FACIAL RECOGNITION AND FINGERPRINT BASED ATM SYSTEM

SAKINAH BINTI KIRUN

BACHELOR OF COMPUTER SCIENCE

UNIVERSITI MALAYSIA PAHANG

UNIVERSITI MALAYSIA PAHANG

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name : _____

Date of Birth : _____

Title : _____

_____

_____

Academic Session : _____

I declare that this thesis is classified as:

☐ CONFIDENTIAL	(Contains confidential information under the Official Secret Act 1997)*
☐ RESTRICTED	(Contains restricted information as specified by the organization where research was done)*
☑ OPEN ACCESS	I agree that my thesis to be published as online open access (Full Text)

I acknowledge that Universiti Malaysia Pahang reserves the following rights:

1. The Thesis is the Property of Universiti Malaysia Pahang
2. The Library of Universiti Malaysia Pahang has the right to make copies of the thesis for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by:

_____	_____
(Student's Signature)	(Supervisor's Signature)
_____	_____
New IC/Passport Number	Name of Supervisor
Date:	Date:

NOTE : * If the thesis is CONFIDENTIAL or RESTRICTED, please attach a thesis declaration letter

THESIS DECLARATION LETTER (OPTIONAL)

Librarian,
Perpustakaan Universiti Malaysia Pahang,
Universiti Malaysia Pahang,
Lebuhraya Tun Razak,
26300, Gambang, Kuantan.

Dear Sir,

CLASSIFICATION OF THESIS AS RESTRICTED

Please be informed that the following thesis is classified as RESTRICTED for a period of three (3) years from the date of this letter. The reasons for this classification are as listed below.

Author's Name
Thesis Title

Reasons (i)

(ii)

(iii)

Thank you.

Yours faithfully,

_____
(Supervisor's Signature)

Date:

Stamp:

Note: This letter should be written by the supervisor, addressed to the Librarian, *Perpustakaan Universiti Malaysia Pahang* with its copy attached to the thesis.

SUPERVISOR'S DECLARATION

I hereby declare that I have checked this project and in my opinion, this project is adequate in terms of scope and quality for the award of the degree of Bachelor of Computer Science (Software Engineering).

_____

(Supervisor's Signature)

Full Name : DR. KOHBALAN A/L MOORTHY

Position : SENIOR LECTURER

Date : 10 DECEMBER 2019

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

_____

(Student's Signature)

Full Name : SAKINAH BINTI KIRUN

ID Number : CB16013

Date : 10 DECEMBER 2019

FACIAL RECOGNITION AND FINGERPRINT BASED ATM SYSTEM

SAKINAH BINTI KIRUN

Thesis submitted in fulfillment of the requirements
for the award of the
Bachelor of Computer Science (Software Engineering) with Honours

Faculty of Computing
UNIVERSITI MALAYSIA PAHANG

JANUARY 2020

ACKNOWLEDGEMENTS

I take this opportunity to express my grateful to Allah for giving me patience and strength to complete this project. I also want to thanks to my supervisor, Dr. Kohbalan A/L Moorthy for giving me opportunity, guidance and many ideas throughout the completion of this project. Every idea and guidance has helped me to find solution to improve the project in various aspects. Also, thanks to my family and friends who constantly gives me motivation and help in completing this project. Lastly, I want to thanks to Universiti Malaysia Pahang for giving me the opportunity to complete my final year project.

ABSTRAK

Teknologi semakin maju sepanjang tahun terutamanya apabila mempunyai tujuan untuk memudahkan kerja harian orang ramai. Peningkatan dalam teknologi dan elektronik telah membawa kepada penciptaan teknologibiometrik dimana orang dapat meningkatkan keselamatan mereka dalam pelbagai aspek. Keselamatan adalah salah satu perkara penting untuk membantu orang melindungi dan melindungi aset mereka sama ada aset fizikal atau aset elektronik. Oleh itu, cara paling maju untuk meningkatkan keselamatan adalah dengan menggunakan teknologi biometrik seperti pengenalan cap jari, pengenalan muka, pengiktirafan iris dan lain-lain. Keselamatan juga aspek yang paling penting dalam menggunakan Mesin Duit Automatik bank atau dikenali sebagai ATM yang membolehkan pengguna mengakses akaun bank mereka menggunakan kad bank dan nombor pin sebagai kata laluan. Walaubagaimanapun, terdapat beberapa masalah dengan kaedah tradisional dalam mengakses mesin ATM dimana pengguna terlupa kad bank mereka atau nombor pin digodam atau diketahui oleh pengguna yang tidak dibenarkan. Oleh itu, pelaksanaan teknologi biometrik digabungkan pada Mesin Duit Automatik (ATM) untuk meningkatkan keselamatan akaun pengguna memandangkan kaedah yang sedia ada tidak terjamin dan selamat. Kaedah ini membolehkan pengguna mengakses akaun mereka menggunakan hanya cap jari dan struktur muka mereka. Ini tidak boleh digodam kerana ciri unik berbeza untuk setiap orang dan ia tidak mungkin dicuri oleh orang lain. Pelaksanaan ini dibina dengan membina sebuah prototaip untuk mengesahkan kaedah biometrik lebih mudah dan lebih selamat daripada kaedah tradisional. Sebagai kesimpulan, laporan ini mendokumenkan ringkasan kaedah biometric cap jari dan pengenalan muka yang terbukti dapat meningkatkan keselamatan kerana ia menggunakan data yang berbeza untuk setiap orang dan bukannya data yang boleh diketahui atau digodam oleh pengguna yang tidak dibenarkan.

ABSTRACT

Technology is advancing throughout the years especially when it comes to facilitate people daily work. Improvement of the technology and electronic have led to creation of the biometric controlled technology where people can improve their security in various aspect. Security is one of the important thing to help people secured and protect their assets whether a physical assets or electronic assets. Therefore, the most advanced way to enhance the security is by using biometric controlled technology such as fingerprint, facial recognition, iris recognition and other. Security also the most important aspects in using the bank Automatic Teller Machine or known as ATM which allows the user to access their bank account using bank card and pin number as a password. However, there are issues with the traditional method in accessing ATM machine where the user forgot their bank card or the pin number is hacked or known by unauthorized user. Therefore, the implementation of biometric controlled technology is embedded to the Automatic Teller Machine (ATM) to improve the security of the user's account since the existing method is not necessarily secured and safe. This method allows the user to access their account using only their fingerprint and facial structure. This is hardly to be hacked as the unique features are different for each person and it is unlikely to be stolen by other people. This implementation is built by developing a prototype to verify the biometric method is easier and more secured than the traditional method. In conclusion, this report document the summary of the biometric method of fingerprint and facial recognition which is proven to improve the security as it uses the data that are different from each person instead of the data that can be known or cracked by unauthorized user.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ATM	Automatic Teller Machine
IDE	Integrated Development Environment
TAC	Type Allocation Code
CEO	Chief Executive Officer
SRS	Software Requirement Specification
SDD	Software Design Document
RUP	Rational Unified Process
RAD	Rapid Application Development

CHAPTER 1

INTRODUCTION

1.1 Introduction

Biometric sensor is an access control system and is becoming an important authentication and verification throughout the use of most of the system in the world. It is rapidly changing as the time goes with many people have try to improve and develop a more secured way of verification that is necessary in most of the system nowadays. It is classified into two types of sensor which is Physiological and Behavioral Biometrics. A few of the biometric sensor of Physiological Biometrics have been developed such as face recognition, fingerprint, and hand geometry. However, question have been raised about the safety of the other biometric sensor since it could be easily being manipulated and duplicated from the user to access the particular system.

Recent development in developing a biometric system has also led to Facial Recognition based for an authentication and verification in a certain system. Several systems have used the Facial Recognition based and it has been proven to be more secured and safe than the other verifications system that has ever been used before.

It is then will be use as a verification for the Automatic Teller Machine (ATM) which will be integrate with the fingerprint based system for the user to do any transaction available in the machine after the user has been verified for their account. Usually, ATM machine is using a Bank ATM card and 6 pin codes for the user to login or enter the machine. However, this type of verification is not quite secured since the pin code can easily been stolen or known to anyone.

1.2 Problem Statement

The problem statements of this project are described on the Table 1 below.

Table 1 Problem Statement

No.	Problem	Description	Effect
1.	Pin code can be hacked	ATM machine usually use a Bank Card and 6-pin code number as the password for the user to access their account by using this machine.	The method is affective yet it is not quite safe and secured since the 6-pin code can easily be stolen or hacked by anyone.
2.	User forget their pin code	The usual method of ATM machine also inefficient since the user have to remember their own pin code or have the pin code to be written somewhere they can easily have access to whenever they forget it.	It is not efficient for the user since the user can easily make a mistake and forget about their pin code when they need to use the ATM machine.
3.	Fingerprint can be duplicate	The verification data can be duplicated by someone else and they can access the user's account.	The account can be access and the account could be used for any fraud activities.

1.3 Goal and Objective

The goal of this project is to develop Facial Recognition and Fingerprin based for the Automatic Teller Machine (ATM) for a more reliable and secured verification process to enable the user to use the ATM machine features.

The objectives of the project are as follows:

i. To study a secured verification process to increase the security of the user's data.
ii. To develop a security system using a combination of Facial Recognition and Fingerprint Based for ATM machine.
iii. To verify the Facial Recognition implementation and Fingerprint improve the security system of the ATM.

1.4 Scope

The scopes of the project are as follows:

i. The development of this project is implemented using Microsoft Visual Studio 2019 with the reference and library of EmguCV and OpenCV.
ii. The Facial Recognition and Fingerprint based system on ATM machine prototype is develop using programming language of .Net and C#.
iii. The system is developed for the Automatic Teller Machine (ATM) verification process only.
iv. The focus of verification method only towards Facial Recognition and Fingerprint Based system.
v. The case study of this project only focuses on the customer who uses the ATM system.
vi. The data used in this project only for testing of the system only.

.

1.5 Report Organization

Chapter 1 of this project is discussing about the introduction of the project, the objective and also the scope of the project. The problem is also stated in this chapter to describe the problem which can be solved by developing the system of this project.

Chapter 2 describe about the literature review of the project. This chapter describes about the existing system that has been done and compares the existing system with the system which will be develop throughout this project.

Chapter 3 explains about the methodology of this project. It discuss about the approach and framework which will be use during the development of this project. It also explains about the hardware, software requirement and design and also the algorithm that is implemented in this project.

Chapter 4 is the implementation of this project. In this chapter, the development and testing of the system is carried out according to the methodology and design that have been explained in the previous chapter.

Chapter 5 is the conclusion of this project. It summaries the development of the project and also explains about the future work which can happen for the system that has been developed.

CHAPTER 2

LITERATURE REVIEW

2.1 Fingerprint and Facial Recognition

Fingerprint and Facial Recognition based is more reliable and secured because every person exist have a different feature of their face and have unique feature of their fingerprint and it is cannot be manipulated or duplicated from another person. The fingerprint uses the unique data which are retrieved using the fingerprint scanner to be used for verification purposes. The facial recognition uses the feature from the image captured from the camera and the unique information from the facial feature and structure is produce to match the facial feature in the database for verification purpose.

There are many types of fingerprint scanner which each scanner gives different type of Software Development Kit (SDK) and gives different level of accuracy. The fingerprint scanner that is embedded and implemented in this project is scanner from Digital Persona of One Touch UareU 4500. Their SDK provides a simple source codes for different programming language such as Csharp, Visual Basic, Java and etc. The source codes includes of simple functions to implement the fingerprint scanner such reading the fingerprint, verify and save the fingerprint template to the device.

Facial Recognition has many methods and technique which can be used to implement the facial recognition such as Support Vector Machine (SVM), Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), Kernel, EigenFace and etc. Dwivedi, Divyansh (2018, Apr 29). The method used in this project is EigenFace techniques with the use of Emgu CV and OpenCV. Emgu CV is a cross platform .Net wrapper to the OpenCV image processing library. This project uses this library to do the facial recognition process.

Facial Recognition process consists of four phases. First process is a pre-processing where the algorithm encodes the unique information of the facial image. The second process is feature extraction where it extracts the feature of the face such as nose, eyes, mouth and face structure. Third process is classification where the feature is classified into unique information for each person and the last process is feature model computation where the face data is retrieve from database and decodes to matching with the face detected. The feature considered in the facial recognition includes nose, eyes, mouth, face shape position, structure, size, and relationship among the feature.

2.2 Existing System

The existing systems of ATM machine are explained on the Table 2 below.

Table 2 Existing System Description

ATM System	Technology	Description
ATM Bank Card	Bank Card, 6-Pin Code	The user need to use their ATM bank card and the 6-pin codes as the pin number to access their account on ATM machine
Cardless ATM Withdraw	Phone Number, TAC Number, Collect Code	The user need to request for the cardless withdrawal in the application and request TAC for confirmation, then the user is allowed to withdraw the money using the collect code sent to the provided phone number
Fingerprint ATM	Fingerprint scanner	The user needs to access their account using the fingerprint scanner to extract the unique features of their fingerprint.

2.2.1 Bank ATM Card /6-Pin Code

ATM Machine is an Automatic teller machine which enables people to withdraw and deposit money from their bank accounts through the machines. The first ATM machine that used plastic cards similar to the current ATM bank card was created by Donald Wetzel in 1969 in United States. The ATM machine is improved to be used with bank card because it could offer a more convenience method for the customer to the standard bank transaction such as withdrawal money, bills payment, and other transaction. Nowadays, the customer could manage their own account affairs without the intervention of the bank. A standard ATM machine consists of devices of computer, magnetic/chip card reader, a keypad, a display screen, a printer and a vault.

Figure 1 Example of ATM Machine

The user will insert the ATM bank card into the card reader on the ATM machine. Then, the card reader will read the card and obtain the user information which contains in the card. After that, the user needs to insert the 6-pin code as the password

for their account before they could use the machine. The ATM machine will verify the pin codes given by the user. If it is verified, the user is allowed to use the ATM transaction of their account and the receipt will be printed out for each complete transaction whether it is successful or invalid. The vault in the ATM machine is where the money is kept for withdrawal purpose.

2.2.2 Cardless ATM Withdrawal

The first cardless ATM cash withdrawal in Malaysia was introduced by Malayan Banking Bhd (Maybank) where customers withdraw their money from ATM machine without using the ATM bank card. According to group head of Community Financial Services, Datuk Lim Hong Tat, cardless withdrawal is among the fastest, most convenient and affordable ways to send cash to family members and friends when they need the cash urgently. The feature of cardless ATM withdrawal is available to those who have a Maybank2u account which is an online application of Maybank which can easily be installed on the user's smartphone.

Figure 2 ATM interface for Cardless withdrawal

The user needs to have an online banking account to sign in into the online application or the user could create the account by register in the official website of the bank.

The cardless ATM withdrawal required the account, recipient phone number and name and the TAC and collect code which will be sent to the recipient phone number. The collect code will give access to the recipient to withdraw the money within the given time before the expiry date of the collect code.

The user needs to sign in to their online banking account and select the cardless withdrawal feature in the application. Then, the user need to enter required information such as recipient phone number and name. After that, the user need to request TAC number to verify the transaction and the collect code will be send to recipient phone number after a successful transaction on the application.

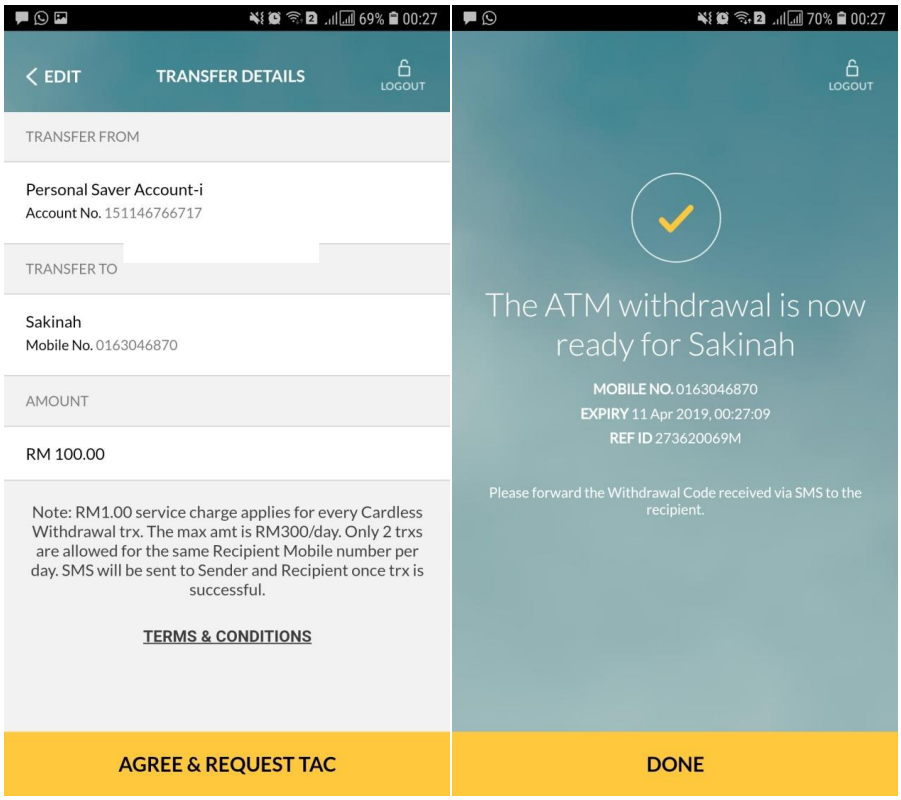


Figure 3 Online application for Cardless Withdrawal

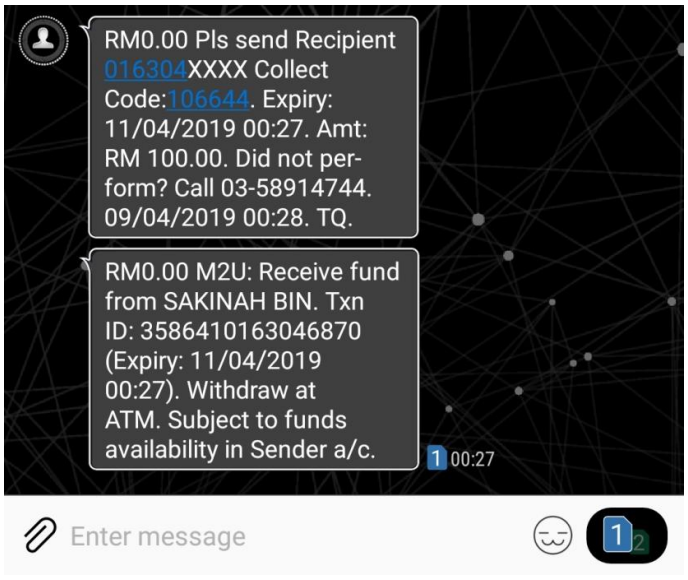


Figure 4 Message of Collect Code for receiver

2.2.3 Fingerprint ATM

Fingerprint ATM system has been developed by one of the South Africa's biggest banks, First National Bank which allow the users to open their account by scan their fingerprint. The fingerprint ATM system allows the user to open and access their account by scanning their fingerprint on the fingerprint scanner which attached and installed to the ATM machine. According to the FNB Points of Presence CEO Lee-Anne van Zyl, Fingerprint method deliver a better benefit in banking process especially for the citizen who rely on the outlets of the bank to do the basic banking services. The purpose of developing the fingerprint ATM system is mostly to increase the security of the ATM system which can prevent any fraud or manipulation data to access the user's account. The security of fingerprint system has been proven since it uses the fingerprint unique feature which extracted by the scanner and stored in the database. The unique feature is what the system use to differentiate between each user and also increase the security of the system.

Figure 5 Fingerprint ATM System

The fingerprint scanner usually is attached to the ATM system and installed within the system. When the user wants to log in to their account, they only need to scan their fingerprint and the system will verify the fingerprint in the database. When the verification is successful, the user is able to access all the function available in the ATM system using their registered account.

2.3 Comparison

Table 3 Comparison of existing systems

ATM System	ATM Bank Card	Cardless ATM Withdraw	Fingerprint ATM
Technology	Bank Card, 6-Pin Code	Phone Number, TAC Number, Collect Code	Fingerprint Scanner
Feature	Withdraw cash, Pay-in cash or cheques, Check Account Balance, Pay Bills, Transfer Money, Change Pin and Top up mobile phone	Withdraw cash only	Scan fingerprint, Withdraw cash, Pay-in cash, Check Account Balance, Pay Bills, Transfer Money, Change Pin and Top up mobile phone
Advantages	• Bank card easy to carry • The information can be retrieved from the card • The password can be change easily if the old password is known	• Easy and fast to use for emergency • Efficient verification using TAC number from the verified user • The collect code have a long duration before expiration	• Higher security • Easy and fast • More efficient
Disadvantages	• Bank card can easily be stolen • The bank card can be fraud • The user could forgot the password	• The recipient phone number might be not active • The collect code can easily be known by anyone	• Fingerprint can be duplicate

The comparison of the three existing systems shows that each system has their own advantages and disadvantages when it comes to security. The Fingerprint and Facial Recognition ATM System is developed to eliminate the disadvantages of the three systems. The fingerprint system itself consists of one problem where the fingerprint can be replicated using a few software or tools which makes the system not fully secured. Therefore, the combination of fingerprint and facial recognition eliminate the problem where the data can be duplicated by other people. Facial structure can be hardly be copied by other people since it features is attached to the owner's body.

2.4 Proposed Solution

The proposed solution to solve the problems in the existing system is ATM machine using Facial Recognition and Fingerprint Based ATM machine. The combination of Facial verification and Fingerprint verification is more secure and safe for the user than the existing systems above. Verification using Biometric Controlled is more secure because it is hardly can be duplicate or stolen. The unique feature of facial feature cannot be duplicate or stolen by another person which makes the ATM machine more secured.

2.5 Conclusion

In conclusion, this chapter describes the existing system features and what the existing system lack of which can be improved by the proposed system. The possible requirements of the proposed system have been gathered from this research to help solve the problems which occur on the existing system.

CHAPTER 3

METHODOLOGY

3.1 Introduction

Software development methodology plays an important role in developing a software system accurately and efficiently. There are many software development methodologies which can be chosen from. All factors must be taken into account when developing the software system to ensure the chosen methodology is the best for the system. Each methodology has its own way on how it works causing it to have advantages and disadvantages. In this chapter, the chosen methodology will be explained thoroughly on how it is used to develop Facial Recognition and Fingerprint Based ATM System.

This chapter also contains the documentation, tools and materials which will be used in developing the system according to the phases of the methodology chosen. For this system, Waterfall Model methodology is chosen as it is more suitable for the system than the other methodologies. The facial recognition and fingerprint recognition model also includes in this chapter.

3.2 Methodology

Other than common methodologies such as Agile, Rapid Application Development (RAD), Dynamic System, Rational Unified Process (RUP) and Spiral Model methodologies, the suitable methodologies for this system is Waterfall Model.

3.2.1 Waterfall Model

Software development process involving major elements in Software Development Life Cycle (SDLC) such as analysis and design. In recent time, Waterfall model is chosen as it is the traditional model that is used as an approach for developing software system. It consists of sequential phases throughout the development of the system. Each phases have a goals in which the team development to accomplish and completed before continue to the next phases in the model.

3.2.2 Why Waterfall Model?

i. Suitable for small projects which the requirements is known well
ii. Tools and materials is specific and understood
iii. Compatible with the development process of the system
iv. No redundant phases as a phase must be completed before proceed to the next phase

3.2.3 Advantageous of Waterfall Model

i. Model is simple and easy to understand and use
ii. Easy to manage due to the rigidity of the model
iii. Each phase deliver a specific process and goals
iv. Phases do not overlap

3.2.4 Waterfall Model Phases

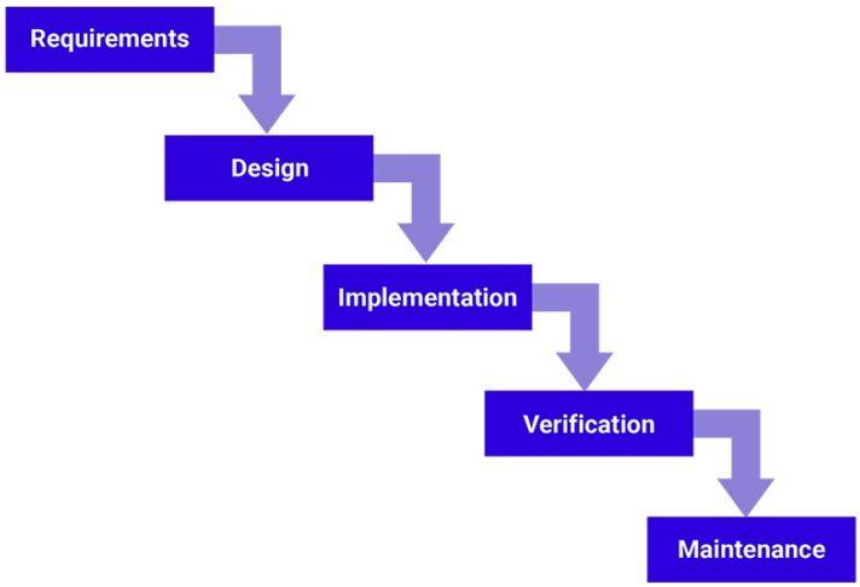


Figure 6 Waterfall Methodology

Waterfall Model consists of five phases which are Requirements, Design, Implementation, Verification and Maintenance.

i. Requirements

Requirements analysis is the first phase in the Waterfall model where it involves understanding the requirements for the system. Understanding the functionality and the specifications of the system to ensure the system is being developed accurately. In this project, the requirements of the system need to be understood such as the function of verification from ATM system, the function available after the ATM account is access, what the system needs to do for the data and other functional and non-functional. The requirements for the system are as follows:

i. The system should allow the administrator to log in using their username and password
ii. The system should allow the administrator to register new customer

iii. The system should verify the customer by their facial image
iv. The system should verify the customer by their fingerprint
v. The user is allowed to withdraw cash from the ATM system
vi. The user is allowed to check the balance of their account
vii. The user is allowed to transfer money to third party account

ii. Design

During this phase, the system design is prepared. It specifies the design and the architecture of the system. It also describe about the hardware and software which will be used for the development of the system. In this project, the system is designed by develop a context diagram and the architecture diagram to show the flow of the system. The database of the system also detailed by identifies the user or actor of the system and the data necessary to be record of each user and also the relationship between the entities. The design phase is documented in the Software Design Document where the database design and the module functions and variables in the system are described.

iii. Implementation

After the system has been carefully design, the development phase of the system is carried out. In this phase, the system design from the previous phase is being implemented to build the prototype of the system. In this project, the architecture of this prototype is object-oriented and developed using programming language of Csharp. The IDE used is Microsoft Visual Studio 2019. The database is run from localhost and each table of entity in the SDD document is created. The classes in the system are created based on the interface in the system and the class consists of functions which are used for input, output and verification purposes.

iv. Verification

In this phase, the system which has been developed is tested. The units which are developed will be tested to find any errors or bug which can cause a system failure. The ATM prototype is tested by three users. Each user will enter their own data and do the verification for fingerprint and facial recognition to access the ATM. Each test results in success and a

few issues is identified to improve the prototype such as the username must be hidden and the attempts for verification is limited to three attempts only.

v. Maintenance

The last phase in Waterfall model is maintenance where it involves making changes to the system to improve the performance and functionality of the system. From this phase, the previous phases of requirements, design, implementation and verification can be conducted again to do the modification to the system for any improvement of the system. In this phase, the system is improved and maintained by improve its interface to be more user-friendly and identifies which data can be changed or updated and eliminate the unnecessary function or data to improve its reliability.

3.2.5 Facial Recognition Model

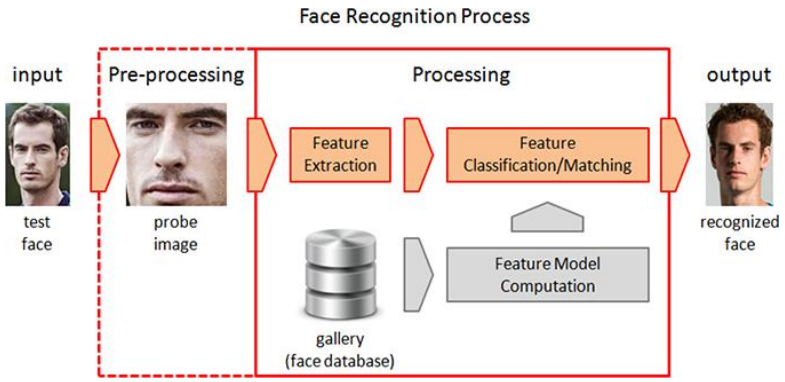


Figure 7 Facial Recognition

The facial recognition starts when the users position their frontal face on the system. The camera will detect facial image and test it as input for the system. Then, the *Pre-processing* stage. The system will capture the facial image detected and process it. It will ensure the image is clear and accurate, the required feature of the face is obtained for the third stage, feature extraction.

In feature extraction, the feature of the face such as nose, eyes, mouth, face shape position, face shape structure is obtain as initialization for the facial recognition techniques to identify the person.

The fourth stage of the model is feature classification/matching where the system classified the unique information obtain from the feature extraction stage and classified it to the particular person as their facial image data and the last stage is feature model computation where the data is insert into the database where the format of the data is change or the facial image data is use to match the data in the database for verification purpose.

3.2.6 Fingerprint Based Model

Figure 8 Fingerprint Based

Fingerprint based system starts when the user put their fingerprint on the fingerprint scanner attached to the system. The first stage of the model is image acquisition where the image of the fingerprint is obtained through the scanner.

The second stage is image processing. The image obtained is process where the fingerprint features is cleared and ensure the feature of the fingerprint can be read and extract. Third stage is feature extraction where the unique information from the fingerprint image is extract and encodes to unique information as the data of the particular person.

Fourth stage is the feature storage where the unique feature and information obtain inserted into the database. In this project, the fingerprint data is converted into binary data type and insert as *Varbinary* format in the *Sql* database.

3.3 Software Requirement Specification (SRS)

The SRS document will show the detail of context diagram, use cases and the framework of the Facial Recognition and Fingerprint based ATM system. SRS document is shown in Appendix A.

3.3.1 Context Diagram

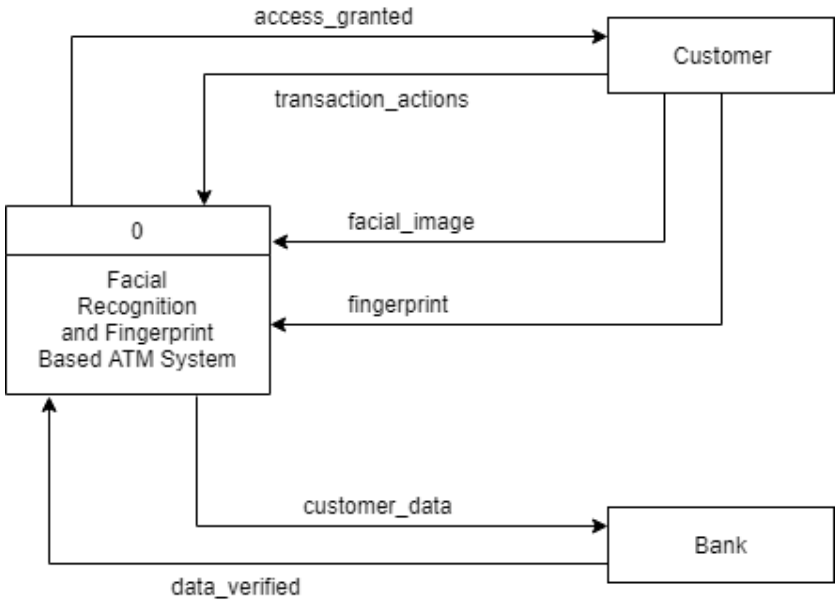


Figure 9 Context Diagram

3.3.2 Use Case Diagram

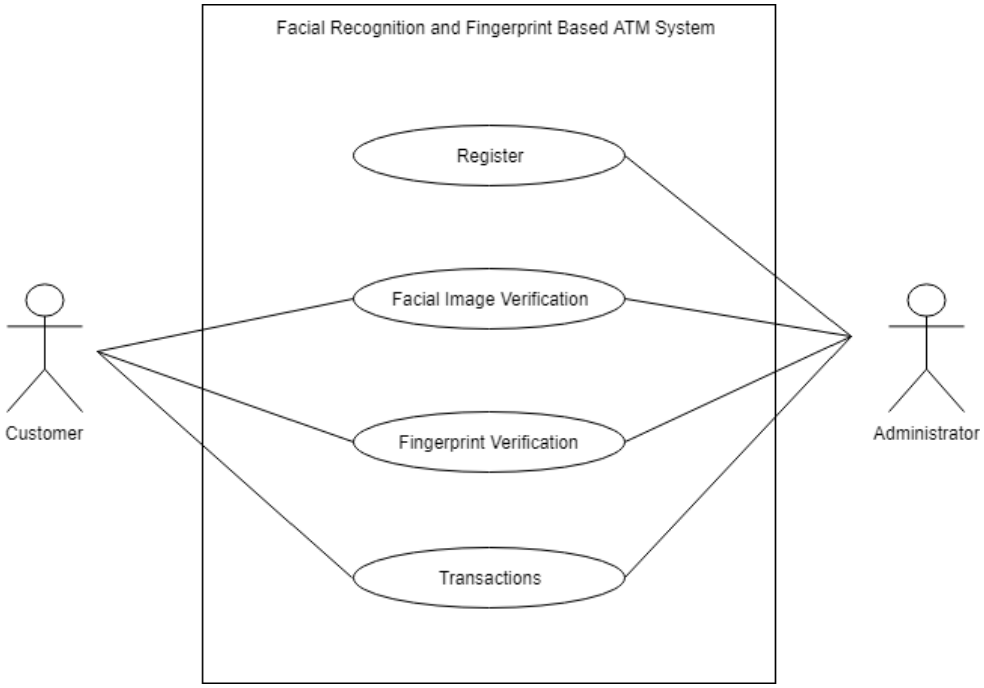


Figure 10 Use Case Diagram

3.4 Software Design Document (SDD)

The SDD document will show the general architecture and the package module of the system. It also defines the description classes in the system uses by the package module. SDD document is shown in Appendix B.

3.4.1 General Architecture

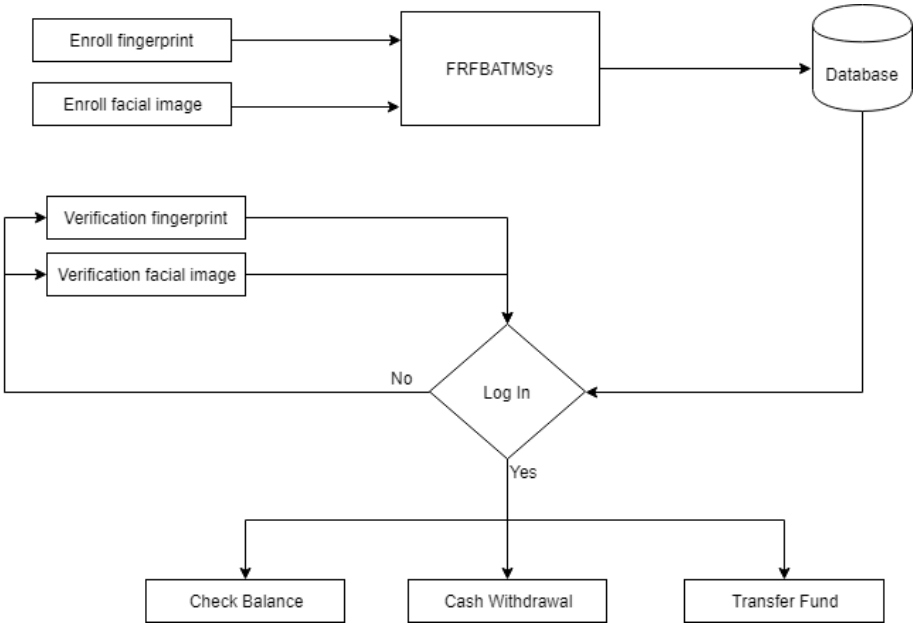


Figure 11 System Architecture

3.4.2 Package Module

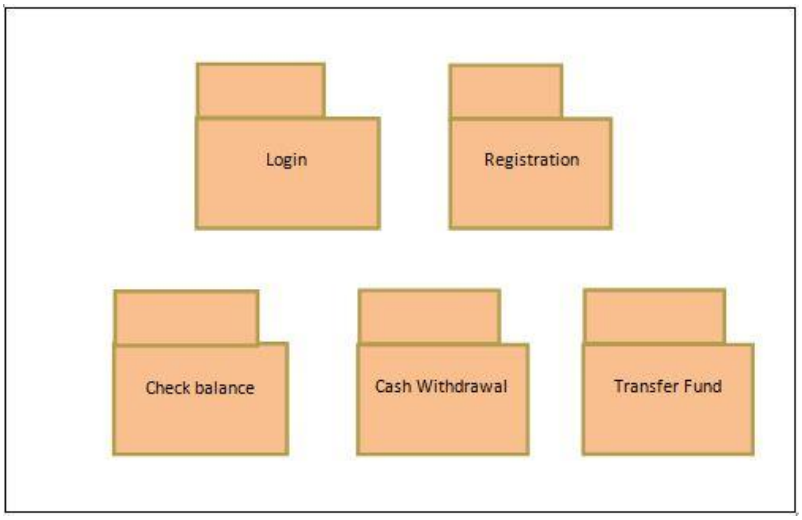


Figure 12 Package Module

i. Login

The login package is responsible for the user verification through the facial image and fingerprint verification after they insert their username.

ii. Registration

The registration package is responsible to allow the administrator to register new customer.

iii. Check Balance

The check balance package is responsible to give access to the user to check their balance account.

iv. Cash Withdrawal

The cash withdrawal package is responsible to allow the customer to access their account and allow them to withdraw their cash from their account

v. Transfer Fund

The package transfer fund allow the user to do a transfer transaction to the third party account

3.5 Software and Hardware Requirements

Table 4 Software Used

Software	Specification	Purpose
Microsoft Windows 10	Operating system platform	Operating system used to develop the system
Microsoft Word 2007	Microsoft Offices software	Software used to prepare the documentation of the system including SRS and SDD
Draw.io	Online Diagram Editor	The tool is used to construct diagram for documentation purposes
Microsoft Visual Studio 2019 with Emgu CV and OpenCV	Integrated Development Environment (IDE)	The software is used to develop the system
.NET and C#	Programming language	The software is build and develop using the suitable programming language

Table 5 Hardware Used

Hardware	Specification	Purpose
URU4500 Digital Persona Biometric Reader	Fingerprint scanner	The scanner is used to retrieve fingerprint from the user for verification purpose
Webcam Laptop ACER Aspire E 14	Camera	The camera is used to capture a facial image from the user
ACER Aspire E 14	Laptop	The laptop is used for development, implementation and testing the ATM system

3.6 Gantt Chart

Gantt chart will show the process of the development system from the beginning to the completion of the project. It will show the process of the development according to the Waterfall model phases. Gantt chart is shown in Appendix C.

3.7 Implementation

The implementation of the system is developed according to the phases of the methodology model which have been chosen above. The development of this project is conducted after the design phase is complete. The implementation of this system is using the hardware and software which stated in the Table 4 and 6. The system is fully implemented in the Microsoft Visual Studio 2019 using C# programming language. The library of *Emgu CV* and *OpenCV* is used to implement the facial recognition system and One Touch SDK is used to implement the fingerprint based system. ATM prototype is build combine with the verification system in the IDE mentioned above.

CHAPTER 4

RESULT AND DISCUSSION

4.1 Introduction

Biometric verification system has been around in the industry for a while where it uses a unique features in each person as their unique information to access their own data and other system. The implementation of the facial recognition and fingerprint based verification system has been developed for a long time to improve the security of many systems. The development of the biometric verification has been also implemented in the Automatic Teller Machine system to improve the security where the data of the user can be protected with a high security

4.2 Technique and Technology

4.2.1 Facial Recognition Technique

Facial Recognition that has been implemented in this system is using a built-in web camera and it captures the facial image of the user using *EigenFace* algorithm and the implementation of the algorithm include the image processing library of *Emgu CV* and *OpenCV* to captures the facial image and extract the unique features from the image.

4.2.2 Fingerprint Technology

Fingerprint system that has been implemented in this system is using DigitalPersona URU4500 scanner to retrieve a fingerprint from the user and the SDK provided with this device is implemented to extract the features from the fingerprint image for a registration and verification purposes.

4.2.3 Facial Recognition and Fingerprint Based ATM System

The Facial Recognition and Fingerprint Based ATM System is developed to improve the traditional ATM System where the user uses their Bank Card and Pin Number to access their bank account and access the ATM features such as cash withdrawal and check balance. The prototype of the system is developed using Microsoft Visual Studio 2019 using **C#** programming language including the image processing library of *Emgu CV* and *OpenCV* in the .NET platform. The system input output library also included to make the fingerprint scanner works. The further explanation and the flow of the system are described below.

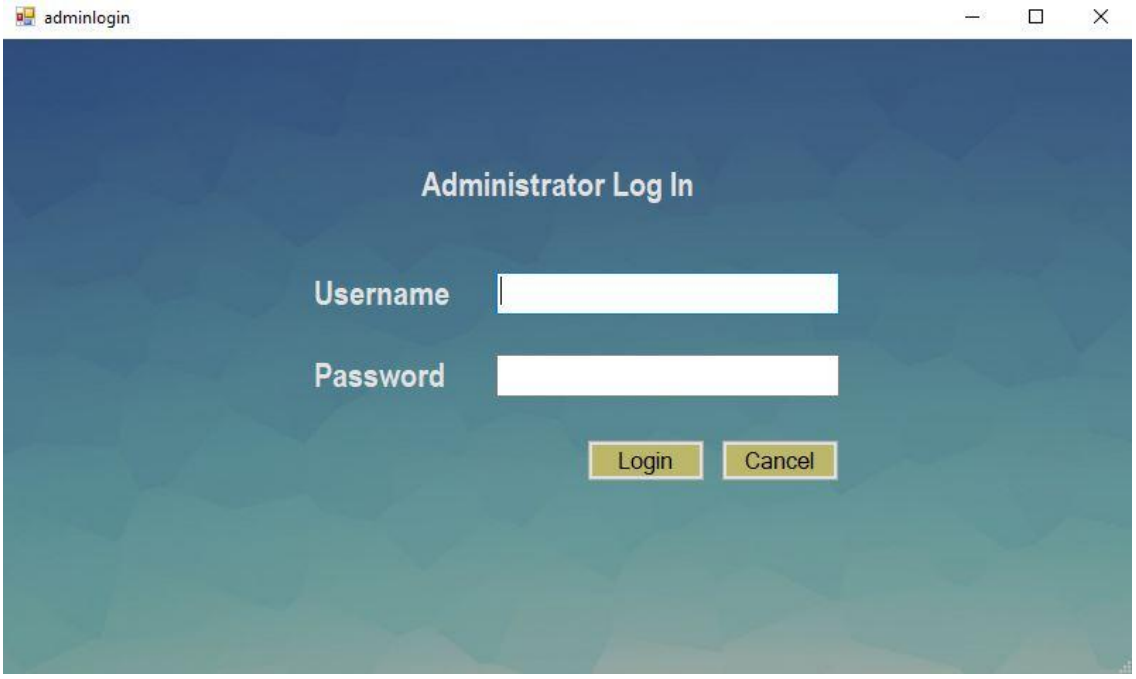


Figure 13 Administrator Login

Figure 13 shows that Administrator need to login before they can register a new customer to the system or update the customer profile. They have to insert their registered username and password and click 'Login' button. Cancel button will lead them to Main Page of the system.

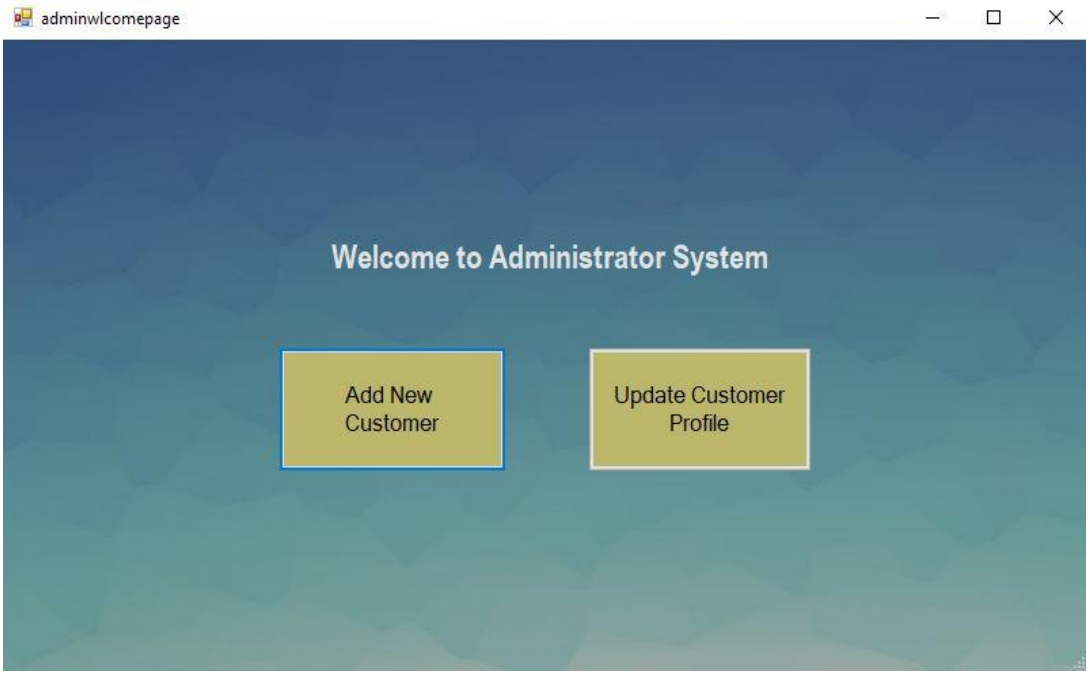


Figure 14 Administrator Features

Figure 14 shows the features that the administrator can do with the system. They can add new customer or update customer profile.

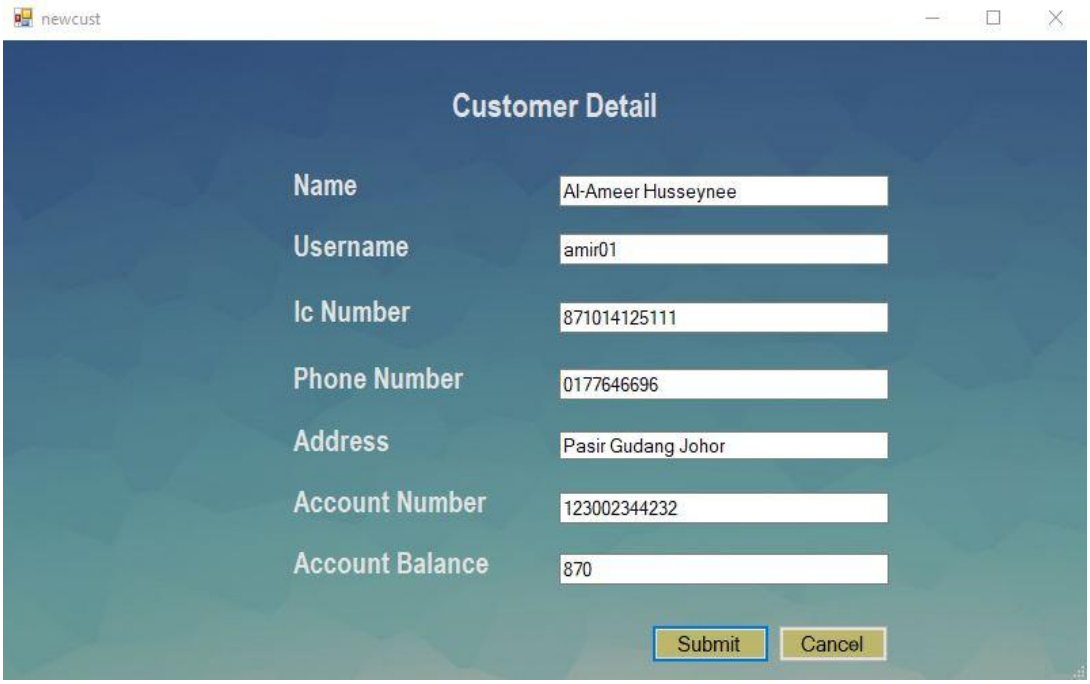


Figure 15 Register New Customer

Figure 15 shows that the information necessary for registration purposes. After administrator click ‘Submit’ button, the information will automatically register to the system database. Then, it will go to the next interface which the administrator required to register the customer’s fingerprint and facial image.

Figure 16 Register Fingerprint

Figure 16 shows that the customer’s fingerprint is scanned. The sample for the fingerprint needed is 4. After 4 samples are obtained, the fingerprint will be registered to the database if the sample set is good quality and correct. Below are the codes on how the fingerprint is insert into the database.

```
base.Process(Sample);

// Process the sample and create a feature set for the enrollment purpose.
DPFP.FeatureSet features = ExtractFeatures(Sample, DPFP.Processing.DataPurpose.Enrollment);

// Check quality of the sample and add to enroller if it's good
if (features != null) try
    {
        //MakeReport("The fingerprint feature set was created.");
        Enroller.AddFeatures(features);     // Add feature set to template.
    }
    finally
    {
        // Check if template has been created.
        switch (Enroller.TemplateStatus)
        {
            case DPFP.Processing.Enrollment.Status.Ready:   // report success and stop capturing
                MemoryStream fingerprintData = new MemoryStream();
                Enroller.Template.Serialize(fingerprintData);
                byte[] fpt = fingerprintData.ToArray();


                SqlConnection con = new SqlConnection(@"Data Source=(LocalDB)\MSSQLLocalDB;AttachDbFilename=C:\Users\acer\Desktop
                string query = "UPDATE customer SET custFingerprint = @custFingerprint WHERE custName = '"+newcust.name1+"'";

                SqlCommand cmddb = new SqlCommand(query, con);
                cmddb.Parameters.Add("@custFingerprint", SqlDbType.VarBinary).Value = fpt;

                try
                {
                    con.Open();
                    cmddb.ExecuteReader();
                    MessageBox.Show("The fingerprint have been added to the system!");
                    Stop();
```

Figure 17 Enroll Fingerprint

The fingerprint is serialized before it converts to byte variable to insert into the database column that has data type of *Varbinary* for the fingerprint.

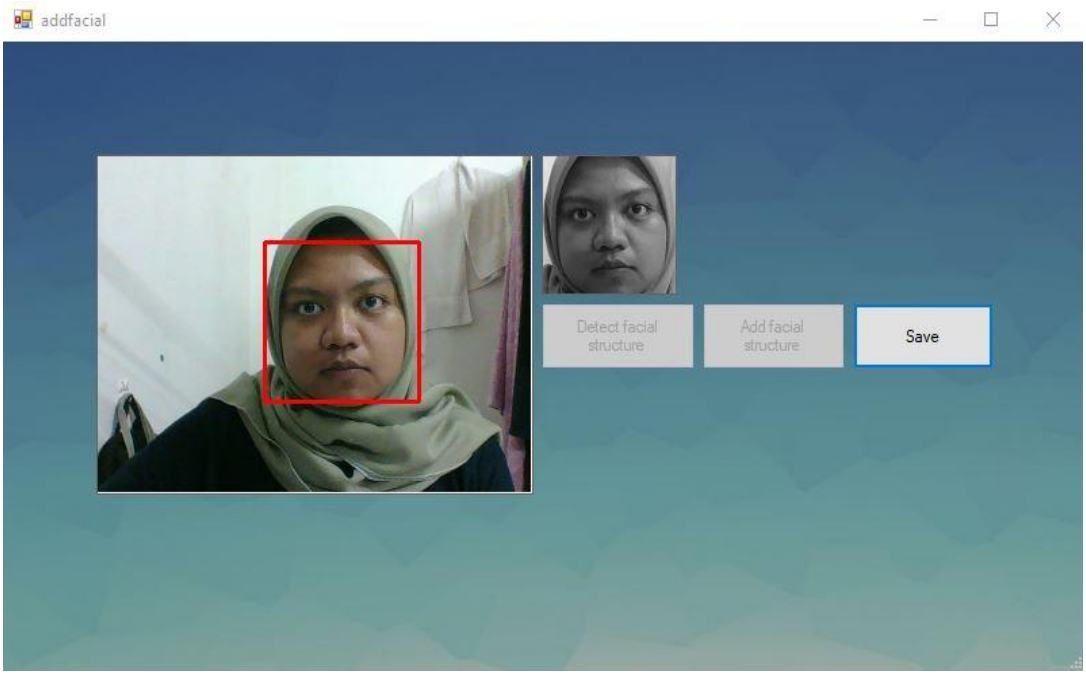


Figure 18 Register Facial Image

Figure 18 shows that the facial image of customer is captured. The first button, 'Detect facial structure' is click to start the camera to find the facial image. After that, the 'Add facial structure' button is click to capture the complete facial image. Then, administrator need to click the 'Save' button to register the facial image to the database. After the facial image registration is complete, the system will go back to the main page of the administrator.

```
//Action for each element detected
foreach (MCvAvgComp f in facesDetected[0])
{
    t = t + 1;
    result = currentFrame.Copy(f.rect).Convert<Gray, byte>().Resize(100, 100, Emgu.CV.CvEnum.INTER.CV_INTER_CUBIC);
    //draw the face detected in the 0th (gray) channel with blue color
    currentFrame.Draw(f.rect, new Bgr(Color.Red), 2);


    if (trainingImages.ToArray().Length != 0)
    {
        //TermCriteria for face recognition with numbers of trained images like maxIteration
        MCvTermCriteria termCrit = new MCvTermCriteria(ContTrain, 0.001);

        //Eigen face recognizer
        EigenObjectRecognizer recognizer = new EigenObjectRecognizer(
        trainingImages.ToArray(),
        labels.ToArray(),
        5000,
        ref termCrit);

        name = recognizer.Recognize(result);

        //Draw the label for each face detected and recognized
        //currentFrame.Draw(name, ref font, new Point(f.rect.X - 2, f.rect.Y - 2), new Bgr(Color.LightGreen));

    }

    //Set the number of faces detected on the scene
    label3.Text = facesDetected[0].Length.ToString();

}
t = 0;
```

Figure 19 Add Facial Images

This is the source code where the system use *EigenObjectRecognizer* to do the recognition of the faces detected on the camera.

```
        BinaryFormatter formatter = new BinaryFormatter();
        formatter.Serialize(ms, TrainedFace);
        fs = ms.ToArray();
    }

    SqlConnection con = new SqlConnection(@"Data Source=(LocalDB)\MSSQLLocalDB;AttachDbFilename=C:\Users\acer\Desktop\AtmSystem1\
    string query = "UPDATE customer SET custfacialimage = @custfacialimage where custName = '"+newcust.name1+"'";

    SqlCommand cmddb = new SqlCommand(query, con);
    SqlParameter param = cmddb.Parameters.Add("@custfacialimage",SqlDbType.VarBinary);
    param.Value = fs;

    try
    {
        con.Open();
        cmddb.ExecuteNonQuery();
        MessageBox.Show("The facial image is added!");

        this.Hide();
        MainPage back = new MainPage();
        back.ShowDialog();

    }
    catch (Exception ex)
    {
        MessageBox.Show(ex.Message);
    }
}

0 references
public addfacial()
{
    InitializeComponent();
    //Load haarcascades for face detection
    face = new HaarCascade("haarcascade_frontalface_default.xml");
```

Figure 20 Data Serialization

The facial data also serialized before it is insert into the database to ensure it is accurate data when it is retrieved from the database to the verification for login.

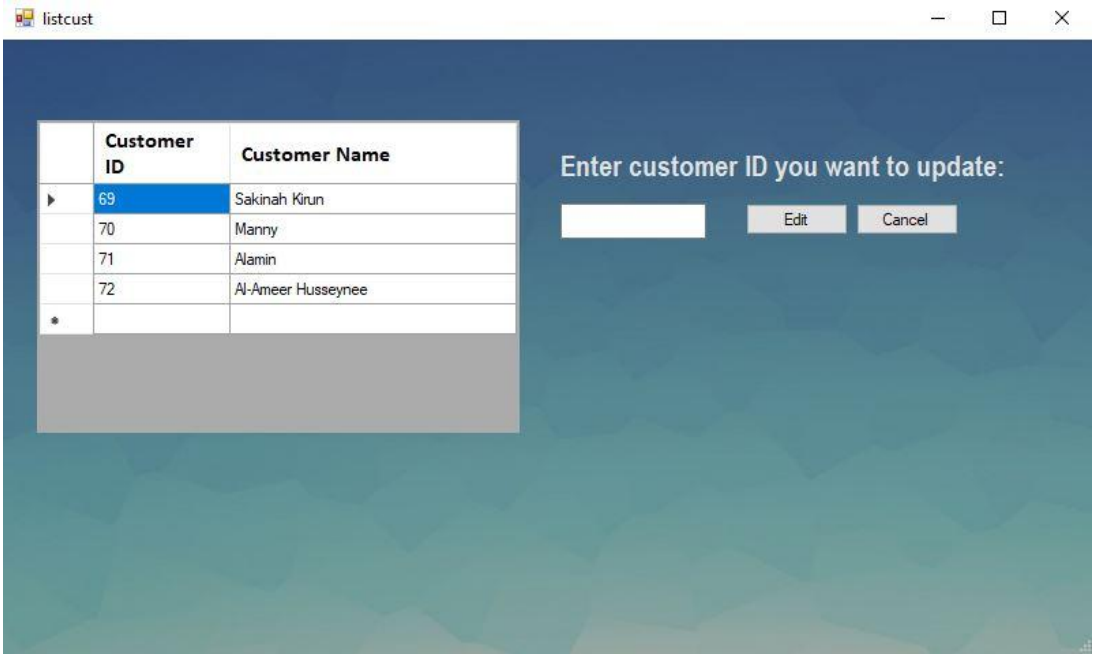


Figure 21 Customer List

Figure 21 shows that the existing customer in the system. The administrator needs to enter the customer id of the customer that needs to update their information. This list can also be used to check if the customer already registered to the system or not.

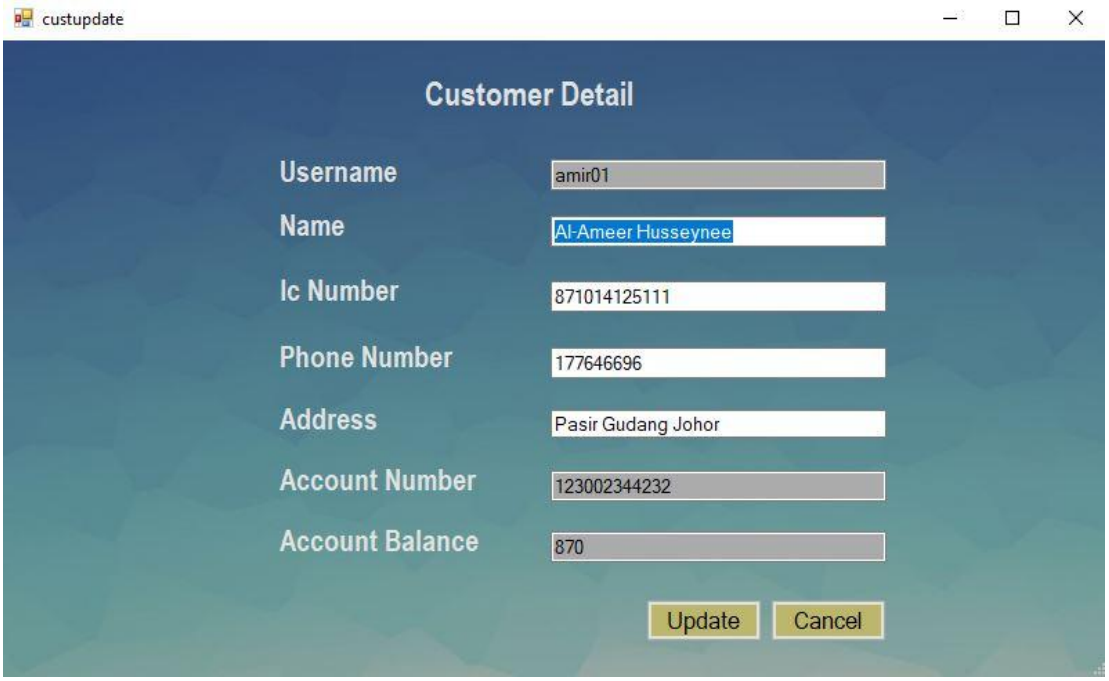


Figure 22 Update Customer Information

Figure 22 shows that the customer information that can be updated by the administrator. However, the username, account number and account balance cannot be edited since the bank policy where it does not allow the account information to be changed once registered. Only the customer name, IC number, phone number and address can be edited and update in the system.

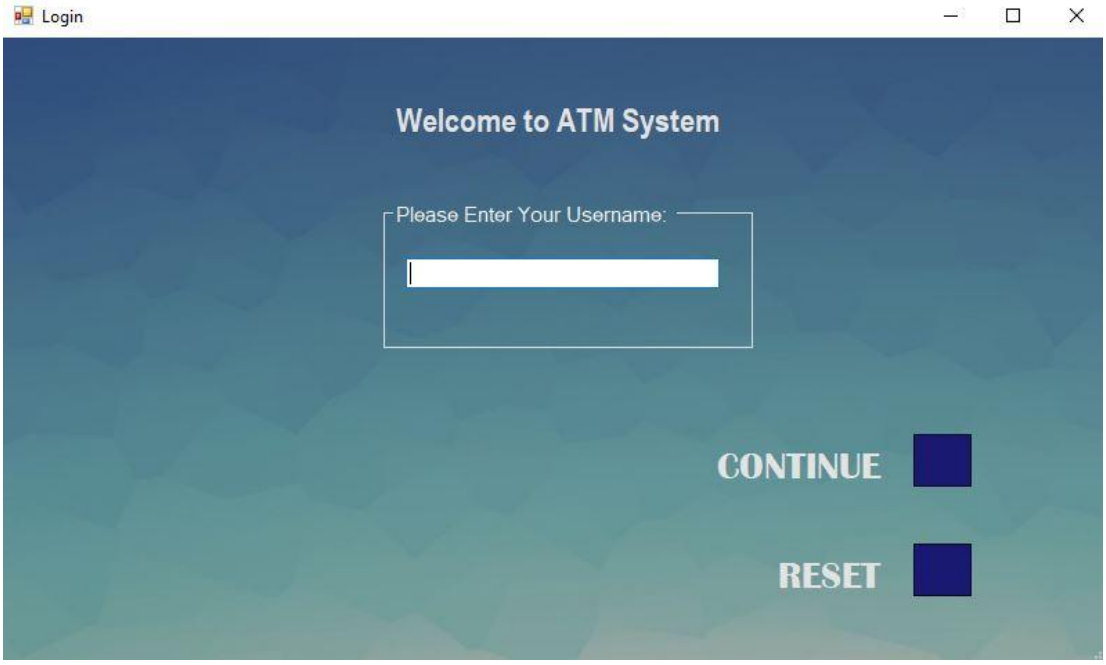


Figure 23 Customer Login

Figure 23 shows the login page where the customer required inserting their username before they can verify their fingerprint and facial image to access the ATM system. After they click 'Continue' button, it will go to the next page where the customer need to verify their fingerprint. 'Reset' button is to reset the username textbox incase the customer enter a wrong username.

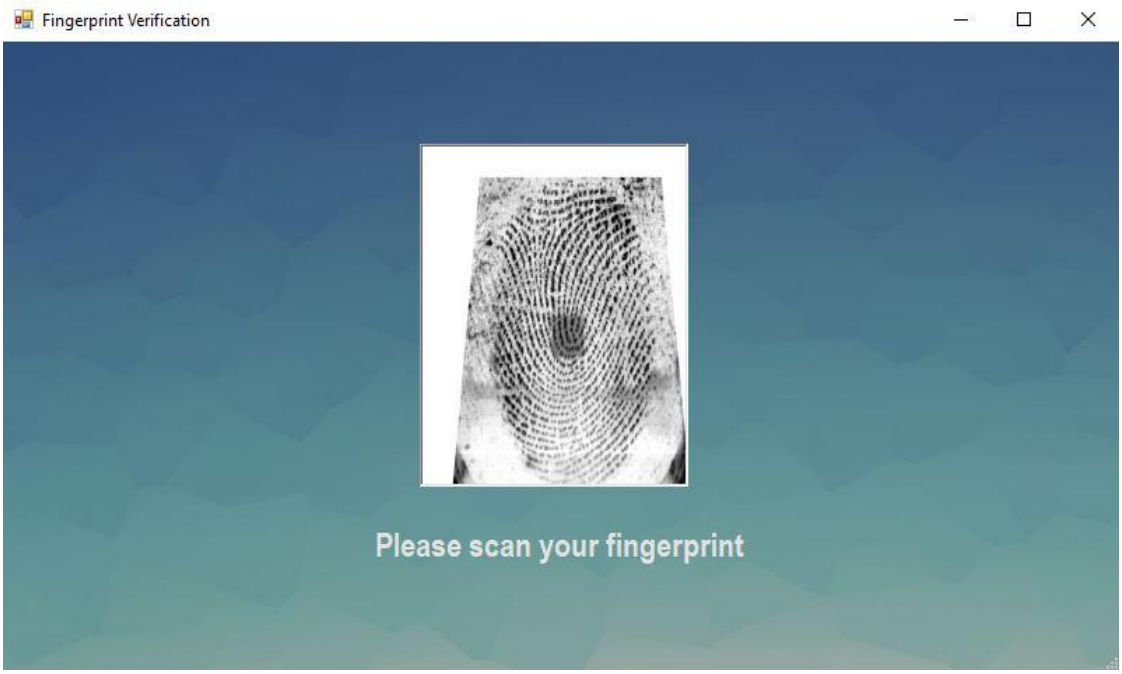


Figure 24 Fingerprint Verification

Figure 24 shows the fingerprint verification. The customer need to scan their fingerprint on the fingerprint scanner attached to the machine. After the fingerprint image is obtained, it will be used to match with the fingerprint data in the database. It is matched, the page will go the next verification method which is Facial Image Verification. Below is the source code where the system retrieve the data from database and verifies the data with the new captured data.

```
1 reference
public ReadFP(DPFP.Template template1)
{
    Template = template1;
    InitializeComponent();
}

5 references
protected override void Init()
{
    base.Init();
    base.Text = "Fingerprint Verification";
    Verificator = new DPFP.Verification.Verification(); //Verification

}

5 references
protected override void Process(DPFP.Sample Sample)
{
    base.Process(Sample);

    features = ExtractFeatures(Sample, DPFP.Processing.DataPurpose.Verification);

    if (features != null)
    {
        DPFP.Verification.Verification.Result resFP = new DPFP.Verification.Verification.Result();
        Verificator.Verify(features, Template, ref resFP);

        if (resFP.Verified)
        {
            status = 1;
            MessageBox.Show("Fingerprint is verified!");

            this.Hide();
            ReadFacial cust = new ReadFacial();
            cust.ShowDialog();
```

Figure 25 Fingerprint Verification

```
1 reference
private void Button3_Click(object sender, EventArgs e)
{
    if (unameBox != null)
    {
        uname1 = unameBox.Text;

        byte[] fpdata2 = GetCustFP();

        if (fpdata2 != null)
        {
            MemoryStream fingerprintData = new MemoryStream(fpdata2);

            DPFP.Template template1 = new DPFP.Template();
            template1.DeSerialize(fingerprintData);

            this.Hide();
            ReadFP match = new ReadFP(template1);
            match.ShowDialog();

        }
        else
        {
            MessageBox.Show("Username Not Found!");
        }
    }
```

Figure 26 Deserialization Data

The fingerprint that is retrieved from database is deserialized and assign to template variable. The template variable and the captured fingerprint is then processed for the verification.

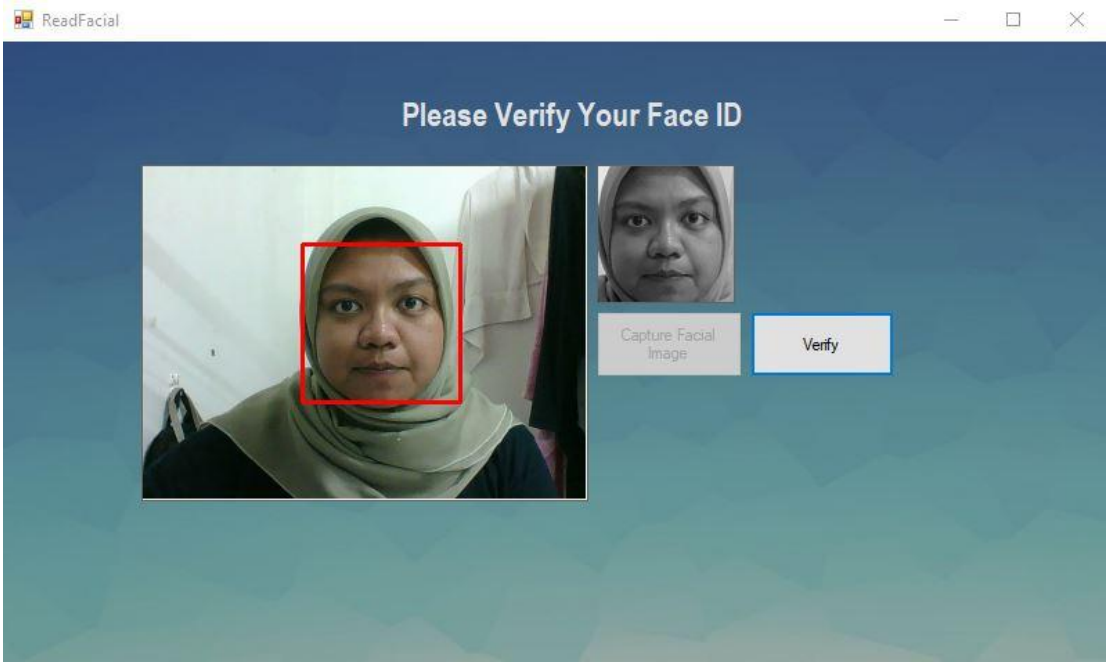


Figure 27 Facial Image Verification

Figure 27 shows that the facial image is captured for verification purposes. The system will load the camera to allow the customer to capture their facial image when they click the 'Capture Facial Image' button. Then, the customer need to click 'Verify' button to verify the facial image captured with the facial image data in the database. If the verification is successful, the customer is allowed to access the main page of the ATM machine and use the ATM features.

```
1 reference
private void Button3_Click(object sender, EventArgs e)
{
    SqlConnection con = new SqlConnection(@"Data Source=(LocalDB)\MSSQLLocalDB;AttachDbFilename=C:\Users\acer\Deskt
    string query = "Select custfacialimage From customer where custUsername = '" + Login.uname1 + "'";

    SqlCommand cmddb = new SqlCommand(query, con);
    SqlDataReader myReader;

    try
    {
        con.Open();
        myReader = cmddb.ExecuteReader();

        while (myReader.Read())
        {

            facedata = (byte[])(myReader["custfacialimage"]);

        }

        using (MemoryStream ms = new MemoryStream(facedata))
        {
            BinaryFormatter formater1 = new BinaryFormatter();
            faceDataDS = (Image<Gray, byte>)formater1.Deserialize(ms);
            string result = RecognizeFace(faceDataDS);
        }

        if (result != null)
        {
            MessageBox.Show("Verified!");
```

Figure 28 Data Retrieval

```
public string RecognizeFace(Image<Gray, byte> faceDataDS)
{
    num = num + 1;
    current = faceDataDS.Resize(300, 250, INTER.CV_INTER_CUBIC);
    Image<Gray, byte> grayScale = current.Convert<Gray, byte>();

    faceDatass.Add(faceDataDS);
    faceLabel.Add("User");

    faceDatass.Add(TrainedFace);
    faceLabel.Add("User");

    MCvAvgComp[][] detected = grayScale.DetectHaarCascade(face, 1.2, 10, Emgu.CV.CvEnum.HAAR_DETECTION_TYPE.DO_CANN
    foreach (MCvAvgComp d in detected[0])
    {
        if (faceDataDS.ToString().Length != 0)
        {
            Image<Gray, byte> dFace = current.Copy(d.rect).Convert<Gray, byte>().Resize(100, 100, Emgu.CV.CvEnum.INT
            MCvTermCriteria criteria = new MCvTermCriteria(num, 0.001);  //count, epsilon value
            EigenObjectRecognizer recognize = new EigenObjectRecognizer(faceDatass.ToArray(), faceLabel.ToArray(),

            MCvFont font = new MCvFont(FONT.CV_FONT_HERSHEY_TRIPLEX, 1, 1);

            name1 = recognize.Recognize(dFace);
            //current.Draw(name, ref font, new Point(d.rect.X - 2, d.rect.Y - 20), new Bgr(Color.Red));
        }
    }

    if (name1 != null)
    {
        string status = "verified";
        return status;
```

Figure 29 Add Data to Training Images

The facial data is retrieved from database and *DeSerialized*. After that, the data is passed to *RecognizeFace* function where the verification process is being done. The

data from database is added to the training images and the process uses *EigenObjectRecognizer* to compare the accuracy between the training images. If it is matches, the algorithm will retrun value empty where it is considered as verified.

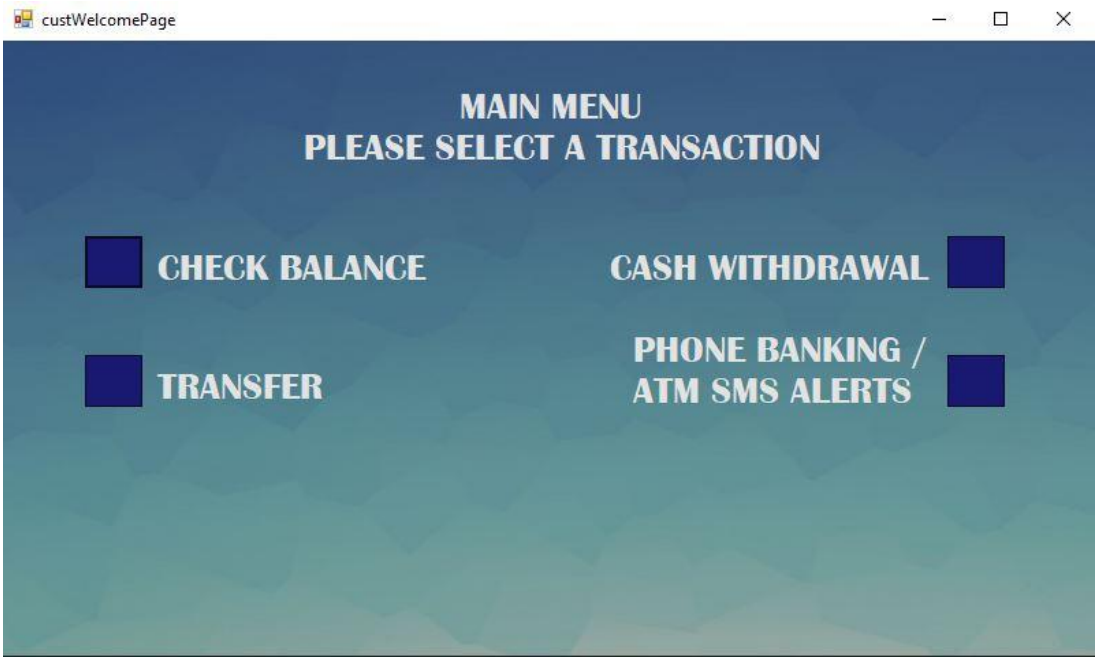


Figure 30 Customer Main Page

Figure 30 shows the main page of the customer after they have successfully login to the system by verifying their fingerprint and facial image.

CHAPTER 5

CONCLUSION

5.1 Introduction

This chapter describes about the conclusion of this project the implementation of the system in this project.

5.2 Conclusion

The security of a system has become more unsafe with the advanced technology that has been developed around the world. It has affected the traditional or the old way of verification where a few systems uses username and password or pin number where it can easily be hacked or known by unauthorized person. By doing this, one's data and personal information is not secured and can be access by other people. However, the latest improvement in security developed is fingerprint system where the users access their data by using their fingerprint. This project purpose is to implement the fingerprint system and improve its security by adding another verification feature where it uses the facial recognition of the user. The system has improved the security features of the ATM system and helps the user to access their account easier.

The implementation of the system is developed using Microsoft Visual Studio 2019 in C# programming language with the use of fingerprint scanner, DigitalPersona URU 4500 and the image processing library of *Emgu CV* and *OpenCV*. The process of the system start when the user access the customer ATM System and they are required to scan their fingerprint and capture their facial image. If the fingerprint and their facial image are verified, then they can access their account and use the ATM features such as cash withdrawal or check balance.

Other than that, the implementation of this system has improved the security and ensures the login process of ATM System is easier. There are many improvements can

be made to the system along with the development of more advanced technology in the future.

5.3 Research Constraint

The implementation of this system challenging since there are not many resources can be obtained. The lack of knowledge also is one of the constraints in the implementation of this system.

5.4 Future Works

Future works of this system can be done by improving the biometric verification method accuracy where it can identify the unique information of a person more accurately. Other than that, the verification method can also be implementing in other system such as Attendance Management System.

REFERENCES

Bansal, Ankur., Agarwal, Mukesh., Sharma, Anima., & Gupta, Anindya. (2013). A Review Paper on Facial Recognition. *Recent and Innovation Trends in Computing and Communication, 1*(4), 224-228.

Hatter, Kathryn. The Disadvantages of Using an ATM Card. (2013, October 21). Retrieved from https://pocketsense.com/disadvantages-using-atm-card-9370.html

R.Arokiasamy, Steven. (2018). *Fingerprint Based Automatic Teller Machine*. Gambang, Pahang: Universiti Malaysia Pahang.

MjroBot. Real-Time Face Recognition: An End-to-End Project. (2018, February 23). Retrieved from https://www.hackster.io/mjrobot/real-time-face-recognition-an-end-to-end-project-a10826

What are the reasons behind the invention of an ATM machine? (2018, May 10). Retrieved from https://www.quora.com/What-are-the-reasons-behind-the-invention-of-an-ATM-machine

Maybank debuts cardless ATM withdrawal. (2017, March 31). Retrieved from https://themalaysianreserve.com/2017/03/31/maybank-debuts-cardless-atm-withdrawal/

Talking ATM to help those with visual disabilities. (2016, Jan 14). Retrieved from https://www.straitstimes.com/singapore/talking-atm-to-help-those-with-visual-disabilities

A.A. Adenowo, Adetokunbo., A. Adenowo, Basirat. (2013). Software Engineering Methodologies: A Review of the Waterfall Model and Object Oriented Approach. *International Journal of Scientific & Engineering Research, 4*(7), 427-434.

Sharma, Lakshay. Waterfall Model (2016, April 17). Retrieve from https://www.toolsqa.com/software-testing/waterfall-model/

Morley, John. (2014). *Academic Phrasebank*. Manchester: The University of Manchester.

Bhanushali, Nisha., Chapaneria, Meghna., Mehta, Krishani., Rathod, Mansing. (2017). Fingerprint based ATM System. *Journal for Research, 2*(12), 31-34.

Perala, Alex. South African Bank Becomes Biometric ATM Pioneer. (2018, May 7). Retrieved from https://findbiometrics.com/south-african-bank-biometric-atm-505075/

Dwivedi, Divyansh. Face Recognition for Beginners. (2018, Apr 29). Retrieved from https://towardsdatascience.com/face-recognition-for-beginners-a7a9bd5eb5c2

Lal. Madan., Kumar, Kamlesh. (2018). Study of Face Recognition Techniques: A Survey. *(IJACSA) International Journal of Advanced Computer Science and Applications,* 9(6), 42-29.

APPENDIX A

FACIAL RECOGNITION AND
FINGERPRINT BASED ATM SYSTEM

FACULTY OF COMPUTING

SOFTWARE REQUIRMENT SPECIFICATION (SRS)

1.0 Introduction

1.1 Purpose

In this SRS document, it will provide the requirements and constraints of the Facial Recognition and Fingerprint Based ATM System. It also describes on the system functions, features and how is it expected to perform based on the requirements propose. This document written to make stakeholder and developer understand more about the system.

1.2 System Identification

This Software Requirement Specification (SRS) belongs to: Facial Recognition and Fingerprint Based ATM System

System Title	:	FRFB_ATMSys
System Abbreviation	:	FRFB_ATMSys_v01
System Identification Number	:	FRFB_ATMSys001

1.3 References

- R.Arokiasamy, Steven. (2018). Fingerprint Based Automatic Teller Machine. Gambang, Pahang: Universiti Malaysia Pahang.
- Morley, John. (2014). Academic Phrasebank. Manchester: The University of Manchester.

1.3 System Overview

The system has four modules which are register, facial image verification, fingerprint verification and transactions.

The system will be used by the customer and administrator which act as the actor of the system. The system allows the customer to log in to the ATM system by verifying their facial signature and fingerprint which will be compared to the data in the database. If the facial signature and fingerprint is verified, the system will give access to the customer to do the transaction available in the system. The transactions available in the system are cash withdrawal, transfer fund and check balance of their account. The facial image and fingerprint are retrieved from customer using the web camera on the laptop and fingerprint scanner which are installed to the ATM system.

The administrator will act as a user who will register a new customer to the ATM system. The administrator will log in to the system and they will add detail of the new customer to the database including their facial image and fingerprint. After the new customer is registered, they can log in to the ATM system through the ATM verification process of facial recognition and fingerprint authentication.

2.0 System Description

2.1 System Perspective

The system will request for facial image and fingerprint from the user which is customer. Then, both data will be sent to the database to verify with the data which is stored in the database. After the data is verified, the system will give access to the customer to make transactions on the ATM system which they can make a cash withdrawal, transfer fund or check the balance of their account. Figure 1 show the interaction between the customer and the system.

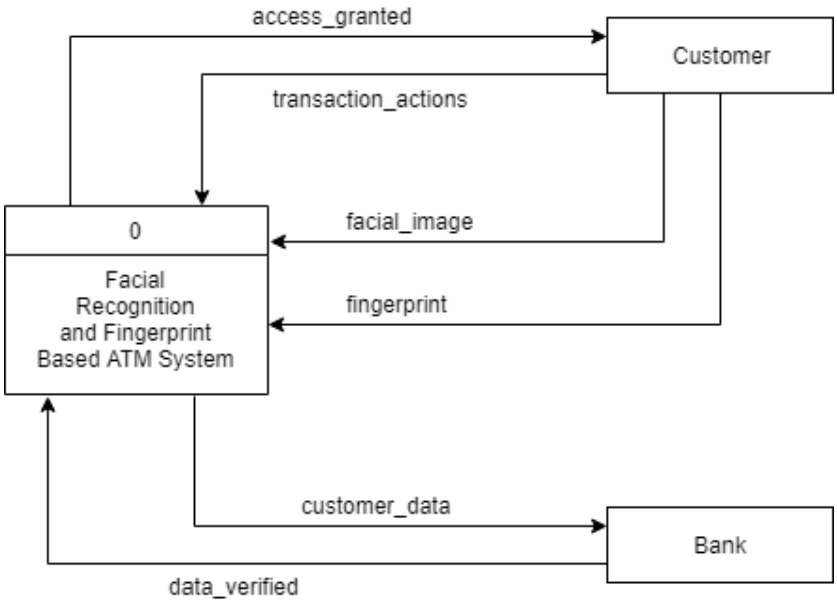


Figure 1: Context Diagram

2.2 System Interfaces

Refer Appendix A.1

2.3 System Functions

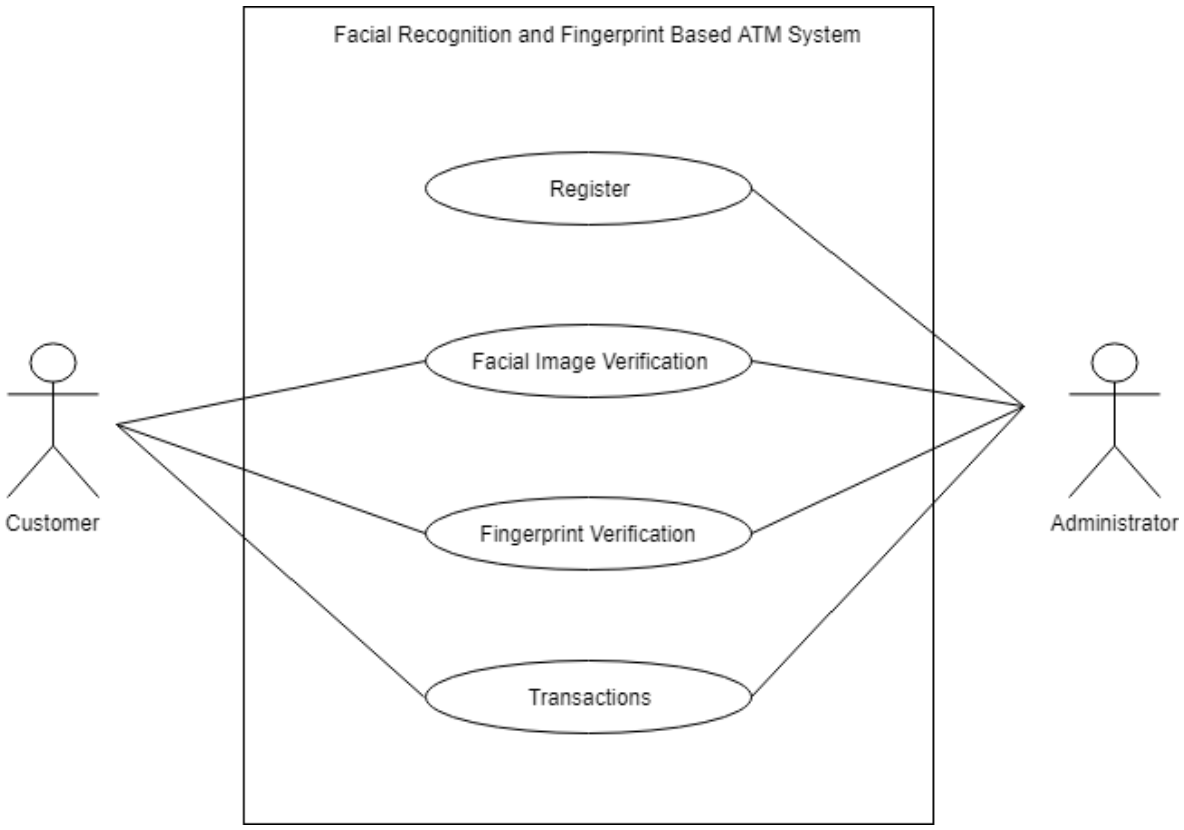


Figure 2: Use Case Diagram

2.4 User Characteristics

User	Education Level	Experience and Technical Expertise
Customer	Any education level	• Basic experience in using ATM system • Able to read and understand English language
Administrator	Diploma or higher education level	• Able to use ATM system for registration • Experience in using Database system

Table 1: User Characteristics

2.5 Constraints

The constraints of the ATM system are as follows:

i. The system should follow the bank policies of ATM system.
ii. The developer should develop the system using a higher-order programming language.
iii. The system should protect the data of the customers.
iv. The verification should not take more than 5 seconds.
v. The features of the ATM system must be easy to understand by the user.
vi. The system should only retrieve data using the hardware which are installed to the system.

2.6 Assumptions and Dependencies

Assumptions:

i. The customer must be at least 16 years old.
ii. The customer must have register to the system with a valid facial image data and fingerprint data to use the system.
iii. The customer is assumed to have a basic knowledge of using the ATM system.

Dependencies:

i. The system required the facial image camera and fingerprint scanner to run properly.

3.0 Specific Requirement

3.1 System Features

3.1.1 Register

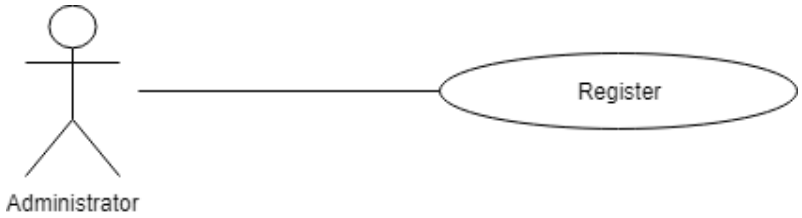


Figure 3: Register Use Case

Use Case ID	Mod_01
Brief Description	This use case is to allow the administrator to register new customer to the ATM system
Actor	Administrator
Pre-conditions	1. The administrator must be an authorize user
Basic Flow	1. The use case begins when the user log in to the system using their username and password. **[E1: Invalid username or password]** 2. The system displays two options for the user. **[A1:Add New Customer][A2:Update Customer Profile]** 3. The use case ends.
Alternative Flow	A1:Add New Customer 1. 1. The user enters the new customer's data. 2. The user click 'Submit' button to insert the data into the database. 3. The system show fingerprint registration interface. 4. The customer scans their fingerprints 4 times. **[E2: Invalid fingerprint samples]** 5. The fingerprint is registered to the database. 6. The system show facial image registration interface.

	7. The user click ‘Detect Facial Structure’ button to start the camera. 8. The user click ‘Add Facial Image’ button to capture the facial image of the customer. 9. The user click ‘Save’ button to insert the facial image data in the database. 10. The use case ends. A2: Update Customer Profile 1. The user enter customer id that want to be updated. 2. The system shows the customer information that can be edited and update 3. The user updates the information. 4. The user click ‘Update’ button. 5. The system updates the information in the database.
Exception Flow	E1: Invalid username or password 1. The user not allowed to log in to the system 2. The user enters the username and password again. 3. The use case continues. E2: Invalid fingerprint samples 1. The system shows invalid fingerprint message 2. The customer scan their fingerprint again 3. The use case continues.
Post-conditions	The new customer’s data is registered to the system
Rules	1. The user must have an authorize account to log in to the system
Constraints	None
Sequence Diagram	Refer Appendix A.2.1

Table 2: Register Use Case Description

3.1.2 Facial Image Verification

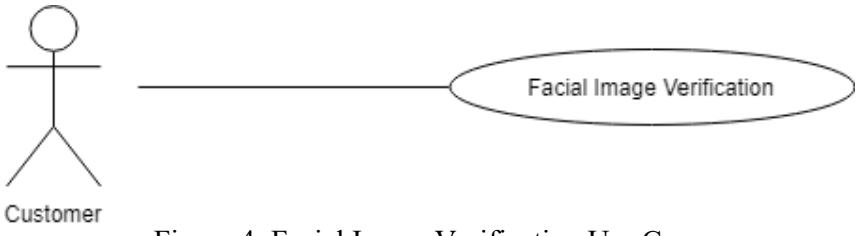


Figure 4: Facial Image Verification Use Case

Use Case ID	Mod_02
Brief Description	This use case is to allow the customer to log in through the facial image verification
Actor	Customer
Pre-conditions	1. The customer must have been registered to the system 2. The customer must have verified their fingerprint
Basic Flow	1. The use case begins when the user enter the system. 2. The system display 'Please Verify Your Face ID'on the system. 3. The user captures their facial image using the camera on the system. 4. The user click 'Capture Facial Image' button to capture their facial image. 5. The user click 'Verify' button to verify their facial image. **[E1:Invalid facial image]** 6. The use case ends.
Alternative Flow	None
Exception Flow	E1: Invalid facial image 1. The user captures their facial image again 2. The system verifies the image in the database. 3. The use case continues.
Post-conditions	The user allows to do the second verification process
Rules	1. The user must have an authorize account to log in to the system
Constraints	1. The image must be clear and high quality for

	verification
Sequence Diagram	Refer Appendix A.2.2

Table 3: Facial Image Verification Use Case Description

3.1.3 Fingerprint Verification

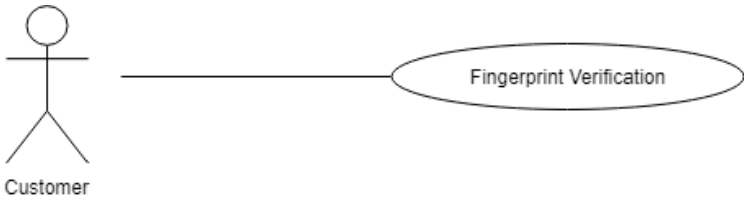


Figure 5: Fingerprint Verification Use Case

Use Case ID	Mod_03
Brief Description	This use case is to allow the customer to log in through the fingerprint verification
Actor	Customer
Pre-conditions	1. The customer must have been registered to the system
Basic Flow	1. The use case begins when the user enter their username and click 'Continue' button on Login interface 2. The system display 'Place Scan Your Fingerprint' on the system. 3. The user scans their fingerprint using the fingerprint scanner attached to the system. 4. The system verifies the fingerprint in the database. **[E1:Invalid fingerprint]** 5. The use case ends.
Alternative Flow	None
Exception Flow	E1: Invalid fingerprint 1. The user scan their fingerprint again 2. The system verifies the fingerprint in the database.

	3. The use case continues.
Post-conditions	The user is log in to the system
Rules	1. The user must have an authorize account to log in to the system
Constraints	1. The fingerprint must be retrieved using fingerprint scanner
Sequence Diagram	Refer Appendix A.2.3

Table 4: Fingerprint Verification Use Case Descriptions

3.1.4 Transactions

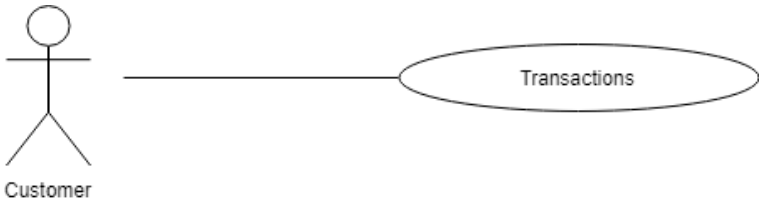


Figure 6: Transactions Use Case

Use Case ID	Mod_04
Brief Description	This use case is to allow the customer to log in through the fingerprint verification
Actor	Customer
Pre-conditions	1. The user must have been registered to the system 2. The user must be verified through the facial image and fingerprint verification
Basic Flow	1. The use case begins when the user is log in to the system. 2. The user can choose the transactions they want to make. **[A1: Cash Withdrawal][A2: Check Balance][A3:Transfer Fund]** 3. The use case ends.
Alternative Flow	A1: Cash Withdrawal 1. The user can choose amount of cash to withdraw 2. The system withdraws the amount from the

	user account. **[E1: Invalid amount]** 3. The use case continues. A2: Check Balance 1. The user's account balance is display on the screen 2. The user continues the transactions 3. The use case continues A3: Transfer Fund 1. The user choose the recipient bank 2. The user enter recipient account number 3. The user click 'Yes' button to confirm 4. The user enter amount to be transfer 5. The user click 'Yes' button to confirm 6. The system display the transfer detail on the screen 7. The user click 'Yes' button to confirm 8. The transfer is successful 9. The use case continues
Exception Flow	E1: Invalid amount 1. The amount is insufficient 2. The user enters the amount again 3. The use case continues
Post-conditions	The user finished do the transactions
Rules	1. The user must have an authorize account to log in to the system 2. The user must be verified by the system
Constraints	None
Sequence Diagram	Refer Appendix A.2.4

Table 5: Transactions Use Case Description

3.2 Requirement Traceability

Use Case ID	Requirement ID	Requirement Description
Mod_01	Mod_01_1 Mod_01_2	• The system should allow the administrator to log in using their username and password • The system should allow the administrator to register new customer
Mod_02	Mod_02_1	• The system should verify the customer by their facial image
Mod_03	Mod_03_1	• The system should verify the customer by their fingerprint
Mod_04	Mod_04_1 Mod_04_2 Mod_04_3	• The user is allowed to withdraw cash from the ATM system • The user is allowed to check the balance of their account • The user is allowed to transfer money to third party account

Table 6: Requirement Traceability

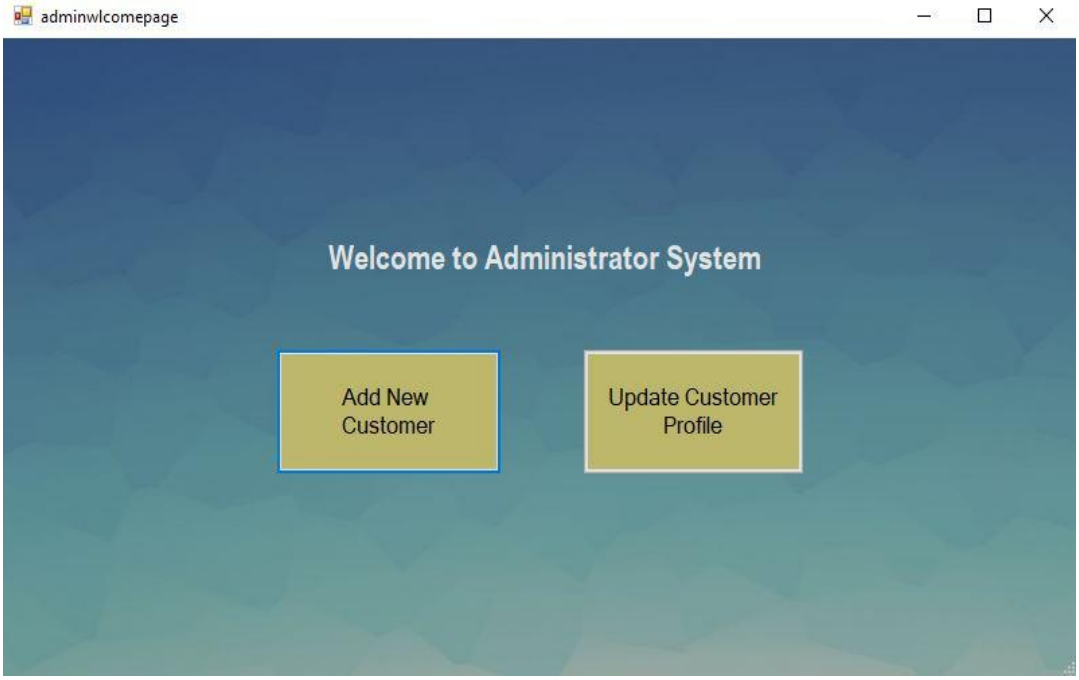
4.0 Acronyms and Abbreviation

Acronyms and Abbreviation	Description
SRS	Software Requirement Specification
FRFB	Facial Recognition and Fingerprint Based
ATM	Automatic Teller Machine
Sys	System
v	Version
Mod	Module

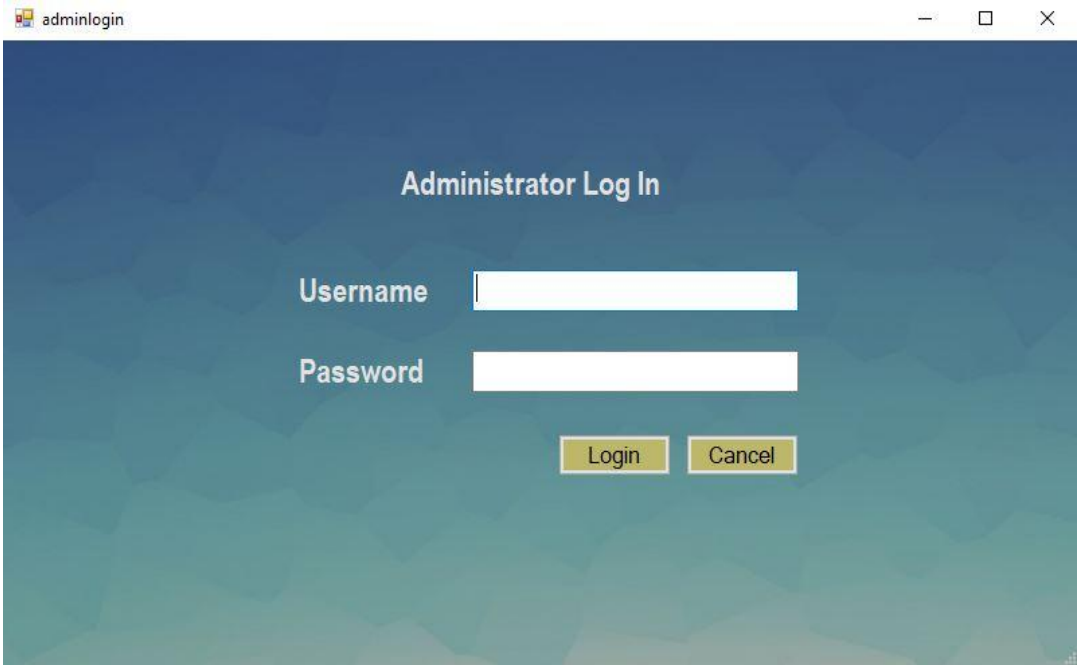
Table 7: Acronyms and Abbreviation

Appendices

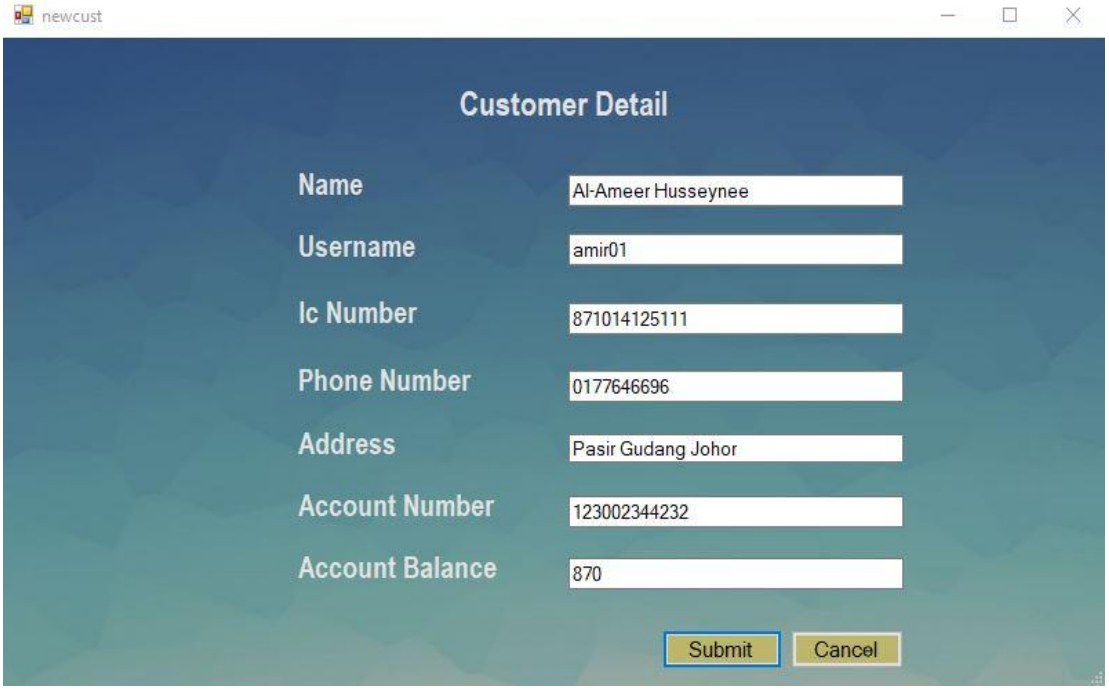
Appendix A.1 – User Interfaces



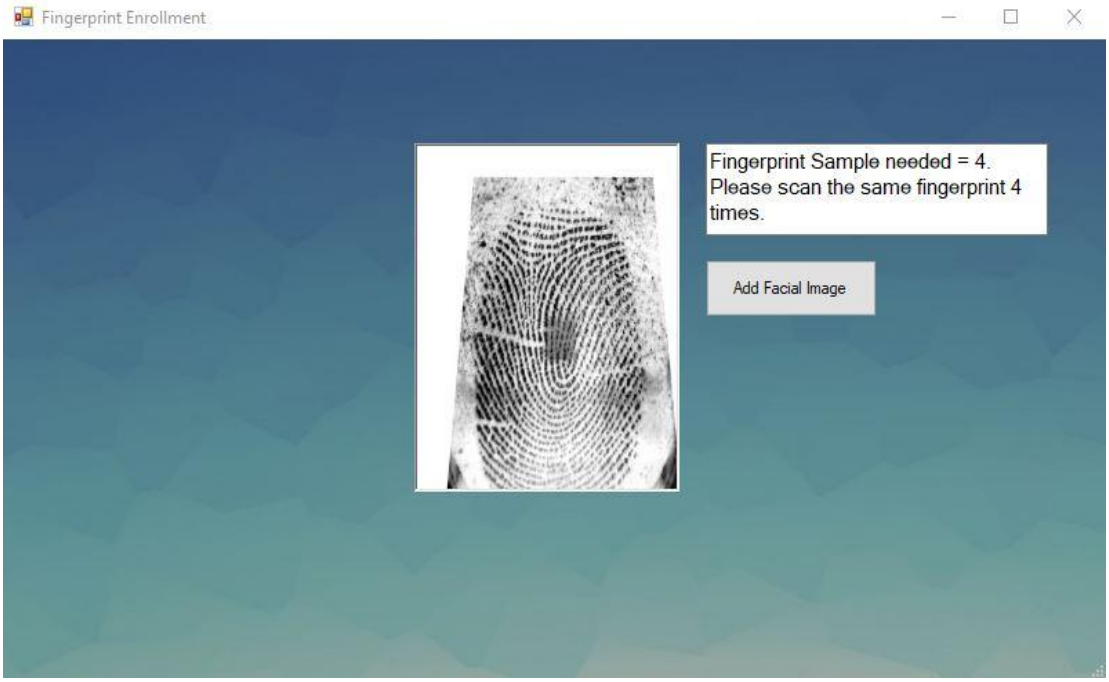
A.1.1: The administrator can choose the function of the system



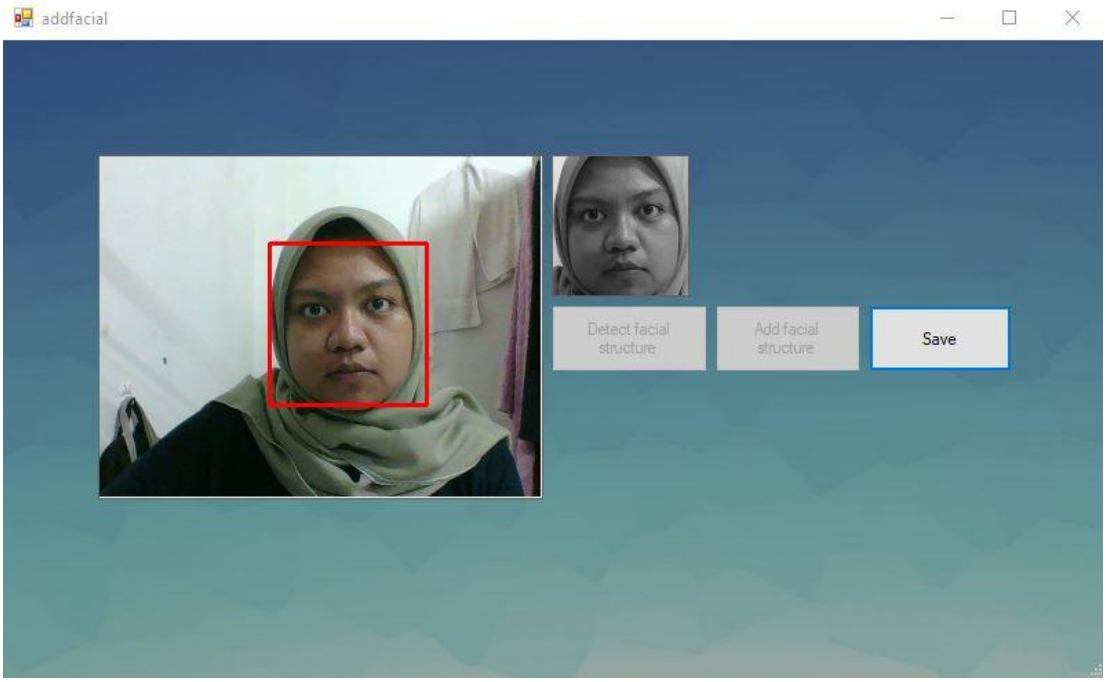
A.1.2: The administrator log in using their username and password



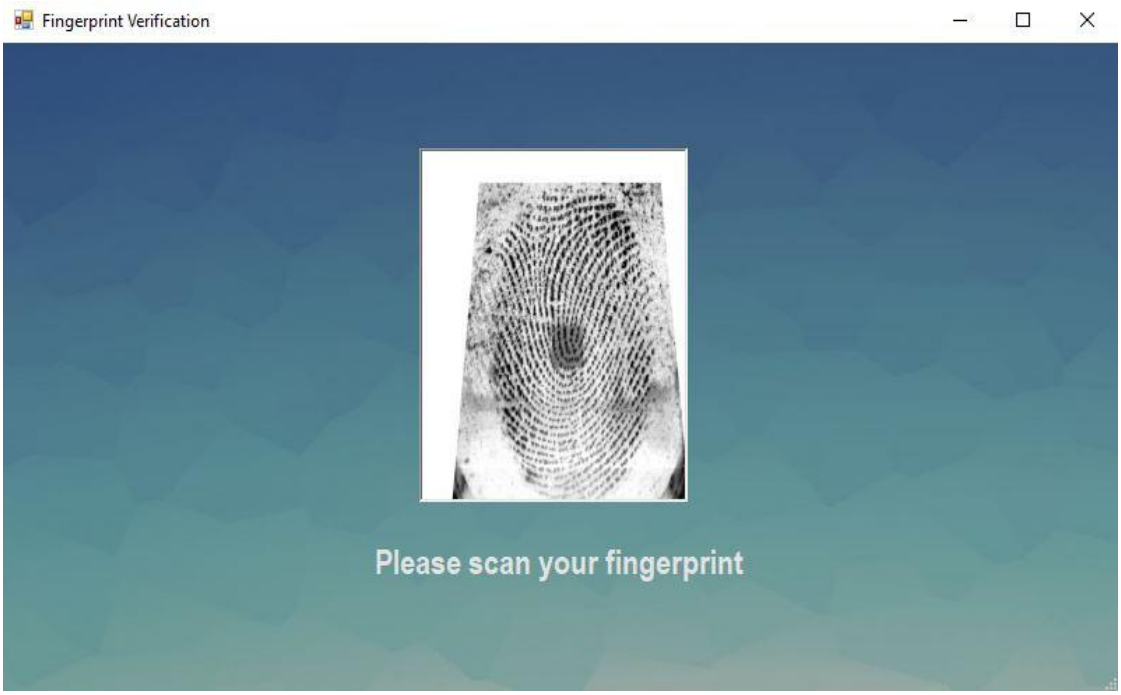
A.1.3: The administrator enter new customer's data



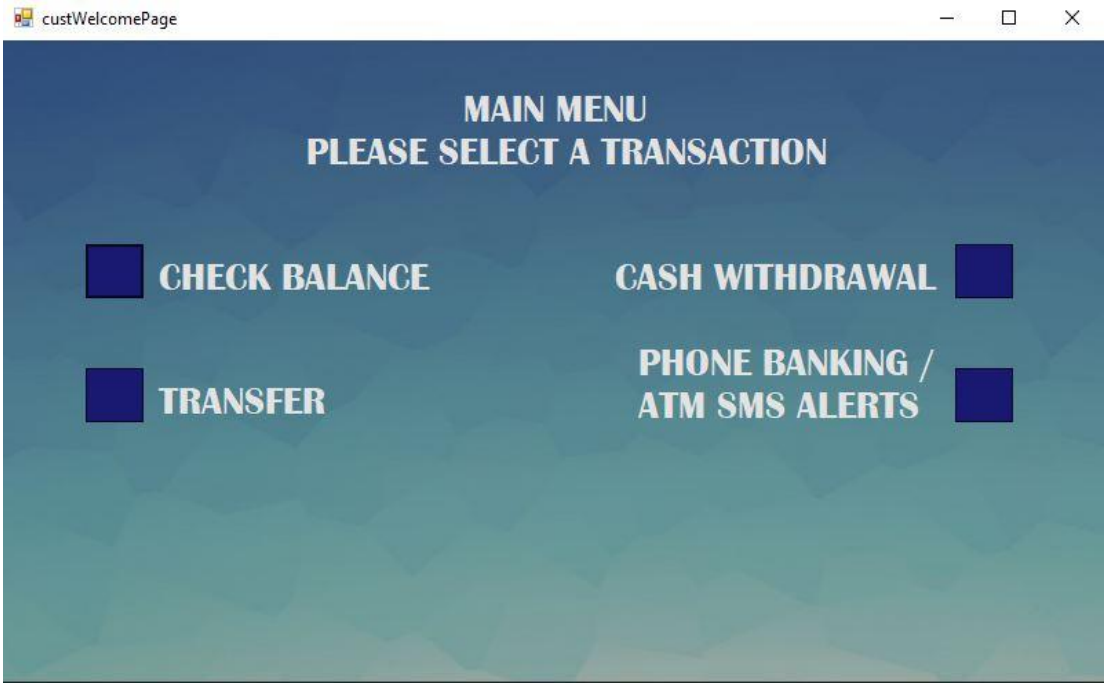
A.1.4: The administrator enter the biometric data of the customer



A.1.5: The customer capture their facial image for verification

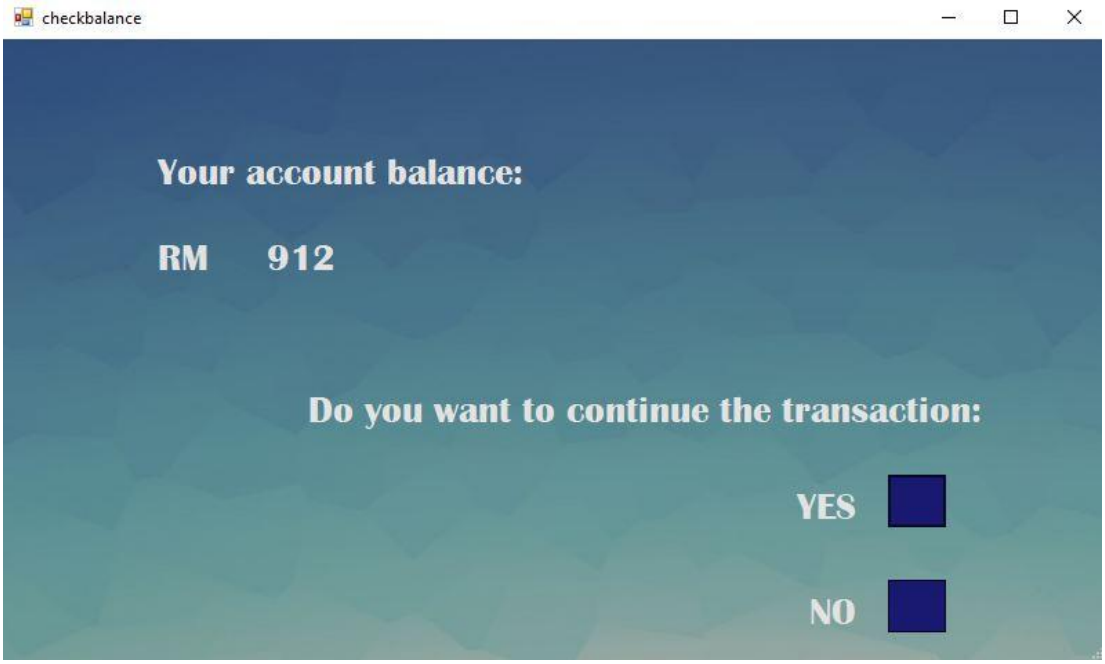


A.1.6: The customer scans their fingerprint for verification



A.1.7: The customer is allowed to make any transactions available in ATM system

A.1.8: The customer can choose amount for cash withdrawal

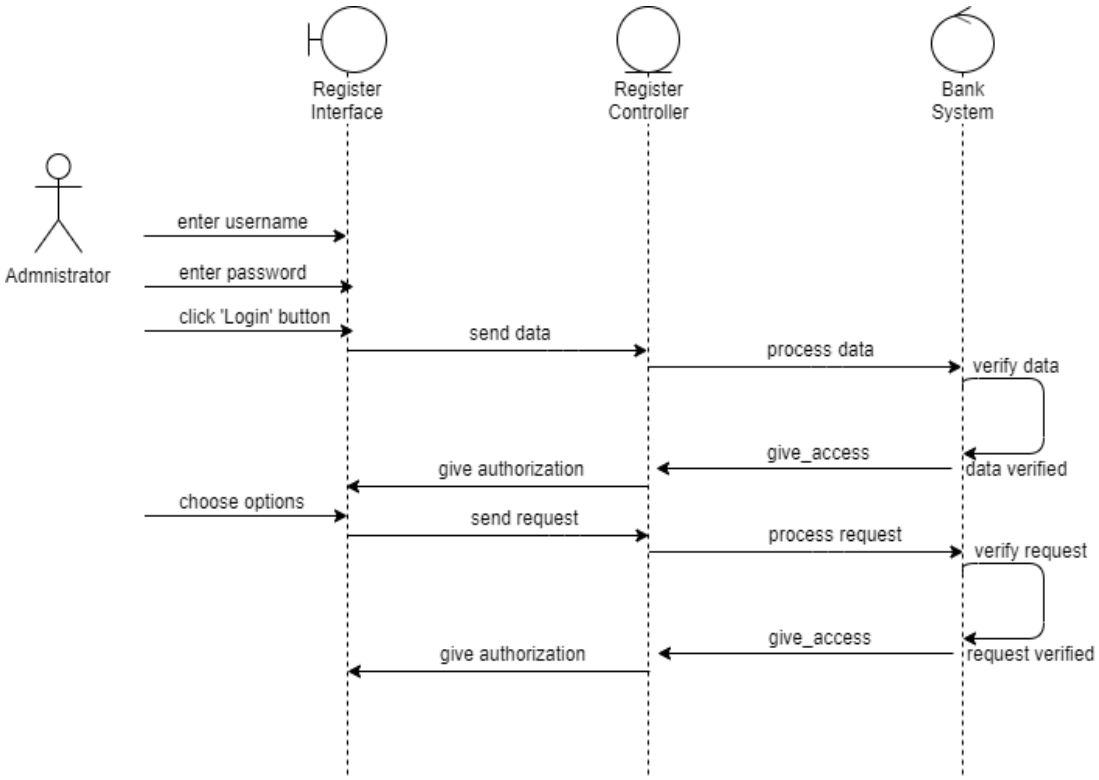


A.1.9: The account balance is display when customer choose check balance button

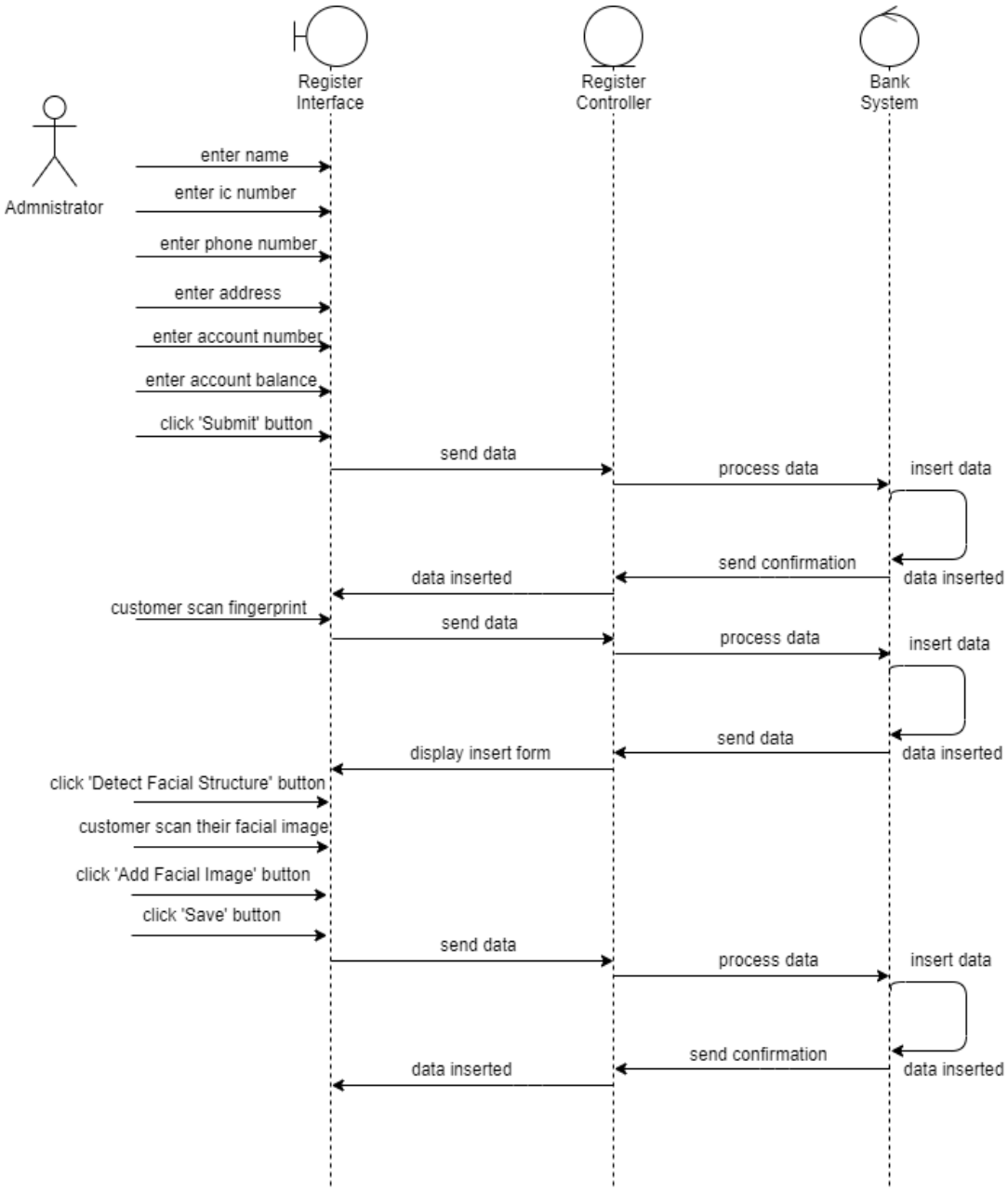
Appendix A.2 – Sequence Diagram

Appendix A.2.1 – Register

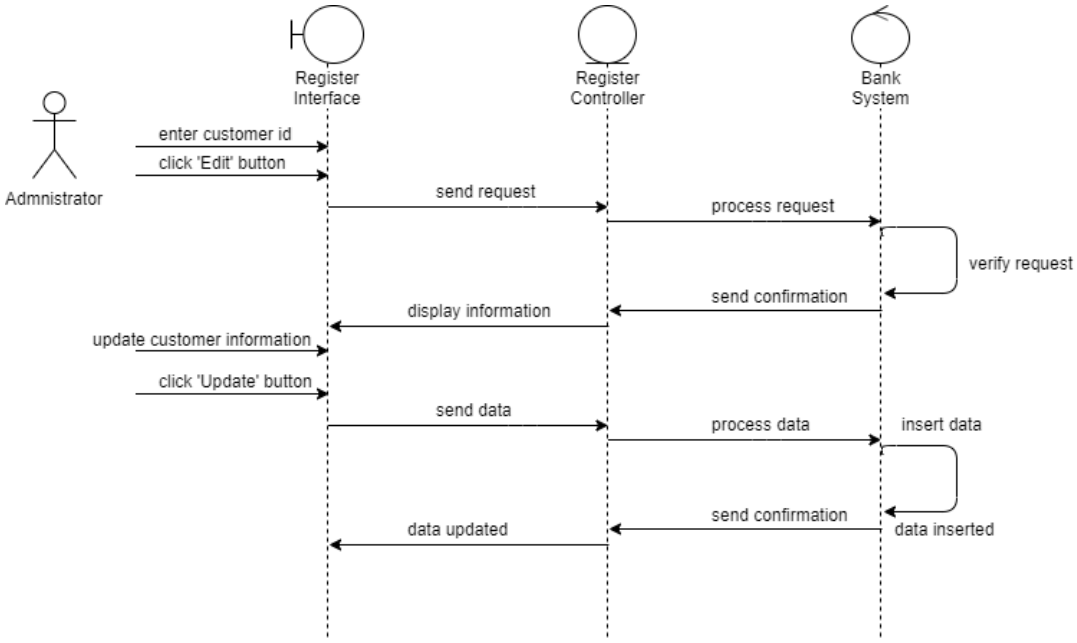
Basic Flow



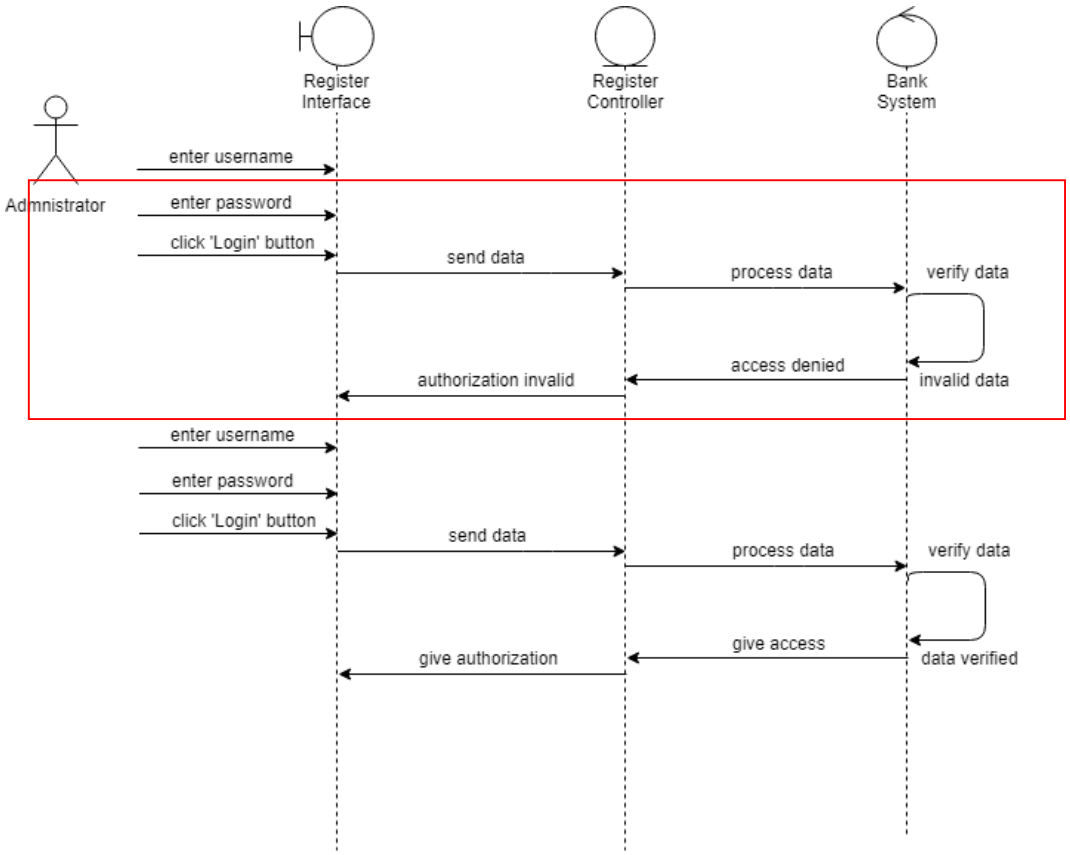
Alternative Flow – Add New Customer



Alternative Flow – Update Customer Profile

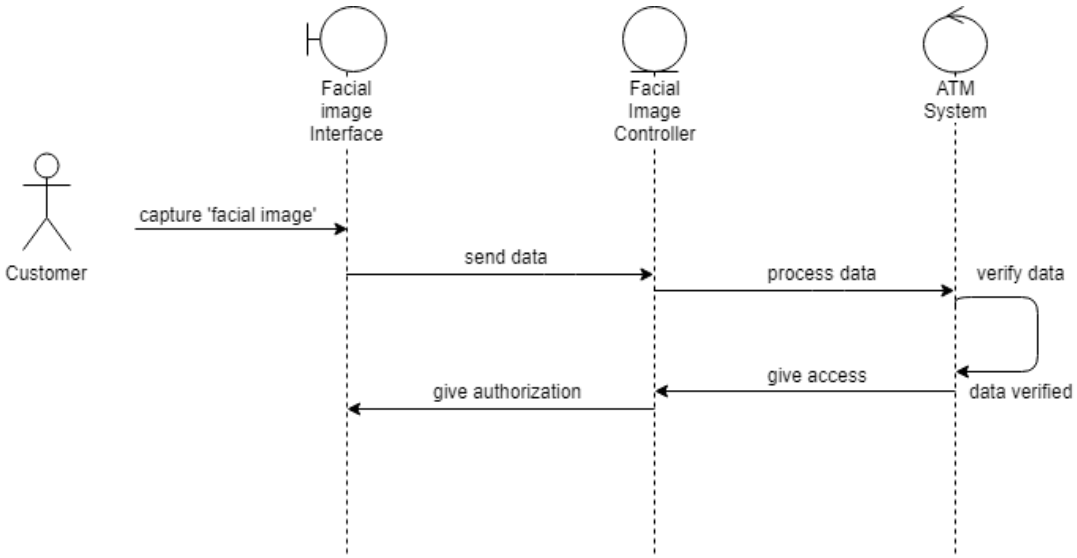

Register
Interface
Register
Controller
Bank
System
Admnistrator
enter customer id
click 'Edit' button
send request
process request
verify request
send confirmation
display information
update customer information
click 'Update' button
send data
process data
insert data
send confirmation
data inserted
data updated

Exception Flow – Username or Password is invalid

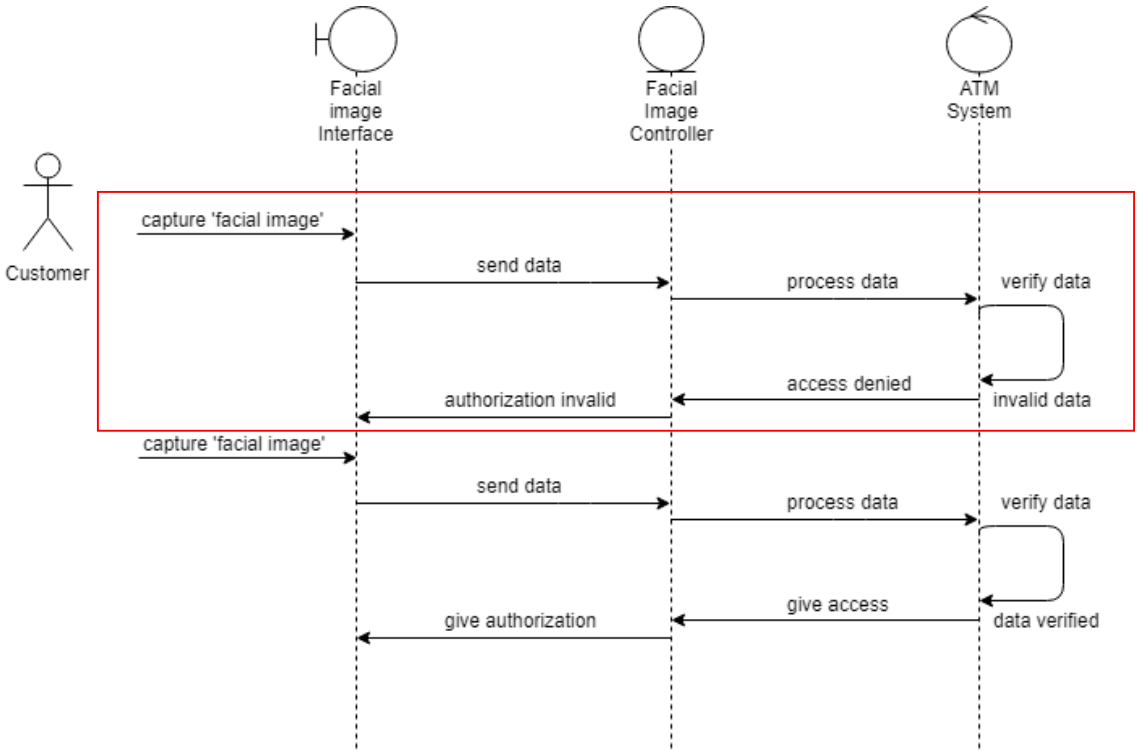


Appendix A.2.2 – Facial Image Verification

Basic Flow

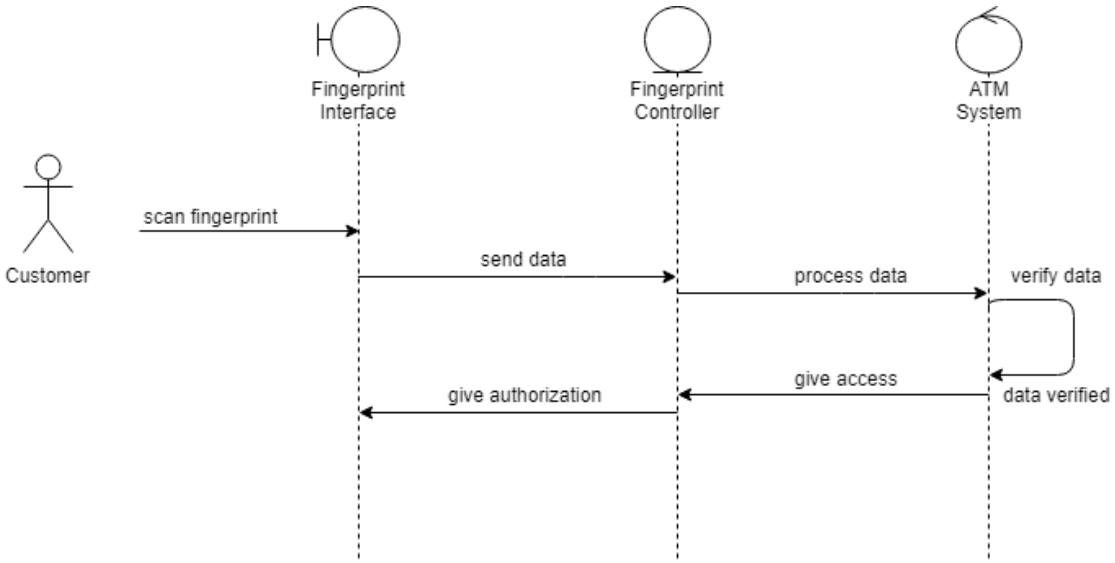


Exception Flow – Image invalid

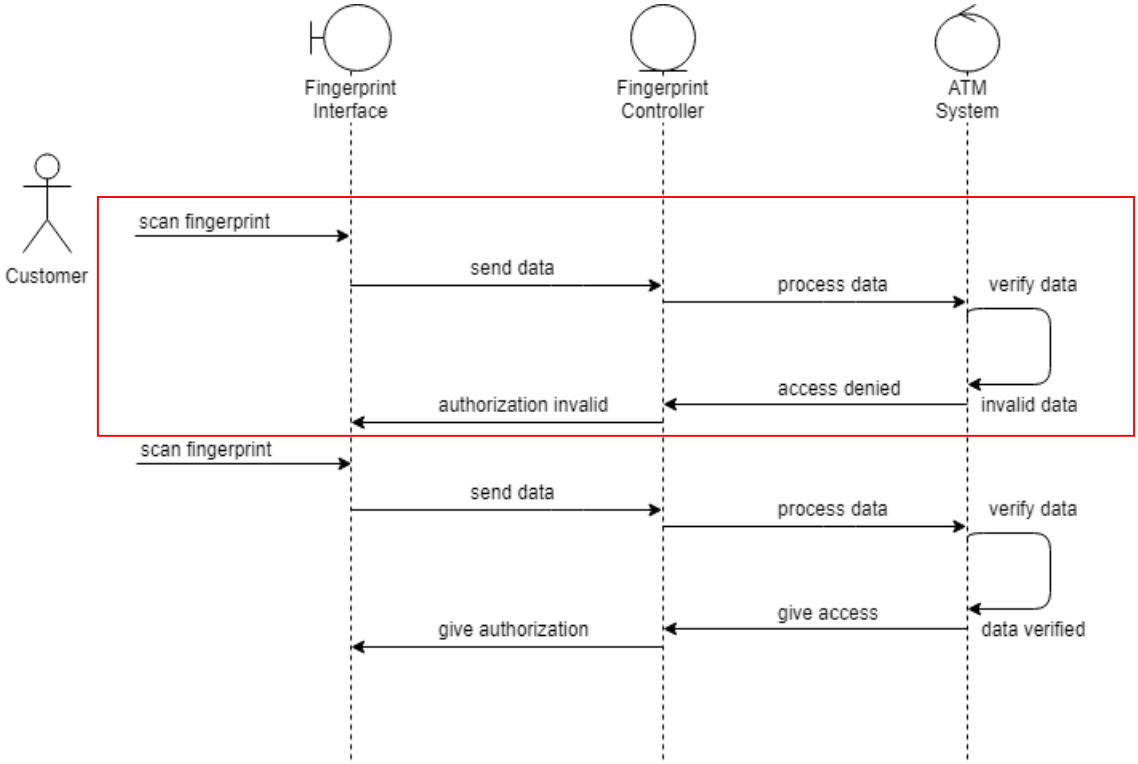


Appendix A.2.3 – Fingerprint Verification

Basic Flow

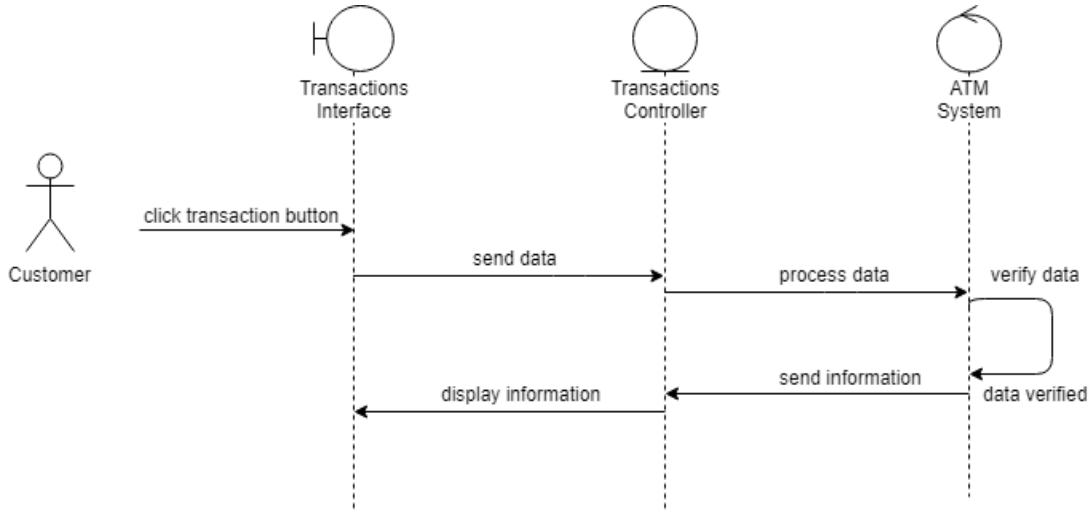


Exception Flow – Fingerprint invalid

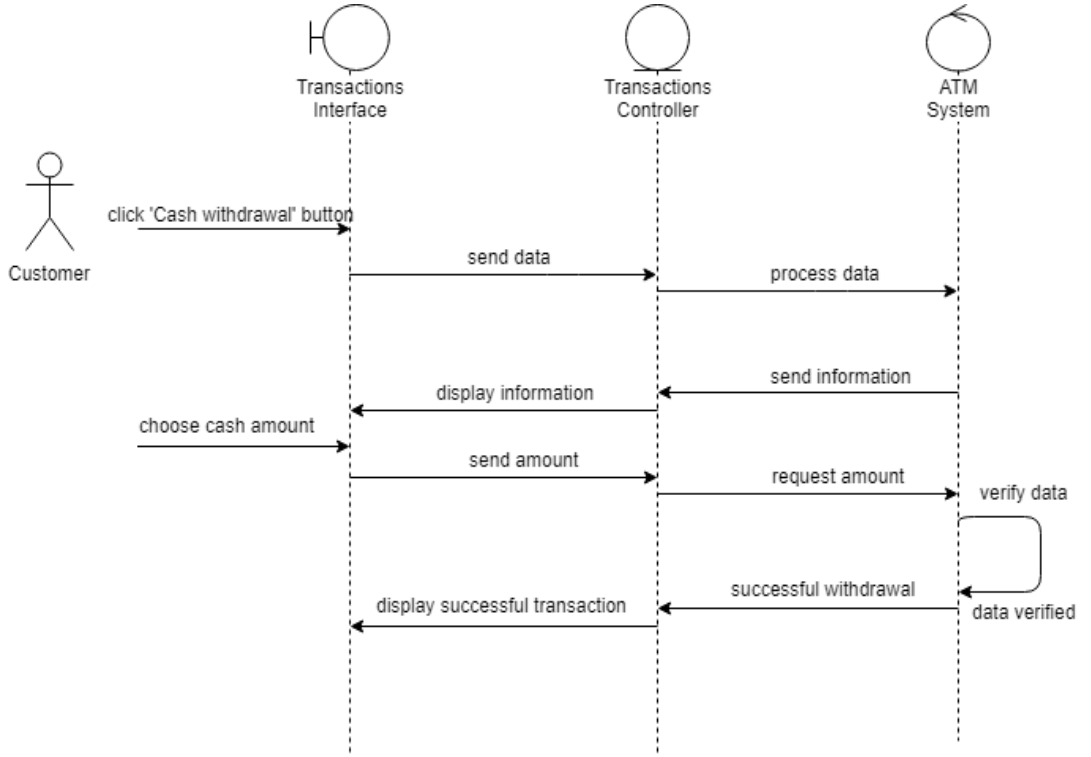


Appendix A.2.4 – Transactions

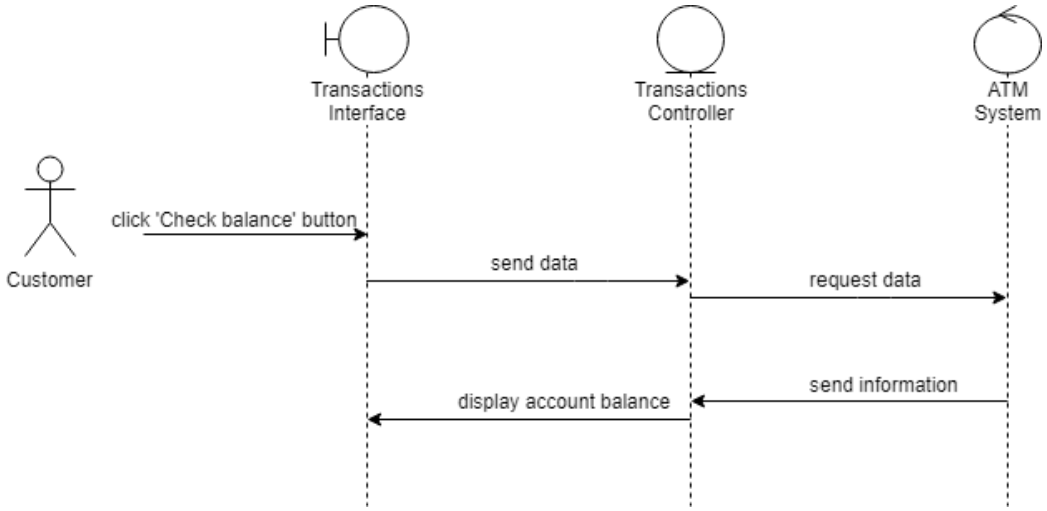
Basic Flow



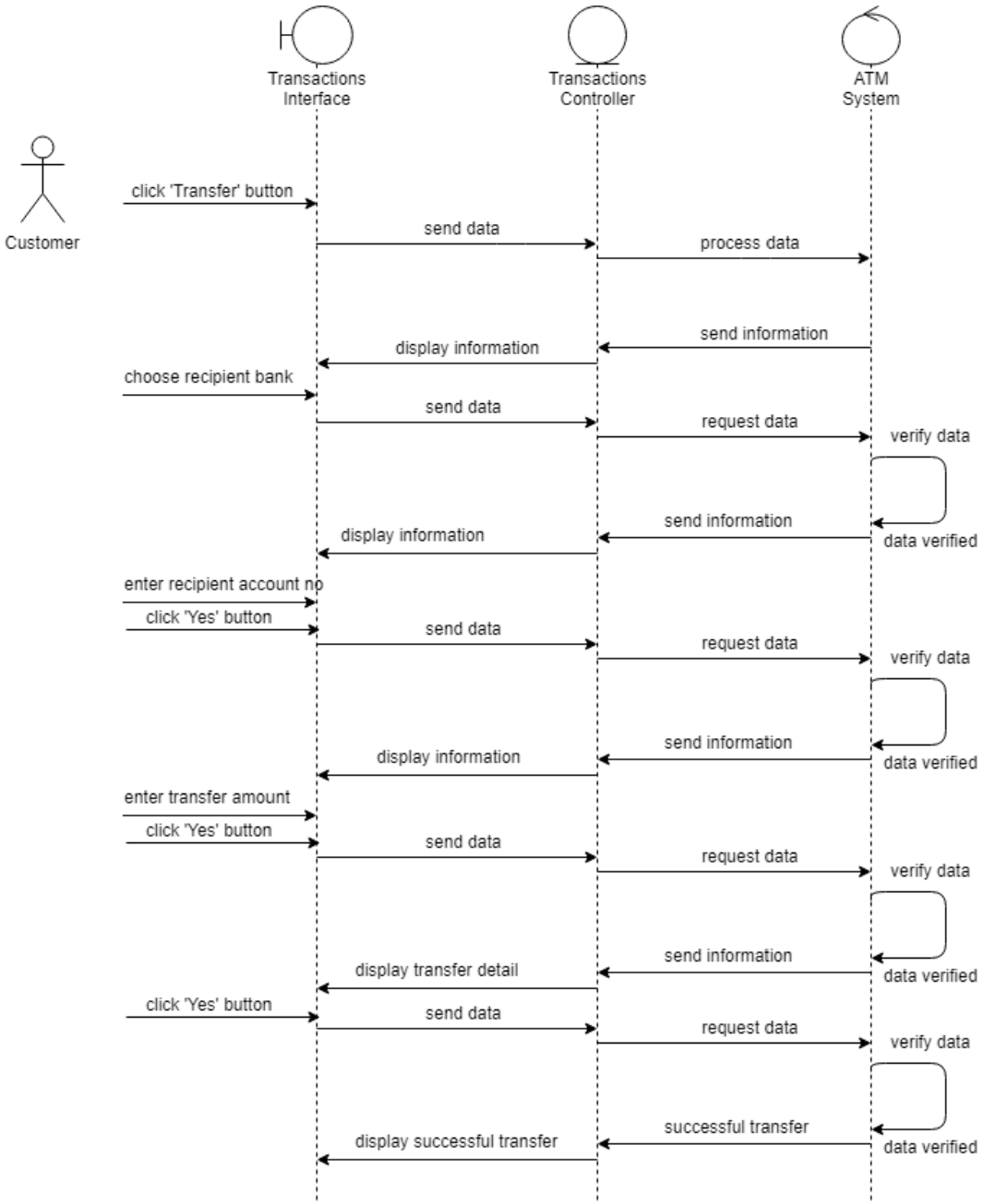
Alternative Flow 1 – Cash Withdrawal



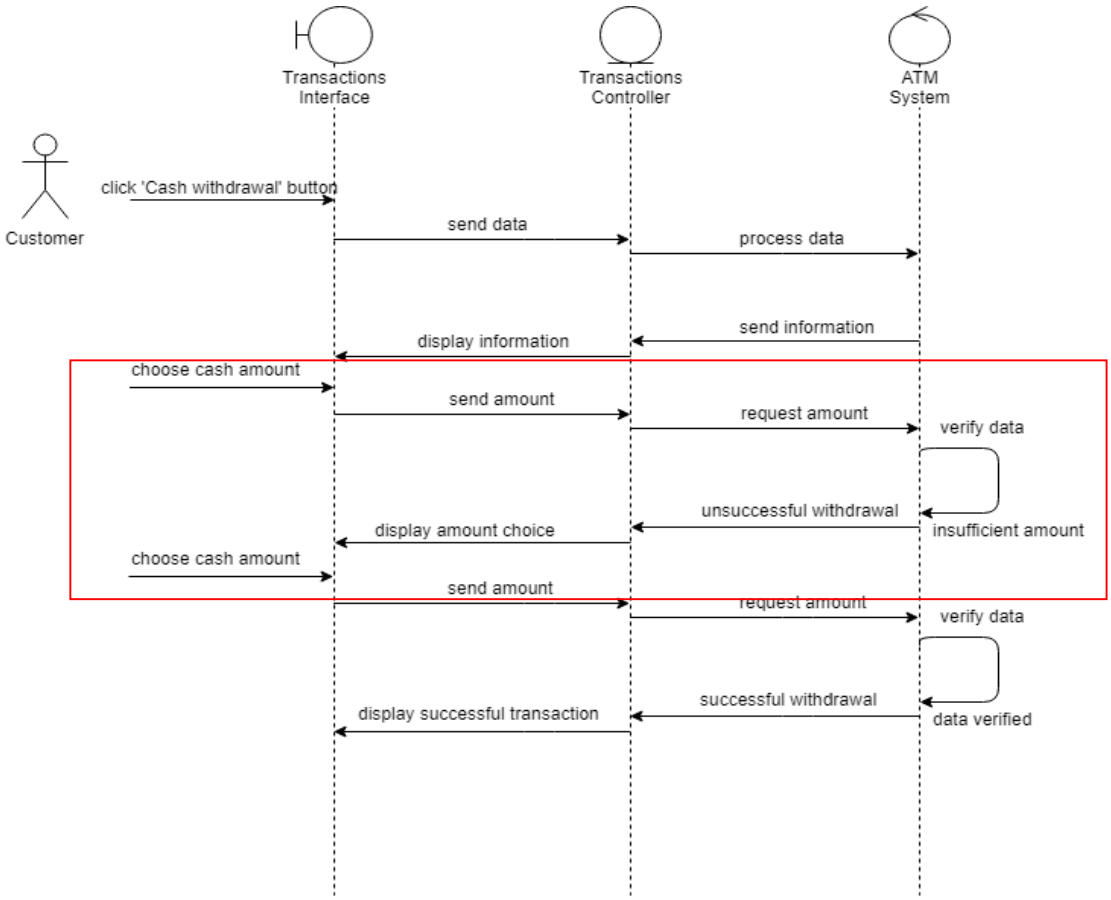
Alternative Flow 2 – Check Balance


Transactions
Interface
Transactions
Controller
ATM
System
Customer
click 'Check balance' button
send data
request data
send information
display account balance

Alternative Flow 3 – Transfer Fund



Exception Flow – Insufficient balance



APPENDIX B

FACIAL RECOGNITION AND FINGERPRINT BASED ATM SYSTEM

FACULTY OF COMPUTING

SOFTWARE DESIGN DOCUMENT (SDD)

1.0 Introduction

1.1 Purpose

The purpose of this document is to describe the Facial Recognition and Fingerprint Based ATM System. The document explained about the detail of the system such as the functions, data design, and relationship between the data, system architecture, and the detail design of the system. This document is intended for both the stakeholders and the system developer as a reference to develop the first version of this system.

1.2 System Identification

This Software Design Document (SDD) belongs to: Facial Recognition and Fingerprint Based ATM System

System Title : FRFB_ATMSys

System Abbreviation : FRFB_ATMSys_v01

System Identification Number : FRFB_ATMSys001

1.3 System Overview

The system has four modules which are register, facial image verification, fingerprint verification and transaction.

The system will be used by the customer and administrator which act as the actor of the system. The system allows the customer to log in to the ATM system by verifying their facial signature and fingerprint which will be compared to the data in the database. If the facial signature and fingerprint is verified, the system will give access to the customer to do the transaction available in the system. The transactions available in the system are cash withdrawal, transfer fund and check

balance of their account. The facial image and fingerprint are retrieved from customer using the web camera on the laptop and fingerprint scanner which are installed to the ATM system.

The administrator will act as a user who will register a new customer to the ATM system. The administrator will log in to the system and they will add detail of the new customer to the database including their facial image and fingerprint. After the new customer is registered, they can log in to the ATM system through the ATM verification process of facial recognition and fingerprint authentication.

1.4 References

- R.Arokiasamy, Steven. (2018). Fingerprint Based Automatic Teller Machine. Gambang, Pahang: Universiti Malaysia Pahang.
- Morley, John. (2014). Academic Phrasebank. Manchester: The University of Manchester.
- Kirun, Sakinah. (2019). Software Requirement Specification (SRS) Facial Recognition and Fingerprint Based ATM System. Gambang, Pahang: Universiti Malaysia Pahang.

2.0 Data Dictionary

2.1 Customer

Field Name	Data Type	Key	Description
custID	Int	PK	Customer ID and act as a primary key
custName	Varchar	Not Null	Customer name
custIcnum	Int	Not Null	Customer identity card number
custPhonenum	Int	Not Null	Customer phone number
custAddress	Varchar	Not Null	Customer address
custAccountnum	Int	Not Null	Customer account number
custAccbalance	Double	Not Null	Customer account's balance
custfacialimage	Varbinary (MAX)	Null	Customer facial image biometric data
custFingerprint	Varbinary (MAX)	Null	Customer fingerprint biometric data
custUsername	Varchar	Not Null	Customer username

Table 1: Data Dictionary for Customer table

2.2 Administrator

Field Name	Data Type	Key	Description
adminUsername	Varchar	PK	Adminstrator ID
adminPassword	Varchar	Not Null	Administrator password for their account

Table 2: Data Dictionary for Administrator tabl

2.3 Transaction

Field Name	Data Type	Key	Description
transactionId	Int	PK	Transaction Id
custID	Int	FK	Customer ID who make the transaction
transactionType	Varchar	Not Null	Transaction Type
transactionDate	Date	Not Null	Transaction Date

Table 3: Data Dictionary for Transaction table

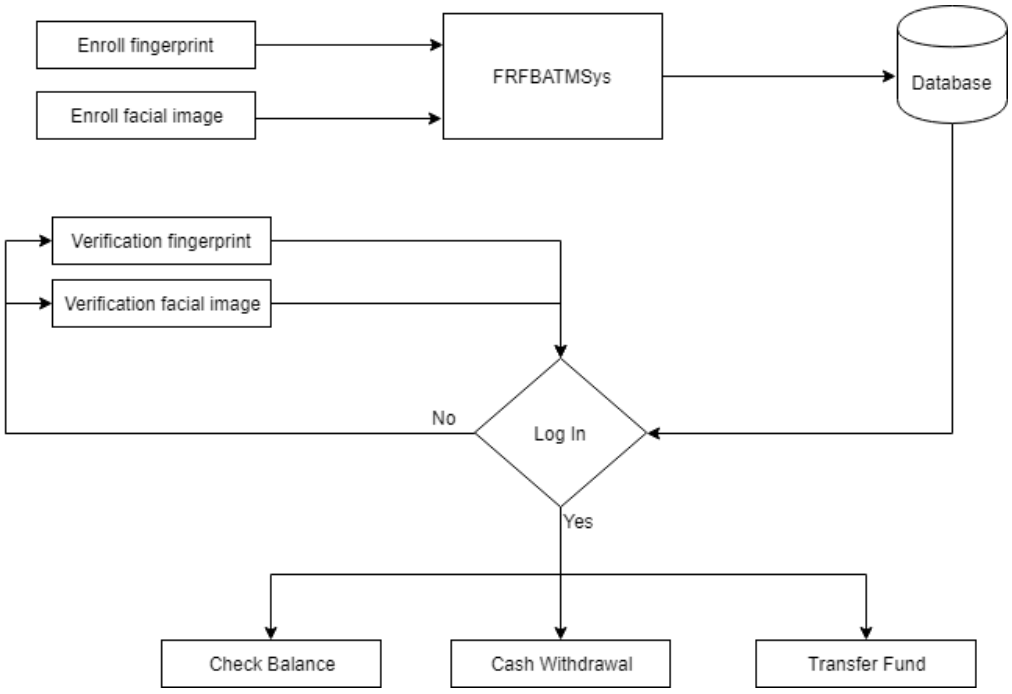
2.4 Transfer

Field Name	Data Type	Key	Description
transferID	Int	PK	Transaction Id
recipientBank	Varchar	Not Null	Recipient Bank Name
recipientName	Varchar	Not Null	Recipient Name
recipientAccount	Integer	Not Null	Recipient Account Number
transferAmount	Double	Not Null	Transfer Amount to the recipient

Table 4: Data Dictionary for Transfer table

3.0 Design Description

3.1 System Architecture



3.1.1 Package Module

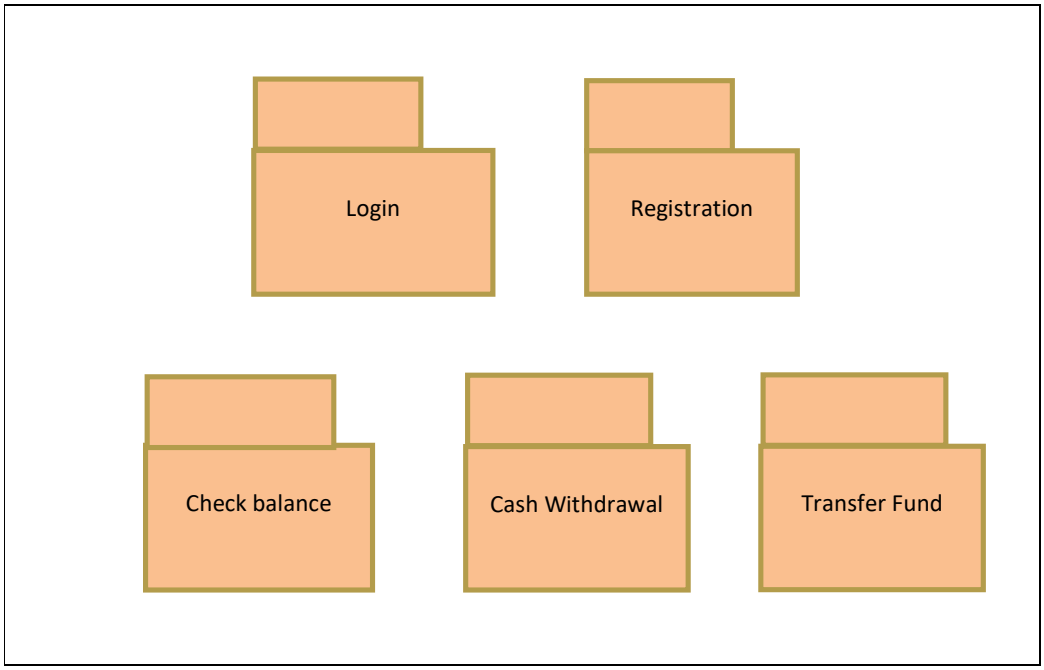


Figure 2: Package Module of ATM System

i. Login

The login package is responsible for the user verification through the facial image and fingerprint verification.

Class	Description
Login	The class is responsible to allow the customer to enter their username for verification purposes
ReadFP	This class allows the customer to verify their fingerprint when they log in to their account.
ReadFacial	This class allows the customer to verify their facial image when they log in to their account.

ii. Registration

The registration package is responsible to allow the administrator to register new customer.

Class	Description
newcust	The class is to allow the administrator to add new customer to the ATM system database
addfingerprint	This class allows the fingerprint features to be extracted using fingerprint scanner
EnrollFingerprint	This class allows the administrator to add customer's fingerprint to the ATM database
addfacial	This class allows the administrator to add customer's facial image to the ATM database
listcust	This class allows the administrator to view the list of existing customer in the database
custupdate	This class allows the administrator to update the customer information

iii. Check Balance

The check balance package is responsible to give access to the user to check their balance account.

Class	Description
checkbalance	The class allow the user to retrieve their account balance amount from the database

iv. Cash Withdrawal

The cash withdrawal package is responsible to allow the customer to access their account and allow them to withdraw their cash from their account

Class	Description
cashWithdraw	The class allow the user to withdraw cash from their account

CashAmount	The class allow the user to choose the amount they want to withdraw from their account

v. Transfer Fund

The package transfer fund allow the user to do a transfer transaction to the third party account

Class	Description
chooseBank	The class allow the user to choose the bank name of the recipient
recipientAccount	The class allow the user to enter the recipient account number for the transfer
transferAmount	The class allow the user to enter the amount to be transferred to the third party account
transferFund	The class allow the user to confirm the transfer fund to the third party account in the system

3.1.2 Package Relationship

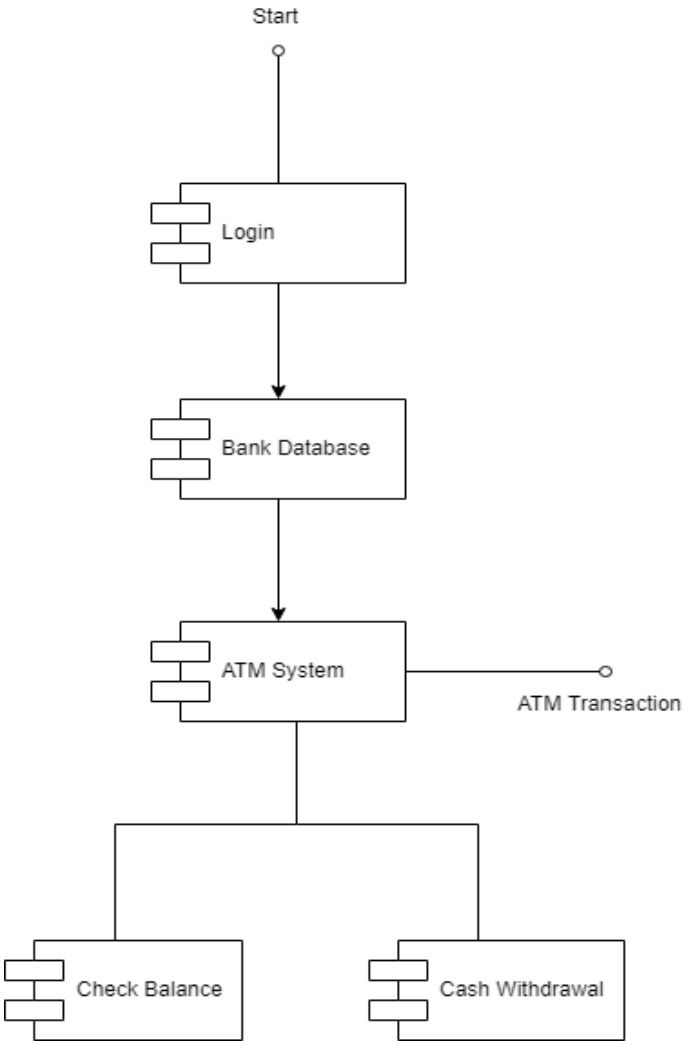
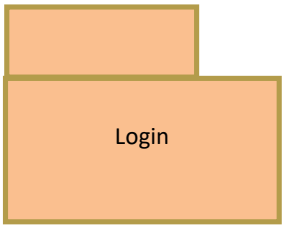


Figure 3: Component Diagram for ATM System

4.0 Detail Design

4.1 Login Package



Class: Login

Class Type	Model Class	
Responsibility	A class to allow user to enter their username for verification purposes	
Methods	Attributes Name	Attributes Type
	custUsername	Varchar
	custFingerprint	Varbinary (MAX)
	Method Name	Description
	Button3_Click ( )	This method is to the fingerprint data using username that is entered by the user
	Button6_Click ( )	This method is to reset the username textbox on the interface

Class: ReadFP

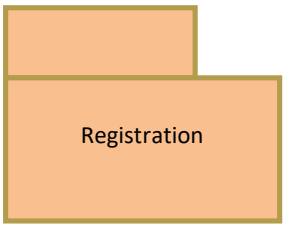
Class Type	Model Class	
Responsibility	A class to verify the fingerprint data of the customer	
Methods	Attributes Name	Attributes Type
	custFingerprint	Varbinary (MAX)
	Method Name	Description
	Verify ( )	This method is to assign the fingerprint retrieved from database to new variable of template
	Process ( )	

		This method is to extract the scanned fingerprint features and verify it with the template

Class: ReadFacial

Class Type	Model Class	
Responsibility	A class to verify the facial image data of the customer	
Methods	Attributes Name	Attributes Type
	Custfacialimage	Varbinary (MAX)
	Method Name	Description
	Button3_Click ( )	This method is to retrieve the facial image data from database and do the verification process
	Button2_Click ( )	This method is to capture the facial image of the customer into the image frame.
	ReadFacial_Load()	This method is to start the camera to capture the facial image.
	FrameGrabber ()	This method is to allow the facial image to be captured and extract the features of the facial image and display into the frame.

4.2 Registration Package



Class: newcust

Class Type	Model Class	
Responsibility	A class to add new customer to the database by the administrator	
Methods	Attributes Name	Attributes Type
	custID	Varchar
	custUsername	Varchar
	custName	Varchar
	custIcnum	Integer
	custPhonenum	Integer
	custAddress	Varchar
	custAccountnum	Integer
	custAccbalance	Double
	Method Name	Description
	Submit_Click () Cancel_Click ()	This method is to enter the customer information to the database. This method is to cancel adding new customer to the database

Class: addfingerprint

Class Type	Model Class	
Responsibility	A class to extract the features of the fingerprint	
Methods	Attributes Name	Attributes Type
	custFingerprint	Varbinary (MAX)
	Method Name	Description
	Init () Process () ConvertSampleTo Bitmap () ExtractFeatures () Button1_Click ()	This method is to initiate the fingerprint scanner to allow the fingerprint to be captured. This method is to display the fingerprint on the image box on the interface. This method is to allow the fingerprint to be convert to bitmap to be display as image. This method is to allow the fingerprint features to be extracted as byte data. This method is to allow the facial image registration after the fingerprint has successfully registered.

Class: EnrollFingerprint

Class Type	Model Class	
Responsibility	A class to enroll the customer fingerprint to the database	
Methods	Attributes Name	Attributes Type
	custFingerprint	Varbinary (MAX)
	Method Name	Description
	Init () Process ()	This method is to initiate the fingerprint scanner and to create new variable for the fingerprint template. This method is to extract the fingerprint features and insert into the database.

Class: addfacial

Class Type	Model Class	
Responsibility	A class to verify the facial image data of the customer	
Methods	Attributes Name	Attributes Type
	Custfacialimage	Varbinary (MAX)
	Method Name	Description
	Button1_Click ()	This method is to initiate the camera for detecting the facial image structure.
	Button3_Click ( )	This method is to add the facial image data to the database for verification process.
	Button2_Click ( )	This method is to capture the facial image of the customer into the image frame.
	FrameGrabber ()	This method is to allow the facial image to be captured and extract the features of the facial image and display into the frame.

Class: custupdate

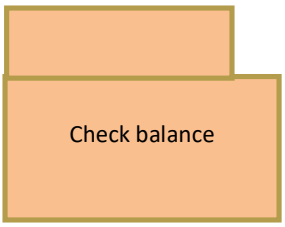
Class Type	Model Class	
Responsibility	A class to update customer information in the database by the administrator	
Methods	Attributes Name	Attributes Type
	custID	Varchar
	custUsername	Varchar
	custName	Varchar
	custIcnum	Integer
	custPhonenum	Integer
	custAddress	Varchar
	custAccountnum	Integer
	custAccbalance	Double
	Method Name	Description

	Custupdate () Submit_Click ()	This method is to retrieve all the customer information from database to display on the interface. This method is to update the edited information of the customer in the database.

Class: listcust

Class Type	Model Class	
Responsibility	A class to view list of existing customer in the database	
Methods	Attributes Name	Attributes Type
	custID	Varchar
	custName	Varchar
	Method Name	Description
	Listcust_Load () Button1_Click ()	This method is to load all the customer and display as a list on the interface. This method is to edit the chosen customer information on the 'custupdate' interface

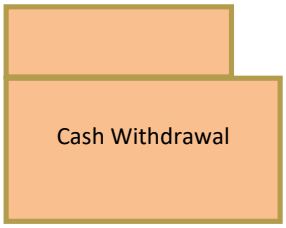
4.3 Check Balance Package



Class: checkbalance

Class Type	Entity Class	
Responsibility	A class to allow the customer to check their account balance in the ATM system	
Methods	Attributes Name	Attributes Type
	custUsername	Varchar
	custAccbalance	Float
	Method Name	Description
	Checkbalance_Load	This method is to display the account balance that is retrieved from the customer welcome page.

4.4 Cash Withdrawal Package



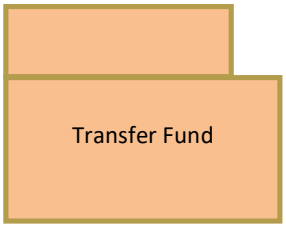
Class: cashWithdraw

Class Type	Entity Class	
Responsibility	A class to allow the customer to choose amount to withdraw and check if the balance is sufficient	
Methods	Attributes Name	Attributes Type
	custID	Int
	custUsername	Varchar
	custAccbalance	Double
	transactionID	Varchar
	transactionDate	Date
	transactionType	Varchar
	Method Name	Description
	ChooseAmount_Click ()	This method is to choose the amount which the user choose to withdraw
	Withdraw_Click ( )	This method is to record the transaction detail in the database and check if the amount for withdrawal in sufficient

Class: CashAmount

Class Type	Entity Class	
Responsibility	A class to allow the customer to withdraw cash from their account in the ATM system	
Methods	Attributes Name	Attributes Type
	custID	Int
	custUsername	Varchar
	custAccbalance	Double
	transactionID	Varchar
	transactionDate	Date
	transactionType	Varchar
	Method Name	Description
	Yes_Click ()	This method is to withdraw the approved amount for withdrawal and subtract the withdraw amount from the customer account balance.

4.5 Transfer Fund Package



Class: chooseBank

Class Type	Boundary Class	
Responsibility	A class to allow the customer to transfer money to the third party account	
Methods	Attributes Name	Attributes Type
	custID	Int
	custUsername	Varchar
	transferID	Int
	recipientBank	Varchar
	Method Name	Description
	recordBank ( )	This method allow the system to record the bank name chosen by the user to the database

Class: recipientAccount

Class Type	Boundary Class	
Responsibility	A class to allow the customer to enter the recipient account number for the transaction	
Methods	Attributes Name	Attributes Type
	custID	Int
	custUsername	Varchar
	transferID	Int
	recipientAccount	Number
	Method Name	Description
	recordAccount ( )	This method allow the system to record the

		recipient account number entered by the user

Class: transferAmount

Class Type	Boundary Class	
Responsibility	A class to allow the customer to enter the transfer amount for the transaction	
Methods	Attributes Name	Attributes Type
	custID	Int
	custUsername	Varchar
	transferID	Int
	recipientAccount	Integer
	transferAmount	Float
	Method Name	Description
	recordAmount ( )	This method allow the system to record the transfer amount on the transaction

Class: transferFund

Class Type	Entity Class	
Responsibility	A class to allow the customer to confirm the transfer money to the third party account	
Methods	Attributes Name	Attributes Type
	custID	Int
	custUsername	Varchar
	transferID	Int
	custAccbalance	Double
	transactionDate	Date
	transactionType	Varchar
	Method Name	Description
	Click_confirmation ( )	This method is to allow user to confirm their transaction and record the transaction in the database.

APPENDIX C

FACIAL RECOGNITION AND
FINGERPRINT BASED ATM SYSTEM

FACULTY OF COMPUTING

USER ACCEPTANCE TEST (UAT)

Table of Contents

1.0 TESTING REPORT

The purpose of this document is to do the User Acceptance Testing (UAT) process for the Facial Recognition and Fingerprint Based ATM System. The result of UAT shows that the system is a eligible for deployment for the end users. The system functions will be fully tested by the users under much type of cases. All errors and failure will also be recorded in this document.

1.1 Facial Recognition

Requirement ID	**Mod_02_1**				
Test Case ID	**TC_02_1**				
Event	**Test Data**	**Expected Result**	**Actual Result**	**Pass / Fail**	**Comment**
Initiate the camera	Click button 'Detect Facial Structure'	The camera is started	The camera is started successfully	Pass	
Capture user facial structure	Click button 'Add Facial Image'	The facial image is captured	The facial image is captured	Pass	
Save the facial image data in the database	Click 'Save' button	The facial image data is inserted into the database	The facial image data is inserted into the database	Pass	
The facial image is captured for verification	Click 'Capture Facial Image' button	The facial image is captured	The facial image is captured	Pass	
The facial image is verified	Click 'Verify' button	The system give access to the user	The system give access to the user	Pass	

1.2 Fingerprint

Requirement ID	**Mod_03_1**				
Test Case ID	**TC_03_1**				
Event	**Test Data**	**Expected Result**	**Actual Result**	**Pass / Fail**	**Comment**
Initiate the fingerprint scanner		The device is started	The device is started	Pass	
The fingerprint is read	Fingerprint input from user	The fingerprint is captured	The fingerprint is captured	Pass	
The fingerprint is added to the database		The fingerprint is inserted	The fingerprint is inserted	Pass	
The fingerprint verification	Fingerprint input from user	Access to the system	Access to the system	Pass	

1.3 Main Interface

Requirement ID	**Mod_04**				
Test Case ID	**TC_04_1**				
Event	**Test Data**	**Expected Result**	**Actual Result**	**Pass / Fail**	**Comment**
Check Balance	Click ‘Check Balance’ button	The interface shows account balance	The interface shows account balance	Pass	
Cash Withdrawal	Click ‘Cash Withdrawal’ button	The interface go to cash withdrawal interface	The interface go to cash withdrawal interface	Pass	
Transfer	Click ‘Transfer’ button	The interface shows bank options for transfer	The interface shows bank options for transfer	Pass	

1.4 Check Balance

Requirement ID	**Mod_04_2**				
Test Case ID	**TC_04_2**				
Event	**Test Data**	**Expected Result**	**Actual Result**	**Pass / Fail**	**Comment**
Show account balance	Click 'Check Balance' button	Shows the user account balance amount	Shows the user account balance amount	Pass	
Continue transaction	Click 'Continue' button	The page go to Main Menu	The page go to Main Menu	Pass	

1.5 Cash Withdrawal

Requirement ID	**Mod_04_1**				
Test Case ID	**TC_04_3**				
Event	**Test Data**	**Expected Result**	**Actual Result**	**Pass / Fail**	**Comment**
Choose Bank	Click amount displayed on the interface	The amount is verified to be sufficient	The amount is verified to be sufficient	Pass	
Confirm to withdraw	Click 'Yes' button	The amount is subtracted with the user account balance	The amount is subtracted with the user account balance	Pass	

1.6 Transfer

Requirement ID	**Mod_04_3**

Test Case ID	TC_04_4				
Event	**Test Data**	**Expected Result**	**Actual Result**	**Pass / Fail**	**Comment**
Choose recipient bank	Click the bank displayed on the interface	The data is saved into database	The data is saved into database	Pass	
Recipient Account number	Enter recipient account number	The data is saved into database	The data is saved into database	Pass	
Transfer amount	Enter transfer amount	The data is saved into database	The data is saved into database	Pass	
Confirmation transfer	Click 'Yes' button	The transaction is recorded and the amount is subtracted with the user account balance	The transaction is recorded and the amount is subtracted with the user account balance	Pass	

2.0 SYSTEM TESTING APPROVAL

	Name	Date
Verified by: _____ Developer	Sakinah Binti Kirun	10/12/2019
Approved by: _____ Client		

APPENDIX D

ID	Task Mode	Task Name	Duration	Start	Finish
1		**Requirements**	**25 days**	**Mon 2/11/19**	**Fri 3/15/19**
2		Discussion with Supervisor	5 days	Mon 2/11/19	Fri 2/15/19
3		Requirements elicitation	10 days	Mon 2/18/19	Fri 3/1/19
4		Analyse Requirements	7 days	Mon 3/4/19	Tue 3/12/19
5		Finalize Requirement	3 days	Wed 3/13/19	Fri 3/15/19
6		**Design**	**28 days**	**Mon 3/18/19**	**Wed 4/24/19**
7		Methodology Design	3 days	Mon 3/18/19	Wed 3/20/19
8		Interface Design	5 days	Thu 3/21/19	Wed 3/27/19
9		Architecture Design	10 days	Thu 3/28/19	Wed 4/10/19
10		Database Design	5 days	Thu 4/11/19	Wed 4/17/19
11		Finalize Design	5 days	Thu 4/18/19	Wed 4/24/19
12		**Implementation**	**65 days**	**Mon 7/1/19**	**Fri 9/27/19**
13		Develop system module	45 days	Mon 7/1/19	Fri 8/30/19
14		Module Testing	10 days	Mon 9/2/19	Fri 9/13/19
15		Complete Development	10 days	Mon 9/16/19	Fri 9/27/19
16		**Verification**	**40 days**	**Mon 9/30/19**	**Fri 11/22/19**
17		System testing	10 days	Mon 9/30/19	Fri 10/11/19
18		Analyse testing result	25 days	Mon 10/14/19	Fri 11/15/19
19		Correct errors	25 days	Mon 10/14/1	Fri 11/15/19
20		Finalize testing	5 days	Mon 11/18/1	Fri 11/22/19
21		**Maintenance**	**15 days**	**Mon 11/25/1**	**Fri 12/13/19**
22		Collect users feedback	5 days	Mon 11/25/19	Fri 11/29/19
23		Improve system and maintenance	10 days	Mon 12/2/19	Fri 12/13/19