Packaging of a Fingerprint Based Access Control System

Dr. Zdenka J. Delalic, Ph.D.[1], Sandeepsarma Josyula[1] and Anand.B
[1]College of Engineering, Temple University, Philadelphia PA 19121 USA

Abstract

Verification for access control is faster and cheaper than identification based access control systems. The aim of this project was to develop a fingerprint based access control system, where the verification or validation of the entry is based upon the data from a RFID card. The multi-hop unit is controlled by a PIC 18F series, RISC processor. The capacitive sensor employed extracts 40 minutiae points, which are verified based on the pre-stored data in the RFID card. The capacitive sensor is capable of detecting human tissue, eliminating brute-force or latent print attacks. The low power RFID reader makes the unit portable. The use of RFID cards and verification mechanisms eliminate the use of a centralized database to store the data of every valid entry. The Infineon RFID card has an operating distance of 5mm, as opposed to 0.5mm normally used in swipe based RFID systems, making it easier to use. The packaged fabricated unit was successfully designed to program new RFID cards with minutiae data obtained from the capacitive sensor. Additional features of the unit include blacklisting entries and emergency exit.

***Index Terms*—Biometrics, RFID, Access control system.**

I. INTRODUCTION

THE aim of the project was to develop an embedded gadget that could provide a foolproof solution for access control biometrics. The developed gadget uses fingerprints as a mode of identification. Every fingerprint is identified based upon the minutia points extracted using the biometric sensor. Each minutia point is recorded as a polar co-ordinate, and this data is used to cross check, while granting or denying access. So, a centralized database had to be maintained. The centralized database is vulnerable to software leaks and brute force attack. To make the unit function autonomously, the data corresponding to the minutia points is stored in a smart card. With the data being stored in the smart card, the necessity of maintaining a centralized database is eliminated. This makes the unit, very reliable and easy to install. However, eliminating the database comes with the cost of more hardware and memory in the developed gadget to extract and compare the minutia points. One more trading factor is the number of blacklisted entries. The entire unit is controlled by the PIC 18F8720 micro-controller.

The second part of this paper illustrates the principle behind extracting the minutiae points. Also, the memory organization in which the data is stored is also explained. Further other parts of the block diagram are briefly introduced.

The third part of the paper illustrates the functional flowchart of enrollment and verification stages.

The fourth part of the paper illustrates the PCB layouts generated for packaging of the embedded gadget.
Future scope and references are included at the end.

II. BLOCK DIAGRAM

The following block diagram, gives a comprehensive view of all the components in the developed access control system.

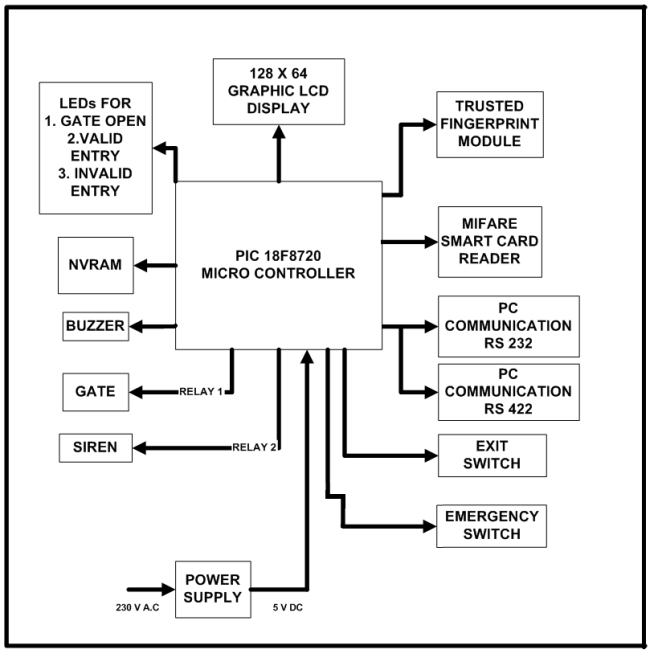

Figure 1. Block Diagram

The trusted finger-pint module is a capacitive sensor and analyzes fingerprints based on image discontinuity principle.

"According to the principle of image discontinuity if two neighboring pixels are of not of the same grey level then they are said to be discontinuous."

The following figure shows how the fingerprint minutia points are extracted based on the image discontinuity principle. The capacitive sensor records a polar coordinate at every point of discontinuity and a set of those polar coordinates are used for verification.

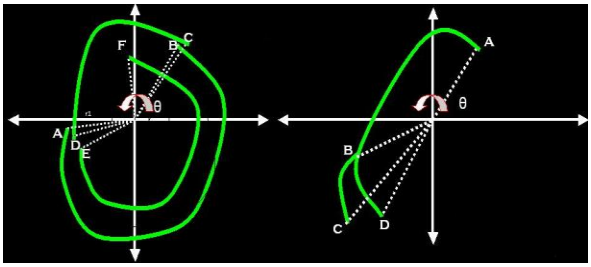

Figure 2. The polar coordinates are formed, where the pattern of the fingerprint is discontinuous. Also, indicated is the case where, the pattern of the fingerprint splits. The point where it splits is also recorded as a polar coordinate.

Capacitive scanners have an edge over conventional retro-reflective capacitive scanners as the capacitive scanner detects the presence of live finger over the sensor. Implementing the capacitive sensor eliminates the possibility of trespassing using latent prints. The onboard capacitive sensor is powered by a 8 bit processor and has a capture rate of 15 frames per second. After the finger is scanned, a negative of the grayscale image of the finger is generated. The capacitive scanner then reduces the width of the patterns to one pixel and then extracts the fingerprints based on the principle of image discontinuity.

The Mifare smart card reader is a high-speed contactless smartcard reader and can read or write data into smartcards. The smart cards employed must store preliminary information along with the minutia point data in them. So, the infinion smartcards are employed, that can store upto 1 KB information. The memory organization of the smart card is shown in Fig. 3

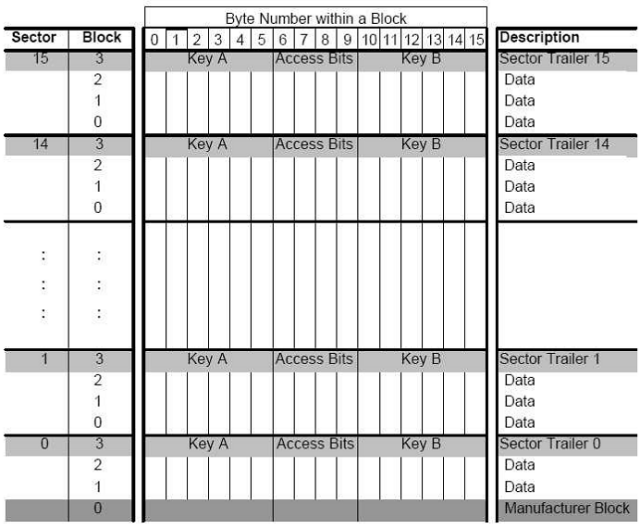

Figure.3 Memory organization of the smart card.

The 1024x8 bit EEPROM memory is organized in 16 sectors with 4 blocks of 16 bytes each. All sectors contain 3 blocks of 16 bytes for storing data. The sector trailer block contains the serial number and the checkbyte info to communicate with the smart card reader.

The entire gadget is interfaced with RS232 port to communicate with the processor. It is used to update the black list entries. RS422 communication port can relay smart card info to a secondary backup space.

Exit switch when activated, will bypass the biometric and smartcard check and will grant access. The emergency switch when activated will leave the electro-magnet lock open, till the emergency is cleared. The buzzer corresponds to the exit switch and the siren corresponds to the emergency switch.

The NVRAM stores startup sequence information corresponding to the PIC microprocessor. The NVRAM also stores, blacklist entries, which are updated using the RS232 port.

III. FUNCTIONAL FLOWCHARTS

The operation of the embedded gadget is divided into two stages, enrollment and verification. When a new user has to be added into the system, the fingerprint module extracts the fingerprint minutiae and transfers it to the smartcard. However the smartcard must be present at least 100mm away from the smartcard reader to communicate.

During the enrollment stage, the fingerprint module extracts polar coordinates based on the finger position. So, for the polar coordinates to match, positioning the finger is critical. Figure 4 shows the GUI callbacks that get displayed on the LCD screen, when the finger is not positioned properly. Generally the thumb is chosen as the reference finger. The thumb finger is made up of less bone structures than other fingers and so, the alignment is similar in most of the cases.

The following is a brief summary of how is the verification done to grant access.

Step 1: Initialize hardware i.e., LCD, Mifare Terminal, PC communication, RTC, NVRAM and I/O's.
Step 2: Call Self Test, If it is satisfied then close gate, ON LCD backlight, OFF siren and On all Red Led's. If it is not satisfied, then check and initialize again.
Step 3: LCD backlight is turned off after 3 sec's and the following messages are displayed on the LCD screen

"FINGER PRINT ACCESS"

This is the initialization of process CONTINUE
Step 4: Verify whether the function to be performed is "EXIT DEVICE" or "EMERGENCY SWITCH" or "EXIT SWITCH" and display

"PLEASE PLACE THE CARD ON THE TRAY"

Step 5: Check whether smart card is present. If yes, then check the application code. If the card is not present, then again. Perform step 4.
Step 6: If the application code is valid, then check client code else it gives a caller beep and verifies whether the card is present.
Step 7: If the card is present, then it displays

"PLEASE REMOVE THE CARD"

Step 8: If the card is absent then go to step 4.
Step 9: Check the client code. If it is valid, then check the key. If the client code is not valid then it displays "ON INVALID CLIENT CODE" and it calls an error beep. Then it goes to step 7. If the card is absent then it goes to CONTINUE.
Step 10: If the key is valid then check if the description is valid. If the key is invalid then it displays "INVALID CARD" and it calls an error beep. Then it goes to step 7. If the card is absent then it goes to CONTINUE.
Step 11: If the description is valid, then check if the black list is enabled. If it is disabled then it goes to CONTINUE.
Step 12: If blacklist is enabled, then it calls black list is verified. If the person is blacklisted, then it denies the access and it calls an error beep. Then it goes to step 7. If the card is absent then it goes to CONTINUE.
Step 13: If the user is not in the black list then it reads code number, name and display them on LCD.
Step 14: Read Finger Print data. If Finger Print reading is completed, then call short beep and display

"PLACE FINGER"
"RIGHT HAND THUMB"

Step 15: After GUI callbacks, check whether the capture was successful.
Step 16: After passing Finger Print buffer to TFM, check whether the match is successful. If yes, then generate Transaction record and store generated transaction in a temporary file location.
Step 17: If the match is not successful, then it displays "SORRY ACCESS DENIED" and calls and error beep and ON "NO GO" led.
Step 18: Displays "CONTACT SECURITY" and then it goes to step 7. If the card is absent then it goes to CONTINUE.
Step 19: After storing generated transaction in a temporary file location, send transaction to database then it displays ""MATCH SUCCESS" and then it calls a long beep along with switching on the "ON GO" led.
Step 20: Open the gate. After a certain time delay, close the gate and off the "ON GO" led.
Step 21: If card is present, then it displays
"PLEASE REMOVE THE CARD" and it calls an error beep.
Step 22: If card is absent, then check for the officer card.

If present – Go to enrollment stage
If absent – Go to CONTINUE

Based upon the organization of the smart card, it can be registered as an "Officer" card, that will activate enrollment mode to register other smartcards into the system.

The following is a brief summary of how is the verification done to grant access.

Step 23: calls beep and display "ENROLLMENT MODE ", display RED led bar and card flash led.
Step 24: Check the card validity.
If valid – send a request to P.C and if request is acknowledged check if
Command =officer ID. If it is not acknowledged, then again check the validity.
If it is not valid – call error beep, display "INVALID CARD", and then it goes to step 7. If the card is absent then it goes to CONTINUE.
Step 25:
If reading officer ID is completed. Send it to host PC.

EXECUTE Starts here
If COMMAND=READ FINGER, then send Finger Print Template.
If COMMAND=WRITE MIF, then Write into Mifare Card.
If COMMAND=WRITE_SEC, then write with security.
If officer card is present then go to EXECUTE
If officer card is absent then exit enrollment mode and it gives a long beep. OFF led's and exit to verification mode. And then go to CONTINUE

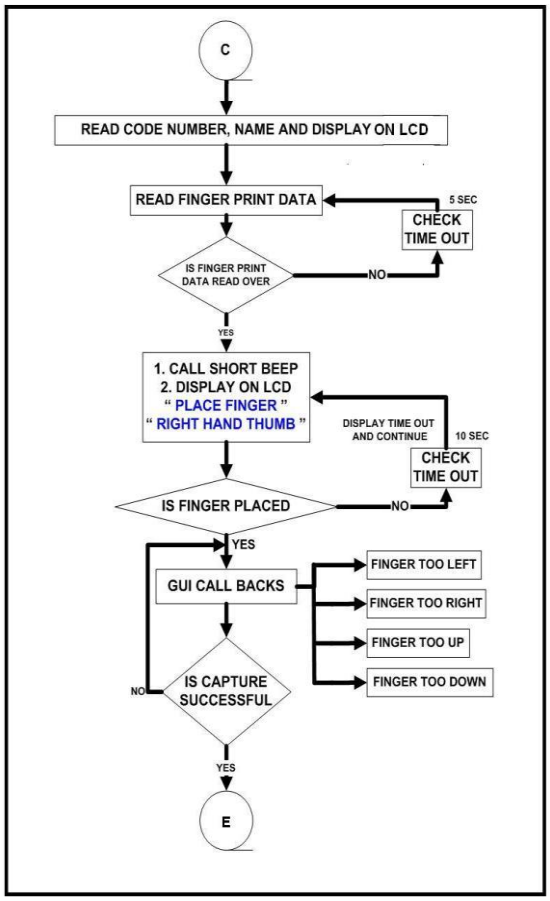

Figure 4. Callbacks displayed on the LCD screen

Figure 5 is the functional flowchart diagram of the enrollment mode, activated when the "Officer" card comes in contact with the card reader.

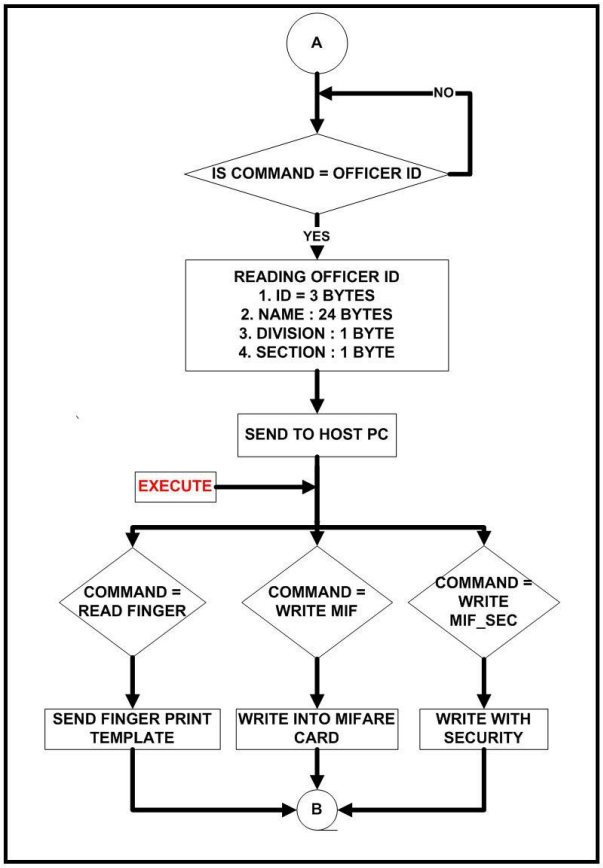

Figure 5. Enrollment Mode

IV. PCB LAYOUTS

The following are the PCB layouts generated for the packaging of the embedded gadget.

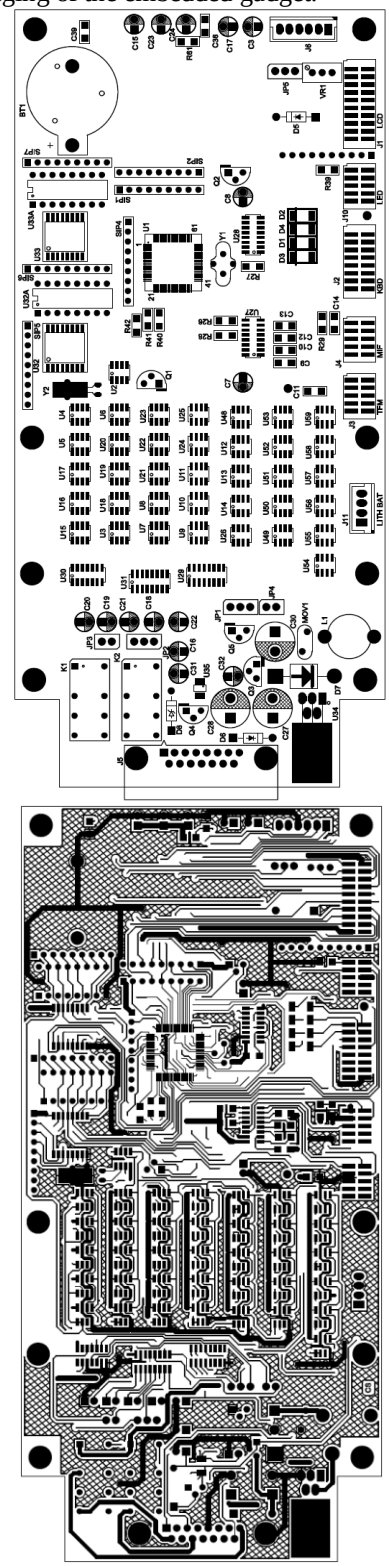

Figure 6. Component placement and interconnects

V. CONCLUSION

Due to the nature of the processor involved the limited memory within the processor and the NVRAM added to it, can support limited number of blacklist entries. The future scope of the project would be to include larger memories and a faster processor that can handle large amounts of data. Currently the number of minutia points cross checked are limited to the size of the smart card's memory. The system can be made more secure by using a smart card with larger memory. Also, with the help of larger memory, a combination of fingers can be used to authenticate, making it even more secure.

REFERENCES

[1] Proceedings of the IEEE, Vol. 94, No. 11, November 2006 - Special Issue on Biometrics : Algorithms and applications .

[2]. POSTNOTE From Parliamentary office of science and technology. BIOMETRICS AND SECURITY

[3] 1999 International Symposium on MicroMechatronics and human Science - A New ID Acquiring Method for Personal Identification system with Fingerprint - Center for Cooperative Research in Advanced Science and Technology, Nagoya University, Japan.

[4] A Secure Card System with Biometrics Capability, The Chinese University of Hongkong, Hongkong, China- Proceedings of The 1999 IEEE Canadian Conference on Electrical and Computer Engineering, Shaw Conference Center, Edmonton, Alberta, Canada.

[5]. BIOMETRICS SECURITY TECHNICAL IMPLEMENTATION GUIDE Version 1, Release 3, 11 October 2005 Developed by DISA for the DOD

[6] Biometrics and Digital Evidence, Chet Hosmer President & CEO WetStone Technologies, Inc. Bobbie Jo Countryman, Computer Forensic Specialist, WetStone Technologies, Inc.

[7] " Biometric Basics" Presented by Department of Defense BiometricsDoD Biometrics Management Office

[8] "Biometrics: separating reality from myth." By Allan Turner and Duane Blackburn MIT ,USA.

[9] Smart Cards for Access Control-Advantages and Technology Choices- HID solutions.

[10]. Issues for Liveness Detection in Biometrics Stephanie Schuckers, PhD, Larry Hornak, PhD ,Tim Norman, PhD- Lane Department of Computer Science and Electrical Engineering WEST VIRGINIA UNIVERSITY

[11]. Automated fingerprint identification systems- 2005 Computer world honors case study