

Design of Fingerprint Biometrics on an Automated Teller Machine (ATM)

BUREMOH, Ekundayo Peter

Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomosho, Oyo State, NIGERIA.

Corresponding Author: dayourburemoh@gmail.com



www.jrasb.com || Vol. 5 No. 4 (2026): August Issue

Received: 03-07-2026

Revised: 15-07-2026

Accepted: 17-07-2026

ABSTRACT

The advancement in technology has resulted in a greater demand for fast and accurate user identification and authentication. The research work aimed at developing standard level of security measure using fingerprint biometric technology. The objectives provide cogent security to customers account and curb the rate of fraud in banking system which secure customer account details and it give access to authorized user which increase the security measure in an ATM machine. The methodology used was survey data analysis which is observation method whereby Visual Basic 6.0 was used to design and integrate fingerprint using the fingerprint reader and software development kit (SDK). The usage of information technology communication was reviewed by proposing a system that improves services of ATM security system. As our focus is on enhancing the process of identification and authentication on ATM, the use of the fingerprint as a suitable substitution for the personal identification number (PIN) was proposed. An embedded system was developed in this paper, which was used for ATM security applications, providing means of cogent security to customers account through the combination of fingerprint code and the ATM card code.

Keywords- Biometric, ATM, PIN, Fingerprint.

I. INTRODUCTION

Fingerprint authentication has been in use for a while and bears more advantages than other biometric technologies. Fingerprint verifications play an important role in forensic application, criminal's investigation, terrorist identification, or any other security purpose. Fingerprint verification is proved as one of the most reliable personal identification scheme. Biometric refers to accurately identifying individual based on his/her distinctive physiological characteristics (e.g. Fingerprint, face retina, iris) or behavioral (e.g. gait, signature, ATM) traits. Fingerprint verification methods include minutiae-based and image-based methods [1].

Rapid development of banking technology has changed the way banking activities are dealt with. One banking technology that has impacted positively and negatively to banking activities and transactions is the advent of Automated Teller Machine (ATM). With an

ATM, a customer is able to conduct several banking activities such as cash withdrawal, money transfer, paying phone and electricity bills beyond official hours and physical interaction with bank staff. In a nutshell, ATM provides customers a quick and convenient way to access their bank accounts and to conduct financial transactions. Personal identification number (PIN) or password is one important aspect in ATM security system. PIN or password is commonly used to secure and protect financial information of customers from unauthorized access.

There is no doubt that fingerprint verification is based on these method so in addition hybridization is also useful for fingerprint verification because fingerprint recognition refers to the automated method of verifying a match between two human fingerprint [2]. Suppose we have twins using the same account though they using same account but their fingerprint (thumb impression) are different. This is known with the use of biometric, However, the financial criminal tamper with the ATM

terminal, steal user's credit cards and password by illegal means. Suppose by mistake one user's card is lost and the password stolen, then the criminal withdraw all the cash in the shortest time. How to carry on the valid identity to the customer becomes the focus in current financial circle. Therefore it is so important that the biometric thumb impression which gives the main identification proof of any unknown person. So, for ATM security using the hybridizing method with biometric fingerprint verification is required.

Fingerprint has intrinsic features that they do not change for whole life and are personally different. And they are easy to use, cheap and the most suitable miniaturization. So, fingerprint verification is an efficient personal verification method that has been the most widely used in comparison with other biometric information [1].

1.1. Statement of the problem

The financial crime case rises repeatedly in recent years, a lot of 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. How to carry on the valid identity to the customer becomes the focus in current financial circle. Traditional ATM systems authenticate generally by using the credit card and the password, the method has some defects. Using credit card and password cannot verify the client's identity exactly. So a security measure is developed and designs to improve security safety on ATM machine which is biometric finger print on ATM machine.

The main aim of this project work is to develop fingerprint base system, which is used for ATM security applications and it has the objectives are ; to provide means of cogent security to customers account through the combination of fingerprint code and the ATM card code; to cub the rate of fraud in banking system.

II. LITERATURE REVIEW

2.1. Historical background on ATM crime

Crime at ATMs has become a nationwide issue that faces not only customers, but also bank operators and this financial crime case rises repeatedly in recent years [3]. A lot of criminals tamper with the ATM terminal and steal customers' card details by illegal means. Once users' bank card is lost and the password is stolen, the users' account is vulnerable to attack. Traditional ATM systems authenticate generally by using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects [4]. The prevailing techniques of user authentication, which involves the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations [5]. Passwords and PINs can be illicitly acquired by direct covert observation. When credit and

ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords - birthdays, phone numbers and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he/she claims to be. Biometric authentication technology may solve this problem since a person's biometric data is undeniably connected to its owner, is nontransferable and unique for every individual. The system can compare scans to records stored in a central or local database or even on a smart card.

Biometrics can be defined as a measurable physiological and behavioral characteristic that can be captured and subsequently compared with another instance at the time of verification. It is automated methods of recognizing a person based on a physiological or behavioral characteristic [6]. It is a measure of an individual's unique physical or behavioral characteristics to recognize or authenticate its identity [7]. Common physical biometrics characteristics include fingerprint, hand or palm geometry, retina, iris and face while popular behavioral characteristics are signature and voice. Biometrics technologies are a secure means of authentication because biometrics data are unique, cannot be shared, cannot be copied and cannot be lost.

2.2. Luther Simjian's ATM

Luther Simjian came up with the idea of creating a "hole-in-the-wall machine" that would allow customers to make financial transactions. In 1939, Luther Simjian applied for 20 patents related to his ATM invention and field tested his ATM machine in what is now Citicorp. After six months, the bank reported that there was little demand for the new invention and discontinued its use.

As analyzed by [8] the United Kingdom identity card scheme. Their analysis approached the scheme from the perspective of high volume public deployment and described a trade-off triangle model. They found that there is a trade-off between several characteristics, i.e., accuracy, privacy and scalability in biometric based identity management system, where emphasis on one undermines the other. [4]

Developed an embedded fingerprint system, which is used for ATM security applications. In their system, bankers collect customers' finger prints and mobile numbers while opening accounts, then customer only access ATM machine. The working of the ATM machine is such that when a customer place a finger on the finger print module it 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 is entered into the ATM machine 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.

As presented by [7] an evaluation of the Netherlands' proposed implementation of a biometric passport, largely focusing on technical aspects of specific

biometric technologies (such as face and fingerprint recognition) but also making reference to international agreements and standards (such as ICAO and the EU's "Extended Access Control") and discussed the privacy issue in terms of traditional security concepts such as confidentiality. [9] proposed an embedded Crypto-Biometric authentication scheme for ATM banking system.

It is most important that when the person enters bank to open his/ her account using ATM then it's necessary to give his/her thumb impression for security purpose. In minutiae-based fingerprint verification is fast verification execution is possible but though two fingerprints have the minutia, they do not necessarily have the same ridge. When the range of fingerprint image input is narrow as enough minutiae are not extracted, the verification confidence decreases but the size of fingerprint image is small, more exact verification is possible [1]. In general, the fingerprint image input for fingerprint verification is Gray image with lightness of 256. If the gray image is changed into a binary fingerprint image through binarization, the ridge and valley of the fingerprint will have consistent lightness and ridges which are discontinued by wrinkles, sweat, pores and finger pressure are connected. Fingerprint authentication is possibly the most sophisticated method of all biometric technologies and has been thoroughly verified through various applications. However, fingerprint is completely unique to an individual and stayed unchanged for lifetime [10]. For this reason this method is suitable for thumb impression on biometric whenever using the ATM (Automatic Teller Machine). This exclusivity demonstrates that fingerprint authentication is far more accurate and efficient than any other methods of authentication. Because fingerprints are now being used as a secure and effective authentication method in numerous fields, including financial, medical and any other entrance control applications. As saying that fingerprint is the most widely used biometric feature for person identification and verification in the field of biometric identification. Fingerprint possesses two main types of features that are used for automatic fingerprint identification and verification one is ridge and other is minutiae. So the ridge and furrow structure that forms a special pattern in the central region of the fingerprint and the other minutiae details associated with the local ridge and furrow structure.

In a traditional biometric recognition system, the biometric template is usually stored on the central server during enrolment, and then the candidate biometric template captured by the biometric device is sent to the server where the processing and matching steps are performed. Same like when the person enters the security code on the ATM machine then the machine wants to get the fingerprint(thumb impression) about that persons who enter the security code if the person is right then the machine gives a positive result otherwise doesn't get result or say 'please try again'. Using this system firstly

collect all the customers fingerprint when they draw bank account and add all fingerprint about that person identification information .Because the biometric machine recognize given fingerprint using False Rejection Rate (FRR) , this image database ,each sample is matched against the remaining samples of the same finger to compute the False Rejection Rate and False Acceptance Rate(FAR) .this also the first sample of each finger in the database is matched against the first sample of the remaining fingers to compute the False Acceptance Rate , So using all these process we can control or stop that the criminal process which gives the duplicate number and draw all cash in ATM. In the former a person to be identified submits a claim, which is either accepted or rejected. In the latter, a person is identified without a person claiming to be identified. Generally in human identification is the association of an identity with a human being, traditionally, password and ID cards have been used for identification to restrict access to secure systems but these methods can be easily breached, for password can be guessed and ID card can be stolen , thus rendering them reliable. One important thing is the fingerprint recognition systems are usually used only for adults. Because we might be able to recognize the fingerprints of infants, the common fingerprint recognition systems are suitable for adults only (due to the area and resolution of fingerprint sensors etc.).

2.3. Biometrics

Biometrics is the science and technology of measuring and statistically analyzing biological data. In information technology, biometrics usually refers to technologies for measuring and analyzing human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, especially for authentication purposes Authentication by biometric verification is becoming increasingly common in corporate and public security systems, consumer electronics and point of sale (POS) applications. In addition to security, the driving force behind biometric verification has been convenience.

Biometric devices, such as finger scanners, consist of:

1. A reader or scanning device
2. Software that converts the scanned information into digital form and compares match point
3. A database that stores the biometric data for comparison

To prevent Identity theft, biometric data is usually encrypted when it's gathered. Here's how biometric verification works on the back end: To convert the biometric input, a software application is used to identify specific points of data as match points. The match points in the database are processed using an algorithm that translates that information into a numeric value. The database value is compared with the biometric input the end user has entered into the scanner and authentication is either approved or denied. Example of biometrics system

is shown in Fig 1 and the interface of users information is shown in Fig 2 respectively

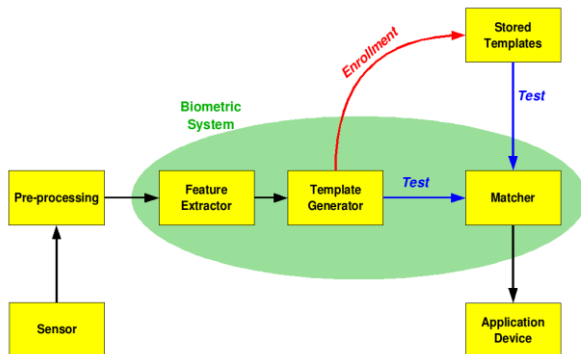


Fig 1: Biometric System

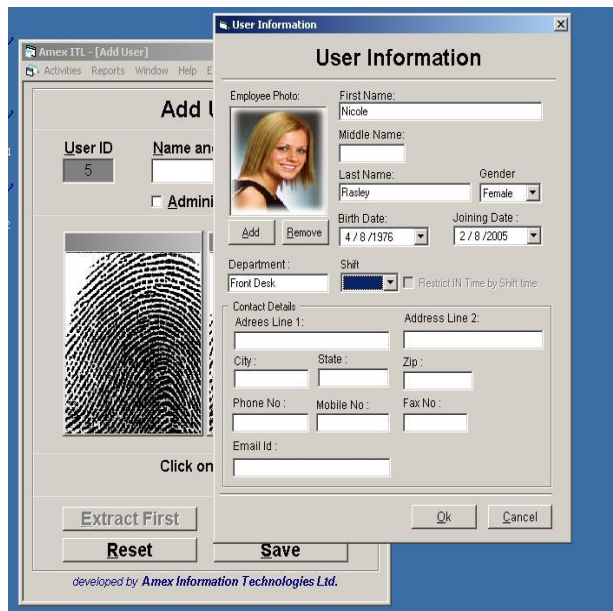


Fig 2: Interface of users information

2.4. Fingerprint

A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. The recovery of fingerprints from a crime scene is an important method of forensic science. Fingerprints are easily deposited on suitable surfaces (such as glass or metal or polished stone) by the natural secretions of sweat from the eccrine glands that are present in epidermal ridges. In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human or other primate hand. A print from the foot can also leave an impression of friction ridges. Deliberate impressions of fingerprints may be formed by ink or other substances transferred from the peaks of friction ridges on the skin to a relatively smooth surface such as a fingerprint card. Fingerprint records normally contain impressions from the pad on the last joint of fingers and thumbs, although fingerprint cards also typically record portions of lower joint areas of the fingers.

Human fingerprints are detailed, unique, difficult to alter, and durable over the life of an individual making them suitable as long-term markers of human identity and may be employed by police or other authorities to identify individuals who wish to conceal their identity, or to identify people who are incapacitated or deceased and thus unable to identify themselves, as in the aftermath of a natural disaster. Fingerprint analysis, in use since the early 20th century, has led to many crimes being solved. This means that many criminals consider gloves essential.

Fingerprint identification, known as dactyloscopy, or hand print identification, is the process of comparing two instances of friction ridge skin impression from human fingers or even the palm of the hand to determine whether these impressions could have come from the same individual. The flexibility of friction ridge skin means that no two finger or palm prints are ever exactly alike in every detail; even two impressions recorded immediately after each other from the same hand may be slightly different. Fingerprint identification, also referred to as individualization, involves an expert, or an expert computer system operating under threshold scoring rules, determining whether two friction ridge impressions are likely to have originated from the same finger or palm. An image of a fingerprint created by the friction ridge structure shown in Fig 3.



Fig 3: An image of a fingerprint created by the friction ridge structure

An intentional recording of friction ridges is usually made with black printer's ink rolled across a contrasting white background, typically a white card. Friction ridges can also be recorded digitally, usually on a glass plate, using a technique called Live Scan. A "latent print" is the chance recording of friction ridges deposited on the surface of an object or a wall. Latent prints are invisible to the naked eye, whereas "patent prints" or "plastic prints" are viewable with the un-aided eye. Latent prints are often fragmentary and require the use of chemical methods, powder, or alternative light sources in order to be made clear. Sometimes an ordinary bright flashlight will make a latent print visible. When friction ridges come into contact with a surface that will take a print, material that is on the friction ridges such as

perspiration, oil, grease, ink or blood, will be transferred to the surface. Factors which affect the quality of friction ridge impressions are numerous. Pliability of the skin, deposition pressure, slippage, the material from which the surface is made, the roughness of the surface and the substance deposited are just some of the various factors which can cause a latent print to appear differently from any known recording of the same friction ridges. Indeed, the conditions surrounding every instance of friction ridge deposition are unique and never duplicated. For these reasons, fingerprint examiners are required to undergo extensive training. The scientific study of fingerprints is called dermatoglyphics.

2.5. Types

2.5.1. Exemplar

Exemplar prints as shown in Fig 4 is the name given to fingerprints deliberately collected from a subject, whether for purposes of enrollment in a system or when under arrest for a suspected criminal offense. During criminal arrests, a set of exemplar prints will normally include one print taken from each finger that has been rolled from one edge of the nail to the other, plain (or slap) impressions of each of the four fingers of each hand, and plain impressions of each thumb. Exemplar prints can be collected using Live Scan or by using ink on paper cards.



Fig 4: Exemplar prints on paper using ink

2.5.2. Latent

Latent prints as shown on a knife in Fig 5, may exhibit only a small portion of the surface of a finger and this may be smudged, distorted, overlapped by other prints from the same or from different individuals, or any or all of these in combination. For this reason, latent prints usually present an “inevitable source of error in making comparisons,” as they generally “contain less clarity, less content, and less undistorted information than a fingerprint taken under controlled conditions, and much, much less detail compared to the actual patterns of ridges and grooves of a finger.



Fig 5: Barely visible latent prints on a knife

2.5.3. Patent

Patent prints are chance friction ridge impressions which are obvious to the human eye and which have been caused by the transfer of foreign material from a finger onto a surface. Some obvious examples would be impressions from flour and wet clay. Because they are already visible and have no need of enhancement they are generally photographed rather than being lifted in the way that latent prints are. An attempt to preserve the actual print is always made for later presentation in court, and there are many techniques used to do this. Patent prints can be left on a surface by materials such as ink, dirt, or blood.

2.5.4. Plastic

A plastic print is a friction ridge impression left in a material that retains the shape of the ridge detail. Although very few criminals would be careless enough to leave their prints in a lump of wet clay, this would make a perfect plastic print. Commonly encountered examples are melted candle wax, putty removed from the perimeter of window panes and thick grease deposits on car parts. Such prints are already visible and need no enhancement, but investigators must not overlook the potential that invisible latent prints deposited by accomplices may also be on such surfaces. After photographically recording such prints, attempts should be made to develop other non-plastic impressions deposited from sweat or other contaminants.

2.5.5. ATM Security threats

Since the introduction of the first automated teller machine (ATM) in 1967, perpetrators have been devising ways to try to steal the cash inside. Because ATMs eliminate the need for round-the clock human involvement and tend to be located in places that make them more vulnerable to attack, they are often attractive targets for perpetrators. ATM crime is not limited to the theft of cash in the ATM. Many ATM attacks seek to obtain a consumer’s personal information, such as their card number and personal identification number (PIN). While these types of identity theft attacks take more effort to net cash for perpetrators, the result is the same—illegally obtaining money. According to estimates by Retail Banking Research, there are more than 2.2 million ATMs deployed worldwide. This is a figure forecasted to exceed 3 million by 2016. As the number of ATMs in use increases, so do the frequency and sophistication of security threats, making the development of fraud prevention measures a top priority for financial institutions (FIs) and ATM manufacturers. This project details a comprehensive overview of the current threats to the ATM channel and best practices in security and consumer safety issues facing the self-service industry. It describes techniques perpetrators use to commit fraud and introduces security management practices and devices designed to keep ATMs secure.

2.6. Types of ATM threats

ATM threats can be segmented into three types of attacks:

1. Card and currency fraud, logical attacks and physical attacks. Card and Currency Fraud Card and currency fraud involves both direct attacks to steal cash from the ATM and indirect attacks to steal a consumer's identity (in the form of consumer card data and PIN theft). The intent of indirect attacks is to fraudulently use the consumer data to Create counterfeit cards and obtain money from the consumer's account through fraudulent redemption.
2. Skimming ATM card skimming is the most prevalent and well known attack against ATMs. Card skimmers are devices used by perpetrators to capture cardholder data from the magnetic stripe on the back of an ATM card. These sophisticated devices—smaller than a deck of cards and resembling a hand-held credit card scanner—are often installed inside or over top of an ATM's factory-installed card reader. When the consumer inserts his card into the card reader, the skimmer captures the card information before it passes into the ATMs card reader to initiate the transaction. The transaction continues in a normal fashion. When removed from the ATM, a skimmer allows the download of personal data belonging to everyone who used the ATM. An inexpensive, commercially available skimmer can capture and retain account numbers and PINs for more than 200 ATM cards.

Typically, criminals design skimming devices to be undetectable by consumers. The following are three kinds of card skimming attacks that can occur:

- i. External card skimming – placing a device over the card reader slot (motorized or dip) to Capture consumer data from the magnetic stripe on the card during a transaction. This is the most common form of card skimming.
- ii. Internal card skimming – gaining access to the top hat of the ATM to modify the card reader or replace the original card reader with an already modified one for the purpose of obtaining Consumer card data during a transaction.
- iii. Vestibule card skimming – in locations where the ATM is located within a vestibule, skimmers are placed on the vestibule door card access reader to capture cardholder data from the magstripe Where the card is read so an unwary consumer inserts their card into the vestibule instead of on the ATM.

A skimming attack is usually combined with other fraudulent devices such as covert cameras or keypad overlays that capture the consumer's PIN as it is being entered on the keypad during a transaction. Some skimming perpetrators have even installed signs on ATMs instructing cardholders to "swipe here first" before continuing with transactions. Another fraudulent method is to portray the additional card reader as a "card cleaner" designed to extend the life and improve the performance of ATM magnetic stripes.

III. METHODOLOGY AND ANALYSIS OF THE EXISTING SYSTEM

The method used in data collection during the course of this research is through the use of internet and direct observation gathered from source in Banking System. Information's are gathered based on the available resources extracted from the research methodology. Hence, in the research the usage of information technology communication is reviewed by proposing a system that improves services of ATM Security system. The language used in designing this proposed system is Visual Basic programming language with a link to the database with the use of Microsoft Access.

3.1. Analysis of data and the existing system

The existing system though computerized but yet there are some limitations detected from system it which leads to the development of the proposed system.

In the world today, fingerprint is one of the essential variables used for enforcing security and maintaining a reliable identification of any individual. Fingerprints are used as variables of security during voting, examination, operation of bank accounts among others. They are also used for controlling access to highly secured places like offices, equipment rooms, and control centers and so on.

3.2. Problem of the existing system

The proposed system that is introduced by Road safety commission is used to find solutions to all problems involving fake driver's license and also the road user identity. This leads to design and implementation involving the use of biometric data capturing in a digital form for Road Safely Commission in order to have the database of all road users and their identity, they encounter a lot of malfunction and error, This well developed system will be developed to tackle and control manual manipulation made by this commission through logistic processing and human intervention, other factors necessary will be handled in the proposed system which will allow the Road Safety Commission to adopt the use of this proposed system.

3.3. Description of the proposed system

The proposed system is to check through the problems and limitations of crimes in Automated Teller Machine (ATM), which include

1. Checking the swelling fraud over an Automated Teller Machine
2. Moving from ordinary pin code to a more secure system similar to the master card whereby the biometric data of users including finger prints would help assessment of account through ATM
3. Mitigating the level of fraud in the banking industry by tracking the challenge of identity theft on ATM machines and helping banks achieve a higher level of know your customer

3.4. Advantages of the proposed system

1. Accuracy: it is enhanced using computerized approach, thereby mastering decision making perfect.
2. Storage capacity: it is enhanced using computerized system have a very large storage capacity, very large computer installations are capable of storing billions of data which could be accessed easily.
3. Maintainable: it can be adopted for use at any time.
4. Security of data: data to be processed or information can be store in secondary storage and these secondary storage devices are kept safety even with back-ups. They are compact and can be kept safely
5. Fast processing: it takes a very short to process the operations of Road Safety Commission by the use.
6. Less labour requirement: with the application of the proposed system, labor requirement is tremendously reduced to its minimal.

IV. DESIGN, IMPLEMENTATION AND DOCUMENTATION OF THE SYSTEM

4.1. Design of the system

Design is a creative process. It is the key to an effective system. It is the process of applying various techniques and principle for the purpose of defining a process or a system in sufficient detail to permit its physical realization.

Software design sits at the technical kernel of the software engineering process and is applied regardless of the development paradigm that is used.

4.2. Input design

The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input design is shown in Fig 6, Fig 7 and Fig 8 respectively

ATM Using Biometrics FingerPrint

A Case Study Of:

First Bank Of Nigeria Plc.



Fig 6: Splash Screen on ATM using Biometrics FingerPrint

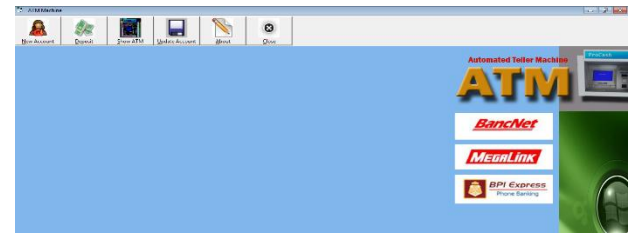


Fig 7: Main Menu of ATM using Biometric FingerPrint

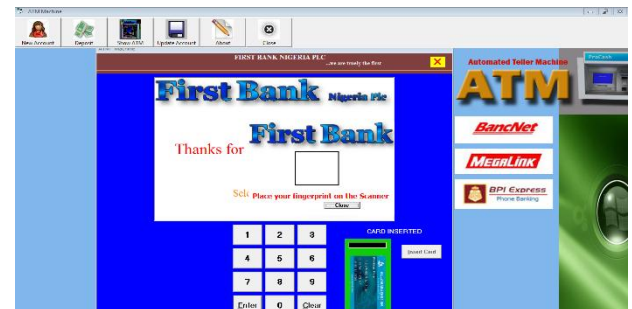


Fig 8: ATM Machine requesting for Fingerprint before you can login.

4.3. Output Design

An efficient and intelligent output design improves the system's relationship to help user decision-making.

Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system easily and effectively to use. Fig 9, Fig 10 and Fig 11 respectively shows the successive output design.

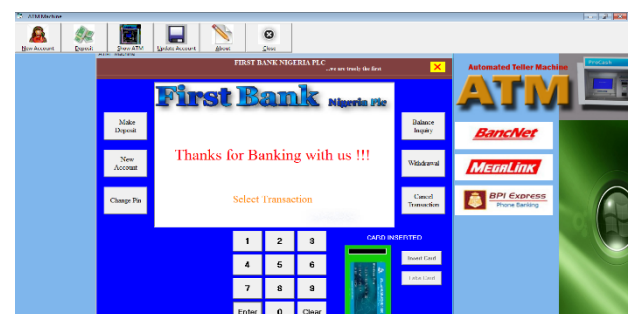


Fig 9: ATM Interface with Accepted Fingerprint

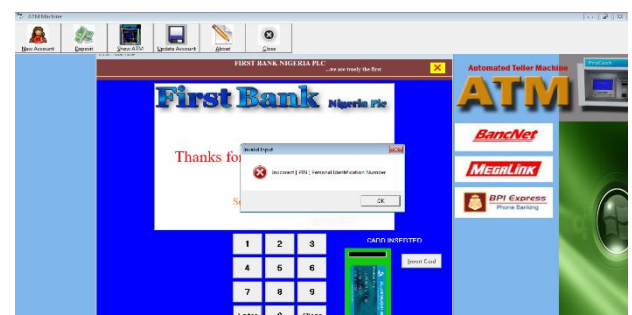


Fig 10: ATM Interface with Incorrect Personal Identification Number (PIN)

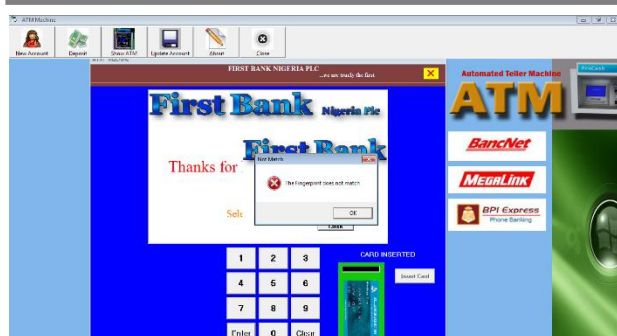


Fig 11: ATM Interface with Correct PIN but Unmatched Fingerprint.

4.4. Database design

The ATM database is shown in Fig 12, the database provides pace for retrieving of various file of messages at any needed time

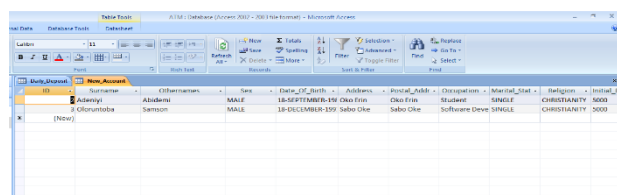


Fig 12: ATM database

4.5. Procedure of the design

The procedure followed during the course of this design includes:

1. Installation of Microsoft visual basic into the system.
2. Designing of the various modules with codes.
3. Test running of the program for error-free and effectiveness.

4.6. System implementation

The proposed system is a system used to used to develop biometric finger print on an automated teller machine and here are the following steps taken and implement a cogent security to customers account through the combination of fingerprint code and the ATM card code, a database that stores biometric data for comparison has been developed. This database checks whether or not the user of the ATM card is the rightful owner and it check the code of ATM before the authentication. The database is designed such a way that the system detects immediately if a fraud is being carried out on other people's card, the database also design to focus on controlling the amount of the input that is required, controlling the errors, avoiding delays and extra step talking which makes it simple and efficient for all users, the database helps in retrieving various files and message at any point in time and at any time needed.

An efficient and intelligent output design is also implemented which helps in the integration of the systems relationship which helps the user to take and make decisions. A well designed output is ensured which helps in ensuring that each output element is easy and efficient to all users without difficulty. Lastly a security measure is

taken to integrate the performance of the automated teller machine in such a way that if the user attempts the code more than five times the system will automatically shot down or seize the ATM card, the measure will curb and reduce the rate of fraud on an automated teller machine.

4.7. Choice of programming language

The choice of programming language used in the development of the software interface is Microsoft Visual Basic programming language while java was used for the back end i.e. the database

4.8. Hardware support

The requirements for the implementation of this proposed system are the following

1. Computer system must have at least 1.7MHZ speed for the processor.
2. 125-512 RAMs
3. At least 20GB and above hard disc or hard drive.
4. At least Pentium III and above board configuration.

4.9. Software support

The software support for this proposed system include training end-user in order to allow different users to access the proposed system.

But to achieve the aims and objectives of the study, there must be a strong AVG antivirus to protect against virus attack etc.

4.10. Implementation techniques used in detail

The implementation techniques used in the Secure ATM transaction using biometrics finger print on a system is done to allow the end-users secure information sent.

4.11. System documentation

4.11.1. Program documentation

Program documentation includes:

1. Installing the software of the proposed system.
2. Click on start at the bottom of the desktop to implement the program.
3. Locate the project by clicking on ATM Security using Finger Print Software.

4.11.2. Maintaining the System

The proposed system can be maintained by training end-users before accessing the system.

1. Always shut down the system.
2. Connect your system to an uninterrupted power supply.

V. CONCLUSION

As our focus is on enhancing the process of identification and authentication on ATM, This project work has proposed the use of the fingerprint as a suitable substitution for the personal identification number (PIN). And in this project work an embedded system was develop, which is used for ATM security applications, which provided means of cogent security to customers account through the combination of fingerprint code and the ATM card code and also cub the rate of fraud in banking system as we all know that fingerprints are the

most acceptable biometrics all over the world in identifying a person. Some governments in the world are still implementing fingerprints technique to identify their citizens and the criminals from the scene of crimes in forensic work. In this project fingerprint are chosen for its uniqueness, ease of use and also convenience to user; as fingerprints can't be stolen, it is not transferable and the user don't need to remember.

REFERENCES

- [1] Kim, J., Chae, H., Lim, S., and Pan, B. (2012). A Study on the Performance Analysis of Hybrid Fingerprint Matching Methods. Pp 45-79
- [2] Maria, V., Alexandra, A., Madalin., S. V., (2012). Automatic Identification Technologies. *International Journal of Scientific and Research Publications*. Vol. 2, Issue 11 pp 259
- [3] Richard, B. and Alemayehu, M. (2006). "Developing E-banking Capabilities in a Ghanaian Bank: Preliminary Lessons. *Journal of Internet Banking and Commerce*. 14 (3) pp 28-108
- [4] Amurthy P. and Redddy, M. (2012), "Implementation of ATM Security by Using Fingerprint recognition and GSM", *International Journal of Electronics Communication and Computer Engineering*. 15(1): pp 203-301
- [5] Ratha, N., Connell, H., and Bolle, M. (2001). "Enhancing Security and Privacy in Biometrics-based Authentication Systems, *IBM Systems Journal*. 6 (5) pp 29-156
- [6] Ratha, K., Chikkerur, S., Connell, H., and Bolle, M. (2007). "Generating Cancelable Fingerprint Templates", *IEEE Transaction on Pattern Analysis and Machine Intelligence*. 10(1) pp 10-57
- [7] Schouten, B., and Jacobs, B., (2009). "Biometrics and their use in e-passports" *Journal of Image and Vision Computing*. Vol. 27, Issue 3, 2. Pp 305-312.
- [8] Shaikh, A. and Rabaiotti, R. (2010). "Characteristic trade-offs in designing large-scale biometric-based identity management systems". *Journal of Network and Computer Applications*. 5(6) pp 211-308
- [9] Das, S and Debbarma, J. (2011) "Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian e-banking System", *International Journal of Information and Communication Technology Research*. 14(2): pp 10-56
- [10] Kant, C. and Nath, R. (2009) Reducing Process-Time for Fingerprint Identification System. Pp 23-78