Fingerprint Based Wireless Terminal for Driving License Verification

Prof. Priya Hankare, Rhythm Billore, Nikhil Deorukhakar , Pushkar Deshpande, Kunal Gandhi

***Abstract*— This paper provides the design method of wireless fingerprint based driving license verification system on ZigBee technology. The system includes terminal fingerprint acquisition, processing, wireless transmission, fingerprint matching, and verification process. The current system involves manual verification of license which is difficult to monitor. The issues of forgery of licenses of migrant people are a serious issue from the security point of view. The issues regarding the fake identity have been raised. In order to overcome such problems and to achieve the simple and high real-time system, we are proposing a low-cost and high-performance wireless driving license verification function, which provides a new wireless driving license system which will be helpful for traffic police and RTOs.**

***Index Terms*— Fingerprint identification, Fingerprint verification, Wireless communication, ZigBee technology**

I. INTRODUCTION

To start with the project it is essential to know the requirements and scope of the project. For a country comprising with almost one sixth of the global population keeping the track of each person is very essential. Developed countries like USA, England Germany etc. have implemented 24 hours traffic surveillance but the cost incurred is too high. Instead of that we can implement "Finger Print Based Wireless Terminal for Driving License Verification".

The fingerprint scanning is most convenient method and has a lot of advantages, such as its unique, permanent, good, anti-fake and easy to use. So it is recognized increasingly by people. Recently while **"ADHAR CARD"** was introduced the finger prints were collected. The data of fingerprints of each person is stored. So we have an advantage that the database is already available. The most prominent feature is that we can track the previous violations so that the data can be used while dealing with the situations like "High Alert". This Project Single handedly deals with the problems like "**Identity Theft"** and "**Document Forgery".**

The working conditions in which it is to be used creates most of the complications as we can't make the device delicate and bulky. So the wireless technology is used so that the device can be used as a handheld device which enhances its usability. For wireless communication we are using zigbee module. ZigBee technology is an emerging technology developed in recent years. Comparing with some existing wireless communication technologies, ZigBee is advantageous in terms of low-power and low-cost. It is very suitable for application to wireless sensor networks. With reliable wireless performance and battery operation, ZigBee gives you the freedom and flexibility to do more.The device if produced at larger scale will not be costly and will be compact enough to be handled easily.

Aiming at the disadvantages of traditional manual driving license verification system, a design method of wireless driving license verification system based on ZigBee technology is proposed. It achieves license verification by fingerprint identification. It is low-cost, low-power and provides high performance.

Manuscript received December 19, 2014.

Prof. Priya Hankare, Rhythm Billore, Nikhil Deorukhakar , Pushkar Deshpande, Kunal Gandhi, Department of Electronics and Telecommunication, K.J.Somaiya Institute of Engineering and Information Technology,Mumbai 400022,India

II. SYSTEM STRUCTURE

The system consists of Fingerprint acquisition module, Transmission and receiving module, Microcontroller and Database and driving license verification workstation. Fingerprint acquisition module is used to realize fingerprint collecting and pre-treatment. Transmitter and receiver ZigBee module is used to send the finger print image to computer. To control all these external devices along with LCD a microcontroller is used. Database and driving license verification workstation is used to store the pre-recorded finger prints and data related to those and realize fingerprint extraction and matching in order to verify the license. If the finger print scanned and some sample in the database matches, license is verified and data related will be displayed. If it doesn't match then the person is not licensed.

III. HARDWARE DESIGN

The system hardware includes: Fingerprint scanner, Microcontroller AT-89S52, 20x4 LCD, ZigBee module, Power supply.

A. Transmitter Block Diagram

This block consists of a finger print module that captures each person's fingerprint as data. The sensor forms the core part of the fingerprint module.

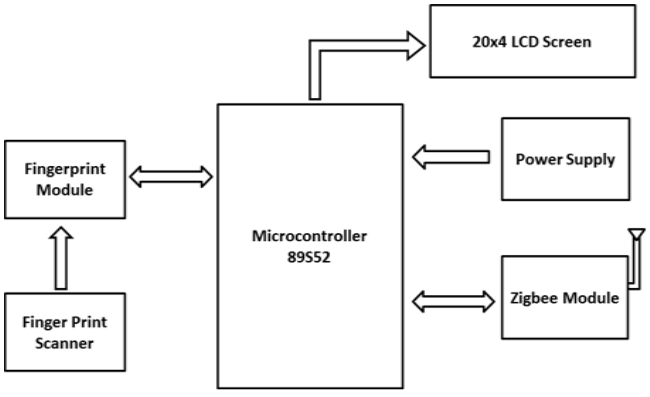

Figure 1: Block Digram

This in turn is connected to a AT-89S52 microcontroller using RS 232 via fingerprint module which provides an interface between the two devices and provides a uniqueID to each data. The microcontroller stores the captured data and sends through the ZigBee transmitter module for further processing.

B. Receiver Block Diagram

The unique id of the captured data is received by the Zigbee receiver module. Fingerprint data will already be stored in central database. Unique id received by the other zigbee module will be compared with one already stored in the data base. If the match is found then data related to that unique id will be transmitted back.

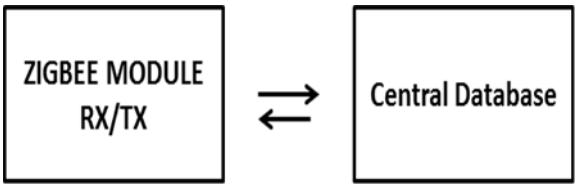

Figure 2: Receiver Block Diagram

When it is received back by the ZigBee module on transmitter side it is passed to the Microcontroller. Microcontroller then displays the verified message along with the data related to that fingerprint on 20x4 LCD.

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. Currently, 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 swiped vertically over the sensor window. It requires no external heat, light or radio source. It is 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. ZigBee has a self healing network. 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

The microcontroller 89S52 proved to be most suitable of all the available processors because of its features. It has 8kb RAM and 256 bytes of ROM. 3 timers and 32 I/O pins makes it easy to use and more appropriate. There are 8 interrupt sources available. There is no need to interface any extra memory which makes it more efficient and practical. Microcontroller plays most crucial part as it handles major operations related to interfacing and controlling the peripheral devices.

G. MAX 232

Max RS 232 is a standard serial port device which is being used in order to remove the problem faced for interfacing at transmitter and receiver port of microcontroller. Since microcontroller has only two ports ,one being transmitter end and other a receiver end and we have to interface zigbee as well as fingerprint module with it. Hence to remove the ambiguity of signal transmission and reception there is need to use this device.

IV. CONCLUSION

Thus the developed system provides wireless driving license verification with fingerprint acquisition and verification through ZigBee. It can automatically realize functions such as information acquisition of fingerprint, processing, wireless transmission, fingerprint matching, and driving license verification. In order to achieve the simple and high real-time system, it realized low-cost and high-performance wireless driving license verification function, which provided a new wireless driving license verification system.

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 ∓ 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 ElectronicTechnique, 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.