Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 2458-9403
Vol. 3 Issue 9, September - 2016

Design and Implementation of a Multifactor Authentication System In ATM Security

Olatunji K. A.,
Department of Computer Science
Afe Babalola University, Ado-Ekiti
Ekiti State, Nigeria
odekunlekenny@yahoo.com

Afolalu C. A.
Department of Computer Science
Afe Babalola University, Ado-Ekiti
Ekiti State, Nigeria
catherinea@abuad.edu.ng

Abiola O. B.
Department of Computer Science
Afe Babalola University, Ado-Ekiti
Ekiti State, Nigeria
abiolatoyinbunmi@gmail.com

***Abstract*—the world has been plagued by crimes regarding the use of ATM. The need for a more secure authentication process has to be put in place. The main objective of this project is to curb the rate of crime that has been affecting the use of ATM in our society. This deficiency in the security of ATM systems was what led to a better security system to be developed.**

A multifactor authentication system in ATM has been developed in this research which comprises of what you know (PIN), what you have (OTP) and who you are (face). The PIN which is a combination of four digits number will be given by the bank with the ATM card whereby the user's can change at any time, The OTP will be sent to the user's phone with the help of the Clickatell API. The face detection and recognition aspects will be implemented with the use of the Viola Jones Algorithm.
This research was implemented using C# as the frontend and MySQL was used for the database. At the end of this work, a more secure authentication system was successfully designed to help reduce the rate of crime at the ATM.

Keywords—ATM; Multifactor; Security; Biometrics; Face.

I. INTRODUCTION

An automated teller machine (ATM) is an electronic telecommunications device that enables the customers of a financial institution to perform financial transactions, particularly cash withdrawal, without the need for a human cashier, clerk or bank teller [1].

Multifactor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction [2].

Multifactor authentication combines two or more independent credentials: what the user knows (password), what the user has (security token) and what the user is (biometric verification). The goal of MFA is to create a layered defence and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target [2].

Biometrics refers to metrics related to human characteristics (e.g. face). Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control [3].

II. REVIEW OF RELATED WORKS

The following works were reviewed and presented as follows:

A. Face Recognisability Evaluation for ATM Applications with Exceptional Occlusion Handling [4].

Motivation

Other research works have suffered from difficulties in tracking down the suspects when their faces are heavily occluded unable to be recognized. It is reported that the suspects tend to take advantage of its weakness by occluding their

faces with typical objects such as sunglasses or masks.

Objective

The objective of the research is to propose a novel method for face recognisability with exceptional occlusion handling (EOH).

Methodology

The methodology used here was face recognition. In order to handle these problems, the proposed method facilitated the exceptional occlusion handling (EOH) process to handle both types of falsely evaluated cases. The EOH can be divided into two different approaches: 1) accepting the falsely rejected cases, 2) rejecting the falsely accepted cases. In short, the EOH should be designed to detect the target objects exclusively although it may hold a slightly inadequate detection rate. The transaction proceeds only after recognizing the face of the user.

Limitation

This paper does not cover various unconstrained illumination conditions and facial postures. In addition, EOH that deals with other types of typical occlusions such as moustache near the mouth were not considered. The ATM does not really authenticate the legal card holder.

B. Enhanced ATM Security System Using Biometrics [5].

Motivation

They considered the numerous security challenges encountered by Automated Teller Machines (ATM) and; given that the existing security in the ATM system has not been able to address these challenges, they saw the need to enhance the ATM security system to overcome these challenges.

Objective

The aim of this study therefore is to develop ATM simulator based fingerprint verification operations in order to reduce frauds associated with the use of ATM.

Methodology

In this paper, they adopted Object Oriented Analysis and Design (OOAD) using JAVA. Object-oriented analysis and design (OOAD) is a software engineering approach that represents a system as a group of interacting objects. Each object represents some entity of interest in the system being modeled, and is characterized by its class, its state (data elements), and its behaviour. Various models can be created to show the static structure, dynamic behaviour, and run-time deployment of these collaborating objects.

Limitation

They should have used a 3-D API for a Graphical User Interface (GUI). Example is openGLin place of Java Swing API. The JDBC architecture could have been extended to three-tier using application server like APPLET server, JSPservleton APACHE thumbcard versus database. There was no fingerprint matching algorithm.

C. Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria E-Banking System [6].

Motivation

This paper focused on vulnerabilities and the increasing wave of criminal activities occurring at Automated Teller Machines (ATMs) where quick cash is the prime target for criminals rather than at banks themselves.

Objective

The primary focus of this work is to develop a fingerprint mechanism as a biometric measure to enhance the security features of ATM for effective banking transactions for banks in Nigeria.

Methodology

The security feature for enhancing the ATM was designed using the client/server approach. There was a link between the customer's identification information, customer's accounts and records in the bank (server). Similarly, a descriptive conceptual approach which includes Unified Modelling language (UML) tools such as use case models, class diagrams etc. was adapted. Microsoft Access 2003 as a database software was employed to create database to store cardholder's information. The work was implemented using Visual Basic 6.0 software tool, used to design the user interfaces and/or cardholder interaction with the ATM Machine.

Limitation

The use of a single biometric measure is not trustworthy enough. The security would have

been better had they used some other form of authentication like a token or a one-time password.

D. Implementation of ATM Security by Using Fingerprint Recognition and GSM [7].

Motivation

The financial crime case rises repeatedly in recent years; many criminals tamper with the ATM terminal and steal user's credit card and password by illegal means. Once user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time, which will bring enormous financial losses to customer.

Objective

The main objective of this system is to develop an embedded system, which is used for ATM security applications.

Methodology

The working of this ATM machine is when customer place finger on the finger print module when it accesses automatically generates every time different 4-digit code as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller.

The code received by the customer should be entered by pressing the keys on the touch screen. After entering it checks whether it is a valid one or not and allows the customer further access.

Limitation

They used Gabor & direction filter algorithm and it is known to be slow in dealing with high capacity requirements.

E. Usability and Biometric Verification at the ATM Interface [8].

Motivation

The methods for increasing security, such as regularly changing PINs and passwords, increasing their length, ensuring they do not form words and ensuring all are different, makes them more difficult to remember and, therefore, error-prone.

Objectives

The aim of this paper is to provide a summary of the user centred aspect of the research they carried out over the last five years to understand attitudes towards, and behaviour with, biometrics verification at the Automated Teller Machine (ATM) interface.

Methodology

With iris verification, for application at ATMs, a wide angle camera finds the head of the person to be identified. A zoom lens then targets in on the user's iris and takes a digital photo. A template of concentric lines is laid on the iris image and a number of specific points are recorded and the information converted into a digital template. This can then be compared with others for verification and identification purposes.

The general interest in iris verification applied to public technology is centred upon its accuracy or reliability, which is much greater than say fingerprints and the fact that the biometric itself can be acquired without the individual having to come into physical contact with the 'end-point'.

Limitation

There is need for more than two forms of authentication process to make the system more secured.

F. Multilevel ATM Security Based on Two Factor Biometrics [9].

Motivation

Security management for networks and data is a major issue now-a-days. Fraudsters are increasing day by day introducing new hacking techniques.

Objective

The main aim of the research is to provide network security for real time application, ATM System. The objective is to propose a unique authentication and encryption technique using two factor biometric pattern of a person.

Methodology

The system combines PIN, thumb print scanning and face recognition. For face recognition PCA and Eigen algorithm was employed, for steganography LSB algorithm and for cryptography AES algorithm was used. Combining these three algorithms, a proposed system was designed.

Limitation

The use of two biometric features is not cost effective. Other authentication methods could have also been applied for the effectiveness of the system.

G. ATM Transaction Security Using Fingerprint/OTP [10].

Motivation

With the advent of modern technology, there is a drastic increase in fraud. One easy way is ATM fraud which includes fraudulent cash transactions, so there is a need to regularly develop consumer favourable systems to deal with these frauds related to ATM transactions.

Objective

This research proposed the use of fingerprint or One Time Password (OTP) verification along with the use of ATM pin in the ATM security.

Methodology

They made use of fingerprint or One Time Password (OTP) verification along with the use of ATM pin. In this system, the user could have third party authentication either temporary or permanent. The first party i.e. the banker maintained a database of the customer including fingerprint and mobile number. The banker would provide the ATM card along with its PIN. For the transaction after entering the ATM pin, the customer would be asked to choose an option either fingerprint or OTP verification. The OTP would be sent to the registered mobile number of the customer through GSM module connected to the system. After authorised verification, the customer would be able to proceed for transaction. Else after three successive wrong attempts, the ATM card would be blocked for 24 hours and a message would be sent to the registered mobile number.

For fingerprint acquisition, customer's finger is pressed over the fingerprint scanner; this linear sensor captures the fingerprint image. This captured image is matched with the database on the remote server. This whole process is controlled by the central microcontroller chip. During the matching process the information is stored in SRAM.

Limitation

Multifactor authentication involving more than two systems could have provided a better ATM authentication security.

H. Enhancing ATM Security Using Fingerprint and GSM Technology [11].

Motivation

There is need to improve security in ATM transactions. Due to tremendous increase in the number criminals and their activities, the ATM has become insecure.

Objective

This paper combines the pin verification and fingerprint recognition technology for identification.

Methodology

The ATMs are networked and connected to a centralized computer (switch), which controls the ATMs. The use of biometric identification is possible at an ATM. The information can be stored at a bank branch or Network Provider. The typical ATM has two input devices (a card reader and keypad) and four output devices (display screen, cash dispenser, receipt, printer and speaker). Invisible to the client is a communications mechanism that links the ATM directly to an ATM host network. The ATM functions much like a PC, it comes with an operating system (usually OS/2) and application software for the user interface and communications.

While most ATMs use magnetic strip cards and personal identification to identify account holders, other systems may use smart cards with fingerprint validation. The ATM forwards information read from the client's card and the client's request to a host processor, which routes the request to the concerned financial institution. If the cardholder is requesting cash, the host processor signals from the customer's bank account to the host processor's account.

Once the funds have been transferred, the ATM receives an approval code authorizing it to dispense cash. This communication, verification, and authorization can be delivered in several ways.

Limitation

Multifactor authentication provides better security for ATM. They should have used the minutia approach for avoiding the database type attacks. These are so many fingerprint recognition models that are available practice with new fingerprint recognition method.

III. MULTIFACTOR AUTHENTICATION DESIGN

The multifactor authentication that was used in this research was based on what you know – knowledge (your bank account number and registered pin), what you have – Possession (your

One-Time Password – OTP as sent to your registered mobile) and who you are – Inherence (facial biometrics – facial recognition as registered on the application). The system diagram is shown below:

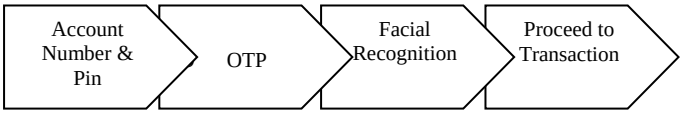

Figure 1: System Diagram for MFA

The windows application that was used in this research is programmed using C# to manage the operation shown in fig 1.0 above. This application stored the following data in its database on user registration: Name, e-mail, phone number, Pin and Facial image.

A. What You Know (Your Account Number and Your Pin)

While registering a user, the application will accept the details listed above and send a pin to the user for their first time login. Hence upon logging into the system, the application will prompt for the account number and pin for authentication. When the user enters both details, the program will verify against its database to ensure the pin is a match for that particular account number serving as a unique identifier for the user.

The user is then required to change this pin to their desired pin number. The application will encrypt this pin using the Secure Hash Algorithm 1 – SHA 1 which makes use of cryptographic hash functions for encryption.

B. What You Have – One Time Password (OTP)

Once the program verifies the correct pin against the account number provided, an OTP will be sent to the user for the next verification process.

The generation of the OTP will be done using a Globally Unique Identifier (GUID) generation process. The GUID is a unique 128-bit number that is produced by the application each time a user is to login.

The OTP to be generated will first be stored in a database with a timestamp and then sent via SMS to a registered phone number of the contact.

The SMS will be sent using a SMS gateway configured to work with the application. The SMS gateway to be used is "Clickatell". The configuration makes use of an API that allows the application to send SMS via its gateway by entering a registered ID on the app that allows the app have access through its gateway.

Once access is granted, the SMS to be sent to the user consists of a short message, the OTP and the time the OTP becomes invalid. The user will receive this message on their phone and proceed to enter the details on the application.

Upon being received by the user, the user will enter the OTP into the application to continue the verification process. For this operation to be successful, the user will have to enter a matching OTP within a space of 10 minutes which is the elapsed time before the OTP expires.

If the time elapses before an OTP is entered into the application by the user or the user enters an incorrect OTP, the OTP generated will be rendered invalid and will be rejected by the application. The user at this stage will need to start the process over again.

C. What You Are - Biometrics (Facial Recognition)

After the verification of the OTP, the user will be required to present a means of verification of who he is, in this research we will be using the image of the face. Once the program verifies the user's image, access to the account will be granted and different operations can be carried out.

Facial recognition will be carried out using EmguCV, which is a cross platform .net wrapper for the OpenCV image processing library. EmguCV allows the use of OpenCV (a C++ image library) on the .net platform with languages like C#.

Face detection and recognition is a section of machine learning; hence application is trained to recognise users by supplying an image of the user. The source can range from a scanned copy of a photograph to a live video stream.

The process of authorization via biometrics is done in two stages:

i. Face Detection
ii. Face Recognition

i. Face Detection

Face detection will be implemented using the Viola-Jones algorithm because it is the easiest ready to use face detection method which is supported by EmguCV and has proven to return

greatly results. In using this algorithm, the system will be making use of a face detector called Cascade Classifier/Detector that has been trained on thousands and thousands of human faces (remember face detection is a subject under machine learning). The training data generated from the faces will be stored in xml files which come by default with the EmguCV package.
For this project, the system made use of the haarcascade_frontalface_alt_tree.xml

ii. Face Recognition

For faces to be recognised, the system needs to train the recognition engine with the data available, the time which this will take would be determined by the processing speed of the computer in use and the size of the dataset.

A new instance of EigenFaceRecognizer was declared which is an EmguCV class as _faceRecognizer, then proceeded to call all the faces stored in the database. Each of the face will be passed to the Train method of the EigenFaceRecognizerclass. The train method takes two major parameters; an array of Images and an array of labels for the images (in our case, userId). The label is what is returned when the face is recognized.

For the recognition of the face, the Predict method of the recognizer engine passing the image to be recognized was used as a parameter.

Viola Jones Algorithm
The Original Viola-Jones Algorithm:
Input: A greyscale image, a scaling factor (s) and scanning factor (p)
Output: The location and size of a detected face

```
Size = detector. Size
while size _ image. height AND size _ image. width
do
    for i from 0 to image. width-size in increments of p
    do
        for j from 0 to image. height-size in increments of p
        do
            if runCascade(subwindow of image of size size located at (i,j)) then
                Add (s,i,j) to detection list
    size = RoundUp (size * s)
return average of detections.
```

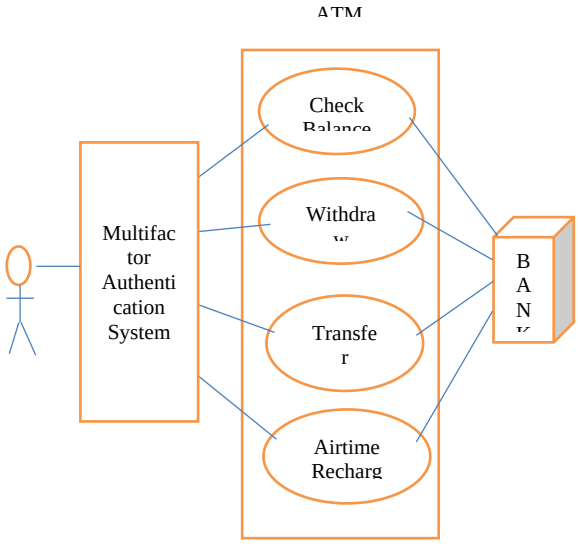

Figure 2: Use Case Diagram of a Bank ATM

The use case diagram of the system is presented above in figure 2 and the overall flow chart of the multifactor authentication model is shown in figure 3.

IV. SYSTEM IMPLEMENTATION AND DISCUSSIONS

The Multifactor Authentication System was implemented using C# as the front end, Visual Studio was used as the compiler and MySQL was the back end (database)/
The application is divided into two:

(i) The registration application
(ii) The main application

i) The Registration Application
a) Registration Page I

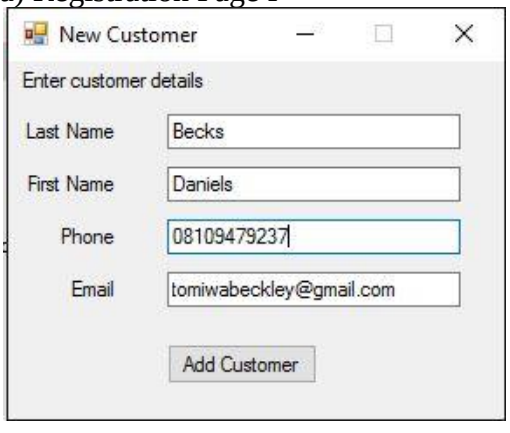

Figure 4: Registration Page I

This is the application that is used to enter the user's credentials into the database. In this module, the customer's first and last names are inputted into the database, along with the user's phone number and their email.

b) Registration Page II

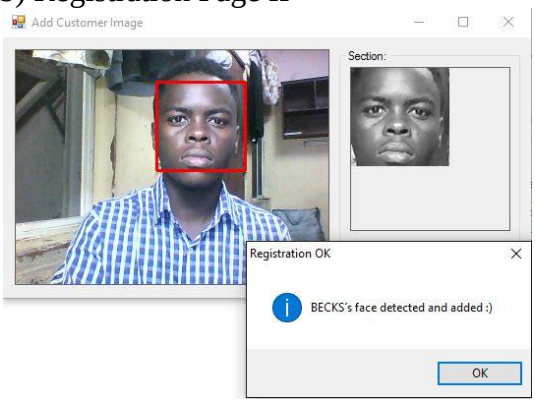

Figure 4.1: Registration Page II

This is the second part of the user's registration; here the picture of the customer's face will be taken and added to the database.

c) Account Details on Phone

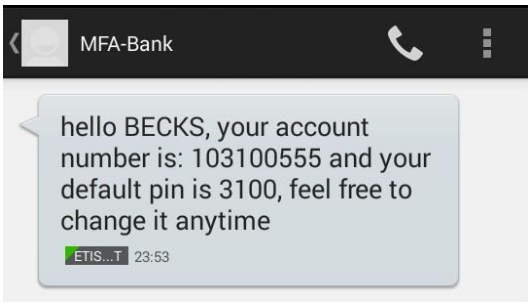

Figure 4.2: Account Number and PIN

This is an example of the system sending a user their account number and their default pin.

ii) The Main Application

a) First Authentication Page (PIN)

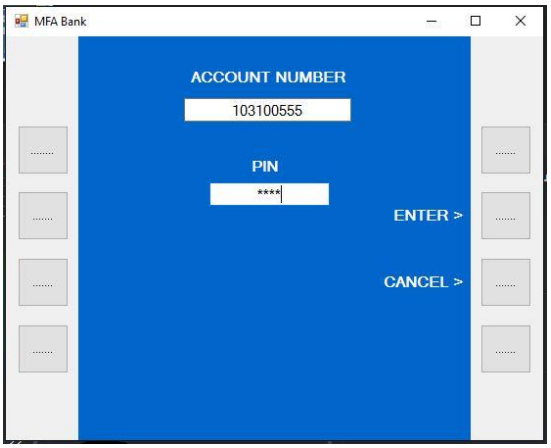

Figure 4.3: First Authentication Page (PIN)

This is the main interface of the application. Here, the user enters their account number and default pin as sent to their mobile phone by the bank. The unique pin code given to each user acts as the first stage of authentication.

b) OTP Sent to Phone

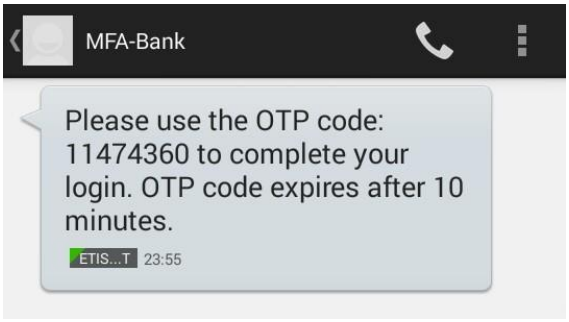

Figure 4.4: OTP sent to User's Phone

The figure above shows an instance of an OTP sent to the user's phone right after the first authentication has been completed, which will then be inputted to the system.

c) Second Authentication Page (OTP)

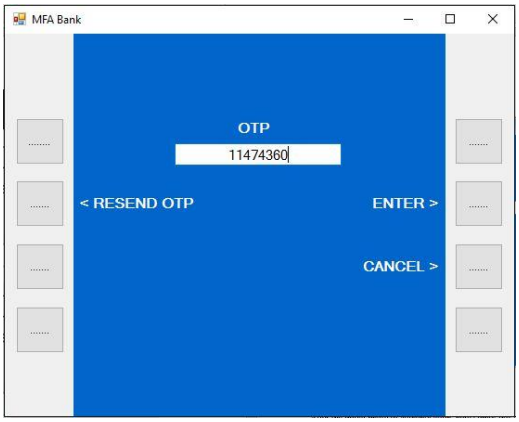

Figure 4.5: Second Authentication Page (OTP)

After the initial phase of authentication, here comes this stage. The user will be asked to enter their one-time password that was sent to them.

d) Third Authentication Page

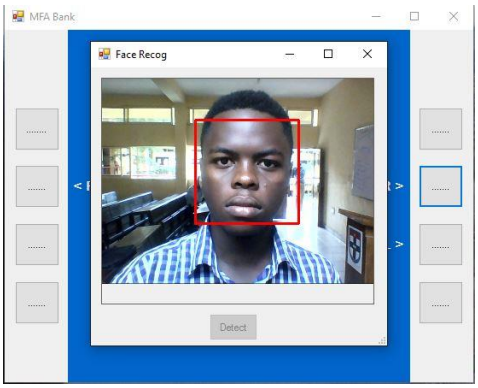

Figure 4.6: Facial Biometric Verification Page

This is the face recognition module. Here, the image of the user will be matched with the images in the database for verification.

e) Error Message I

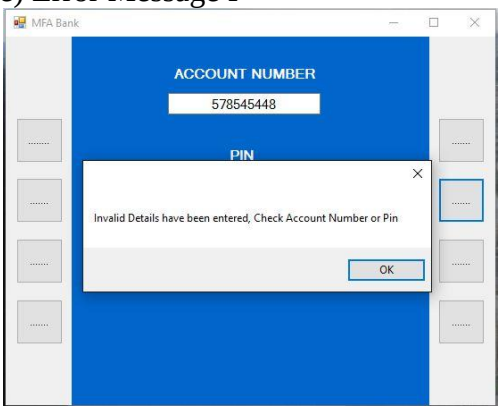

Figure 4.7: Error Message for the First Authentication Page (Account Number and PIN)

This is an error message that shows when an intruder tries to access the account of another user. If the intruder enters either the wrong account number or pin, the system asks the intruder to crosscheck the details.

f) Error Message II

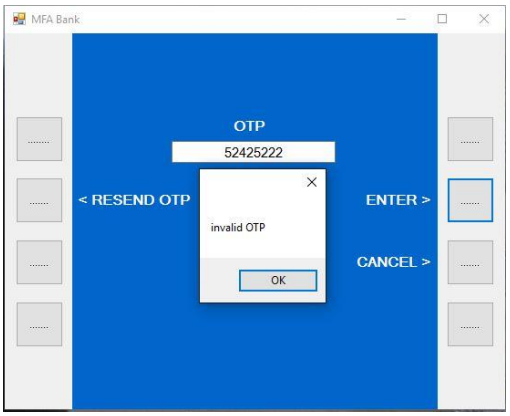

Figure 4.8: Error Message for the Second Authentication Page (OTP)

This is an error message that shows when an intruder/the user input the wrong OTP. The user then has to ask the system to resend the OTP.

g) Error Message III

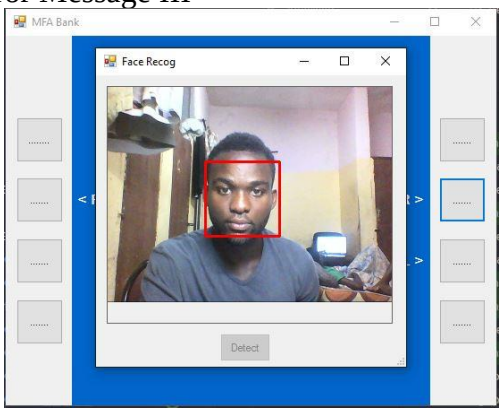

Figure 4.9: Error for the Facial Biometric Verification Page

If an intruder was able to beat the first two stages of authentication, it might not be able to be successful when it comes to facial biometrics. If the intruders face does not match with the face of the user with this account number and PIN in the password, the system gets stuck at this point, no further processes can be carried out and the intruder will have to exit the system.

h) ATM Home Page

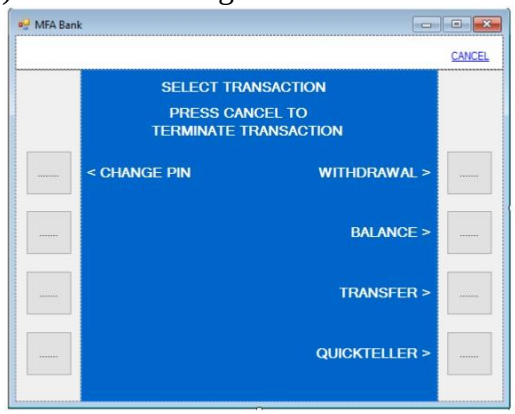

Figure 4.10: Main ATM Interface

This is the initial interface after the three authentication phases has been successfully passed through.

i) Withdrawal Page

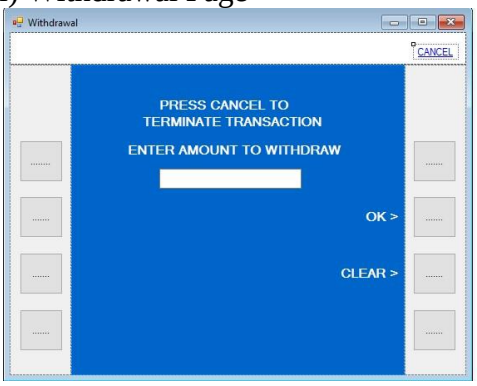

Figure 4.11: Withdrawal Page

Withdrawal interface, here is where the user enters the amount they want to withdraw from the ATM.

j) Balance Enquiry Page

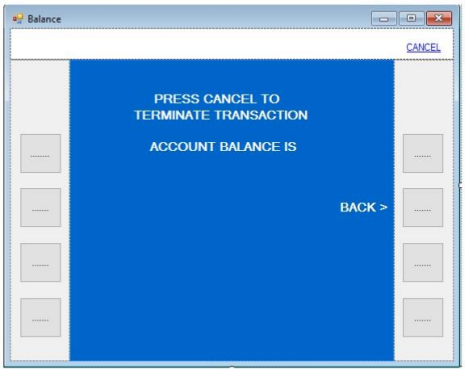

Figure 4.12 Balance Enquiry Page

This is the interface for checking balance

k) Change Pin Page

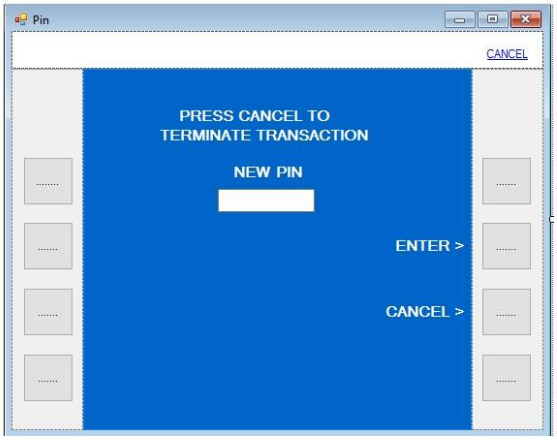

Figure 4.13: Change Pin Page

The user can the change their pin code to any 4 digits of their choice from the default pin given to them by the bank.

V. CONCLUSION

At the end of this research, a multifactor authentication system for securing ATMs to help reduce crime rates at the ATM was developed. Multifactor Authentication in ATM is a very important technology which should be adopted in various financial institutions to curb the crime rate that has been facing the country. This project has helped in providing a more secure way of protecting user's account. It brought what you know, what you have and who you are (factors) together to function as one. The system was implemented with C# using MS Visual Studio 13.

The PIN which is a combination of four digits number is given by the bank which can be changed by the user's at any time, the OTP was sent to the user's phone with the help of the Clickatell API. The face detection and recognition aspects were implemented with the use of the Viola Jones Algorithm.

REFERENCES

[1] C. A. Jegede, "Effects of Automated Teller Machine on the Performance of Nigeria Banks". American Journal of Applied Mathematics and Statistics, 2.1 (2014): 40-46.

[2] http://www.searchsecurity.techtarget.com/definition/multifactor-authentication-MFA/ (accessed - April 21, 2016).

[3] A. Jain, L. Hong and S. Pankanti, "Biometrics Identification." Communications of

the Association for Computer Machinery, February 2000, Vol. 43, Issue 2, pp 91-98.

[4] S. Eum, J. Suhr and J. Kim,. "Face Recognisability Evaluation for ATM Applications with Exceptional Occlusion Handling." In proceedings of Institute of Electrical and Electronic Engineers Conference on Computer Vision Recognition Workshops, School of Electrical and Electronic Engineering, Yonsei University, Republic of Korea, June 2011, pp 82-89.

[5] S. Oko and J. Oruh, "Enhanced ATM Security System Using Biometrics." International Journal of Computer Science Issues, September 2012. Vol. 9, Issue 5, No 3, pp 352-357.

[6] O. Ibidapo, O. Zaccheous, Akinyemi, O. Omogbadegun and O. Oyelami, "Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria E-Banking System." International Journal of Electrical & Computer Sciences, Vol. 10, Issue 6-December 2010, pp 68-73.

[7] P. Krishnamurthy and M. Redddy, "Implementation of ATM Security by Using Fingerprint Recognition and GSM." International Journal of Electronics Communication and Computer Engineering, 2012, Vol. 3, Issue 1. pp 83-86.

[8] L. Coventry, A. Angeli and G. Johnson, "Usability and Biometric Verification at the ATM Interface." Advanced Technology and Research NCR Financial Solutions Division. Vol. 5, Issue 1-April 2003, pp 153-160.

[9] P. Mali, S. Salunke, R. Mane and P. Khatavkar P, "Multilevel ATM Security Based on Two Factor Biometrics." International Journal of Engineering Research & Technology October 2012. Vol. 1, Issue 8, pp 1-6.

[10] K. Pandey, M. Masoom, S. Kumari and P. Dhiman, "ATM Transaction Security Using Fingerprint/OTP." Journal of Emerging Technologies and Innovative Research, March 2015. Vol. 2, Issue 3, pp 448-453.

[11] V. Padmapriya and S. Prakasam, "Enhancing ATM Security Using Fingerprint and Gsm Technology." International Journal of Computer Applications, October 2013. Vol. 80, Issue 16, pp 43-46.