Wireless Fingerprint Attendance Management System

YONGQIANG ZHANG JI LIU
Department of Information and Electrical Engineering
Hebei University of Engineering
Guangming South Street #199, Handan, Hebei
P.R.China
http://wisdom.hebeu.edu.cn

Abstract: - Fingerprint verification is one of the most reliable personal identification methods in biometrics .With the rapid development of fingerprint verification, a number of its applications have been proposed until now including time attendance system etc. In this paper, a wireless fingerprint attendance management system is designed and implemented .This system based biometrics and wireless technique solves the problem of spurious attendance and the trouble of laying the corresponding network. It can make the users' attendances more easily and effectively.

Key-Words: - fingerprint verification; personal identification; biometrics; attendance management; wireless

1 Introduction

While the move towards the digital era is being accelerated every hour, biometrics technologies have begun to affect people's daily life more and more.

Biometrics technologies verify identity through characteristics such as fingerprints, faces, irises, retinal patterns, palm prints, voice, hand-written signatures, and so on. These techniques, which use physical data, are receiving attention as a personal authentication method that is more convenient than conventional methods such as a password or ID cards.

Biometric personal authentication uses data taken from measurements. Such data is unique to the individual and remains so throughout one's life. This technology has been applied for controlling access to high-security facilities, but it is now being widespread developed in information systems such as network, e-commerce, and retail applications.

In these technologies, fingerprint becomes the most mature and popular biometrics technology used in automatic personal identification. In the beginning, fingerprint verifying used in the military affairs and in the criminal identification. But now, this technology is also being used in several other applications such as access control for high security installations, credit card usage verification, and employee identification [1]. The reason for the popularity of fingerprint verifying is that fingerprints satisfy uniqueness, stability, permanency and easily taking. Just for this, a number of fingerprint verification approaches have been proposed until now [2].

This paper introduces a wireless fingerprint attendance management system. This system is an application of the fingerprint verifying and RF wireless techniques and it is mainly used for employee identification. Through practices, this system is proved to be easy-to-use and effectively.

And this paper is organized as follows. Section 2 describes the technological requirements for this system design. Section 3 outlines the functions of this system briefly and describes the hardware and software design of this system. Section 4 introduces some key problems in the implement of this system and finally Section 5 contains conclusions and future research plan.

2 Requirements for System Design

2.1 Authentication Using Fingerprints

Canonical and scientific modern company management system is the requirement for creating a cost-effective, rapid developing corporation. And attendance management is an important part of corporation management system. It can be in contact with salary of employee, work efficiency of corporation and even affects business image of company and staff morale. So the problem of reasonably, effectively and scientifically managing of staff attendances has become all companies facing issue.

Traditional styles of attendance management include hand-written signatures, card bell, magnetic card, IC card and RF card attendance machines. These styles cannot avoid replacer checking out just because that people can be separated from cards.

The great advantage of the authentication using fingerprints is the irreplaceable nature. Through the analysis of the overall and local characteristics of fingerprint such as ridges, valleys, ending, bifurcation points and ridge divergence points, we can extract enough detail data. Such data is unique to the individual and remains so throughout one's life [1]. We can use these data to identify or verify a person operating as follows: (1) a digital image of one person's fingerprint to be verified is captured;(2) a feature extracting algorithm is carried out;(3) minutiae are extracted and stored as a template for verifying later;(4) people to be verified place his finger on the fingerprint sensor so as to extracting the minutiae from the captured image; (5) a matching algorithm is applied to matches the minutiae with the stored template previously[3][4][5][6]. The overall block diagram of the fingerprint verifying is shown in Figure 1.

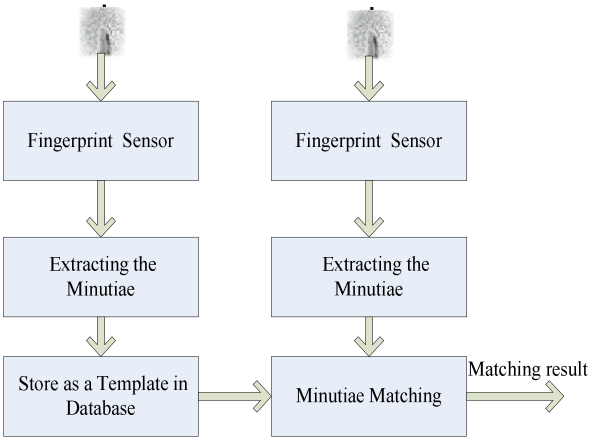

Fig.1 Fingerprint verifying process

2.2 Transmission Using Wireless Technique

There are mainly two kinds of fingerprint attendance management system on the market. One is on-line fingerprint attendance management system and the other is off-line fingerprint attendance management system.

On-line system always needs to connect with a PC or workstation and all the fingerprints' templates of people to be verified must stored in the database in the PC or workstation. Thereby, matching fingerprints needs the support of the background PC. This kind of attendance management system is easy to paralysis in case of malfunctions of fingerprint attendance machines, transmission line or PC. Once several systems connect to form a network, burden of PC and the response time of the system will be added.

By contraries, one off-line fingerprint attendance management system can finish all the process including capturing the image of fingerprint, extracting minutiae, storing and matching. All the operating of matching fingerprint needn't support of PC and the burden of PC is lightened. The same systems can connect to form a 485 network and finally connect to the center PC of management system. So off-line systems are widely used in many occasions. And the shortcomings of this system are that there must be a managing PC nearly and it is difficult to lay the transmission lines where topography is bad.

With the development of wireless techniques such as RFID, GPS, Wi-Fi, Bluetooth etc, many companies manufacture wireless modules. So we can adopt the wireless techniques to solve above-mentioned questions.

3 Functions and Composing of this System

Nowadays, bulk of automatic fingerprints recongnition system is constantly smaller. Complex fingerprints verifying algorithms can be solidified in a small embedded processing module. This module and fingerprints sensor, external control interface constitute embedded fingerprint verifying system. This wireless fingerprint attendance management system is designed and realized based on automatic fingerprints recognition module and RF wireless module. Basic functions of this system include:

(1) Take the task of users' attendances;
(2) Transmit the information of attendances to the managing PC;
(3) As a terminal of information, display useful information transmitted by PC on LCD.

3.1 Hardware Design

The hardware part of wireless fingerprint attendance management system is mostly made up of fingerprint verifying module, microcontroller, power module, wireless communication module, real-time clock module, keyboard module and LCD display module. Figure 2 shows the architecture of hardware design.

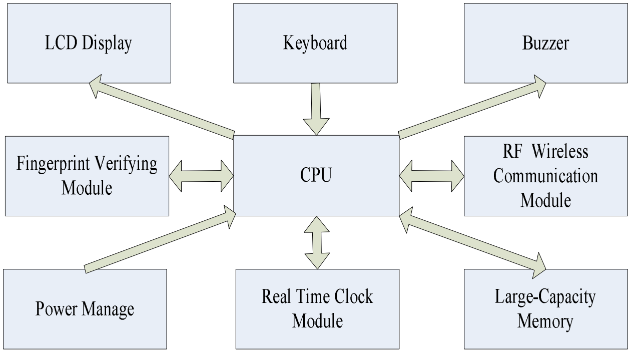

Fig.2 Architecture of hardware design

3.1.1 CPU and Fingerprint Verifying Module

Of all the components, fingerprint verifying module, microcontroller and RF wireless communication module are the core of this system. And hardware design is taking microcontroller (CPU) as center. We choose AT89C5122 as the microcontroller of this system which is a high-performance CMOS derivative of the 80C51 8 bit microcontrollers produced by Atmel Corporation. This chip not only has keyboard interrupt interface, UART, hardware watchdog and enough large RAM, Flash RAM, I/O ports but also has a self powered USB port. So it is fit for the embedded application systems well. Fingerprint verifying module is composed of fingerprint processing module and fingerprint sensor. In Figure 3, fingerprint processing module is showed in broken line frame.

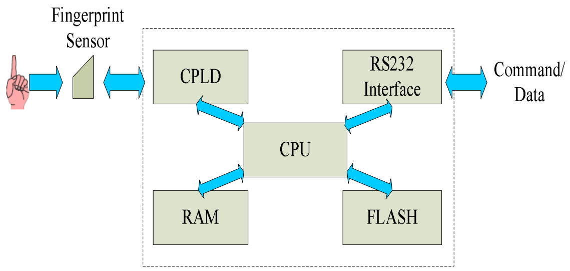

Fig.3 Fingerprint processing module

Fingerprint processing module communicates with microcontroller module using RS232 interface in the form of transmitting and receiving data packet[7]. We define the format of 12 bytes data packet as:

1 Byte	1 Byte	2 Bytes	2 Bytes	2 Bytes	2 Bytes	1 Byte	1 Byte
0	Com-mand	P1	P2	Lw-Extra Data	Hw-Extra Data	Error Code	Check Sum

Table 1 Format of communicating data packet

Data packet is divided into two categories: Command Packet and Response Packet. Command packet which needs to be set command byte, p1 (parameter 1) and p2 (parameter 2) bytes is transmitted to fingerprint verifying module by microcontroller. Fingerprint verifying module works under the command packet and responses the Response packet which has the same command byte but has the extra data in the eighth to tenth bytes and error code. Error code and check sum bytes can be used to check on the operations of fingerprint verifying module.

There are basically five operations for fingerprint verifying module: (1) Registering Fingerprints; (2) Modifying Fingerprints; (3) Deleting Fingerprints; (4) Verifying Fingerprints; (5) Identifying Fingerprints.

For example, command packet and response packet of registering a user's fingerprint are:

FP_REGISTER_START Command Packet							
0x00	0x50	ID	0	0	0	0x00	Chk
FP_REGISTER_STRAT Response Packet							
0x00	0x50	0	0	0	0	0x00	Chk
FP_REGISTER_End Command Packet							
0x00	0x51	ID	0	0	0	0x00	Chk
FP_REGISTER_End Response Packet							
0x00	0x51	0	0	0	0	0x00	Chk

Table 2 Registering a user's fingerprint

3.1.2Wireless Communication Module Design

As an embedded system, we need that wireless module has low power dissipation, longer transmission distance, better anti-disturbing capability and small package. We choose PTR2000+[8] wireless module as wireless communication module which is based on nRF401 chip. This module is designed to operate in the 433MHz ISM (Industrial, Scientific and Medical) frequency band and it features Frequency Shift Keying (FSK) modulation and demodulation capability[9]. It operates at bit rates up to 20k bit/s, effective transmission distance over 1000m and needs few external components fully meeting the needs of this system. And it is easy to be used. Data input pin (DI) and data output pin (DO) of PTR2000+ can be connected to TXD, RXD of UART of AT89C5122 directly. To control the PTR2000+ to receive or transmit, TXEN pin is connected to one I/O pin of AT89C5122. TXEN=1 selects transmit mode and TXEN=0 selects receive mode.

CPU communicates information with PTR2000+ module by UART and controls PRT2000+ to transmit information such as attending records and system log. Also there is receiving terminal of PTR2000+ near the managing PC. Of course, there needs a voltage converter IC (MAX232) to convert TTL level to RS-232 electrical level when PTR2000+ is connected to the serial ports of PC. RST of COM can be connected to TXEN pin of PTR2000+ to switch its status of transmitting or receiving. So it realizes the function of wireless transmitting attendances information to PC.

3.1.3 Man-Machine Interface and Other Hardware Design

Man-machine interface includes keyboard, buzzer and LCD display system. The former is used for people to input users' ID or commands, the function of the second is to give users a hint and the last is used to display the information of date, time, user ID, error code, status and system log.

Real-time clock in the fingerprint management system is the benchmark of attending records. We use DS1302 trickle charge timekeeping chip containing an RTC by Dallas Semiconductor Corporation. It not only can satisfy the accuracy of the time, but also continues to work by battery when power is low.

There is also a mess storage memory (EEPROM) AT24C512 in this system which is used to store the records of attendances. These records are made to be copies of attending info which are transmitted to PC by wireless module. And USB port gives the managers of this system a way to download these records in case of data packets lost in the wireless transmission.

3.2 Software Design

The software of wireless fingerprint attendance management system includes controlling software and managing software installed in managing PC or workstation.

3.2.1 Controlling Software Design

Controlling software in this system is mainly divided into four categories: fingerprints verifying and identifying, managing fingerprints of users, system setting, wireless communication managing.

The simple flowchart of controlling software of this system is shown in Figure 4.

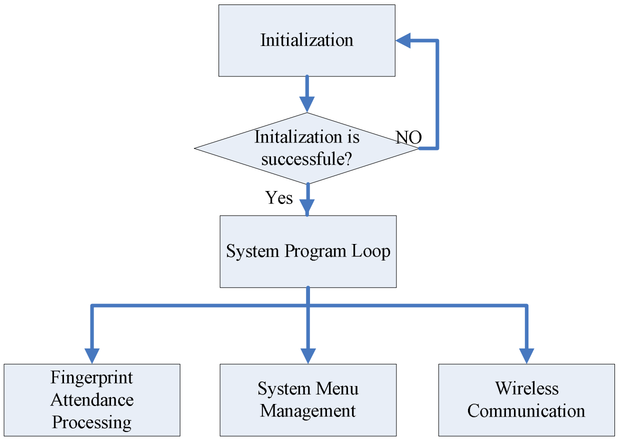

Fig.4 Flowchart of controlling software

System initialization including keyboard, LCD, serial port and PTR2000+ initial program is arranged firstly. Then system enters the program loop waiting for key down message and serial port interrupt. Attendances operations and system menu setting operations are carried out in keyboard processing program by the way of users or manager press keys to send keyboard interrupt message to system program. Operations of registering, deleting, modifying fingerprints are in the system setting menu.

Only manager has the right to enter system setting menu after verifying his/her fingerprints. System menu setting also includes time setting, bit rate of communication, styles of wireless communication and so on. All these programs are programming in C language.

3.2.2 Transmission Protocol Design

Uncertain outside factors may be occurred in wireless transmission such as electromagnetic interference, power and noise interference. So we must supply a wireless transmission protocol which can do error correcting and detecting effectively. The first thing of protocol is to identify noise and valid data. Often noise is raised with random bytes, so we can find some combinations of some fixed bytes to be the beginning of valid data packets. After testing, we find that the combination of 0xFF, 0xFF and 0x00 has low frequency in noise and we make this combination as the beginning of data packets to be transmitted and received. A simple protocol is designed like this:

[0xFF][0xFF][0x00][Packet Type][Data 0]… [Data n][Check Sum].

Packet type represents the data type of command or data. In this system, valid data transmitted by fingerprint attendance system include machine ID, users' ID, time of attending.

3.2.3 Design of Management Software on PC

Management software consists of communication interface DLL[10] and corresponding management setting program. Communication interface DLL charges the communication between wireless communication module and PC and management setting program is able to transmission data processing, information of stuff and shift managing, inquiry and print information of attendances.

4 Debugging and Implementation

In fingerprint verifying module debugging and implementation, we choose 300 fingerprints as samples of fingerprints verifying testing. There are totally 1200 times of matching, and the verification rate is 98.3%, the rejection rate is 9.2%. In wireless transmission testing, we find that there is much noise in data transmission and the transmission distance cannot reach ideal distance. To solve these problems, we adopt some measures as follows:

(1) add filter circuit to power to reduce power

interferences;

(2) CPU and PTR2000+ have separate power supply and oscillator is set near CPU;

(3) PCB divides into some partitions such as strong, weak signals zone, digital and analog zone;

(4) In software, transmission uses short data packets and adds delay time at interval time.

Results show that the phenomenon of data packets losing rarely occurs. Data transmission is steady and reliable and transmission distance satisfies system needs. Wireless transmission solves the shortcoming of this system that there must be a managing PC nearly and it is difficult to lay the transmission lines where topography is bad.

Attending people finish their attendances by pressing their fingerprints on sensor. This system can transmit users' attending records to managing PC in three modes: immediate, timing and response. And it can be an intelligence terminal receiving information such as a meeting notice as well. To avoid the data packets lost, manager can check attending records with the downloaded data copies via USB port. This system accomplishes these functions well.

The characters of this system are that single system not only completes its functions but also same systems can form a network. Figure 5 shows that a network formed by four such systems is implemented.

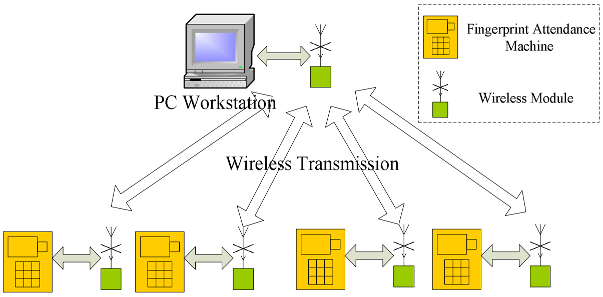

Fig.5 A network formed by four such systems

In such a network, PC receives data from each fingerprint attendance subsystem via wireless transmission channels and sends command to manage every subsystem uniformly. And they communicate with each other according to different machine ID of data packets.

5 Conclusions and Future Work

This paper describes the techniques used in a fingerprint verifying system and wireless transmission as well as an implement of such a system by means of a wireless fingerprint attendance management system. This system has the functions of fingerprint verifying, checking on attendances independently, wireless communication and so on. Comparing with magnetic card, IC card and wire fingerprint attendance management systems, it solve the problem of replacer punching card and the trouble of laying the transmission lines.

The performance of this system meets the needs of daily attendance management in various enterprises and institutions. It has good market prospects.

While the rapid development of chip and computer technologies, many new methods should be used in such system e.g. RFID technology and other biometrics technologies like retinal verifying to enhance the reliability of recognition and adopt new wireless technologies like GPRS to solve the problem of the bad quality transmission channel and so on.

References:

[1]Yoshiaki Isobe, *Development of Personal Authentication System Using Fingerprint with Digital Signature Technologies*, Proceedings of the 34th Hawaii International Conference on System Sciences, 2001, pp. 9 -15.

[2]Younhee Gil, *Access Control System with High Level Security Using Fingerprints*, IEEE the 32nd Applied Imagery Pattern Recognition Workshop (AIPR'03), 2003, pp. 238-243.

[3]Gwo-Cheng Chao, *Embedded Fingerprint Verification System*, IEEE the 2005 11th International Conference on Parallel and Distributed Systems (ICPADS'05)*,*Vol.2, 2005, pp. 52-57.

[4]Yang-Koo Kang, *Real-Time Fingerprints Recognition Mechanism-based Digital Contents Protection System for Interaction on the Web*, IEEE the 2001 Pacific Rim International Symposium on Dependable Computing (PRDC.01)*,* 2001, pp.304-307.

[5]Naslini K.Ratha, *An FPGA-based Point Pattern Matching Processor with Application to Fingerprint Matching*, the Computer Architectures for Machine Perception (CAMP '95). 1995, pp. 394-401

[6]D.Maltoni, D.Maio, A.k.Jain, S.Prabhakar, *Handbook of Fingerprint Recognition*, Springer, New York, 2003

[7]*FDA01 Developer's Guide*, SecuGen Co., DC1-0001B Rev B

[8]PTR2000 web site, http://www.xuntong.com

[9]Weisman, G.J., *The Essential Guide to RF and Wireless,* Prentice Hall, 2003

[10]Jianwei Gong, *Visual C++ / Turbo C serial port communication programming and implementation*, Electronics Industry, Beijing, 2004