BIOMETRIC HIGH SECURE AND COST EFFECTIVE FINGER VEIN AUTHENTICATION SYSTEM FOR ATM

Karthick C., Kumaresan R. and Senthilkumar S.
Department of Electronics and Communication Engineering, Sathyabama University, Chennai, India
E-Mail:karthivlsi13@gmail.com

ABSTRACT

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, Finger Vein Recognition System using template matching and Implementation using Matlab shows that the finger vein authentication system offers the following adverse features such as cost effective and more secure and accurate level of authentication to performs well for user identification.

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

1. 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.

1.1. Digital code lock

(Anil K. Jain, Arun Ross and SalilPrabhakar, 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].

1.2. Biometrics

(R and Mary LourdeDushyantKhosla, 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].

1.3. 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].

1.4. 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].

1.5. Fingerprint technology (existing system)

(Sagar S. Palsodkar, Prof S.BPatil, 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 authoritiesthroughout the world, until it quickly faded when itwas discovered that some people shared the samemeasurements and based on the measurements alone,two people could get treated as one. After this, thepolice used finger printing, which was developed byRichard Edward Henry of Scotland Yard, instead.Essentially reverting to the same methods used by theChinese for years. There are many steps in the historyof fingerprinting as a way to identify criminals [12].

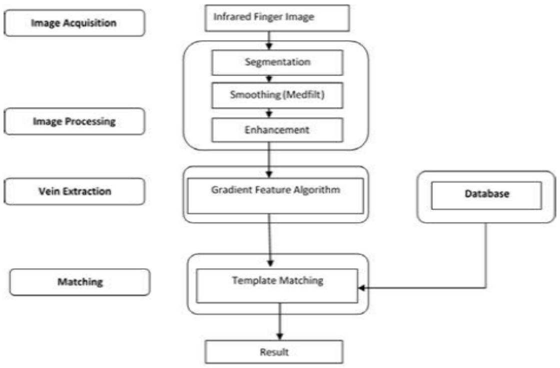


Figure-1. Finger print security system [12].

EXISTING RESULT

Figure-2 shows the hardware setup for Existing system. It has been demonstrated successfully using FIM3030 (Finger print scanner) and LPC2148 (ARM7 Microcontroller).

A subset of fingerprint impressions acquired with various sensors was provided to registered participants, to allow them to adjust the parameters of their algorithms

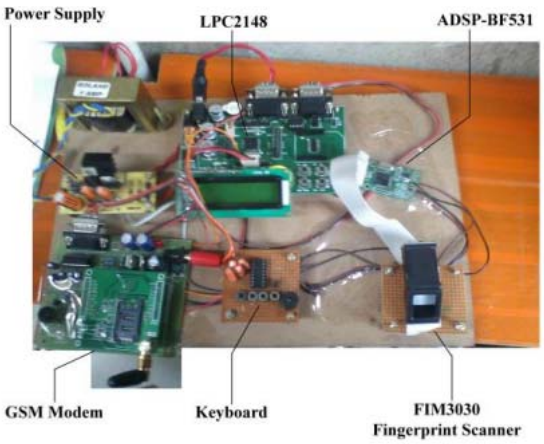


Figure-2. Hardware setup developed for the existing system.

2. PROPOSED SYSTEM

2.1. Block diagram of fingervein based security system

Figure-3 shows the block diagram of Finger vein secuity system. It mainly consists of PIC16F877A MCU, Finger Vein Module, Encoder, Decoder, GSM, RF transmitter and Receiver, Alarm and LCD display description are given below.

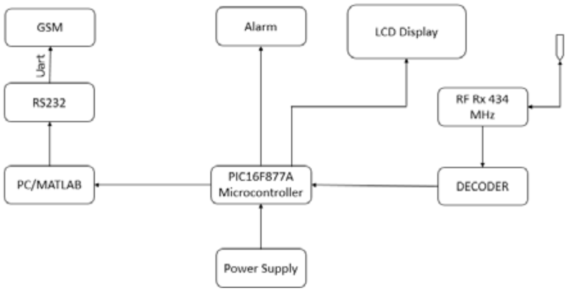
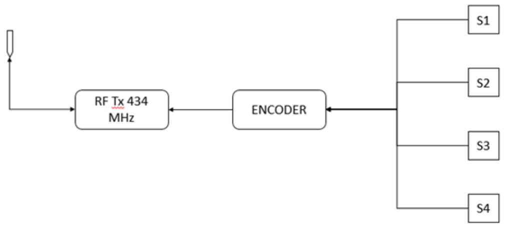


Figure-3. Finger vein security system [13].

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, HT648Ldecoder (10 bit for address and 8 bit for data).but in Indian market it is hard to find these two. but (HT12E and D) are available every ware the pin diagram of the ICs will be as follows



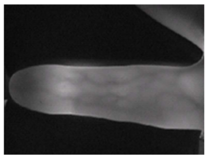


Figure-4. Finger vein recognition block[13].

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.

RFTransmitter

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.

RFReceiver

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.

GSMand 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 andalarm

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

Discrete wavelets transform

The discrete wavelet transform (DWT) is a linear transformation that operates on a data vector whose length is an integer power of two, transforming it into a numerically different vector of the same length. It is a tool that separates data into different frequency components, and then studies each component with resolution matched to its scale. DWT is computed with a cascade of filtering's followed by a factor 2 subsampling

DWT tree

H and L denotes high and low-pass filters respectively,

Elements aj are used for next step (scale) of the transform and elements dj, called wavelet coefficients, determine output of the transform. l[n] and h[n] are coefficients of low and high-pas filters respectively One can assume that on scale j+1 there is only half from number of a and d elements on scale j. This causes that DWT can be done until only two aj elements remain in the analyzed signal these elements are called scaling function coefficients.DWT algorithm for two-dimensional pictures is similar.

The main feature of DWT is multi scale representation of function. By using the wavelets, given function can be analyzed at various levels of resolution. The DWT is also invertible and can be orthogonal. Wavelets seem to be effective for analysis of textures recorded with different resolution. It is very important problem in NMR imaging, because high-resolution images require long time of acquisition. This causes an increase of artifacts caused by patient movements, which should be avoided. There is an expectation that the proposed approach will provide a tool for fast, low resolution NMR medical diagnostic.

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.

PROPOSED RESULT

Figure-5shows the hardware setup for proposed system. It has been demonstrated successfully using Finger vein scanner and Microcontroller PIC16F877A.The average times required for feature extraction and matching in our system are 343ms and 13ms, respectively. For the whole system, plus the time for image capturing, the time required for the authentication of a user is less than 0.8 s. Although the feature extraction in our system is a little bit more complicated than that in Song's method (finger print), our system achieves an EER (Equal Error Rate) of 0.07%, indicating that our method significantly outperforms previous methods.

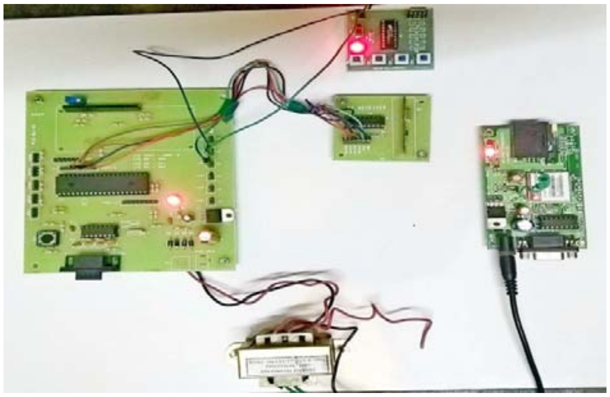


Figure-5. Hardware setup developed for the proposed system.

Biometric	Accuracy	Size of template	Cost	Security level	Stability
Finger vein (proposed)	High	Medium	Low	High	High
Finger print (Existing)	Medium	Small	High	Low	Low

CONCLUSIONS

In this paper, we presented a finger-vein based low cost effective and more secure and accurate level of biometric 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.

REFERENCES

[1] Lee H, S. H. Lee, T. Kim, and H. Bahn. 2008. Secure User Identification for Consumer Electronics Devices. IEEE Transactions on Consumer Electronics. 54(4): 1798-1802.

[2] Anil K. Jain, Arun Ross and SalilPrabhakar. 2004. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology. 14(1).

[3] R Mary LourdeDushyantKhosla. 2010. Fingerprint Identification in Biometric Security Systems. International Journal of Computer and Electrical Engineering. 2(5).

[4] Ravi. J K. B. Raja Venugopal.K.R. 2009. Fingerprint recognition using minutia score matching. International Journal of Engineering Science and Technology. 1(2): 35-42.

[5] Pramila D Kamble and Dr.Bharti W. Gawali. 2012. Fingerprint Verification of ATM Security System by Using Biometric and Hybridization. International Journal of Scientific and Research Publications. 2(11).

[6] D.Shekar and Goud and IshaqMd and PJ. Saritha. 2012. A Secured Approach for Authentication System using Fingerprint and Iris” Global Journal of Advanced Engineering Technologies. 1(3).

[7] UmutUludag, SharathPankanti, SalilPrabhakar, Anil K. Jain. 2004. Biometric Cryptosystems: Issues and Challenges. IEEE. 92(6).

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

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

[10] Dr. V. Vaidehi, K. GayathriS. Vignesh. 2011. Efficient face detection and recognition using block independent component analysis and clustering IEEE-International Conference on Recent Trends in Information Technology, ICRTIT2011.

[11] Anil k. Jain, Ling Hong, SharathPankanti, Ruud Bolle. 2008. An Identity-Authentication System using Fingerprints. IEEE. 85(9).

[12] Sagar S. Palsodkar, Prof S.BPatil. 2014. Biometric and GSM Based Security for lockers. International Journal of Engineering Research and Application ISSN: 2248-9622, Vol.4.

[13] Kumaresan R, Senthilkumar S, Karthick C. Highsecure finger vein authentication system for ATM. Research Journal of Pharmaceutical. Biological and Chemical Sciences (RJPBCS), ISSN: 0975-8585.