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

**Department of Computer Engineering**



Project Report on

Querencia: Encrypted Biometric authenticated ATM System.

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

Academic Year 2021-2022

# ABSTRACT

In India, the concept of Biometric detection-based systems is not widespread. The biometric data is already recorded at the banks but not used extensively. Biometric data being unique to the individual and not capable of being duplicated, can be used to ensure greater accuracy of identification. Currently, the ATM systems in India work on PIN meaning that if someone has the ATM card and its PIN, he/she can access the account. But, this can prove dangerous because if an attacker surfs the PIN and somehow manages to steal the ATM card, he can empty the bank account within seconds. So, to increase the level of security in this traditional ATM process, we plan to develop an encrypted biometric authentication system that would provide a 2-step authentication by using the biometric characteristics of an individual which include fingerprint and iris patterns along with PIN in order to ensure maximum security and prevent such attacks.

# INDEX

|  |  |  |
| --- | --- | --- |
| **CHAPTER NO.** | **TITLE** | **PAGE NO.** |
| **1** | **Introduction** | **1** |
| 1.1 | Introduction | 1 |
| 1.2 | Motivation | 1 |
| 1.3 | Drawback of the Existing System | 1 |
| 1.4 | Problem Definition | 2 |
| 1.5 | Relevance of the Project | 2 |
| 1.6 | Methodology Used | 2 |
| **2** | **Literature survey** | **4** |
| 2.1 | Research papers | 4 |
| 2.1.1 | Overview of Fingerprint Recognition System | 4 |
| 2.1.2 | Overview of Fingerprint Recognition System | 4 |
| 2.1.3 | Iris recognition techniques: A Literature Survey | 5 |
| 2.1.4 | Fingerprint Recognition Using Minutiae Score Matching | 5 |
| 2.1.5 | Fingerprint minutiae extraction using deep learning | 6 |
| 2.1.6 | A review of iris recognition algorithms | 6 |
| 2.1.7 | IRIS RECOGNITION SYSTEM | 7 |
| 2.1.8 | Fingerprint Recognition for Person Identification and Verification Based on Minutiae Matching | 8 |
| 2.2 | Patent search | 8 |
| 2.2.1 | METHOD AND APPARATUS FOR AUTHENTICATING FINANCIAL | 8 |

|  |  |  |
| --- | --- | --- |
|  | TRANSACTIONS |  |
| 2.2.2 | BIOMETRIC AUTHENTICATION UTILIZING UNIQUE BIOMETRIC SIGNATURES AND PORTABLE ELECTRONIC DEVICES | 9 |
| **3** | **Requirements** | **10** |
| 3.1 | Functional Requirements | 10 |
| 3.2 | Non-Functional Requirements | 10 |
| 3.3 | Constraints | 11 |
| 3.4 | Hardware and Software Requirements | 11 |
| 3.5 | Technologies and Tools utilized for proposed system | 12 |
| 3.6 | Project Proposal | 12 |
| **4** | **Proposed Design** | **14** |
| 4.1 | Block diagram of the proposed system | 14 |
| 4.2 | Modular diagram of the proposed system | 16 |
| 4.3 | Detailed Design | 18 |
| a | DFD diagrams | 18 |
| b | Flowchart | 21 |
| c | ER diagram | 23 |
| d | Screenshots of implementation | 23 |
| 4.4 | Proposed Algorithms | 27 |
| 4.5 | Dataset used and its Specifications | 29 |
| 4.6 | Gantt Chart | 31 |
| **5** | **Proposed Results and Discussions** | **32** |
| 5.1 | Determination of accuracy | 32 |
| **6** | **Plan of action for the next semester** | **33** |
| 6.1 | Work done till date: | 33 |

|  |  |  |
| --- | --- | --- |
| 6.2 | Plan of action for the next semester | 33 |
| **7** | **Conclusion** | **34** |
| **8** | **References** | **35** |
| **9** | **Appendix** | **36** |
| a | List of Figures | 36 |
| b | Paper publication | 37 |
| 1 | Draft of the paper submitted for evaluation | 37 |
| 2 | Plagiarism report of the paper draft | 37 |
| 3 | Proof of paper submission | 38 |
| 4 | Screenshot of project review sheet 1 | 40 |

**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 are 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 exists. 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.

## Drawback of the Existing System

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.

## 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.

## 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.

## Methodology Used

At the Bank:

Record of biometric data of customer is stored in the system using fingerprint scanning device and iris infrared scanner.

Encryption of biometric data using Advanced Encryption Standard (AES) Algorithm. *[1]*

At the ATM:

The fingerprint acquired from the user is encrypted and added to a block in the chain for authentication. The facial recognition system captures the image and then encrypts the data, adding it to the block.

This encrypted block is then transmitted over the secured channel to the central banking terminal. At the banking terminal, the data is decrypted and compared with the data registered at the bank. The authentication is valid if the minutiae and iris matching are successful.

Once users are authenticated, they are permitted to withdraw cash from their account.

Biometric Authentication:

The encrypted customer data from the bank is decrypted. The encrypted block received from Blockchain is then decrypted and verification and matching is done.

If the user is legitimate, the transaction is processed, else the transaction is declined.

We propose strong encryption algorithms to keep the data secure in decentralized ledgers that can only be accessed by those by the one in authority, or if the authoritative figures have granted others access.

# CHAPTER 2: LITERATURE SURVEY

## 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.

### 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.

### 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.

### 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.

### 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.

## Patent search

### 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.

### 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.

# CHAPTER 3: REQUIREMENTS

## 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:

* + - Choose a language of his choice.
    - Withdraw money.
    - Deposit money.
    - Check account balance.
    - Change account PIN.

## 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.

## 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.

## Hardware and Software Requirements

HARDWARE:

* + - Intel i5 processor
    - Input devices: Keyboard, Infrared Camera, Fingerprint Scanning Device
    - Output devices: Monitor

SOFTWARE:

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

## Technologies and Tools utilized for proposed system

* + - AES algorithm for security and authentication.
    - Image processing algorithms for minutiae and iris matching. Tools:
    - MATLAB as an image processing toolbox.
    - VS code for collaborative coding.

## Project Proposal

The prime intention of this project is to eliminate the challenges caused due to usage of cards in the ATM and extemporize the process of cash withdrawal *[10]*. In this project, we would build a system that will store the biometric information of customers in the database in an encrypted format and verify and authenticate the same during cash withdrawals at the ATM.

For Fingerprint Recognition:

Minutiae matching system consists of:

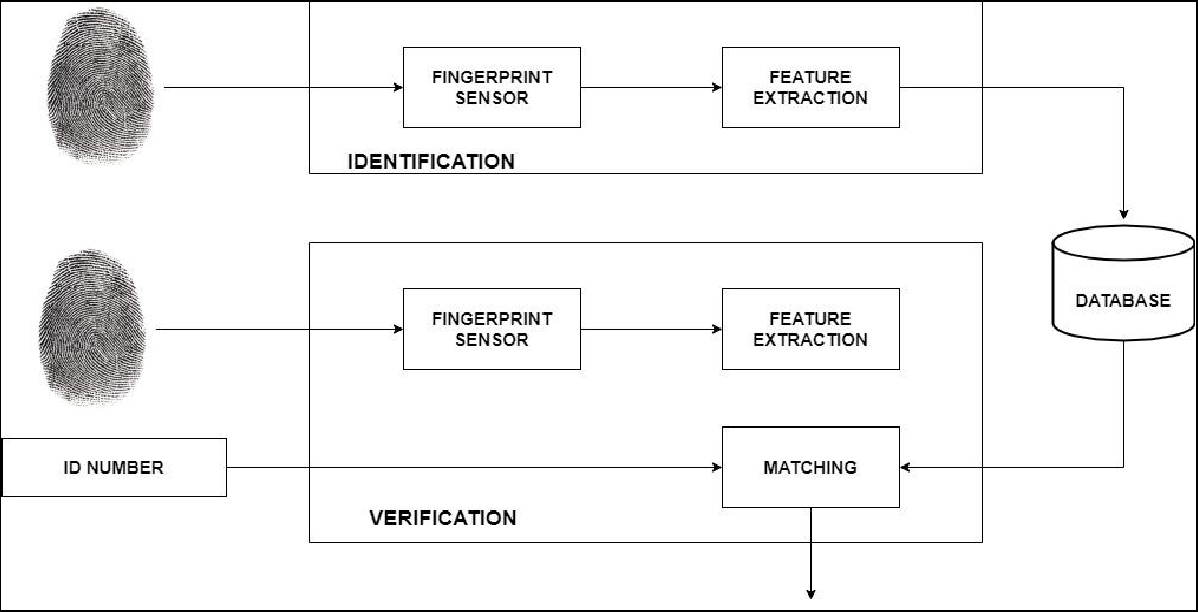
* + - Image pre-processing:
* Image Enhancement
* Making segmentation mask
* Binarization
* Thinning
  + - Feature Extraction:
* Finding Minutiae
* Filter False Minutiae
  + - Matching:
* Load database
* Registration
* Compute Matching Score

For iris recognition:

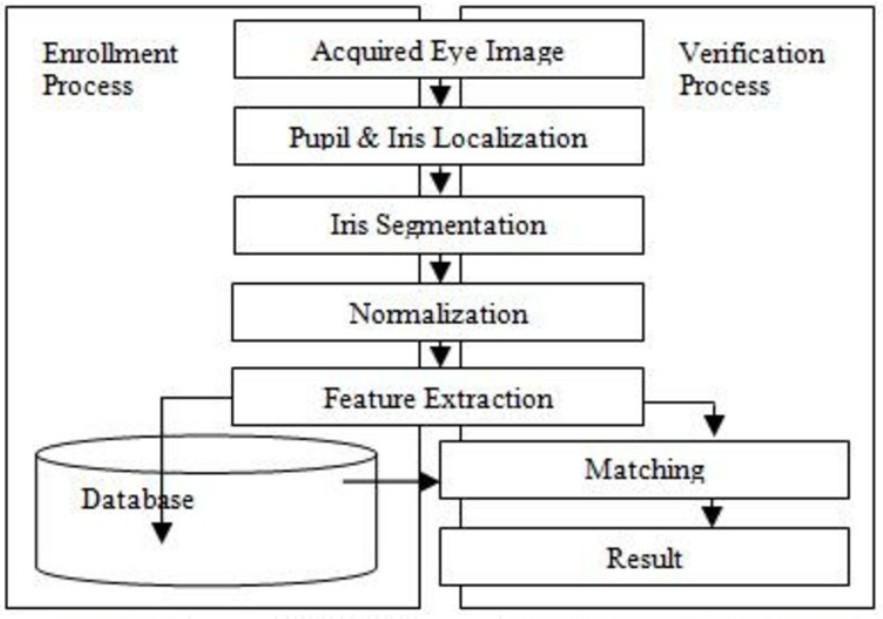
* + - Iris recognition system consisting of four main stages - segmentation, normalization, feature extraction, and matching would be implemented.
    - The commonly used algorithms like the Hough transform, rubber sheet model, wavelet, Gabor filter, and hamming distance would be used in iris recognition stages.

# CHAPTER 4: PROPOSED DESIGN

## Block diagram of the proposed system



**Fig. 1: Block diagram for fingerprint recognition**



Explanation:

**Fig. 2: Block diagram for iris recognition**

The functioning will start from swiping the ATM card and end with a message whether the Transaction was successful or not. The user needs to enter the ATM card into the swipe folder of the machine, followed by entering the card PIN provided by the bank or set by the user. A series of options will be provided on the screen of the ATM system after the user has entered the card PIN, the user will choose a single option according to his need/requirement. If the user goes with the Cash withdrawal option, then he needs to enter the amount that he/she wants to withdraw.

Now, the user will be asked to prove his/her identity, by authorizing his biometric data i.e., by scanning the fingerprint and iris patterns. Scanning will then lead to feature extraction and matching of the extracted data with the bank database. If the data matches with the bank database, the transaction status will be shown as successful otherwise the transaction would be declined.

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 encrypted using blockchain and sent to the bank for biometric authentication. If the user is legitimate, then the transaction is processed else declined.

The fingerprint recognition mainly consists of the following steps: Image pre-processing, Feature Extraction and matching.

At the ATM, the identification process takes place by scanning the fingerprint and extracting its features. Similarly at the bank recorded data is used for verification.

The steps performed in Image pre-processing:

Image Enhancement Making segmentation mask Binarization

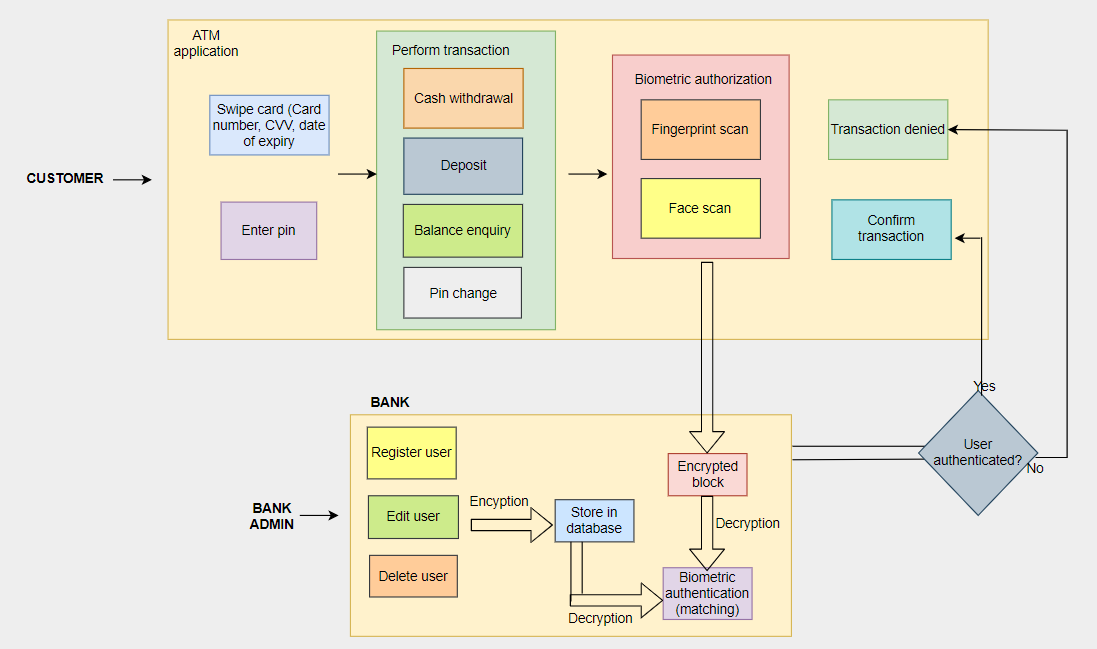
Thinning

Feature Extraction:

Finding Minutiae Filter False Minutiae

The main steps in iris recognition are enrollment, verification and identification. For both enrollment and verification, the iris image has to undergo preprocessing stages of localization, segmentation, normalization and feature extraction. The commonly used algorithms like the Hough transform, rubber sheet model, wavelet, Gabor filter, and hamming distance would be used in iris recognition stages.*[11]*

## Modular diagram of the proposed system



**Fig. 3: Modular diagram of the proposed system**

Explanation:

The system consists of two main segments, one is the customer segment (ATM interaction module) and the second is the banking segment. Each segment consists of several modules to deal with.

The first segment consists of:

1. Swipe Card Module: The user needs to swipe the card in the machine and all the required details such as Card number, CVV, etc. will be fetched.
2. Enter PIN Module: The user will be asked to enter the PIN to get further access to the account. 3.Perform Transaction Module: This module consists of several operations that a user may want to perform. Such operations include Cash-Withdrawal, Balance Enquiry, PIN change, etc.
3. Biometric Authorization Module: The user will be asked to provide his biometric details such as Fingerprint Scan and Iris Scan through physical fingerprint and eye scanning respectively.
4. Transaction Denied and Confirm Transaction Module: These modules are Confirmation modules that confirm the status of a transaction.

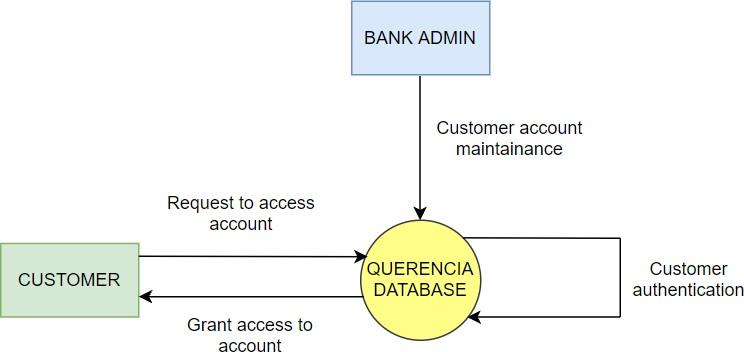
The second segment consists of:

1. Register User Module: This module provides a method for the Registration of new users. Whenever a case of New User registration would arise, this module would be used to add the user details such as Name, Address, Mobile, Biometric Data, etc.
2. Edit User Module: To edit or make some changes in the existing users' data, this module is created. Changes may be in the Name, Address, Mobile number, e-mail, etc.
3. Delete User Module: To remove a customer's account or to delete any customers' account permanently this module would be used.
4. Store in Database Module: Saving or storing the newly added user data or modified user data into the database would be carried out by this module.
5. Biometric Authentication Module: Matching the current Biometric data of a customer (provided via ATM), to the saved customer's Biometric data in the database would be carried by this module. This is the Verification Module.

## Detailed Design

### DFD diagrams:

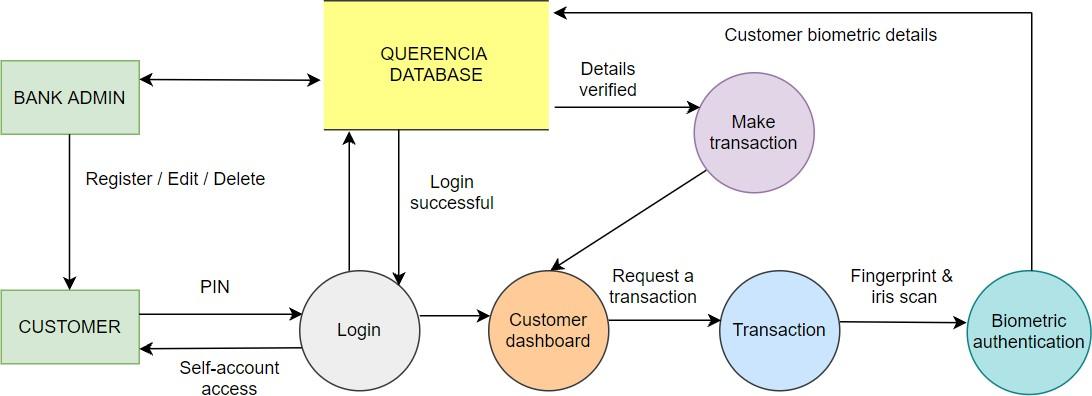
DFD level 0:



**Fig. 4: DFD level 0**

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.

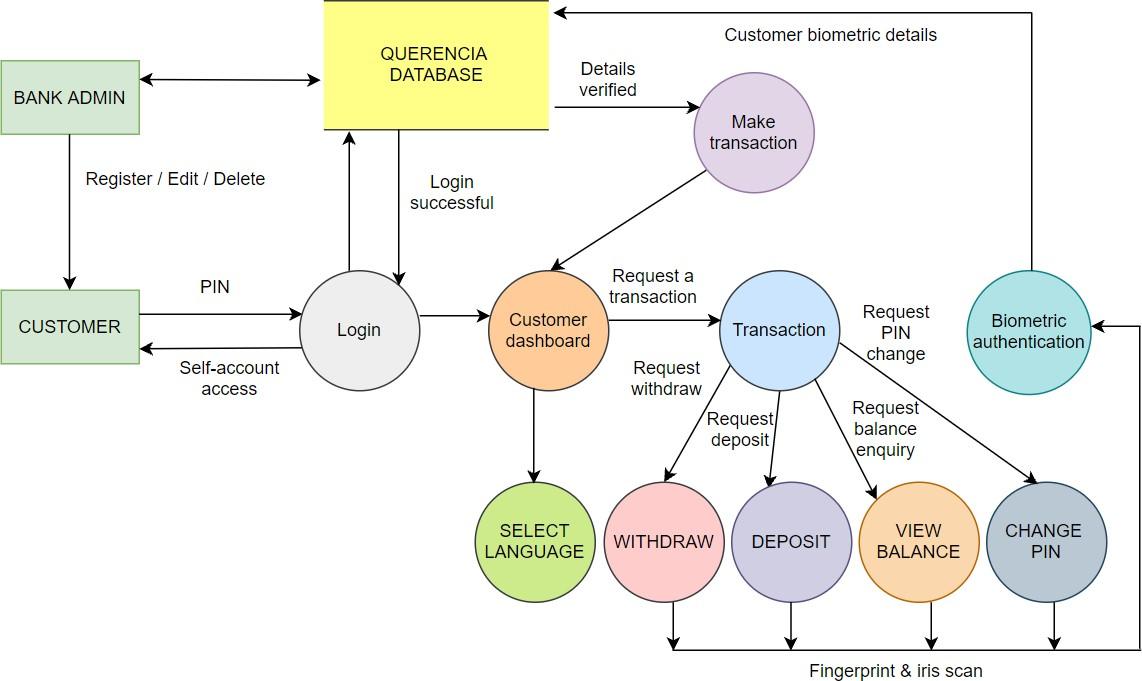
### DFD level 1:



**Fig. 5: DFD level 1**

This diagram shows a clearer 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.

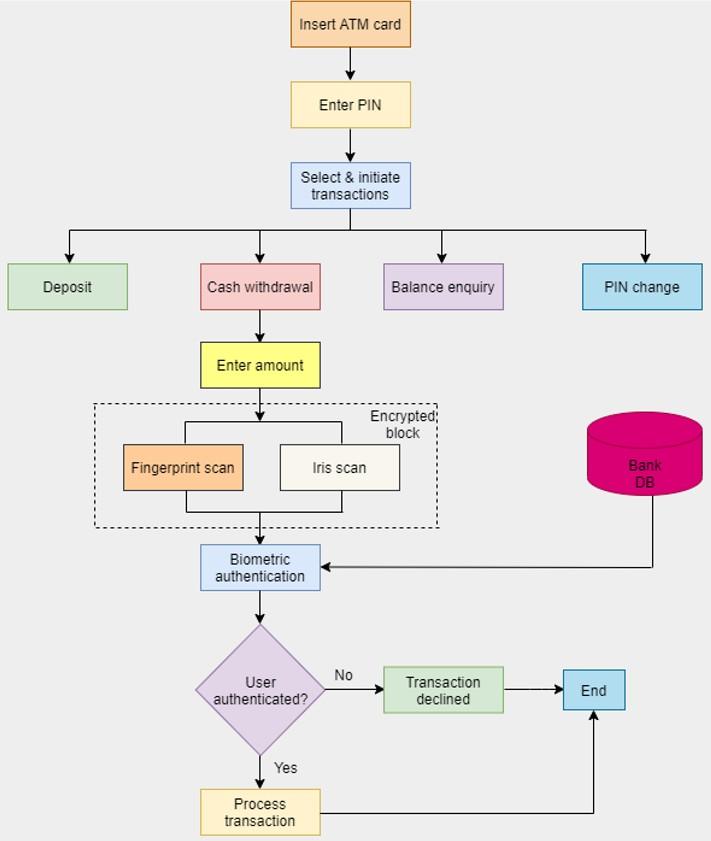
### DFD level 2:



**Fig. 6: DFD level 2**

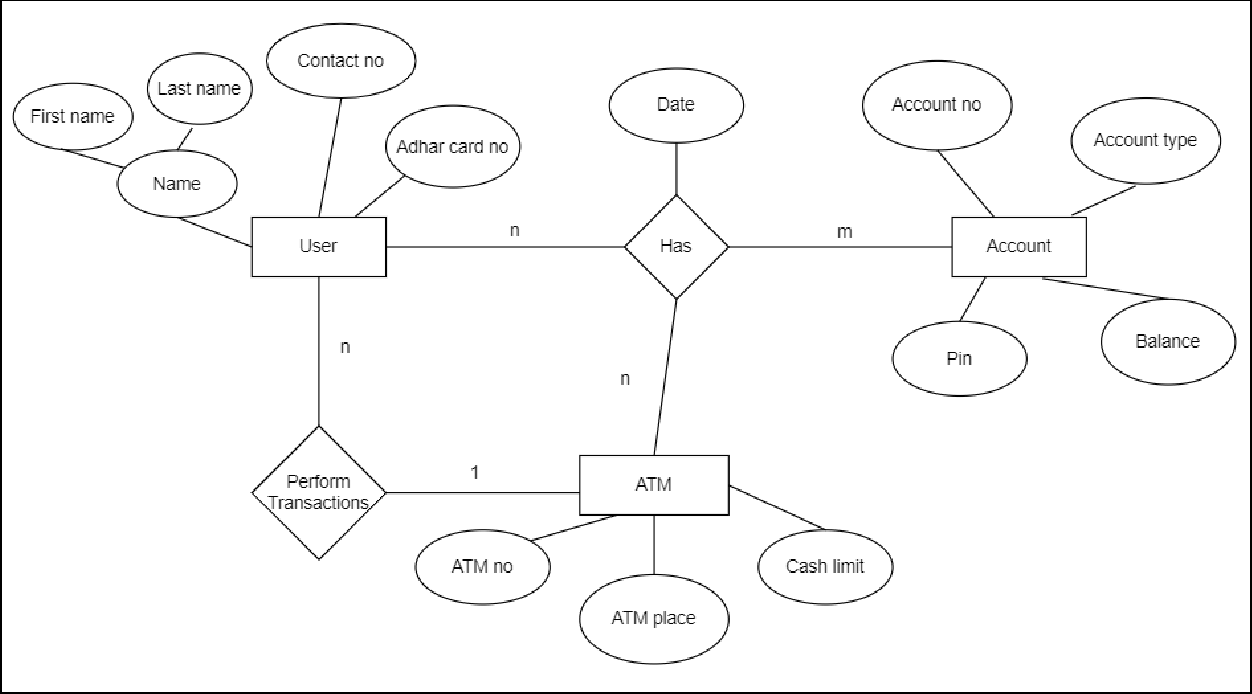
This is the most detailed description of our system. The customer can also choose a language of his choice. In addition to level 1 flow, it also shows different transactions that can be performed by the customer like withdraw, deposit, balance enquiry and change pin. Any transaction request will be followed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

### Flowchart



**Fig. 7: Flowchart**

### ER diagram

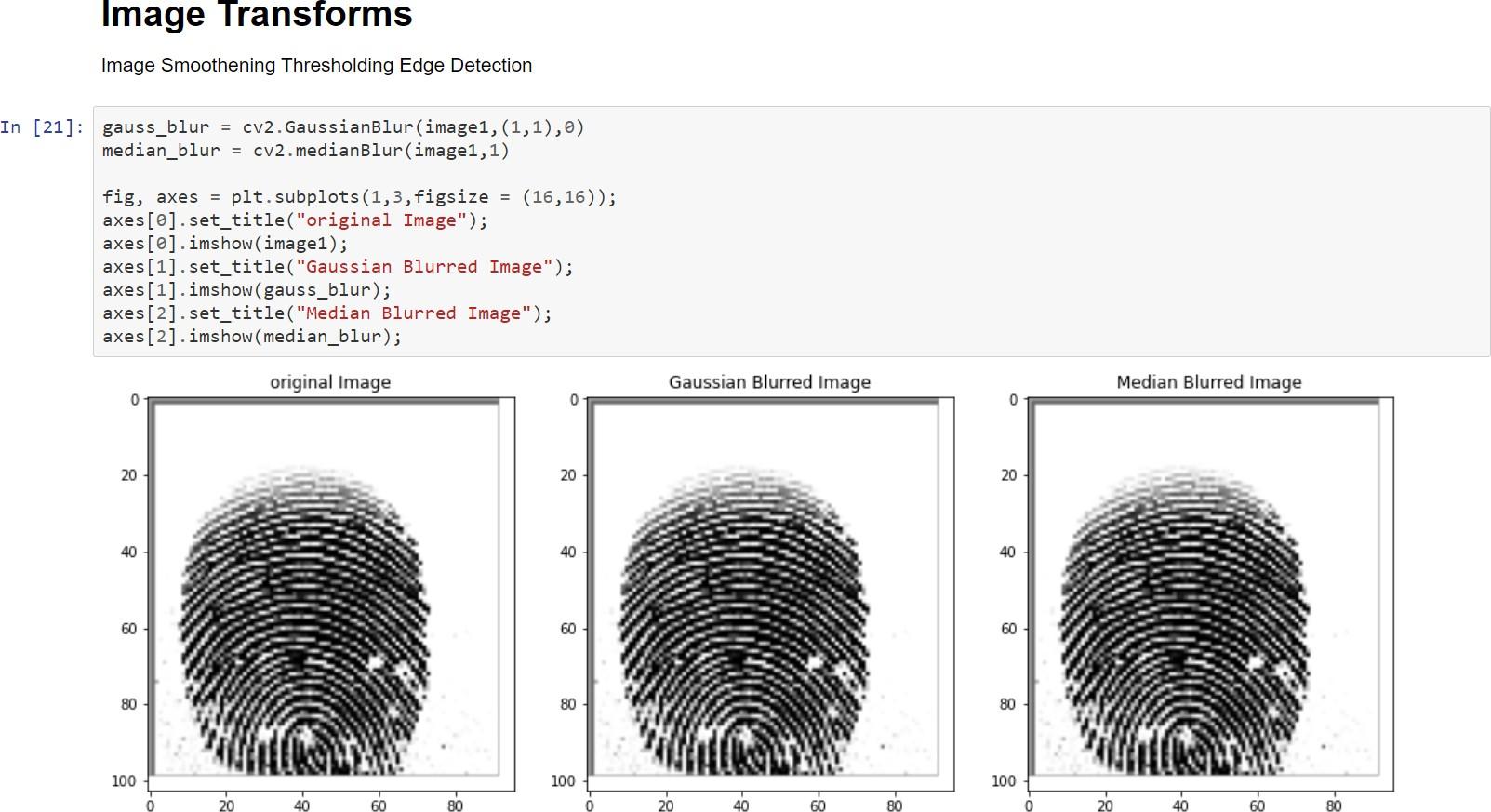


**Fig 8 . ER diagram**

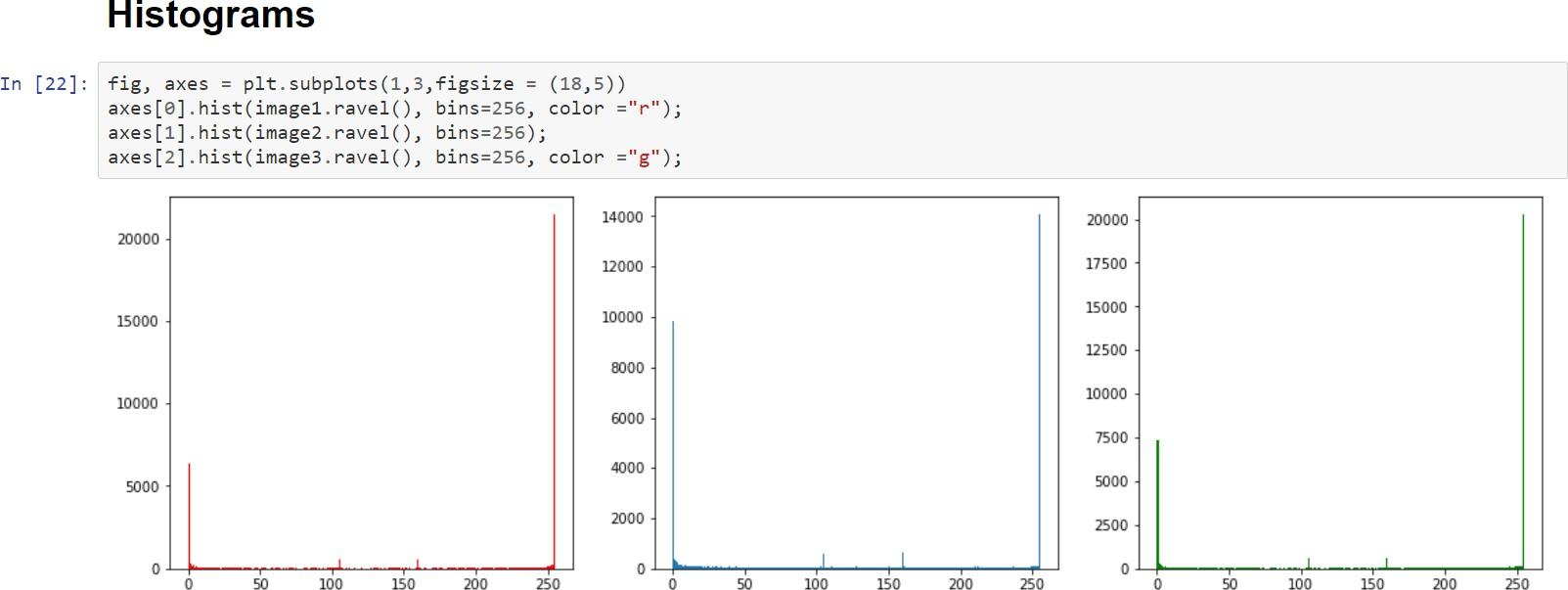
### Screenshots of implementation



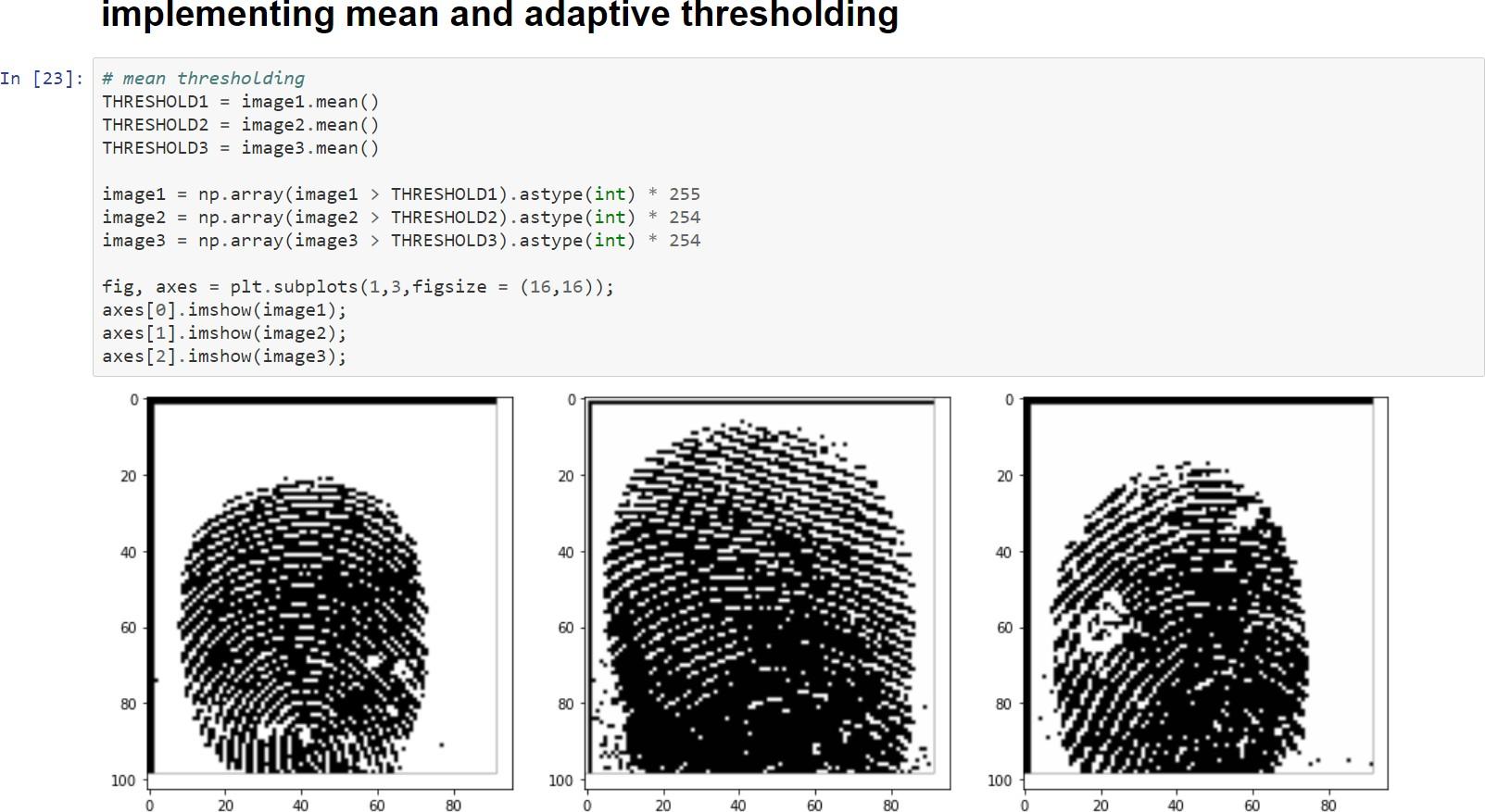
**Fig 9: Displaying random images from the data**



**Fig 10: Image transforms**



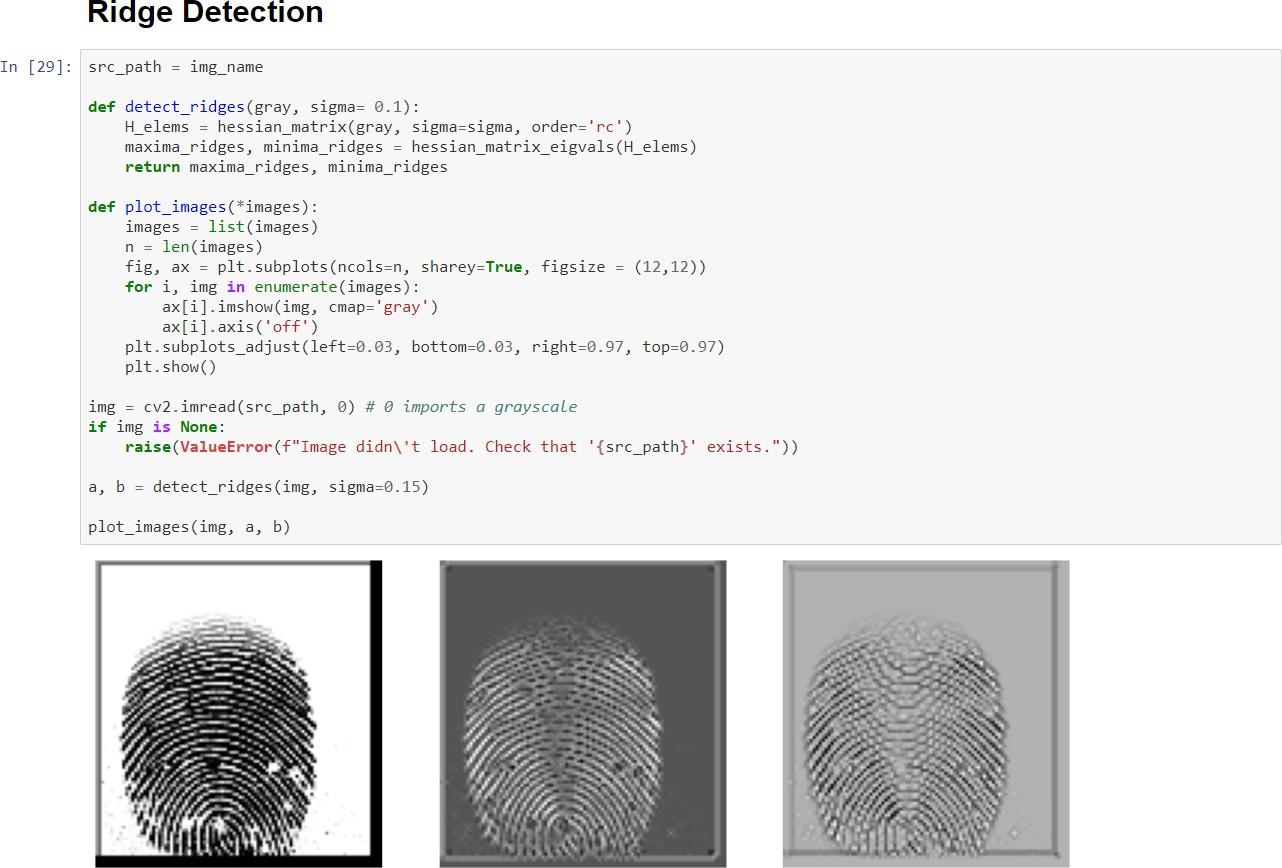
**Fig 11: Histograms**



**Fig 12: Mean thresholding**



**Fig 13: Adaptive thresholding**



**Fig 14: Ridge detection**

## Proposed Algorithms

#### For Fingerprint recognition:

MINUTIAE EXTRACTOR:

Pre-processing:

* Image Enhancement - Histogram equalization and Fourier transform
* Image Binarization - Threshold method
* Image Segmentation - block direction estimation and Morphological methods.

Minutiae extraction:

* Thinning - Iterative parallel thinning
* Minutia Detection - Crossing Number Minutia Post-processing:
* False Minutiae Removal MINUTIAE MATCHER:
* Calculate the degree of similarity.

Alignment-based match algorithm:

Alignment Stage: Calculate the similarity of the set of ridges associated with the minutia. Match Stage: Elastic match algorithm.

#### For Iris Recognition:

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

1. Segmentation

* Hough transform (time efficient but less accuracy)
* 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 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 Weighted Euclidean distance and Canberra distance metric.

Biometric encryption:

* Finger Minutiae and Iris biometric data will be encrypted using Advanced Encryption Standard (AES) Algorithm.
* After feature extraction, the image is converted into a NumPy array and then encryption is performed.

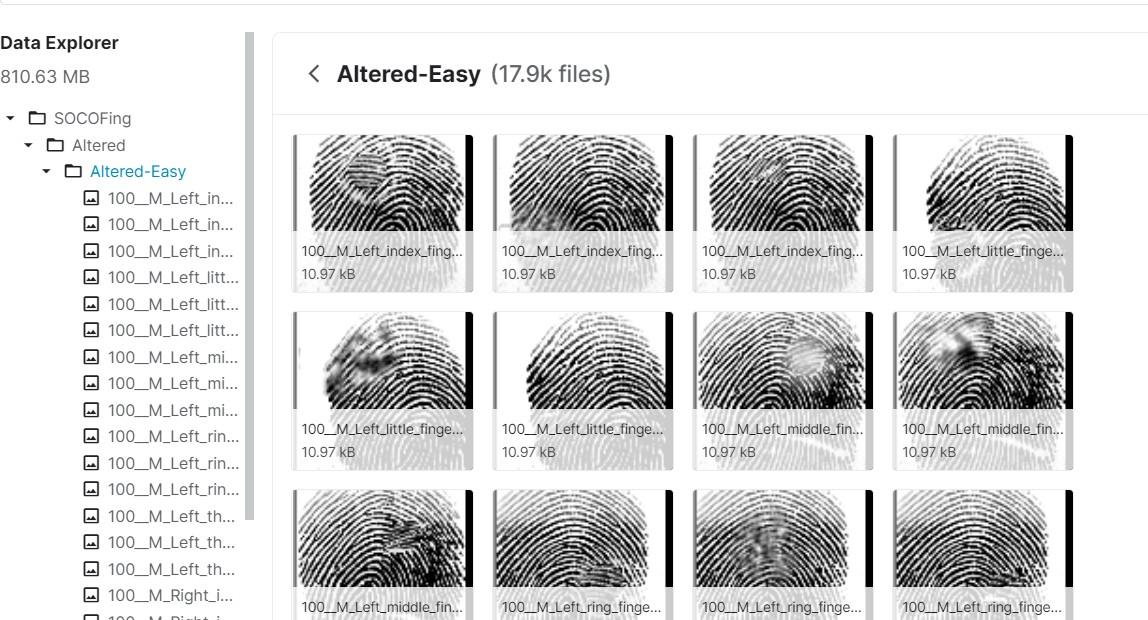
Advanced Encryption Standard (AES) Algorithm:

* It is a 128-bit private key algorithm
* At the banking terminal the image is decrypted using the same key. Based on the decrypted image, matching is performed to verify the presented fingerprint image belongs to the claimed user. The authentication is signed if the minutiae matching is successful. Similar process is followed for Iris authentication.
* In cryptography, the Advanced Encryption Standard (AES) is also known as the Rijndael algorithm.
* AES uses higher length key sizes such as 128, 192 and 256 bits for encryption. Hence it makes the AES algorithm more robust against hacking.
* For 128 bit, about 2^128 attempts are needed to break. This makes it very difficult to hack it as a result it is a very safe protocol.

## Dataset used and its Specifications

MINUTIAE DATASET:

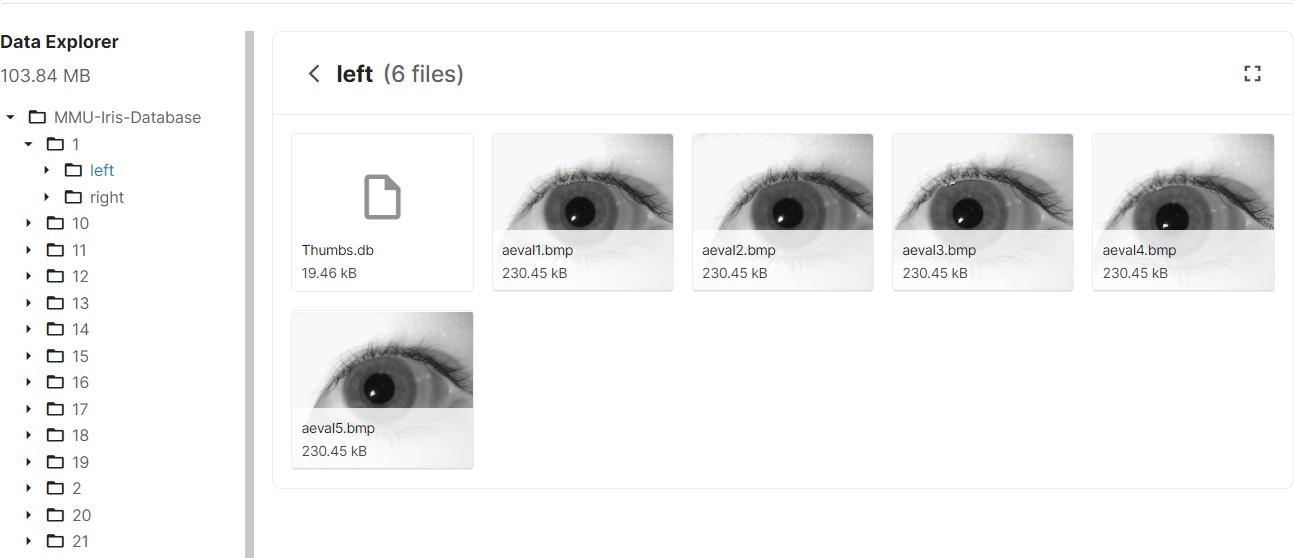
Sokoto Coventry Fingerprint Dataset (SOCOFing) is a biometric fingerprint database designed for academic research purposes. SOCOFing is made up of 6,000 fingerprint images from 600 African subjects and contains unique attributes such as labels for gender, hand and finger name.



**Fig. 15: Minutiae dataset.**

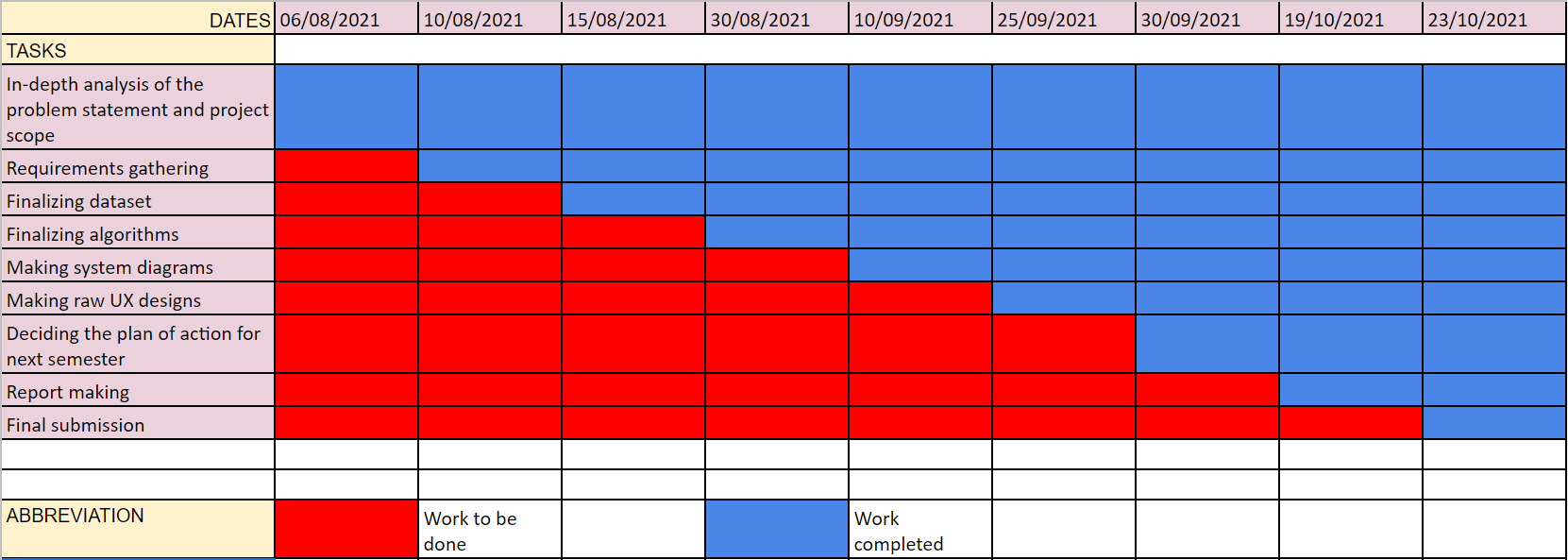
IRIS DATASET:

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



**Fig. 16: Iris dataset**

## Gantt Chart



**Fig. 17: Gantt Chart**

Explanation: A Gantt chart is a type of bar chart that diagrammatically describes a project schedule. As shown in the figure, the X-axis represents the dates and the Y-axis represents various tasks that were planned earlier. The red cells represent the work to be done and the blue cells represent the work already done.

# CHAPTER 5: PROPOSED RESULTS AND DISCUSSIONS

## 5.1 Determination of accuracy

To fully assess the accuracy and effectiveness of algorithms, we would test the model on three publicly available databases under different configurations. The identification evaluation criterion is designated to the recognition accuracy, which is defined as the ratio of the number of correct recognitions to the total number of recognitions.

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 unauthorized persons are incorrectly accepted.

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

In case of fingerprint recognition, the other important factor is minutiae matching score which is calculated as given below:

Matching score = (No. of matched minutiae / Maximum number of minutiae) \* 100 %

# CHAPTER 6: PLAN OF ACTION FOR THE NEXT SEMESTER

## Work done till date:

We have studied various research papers and on the basis of prominent observations, we have finalized our dataset and algorithms. We are going to follow an agile methodology for the implementation of our project. We have also identified the functional as well as non-functional requirements, hardware and software specifications and the constraints of our project. We have also developed raw UI design screens for the project which will later be converted into prototypes and finally into front-end code. We have also implemented a small code for the fingerprint feature extraction.

## Plan of action for the next semester:

We are going to chalk out the most important algorithms first and prioritize them. We would also identify the possible risks during the implementation process. Then we would implement the algorithms of fingerprint and iris recognition. After this, we are going to integrate them with the underlying hardware that is to be used for the actual scanning process. We would then design our database schema. Lastly, we would convert our prototypes into a fully-functional front-end code and this code would again be integrated with the backend which would complete our said project.

# CHAPTER 7: CONCLUSION

* + - Our system takes the security level of the traditional ATM transaction process a step further by mandating the 2-step biometric authentication process.
    - The biometric characteristics of an individual cannot be stolen, copied or duplicated that easily and it is almost impossible to bypass both fingerprint and iris scan techniques by doing this, which makes our system super secure.
    - Such smart and highly secure systems can soon become a reality with proper planning.

# CHAPTER 8: 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.*

# CHAPTER 9: APPENDIX

## List of Figures

|  |  |  |
| --- | --- | --- |
| Figure Number | Heading | Page no. |
| Fig 1 | Block diagram for fingerprint recognition. | 14 |
| Fig 2 | Block diagram for iris recognition**.** | 15 |
| Fig 3 | Modular diagram of the proposed system. | 16 |
| Fig 4 | DFD level 0. | 19 |
| Fig 5 | DFD level 1 | 20 |
| Fig 6 | DFD level 2 | 21 |
| Fig 7 | Flowchart | 22 |
| Fig 8 | ER diagram | 23 |
| Fig 9 | Displaying random images from the data | 24 |
| Fig 10 | Image transforms | 24 |
| Fig 11 | Histograms | 25 |
| Fig 12 | Mean thresholding | 25 |

|  |  |  |
| --- | --- | --- |
| Fig 13 | Adaptive thresholding | 26 |
| Fig 14 | Ridge detection | 26 |
| Fig 15 | Minutiae dataset | 30 |
| Fig 16 | Iris dataset | 31 |
| Fig 17 | Gantt Chart | 31 |

* 1. **Paper publication**
     1. Draft of the paper submitted for evaluation [LINK](https://drive.google.com/file/d/1vlztGZLpztt4McBJ9drvKlq53dNbvEnn/view?usp=sharing)
     2. Plagiarism report of the paper draft

