris recognition studies. It also discusses the most famous algorithms used in different stages of iris recognition.

1. Inference drawn:

If the iris recognition algorithms are further developed and optimized for low-cost dedicated hardware, they can be used in various applications and domains.

### 2.1.7 IRIS RECOGNITION SYSTEM:

*Sevugan, Prabu & Swarnalatha, P. & Gopu, Magesh & Sundararajan, Ravee. (2017). IRIS RECOGNITION SYSTEM. International Research Journal of Engineering and Technology. [8]*

1. Abstract of the research paper:

This paper surveys the image quality of images acquired from a standard camera and recognizes the most imperative issues in this regard. The purpose of this project is to study the unique pattern of the iris in the human eye and measure the performance on the basis of various factors which introduce errors and influence the execution and accuracy of this idea like different types of noises and reflections from light sources.

1. Inference drawn:

Iris recognition systems are highly dependent on the nature of the iris images acquired and most importantly on the light level which plays an important role in determining the image quality. Other contributing factors include focus, disturbances, reflections and the level of occlusion and hindrance.

### 2.1.8 Fingerprint Recognition for Person Identification and Verification Based on Minutiae Matching:

*M. M. H. Ali, V. H. Mahale, P. Yannawar and A. T. Gaikwad, "Fingerprint Recognition for Person Identification and Verification Based on Minutiae Matching," 2016 IEEE 6th International Conference on Advanced Computing (IACC), 2016, pp. 332-339, doi: 10.1109/IACC.2016.69. [9]*

1. Abstract of the research paper:

The paper talks about the four fingerprint recognition stages but the main crux is upon the last stage of this process which is matching(identification & verification) stage to match two minutiae points by using the minutiae matcher method in which the similarity and distance measures are used. It calculates the accuracy of the system on the basis of FAR and FRR score.

1. Inference drawn:

The comparison between the two fingerprint databases FVC 2000 and FVC 2002 reveal that the accuracy of FVC 2002 is much better than the accuracy of FVC 2000. The recognition system evaluates with two factors: FAR and FRR. In this system the result of FAR is 0.0154 and FRR is 0.0137 with Accuracy equal to 98.55%.

## **2.2 Patent search**

### 2.2.1 METHOD AND APPARATUS FOR AUTHENTICATING FINANCIAL TRANSACTIONS:

US20030149661A1

Abstract of the patent:

It proposes a system for the authentication of financial transactions using a remote terminal and includes a methodology for sampling a unique biometric fingerprint pattern of the user. The captured image is digitized and forwarded to the clearing house to identify the correct account for transaction processing.

### 2.2.2 BIOMETRIC AUTHENTICATION UTILIZING UNIQUE BIOMETRIC SIGNATURES AND PORTABLE ELECTRONIC DEVICES:

US8499164B2

Abstract of the patent:

It discusses a method for user authentication at entry points using RFID tags and cellular wireless communication data and links. It also mentions the practical usage of such systems, e.g border crossing.

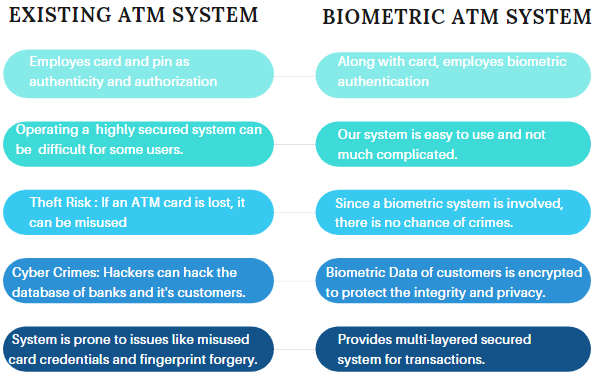
## **2.3 Inference Drawn**

The accuracy of our system will be dependent upon the FAR and FRR scores.

**False Acceptance Rate (FAR)**: the percentage of identification instances in which unauthorised persons are incorrectly accepted.

**False Rejection Rate (FRR)**: the percentage of identification instances in which authorised persons are incorrectly rejected.

## **2.4 Comparison with the Existing Systems**



**Fig. 1: Comparison of proposed system with existing system**

# **CHAPTER 3: REQUIREMENT GATHERING**

## **3.1 Introduction to Requirement Gathering**

The requirement gathering is a process of requirements discovery or generating list of requirements or collecting as many requirements as possible by stakeholders. It is also called as requirements elicitation or requirement capture.Analysts and engineers communicate with the client and end-users to know their ideas on what the software should provide and which features they want the software to include.

## **3.2 Functional Requirements**

* + - New user should be able to register his biometric characteristics in the system.
    - Users should be able to login into his account through his own PIN and biometric features.
    - Users should be allowed to seek help from the system wherever necessary.
    - Users should be shown an appropriate error/success message or any other necessary warnings and prompts wherever required.

After user authentication, user should be able to:

* + - Withdraw money.
    - Deposit money.
    - Check account balance.
    - Change account PIN.

## **3.3 Non-Functional Requirements**

* + - Availability: The system should be available for use 24\*7 ( barring the time needed for maintenance).
    - Security: User’s confidential data such as PIN and biometric characteristics must be stored in a highly encrypted form in the database.
    - Reliability: Only authenticated users should be allowed to access their own account and perform transactions.
    - Performance: Response time of the system should be good.
    - Usability: The system should have a user-friendly and easy-to-use design with clear instructions/messages to the users whenever and wherever necessary to increase the user experience.

## **3.4 Hardware, Software, Technologies and Tools Utilized**

HARDWARE:

* + - Intel i5 processor
    - Input devices: Keyboard, Infrared Camera, Fingerprint Scanning Device (R-305 module)
    - Output devices: Monitor
    - Arduino UNO
    - Male-female jumper wires
    - USB cable

SOFTWARE:

* Operating System: Windows
* Browsers: Chrome and any other web page supporting browser.
* Language: Python, Arduino

TECHNOLOGIES:

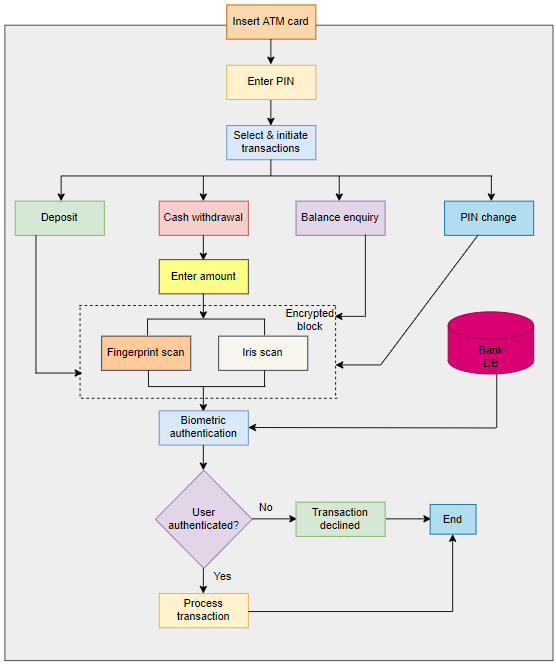
* + - Image encryption for security and authentication.
    - Image processing algorithms for minutiae and iris matching.

## **3.5 Constraints**

* + - The ATM system should have internet Connectivity.
    - For fingerprint authentication:
      * Fingers of the user should be clean.
      * Working of the system can be affected by skin conditions of people.
    - For Eye recognition:
      * Use of goggles, glass, eyelashes and contact lenses will hamper the authentication process.
      * Iris is partially blocked by eyelids which is difficult to control by individuals due to frequent blinking.
    - No IOT device being used, hence card details have to be taken manually.
    - No one other than the user can withdraw cash from the ATM.

# **CHAPTER 4: PROPOSED DESIGN**

## **4.1 Block Diagram of the System**

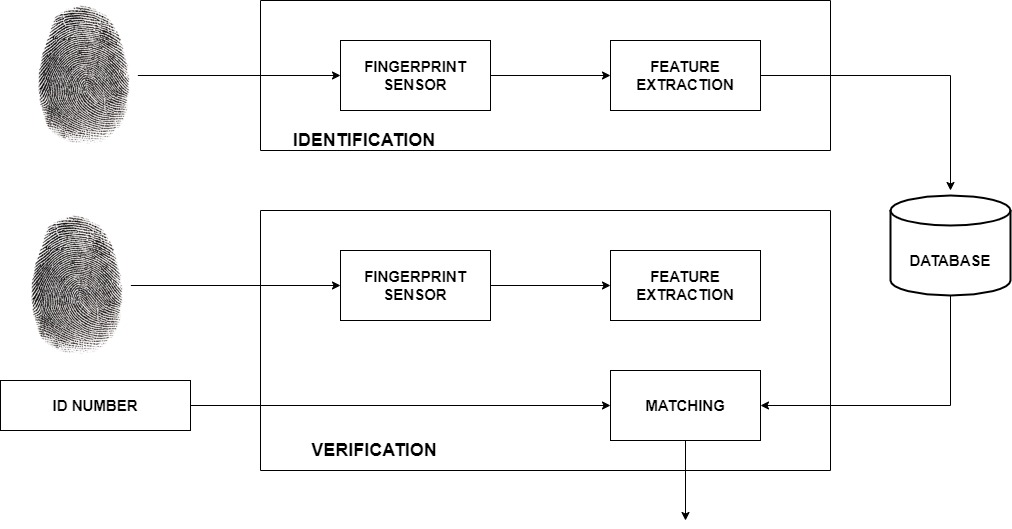


**Fig. 2: Block diagram for proposed system**

The above diagram (Fig. 2) is the Block Diagram of our proposed system. The process starts with Inserting of ATM card. Then the user will be asked to enter the PIN. After PIN matching, four different options related to the user account are provided to the user. Deposit, Cash-Withdrawal, Balance-Enquiry and PIN Change. According to the user requirements, the user will select the desired option and proceed.

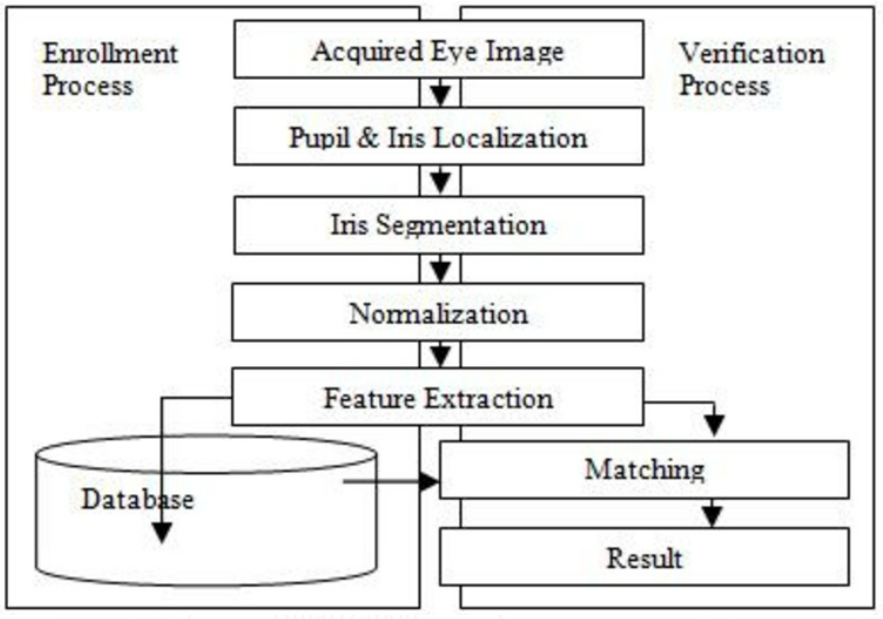
For any of the provided options that user selects, he/she will be asked to go for Biometric Authentication to proceed and Successful Biometric Matching will result in Successful transaction.

Unlike any other complicated secured systems, our system is easy to use. It is designed such that the system is convenient to use. So the user will swipe the atm card, enter a pin, select and initiate a transaction. Suppose the user chooses to withdraw some cash, then the user will enter the amount and proceed. Now the user has to scan his finger and eye through the scanner for authentication. This data will then be sent to the bank for biometric authentication. If the user is legitimate then the transaction is processed else declined.

****

**Fig. 3: Block diagram for fingerprint recognition**

The above diagram (Fig. 3) describes the working and matching of fingerprints of the user with the pre-stored biometric details of the user. The fingerprints are identified and matched with the database to check the validity of the user.

****

**Fig. 4: Block diagram for iris recognition**

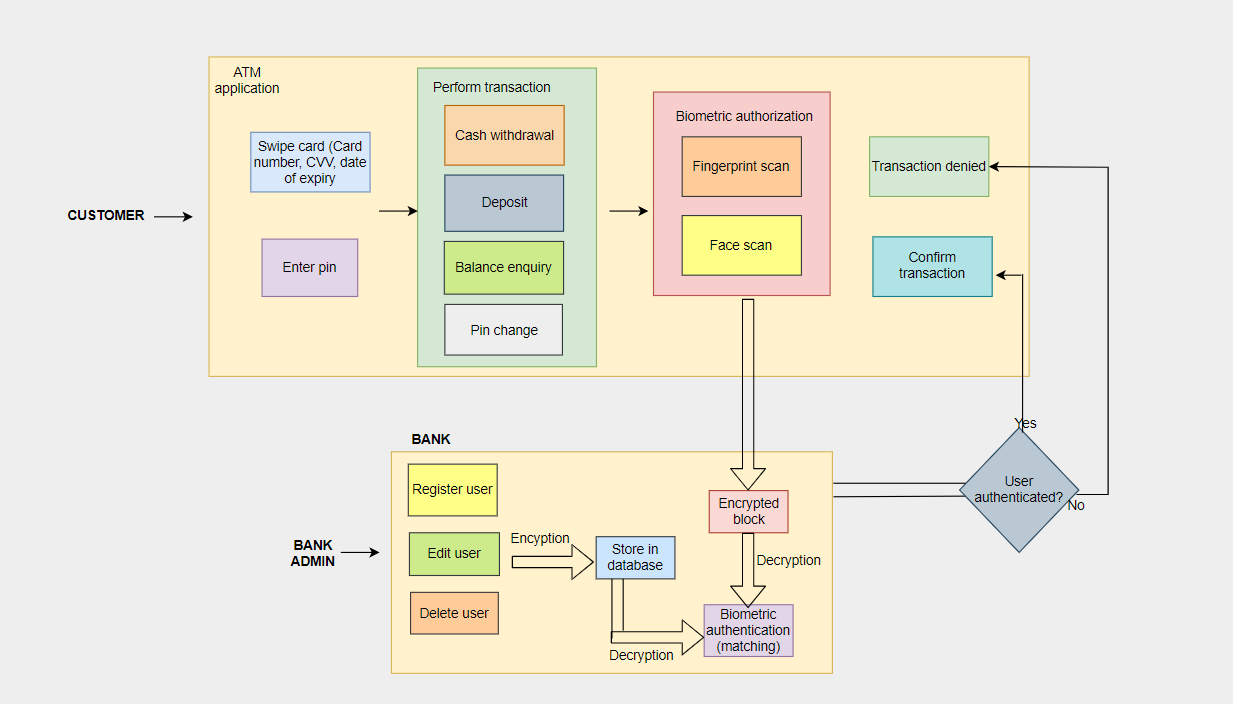
The above diagram(Fig. 4) gives an idea of the working of the Iris Recognition module. From the enrollment process to the verification process, the above diagram covers all the steps.

****

**Fig. 5: Hardware connections for interconnecting Arduino UNO with R-305 Fingerprint module**

The above diagram(Fig. 5) shows Arduino UNO, which is a low-cost, flexible, and easy-to-use programmable open-source microcontroller board that can be integrated into a variety of electronic projects. We have used arduino with the fingerprint scanner integration.

## **4.2 Modular Diagram of the System**



**Fig. 6: Modular diagram of proposed system**

Our Querencia ATM system mainly comprises of two portals:

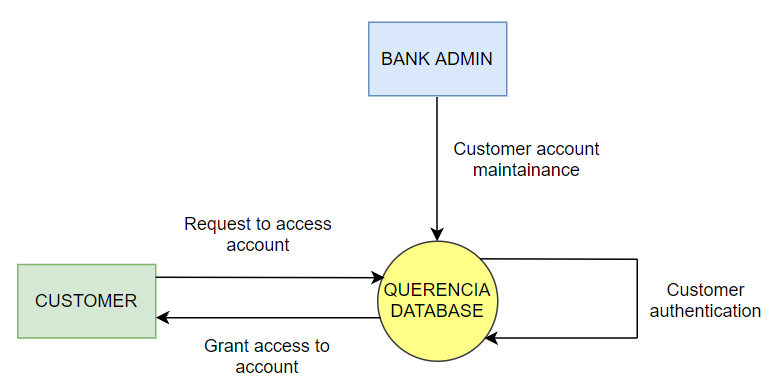
1. the admin portal at the bank
2. the ATM system at the user end.

At the admin: when a customer opens an account at the bank; complete details of the customer are stored at the banking terminal. The details also include the fingerprint and eye data. This is called the enrollment phase. Fingerprint image and image of eye is acquired and enhanced, and the features are extracted. This encrypted image is transmitted to the central banking server.

At the ATM: When a user arrives at the ATM to perform a transaction, the card credentials and the ATM pin are taken as input and verified from the database. The transaction is initiated ; Now this is the claimant phase. At the time of transaction fingerprint is acquired at the ATM terminal using high resolution fingerprint scanner and image of eye is captured using infrared scanner. These biometric images are sent for authentication. The matching of fingerprint and iris is done in the backend.The claimant and enrolled Images are compared and score matching is done. If The matching score is above the threshold value, the user is authenticated and the transaction is initiated. If the matching score is below threshold value, the user is marked invalid and the transaction is denied.

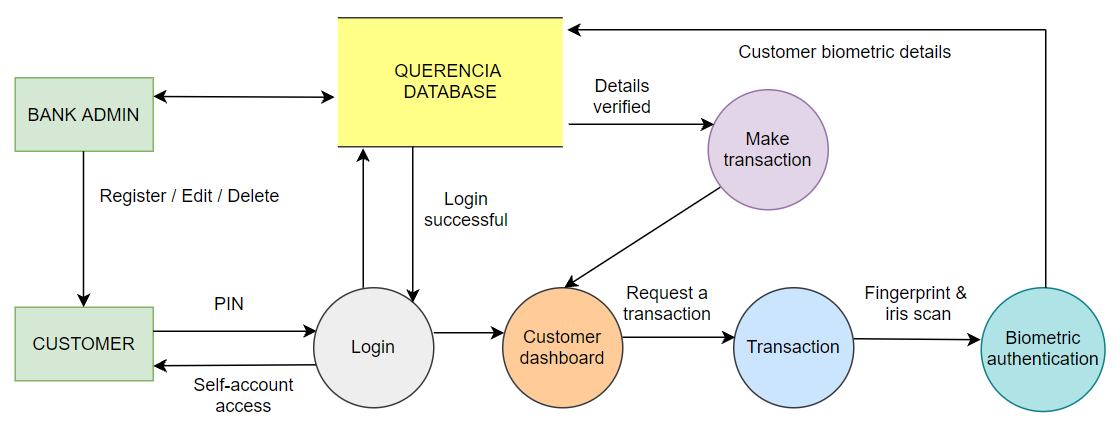
## **4.3 Detailed Design of the System**

**DATA FLOW DIAGRAMS (DFD)**



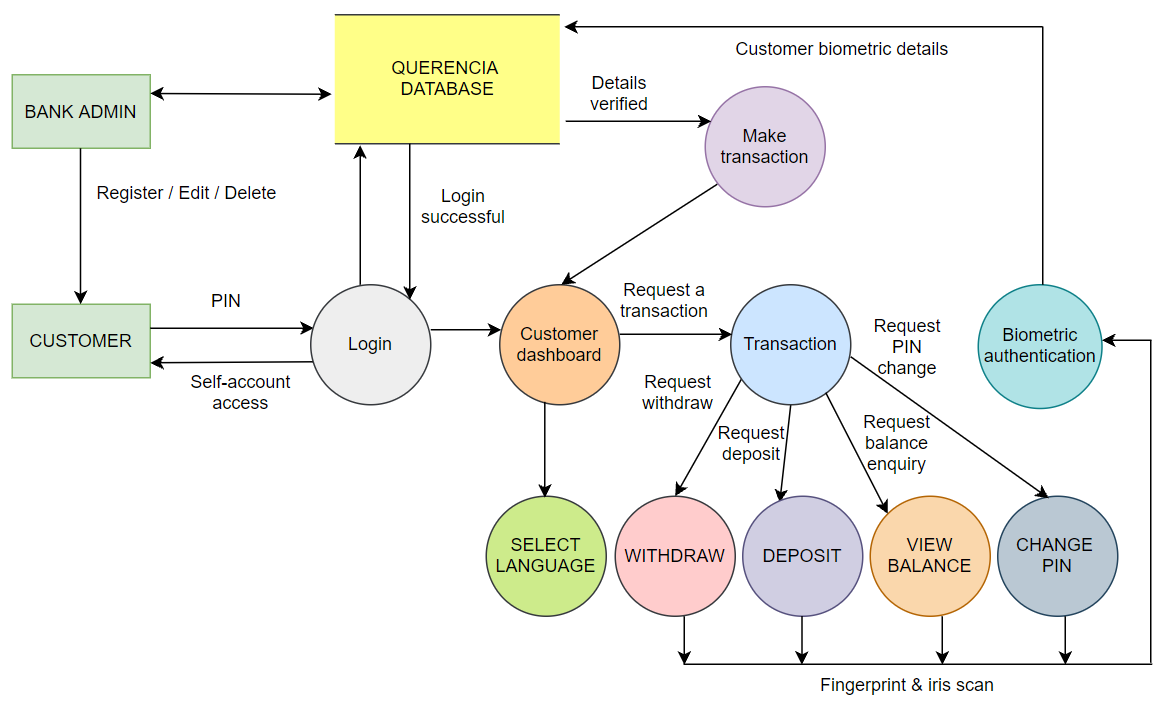
**Fig. 7: DFD level-0 diagram of proposed system**

This is the high-level diagram showing 2 entities-customer & bank admin. The customer will request account access which will be processed by the database. Upon authentication, the system will grant access to the customer. The bank admin is responsible for managing the customer accounts.

****

**Fig. 8: DFD level-1 diagram of proposed system**

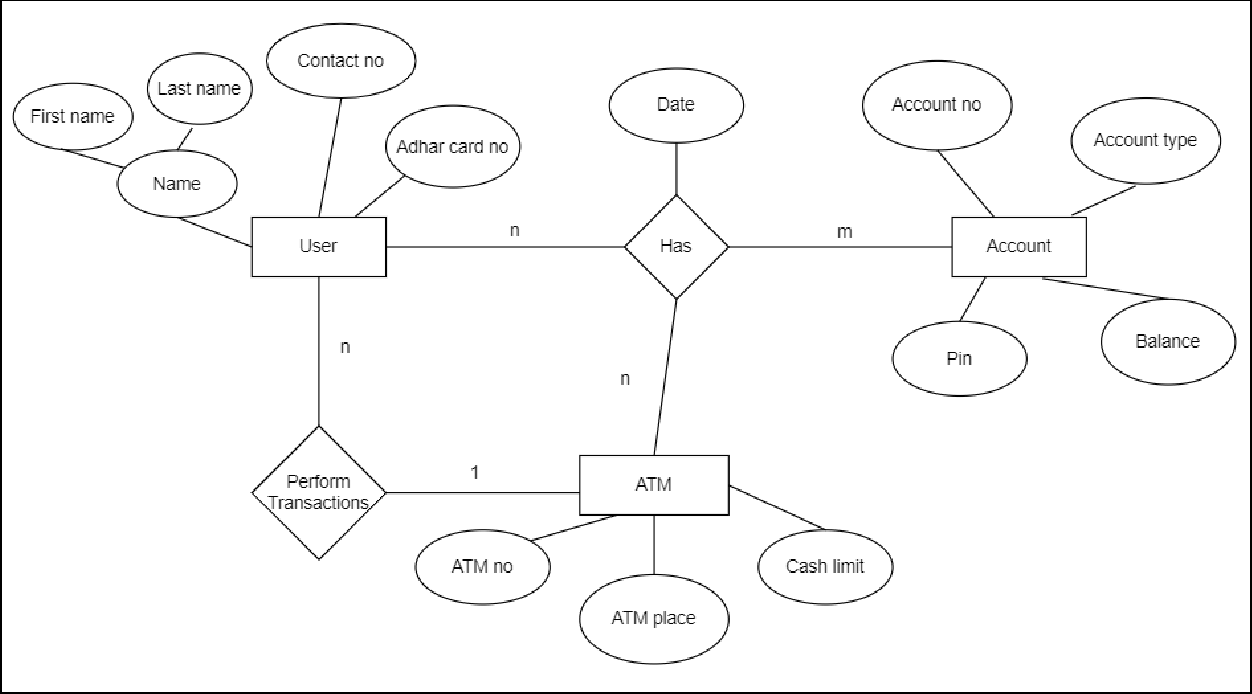
This diagram shows a more clear picture of level 0. The bank admin can register/edit/delete a customer and can communicate directly with the database.The customer will enter PIN to login into his/her account. If the PIN is correct, the customer will get access to his account and will land on the customer dashboard page. From here, the customer will make a request for a transaction and in order to complete the transaction, he/she will have to go through the biometric authentication process. Here, the customer must complete his/her fingerprint scan as well as iris scan. These details will then be processed by the database and if they match with the details which were stored at the time of registration, only then the transaction will be initiated and completed.

****

**Fig. 9: DFD level-2 diagram of proposed system**

This is the most detailed description of our system. The customer can also choose a language of his choice. In addition to level 1 flow, it also shows different transactions that can be performed by the customer like withdraw, deposit, balance enquiry and change pin. Any transaction request will be followed by biometric authentication as explained earlier.

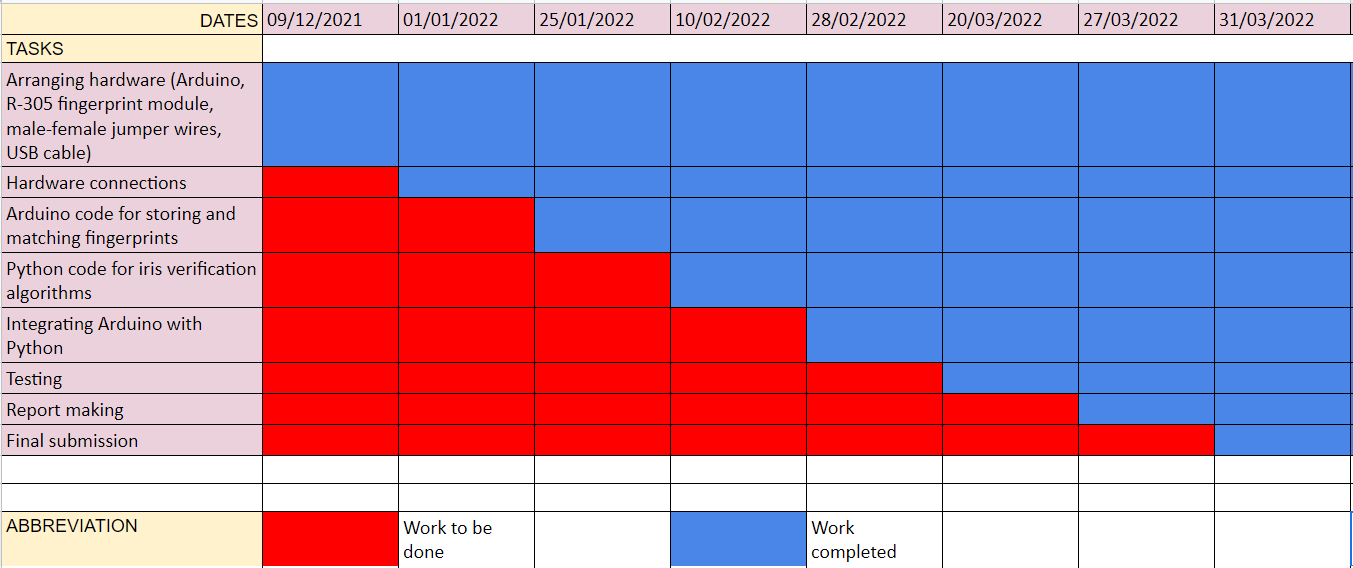
**ENTITY RELATIONSHIP DIAGRAM (ER)**

****

**Fig. 10: ER diagram of proposed system**

The ER diagram shows the entities of our system and the relationships between them. Each entity has a few attributes.

## **4.4 Gantt Chart**



**Fig. 11: Gantt chart**

As clear from the diagram given above, the project implementation took us nearly 2 months and the testing process lasted for about a month. We had divided the project plan into several tasks, handled by different team members.

# **CHAPTER 5: IMPLEMENTATION OF THE PROPOSED SYSTEM**

## 

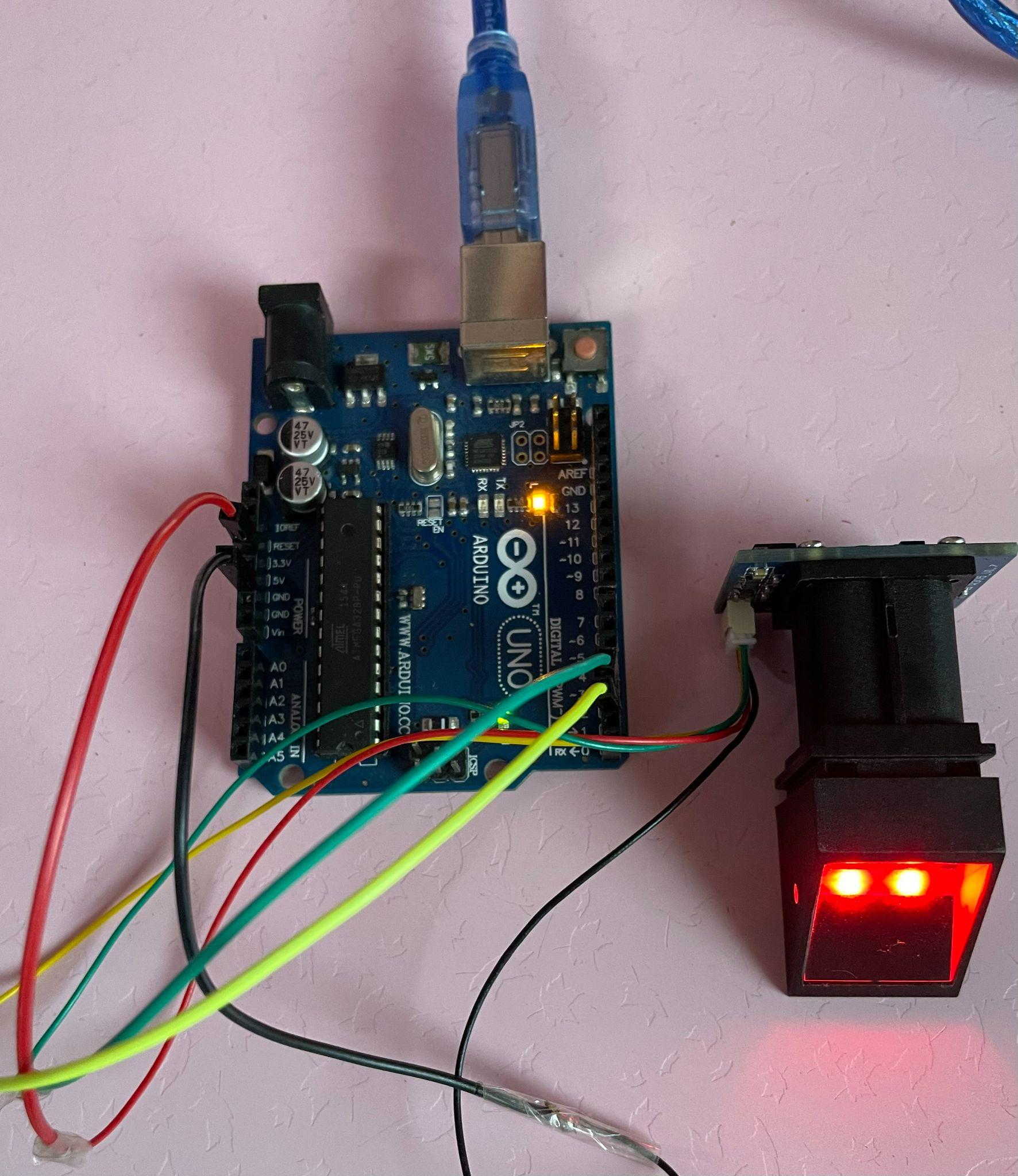
## **5.1 Methodology Employed for Development**

For Fingerprint Recognition:

We have stored a few fingerprint samples in R-305.

Fingerprint recognition:

* R-305, being the serial scanner, we have used serial communication between the scanner and the Python code.
* For every fingerprint captured by the scanner successfully, a unique fingerprint ID is assigned to it.
* The biometric fingerprints are stored securely within the scanner itself.
* We retrieve the fingerprint ID during the matching process to uniquely identify the customer.



**Fig. 12: R-305 Fingerprint Module**

For Iris Recognition:

Visible and near-infrared light scanners are used to take a high-contrast image of the user's iris.

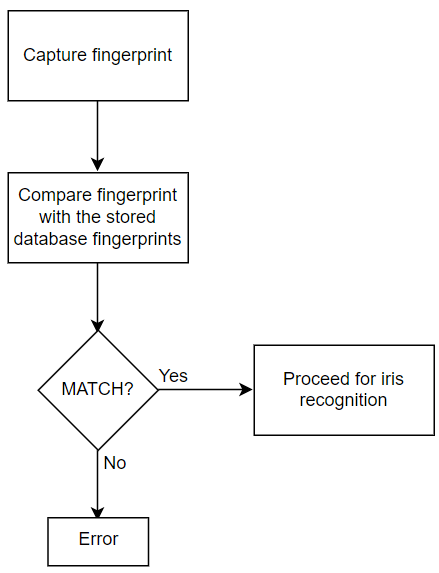
Iris recognition phases:

* Segmentation
* Normalization
* Feature Extraction
* Matching

## **5.2 Algorithms and Flowcharts for Modules Developed**

Fingerprint recognition:

1. Place the finger on the scanner when asked by the application (before performing any transaction).
2. If the finger has been placed properly, the fingerprint gets captured properly.
3. The captured fingerprint is then compared with the stored fingerprint and if a match is found, the application directs us towards iris recognition.
4. The finger must be placed firmly while registering the fingerprint to capture more details and increase the accuracy.



**Fig. 13: Fingerprint recognition flowchart**

Iris recognition:

1. Segmentation

* Hough transform(time-efficient but less accurate)

Circular hough transform is used to detect radius and center coordinates of pupil and iris region.

Parabolic Hough transform is used to deduce eyelids.

* Daugman Integro-differential operator

Time-consuming but more accurate.

Locates the iris and pupil region along with the border of the iris.

1. Normalization

* Daugman rubber sheet model

Produces the iris region by nullifying the effects of dimensional inconsistencies.

Transforms a segmented image into a fixed dimensional rectangular box and polar conversion of the iris image is done.

1. Feature Extraction

* Gabor Filter

This filter is sensitive to textures with specific orientation and wavelength.

Based on feature extraction, unique iris templates are generated.

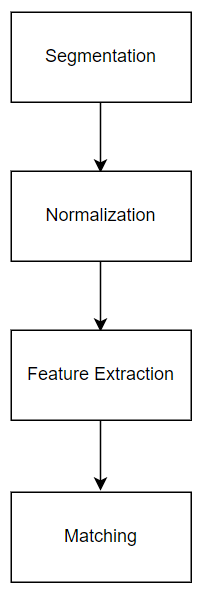
The extracted features are encoded to generate unique mathematical templates for the iris.

1. Matching:

Both the iris templates-iris template received from ATM and template stored at the Bank's database, are compared to check similarity and dissimilarity.

Bitwise comparison is performed using the Hamming distance metric.

The other proposed equations are the Weighted Euclidean distance and Canberra distance metric.

****

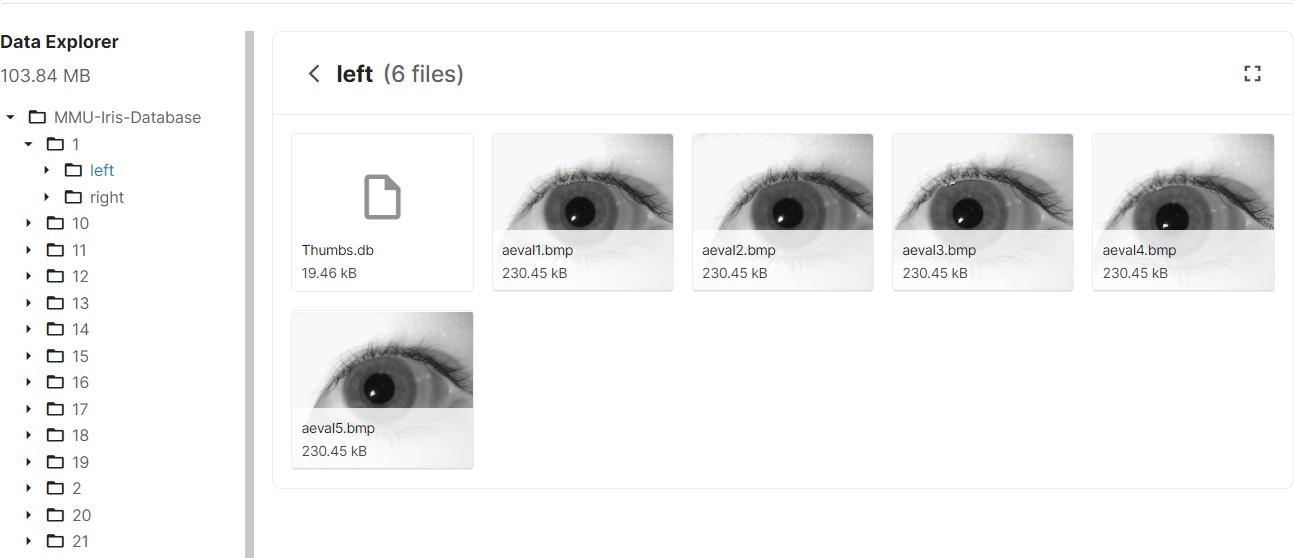
**Fig. 14: Iris recognition flowchart**

## 

## **5.3 Dataset Source and Utilization**

Iris Dataset Source: Kaggle

This Dataset consists of both 5 close-up B/W images each of the left and right eyes of 46 persons(46 directories), totaling 460 images along with a few empty files. Each directory 'i' has folders left/right that carries 5 images each of both eyes for person 'i'.



**Fig. 15: Iris dataset**

Dataset Utilization: We have used this dataset in our Iris recognition phase. After the successful matching of fingerprints, the application takes the user to the iris recognition phase. If the iris image is matched, only then the transaction is completed.

# 

# 

# 

# 

# 

# **CHAPTER 6: TESTING OF THE PROPOSED SYSTEM**

## **6.1 Introduction to Testing**

Software testing can be stated as the process of verifying and validating that software or application is bug-free, meets the technical requirements as guided by its design and development, and meets the user requirements effectively and efficiently with handling all the exceptional and boundary cases.

The process of software testing aims not only at finding faults in the existing software but also at finding measures to improve the software in terms of efficiency, accuracy, and usability. It mainly aims at measuring the specification, functionality, and performance of a software program or application.

Software testing can be divided into two steps:

1. Verification: it refers to the set of tasks that ensure that software correctly implements a specific function.

2. Validation: it refers to a different set of tasks that ensure that the software that has been built is traceable to customer requirements.

Verification: “Are we building the product right?”

Validation: “Are we building the right product?”

Software Testing can be broadly classified into two types:

1. Manual Testing: Manual testing includes testing software manually, i.e., without using any automated tool or any script. In this type, the tester takes over the role of an end-user and tests the software to identify any unexpected behavior or bug. There are different stages for manual testing such as unit testing, integration testing, system testing, and user acceptance testing.

Testers use test plans, test cases, or test scenarios to test software to ensure the completeness of testing. Manual testing also includes exploratory testing, as testers explore the software to identify errors in it.

2. Automation Testing: Automation testing, which is also known as Test Automation, is when the tester writes scripts and uses other software to test the product. This process involves the automation of a manual process. Automation Testing is used to re-run the test scenarios that were performed manually, quickly, and repeatedly.

Software techniques can be majorly classified into two categories:

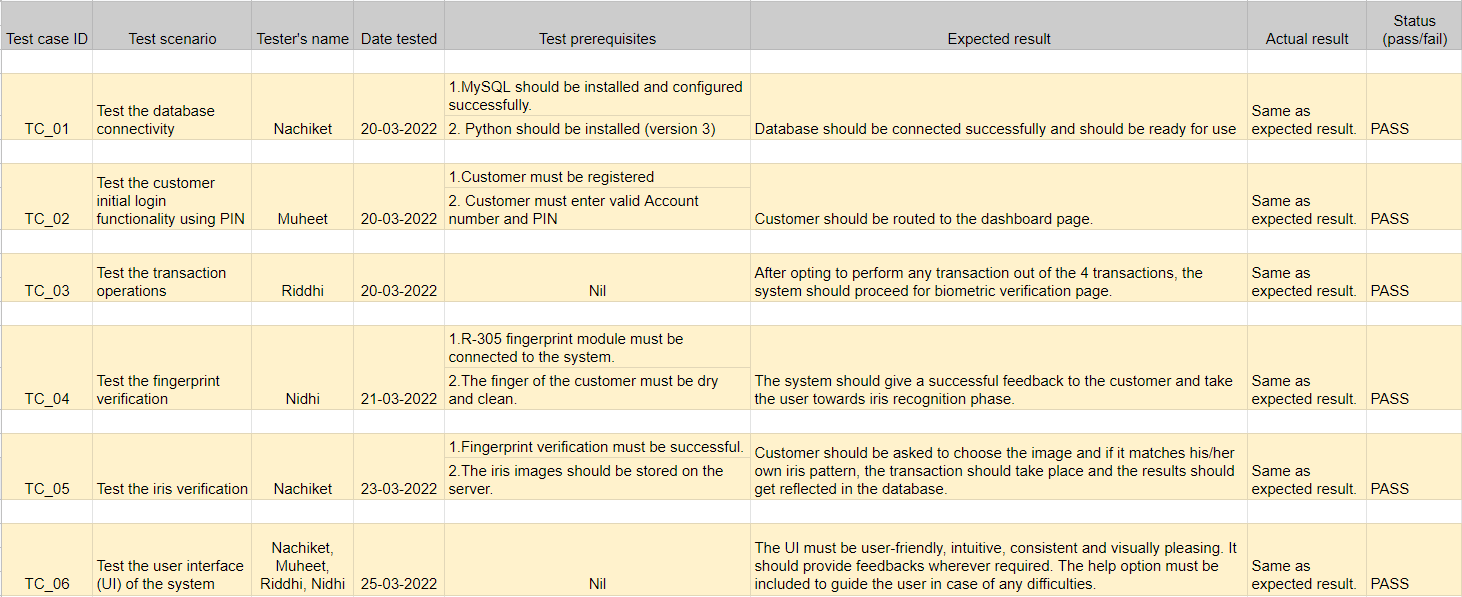
1. Black-Box Testing: The technique of testing in which the tester doesn’t have access to the source code of the software and is conducted at the software interface without concern with the internal logical structure of the software is known as black-box testing.

2. White-Box Testing: The technique of testing in which the tester is aware of the internal workings of the product, has access to its source code, and is conducted by making sure that all internal operations are performed according to the specifications is known as white box testing.

## **6.2 Types of Tests Considered**

1. Unit testing: Here, we tested the individual modules of our system such as the home page, dashboard, transaction operations, etc. These were tested one by one as they appear to the customer using our system.
2. Integration testing: Here, the individual modules developed earlier were integrated and integration issues that arose were fixed. The Arduino code was integrated with Python code and the bugs were fixed as well.
3. System testing: Although the integration of Arduino and Python was successful, some issues were not allowing the code to detect the R-305 fingerprint module. They were fixed at this stage.
4. Acceptance testing: Here, we tested the system as one unit together to check whether it was as per the requirements. It consisted of both White box as well as Black box testing.
5. Usability testing: Here, we tested the UI of the system; whether it was user friendly or not, whether the novice users could understand the system and were able to deal with it comfortably or not, whether the flow and navigation of the system was simple or not, whether the readability of the text, the colors and the visual appeal of the application in general was pleasing to the eye or not.

## **6.3 Test Case Scenarios Considered**



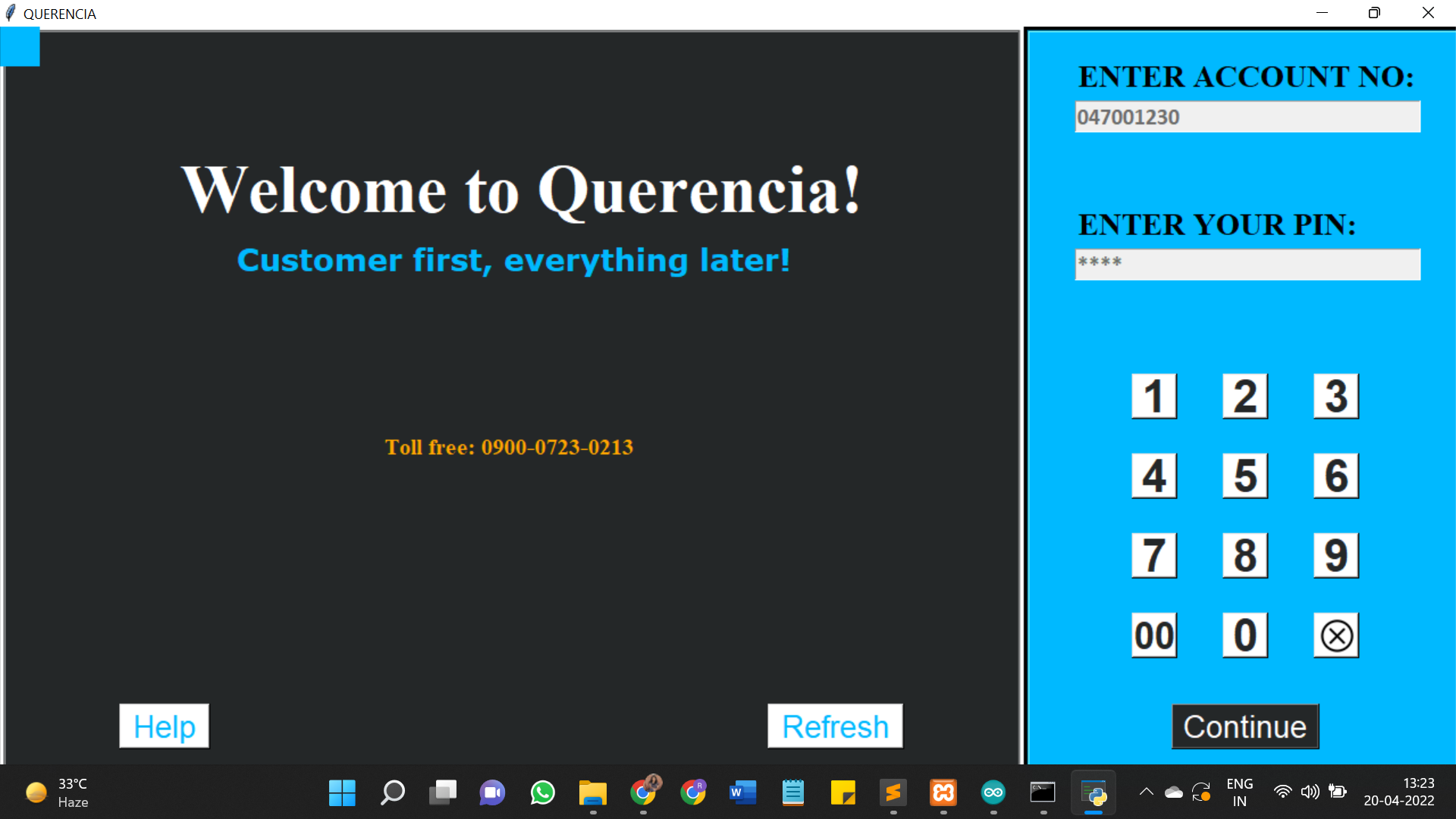
**Fig. 16: Test case scenarios**

## **6.4 Inference Drawn from Test Cases**

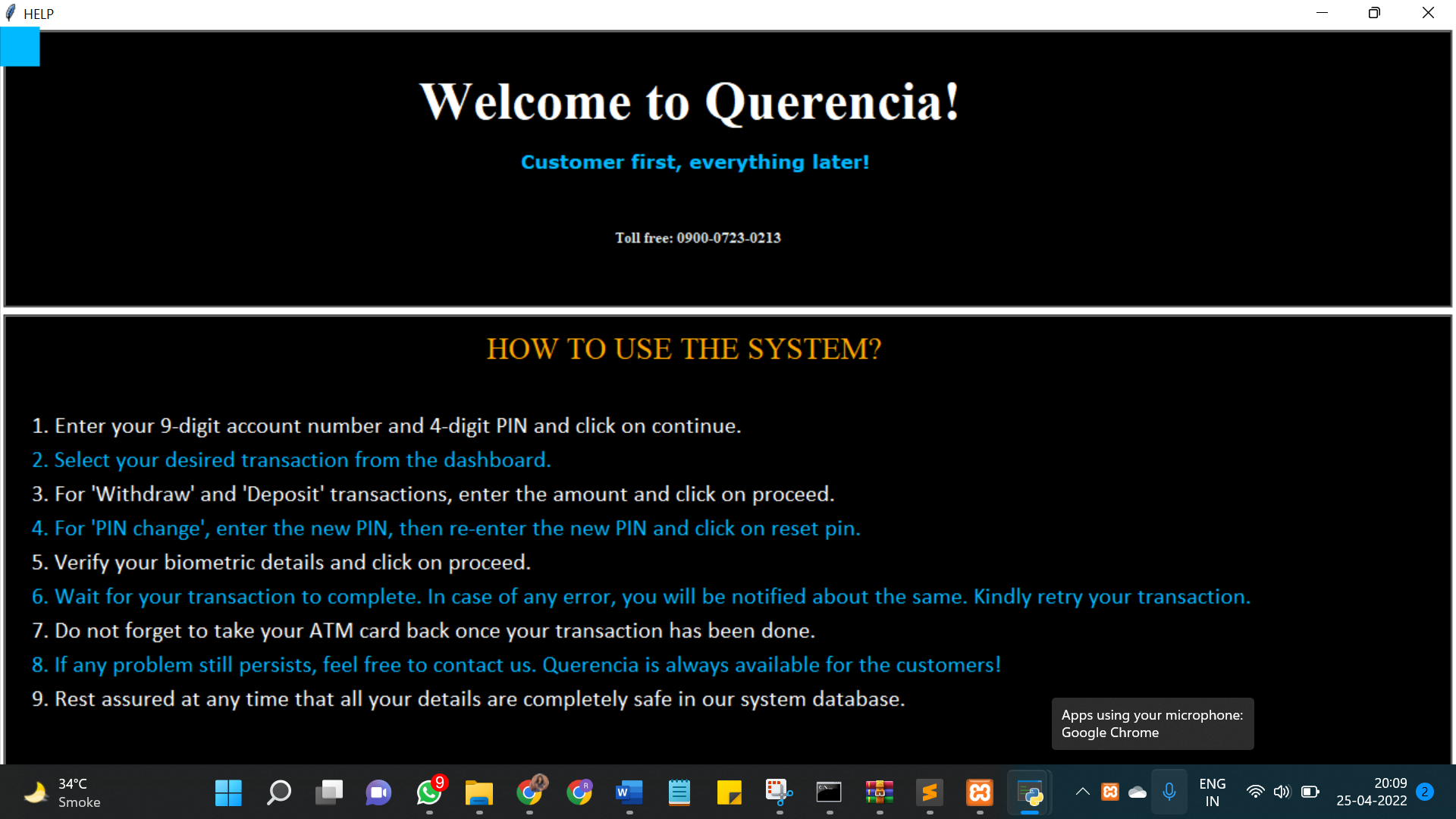
1. We carried out both Black-box testing and White-box testing on the system.
2. The system seems to be working fine for the scenarios that we tested.
3. The system is ready for use in a real-time environment.

# **CHAPTER 7: RESULTS AND DISCUSSIONS**

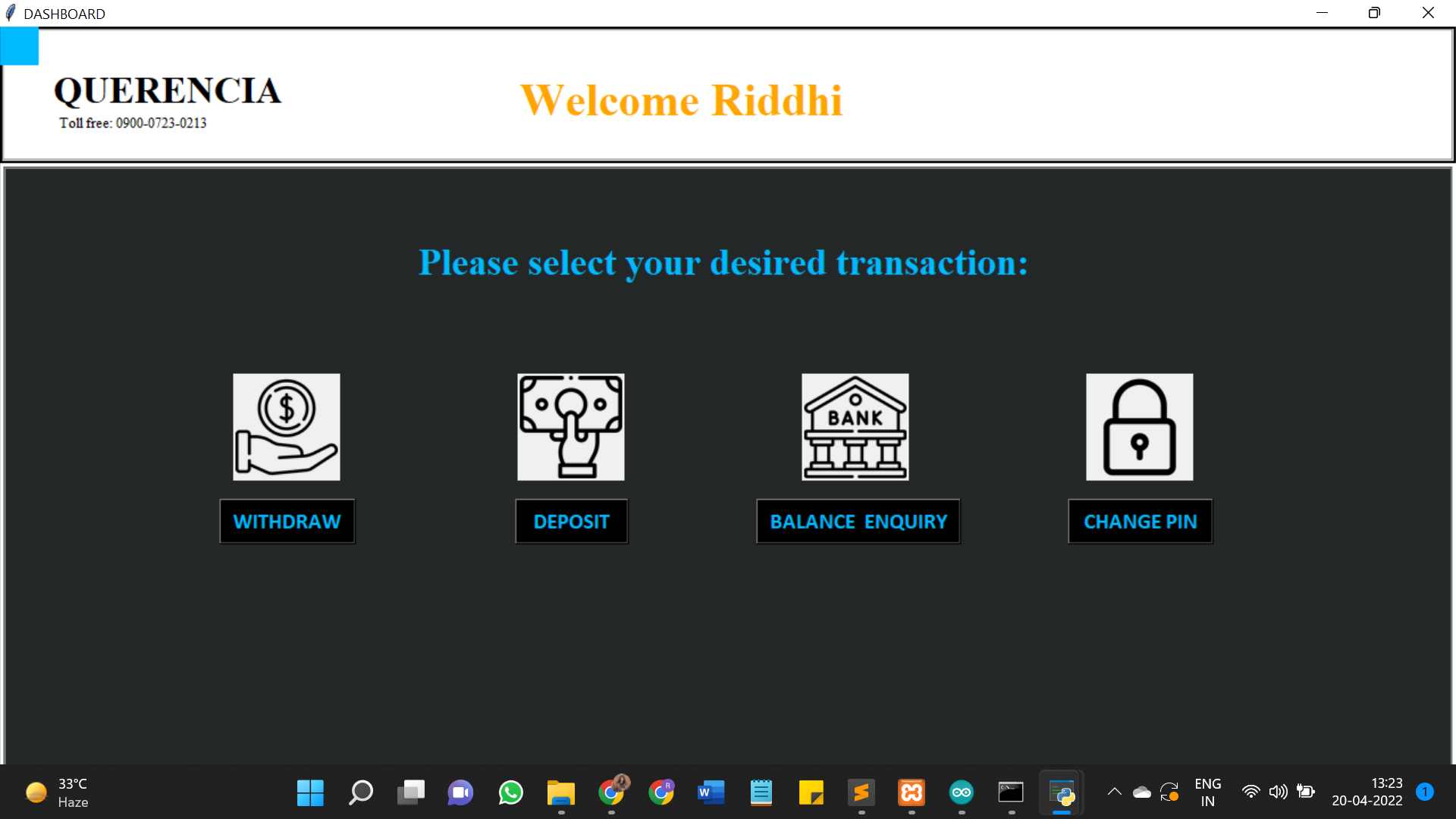
## **7.1 Screenshots of User Interface (UI)**



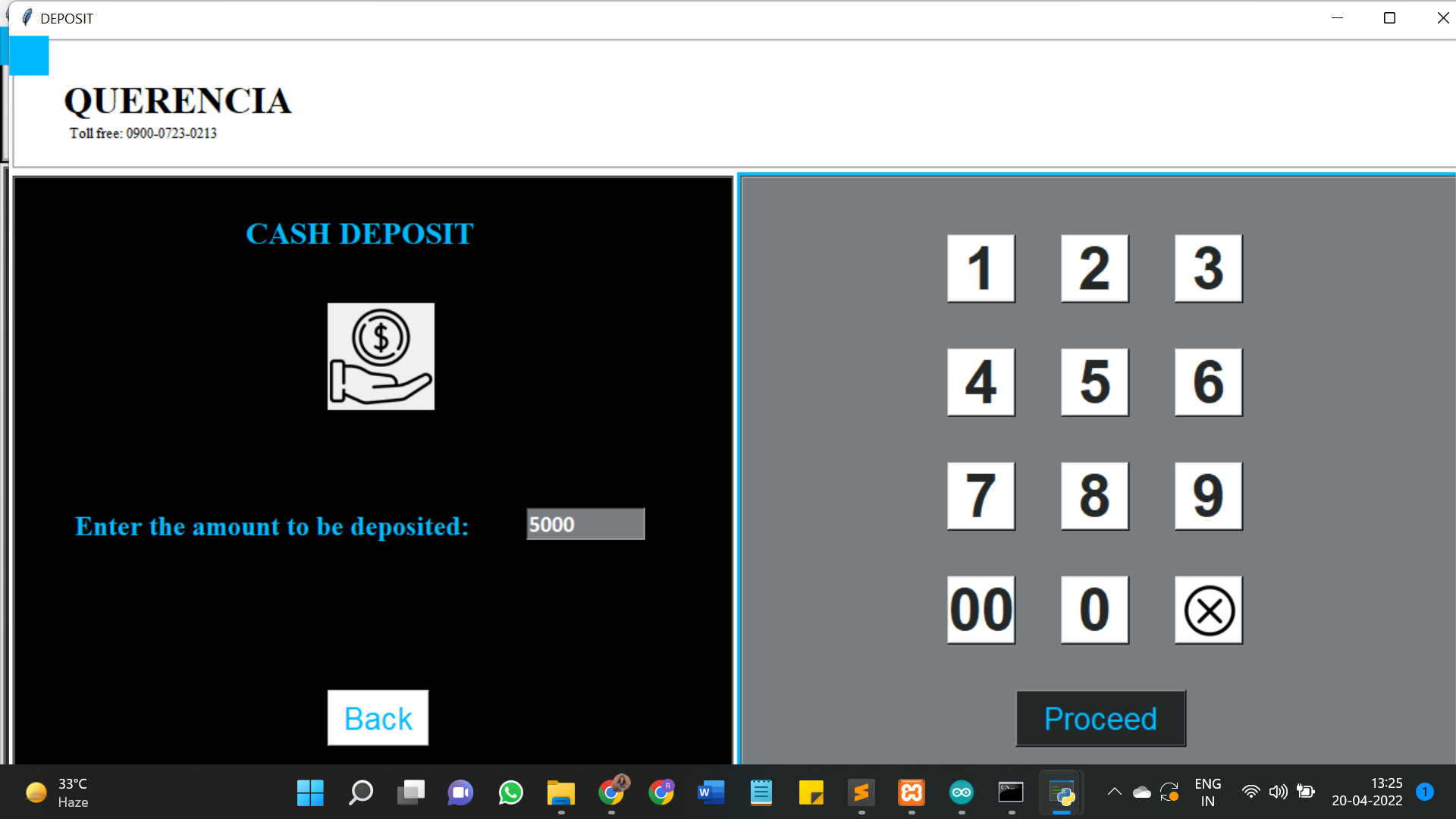
**Fig. 17: Home Screen**

****

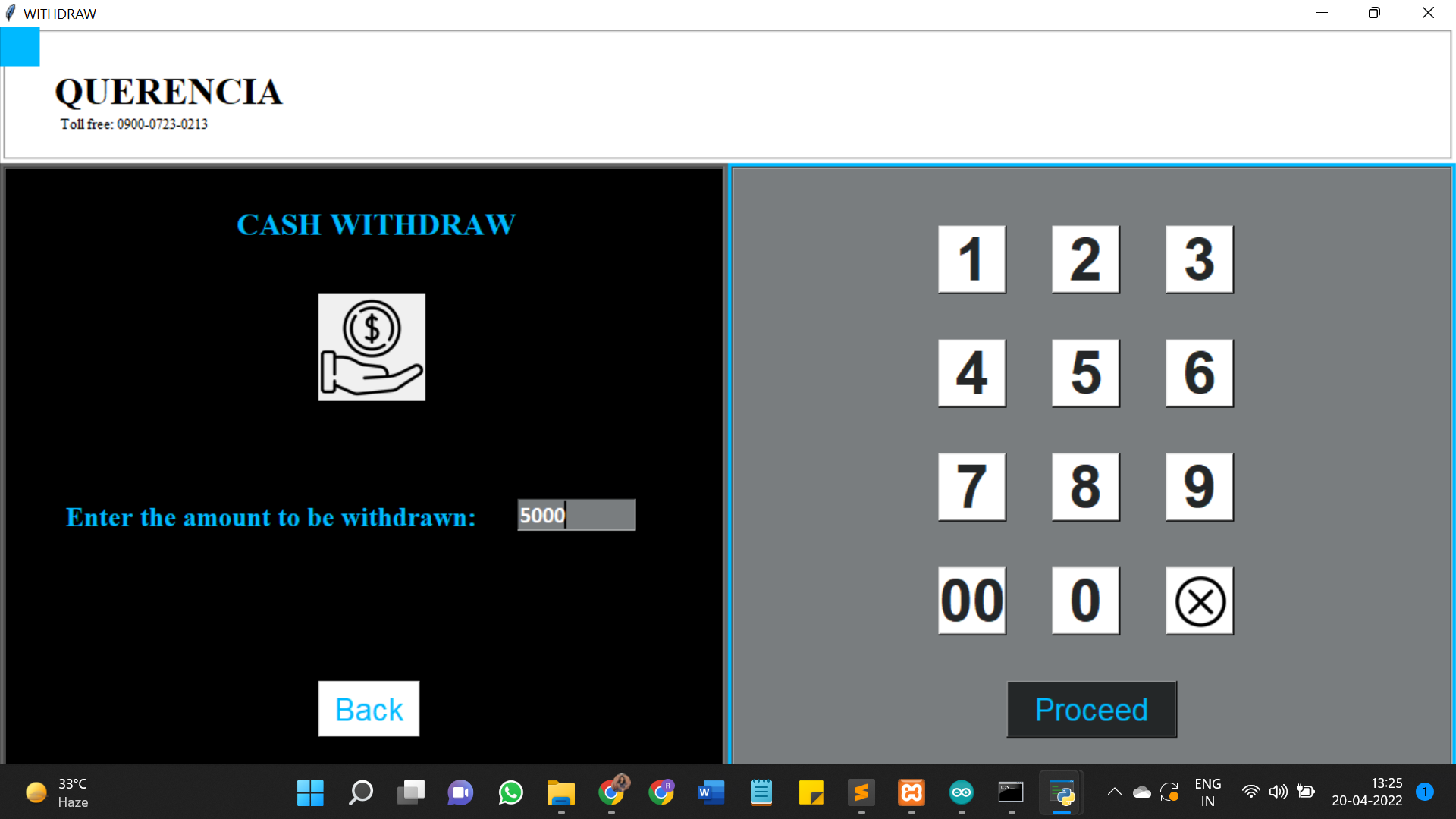
**Fig. 18: Help screen**



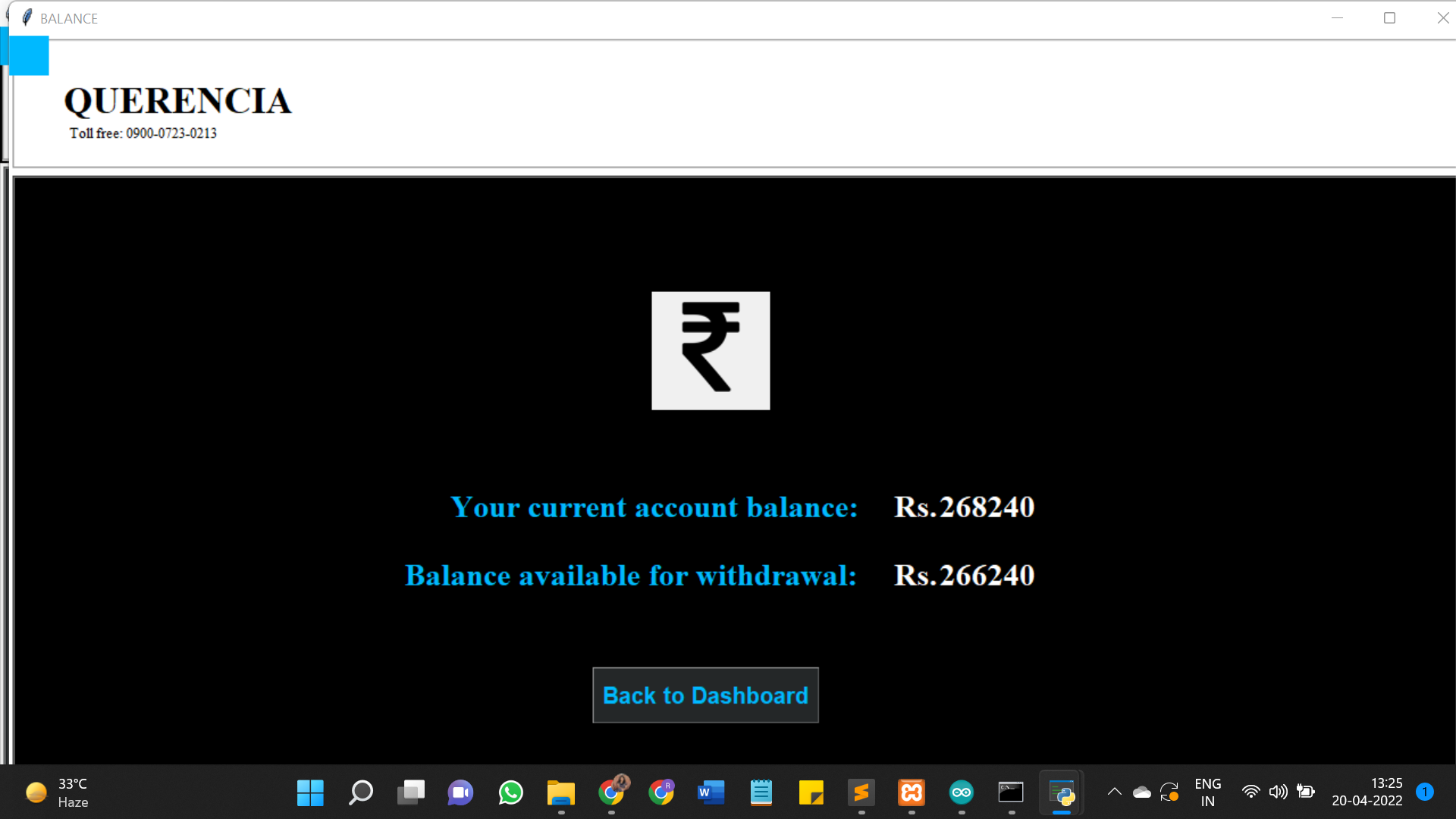
**Fig. 19: Dashboard**



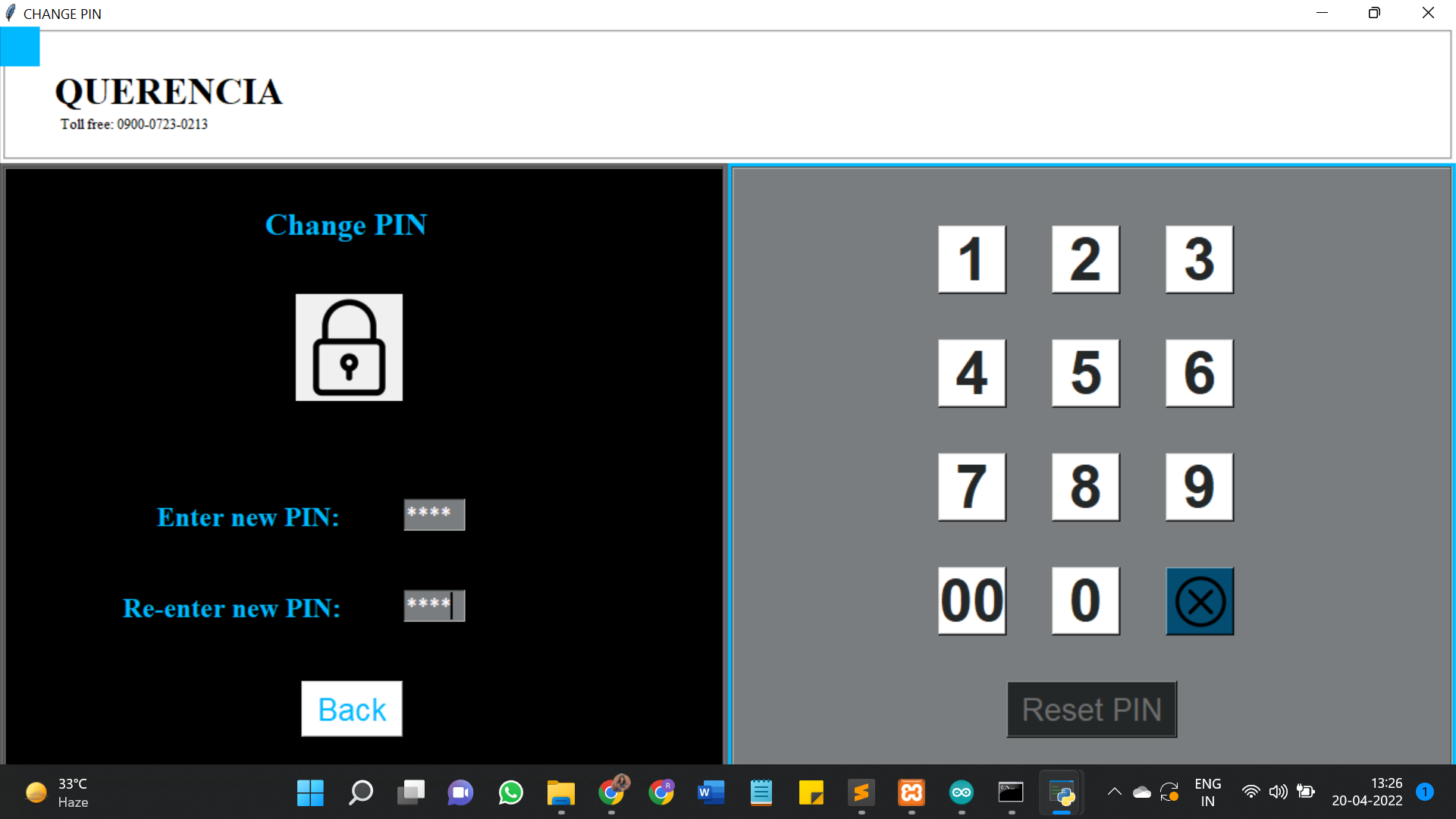
**Fig. 20: Deposit**



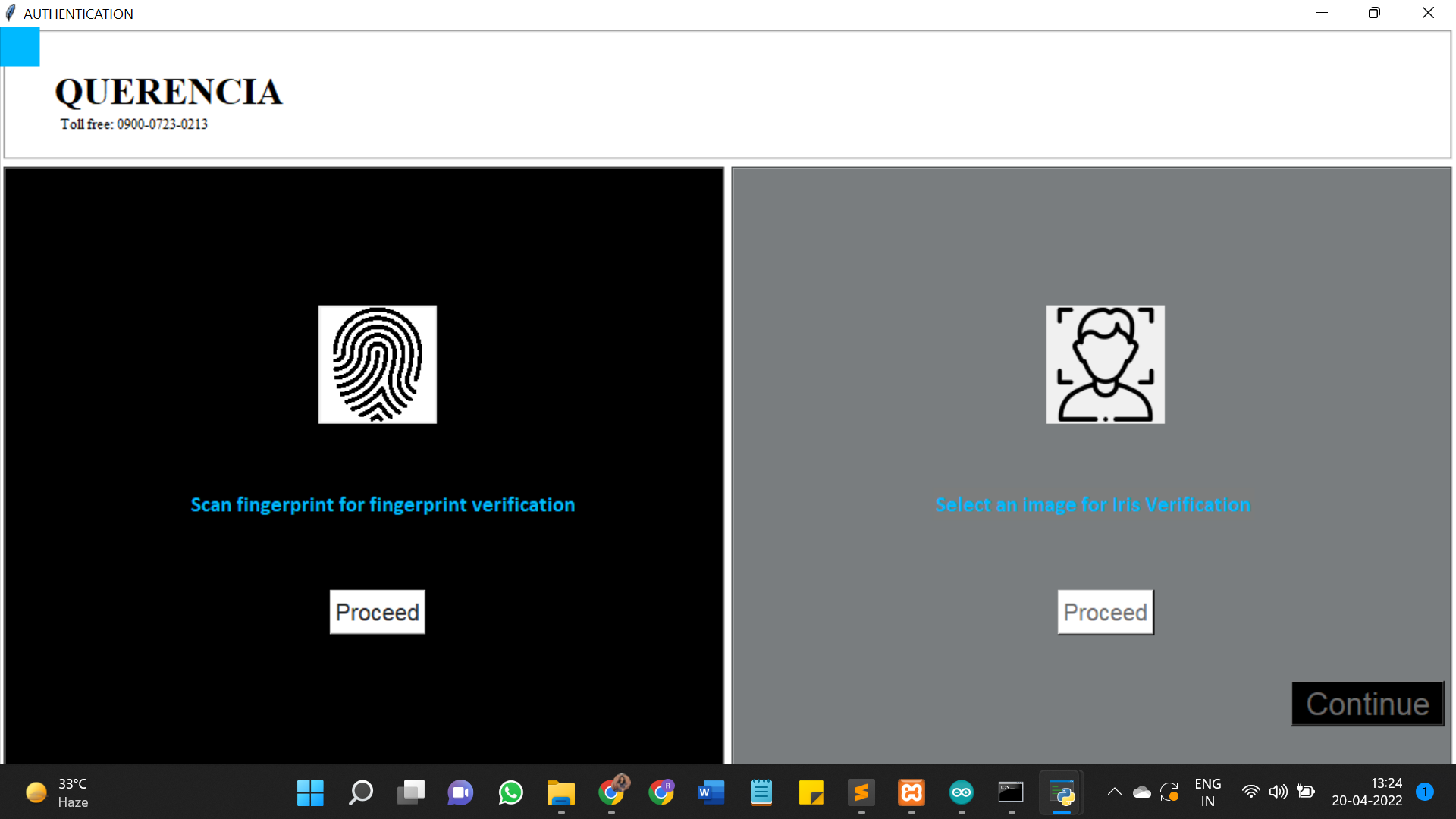
**Fig. 21: Withdraw**



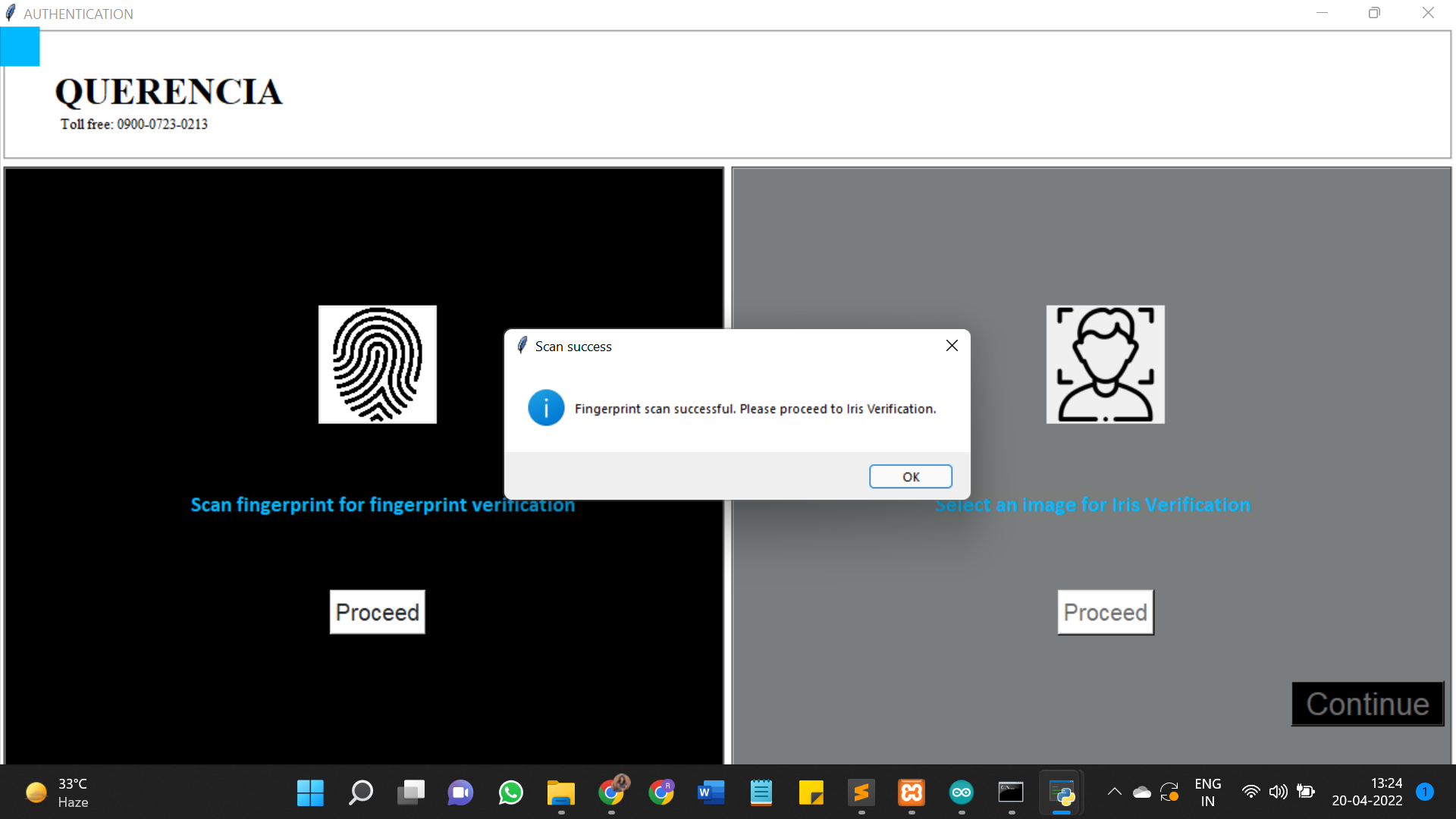
**Fig. 22: Balance Enquiry**



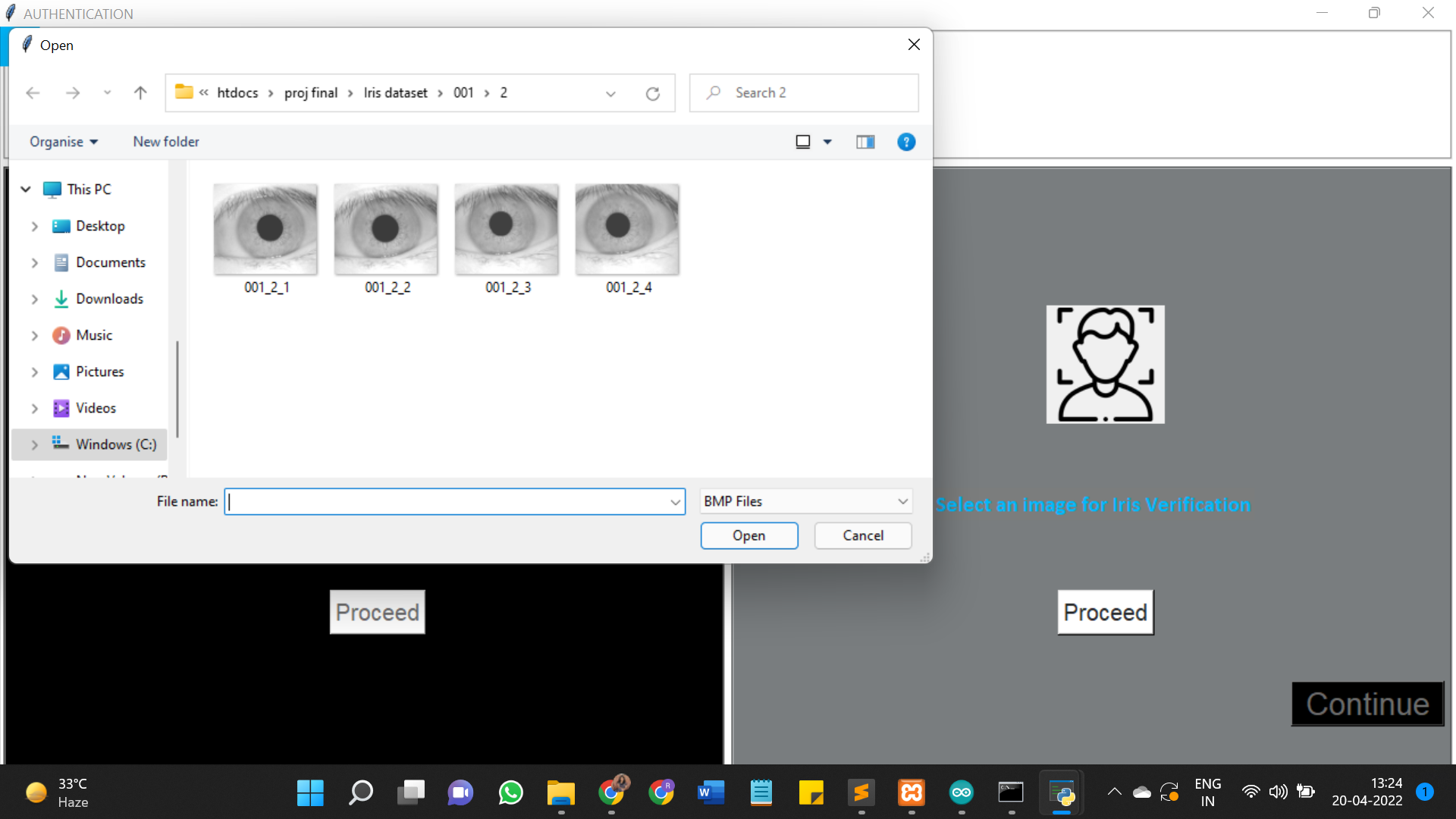
**Fig. 23: Change PIN**



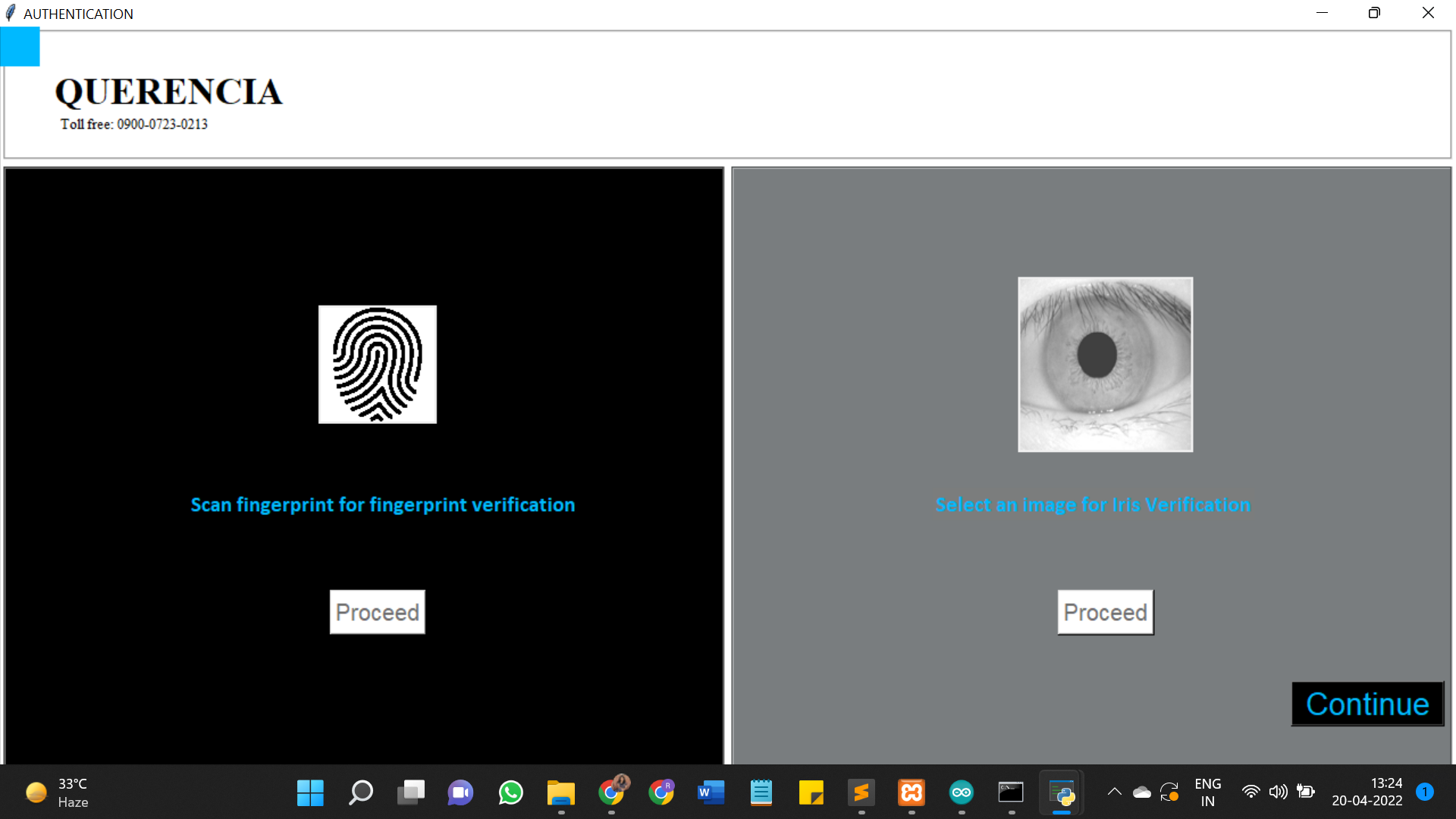
**Fig. 24: Biometric authentication**



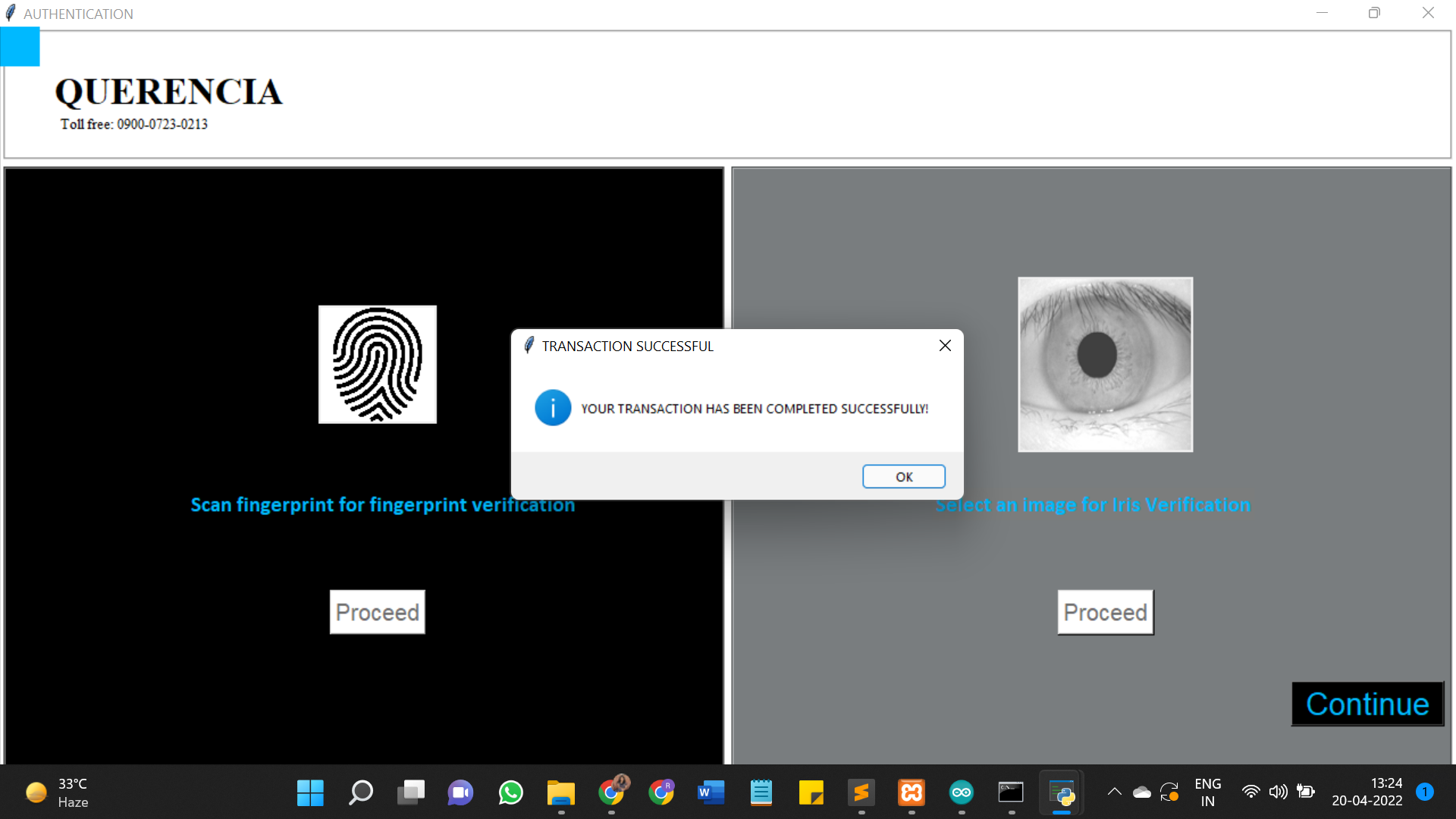
**Fig. 25: Fingerprint authentication successful**



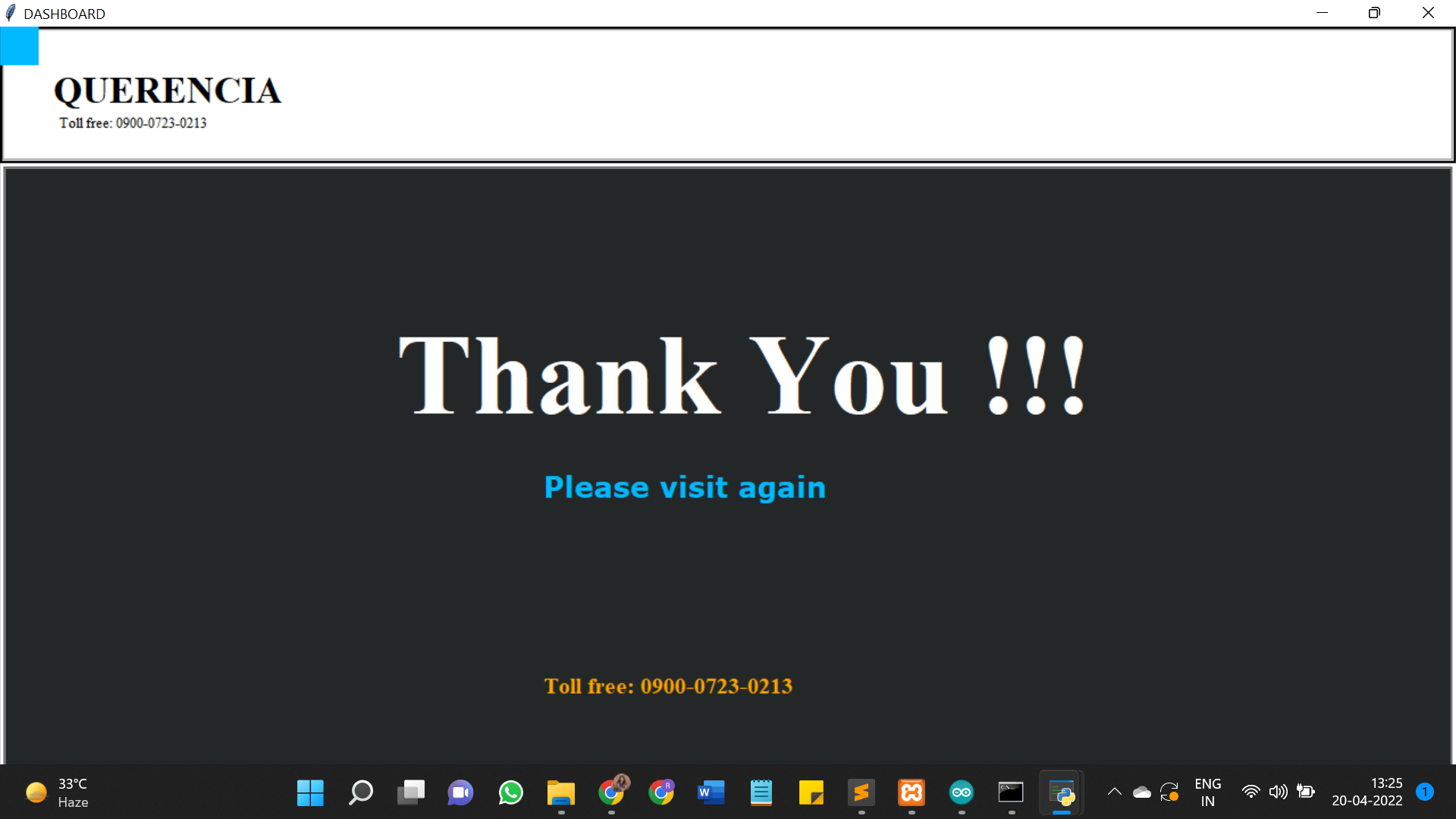
**Fig. 26: Iris image selection**



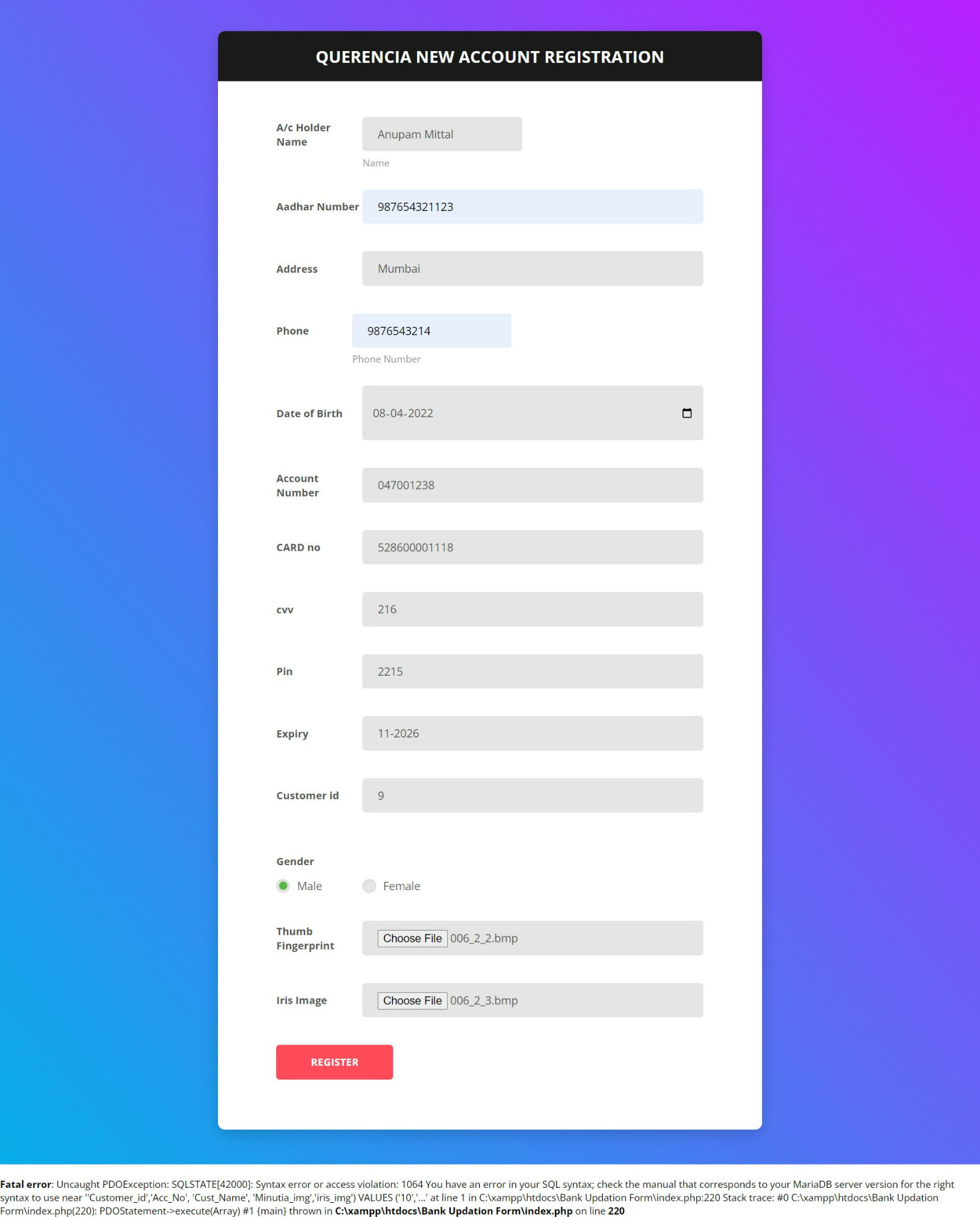
**Fig. 27: Iris authentication**



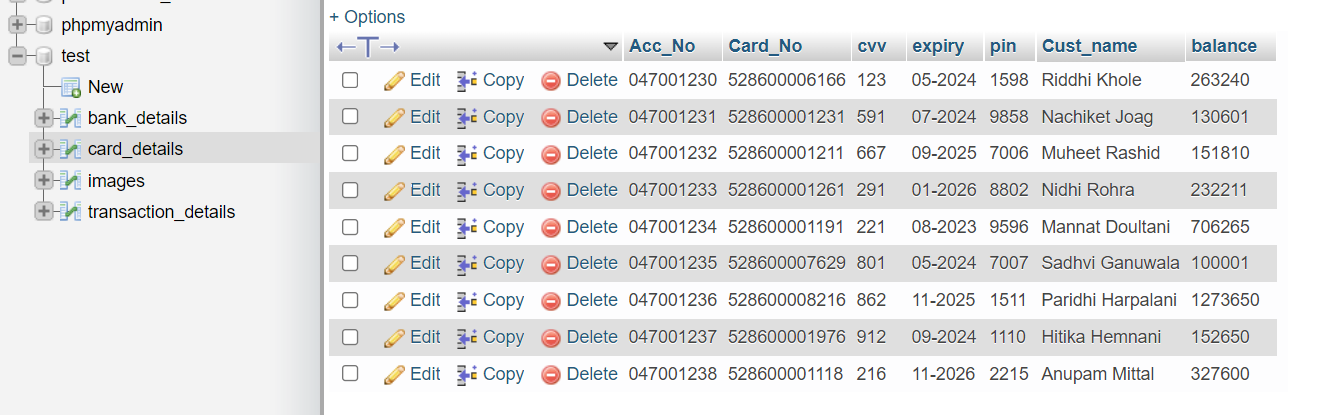
**Fig. 28: Iris authentication successful and transaction completed**



**Fig. 29: Thank you message**



**Fig.30: New account registration**



**Fig.31: Customer Details database**

## 

## **7.2 Performance Evaluation Measures**

In a biometric system, the primary evaluating factor is the accuracy of fingerprint recognition and Iris recognition. In this system, the fingerprint recognition module and the iris recognition module give nearly 100% Accurate results. One of the reasons for this accuracy is that we have considered One-to-one (1:1) matching of fingerprints in the database. One-to-one (1:1) matching is typically used in cases where security is a high priority. This method is more secure than 1:N because 1:1 matching requires the person to present information that identifies themselves.

However, before implementing this system we underwent multiple approaches and compared the accuracy of those systems. We built a fingerprint recognition system using MATLAB, and the Minutiae Score Matching algorithm to compute a similarity score. Based on this similarity score and the threshold score, it determines whether the fingerprint is matched or not. This system gave an accuracy score of about 85%. Since FMR and FNMR are the most common metrics used to evaluate the performance of biometric systems, we have drawn a graph of FMR Vs FMNR, which is discussed further in chapter 7.5.

## **7.3 Input Parameters/ Features Considered**

The application is a replica of an ATM system, added the concept of biometrics to enhance the security. For a successful transaction to take place we consider the following input parameters:

* Account Number of the user
* PIN
* Action to be Performed
* Fingerprint of the user
* Iris Image

For the matching of fingerprint, the features of minutia that we consider are illustrated in the following table:

|  |  |
| --- | --- |
|  | **TERMINATION** |
|  | **BIFURCATION** |
|  | **CROSSOVER** |
|  | **POINT OR ISLAND** |
|  | **INDEPENDENT RIDGE** |
|  | **SPUR** |
|  | **LAKE** |

**Table.1: Features of Minutiae**

The R-305 module makes use of certain performance parameters to facilitate the system’s efficiency.

**Baud rate control**

This Parameter controls the UART communication speed of the Modul. Its value is an integer N, N= [1, 12]. Corresponding baud rate is 9600\*N bps.

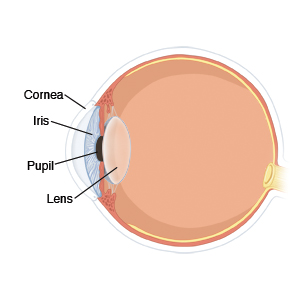
**Security Level**

The Parameter controls the matching threshold value of fingerprint searching and matching. The security level is divided into 5 grades, and the corresponding value is 1, 2, 3, 4, 5. At level 1, FAR is the highest and FRR is the lowest; however at level 5, FAR is the lowest and FRR is the highest.

**Data package length**

The parameter decides the max length of the transferring data package when communicating with the upper computer. Its value is 0, 1, 2, 3, corresponding to 32 bytes, 64 bytes, 128 bytes, and 256 bytes respectively.

## For Iris Recognition we have considered left and right Iris images of humans, along with the position of pupils and eyelids.

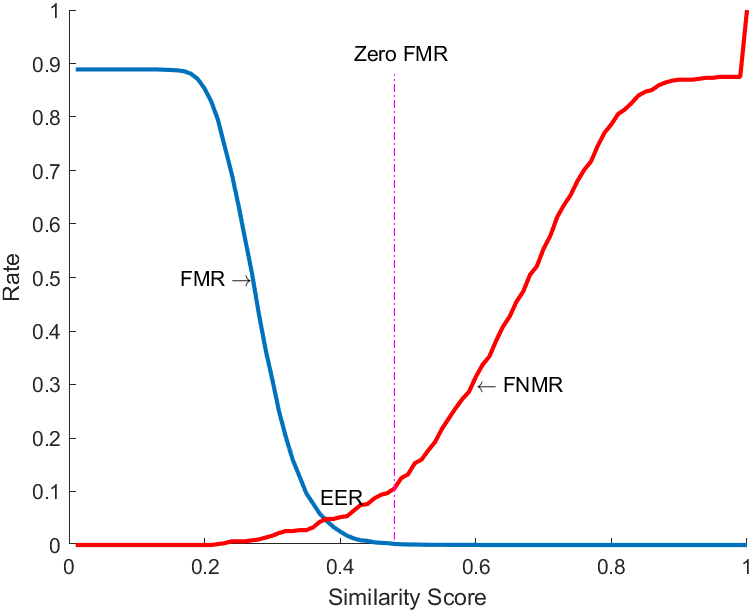


**Fig. 32: Eye Anatomy**

## **7.4 Comparison of Results with Existing Systems**

As far as the existing systems are concerned, there is currently no ATM system that employs a biometric system. However, we have made research by comparing various biometric systems for fingerprint recognition. Comparing those systems with our system will be a significant discussion.

In an existing biometric system, which we have implemented in MATLAB, the accuracy was found to be **87%** which was very less for an ATM System to work. The graphical representation of FMR and FNMR is given in figure 7.2 which clearly shows that there is a false matching and false non-matching results (ideally - 0 ).



**Fig. 33. FMR & FNMR**

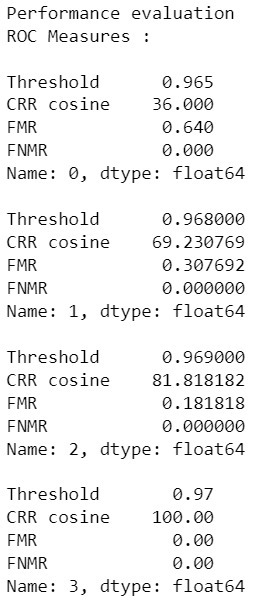
On the other hand, Since we have used the R-305 fingerprint module, which is a high-precision and high-performance device, our system has an accuracy of nearly **100%**, provided that the user is registered and has an account with the bank.

For iris, if the cosine distance is more than the threshold, then it is 1 (accepted) otherwise it is 0 (rejected). Threshold=0.97 gives accurate results. The value of the correct correction rate(crr) is given by the count of the iris that are correctly matched divided by the count of the total number of iris. Thus we calculate crr cosine value.

To calculate ROC, we use the matching\_cosine\_ROC we got from IrisMatching() and compare it with our actual matching\_cosine answer to calculate the FMR and FNMR.

FMR= no. of images incorrectly accepted / total number of accepted images

FNMR = no. of images incorrectly rejected / total no of rejected images



**Fig. 34. ROC measures**

## **7.5 Inference Drawn**

Various trials have been done to develop a biometric ATM system, worldwide. After comparing various systems, we can conclude that the R-305 fingerprint module is an ideal fit for a Biometric ATM system as it can provide the most efficient transaction to happen. It gives a good accuracy with the only exception that the fingerprint should be placed correctly on the scanner and there should not be any difference in the trait of the fingerprint scanned and the one stored in the database. Along with Fingerprint and Iris recognition, the performance of the ATM system is boosted with security like never before.

# **CHAPTER 8: CONCLUSION**

## **8.1 Limitations**

* Some people (majorly senior citizens and illiterate people) may not feel comfortable to use the technology-packed system due to digital illiteracy and/or less technological acquaintance and hence may hesitate to use it.
* Not suitable for people with eye problems (e.g. cataract surgeries which can alter the iris patterns in the eye leading to errors in biometric verification and hence would lead to a failure during user authentication)
* Not suitable for totally blind people.

## **8.2 Conclusion**

* Although the biometric authentication system has been employed today in mobile phones and laptops heavily and for recording attendance in many schools and colleges, it has not been implemented in any other domain so extensively, especially in the banking sector. Our solution could serve as a good attempt to utilize the biometric system in banking effectively as it is a blend of biometric and cryptography techniques.
* It is extremely difficult or rather almost impossible for the attackers to tamper with the system and bypass the 3-layer authentication procedure illegally. Thus, our proposed system guarantees a great level of security altogether.
* Such systems when deployed at banks, would be preferred by the customers which will indirectly have a positive impact on the business of banks.
* The biometric system is revolutionizing globally and many industries are innovating its usage across their products for the convenience and safety of their customers.

## **8.3 Future Scope**

* Introducing the concept of nominees for user authentication: In cases of emergency such as an accident or death of an account holder, his/her biometric patterns cannot be used for authentication. In such scenarios, his/her closest relative/s should be allowed to access the account. Hence, their fingerprint and iris patterns have to be stored in the database right at the time of the biometric registration of the account holder while opening a new bank account.
* Detection of fingerprint forgery: Detecting attempts of identity theft and violation and bypassing of the fingerprint authentication mechanism by using machine learning algorithms, raising a red flag immediately and reporting such cases to concerned authorities.
* Mobile app: A mobile app (for the respective bank) may be developed to authenticate the users directly via app (for those with mobile phones having a built-in fingerprint scanner and a camera) to further escalate their user experience.

**References**

1. *Nawaz, Ali & Hossain, Fakir & Khan, Grihan. (2013). Biometric Authentication Scheme for ATM Banking System Using Energy Efficient AES Processor.*
2. *Ali, Mouad & Mahale, Vivek & Yannawar, Pravin & Gaikwad, Ashok. (2016). Overview of Fingerprint Recognition System. 10.1109/ICEEOT.2016.7754902.*
3. *a J, Bhuvaneshwari. (2019). SECURE & ENHANCED ATM WITH BIOMETRIC AUTHENTICATION.*
4. *Nithya, Alice & Lakshmi, C.. (2015). Iris recognition techniques: A Literature Survey. International Journal of Applied Engineering Research. 10. 32525-32546.*
5. *Ravi, J. & K B, Raja & K R, Venugopal. (2010). Fingerprint Recognition Using Minutiae Score Matching. CoRR. abs/1001.4186.*
6. *L. N. Darlow and B. Rosman, "Fingerprint minutiae extraction using deep learning," 2017 IEEE International Joint Conference on Biometrics (IJCB), 2017, pp. 22-30, doi: 10.1109/BTAS.2017.8272678.*
7. *Ng, Richard & Tay, Yong Haur & Mok, Kai. (2008). A review of iris recognition algorithms. Proceedings - International Symposium on Information Technology 2008, ITSim. 2. 1 - 7. 10.1109/ITSIM.2008.4631656.*
8. *Sevugan, Prabu & Swarnalatha, P. & Gopu, Magesh & Sundararajan, Ravee. (2017). IRIS RECOGNITION SYSTEM. International Research Journal of Engineering and Technology.*
9. *M. M. H. Ali, V. H. Mahale, P. Yannawar and A. T. Gaikwad, "Fingerprint Recognition for Person Identification and Verification Based on Minutiae Matching," 2016 IEEE 6th International Conference on Advanced Computing (IACC), 2016, pp. 332-339, doi: 10.1109/IACC.2016.69.*
10. *Muley, Abhinav & Kute, Vivek. (2018). Prospective solution to bank card system using fingerprint. 898-902. 10.1109/ICISC.2018.8398930.*
11. *Nanayakkara, Samitha & Meegama, R. (2020). A Review of Literature on Iris Recognition. International Journal of Research. 106-120. 10.32968/1632-2882.*

**Appendix**

## **1. Paper I and II Details**

a. Paper published

Paper 1 link: [ICCIS\_2021\_Paper\_430.pdf](https://drive.google.com/file/d/1RhNtWVEkBbGy-fbYlul0rCZJvGlcwB8N/view?usp=sharing)

b. Certificate of publication/presentation

Paper 1:Presentation certificate:

