IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

An Efficient Biometric Attendance System using Fingerprint Verification Technique

Jayant Waman Gonnade[*1], Sagar Kantilal Deore[2], Ajit Vijaysing Rajput[3], Sumit Venkatrao Chalganje[4]

Veermata Jijabai Technological Institute(VJTI), Mumbai, India

jayantgonnade99@gmail.com

Abstract

Biometrics based technologies are supposed to be very efficient personal identifiers as they can keep track of characteristics believed to be unique to each person. Among these technologies, Fingerprint identification is one of the most popular and reliable personal biometric identification methods. The main aim of this paper is to develop an accurate, efficient automatic attendance system using fingerprint verification technique. We propose a system in which fingerprint verification is done by using extraction of minutiae technique and the system that automates the whole process of taking attendance, Manually which is a laborious and troublesome work and waste a lot of time, with its managing and maintaining the records for a period of time is also a burdensome task. For this purpose we use fingerprint verification system using extraction of minutiae techniques and Embedded system. The experimental result shows that our proposed system is efficient and low cost in verification of user fingerprint.

Keywords: Fingerprint Recognition; Bifurcation; Ridge; Minutia.

Introduction

Cryptographic technique is being widely used for ensuring the secrecy and authenticity of information [1]. Although several cryptosystems have proven security guarantees (e.g., AES and RSA), the security relies on the assumption that the cryptographic keys are known only to the legitimate user. Maintaining the secrecy of keys is one of the main challenges in practical cryptosystems. However, passwords can be easily lost, stolen, forgotten, or guessed using social engineering and dictionary attacks. Limitations of password-based authentication can be alleviated by using stronger authentication schemes, such as biometrics. Biometric systems establish the identity of a person based on his or her anatomical or behavioral traits, such as face, fingerprint, iris, voice, etc. Biometric authentication is more reliable than password-based authentication because biometric traits cannot be lost or forgotten and it is difficult to share or forge these traits. Hence, biometric systems offer a natural and reliable solution to the problem of user authentication in cryptosystems.

We know about some commonly used biometric techniques are used for objective identification and verification are like iris recognition, voice identification, facial recognition, fingerprint identification, DNA recognition, hand geometry recognition, signature recognition, and gait recognition . Biometrics techniques are widely used in various areas like building security, forensic science, ATM, criminal identification and passport control [2]. In our proposed automatic attendance system we uses fingerprint recognition technique [3] for obtaining the attendance. The fingerprint recognition is widely used for many other purposes and it is widely popular technique. Fingerprint verification is very convenient and reliable way to verify the person's Identity. It is believed that no two people have identical fingerprint in this world [4], so the fingerprint verification and identification is most popular way to verify the authenticity or identity of a person wherever the security is a problematic question. The reason for popularity of fingerprint technique is uniqueness of person arises from his behaviour; personal characteristics are like, for instance uniqueness, which indicates that each and every fingerprint is unique, different from one other. Universality, that means every person hold the individual characteristics of fingerprint. Permanence, means that fingerprint are permanent, are impossible to change or forgot, and can never be stolen. Collectability means that we can measure fingerprint quantitatively.

In present scenario, the various uses of fingerprint verification are widespread like authentication to logon machine and others but still majorly for law enforcement applications. There are a

lot of expectations that the use of fingerprint recognition will increase which is dependent of some factor involved like small fingerprint capturing devices, fast computing hardware, and awareness on easy to use methods for security. This paper cover the topics on fingerprint recognition, algorithm and our proposed system, which is so cheap, handy that can be affordable to any institute and organization.

Fingerprint Recognition

A fingerprint is the print or the impression made by our finger because of the patterns formed on the skin of our palms and fingers since birth. With age, these marks get prominent but the pattern and the structures present in those fine lines do not undergo any change [5]. For their permanence and unique nature, they have been used since long in criminal and forensic cases.

Shown below, is a fingerprint pattern obtained from an optical sensor. The figure shows faint and dark lines emerging from a particular point and whirling around it all over the finger.

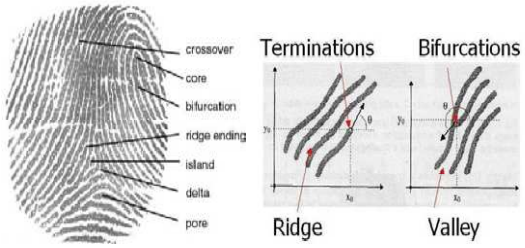

Figure 1. (a) The fingerprint image, which describes the important feature in fingerprint. (b) Minutiae points

Every fingerprint consists of ridges and furrows. These ridges and furrows are known to show good similarities but when it comes to identifying a person or distinguishing between two different prints, these do not prove efficient enough. Research shows that fingerprints are not distinguished by ridges and furrows but by Minutia. Minutia refers to some abnormalities in a ridge, which shall be discussed in detail in the following pages.

As already mentioned, Minutia are abnormal points in a ridge. There can be various such Minutia but the two most important and useful minutia types are Termination and Bifurcation. Termination refers to the abrupt ending of a ridge, as shown in fig.1. Bifurcation on the other hand refers to the point on the ridge where branching occurs, as shown in fig 1.

Fingerprint recognition consists of fingerprint identification and verification. Fingerprint identification refers to specifying one's identity based on his fingerprints. The fingerprints are captured without any information about the identity of the person. It is then matched across a database containing numerous fingerprints. The identity is only retrieved when a match is found with one existing in the database. So, this is a case of one-to-n matching where one capture is compared to several others. This is widely used for criminal cases. Fingerprint verification is different from identification in a way that the person's identity is stored along with the fingerprint in a database. On enrolling the fingerprint, the real time capture will retrieve back the identity of the person. This is however a one-to-one matching. This is used in offices like passport offices etc. where the identity of a person has to be checked with the one provided at a previous stage.

The approach that we have concentrated on in recognition of the fingerprints is the minutia based approach. In this approach the ridge bifurcations and terminations are taken into consideration for analyzing each fingerprint. The representation is based on these local features.

The scanner system uses highly complex algorithms to recognize and analyze the minutia. The basic idea is to measure the relative portion of minutia. Simply, it can be thought of as considering the various shapes formed by the minutia when straight lines are drawn between them or when the entire image is divided into matrix of square sized cells. If two fingerprints have the same set of ridge endings and bifurcations forming the same shape with the same dimension, there' s a huge likelihood that they are of the same fingerprint. So, to find a match the scanner system has to find a sufficient number of minutia patterns that the two prints have in common, the exact number being decided by the scanner programming.

System Structure

The system consists of fingerprint verification module, Microcontroller circuit, PC, keypad and display. Fingerprint verification module is used to realize fingerprint collecting and pre-treatment. Print of finger is captured and stored in module. Microcontroller circuit used to interact with module, computer, keypad and display. Keypad is used to perform operation like adding finger print, deleting finger print, mark attendance etc. and corresponding results are displayed on LCD display.

Hardware Design

System hardware includes Atmega32 microcontroller, 16x4 LCD Display, SM630 fingerprint detection module, timer circuit and keypad.

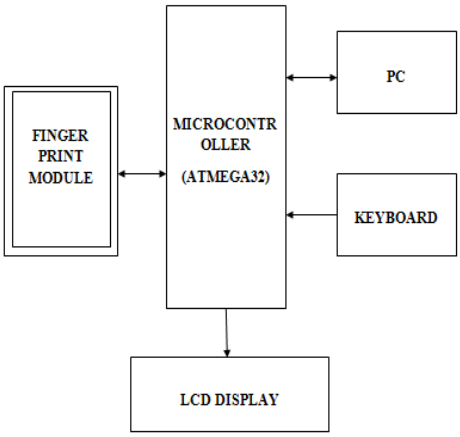

Figure 2:Block diagram of system

A. Fingerprint verification module:

Module used In this system is SM630 which is background highlight optical fingerprint verification module. 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. Compared to products of similar nature, SM630 consist the following unique. features : Self-proprietary Intellectual Property, High Adaptation to Fingerprints, Low Cost, Algorithm with Excellent Performance, Easy to Use and Expand, Low Power Consumption, Integrated Design, Perfect Technical Support.

B. RTC DS1307

The DS1307 serial real-time clock (RTC) is a low-power, full binary-coded decimal (BCD) clock/calendar plus 56 bytes of NV SRAM. Address and data are transferred serially through an I2C, bidirectional bus. The clock/calendar provides seconds, minutes, hours, day, date, month, and year information. The end of the month date is automatically adjusted for months with fewer than 31 days, including corrections for leap year. The clock operates in either the 24-hour or 12-hour format with AM/PM indicator. The DS1307 has a built-in power-sense circuit that detects power failures and automatically switches to the backup supply. Timekeeping operation continues while the part operates from the backup supply.

C. Micro controller

High-performance RISC CPU**,** Only 35 single word instructions to learn**,** Direct, indirect and relative addressing modes, Power-on Reset (POR)**,** Power-up Timer (PWRT) and**,** Oscillator Start-up Timer (OST)**,** Programmable code-protection**,** Low-power, high-speed CMOS FLASH/EEPROM technology**,** In-Circuit Debugging via two pins, Single 5V In-Circuit Serial Programming capability**,** Wide operating voltage range: 2.0V to 5.5V**.** High-performance RISC CPU: Only 35 single–word instruction to learn. Operating speed: DC- 20MHz clock input, DC-200ns instruction cycle.

D. RS 232

PC in general cannot directly communicate with peripherals that are available. The reason behind this is the difference in their working logic. PC generally works in positive logic. The microcontroller that actually acts as the peripheral here works in negative logic. It becomes important to change the logic between them when they communicate with each other. RS232 is very important for standard serial interfacing with PC where change of logic is achieved. PC communicates with peripherals through serial com1 or com2.

Working of the System

As shown in the block diagram, the entire processing will be done by the microcontroller. The communication between microcontroller unit (MCU) and the fingerprint detection module and also that between MCU and the PC will take place serially.

There will be two phases in the working of MCU, i.e., two different programs running at two different occasions. In the first phase, the fingerprints of all the attendants would be loaded into the module SM630 with open access to all. But this will be done under general supervision. Thus, every person working at the time of introduction of this biometric attendance system will have an identity in the memory of the SM630. Especially, there are some people who will be appointed as the supervisors are supposed to have their fingerprints at the first few addresses in the SM630.

Next, in the second phase, a new program will be introduced into the MCU and will remain in the MCU thereafter. This will operate, by default, in fingerprint detection mode where premium function of the MCU will be to update the attendance register in the PC while keeping detecting the fingers placed on the module. In general, adding a new fingerprint in this mode will not be allowed, in that, the access to the “ADD FINGERPRINT” mode will be restricted.

The procedure to be followed in the two phases is as follows. In the initial phase, persons will have to keep their finger (thumb) on the SM630 for the specified time one by one to get their IDs loaded into the system. They will have to keep their fingers and press the corresponding switch until the system acknowledges them of the successful entry of their fingerprint. Obviously, the first few should be the supervisors as mentioned earlier. This is required in the second phase for the MCU to identify the

supervisors. When a new fingerprint is to be added due to new appointments, first of all, toggle the operating status of the MCU using the switch corresponding to "ADD FINGERPRINT" mode. Before the new attendants presses his finger on the module in order to add his fingerprint, any one of the supervisors who is present at that time will press his finger. This will validate the addition of a new fingerprint thus making the access to the "ADD FINGERPRINT" mode very well supervised and hence restricted. In the end, again the switch corresponding to the "FINGERPRINT DETECTION" mode will be toggled and normal working should resume.

Conclusion

Thus the developed system provides fingerprint acquisition module and attendance management module in computer. It can realize automatically such functions as information acquisition of fingerprint, processing, fingerprint matching, and attendance management. A fingerprint acquisition module was designed by using the fingerprint sensor. In order to achieve the simple and high real-time system, it realized low-cost and high-performance fingerprint attendance function, which provided a new fingerprint attendance system for enterprises and institutions. To design and develop a low cost and easily mountable fingerprint attendance system using this mechanism for industries, colleges, hospitals, government offices etc.

References

[1] Josphineleela.R, Dr.M.Ramakrishnan *"Attendance System Using Fingerprint Reconstruction technique"* (IJCSIS) International Journal of Computer Science and Information Security,Vol. 10, No. 3, March 2012

[2] Anil K. Jain, Arun Ross and Salil Prabhakar, *"An introduction to biometric recognition"* Circuits and Systems for Video Technology, IEEE Transactions on Volume 14, Issue 1, Jan. 2004 Page(s):4 – 20.

[3] D. Maltoni, D. Maio, A. K. Jain, S. Prabhaker, *"Handbook of Fingerprint Recognition"* Springer, New York, 2003.

[4] Kuntal Barua, Samayita Bhattacharya, Dr. Kalyani Mali, *"Fingerprint Identification"* Global Journal of Computer Science & Technology Volume 11 Issue Version 1.0 April 2011.

[5] Chitresh Saraswat, Amit Kumar *"An Efficient Automatic Attendance System using Fingerprint Verification Technique"*Chitresh Saraswat et al. / (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010, 264-269.