International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 02
February 2017

Design and Development of Portable Security System Based on Fingerprint Identification

DONGARI SATISH
DEPARTMENT OF ECE
HOLYMARY INSTITUTE OF TECHNOLOGY AND SCIENCE

DR. K. V. MURALI MOHAN
PROFESSOR
DEPARTMENT OF ECE
HOLYMARY INSTITUTE OF TECHNOLOG AND SCIENCE

Abstract— Biometrics technology is rapidly progressing and offers attractive opportunities. In recent years, biometric authentication has grown in popularity as a means of personal identification in security systems. The prominent biometric methods that may be used for authentication include fingerprint, palm print, handprint, face recognition, speech recognition, dental and eye biometrics. In this paper, we done biometric verification by using a microcontroller based prototype of security access system using a fingerprint sensor module and we can control the loads by android APP. A 32-bit LPC2148 microcontroller developed by Microchip Technology is used in the system. The necessary software is written in Embedded 'C' and the system is tested.

KEYWORDS: Microcontroller, Fingerprint, Biometric, Recognition, Embedded system.

I. INTRODUCTION

The skin on our palms and fingers exhibits a flow like patterns of ridges and valleys. The papillary ridges on the finger, called friction ridges, which help the hand to grasp objects and increase friction and improve the tactile sensing of the surface structure. These ridge patterns are now scientifically proved as unique for each person. The cuts and burns in a person's finger may alter these patterns temporarily but they reappear after the injury heals. Fingerprints are now used widely for identification and verification purpose. They are used for attendance purpose in organizations to avoid proxy for criminal identification like terrorist, murderer and violators and also in passports (a matter of national high importance) of person.

Here in this project we have tried to automate a classroom attendance procedure by using a fingerprint recognition module interfaced with 8051 microcontroller [28]. A fingerprint recognition system can be used for both verification and identification. In verification, the system compares an input fingerprint to the "enrolled" fingerprint of a specific user to determine if they are from the same finger (1:1 match). In identification, the system compares an input fingerprint with the prints of all enrolled users in the database to determine if the person is already known under a duplicate or false identity (1:N match)[27][29].

This report also involves the product based design of a physical fingerprint system and also layout of fingerprint matching algorithm. It uses various concepts of embedded system and has tried to make the hardware a marketable portable

II.LITERATURE REVIEW

Various fingerprint matching systems have been proposed which emphasizes on minutiae information, local ridges [1]; some studies are based on singularity point's position, orientation [2], and relative distance detection, novel printing [2, 3, 4, 5] novel EESM-based fingerprint algorithm for indoor positioning [6].

Some consider efficient and low cost embedded platforms [7, 8, 9] for authentication whereas some focus on performance for large databases [10] and speed [11], to recognize a fingerprint. Other studies implement two-server [12] and multi-server [13] topology and cryptography fingerprint recognition systems. As mentioned in techniques such as DSP [14, 15, 16] and RF-card; field programmable gate array (FPGA) using neural networks [17]; keystroke dynamics [18]; FPC1011C sensor [19], Hidden Markov Models [20],

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 02
February 2017

Threshold Visual Cryptography [21] is used for identification purposes. Automatic Fingerprint Identification System (AFIS), in fingerprint recognition is also helpful to access control system of automobiles [22]. In another study, Delaunay Quadrangle method using topology code has been used for authentication [23]. Fingerprint authentications are also used in ATMs [24]. Some fingerprint matching systems are also based on model-based designs [25, 26].

III. TOP LEVEL SYSTEM DESCRIPTION

Figure.1 shows the block diagram of the Microcontroller based security system. This design combines the Microcontroller with the Fingerprint Module, display, and communication interfaces. This integration accelerates development while maintaining design flexibility and simplifies testing. Figure.1 shows the block diagram of the Microcontroller based system. The design combines the microcontroller with the Fingerprint Module, display, and communication interfaces. This integration accelerates development while maintaining design flexibility and simplifies testing.

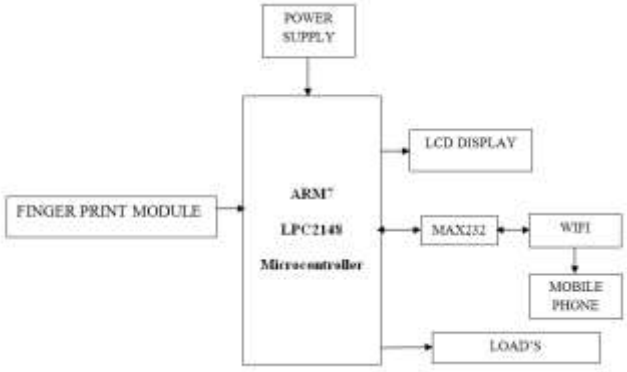


Fig.1Top Level system Diagram

The design includes following three modes:

Mode 1: The fingerprint module is connected with the PC using RS232 through serial communication. The Software called SFG Demo is then used for interfacing purpose. The fingerprint module is interfaced with the PC through the SFG Demo. By using SFG Demo software we are storing the fingerprint template of all the individuals with a unique id inside the fingerprint module.

Mode 2: Then we are connecting fingerprint module with microcontroller, the use of microcontroller is to extract the data from fingerprint module .By using microcontroller1 we are receiving the enrollment id or unique id of specific person. For example- Suppose if in a class, templates of all the students are stored. Then when a student places his/her finger in the fingerprint sensor, matching of template takes place in 1: N fashion inside the fingerprint module. Then the unique ids are received by using microcontroller

IV.ARCHITECTURE OF MATCHING INSIDE FINGERPRINT MODULE (R305)

It is actually very difficult to devise a proper algorithm for matching of fingerprint and making the algorithm robust. This chapter discusses the current state of the art feature extraction techniques and gives a literary review of algorithm of matching the extraction.

Data Acquisition

Traditionally in law enforcement applications fingerprints were acquired off-line by transferring the inked impression of thumb on a paper. Recently, the automated fingerprint verification systems use live-scan digital images of fingerprint acquired from a fingerprint sensor or module. These sensors or module are based on optical, capacitance, ultrasonic and thermal and other imaging technologies.

The optical sensors are most popular and are fairly expensive. These sensors are based on FTIR (Frustrated Total Internal Reflection) technique. When a finger touches the sensor surface which actually is a side of a glass prism, in which one side of the prism is illuminated through a diffused light. While the fingerprint valleys that do not touch the sensor surface reflect the light, ridges that touch the surface absorb the light. The sensor exploits this differential property of light reflection to differentiate the ridges (which appear dark) from valleys.

Fig.2 R305 module and fingerprint recognition with various features

Like the optical sensor algorithm for data acquisition there are two other algorithms for data acquisition namely, capacitive sensor utilization method and ultra sound technology based sensors. As in our project we have tried to use the first one that is optical sensors method. So we have not described the other two methods

Image Pre-processing

The pre-processing steps try to compensate for the variations in lighting, contrast and other inconsistencies which are introduced by the sensor during acquisition process. There are many processes but presently some methods are very famous which the following are:

Gaussian Blur: A convolution operation which applied to the original fingerprint image to reduce image noise introduced by sensor during data acquisition.

Sliding window contrast adjustment: Sliding window contrast adjustment is used to compensate for any lighting inconsistencies within a fingerprint and to obtain contrast consistencies among different fingerprints

Histogram based intensity level adjustment: This is a final step is to further enhance the ridges and valleys.

Feature extraction

The feature extraction technique for minutiae points (bifurcations and endings), pores and ridge contours is described in this section.

Minutiae Extraction:

Most of the minutiae extraction techniques trace the fingerprint skeleton to find different types of minutiae points. Orientation Estimation: A fingerprint image is an oriented texture pattern and a ridge orientation at a pixel (x, y) is the angle that the ridges within a small neighborhood centered at (x, y) form with the horizontal axis. Thus a fingerprint is divided into many blocks. An analysis of gray scale gradient within a block is done to estimate the representative ridge orientation within that block. Segmentation: During this stage the portions of the fingerprint image depicting the finger foreground is segmented. This further eliminates the spurious features from background and noisy region within a fingerprint.

Ridge Detection:

An important property of the ridges in a fingerprint image is that the gray level values on ridges attain their local maxima along a direction normal to the local ridge orientation. The resulting ridge map often contains false ridges in the form of holes and speckles. The ridge map is cleaned using a connected component algorithm. Finally the ridges are thinned using standard thinning algorithm.

Minutiae Detection:

The minutia points are then extracted from the thinned ridge map by examining the 8 neighborhood of each ridge skeleton pixel. The ridge breaks, Ridge bending direction and width are the information extracted but this may contain spurious minutiae. This may occur due to presence of noise, ridge breaks (even after enhancement) and image processing artifacts. Post processing: A number of heuristics are used to remove spurious minutiae. False minutiae are generally found at the borders as the ridges end abruptly. These false minutiae at the border can be recognized by examining the number of foreground pixels in a region around minutia point. If number of foreground pixels is relatively small then the minutia point can be removed.

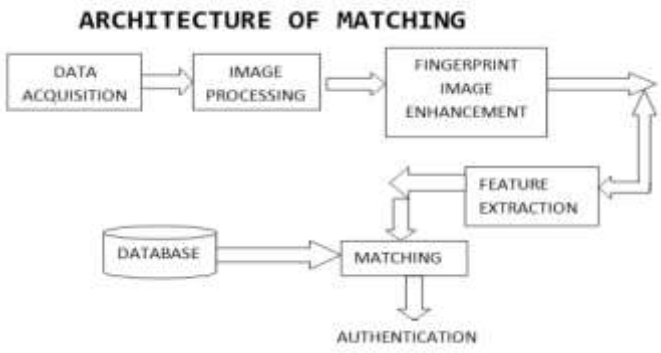


Fig. 3 Architecture of fingerprint matching algorithm

V. MODEL BASED DESIGN AND SIMULATION

Model based design approach is an ideal approach for Embedded System Design. There are many system model tools available from various vendors. These tools facilitate the design of hardware and software before actual physical implementation of the system. Proteus tool is used for this project. The Proteus tool also provides virtual instruments like Oscilloscope, Logic analyzer to monitor the signals of the system. Step by step design process of building the microcontroller system by interfacing switch, LED, LCD, Serial Communication and Fingerprint Module and using the assembly language programming Proteus allows assembly code to be assembled and downloaded on the virtual microcontroller. For C language coding Keil compiler is used.

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 02
February 2017

The generated hex code is used to configure and run the system.

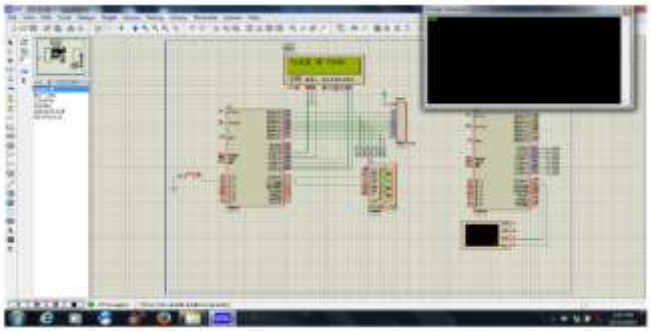
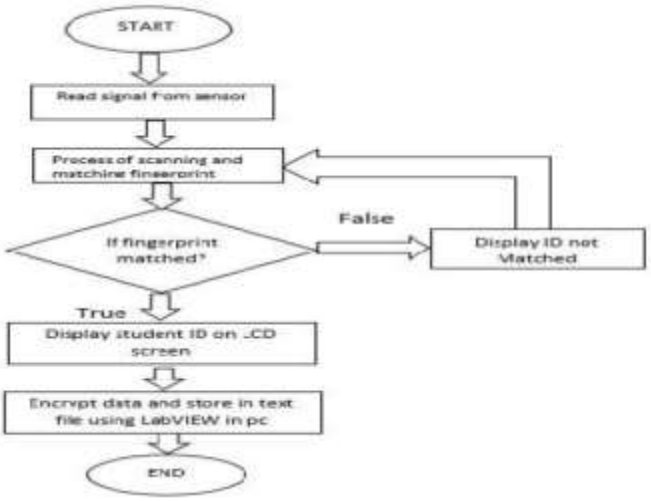


Fig. 4 Schematic and Proteus Simulation Model

Figure 5 describes the flow chart of the proposed fingerprint attendance system. First, the device will read the signal from fingerprint sensor as shown in Figure.



VI. RESULTS AND DISCUSSION

The security can save each person's fingerprint, hence makes the system more robust. During enrolment the person's fingerprints is assumed to be clean, not dry or damp, no scratches and not swollen.

Problems	Fingerprint Snapshot	Problems	Fingerprint Snapshot
Finger Misplacement		Dirty Finger	
Orientation		Skin Problems	
Wet Finger			

Members are required to place their fingerprint. After the enrolment stage, the data will be saved in the fingerprint scanner and the verification system takes place by comparing the capture fingerprint characteristic with the previously enrolled data. Table I shows the types of issue that might occur when taking attendance system acquiring fingerprint for attendance purposes. We considered all of these factors for the product which are user-friendliness, convenience, portability, and heating resistance.

VII. CONCLUSIONS

This paper has presented the design and development of portable security system which is based on fingerprint identification. The system helped to reduce many issues such as, power consumption, security access, load controlling helps to ease the owners to keep data of related person's the encryption technique adds more security so there will be no anonymous fingerprint which is able to tamper with the recorded data, Future works will be making this system wireless and using IOT (internet of things) concept.

REFERENCES

[1] K A. Nagaty,"An Energy-Based Fingerprint Matching System",Consumer Communications and Networking Conference, 2004. CCNC 2004. First IEEE.

[2] C. Militello, V. Conti, F. Sorbello,S. Vitabile,"A Novel Embedded Fingerprints Authentication SystemBased on Singularity Points",International Conference on Complex,

Intelligent and Software Intensive Systems,0-7695-3109-1/08 $25.00 © 2008 IEEE.

[3] G. S. Ng1*, X. Tang, D. Shi11"Adjacent Orientation Vector Based Fingerprint Minutiae Matching System", Proceedings of the 17th International Conference on Pattern Recognition (ICPR'04) 1051-4651/04 $ 20.00 IEEE

[4] Wang Yuan1 Yao Lixiu1 Zhou Fuqiang2,"A Real Time Fingerprint Recognition System Based OnNovel Fingerprint Matching Strategy",1- 4244-1135-1/07/$25.00 ©2007 IEEE.

[5] Bifari, E.N.; Elrefaei, L.A."Automated Fingerprint Identification System Based on Weighted Feature Points Matching Algorithm", 978-1-4799-3080-7114/$31.00 ©2014 IEEE

[6] Fan Wang, Zhengyong Huang, Hui Yu, Xiaohua Tian, Xinbing Wang, Jinwei Huang"EESM-based Fingerprint Algorithm for Wi-FiIndoor Positioning System"2013 2nd IEEE/CIC International Conference on Communications in China (ICCC): Wireless Networking and Applications (WNA),978-1-4673-2815-9/13/$31.00 ©2013 IEEE.

[7] Marcos Faundez-Zanuy & Joan Fabregas"Testing Report of a Fingerprint-Based Door-Opening System",IEEE A&E SYSTEMS MAGAZINE. JUNE 2005.

[8] Pallav Guptat, Srivaths Ravi*, Anand Raghunathan*, Niraj K. Jhat"Efficient Fingerprint-based User Authentication for Embedded Systems",DAC2005, June l3-17,2005, Anaheim, Califomia, USA. Copyright 2005 ACM 1-59593-05 8-2/05/0004 .

[9] Maitane Barrenechea1,Jon Altuna2,Miguel San Miguel2 "A Low-Cost FPGA-based Embedded Fingerprint Verification and Matching System",250 - 261, DOI: 10.1109/WISES.2007.4408496,2007.

[10] Pablo David Gutiérrez, Miguel Lastra, Francisco Herrera, and José Manuel Benítez"A High Performance Fingerprint Matching System for Large Databases Based on GPU",IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 1, JANUARY 2014.

[11] Haiyun Xu, Raymond N. J. Veldhuis, Tom A. M. Kevenaar, and Ton A. H. M. Akkermans"A Fast Minutiae-Based Fingerprint Recognition System",IEEE SYSTEMS JOURNAL, VOL. 3, NO. 4, DECEMBER 2009,1932-8184/$26.00 © 2009 IEEE.

[12] Radu F. Miron, Tiberiu S. Letia and Mihai Hulea "Two Server Topologies for a Distributed Fingerprint-BasedRecognition System" System Theory, Control, and Computing (ICSTCC), 2011 15th International Conference,2011.

[13] D. Bennet,Dr. S. Arumugaperumal"Fingerprint Based Multi-Server Authentication System"978-1-4244-8679-3/11/$26.00 ©2011 IEEE.

[14] Lei Zhang, Mei Xie "Realization of a New-style Fingerprint Recognition System Based on DSP",Proceedings of 2008 IEEE International Symposium on IT in Medicine and Education,978-1-4244-2511-2/08/$25.00 ©2008 IEEE.

[15] Maddu Kamarajui , Penta Ani! Kumar2 "DSP based Embedded Fingerprint RecognitionSystem",2013 13th International Cmiference on Hybrid Intelligent Systems (HIS) ,978-1-4799-2439-4/13/$31.00 ©2013 IEEE.

[16] Yanpeng Wang 1 Qing Li 2 Li Zhang 3"Design of Embedded Fingerprint Identification System Based on DSP"Anti-Counterfeiting, Security and Identification (ASID), 2011 IEEE International Conference ,978-1-61284-632-3/11/$26.00 ©2011 IEEE.

[17] P. Lorrentza , W. G. J. Howellsb,K.D. McDonald-Maierc"A Fingerprint Identification System using adaptive FPGA based Enhanced Probabilistic Convergent Network",2009 NASA/ESA Conference on Adaptive Hardware and Systems,978-0-7695-3714-6/09 $25.00 © 2009 IEEE DOI 10.1109/AHS.2009.8.

[18] G.Vinoth Kumar,K.Prasanth ,S.Govinth Raj ,S.Sarathi ,"Fingerprint Based Authentication System with Keystroke Dynamics for Realistic User"© IEEE 2014 IEEE Conference Number - 33344 July 8, 2014, Coimbatore, India.,

[19] Fengling Wang1 , Yuanyi Zhang2"Study and Design of Intelligent Authentication System Based on Fingerprint Identification"2009 Second International Symposium on Knowledge Acquisition and Modeling,978-0-7695-3888-4/09 $25.00 © 2009 IEEE.

[20] Arash Azarnoush ,Kourosh Kiani "Improving the Performance of an HMM-based Fingerprint Recognition System"Computer Applications & Research (WSCAR), 2014 World Symposium,978-1-4799-2806-4/14/$31.00 ©2014 IEEE.

[21] Rajeswari Mukeshi, V.J.Subashini2 "Fingerprint Based Authentication System Using Threshold Visual Cryptographic Technique"IEEEInternational Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012.

[22] Zhaoxia Zhu; Fulong Chen"Fingerprint Recognition-Based Access Controlling System for Automobiles" 2011 4th International Congress on Image and Signal Processing,978-1-4244-9306-7/11/$26.00 ©2011 IEEE.

[23] Wencheng Yang, Jiankun Hu, and Song Wang"A Delaunay Quadrangle-Based Fingerprint Authentication System with Template Protection Using Topology Code for Local Registration and Security Enhancement" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 7, JULY 2014.

[24] H. Lasisi and A.A. Ajisafe "Development of stripe biometric based fingerprint Authentications systems in automated teller machines" 2012 2nd International Conference on Advances in Computational Tools for Engineering Applications (ACTEA),978-1-4673-2489- 2/12/$31.00 ©2012 IEEE.

[25] Rosario Arjona and Iluminada Baturone"Model-based Design for Selecting FingerprintRecognition Algorithms for Embedded Systems"Electronics, Circuits and Systems (ICECS), 2012 19th IEEE International Conference,978-1-4673-1260-8/12/$31.00 ©2012 IEEE.

[26] Xi Cheng, Sergey Tulyakov and Venu Govindaraju"Minutiae-based Matching State Model for Combinations in Fingerprint Matching System"2013 IEEE Conference on Computer Vision and Pattern Recognition Workshops,978-0-7695-4990-3/13 $26.00 © 2013 IEEE.

[27] Abhishek Rawat, Indian Institute of Technology, Kanpur. "A hierarchical fingerprint matching system", A thesis for b.tech m.tech dual degree, published in 2009. Prof. Shashank Pujari,Prangyadarshini Behera ,Devendrakumar Yadav,"HELIANTHUS - SMART SOLAR PANEL" International Journal of Communication Network Security ISSN: 2231 – 1882, Volume-2, Issue-1,