International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.2, No.10, October 2013 DOI:10.15693/ijaist/2013.v2i10.6-10

ARM Based Monitoring and Controlling of Bank Security System

K.Nagarajan1, P.Kumar 2 and M.Mohammed kasim 3

Assistant Professor, Dept of ECE,

Nehru Institute of Engineering and Technology, Coimbatore, Tamilnadu. India

Abstract

In today's real time modern industrialized world security systems place a vital role. This bank Security system is a prime concern in our day-today life. Now a day's everyone wants to be as much secure as possible. IR based security is a low cost, so that the concept is implemented by using ARM TDMI Processor. The system is fully controlled by the ARM processor which has a 4Kbytes of ROM for the program memory. The system has an IR transmitter and IR receiver. When somebody enters in to bank then the buzzer will be on. ARM processor continuously monitor the infrared receivers, when any object pass through the IR receiver's then the IR rays falling on the receiver's are obstructed this obstruction is sensed by the microcontroller. The implementation is made simpler by using IR sensor to detect the person or track the person. The system includes the IR sensor, microcontroller, LCD display, buzzer and 5V power is supplied to operate the system. The system uses a compact circuitry built around ARM processor program are developed in Embedded C. Flash magic is used for loading program into ARM TDMI PROCESSOR. In this system, ARM TDMI PROCESSOR continuously monitors the sensors of the biometric system (iris scanner and vein detector), the keypad for the authenticated code i.e. unique password and registered identification number, and the output of wireless motion detector. The wireless motion detector will be active during nights and if any variation occurs in its output, it will be sensed by the and alert sound ARM processor will be given by it.

Index Terms- *Security System, Biometrics, Authentication, Iris Scanner, Unique Password*

1.1 INTRODUCTION

The present system of security is not very efficient as it can be easily faked by the smart larceners as they can get hold of the keys or the passwords. Also it's a painstaking job for the administration of the banks to keep an account of the locker activities as there is no dedicated employee appointed for this. To get rid of these issues, bank security system like this one is needed which does not require any manual presence of the officer. This also reduces the waiting time of the customers. When any new customer wants to open a bank locker, they are supposed to get there iris scan and vein recognition scan done. They are also given a unique password and another password is any registered proof like the driving license number, passport number, voter id number or any other government authorized proof is also made of.

They are also supposed to give alternatives to all the above samples so that it can be used to access the lockers in case of any mishap. The motion detector which functions in night helps in safeguarding the locker area for any theft furthermore. Biometrics (or biometric authentication) refers to the identification of humans by their characteristics or traits. Computer science, biometrics to be specific, is used as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance.Biometricidentifiersarethedistinctive, measurable characteristics used to label and describe individuals. The first time an individual uses a biometric system is called enrolment. During the enrolment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrolment. Biometrics working system can be written in steps as. a) An enrolment is done by capturing and storing the data of any individual in the form of templates. b) Templates are stocked for future verifications. c) If any user wants to be authenticated, he again scans his iris or vein and hence generating new template. This is compared with the other stored templates. d) After this, the comparison is rated and if it crosses the threshold level then they are authenticated or else it gives one more try.

2. TECHNOLOGIES USED

2.1 Iris Scanner

A vein Iris scanning may seem to be something which is very innovative but it's a simple CCD (Charge Coupled Device) digital camera which uses visible and near-infrared light to capture a clear, high-contrast picture of a person's iris. The use of near-infrared light is to differentiate the pupil and iris of a person as a person's pupil is very black, making it easy for the computer. When we look into an iris scanner, the camera, which is 3 to 10 from your eyes, takes a picture, the computer locates: a) The centre of the pupil b) The edge of the pupil c) The edge of the iris d) The eyelids and eyelashes, then analyzes the patterns in the iris and translates them into a template Iris scanners are becoming a source of authentication of any individual as everyone has unique eyes. There are more than 200 reference points stored in every template for comparison. Though the iris is visible its protected, and does not change with time. In most cases, people's eyes even remain unchanged post an eye surgery. Even the blind people (with irises) can use this facility. Also, the presence of eyeglasses or contact lenses does not cause interference. The hardware part of wireless iris recognition system is made up of iris recognition verifying module, microcontroller, power module, real-time clock module, and LCD display module. Figure 1 shows the architecture of hardware design. ARM TDMI Processor is interfaced using RS232 interface in the form of transmitting and receiving data packet with the output of the CPU. The power module supplies the necessary power and makes sure that the system is functional even when the available power is less. The real time clock module satisfies the accuracy of the time needed for the database purpose. The LCD display tells if the authentication is confirmed or not. The leads to the next arm proceesorlevel even if the validation fails.

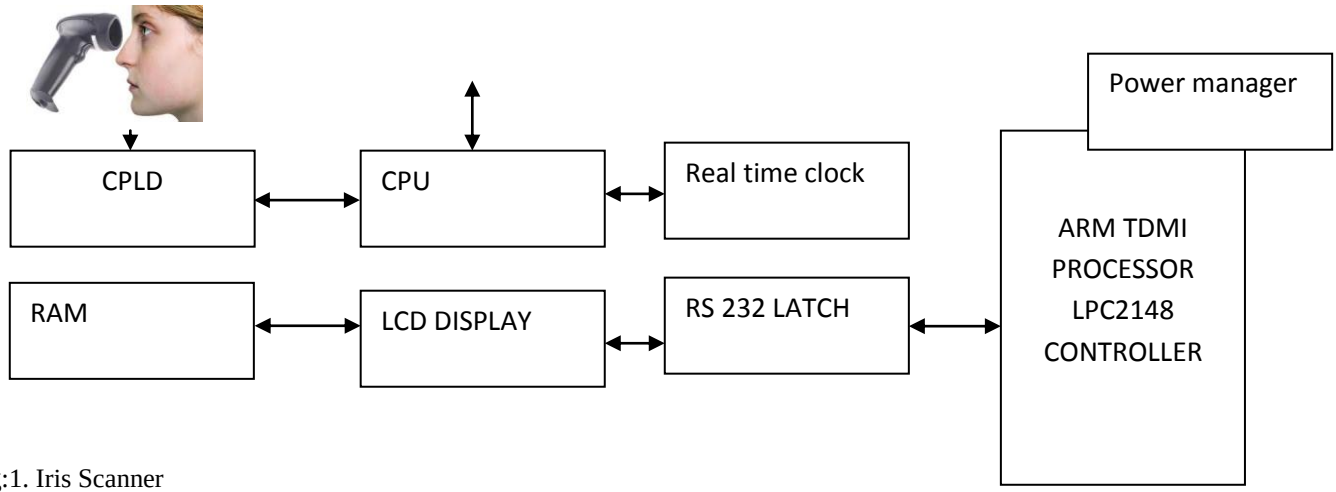

Fig:1. Iris Scanner

2.2.Vein Detector

As mentioned in case of irises, every individual's veins are completely distinctive. Even the twins don't have identical veins. The right and left sides of any individual's veins are also different. Most of the veins are not visible through the skin, and hence can't be simply forged or fiddled with. Similar to to the case of iris, their shape does not change with age. In this system, you can use your finger, wrist, palm or the back of your hand to scan. The near-infrared light is used by the camera to capture the image. The light is absorbed by the haemoglobin and the veins appear to be black in picture. This The hardware architecture consists of a Near-infrared Camera which is a device intended for capturing of the veins patterns. They are processed for verification by the CPU by the Complex Programming Logic Design (CPLD).

The device consists of an illumination unit with infrared diodes (recommended wavelengths are around 900 nm), a digital signal processor is attached for video pre-processing and image enhancement and processing. Then, there is a ARM TDMI PROCESSOR to control the peripherals. The memory is present to store the enciphered templates. When a limb is placed in its nearby region of the led source, it radiates the infrared rays on the hand and then the IR camera captures the image of veins and then stores them. Figure.2 shows the architectural arrangement.

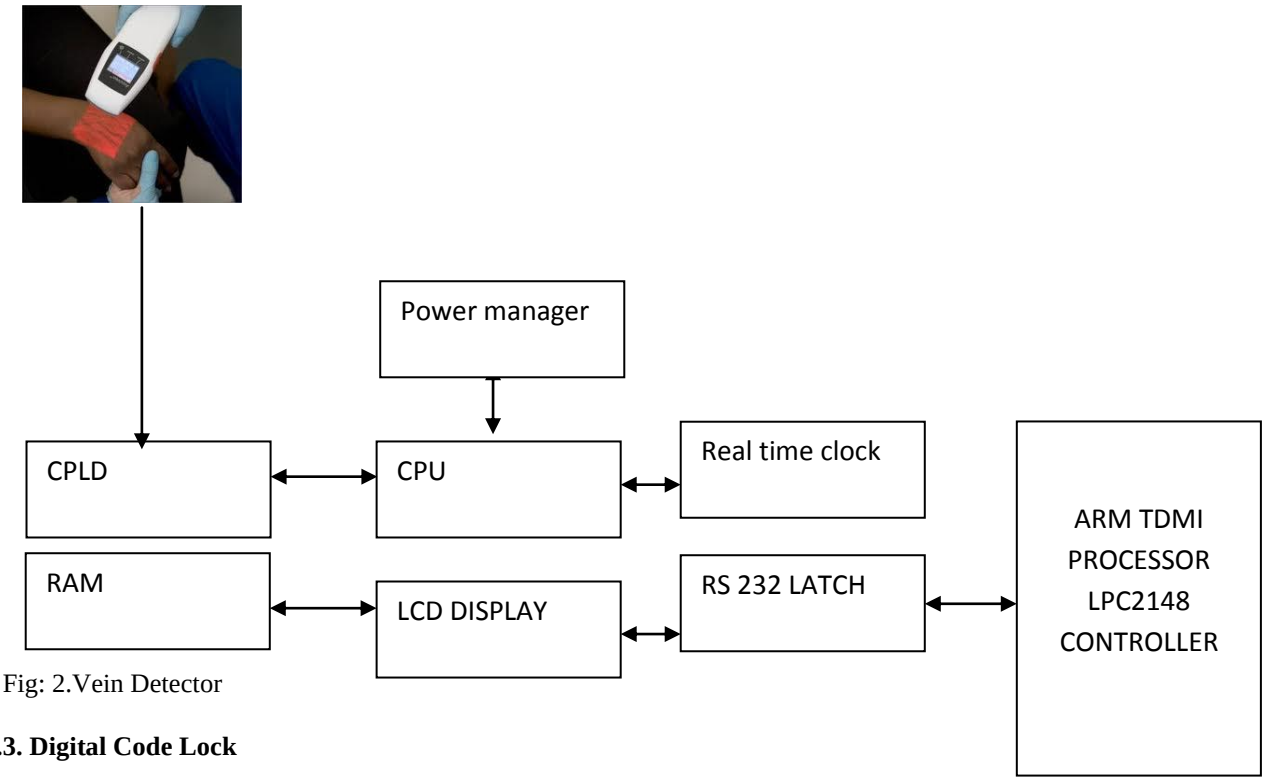

Fig: 2.Vein Detector

2.3. Digital Code Lock

This is a lock which unlike the above two is not common to the locker cluster. It's individually installed at the door of every locker. This is a ARM TDMI Processor based digital lock system which gets open if the right password is entered. The password is numeric without any characters. The password of 6 numbers is mandatory. This lock is interfaced with the ARM TDMI Processor and has a memory with it for the storage of password. The whole system is not so expensive and hence can be installed at every locker. This will authenticate the person and will act as a medium to lead the locker holder to the next level of validation. This will be issued to the holder when they opt for the locker and can be changed only by the authorized bank officials after their validation is done. There are three trials given, if the validation is not done then the system gives in danger signal and the authentication fails. This lock consists of a LCD screen, keyboard and an ARM TDMI Processor. The keyboard consist of 12 keys (4*3) from 1,2,3,4,5,6,7,8,9,*,0,# and is used to input the password. Where * is used to delete one single digit. When 6 digit passwords are being entered, #is pressed to submit that password. LCD screen is used for display. Here LCD is used to show the typed digits and to acts as an interface between the ARM TDMI PROCESSOR and the user. The architecture has been shown in figure picture is used to create a template which is stored and then compared whenever required.

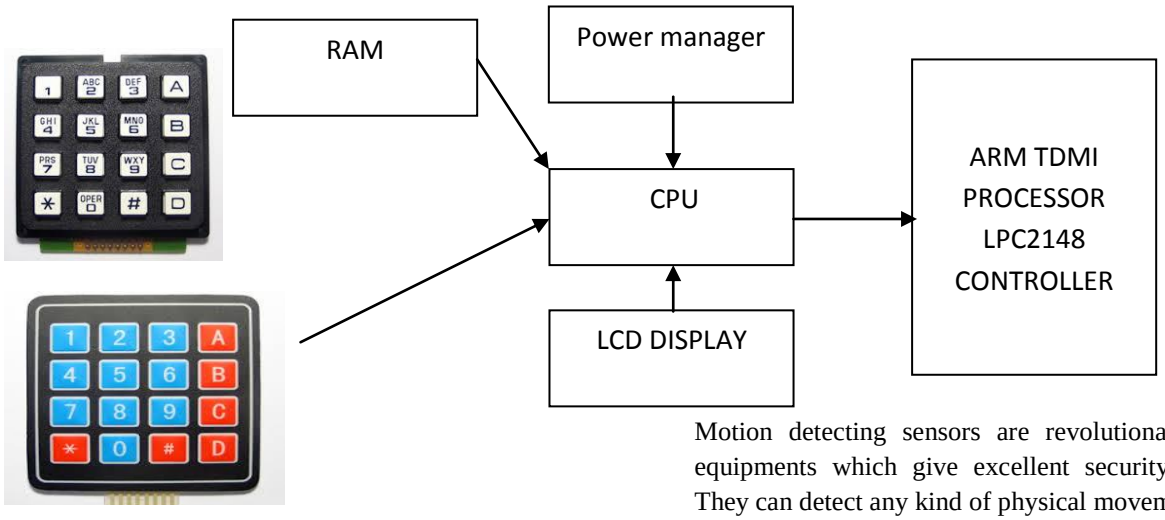

Fig: 3.Digital Code Lock

2.4. Identification Number

Quiet similar to the above digital code lock, it works on the same principle. This is the only thing which identifies the user as the registered nationalist as the password here is the government registered identification number. It can be anything driving license, passport, voter id, PAN card or any other proof. This is the same as the one used for the identification purpose while opening an account or a locker. This is set by the bank administration after verification. This is the last step of authentication, after this the locker can be accessed. This is an alphanumeric key and the number of characters depends on the proof used. This again gives you three chances to validate yourself and access the locker. After the trials are given, any further entry will give siren to the bank officials. The hardware is the same as in the above digital clock just with the presence of an alphanumeric keypad instead of a numeric one.

2.5. Wireless Motion Detector

Motion detecting sensors are revolutionary security equipments which give excellent security to banks. They can detect any kind of physical movement in their environs and can elicit alarm with the help of infrared heat sensors. The crystals, which show piezoelectric effect i.e. if they encounter any slightest change in the infrared radiations in the form of heat they generate current on their surface, are the material which are used as thermal sensors. Every human body emits infrared radiation which is approximately 9.4 micrometer in wavelength. Hence, motion of any human results in changes in local infrared radiation pattern in the vicinity of the sensor. With the use of 'Fresnel lens', the radiation can be focused on the sensor. As this is made to function only in night there is no possibility that any sunlight related temperature changes triggers the response of a motion sensor unnecessarily.

Wireless motion detector consists of arm processor and PIR sensor module. PIR sensor is a 3 pin connector: VCC, output and ground. Whenever a motion is sensed, its voltage reaches its peak. ARM TDMI PROCESSOR manages the voltage of collector of the transistor. During normal conditions, transistor is cut off and collector voltage at its high. When the motion is sensed, the high output from the sensor module saturates the transistor and the voltage at the collector drops down to logic low and the alarm is switched on.

3. Flow of Control

The bank locker has a series of equipments. Once the person enters the locker area, he/she has to undergo four authentication tests. First among them is the iris scan. In this test the iris of the person is scanned using a special machine, which compares the iris with the scanned records stored at the time of opening of the account. After this, the next step is vein detection. Every person has a unique vein position and this detector would compare present vein template with the stored templates. If none of these two tests are cleared then the alarm would be raised. But if any one of the authentication tests is being cleared then the next step is the digital code lock in which a person has to enter a unique code which is given to every account holder during the opening of an account. The final step is the number in the registered identification card. One has to

select the identification proof which was submitted during the opening of an account and the matching code has to be entered.

All the final outputs of these equipments are interfaced with an arm processor which checks for authentication. Out of the four levels if any three outputs are validated the locker opens. This is very helpful in many ways. In case, a person fails to bring his registered identification number or has lost his possession, he can still manage to open the locker if the other three authentications are positive. Similarly, if someone is unable to validate the first two scans, an alarm is raised by the system. The wireless motion detector is programmed in such a way that it works after the bank's closing hour till the time the bank opens. It can even work on specific days when the bank is off. The alarm system is designed in such a way that it gives alarm not only to the security officials in the bank but to the local police station as well. If anyone tries to enter into the range of the wireless motion detectors, an alarm is sent to the security official, nearby police station and the top bank officials. In this manner, the bank lockers ensure foolproof security.

4. Conclusion

This is a real time application based paper which tells that there is a need to bring in a revolution in the bank locker security system by making the procedure a little easy and more systematic for the bank officials. This is just a proposed model which when implemented would surely give a very good protection of the lockers curbing theft and making the lockers more reliable. The assurance it will give to the bank customers will force them to use it and hence protect their valuables from theft or any kind of robbery. This not aims at easing the work load of the bank official but also makes it a easy and comfortable process for its users, the general public. As
this is protected by the vicinity sensor hence can detect any unwanted or forced entry inside the bank locker area and can protect the lockers n the lockers in the most efficient way.

REFERENCE

[1] http://en.wikipedia.org/wiki/Biometrics
[2] http://science.howstuffworks.com/biometrics4.htm
[3] http://science.howstuffworks.com/biometrics5.htm
[4]http://www.buzzle.com/articles/motion-sensors-wireless motion-detectors.html
[5] http://www.trendhunter.com/photos/42881/3
[6]http://aumkw.academia.edu/SeifedineKadry/Papers/793786/Wireless_attendance_management_system_based_on_iris_recognition
[7] http://www.sersc.org/journals/IJBSBT/vol1_no1/2.pdf
[8]http://www.engineersgarage.com/microcontroller/8051projects/electronic-code-lock-with-password-using-at89c51-circuit
[9] http://www.futurlec.com/Keypads.shtml
[10] http://embedded-lab.com/blog/?p=1334
[11] http://www.microchip.com/forums/m580847.aspx
[12] Ani1 K. Jain, Arun Ross, and Sharath Pankanti, “A Prototype Hand Geometly-based Verification System,” Proc. of 2nd Int. Conf. on Audio- and Video-based Biometric Person Authentication, Washington D.C., pp.166-171, March 22-24, 1999.
[13] Daugman, John (2003). "The importance of being random: statistical principles of iris recognition" (PDF). Pattern Recognition 36 (2): –291. doi:10.1016/S0031 - 3203(02)00030-4
[14] Daugman, John (2003). "The importance of being random: statistical principles of iris recognition" (PDF). Pattern Recognition 36 (2): 279–291. doi:10.1016/S0031-3203(02)00030-4