Implementation of the Enhanced Fingerprint Authentication in the ATM System Using ATmega128 with GSM Feedback Mechanism

Kennedy Okokpujie, Funminiyi Olajide, Samuel John, Chinyere Grace Kennedy

Abstract- ATM was introduced to boost the cashless policy in Nigeria. Current trend of Cybercrime facilitate the need for an enhanced fingerprint application on ATM machine with GSM Feedback mechanism. The mechanism enable unassigned fingerprint authentication of customers with quick code and secret code. The project enhances the security authentication of customers using ATM. A core controller using fingerprint recognition system of ATmega128 in-system programmable flash is explored. An SM630 fingerprint module is used to capture fingerprints with DSP processor and optical sensor for verification, using AT command of GSM module for feedback text messaging (i.e. sending of Quick and Secret-Codes respectively). Upon system testing of capable reduction of ATM fraud using C program, the new method of authentication is presented.

Keyword- Automated Teller Machine (ATM) , ATmega128, GSM Module, Language C program, SM360 Fingerprint Module

1. Introduction

The ATM card and PIN have proven to be inadequate security due to the continuous rising threat of ATM related frauds in the emerging global cashless economy. For instance in Nigeria, there are various security breaches and ATM related fraud has risen from 1.6 billion naira (10 million USD) in 2010 to 40 billion naira (250 million USD) in 2013. However, some other countries have higher figures [12]. With technology advancement in electronic banking, bank customers have embraced the use of ATM (Automated Teller Machine) being a unique banking product in Nigeria.

Data from the Nigeria Inter-Bank Settlement System (NIBSS) has revealed that the highest number of fraudulent transactions in the banking sector takes place on Automated Teller Machines (ATMs) with 43 per cent of electronic banking frauds, followed by internet banking which was responsible for 34 per cent [9]. The NIBSS data showed that three per cent of electronic banking fraud took place on Point of Sales (PoS) terminal while e-commerce was responsible for one per cent of electronic banking fraud and others, 19 per cent.

ATM is an electronic gadget that has its roots embedded in the accounts and records of a banking institution [5]. It is a machine that allows the bank's customers to carry out banking transactions like; cash transfers between or among same bank (intra bank-transfer), between or among different bank (inter-bank transfer), between or among a bank customer account and a mobile phone account (mobile money transfer), account balance enquiries, payment of utility bills (electricity bill, water rate, etc.), recharging of air time, cable bill payment, governments levy (Vehicle particulars, custom duties, tenement rate, import and export duty, personal tax income) and cash withdrawal. ATM machine with its 24hours availability also allows those who have no access to internet to carry out their transactions anytime but on real time online platform. This operation has led to ever increasing demand of ATM services been rendered by banks.

Traditional authentication systems (use of PIN) cannot discriminate between an impostor who fraudulently obtains the access privileges (card and PIN) and the genuine user [1][6]. Therefore, to gain the ATM machine user's confidence, a second level biometric authentication security has to be put in place in conjunction with the already existing personal identification number (PIN). The activities of ATM fraudsters in Nigeria have brought about financial hardship and devastation to victims and their families. These activities can also have negative effects on a nation's economy and has cause the erosion of trust of banking institutions by the banking public. Hence, there is need to urgently tackle this problem.

2. Design Consideration and Specification

The embedded ATM client verification system is based on fingerprint recognition which is designed to

Kennedy Okokpujie[1], Funminiyi Olajide[2], Samuel John[3], Chinyere Grace Kennedy[5]
[1,3]Department of Electrical and Information Engineering
[2]Department of Computer and Information Sciences
Covenant University, Ota, Ogun State. Nigeria.
[4]Dept. of Computer Science and Engineering,
Ewha Womans University, Seoul, South Korea
[1]kennedy.okokpujie@covenantuniversity.edu.ng;
[2]funminiyi.olajide@cu.edu.ng;
[3]samuel.john@covenantuniversity.edu.ng,
[4]gkennedy@ewhain.net

improve on the performance of the existing ATM system. The ATmega128 chip is used as the core of this embedded system which is associated with the technologies of fingerprint recognition, GSM feedback mechanism and current high speed network communication. The primary features of the developed system are:

- Fingerprint recognition: The masters' fingerprint information was used as the standards of detection. It must certify the feature of the human fingerprint before using ATM system.
- Remote verification: System that can compare current client's fingerprint information with remote fingerprint data server.
- GSM: There is customer's secret code (i.e. S-Code) generated upon registration of fingerprint in the bank. In an exception of fingerprint verification error of a genuine user, the system demands the customer secret code. In order not to deny a genuine customers access into his/her account, the system is capable to quickly generate a unique 4-digit access code (i.e. Q-Code) on a condition that the customer supplied a correct secret code. This 4-digit access code will be sent as OTP (One Time Password) message code to mobile phone of the authorized customer.
- Two discriminate analysis systems: Unimodal Biometric and Two-tier Security. Two-tier security is used to provide two levels of security. In unimodal system, if the fingerprint system fails (this situation happens very rarely) then, two level security units will take over and further queries will be required from such a user.

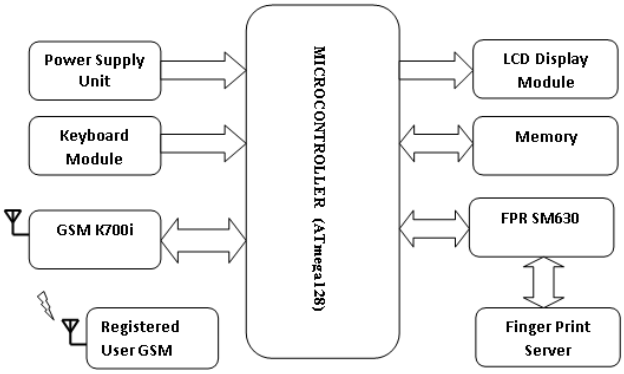

Figure 1.0: Block diagram of the designed system

3.0. Design Analysis of different Sections of the System

The design and implementation of the security for ATM terminals system consist of two parts which are hardware and software. The hardware is designed by the rule of embedded system and the aspect of software consists of several parts [7]. Figure 1 shows the major system modules and their interconnections.

3.1. Microcontroller (ATMEGA128)

The system uses ATmega128 from ATMEL family; it is the core controller in the system. ATmega128 is an 8-bit Atmel microcontroller with 128Kbytes in-system programmable flash with advanced RISC (Reduced Instruction Set Computer) Architecture of 32 x 8 general purpose working register plus peripheral control registers with full static operation. It offers high performance for very low power consumption and cost. The Atmel architecture is based on RISC principles, and the instruction set and related decoding mechanism are much simpler than those of micro-programmed Complex Instruction Set Computers (CISC). This simplicity results in a high instruction throughput up to 16MIPS at 16MHz and an impressive real-time interrupt response from a small and cost-effective chip. (Amtel Microcontroller, 2011)

The Atmel memory interface has been designed to allow the performance potential to be realized without incurring high costs in the memory system. Speed-critical control signals are pipelined to allow system control functions to be implemented in standard low-power logic, and these control signals facilitate the exploitation of the fast local access modes offered by industry standard dynamic RAMs. The ATmega128 device is supported with a full suite of program and system developed tools including: C compilers, macro assemblers, program debuggers/simulators, in-circuit emulators and evaluation kits. These made it suitable for the actualization of the project.

3.2. Fingerprint Module (SM630)

The communication with the fingerprint module is made through (RXD0/PDI) PE0 port [2] and (TXD0/PDO) PE1 port [3] via UART0 of ATmega128. A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. [14]. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching as shown in Figure 2[2].

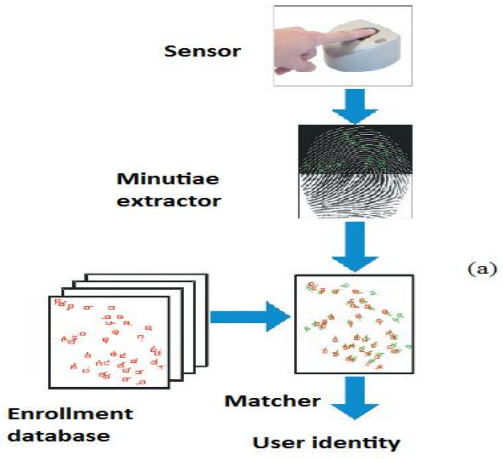

Figure 2: A typical automated fingerprint recognition system,

Evolutionary standalone fingerprint recognition module SM630 is ideal for on-line applications because it allows ASCII commands to manage the device from the host. On-line functionality, can verify fingerprints and them store on non-volatile memory. The most important module of the system is the fingerprint scanner. The SM630 by Miaxis was used. It consists of optical fingerprint sensor, high performance DSP processor and flash. It boasts of functions such as fingerprint login, fingerprint deletion, fingerprint verification, fingerprint upload, fingerprint download etc. [8]

The SM630 has the following unique features hence was used to actualize this project:

- High Adaptation to Fingerprints: When reading fingerprint images, it has self-adaptive parameter adjustment mechanism, which improves imaging quality for both dry and wet fingers. It can be applied to a wider public.
- Algorithm with Excellent Performance: SM630 module algorithm is specially designed according to the image generation theory of the optical fingerprint collection device. It has excellent correction & tolerance to deformed and poor-quality fingerprint.
- Easy to Use and Expand and Low Power Consumption: operational current <80mA.
- Integrated Design: Fingerprint processing components and fingerprint collection components are integrated in the same module. The size is small and there are only 4 cables connecting with HOST, much easier for installation. The operating Voltage: 4.3V～6V, Operating Current : <80mA（Input voltage 5V）,Power-on Time : <200ms（Time lapse between module power-on to module ready to receive instructions, Tolerated Angle Offset : ±45°, User Flash Memory : 64Kbyte, Interface Protocol: Standard serial interface （TTL level, Communication Baud Rate: 57600bps Operating Environment: Temperature: -10℃～+40℃ and Relative humidity: 40％RH～85％RH（no dew).

3.3. GSM MODULE

Global System for Mobile Communications (GSM) is the most popular standard for mobile phones in the world. GSM has over two billion users worldwide and is available in over 213 countries and GSM represents 82.4% of all global mobile connections. GSM uses a variation of Time Division Multiple Access(TDMA) and GSM is the most widely used of the three digital wireless telephone technologies (TDMA, GSM, and CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1800 MHz frequency band[4].

The GSM module used in implementing this system is Sony Ericsson K700i; IC4170B-A1021041. K700i GSM engines operate in the GSM 900 MHz, 1800MHz and 1900MHz frequency bands. As shown in Figure 3 , we do not replace the PIN verification. If PIN is correctly entered, system will capture it and match fingerprint of the customer . But if fingerprint does not match, due to any challenge with the fingerprint reader or the customer finger, the system will give the customer opportunity to enter his sceret code. If this is correctly entered, a Quick code (Q-code) is generated by the system and it is sent to the customer mobile phone.When the Q-code of the user is correctly entered the customer will be able to carry out banking transactions otherwise the customer account is block upon three unsucessful attempts. The security provided by this system is foolproof.

3.4. User Interface

The user interface includes the input and output devices and this makes communication with the system easier. An Alphanumeric LCD Display was used with the following features: 4-bit mode – 4-bit (nibble) data transfer and does not use DB0-DB3 – Each byte transfer is done in two steps: high order nibble, then low order nibble, interface requires only 7 I/O pins of microcontroller (DD4-DB7, RS, R/W and E). It is a 20 by 4 character-only LCD display with four character line and 20 characters per line.The matrix keypad consists of several buttons which are arranged in a matrix array for 4x4 keys and interfaced with

ATmega120 through GPIO of PC0 (A8) port through PC7 (A15) port. [3]

3.5. Power Supply

This section supplies power to all the sections mentioned above. It basically consists of a transformer to step down the 220V ac to 15V ac followed by a diodes bridge-rectifier. After rectification process, the obtained rippled dc is filtered using a capacitor filter of C=1000μF. A positive voltage of 3.5V and 5V are made available through LM317T and LM7805 to various on board components.

4.0. Software Design

The embedded platform discussed aboved is programmed in language C with AVR studio to follow the program logic as shown in Figure 3.

Using AVR Studio For C Programming.

AVR Studio is a large piece of software, it supports several of the phases required when programming the ATmega128 microcontroller. AVR Studio is an Integrated Development Environment (IDE) for writing and debugging AVR applications in Windows 9x/ME/NT/2000/XP/VISTA /WIN 7 environments. AVR Studio provideded us with a project management tool, source file editor, simulator,assembler and front-end for C/C++, programming, emulation and on-chip debugging. AVR Studio supports the design, development, debugging and verification aspects of the system.
In programming the ATmega128 microcontroller, four major stages were involved:

- *Create an Atmel Studio project,*
- *Compile C code to produce a HEX file,*
- *Debugge C program using the simulator,*
- *Download HEX file to the STK500 development board and running it.[12]*

4.1. Embedded Language C

The AVR Studio 4 platform put forward the options for assembly language and high level language programming. C language being the most convenient language to access different port pins of ATmega128, we programmed the algorithm to control the SM630 fingerprint module through host controller ATmega128 in C language. The program follows the control actions as shown in Figure 3. The program segments to access UART, LCD, RTC, ADC, DAC, are included by linking through UART0.h, LCD.h, RTC.h, ADC.h, DAC.h header files respectively.

5.0 Design Process of the Fingerprint ATM System.

The construction started with the circuit design and this was accomplished with the labcenter Proteus software. Circuit was drawn and double checked, however in order to simulate the performance of the circuit, the software for the atmega128 controller has to be developed first. The design environment was therefore switched over to Atmel AVR-Studio. The AVR-Studio is a software development and debugging environment for the Atmel AVR microcontroller family, to which the atmega128 belongs.

The Atmel AVR-Studio however relies on AVR-GCC compiler for its code compilation. Codes were then developed and compiled in the studio. After successful compilation, codes were then imported into Proteus for simulation. Debugging the code henceforth, involves switching back and forth between AVR-Studio to edit the code and Proteus to simulate it.

On completion of the simulation, the PCB design was done using the Proteus Ares package. The Ares autoplacer and autorouter was used to design the PCB. After routing the PCB, the fabrication was then done using the toner heat transfer method and followed by etching in a solution of hydrochloric acid. After etching, the board was drilled and components mounted appropriately.

6.0. Operational Principle of the Designed System.

As shown in Figure 3, researcher do not replace the PIN verification. If PIN is correctly entered, system will capture it and match fingerprint of the customer. But if fingerprint does not match, due to any errors with the fingerprint reader or the customer finger, the system will give the customer opportunity to enter his sceret code. If this is correctly entered, a Quick code (Q-code) is generated by the system and it is sent to the customer mobile phone. When the Q-code of the user is correctly entered, customer can carry out banking transactions otherwise, the customer account is block upon three unsucessful attempts. The security provided by this system is foolproof.

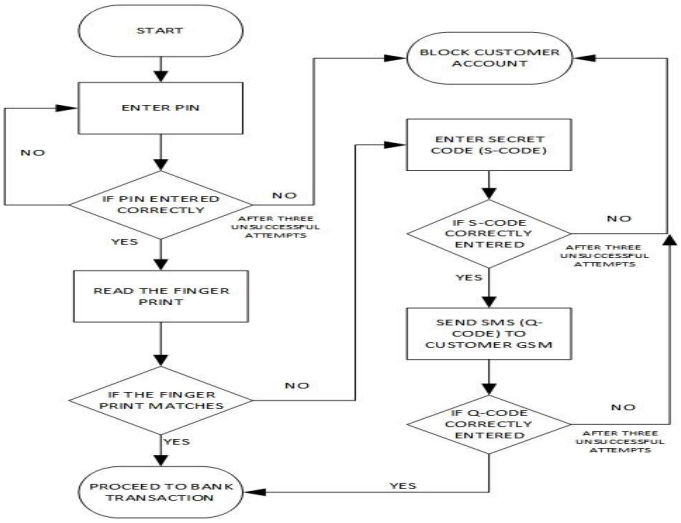

Figure 3: Software designed and flow chart of the designed system.

7.0 Testing Of The Biometric Atm System.

The testing of the designed system was carried out in an academic environment and with the following sample of customers database in Table 1.0 was created by the system. The system is capable of generating and assigning account to the newly registered customer on suppling following customer detail via the system administrator menu in this format. For example:

Name= Mike Joseph
Contact=8253325661
Pin=5201
Balance=7000
Secret=2211

On receiving this customer information by the system, the system is programmed to automatically generate an account number for the customer information and then sent forth a text message to the customer's registered mobile phone (e.g 8253325661) in this format type:

KKK bank alert
Account name: Mike Joseph
Account number:1234620062
Balance:N7,000.00K

On receiving this information, the customer goes to the bank and input the account information on the biometric ATM, and also register his right thumb with the account. This is verified by the bank officer. This completes the registration process of the new customer using the designed Enhenced Biomteric ATM with GSM feedback Mechanism. The information from one thousand (1000) different customers were processed and subjected to testing as sample shown in Table 1.0.

Table 1.0: Sample of Customer database generated by the designed system

S/N	ACCOUNT NAMES	ACCOUNT NO.	REGD. GSM NO.	DATE CREATED	PIN	OPENING BALANCE	S-CODE
1	Mike Joseph	1234200620	8253325661	4/1/2016	5201	N7,000.00K	2211
2	Osato Osaro	1234620062	8123446844	7/1/2016	7342	N4,000.00K	2012
3	Babatude Ola	1234000620	8765432309	7/1/2016	8974	N8,000.00K	1987
4	Obinna Stone	1234000240	8675849302	18/1/2016	1537	N2,000.00K	1642
5	Fred Oba	1234620006	8908765432	21/1/2016	9999	N9,000.00K	1773
6	Abbas clement	1234620064	8432567189	3/2/2016	2387	N3,000.00k	3879
…	…	…	…	…	…	…	…
1000	Oluwa Light	1234000622	8876994321	9/1/2015	2496	N5,000.00K	4382

3.0. RESULT PRESENTATION AND ANALYSIS.

Fingerprint identification system performance is measured in terms of the following parameters and were used to analyze the result of the designed biomteric ATM system [10][11].

A. False Rejection Rate (FRR): The probability that a system will fail to identify an enrollee. It is also called type 1 error rate. This is as well known as false nonmatch rate (FNMR).

FRR = NFR÷NEIA = 0 ÷ 1000 = 0

NFR = number of false rejection rates = 0
NEIA = number of enrollee identification attempt = 1000

B. False Acceptance Rate (FAR): The probability that a system will incorrectly identify an individual or will fail to reject an imposter. It is also called as type 2 error rate. This is as well known as false match rate (FMR).

FAR = NFA÷NIIA = 0 ÷ 550 = 0

NFA = number of false acceptance = 0
NIIA = number of imposter identification attempts = 550

C. Response Time (RT): The time period required by a biometric system to return a decision on identification of a sample. The average response time of the designed system is 1.5 seconds.

D. Decision Threshold (DT): The acceptance or rejection of a data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that

the system can be made more or less strict depending on the requirements of any given application. The decision global threshold used in this project is 30

E. Enrollment Time (ET):The time period a person must spend to have his/her fingerprint reference template successfully created. The enrollment time of the designed system is one second.

F. False positive identification rate (FPIR): This occurs when the system finds a hit for a query fingerprint that is not enrolled in the system.

$$\mathbf{FPIR = 1 - (1 - FMR)^N}$$

$$\mathbf{FPIR = 1- (1- 0)^{1000} = 1- (1)^{1000} = 1- 1 = 0}$$

G. False negative identification rate (FNIR): occurs when it finds no hit or a wrong hit for a query fingerprint enrolled in the system. The relationship between these rates is defined by

$$\mathbf{FNIR = 1- (1 - FNMR)^N}$$

$$\mathbf{FNIR = 1- (1-0)^{1000} = 1- (1)^{1000}= 1-1 = 0}$$

where N is the number of users enrolled in the system = 1000.

Where FMR = FNMR = 0 from system testing.

H. Average time of transaction using the designed system, (Normal process time): 50 Seconds.

I. Average time of transaction which using the feedback GSM mechanism.(Q-code and S-code): 2 minutes.

Some other senarios that were experienced in the designed system, for example in the case of using wrong fingerprint thrice for four of the above customers, Q-code were generated and sent to the customers' GSM phone numbers with which they were able to gain access into their accounts only after they have supplied the correct secrete code (S-Code) numbers.

8.0. CONCLUSION

An enhanced biometric ATM with GSM feedback mechanism has been designed, constructed and tested. The proposed system has overcome the limitations that exists in other methods and provides a secured and safe environment that saves the hard earned money of the user. The system has proved to be 95.79% successful from our analysis. The designed system provides an alternative method for verification if the fingerprint operation has a challenge which is via a mobile phone upon correct entering of the customer S-code. The designed system is capable of eliminating ATM fraud.

REFERENCES

(1) Agbontaen F.O. & Orukpe P. E. "Secured Online Payment using Biometric Identification System". (2013) Advanced Materials Research,Trans Tech Publications, Switzerland Vol. 824 (2013) pp 193-199

(2) Anil K. J., Jianjiang F., Abhishek N. & Karthik N.,(2008) "On Matching Latent Fingerprints," *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, pp.1-8, 2008.

(3) Atmel Microcontroller with 128KBytes In-System Programmable Flash technical maunal © (2011) Atmel corporation, 2467XS–AVR–06/11.

(4) http://www.tech-faq.com/gsm.shtml

(5) Ibidapo, O. Akinyemi, Zaccheous O. Omogbadegun, and Olufemi M. Oyelami (2010)"Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria EBanking System". International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 10 No: 06

(6) Khatmode R. P., Kulkarni R.V., Ghodke B. S. Chitte P. P., Anap S. D. (2014) "ARM7 Based Smart ATM Access & Security System Using Fingerprint Recognition & GSM Technology".International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 2, February 2014, pages 856-860.

(7) Mashurano J. & Wang I. (2013) "ATM Systems Authentication Based On Fingerprint Using ARM Cortex-M3". International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 2 Issue 3, March – 2013, pages 1-6.

(8) Miaxis Biometrics Co., Ltd. SM630 Fingerprint Verification Module User Manual 2008-07-01 V1.0.

(9) NIBSS 2015 www.nibss-plc.com.ng accessed 23.12.2015

(10) Pennam K. & Maddhusudhan M.R., (2012) "Implementation of ATM Security by Using Fingerprint recognition and GSM" International Journal of Electronics Communication and Computer Engineering, Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X, pages 83-86.

(11) Pravinthraja S. and Umamaheswari K., (2011) "Multimodal Biometrics for Improving Automatic Teller Machine Security". Bonfring International Journal of Advances in Image Processing, Vol. 1, Special Issue, December 2011, pages 19-25.

(12) Research data on e-fraud in Nigeria by the Financial Institutions Training Centre (FITC), 2014

(13) Ronald J. T., Neal S. W., Gregory L. M., (2009) "Digital Systems: Principles and Applications, 10th Edition", ISBN: 0131725793, published by Pearson Education, Inc.

(14) Vaibhav R. Pandit, Kirti A. Joshi & Narendra G. Bawane (2013) "ATM Terminal Security using Fingerprint Recognition". International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868, pages 14-18.