

Development of Microcontroller-Based Biometric Locker System with Short Message Service

Crystalynne D. Cortez, Jaswinder S. Badwal, Jocelyn R. Hipolito, Ditche Jane C. Astillero, Melvie S. Dela Cruz, and Jaira C. Inalao

Abstract—The study was a development of a microcontroller based biometric locker system with short message system (SMS) which ensures the security of personal and confidential belongings of a person. Developmental research method which was comprised of hardware development and software development were utilized in the study. The system was able to scan finger, match it with the saved pattern and unlock the locker. Global system for mobile (GSM) module was able to send text message containing the auto-generated passcode of the locker when an unrecognized fingerprint was encountered. As a result, all the hardware components functioned normally and efficiently. The program uploaded to the system run consistently as the device performed its functions.

Index Terms—Biometric locker, SMS technology, microcontroller project, biometric system.

I. INTRODUCTION

Theft is one of the major problems in schools and offices. To minimize these incidents, different ways to secure belongings and documents were done. Most universities and offices use lockers and cabinets for storing files, securing belongings and keeping of important documents for privacy and security purposes. However, some lockers used ordinary padlocks and were shared by two or more users. Common lockers do not guarantee full safety and security of property because ordinary padlocks can be opened by force.

Biometric is considered as one of the most effective method when it comes to security. Biometric is an automated technique of recognizing a person based on his physical attributes which includes face, fingerprint, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric data are considered as different and distinct from personal information because it cannot be reverse-engineered to recreate any personal information and cannot be stolen to attempt theft [1].

Fingerprints are the most common biometric technology used in many applications. The fingerprints recognition and matching is one of the simplest ways of verifying a person's identity. It requires the imaging and comparison of the print

pattern which includes the ridges and minutia points. These patterns are unique to every individual [2].

Several studies using fingerprint biometric recognition were conducted to improve locker systems. One among them was the study of Lay, Yang and Tsai (2011) entitled "Biometric Locker System" wherein fingerprint recognition technique was used to open and close the lock of a storage locker system. The system first captured the fingerprint of the locker renter and matched the fingerprint to reopen the locker door. This was done to reduce troubles about keys and to ensure the security of the renter [3].

Similarly the study conducted by Gangi and Gollapudi (2013) entitled "Locker Opening and Closing System Using RFID, Fingerprint, Password and GSM," had designed and implemented a locker security system based on the integration of radio frequency identification (RFID), fingerprint, password and global system for mobile (GSM) technologies that can activate, authenticate, and validate the user to unlock the door for secure access. In this system, the RFID reader reads the ID number first and determines if it is valid. If the id number is valid, that is the time that the system gives access to the fingerprint scanner. Then it will scan the fingerprint, and if matched, the microcontroller sends the password to the authenticated person mobile number. The person then has to enter the passwords to the system [2].

Another study entitled "Fingerprint Based Bank Locker System Using Microcontroller" which was conducted Pavithra, Myna and Kavyashree, designed and implemented a fingerprint based bank locker system using microcontroller that provide a perfect security to the bank lockers and to make the work easier [4].

Although there were existing studies about biometric lockers, the study aimed to develop an improved prototype. After the third attempt, the system will send a notification short message service (SMS) to the owner when an unrecognized fingerprint was detected by the biometric sensor, as innovation to the study. The SMS contains the auto-generated passcode which will be used to unlock the locker. To enter the passcode, the system included a built-in keypad in the design. These were done to increase safety of the stored belongings in the locker.

II. OBJECTIVES OF THE STUDY

The study aimed to develop a prototype of a microcontroller-based locker system that can:

- 1) Enroll fingerprints of the thumb and index fingers, and saves these patterns in the system.
- 2) Unlock the locker using fingerprint or auto-generated

Manuscript received September 20, 2014; revised December 29, 2014.

C. D. Cortez is with the Computer Education Department of Centro Escolar University, Mendiola, Manila, Philippines (e-mail: crystalynnecortez2179@gmail.com).

J. S. Badwal, J. R. Hipolito, D. C. Astillero, and M. S. Dela Cruz were with Computer Engineering in Centro Escolar University, Mendiola, Manila, Philippines (e-mail: badwal1525@gmail.com, jocelynhipolito@gmail.com, ditchejane@gmail.com, melvie.delacruz@gmail.com).

J. C. Inalao was with Computer Engineering in Centro Escolar University, Mendiola, Manila, Philippines. She is now with Ocwen Financial Corporation, Manila, Philippines (e-mail: jairainalao@gmail.com).

passcode.

- 3) Send text message of the passcode when an unrecognized fingerprint is encountered during the third attempt.

III. MATERIALS AND METHODS

Developmental method was used in this study that involved the systematized use of the concepts of an existing device to develop a new system. Prototyping technique was also used to assemble a working model of the system. The study involved hardware development wherein the system was created using components available in the market; and software development wherein programs were created using available programming language for the microcontroller unit.

Fig. 1 shows the block diagram of the biometric locker system. A 9-12V_{dc} was used to supply power to the system. The microcontroller ATMEGA 644 housed in Arduino board was utilized to interface the input and output hardware devices. Input devices include the fingerprint sensor for biometric recognition, keypad was for the encoding of passcode and real time clock for display of current date and time. The output devices include GSM module for sending of SMS that contains the passcode, solenoid lock and 2 × 16 LCD for display of the locker's operations. The microcontroller was programmed using Arduino Integrated Development Environment (IDE).

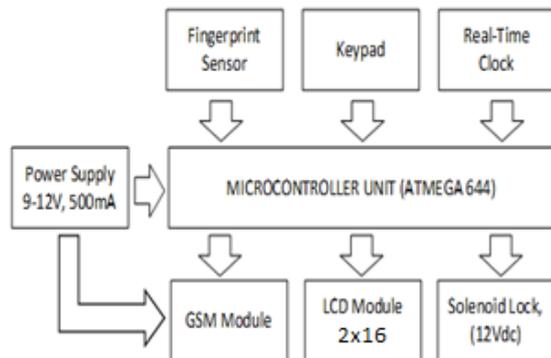


Fig. 1. Block diagram of the biometric locker system with SMS.

ATmega644 housed in Arduino board, was the microcontroller unit used in the system. It controlled the functions of the biometric locker system. The ATmega644 is a 40 pins, low-power complementary metal oxide semiconductor (CMOS), 8-bit microcontroller based on the AVR enhanced reduced instruction set computer (RISC) architecture. ATmega644 can achieve throughputs approaching 1 million instructions per second per MHz through the execution of powerful instructions in a single clock cycle. This allowed the optimization of power consumption versus processing speed in system designs [5]. It can store up to 64 kbytes of program instructions. The Arduino board of the ATmega644 was compatible to other input and output hardware devices used in the biometric locker system.

Fingerprint scanner or fingerprint reader is used to detect the user's identification. It is an electronic device used to live-scan digital images. This inkless process is acquired by directly sensing the finger surface. The general procedure of a fingerprint scanner is that a sensor reads the ridge pattern on

the finger surface and converts the analog reading into digital codes using an analog to digital converter. An interface module like microcontroller is responsible for communicating with external devices [6].

Fingerprint recognition is the main function of a scanner wherein it comprised of two stages, enrollment and verification. During enrollment, fingerprints are scanned, analyzed and matched, then stored in a coded form. Once the fingerprint is enrolled, verification takes place wherein the user will check if the fingerprint matched the saved patterns. These patterns were analyzed using minutiae where the lines of the fingerprint are terminated into two. The distance and angles of the minutiae are used as algorithm in turning the information with unique numeric code [7].

Keypad is used to input the passcode of the locker. A 12 key-keypad is arranged in a 3 × 4 format requiring seven connections and usually arranged in a matrix format to reduce the number of input/output (I/O) connections [8].

GSM module is incorporated in the design to enable the system send notification message to the locker user. Cheap GSM module known as SIMCOM900D was embedded to the system.

IV. RESULTS AND DISCUSSION

A. Fingerprint Enrollment

Fingerprint enrollment and recognitions were conducted to ensure that the biometric sensor was properly interfaced to the microcontroller unit. For security purposes, enrollment of fingerprints was done using a third party software. The patterns of the index and thumb fingers were saved in the system to be used for unlocking the locker. The system successfully enrolled the fingerprints of the user as shown in Fig. 2.

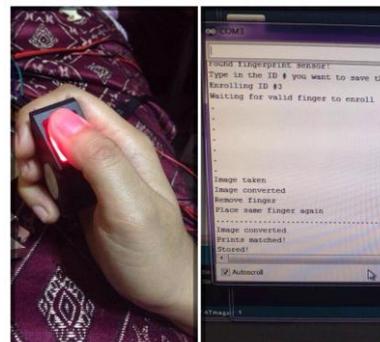


Fig. 2. Fingerprint enrollment.



Fig. 3. Initialization of the system.

After enrollment the system was ready to be used. During start-up, the microcontroller initially checked the connections of the real-time clock, GSM module and fingerprint sensor. Fig. 3 shows that the system successfully initialized the hardware devices connected to it. "Found sensor" message displayed to the 2 × 16 LCD monitor indicated that the locker was on its ready state.

After initialization or if the locker is idle, the system displayed the current date and time. Fig. 4 shows this operation. Current date and time fetched from the real time clock was displayed in the 2 × 116 LCD.



Fig. 4. Idle operation of the locker.

B. Fingerprint Recognition

If the locker will be used by the user, he needed to scan his fingerprint, either the thumb or index finger. The fingerprint of the user should match the pre-enrolled fingerprints. Fig. 5 shows that the system was able to detect the enrolled fingerprint of the user. The ID number of the fingerprint was displayed and the locker was unlocked or opened.



Fig. 5. Found fingerprint ID displayed on LCD.

C. Passcode Generation

Passcode was generated once the system encountered the third attempt of an unrecognized fingerprint. The microcontroller unit will immediate trigger the GSM module to send the passcode to the pre-enrolled mobile number of the user. Fig. 6 shows the attempts to unlock the locker. If the fingerprint was not recognized, error message "ID NOT FOUND! Try Again!" was displayed in the LCD. On the third attempt, "INVALID" error message was displayed. GSM module was triggered by the microcontroller unit to send text message to the mobile number of the user.

After the third attempt of unmatched fingerprint, the system

automatically sent the passcode via a text message to the owner. The message should was sent to and received by the mobile number as shown in Fig. 7.

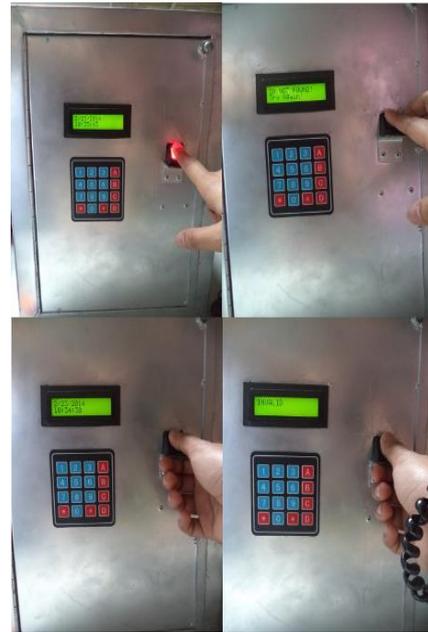


Fig. 6. System failed to recognize the fingerprint.

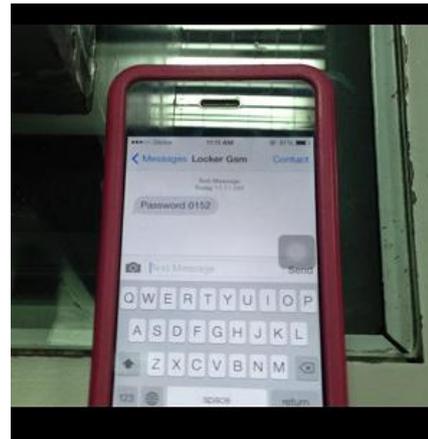


Fig. 7. Passcode sent to the programmed mobile number of the user.

D. Passcode Recognition

The received passcode was entered to the system as shown in Fig. 8. To denote that the entered passcode matched the system's generated passcode, LCD displayed "Door Unlocked!" The code was accepted and the locker had been unlocked.

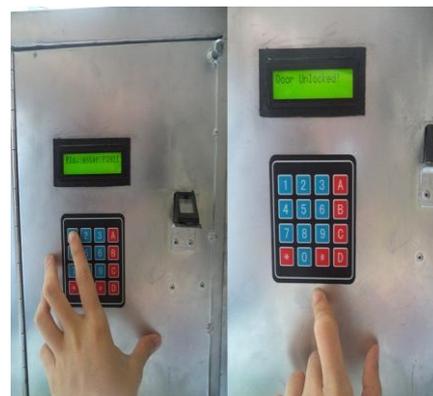


Fig. 7. Entering of auto-passcode to the locker.

V. CONCLUSION

Based from results of the developed biometric locker system, the programs uploaded to the microcontroller successfully facilitated its operations. The components used for the system were compatible with the microcontroller unit. It had executed the following functions effectively:

- 1) Proper enrollment, saving and scanning of the thumb and index fingerprints of the user;
- 2) Correct fingerprint and passcode recognition and detection to open the solenoid lock of the locker.
- 3) Proper establishment of the connection between the microcontroller unit and GSM module enabling the sending of text message for the auto-generated passcode to the user, when an unrecognized fingerprint was detected. The system had accepted the auto-passcode entered to the system.

ACKNOWLEDGMENT

The researchers would like to acknowledge the support of Computer Education Department and Research and Evaluation Office of Centro Escolar University, Manila.

REFERENCES

- [1] (2013). What is biometric? *Easy Clocking*. [Online]. Available: http://www.bioelectronix.com/what_is_biometrics.html
- [2] R. R. Gangi and S. S. Gollapudi, "Locker opening and closing system using RFID, fingerprint, password and GSM," *International Journal of Emerging Trends & Technology in Computer Science*, vol. 2, issue 2, March-April 2013.
- [3] Y. L. Lay, H. J. Yang, and C. H. Tsai, "Biometric locker system," in *Proc. the World Congress on Engineering and Computer Science*, vol. 1, San Francisco, USA, October 2011.
- [4] B. C. Pavithra, B. C. Myna, and E. M. Kavyashre, "Fingerprint based bank locker system using microcontroller," in *Proc. IRF International Conference*, Pondicherry, India, April 5, 2014, pp. 155-160.
- [5] *Atmel Corporation*, ATmega644 datasheet.
- [6] D. Matoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, 2nd ed., London: Springer Verlag London Limited, 2009, ch. 2, pp. 57-58.
- [7] C. Woodford. (June 3, 2014). Biometric fingerprint scanners. *Explain That Stuff*. [Online]. Available: <http://www.explainthatstuff.com/fingerprintsensors.html>.
- [8] A. O. Oke, A. A. Adigun, A. S. Falohun, and F. O. Alamu, "Development of a programmable electronic digital code lock system," *International Journal of Computer and Information Technology*, vol. 2, issue 1, pp. 127-131, January 2013.



Crystalynne D. Cortez was born on September 10, 1985. She obtained her master of science in electrical engineering in Technological University of the Philippines in April, 2014. She graduated the bachelor of science in electronics and communications engineering at University of the City of Manila in April, 2006.

She is a full-time faculty member of Computer Education Department of Centro Escolar University (CEU), Manila, Philippines from 2009 until present, handling professional and research subjects in computer engineering, computer science and

information technology courses. She, together with her colleagues had won 2nd place in poster presentation for the paper, "Development of microcontroller-based biometric locker system" during CEU Search for the Best Undergraduate Research 2014. Her recent paper publication is entitled "Validation of the developed multi-gas monitoring system," *Periodical on Applied Mechanics and Materials*, vol. 666, pp. 245-250, October 2014. Her major field of researches falls with microcontroller projects, environmental engineering and biosensors.

Engr. Cortez is a member of IACSIT since May, 2014.



Jaswinder S. Badwal was born on October 25, 1993. He obtained his bachelor of science in computer engineering in Centro Escolar University in April, 2014.

He had been a finalist for CEU Search for the Best Undergraduate Research 2014 and won 2nd place in poster presentation for the paper, "Development of microcontroller-based biometric locker system." His major field of research interest falls with microcontroller projects.



Jocelyn R. Hipolito was born on November 1, 1992. She obtained her bachelor of science in computer engineering in Centro Escolar University in April, 2014.

She had been a finalist for CEU Search for the Best Undergraduate Research 2014 and won 2nd place in poster presentation for the paper, "Development of microcontroller-based biometric locker system." Her major field of research interest falls with microcontroller projects.



Ditch Jane C. Astillero was born on February 10, 1993. She obtained her bachelor of science in computer engineering in Centro Escolar University in April, 2014.

She had been a finalist for CEU Search for the Best Undergraduate Research 2014 and won 2nd place in poster presentation for the paper, "Development of microcontroller-based biometric locker system." Her major field of research interest falls with microcontroller projects.



Melvie S. Dela Cruz was born on February 20, 1993. She obtained her bachelor of science in computer engineering in Centro Escolar University in April, 2014.

She had been a finalist for CEU Search for the Best Undergraduate Research 2014 and won 2nd place in poster presentation for the paper, "Development of microcontroller-based biometric locker system." Her major field of research interest falls with microcontroller projects.



Jaira C. Inalao was born on May 30, 1993. She obtained her bachelor of science in computer engineering in Centro Escolar University in April, 2014.

She had been a finalist for CEU Search for the Best Undergraduate Research 2014 and won 2nd place in poster presentation for the paper, "Development of microcontroller-based biometric locker system." Her major field of research interest falls with microcontroller projects.