BIOMETRIC AUTHENICATION BASED VEHICULAR SAFETY SYSTEM USING ARM PROCESSOR.

CH.SURENDRA KUMAR[1]
PG scholar, Dept. of ECE
PBR VITS,KAVALI,NELLORE,INDIA
Email: surichakkirala@gmail.com

A SUMAN KUMAR REDDY[2]
ASSOCIATE PROFESSOR, Dept of ECE
PBR VITS,KAVALI,NELLORE,INDIA
Email: suman.vits@gmail.com

J. RAJ PRAVEEN[3]
ASSISTANT PROFESSOR, Dept of ECE
SVCN,NELLORE,INDIA
Email: rajpraveenece@gmail.com

***Abstract*: In vehicle security system, the objective is to prevent the theft of vehicle and ensure safe driving. One level of ensuring authentication of driving is through finger print recognition system that authenticates a user being an authorized person to have access to the ignition system. In this work we propose a multi level authentication for vehicles. In this system, the finger print image of the eligible driver will be programmed into a smart card and this card along with real time finger print scanner is employed to authenticate the driver. If there is no match between the image stored in smart card and the real time image acquired by finger print scanner vehicles ignition system will stay in OFF state. While issuing the license, the specific person's fingerprint is to be stored in the card. Automobiles are equipped with a card reader capable of reading the particular license. The same vehicle should have the facility of biometric reader device.**

Keywords: Vehicle security, Finger prints detection, authorization, smart card.

I. Introduction

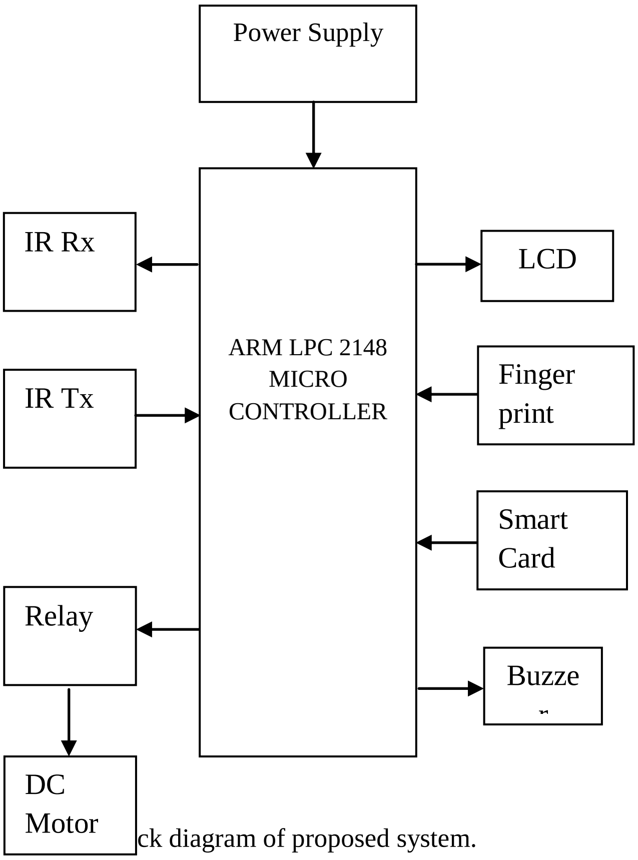
Vehicle usage became important everywhere in the world and also preventing it from theft is required. Automobile manufacturers are incorporating security features into their products by introducing advanced automated technologies to avoid the thefts particularly in case of cars. Security features are provided by Biometric and non-biometric methods. Sometimes security systems fail due to hacked password and encryption of decrypted data, but it is almost impossible to make duplicate of distinctive characteristics. Biometric systems are modern and techniques like fingerprint recognition, iris recognition and facial recognition are becoming popular. Of these, fingers print recognition and detection systems are easy to deploy, sophisticated and persons can be identified without their knowledge.

In vehicle security system, the objective is to prevent the theft of vehicle and ensure safety of vehicle by avoiding the means of theft. One level of ensuring authentication of driving is through finger print recognition system that authenticates a user being an authorized person to have access to the ignition system. Biometric identification based security systems are considered to be the most secure especially due to their ability to identify people with minimal ambiguity[1]. It uses a finger print detection and recognition system that identifies and verifies a person automatically by extracting unique features from an image. Fortunately, automated biometrics in general can provide a much more accurate and reliable user authentication method and fingerprint recognition is widely used. Identifying a person based on his or her physiological characteristics is the key factor of biometric recognition.

II. Proposed system

The proposed system was developed using LPC 2148 microcontroller based on ARM 7 architecture, finger print recognition module, smart card and proximity sensor. The smart card consists of finger print of the authorized driver. If this smart card is inserted into the vehicles security system only then the driver's authenticity will be verified by the system and will be allowed to drive the vehicle. In the prototype developed we used a relay and a motor to replace the conventional ignition system. Once the driver's identity is verified the system will perform check on seat belt safety. The seat belt safety system is incorporated with proximity sensor. So the output from the IR module will be read by ARM processor and ignition will be given access through relay. Thus a multi level safety system will help in authorized use of vehicle.

The block diagram of the system is as shown in the figure (1)



ck diagram of proposed system.

The modules of the proposed system are explained below:

a. Finger print recognition module:

This bio metric device is capable of storing physical images in binary form. Later the binary versions can be used to authenticate the user.

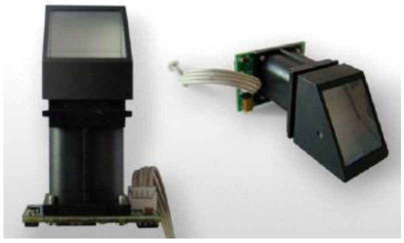


Fig2; finger print recognition module

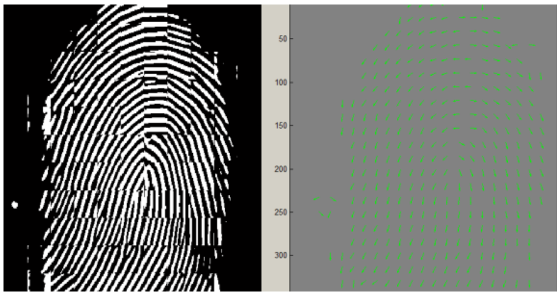


Fig3: template showing image stored inside a smart card.

It features with the SEA/RSA accelerator engines, the embedded non-volatile memory (Flash/OTP), the fingerprint processing accelerator and its algorithm firmware. Cordis 5+ is the 32-bit RISC core which is featured with 16-/32-bit ISA and Harvard bus architecture. The Enhanced DSP instruction extensions are supported by this core system. In addition, a 5-stage pipeline is used to increase the amount of parallel processing, giving the most performance out of each clock cycle. It is suitable for System on Chip (SOC) products targeted at consumer electronics, networking infrastructure, automotive and other price-sensitive markets. The image of synochip[5] is shown in the fig (2).

b. Smart card reader:

There are different types of biometric identification methods employed in access control like fingerprint recognition [2], facial recognition. Biometric identification technology has been promoted for its ability to significantly increase the security level of systems. All biometric identification devices work similarly, by comparing the template stored in its flash memory to the real-time scan obtained during the process of identification. If there is a high or enough degree of probability that the template in the memory is compatible match with the live scan (the scan belongs to the authorized person), the identification details of that person are sent to a control panel, here an LCD module. The control panel consisting of ARM 2148 processor [3] then checks the permission level of the user and determines whether access should be allowed to ignition system. Smart cards are of two types: contact dependent and contactless. Both have an embedded microprocessor/controller and memory. The smart card differs from the proximity card. Proximity card has only one function: to provide the reader with the card's identification number.

The difference between the two types of smart cards is the manner with which the microprocessor on the card communicates with the external world. Licenses are replaced with these smart cards[4]. A contact dependent smart card must physically touch the contacts on the reader to transfer information between them. Since contact cards must be inserted into readers proper care must be taken to insert in the proper orientation and nominal speed. Such a transaction is not acceptable for most access control applications. The use of contact smart cards as physical access control is limited mostly to vehicle parking zone applications when payment data is stored in card memory and when the speed of transactions is not a key performance factor.

A contactless smart card uses the radio-based technology and the frequency band used it uses is a higher frequency (13.56 MHz instead of 125 kHz), which allows the transfer of large amount data, and multi point communication with several cards at the same time. A contactless card does not have to touch or get in contact with the reader or even be taken out of a wallet. Most access control systems only read serial numbers of contactless smart cards and available memory is not utilized. This memory is used for storing biometric data (i.e. fingerprint template, iris pattern) of a user. In such case a biometric reader first reads the template on the smartcard and then compares it to the finger print (hand, eye, etc.) presented by the user. In this way biometric data of users does not have to be distributed or networked and stored in the memory of controllers or readers, which simplifies the system and reduces memory requirements.

III. System architecture

The system consists of smart card reader, controller module, seat belt sensing module, ignition system module and the smart card which is inserted into the system by the user. A fingerprint match causes the data pins to be in a high logic level and ideally output about 5volts while a fingerprint mismatch makes the data pins to be in a low logic level and ideally output 0volts. An interface control circuit was constructed to link the ignition system of a vehicle with the host processor through relay. This circuit provides a high degree of electrical isolation between the PC and the ignition system which operate at different voltage levels.

Table 1: operational behaviour of proposed system

Input	Expected output
Place smart card	Read contents of card and prompt to place finger on module.
Swipe your finger on the biometric module	Compares the real time scan with image stored in smart card and display result on LCD
If Lcd shows authorized user, then fasten your seat belt.	The IR module shows a low so buzzer will be off, if seat belt is not tied then buzzer will be high.
Then user is allowed to access ignition control of vehicle.	Motor will be powered up through relay.

a. ARM 7 LPC 2148:

ARM 7 LPC2148 is a 32-bit microcontroller. It offers high performance and very low power consumption. The architecture of ARM is based on RISC (Reduced Instruction Set Computer) principles. The instruction set and related decode mechanism are simpler than those of complex instruction set computers. This results in very high throughput and real-time interrupt response becomes impressive from a small and cost effective core. . It is especially used in portable devices due to its low power consumption and reasonable performance features.

1. ARM 7 microcontrollers comes in a tiny LQFP64 package with 16/32 bits.
2. On-chip static RAM of 8 to 40 kB and on-chip flash memory of 32 to 512 kB with 12b bit wide interface/accelerator

which enables a high-speed 60 MHz operation.
3. In System Programming/In Application Programming (ISP/IAP) is possible through an on-chip boot loader software.
4. The operating voltage range of CPU is 3 to 3.6V with 5V tolerant I/O pads.
5. Power saving mode with idle and power down.
6. A total of 21 external interrupt pins are available.
7. A maximum clock frequency of 60 MHz is available for CPU from a programmable on-chip PLL with 100 µs settling time.
8. A total of 45 fast general purpose I/O pins which are tolerant up to 5V are available.

IV. Results

The following figure explains the status of developed system on power up. The finger print recognition system starts scanning the smart card first and later it compares real time finger print from the user. If the matching algorithm gives a match between stored image and current image, then system gives control over the ignition system. It also ensures safety by including a seat belt warning system using proximity sensor.

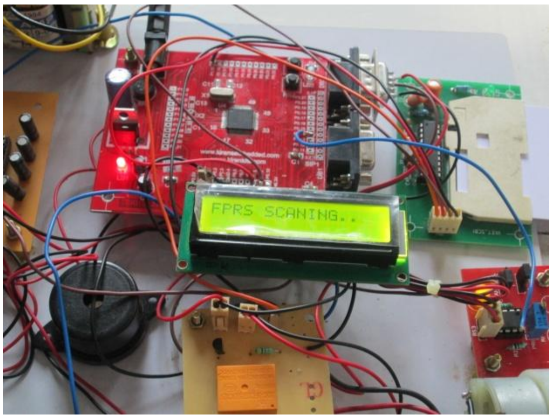


Fig4: security system scanning inputs to perform match.

V. Conclusion and future scope

The developed system ensures that only authorized drivers can drive the vehicle and misuse of vehicles by others can be prevented. The system also provides facility for monitoring seat belt status. It also gives time to get the system repaired if any malfunction exists. The system makes sure that vehicle's access is given to only authorize personal and thus accidents can also be averted. The developed prototype serves as an impetus to drive future research, geared towards developing a more robust and embedded real-time fingerprint based ignition systems in vehicles.

The present module can be extended to including a GSM-GPS module for additional safety so that even if the vehicle is stolen by trespassing the security module we can relocate the vehicle using satellite coordination.

References:

1. Priya Darshini.V "Multilevel Security System for Automotives using RFID and Biometric Techniques in LabVIEW", International Journal of Advanced Research in Electrical, Electronics and Instrumentation EngineeringVol. 2, Issue 4, April 2013
2. Anil Jain, Arun Ross and Salil Prabhakar, "Fingerprint Matching Using Minutiae And Texture Features," Fingerprint Matching Using Minutiae And Texture Features", in Proc. of Int'l Conference on Image Processing (ICIP), pp.282-285, Thessaloniki, Greece, Oct 7 - 10, 2001
3. www.nxp.com/lpc_2148
4. Rubella, J.A. "Fingerprint based license checking for auto-mobiles" Advanced Computing (ICoAC), 2012 Fourth International Conference
5. www.synochip.com/en