Wireless Fingerprint Attendance System using ZigBee Technology

L.Rajasekar[1] S.Vivek[2]

[1]*Bannari Amman institute of technology, Assistant Professor, Department of Electronics and Instrumentation Engineering, Sathyamangalam, Tamilnadu.*
[2]*Bannari Amman institute of technology, M.E.Embedded systems, Sathyamangalam, Tamilnadu.*
`Email_id:viveksaminathan3@gmail.com`

Abstract

In this paper provides the design method of wireless fingerprint attendance system based on ZigBee technology. The system includes terminal fingerprint acquisition module and attendance management module through computer. It can realize automatically such functions as information acquisition of fingerprint, processing, wireless transmission, fingerprint matching, and attendance management. Considering the fact and topology of ZigBee network, a fingerprint acquisition module and a wireless alarm module were designed by using the fingerprint sensor and module respectively. The whole system was implemented wireless alarm through messages and internet in the GSM web. In order to achieve the simple and high real-time system, it realized low-cost and high-performance wireless fingerprint attendance function, which provided a new wireless fingerprint attendance system for enterprises and institutions.

Index Terms ZigBee technology, Fingerprint identification, Attendance System, Wireless communication, Wireless Alarm.

1. INTRODUCTION

Normally, The Attendance management can reflect truly staff attendance, which provides references for competent authorities. Attendance management is one of the most basic and important management links. Currently, the magnetic card attendance system is widely used. This pattern is Flexible and practical. But it has some disadvantages. For example, the card is easy to lost and damage. The fingerprint has a lot of advantages, such as unique, permanent, good anti-fake and easy to use. So it is recognized increasingly by people. ZigBee technology is an emerging technology developed in recent years. Comparing with some existing wireless communication technologies, ZigBee has advantages in low-power and low-cost. It is very suitable for application to wireless sensor networks. Aiming at the disadvantages of traditional wire attendance system, a design method of wireless fingerprint attendance system based on ZigBee technology is proposed. It achieves attendance management by fingerprint identification. At the same time, the system combines ZigBee wireless technology and attendance management. It realized low-cost, low-power and high-performance fingerprint information acquisition, transmission and recognition function, which provided a new attendance way for enterprises and institutions. As a public network with wide coverage, GSM supports real-time transmission, lower operation costs and SMS service and internet access. So it can be widely used in wireless alarm of access control system.

2. SYSTEM STRUCTURE

The system consists of fingerprint acquisition module, Transmission and receiving module, and attendance Management workstation. Fingerprint acquisition module is used to realize fingerprint collecting and pre-treatment. Transmission and receiving ZigBee module is used to send the finger print image to computer. Attendance management workstation is used to realize fingerprint extraction and matching in order to realize attendance function. If the finger prints feature and some sample in the database matches, access is permitted, or there will be alarm. There in to, alarms are divided into local alarms and wireless ones. Local alarm is given by sound and light lamps. Wireless alarm send messages to the concerned mobile phone by GSM module through which connect GSM network. And it is also sent to The PC alarm monitoring center by GSM internet network.

3. HARDWARE DESIGN

The system hardware includes: Fingerprint sensor, PIC Microcontroller, ZigBee module, Wireless alarm: GSM, Local alarm: Light, Buzzer.

A. Transmitter Block Diagram

This block consists of a finger print module that captures the data which is a person's fingerprint. The sensor forms the core part of the fingerprint module. This in turn is connected to a PIC16F877A microcontroller using RS232. The microcontroller stores the captured data and identifies a unique ID for the data. The unique id of the captured data is sent through the ZigBee transmitter module for further processing.
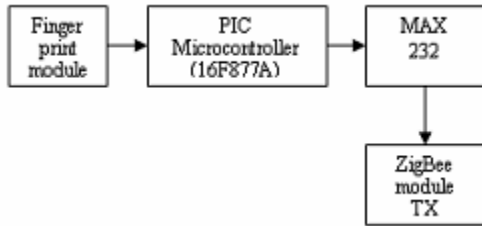
Figure.1 Transmitter block Diagram

B.Receiver Block Diagram
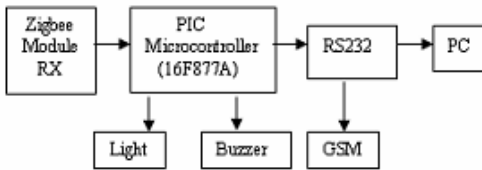
Figure.2 Receiver Block Diagram

The unique id of the captured data is received by the Zigbee receiver module and is forwarded toPIC16F877Amicrocontroller. The database of the person's that has been stored in microcontroller is compared with the unique id. If they match then a signal is indicated using the light and the buzzer.

The microcontroller then sends the data to PC through MAX232. The data is sent to PC for a specified time interval. The PC thus sends the information to the GSM using MAX232 further it is sent to mobile through message.

C.Finger Print Scanner

In today's world, the need for effective security is evident. Without effective security, many everyday activities are compromised. Specific security concerns include: Protecting computer systems, PDA's, mobile phones, Internet appliances and similar devices from unauthorized access or use.

Protecting motor vehicles and other valuable items from unauthorized access or use preventing theft and fraud in financial transactions, in particular electronic transactions, including credit card payments and payments via the Internet. Restricting access to workplaces warehouses and secures areas, such as military installations, to authorized personnel. Screening access to public transportation, in particular air travel. Authenticating the identity of an individual in drivers' licenses, health cards, ID cards, and similar administrative documents.

A major factor in ensuring security is the unique identification of individuals, or the authentication that a person is who he or she claims to be. This must be done reliably, rapidly, non-intrusively and at reasonable cost. In the past, this has been done by methods such as security

tokens (passports, badges, etc.), secure knowledge (passwords PIN codes, signature, etc.) or recognition by a guardian (doorkeeper). These traditional approaches are all limited with respect to the above criteria. A promising approach for the future is biometrics. Biometrics offers a convenient, reliable and low-cost means of identifying or authenticating individuals, and can be implemented in unsupervised and remote situations. Biometrics seeks to identify individuals uniquely by measuring certain physical and behavioral characteristics and extracting a sample (also called a sampled template or live template) from these measurements in a standard data format. This sample is compared with a template (also called an enrolled template or signature), based on the same characteristics, that has been established as the unique identity of that individual and stored in the security system. A close match between sample and template confirms the identity of the individual.

Attention has been focused on a small number of physical characteristics that can identify individuals uniquely, notably voice, gait, face, iris and retina patterns, palm prints and fingerprints. (DNA is excluded from this list because DNA sampling is intrusive and slow.) Work is proceeding to develop electronic recognition systems based on all of these. This article focuses on fingerprints as the most advanced mature and well-developed option. Based on centuries of experience and extensive research, fingerprints are at present considered to be the Most reliable biometric for uniquely identifying an individual. In spite of some recent legal challenges in the USA, they are still regarded as giving proof of identity beyond reasonable doubt in almost all cases. The majority of the biometric-based security systems in operation today are based on fingerprint recognition.

D.Finger Chip Technology

Finger Chip IC for fingerprint image capture combines detection and data conversion circuitry in a single rectangular CMOS die. It captures the image of a fingerprint as the finger is swept vertically over the sensor window. It requires no external heat, light or radio source. Most reliable biometric for uniquely identifying an individual. In spite of some recent legal challenges in the USA, they are still regarded as giving proof of identity beyond reasonable doubt in almost all cases. The majority of the biometric-based security systems in operation today are based on fingerprint recognition.

E. ZIGBEE

ZigBee is a low-cost, low-power, wireless mesh network standard. The low cost allows the technology to be widely deployed in wireless control and monitoring applications. Low power-usage allows longer life with smaller batteries. Mesh networking provides high reliability and more extensive range. The technology is

intended to be simpler and less expensive than other WPAN's such as Bluetooth. ZigBee chip vendors typically sell integrated radios and microcontrollers with between 60 KB and 256 KB flash memory.

ZigBee operates in the industrial, scientific and medical (ISM) radio bands; 868 MHz in Europe, 915 MHz in the USA and Australia, and 2.4 GHz in most jurisdictions worldwide. Data transmission rates vary from 20 to 250 kilobits/second.

The ZigBee network layer natively supports both star and tree typical networks, and generic mesh networks. Every network must have one coordinator device, tasked with its creation, the control of its parameters and basic maintenance. Within star networks, the coordinator must be the central node. Both trees and meshes allow the use of ZigBee routers to extend communication at the network.

F. 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.

G. 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.

H. GSM Module

PC: This unit contains the software components such as the server and security System through which the area security can be controlled and monitored. GSM Modem: It is a hardware component that allows the capability to send and receive SMS to and from the system. The communication with the system takes place via RS232 serial port. Cell phone can be attached at the place of GSM hardware but it limits the hardware functionality such as sending or receiving of SMS.

I. Working of GSM module

GSM hardware tests are run in order to check the hardware support. The system will call GSM modem and it will get activated.

After activation the Modem will check for hardware support. If the hardware is missing or some other hardware problem there will be error, resulting in communication failure and the application will be terminated.

If hardware responds then the serial port will be opened for communication and GSM hardware will allow transmission of SMS. The system will then connect and after connection establishment the system will be able to detect intrusion and will alert user about the breach and similarly the system will update status of appliances by receiving SMS from the pre-defined cell number. SMS will be silently ignored if cell number is unauthorized.
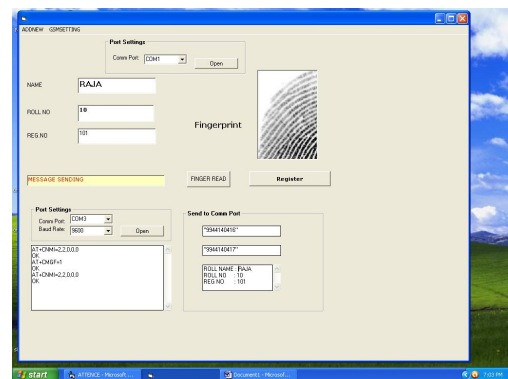
4. RESULT OF PROJECT

Figure.3 Output Window

5. 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, wireless transmission, fingerprint matching, and attendance management .A fingerprint acquisition module and a wireless alarm module were designed by using the fingerprint sensor and GSM module respectively. The whole system was implemented wireless alarm through messages and internet in the GSM web. In order to achieve the simple and high real-time system, it realized low-cost and high-performance wireless fingerprint attendance function, which provided a new wireless fingerprint attendance system for enterprises and institutions. To design and develop a low cost and easily mountable advanced fingerprint attendance system using wireless technology for industries, colleges, hospitals, government offices etc..

REFERENCES

1. Ming-jin Xu, Xin-hong Wu, "Application of FPS200 based on DSP embedded system", Journal of Chongqing University, no.6, 2006, pp.23-25.
2. E. Jovanov, D. Raskovic, J. Price, A. Moore, J. Chapman, and A.Krishnamurthy, "Patient Monitoring Using Personal Area Networks of Wireless Intelligent Sensors", Biomedical Science Instrumentation, vol.37, 2001, pp. 373-378.
3. C. G. Xie, "ARM-Based Automatic Fingerprint Identification System", Microcomputer Information, Vol. 25, No.1-4, 2009, pp. 292-294
4. J.-M. Nam, S.-M. Jung, D.-H. Yang and M.-K. Lee, "Design and Implementation of 160 ﾃ 192 Pixel Array Capacitive-Type Fingerprint Sensor", Circuits, Systems &Signal Processing, Vol. 24, No. 4, 2005, pp. 401-413.
5. L. Zhang, "Based on DSP and RF Card Embedded Fingerprint Identification System Design and Implementation of [D]", University of Electronic Science and Technology of China, Chengdu, 2009.
6. H. Guo, Y. S. Guo and Y. Chen, "The Implementation of Remote Meter Reading System
7. Based on Linux and GPRS", Application of Electronic Technique, Vol. 34, No.11, 2008, pp. 82-84.
8. F. Ding, "ARM-Based Fingerprint Identification System Research and Implementation of [D]", South China University of Technology, Guangzhou, 2007.
9. Z. M. Ma and Y. H. Xu, "ARM Based Embedded Processor Architecture and Application", Beijing iversity of Aeronautics and Astronautics Press, Beijing, 2002.
10. K. Al-Begain, I. Awan and D. D. Kouvatsos, "Analysis of GSM/GPRS Cell with Multiple Data Service Classes," Wireless Personal Communications, Vol. 25, No. 1, 2003,pp. 41-57.
11. Y. Li, "MCLinux Based on ARM Embedded System Theory and Application", Tsinghua University Press, Beijing, 2009.
12. J. K. Zhang and X. Q. Zhang, "Embedded Linux System Development Technology Xiangjie—Based on ARM", Posts & Telecom Press, Beijing, 2006.
13. M. F. Du, "Development of Ethernet Interface for Smart Entry Controller Based on ARM & Linux Architecture", Computer Engineering, Vol. 33, No. 16, 2007, pp. 234-236.
14. C. J. Zhang, "System of Defending to Rob by Tailing Behind of Double Gate by Chip Microcomputer Control", Compu Ter Engineering and Applications, Vol. 43, No. 5, 2007, pp. 79-81.