Research Journal of Pharmaceutical, Biological and Chemical Sciences

High secure finger vein authentication system for ATM.

Kumaresan R, Senthilkumar S, and Karthick C*.

Department of ECE, Sathyabama University, Chennai, Tamil Nadu, India

ABSTRACT

In this paper, Finger vein recognition is a method of biometric authentication that uses pattern recognition techniques based on images of human finger vein patterns beneath the skin's surface. Finger vein recognition is one of many forms of biometrics used to identify individuals and verify their identity. Finger Vein ID is a biometric authentication system that matches the vascular pattern in an individual's finger to previously obtain data. The technology is currently in use or development for a wide variety of applications, including credit card authentication, automobile security, employee time and attendance tracking, computer and network authentication, end point security and automated teller machines. The demand for simple, convenient, and high security authentication systems for protecting private information's stored in mobile devices has steadily increased with the development of consumer electronics. The personal information's can be protected in the form of biometrics which uses human physiological or behavioural features for personal identification. In our proposed system, the Real Time Embedded Finger Vein Recognition System using template matching and Implementation using Matlab shows that the finger vein authentication system performs well for user identification.

Keywords: biometric, microcontroller, MATLAB, figure vein, security system, personal computer.

*Corresponding author

INTRODUCTION

Finger vein biometric authentication is a recent identification system in this modern era. This technology is used for wide variety of applications including credit card authentication, automobile security, employee time and attendance tracking, computer and network authentication, and so on [1].

Currently, passwords, Personal Identification Numbers (4-digit PIN numbers) or identification cards are used for personal identification. However, cards can be stolen, and passwords and numbers can be guessed or forgotten. To solve these problems, biometric authentication technology which identifies people by their unique biological information is attracting attention. Biometrics can be defined as recognizing and identifying a person based on physiological or behavioral characteristics. In biometric authentication, an account holder's

Body characteristics or behaviors (habits) are registered in a database and then compared with others who may try to access that account to see if the attempt is legitimate. Fujitsu has researched and developed biometric authentication technology focusing on the methods: fingerprints, faces, voiceprints.

Biometrics studies commonly include fingerprint, face, iris, voice, signature, and hand geometry recognition and verification. Many other modalities are in various stages of development and assessment. Among these available biometric traits fingerprint proves to be one of the best traits providing good mismatch ratio, high accurate in terms of security and also reliable. The present scenario to operate a bank locker is with locks which are having keys. By this we can't say that we are going to provide good security to our lockers. To provide perfect security and to make our work easier, we are taking the help of two different technologies viz. embedded systems and biometrics. An Embedded system is a multi-agent system and computer system designed for specific control functions within a larger system, often with real-time computing constraints. Embedded systems contain processing cores that are either microcontrollers or digital signal processors (DSP).The key characteristic, however, is being dedicated to handle a particular task. Since the embedded system is dedicated to specific tasks, design engineers can optimize it to reduce the size and cost of the product and increase the reliability and performance. Some embedded systems are mass-produced, benefiting from economies of scale. Firstly discussing about Biometrics we are concentrating on Fingerprint scanning. For this we are using R303A as a scanner. This module has in-built ROM, DSP and RAM. In this we can store up to 100 user's fingerprints. This module can operate in 2 modes they are Master mode and User mode. We will be using Master mode to register the fingerprints which will be stored in the ROM present on the scanner with a unique id.

IDENTIFICATION NUMBER

Identification number is the only thing which identifies the user as the registered nationalist as the password, government registered identification number 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. After verification it is set by the bank administration. This is the last step of authentication, after this the locker can be accessed. An alphanumeric key and the number of characters depend on the proof used. This gives three chances to validate the user and access the locker. After the trials are given, any further entry will give alarm to the bank officials. Finger Vein ID is a biometric authentication system that matches the vascular pattern in an individual's finger to previously obtained data. Hitachi developed and patented a finger vein ID system in 2005.[1] The technology is currently in use or development for a wide variety of applications, including credit card authentication, automobile security, employee time and attendance tracking, computer and network authentication, end point security and automated teller machines.[citation needed]

To obtain the pattern for the database record, an individual inserts a finger into an attester terminal containing a near-infrared LED (light- emitting diode) light and a monochrome CCD (charge-coupled device) camera. The hemoglobin in the blood absorbs near-infrared LED light, which makes the vein system appear as a dark pattern of lines. The camera records the image and the raw data is digitized, certified and sent to a database of registered images. For authentication purposes, the finger is scanned as before and the data is sent to the database of registered images for comparison. The authentication process takes less than two seconds

DIGITAL CODE LOCK (Anil K. Jain, Arun Ross and Salil Prabhakar,2004)

Digital Code Lock is a lock which is individually installed at the door of every locker. This is a microcontroller 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 microcontroller 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 a microcontroller 8051.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 microcontroller and the user. Unlike the use of above forms of authentication such as passwords, tokens or digital code lock, biometric recognition provides a strong link between an individual and a claimed identity. It is very difficult to perform the type of check without the use of biometrics [2].

BIOMETRICS (R and Mary Lourde Dushyant Khosla, 2010)

The term "Biometrics" is derived from the Greek words bio (life) and metric (to measure). Biometrics can be defined as recognizing and identifying a person based on physiological or behavioral characteristics. Biometrics is becoming an interesting topic now in regards to computer and network security. However the ideas of biometrics have been around for many years[3].

SIGNATURE IDENTIFICATION (Anil k. Jain, Ling Hong, Sharath Pankanti, Ruud Bolle, 2008)

Signature identification is the analyses of the way a user signs his or her name. The process used by a biometric system to verify a signature is called dynamic signature verification (DSV). The angle at which the pen is held, the number of times the pen is lifted, the time it takes to write the entire signature, the pressure exerted by the person while signing, the variations in the speed with which different parts of the signature are written. Advantages are, Unique for every individual and user himself can decide the identity, lesser false acceptance rate, relatively cheap technology, No expert training required. Disadvantages are signature of a person may change after a long time like if an user gone through an accident and he cannot use his hand and then he signs after a long time, his sign and pressure points may change, High false rejection rate Pressure points may change because of weather or some disease. System can be fooled by imitating Profile Database [11].

VOICE RECOGNITION (D.Shekar and Goud and Ishaq Md and PJ. Saritha, 2012)

Voice recognition is the Identification using the acoustic features of speech that have been found to differ between individuals. Advantages are Easy to use and require no special training or equipment, relatively inexpensive compared to other biometrics and Consumers prefer to use voiceprints over other biometric technology for identification according to a Chase bank's research study. In computer science and electrical engineering, speech recognition (SR) is the translation of spoken words into text. It is also known as "automatic speech recognition" (ASR), "computer speech recognition", or just "speech to text" Disadvantages are When processing a person's voice over multiple channels such a microphone and then over a telephone reduces the recognition rate, Physical conditions of the voice such as those due to sickness, affect the voice verification process, Environment noise reduces the overall accuracy and effectiveness of the recognition, The storage requirement for voiceprint database can be very large, a person's voice changes over time[6]

FACE RECOGNITION (Dr. V. Vaidehi, K. Gayathri ,S. Vignesh,2011)

Face recognition uses the visible physical structure of the face and analyses the spatial geometry of distinguishing features in it identify an individual. Facial recognition systems have a higher relative unit cost, they do offer increased accuracy levels. Inherently the technology has a number of advantages, most notably, that it is readily acceptable by the public and relatively easy to integrate with other security systems,

particularly CCTV. But development work still needs to be done to improve its performance. It needs to make allowance for the changes that occur to the human face over time - aging, facial hair, skin tone, glasses, etc. All of which could impede the recognition software. And technically, the effect of prevailing light conditions and the angle of the image need to be reduced, thereby allowing faster and more accurate processing [10].

IRIS SCAN (Pramila D Kamble and Dr. Bharti W. Gawali, 2012)

The iris is the colored ring of textured tissue that surrounds the pupil of the eye. Advantages are very high accuracy, verification time is generally less than 5 seconds, the eye from a dead person would deteriorate too fast to be useful, so no extra precautions have to been taken with retinal scans to be sure the user is a living human being. Disadvantages are Intrusive, a lot of memory for the data to be stored, Very expensive, difficult to use because of positioning eye requires more time for matching with database stored. Canadian airports started using iris scan in 2005 to screen pilots and airport workers. Pilots were worried about the possibility that repeated scans would negatively affect their vision, and Performance can be affected by certain eye problems, such as cataracts, and if the user is wearing colored contact lenses or sunglasses and these are the drawbacks[5].
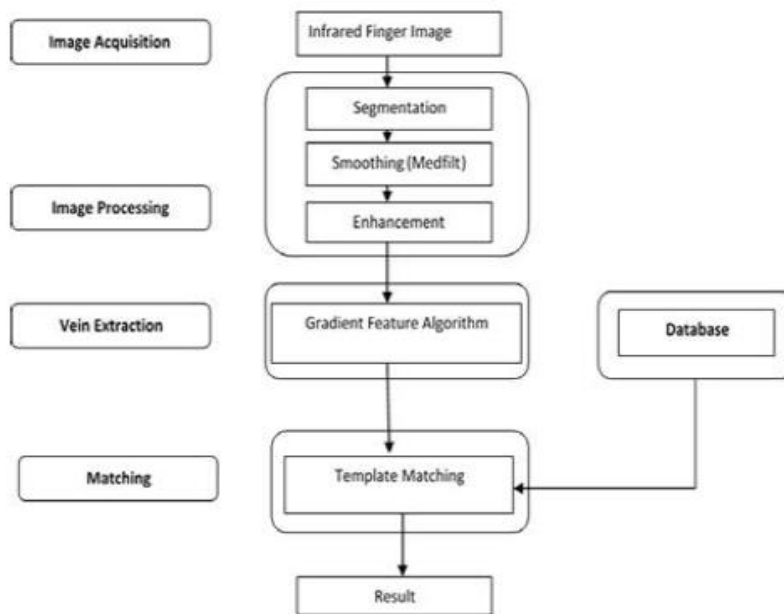

Fig 1 . Finger Print security system[12]

FINGERPRINT TECHNOLOGY (Sagar S. Palsodkar, Prof S.B Patil,2014)

In the 1890s, an anthropologist named Alphonse Bertillon sought to fix the problem of identifying convicted criminals and turned biometrics into a distinct field of study. He developed 'Bertillon age', a method of bodily measurement which got named after him. The problem with identifying repeated offenders was that the criminals often gave different aliases each time they were arrested. Bertillon realize d that even if names changed, even if a person cut his hair or put on weight, certain elements of the body remained fixed, such as the size of the skull or the length of their fingers. His system was used by police authorities throughout the world, until it quickly faded when it was discovered that some people shared the same measurements and based on the measurements alone, two people could get treated as one. After this, the police used finger printing, which was developed by Richard Edward Henry of Scotland Yard, instead. Essentially reverting to the same methods used by the Chinese for years. There are many steps in the history of fingerprinting as a way to identify criminals [12].

BLOCK DIAGRAM OF FINGERVEIN BASED SECURITY SYSTEM (PROPOSED SYSTEM)

The block diagram mainly consists of PIC16F877A MCU, Finger Vein Module, Encoder, Decoder, GSM, RF transmitter and Receiver, Driver unit, Alarm and LCD display.
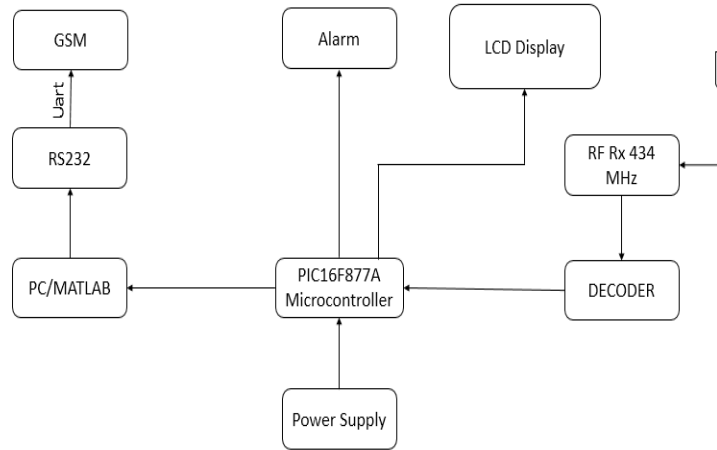
Fig 2: Finger vein security system

HARDWARE EXPLANATION

ENCODER (HT-12E)

We can establish a serial communication between the modules or we can go for encoders at the Tx unit and a decoder at the Rx unit These are 12 bit encoder and decoder pair available .8bits are assigned for address and 4 bits are for data. There are other pairs available like HT640 encoder, HT648L decoder (10 bit for address and 8 bit for data).but in Indian market it is hard to find these two. but (HT12E & D) are available every ware. The pin diagram of the ICs will be as follows
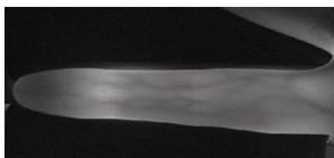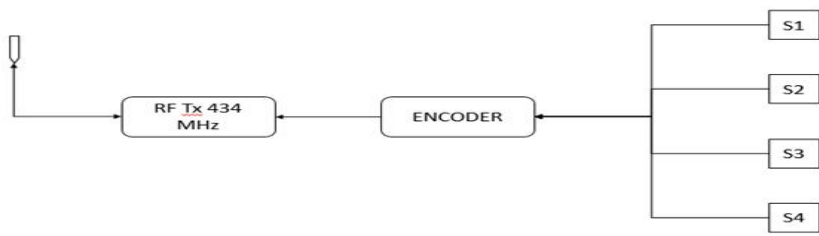
Fig 2.2 Finger Vein recognition block

DECODER (HT-12D)

The decoder having 18 PIN DIP with Operating Voltage of 2.4V ~ 12.0V The CMOS Technology is used in the decoder chips with Low Power and High Noise Immunity and Low Stand by Current

RF TRANSMITTER

Radio Frequency, any frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space. Many wireless technologies are based on RF field propagation. Radio Frequency: The 10 kHz to 300 GHz frequency range that can be used for wireless communication. Also used generally to refer to the radio signal generated by the system transmitter, or to energy present from other sources that may be picked up by a wireless receiver. The TWS-434 extremely small, and are excellent for applications requiring short-range RF remote controls.

RF RECEIVER

RWS-434: The receiver also operates at 433.92MHz, and has a sensitivity of 3uV. The WS-434 receiver operates from 4.5 to 5.5 volts-DC, and has both linear and digital outputs. The RF module, as the name suggests, operates at Radio Frequency. Transmission through RF is better than IR (infrared) because of many reasons. Firstly, signals through RF can travel through larger distances making it suitable for long range applications. Also, while IR mostly operates in line-of-sight mode, RF signals can travel even when there is an obstruction between transmitter & receiver .This RF module comprises of an RF Transmitter and an RF Receiver. The transmitter/receiver (Tx/Rx) pair operates at a frequency of 434 MHz. An RF transmitter receives serial data and transmits it wirelessly through RF through its antenna connected at pin4. The transmission occurs at the rate of 1Kbps - 10Kbps.The transmitted data is received by an RF receiver operating at the same frequency as that of the transmitter.

GSM & LCD:

GSM modems can be a quick and efficient way to get started with SMS, because a special subscription to an SMS service provider is not required As explained earlier (refer GSM interfacing with 8051), a line converter MAX232 is employed to convert the RS232 logic data of GSM Module to TTL logic so that it can be processed by the microcontroller. In this project, instead of RS232 logic data, TTL logic output has been taken and thus PIC16F877A has been directly connected with GSM Modem without any line converter in between. The following diagram shows the TTL input and output of GSM modem used.

This is the pin diagram of a 16×2 Character LCD display. As in all devices it also has two inputs to give power Vcc and GND. Voltage at VEE determines the Contrast of the display. A 10K potentiometer whose fixed ends are connected to Vcc, GND and variable end is connected to VEE can be used to adjust contrast. A microcontroller needs to send two information's to operate this LCD module, Data and Commands. Data represents the ASCII value (8 bits) of the character to be displayed and Command determines the other operations of LCD such as position to be displayed.

RS232 & ALARM:

The RS-232 is placed to work in the low power shutdown mode. The system will shut down whenever the RS-232 device is not used. The auto shutdown pulse will shut itself down whenever there is not any activity on the signal for 30sec. It means that whenever a transceiver is connected to the RS-232 port but it is not sending data. The Pin 2 and Pin 3 are used for transmitting and receiving the data. The Pin 5 is used to connect to ground. The Max 232 device is used to communicate with the DTE and DCE devices through RS-232 cable.

The switches are interfaced to a microcontroller of PIC16F family, when a certain number of switches are pressed which exceeds the predefined number then microcontroller generates an output to switch on a buzzer alerting the authorities about a possible stampede. The status is also displayed on the LCD which is duly interfaced to the microcontroller.

SOFTWARE EXPLANATION

MPLAB:

MPLAB® X IDE is a software program that runs on a PC (Windows®, Mac OS®, Linux®) to develop applications for Microchip microcontrollers and digital signal controllers. It is called an Integrated Development Environment (IDE), because it provides a single integrated "environment" to develop code for embedded microcontrollers.

MPLAB® X Integrated Development Environment brings many changes to the PIC® microcontroller development tool chain. Unlike previous versions of the MPLAB® IDE which were developed completely in-house, MPLAB® X IDE is based on the open source Net Beans IDE from Oracle. Taking this path has allowed us to add many frequently requested features very quickly and easily, while also providing us with a much more extensible architecture to bring you even more new features in the future.

CONCLUSION

In this paper, we presented a finger-vein based biometric security system that can be used for security based electronic devices. The method can extract the finger-vein feature for recognition from the NIR images. This method uses single sample and is convenient to the application. This work can be extended with increasing the database for further verification.

SURVEY COMPARISON

Author	Description
(Anil K. Jain, Arun Ross and Salil Prabhakar	Biometric(iris) Recognition is used to security system, It is difficult to do for multiple times
R Mary Lourde Dushyant Khosla	Fingerprint Identification in Biometric Security Systems. Security less device
Anil k. Jain, Ling Hong, Sharath Pankanti, Ruud Bolle	A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger
D.Shekar and Goud and Ishaq Md and PJ.Saritha	A facial recognition system, a computer application for automatically identifying a person from a digital image or a video frame from a video source
Dr. V. Vaidehi, K. Gayathri *S. Vignesh	face detection and recognition using block independent component analysis and clustering. Not secure for high end applications
Pramila D Kamble and Dr. Bharti W. Gawali	Fingerprint Verification of ATM Security System.it uses security less communication
Sagar S. Palsodkar, Prof S.B Patil	Biometric and GSM Based Security for lockers.it is having signal problem

REFERENCES

[1]   Lee H, S. H. Lee, T. Kim, and H. Bahn, "Secure User Identification for Consumer Electronics Devices", IEEE Transactions on Consumer Electronics, Vol. 54, No. 4, pp. 1798-1802, Nov. 2008.
[2]   Anil K. Jain, Arun Ross and Salil Prabhakar "An Introduction to Biometric Recognition" IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, no. 1, January 2004.
[3]   R Mary Lourde Dushyant Khosla "Fingerprint Identification in Biometric Security Systems" International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010.
[4]   Ravi. J K. B. Raja Venugopal.K.R "fingerprint recognition using minutia score matching". International Journal of Engineering Science and Technology Volume: 1(2), 2009, 35-42.
[5]   Pramila D Kamble and Dr. Bharti W. Gawali "Fingerprint Verification of ATM Security System by Using Biometric and Hybridization" International Journal of Scientific and Research Publications, Volume 2, Issue 11, November 2012.
[6]   D.Shekar and Goud and Ishaq Md and PJ. Saritha "A Secured Approach for Authentication System using Fingerprint and Iris" Global Journal of Advanced Engineering Technologies, Volume 1,Issue 3-2012.
[7]   Umut Uludag, Sharath Pankanti, Salil Prabhakar, Anil K. Jain "Biometric Cryptosystems: Issues and Challenges" IEEE, Vol. 92, no. 6, June 2004.

[8]   R. Rasu P. Krishna Kumar, M. Chandraman "Security for ATM Terminal Using Various Recognition Systems" International Journal of Engineering and Innovative Technology (IJEIT)Volume 2, Issue 4, October 2012.

[9]   P. Viola, M. Jones. "Rapid object detection using a Boosted cascade of simple features". In : IEEE Conference on Computer Vision and Pattern Recognition, pp. 511-518, 2001.

[10]   V. Vaidehi, K. Gayathri *S. Vignesh "Efficient face detection and recognition using block independent component analysis and clustering IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011.

[11]   Anil k. Jain, Ling Hong, Sharath Pankanti, Ruud Bolle "An Identity-Authentication System using Fingerprints" .IEEE Vol.85 No.9 September 2008.

[12]   Sagar S. Palsodkar, Prof S.B Patil "Biometric and GSM Based Security for lockers "International Journal of Engineering Research and Application ISSN: 2248-9622, Vol.4, December2014.