

An Embedded Real-Time Finger-Vein Recognition System for Security Levels

T.Y,V Bhanu kiranmai

P.G Student.

8498906127

K .Amruthavally

Associate Professor

G.Harish

Assistant Professor

tupakula.balu@gmail.com, katary.amrutha@gmail.com, bobbyharish440@email.com

Abstract— In this project, we propose a real-time embedded finger-vein recognition system (FVRS) for authentication on mobile devices. The system is implemented on an embedded platform and equipped with a novel finger-vein recognition algorithm. The proposed system consists of four hardware modules: radio frequency identification system, image acquisition module, embedded main board, and human machine communication module. RFID module will start the very initial communication between the user and the device. The image acquisition module is used to collect finger-vein images. The Embedded main board including the Microcontroller chip, memory (flash), and communication port is used to execute the finger-vein recognition algorithm and communicate with the peripheral device. The human machine communication module (LED or keyboard) is used to display recognition results and receive inputs from users.

Keywords— *Finger vein recognition system, RFID module, Embedded platform, communication module, image acquisition module*

INTRODUCTION

Today, security is very much essential in all kind of activities. Illegal activities are happening in every place today. So government and corporate sections are concentrating mainly on the security levels with their every invention. This will bring privacy all over the world. So in a thought of bringing privacy through security level[2], this project has been developed. This FVR system mainly uses three divisions which are image acquisition module, embedded main board, and human machine communication module. Each unit is having its own major role over the project. In this paper, two major areas have been focused. Those are authentication[5] and identification. FVR system performs the authentication function with the finger vein recognition. Every time when the user is going to use the system, the finger vein will be scanned and comparison will be done.

Finger vein recognition is very effective when compared with pattern recognition, pin number security the other type of Biometric[1] security methods like finger print security, palm print security, image scanning and some recognition techniques. FVR system uses the vein scanning. As it is related to the biological factor, it is very difficult to change the vein information of a user. So, this system can provide more security[3] than any other security level. In this FVR system, we are focusing on high security[4] with RFID technology. Initially each and every user will be given with one RFID secret card. This will make an effective initial communication between the user and the device. This technique will make the device to extract the user information from its memory.

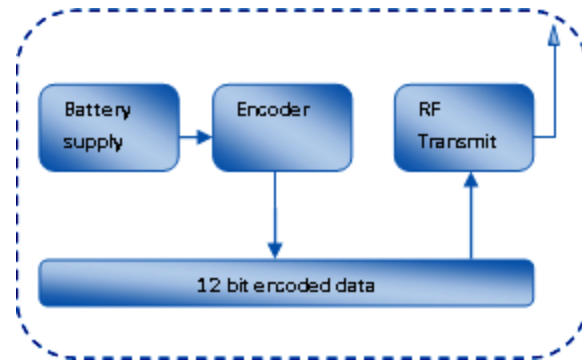


Figure 1 will illustrates this feature.

Figure 1: FVRS – Active secret card section

In FVR system, the RFID module is used to collect the user data base. With this system, an unique code will be generated for each and every user for storing the finger vein[9] details in the server. Here an active RFID technology is used for creating the secret signal. The encoded signal will be continuously transmitted by the card if it is in on state. This RFID will reduce the complexity of the image acquisition module. As the RFID have an unique signal it can store only one vein information. So authentication and identification will become soon. Because of these features the FVRS will be a faster recognition system.

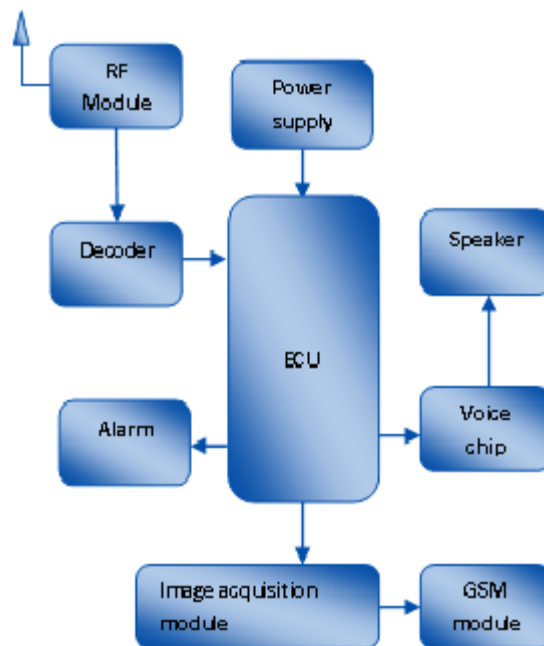


Figure 2: FVRS – ATM Recognition unit

In this section, RF receiver module is attached with the embedded control unit. This unit receives the secret digital data from the card and it will be given to the controller. In the FVRS recognition unit, vein images will be stored in the image acquisition module. If RF receiver receives any digital code, then automatically code verification will be done inside the embedded control unit. If the code is matched then an asynchronous command will be given to the image acquisition[10] module. Then the vein image comparison will be done inside the processor. If the image is matched then automatically the device will go to its working state.

To this ECU further we have interfaced a GSM module. With this module we can develop the password system. When any access has been there means automatically an intimation will be given to the controlling authority. The unit will send a password with this intimation. It will make a very effective security to the user. This password will be working for one time. It will play an effective authentication process. This mobile GSM communication module will not only send the intimation for authorise but also for unauthorised.

DESIGN AND IMPLEMENTATION

This project is implemented in an effective way to improve the security. Initially an active RF method is used to provide a basic security and to initialize the communication between the FVRS mobile device and the user. For a user single card will be provided. This card contains a digital data which will acts as a key to the image recognition unit. The FVRS – mobile recognition unit first checks the address bits from the transmitter section. If address is matched then the corresponding data signal will be passed to the controller unit. Through this method identification of the user will be implemented effectively. Now the controller unit will send a signal to the image acquisition unit to open the data base vein detail.

Image acquisition unit will process the user's vein image with the database image. This will work through different image processing techniques. For an easy identification alert system is also embedded in this unit. If any mismatch is found then automatically the ECU will alert the entire system continuously. At the same time intimation will be given to the users security number. This intimation is common for authentication. If anything happens in the FVRS - Mobile recognition unit, then the corresponding result will be transferred to the security number without any delay. If the vein image is matched in the image acquisition module then, a secret password will be send to the security number of the user. The user should enter the particular password for further accessing. This will bring more security to the user.

OVERVIEW OF THE FVRS UNIT

The FVRS – Mobile unit has the following important module section. Those are radio frequency identification system, image acquisition module, embedded main board, and human machine communication module. These sections which will play the important role.

In the existing method, there is a long list of available biometric patterns[8], and many such systems have been developed and implemented, including those for the face, iris, fingerprint, palmprint, hand shape, voice, signature, and gait. Notwithstanding this great and increasing variety of biometrics patterns, no biometric has yet been developed that is perfectly reliable or secure. For example, fingerprints and palm prints are usually frayed; voice, signatures, hand shapes and iris images are easily forged; face recognition can be made difficult by occlusions or face-lifts and biometrics, such as fingerprints and iris and face recognition, are susceptible to spoofing attacks, that is, the biometric identifiers can be copied and used to create artefacts that can deceive many currently available biometric devices.

In this Proposed FVRS – Mobile recognition unit, Finger vein[6] recognition unit is used. The finger-vein is a promising biometric pattern for personal identification in terms of its security and convenience. The vein is hidden inside the body and is mostly invisible to human eyes, so it is difficult to forge or steal. The non-invasive and contactless capture of finger-veins ensures both convenience and hygiene for the user, and is thus more acceptable. The finger-vein pattern[7] can only be taken from a live body. Therefore, it is a natural and convincing proof that the subject whose finger-vein is successfully captured is alive.

SYSTEM HARDWARE

ARM Processor:

The ARM7 family includes the ARM7TDMI, ARM7TDMI-S, ARM720T, and ARM7EJ-S processors. The ARM7TDMI core is the industry's most widely used 32-bit embedded RISC microprocessor solution. Optimized for cost and power-sensitive applications, the ARM7TDMI solution provides the low power consumption, small size, and high performance needed in portable, embedded applications. The ARM7TDMI core uses a three-stage pipeline to increase the flow of instructions to the processor. This

allows multiple simultaneous operations to take place and continuous operation of the processing and memory systems. As the processor is having a high speed it is easy to make the communication between the RF module and the Image acquisition module

Operating modes

The ARM7TDMI core has seven modes of operation:

- User mode is the usual program execution state
- Interrupt (IRQ) mode is used for general purpose interrupt handling
- Supervisor mode is a protected mode for the operating system
- Abort mode is entered after a data or instruction pre fetch abort.
The interrupt setting of ARM supports the DHLS to response to the interrupt coming from the server section.

Interrupt controller

The Vectored Interrupt Controller (VIC) accepts all of the interrupt request inputs from the home server section and categorizes them as Fast Interrupt Request (FIQ), vectored Interrupt Request (IRQ), and non-vectored IRQ as defined by programmable settings. These interrupt settings will give a quick response to the RF decoder. So that address verification will be very faster and signal for image processing will be given to the image acquisition module.

Wireless communication:

RF communication:

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

Transmitter:

The TWS-434 extremely small, and are excellent for applications requiring short-range RF remote controls. The TWS-434 modules do not incorporate internal encoding. If simple control or status signals such as button presses or switch closures want to send, consider using an encoder and decoder IC set that takes care of all encoding, error checking, and decoding functions

The transmitter output is up to 8mW at 433.92MHz with a range of approximately 400 foot (open area) outdoors. Indoors, the range is approximately 200 foot, and will go through most walls.



Figure 3: RF Transmitter

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.

A 0 volt to Vcc data output is available on pins. This output is normally used to drive a digital decoder IC or a microprocessor which is performing the data decoding. The receiver's output will only transition when valid data is present. In instances, when no carrier is present the output will remain low.

The RWS-434 modules do not incorporate internal decoding. If you want to receive Simple control or status signals such as button presses or switch closes, you can use the encoder and decoder IC set described above. Decoders with momentary and latched outputs are available



Figure 4: RF receiver

GSM

A GSM modem is a wireless modem that works with a GSM wireless network. Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication. GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard that would formulate specifications for a pan-European mobile cellular radio system operating at 900 MHz

GSM provides recommendations, not requirements. The GSM specifications define the functions and interface requirements in detail but do not address the hardware. The reason for this is to limit the designers as little as possible but still to make it possible for the operators to buy equipment from different suppliers. The GSM network is divided into three major systems: the switching system (SS), the base station system (BSS), and the operation and support system (OSS). The basic GSM network elements are shown in below figure.

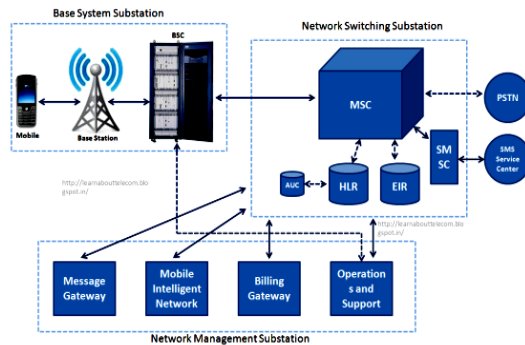


Figure 5: GSM network Topology

GSM modems support an extended set of AT commands. These extended AT commands are defined in the GSM standards. With the extended AT commands, you can do things like:

- ❖ Reading, writing and deleting SMS messages.
- ❖ Sending SMS messages.
- ❖ Monitoring the signal strength.
- ❖ Monitoring the charging status and charge level of the battery.
- ❖ Reading, writing and searching phone book entries.

Sending the message :

To send the SMS message, type the following command:

```
AT+CMGS="+31638740161" <ENTER>
```

Replace the above phone number with your own cell phone number. The modem will respond with:

```
> (Response from the modem)
```

You can now type the message text and send the message using the <CTRL>-<Z> key combination:

```
Hello World ! <CTRL-Z>
```

Here CTRL-Z is keyword for sending an sms through the mobile device. After some seconds the modem will respond with the message ID of the message, indicating that the message was sent correctly:

IMAGE AQUITION

A [color model](#) is an abstract mathematical model describing the way [colors](#) can be represented as [tuples](#) of numbers, typically as three or four values *color components* (e.g. [RGB](#) and [CMYK](#) are color models). However, a color model with no associated mapping function to an [absolute color space](#) is a more or less arbitrary color system with no connection to any globally understood system of color interpretation.

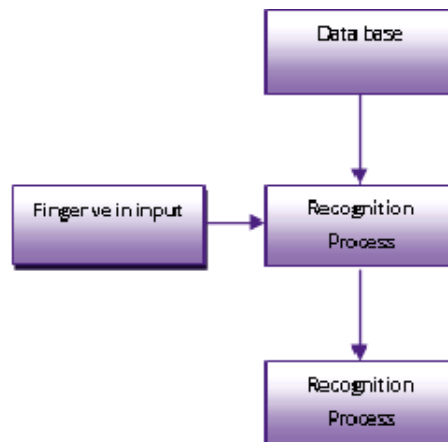
Adding a certain mapping function between the color model and a certain reference color space results in a definite "footprint" within the reference color space. This "footprint" is known as a [gamut](#), and, in combination with the color model, defines a new **color space**. For example, [Adobe RGB](#) and [RGB](#) are two different [absolute color spaces](#), both based on the RGB model.

In the most generic sense of the definition above, color spaces can be defined without the use of a color model. These spaces, such as [Pantone](#), are in effect a given set of names or numbers which are defined by the existence of a corresponding set of physical color swatches. This article focuses on the mathematical model concept.

RECOGNITION

Applications range from tasks such as industrial [machine vision](#) systems which, say, inspect bottles speeding by on a production line, to research into artificial intelligence and computers or robots that can comprehend the world around them. The computer vision and machine vision fields have significant overlap. Computer vision covers the core technology of automated image analysis which is used in many fields. Machine vision usually refers to a process of combining automated image analysis with other methods[12] and technologies to provide automated inspection and robot guidance in industrial applications.

As a scientific discipline, computer vision is concerned with the theory behind artificial systems that extract information from images. The image data can take many forms, such as video sequences, views from multiple cameras[11], or multi-dimensional

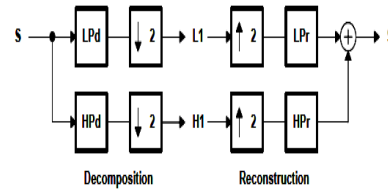


data from a medical scanner.

Figure 6 : FVRS image process method

WAVELET ANALYSIS

The discrete wavelet transform (DWT) was developed to apply the wavelet transform to the digital world. Filter banks are used to approximate the behaviour of the continuous wavelet transform. The signal is decomposed with a high-pass filter and a low-pass filter. The coefficients of these filters are computed using mathematical analysis and made available to you.



Where

- ❖ LPd: Low Pass Decomposition Filter
- ❖ HPd: High Pass Decomposition Filter
- ❖ LPr: Low Pass Reconstruction Filter
- ❖ HPr: High Pass Reconstruction Filter

HAAR WAVELET ANALYSIS

In mathematics, the **Haar wavelet** is a sequence of rescaled "square-shaped" functions which together form a [wavelet](#) family or basis. Wavelet analysis is similar to [Fourier analysis](#) in that it allows a target function over an interval to be represented in terms of an [orthonormal](#) function basis. The Haar sequence is now recognised as the first known wavelet basis and extensively used as a teaching example.

DESIGN FLOW

The flow diagram of FVRS- Mobile unit is given below. It shows all the step by step function of finger vein recognition system. Initially the device will wait for an RF signal from the user to activate the communication between the embedded control unit and the image acquisition unit. Then the finger vein image of the user will be compared with the unique data base image. Then the authentication result will be send to the security number of the user.

Firstly initialize the image from the data base through the matlab then the image is resize to 1/3 size for low noise image and go for histogram for the enhancement of the image and compare the image with user and database, if image is not compared then security number is get to the mobile, if image is compared then security number is get to the mobile through voice alert. According to the security number

The transaction of ATM is opened according to Bank name & Pin Number. After entering the pin number the transaction is being processed.

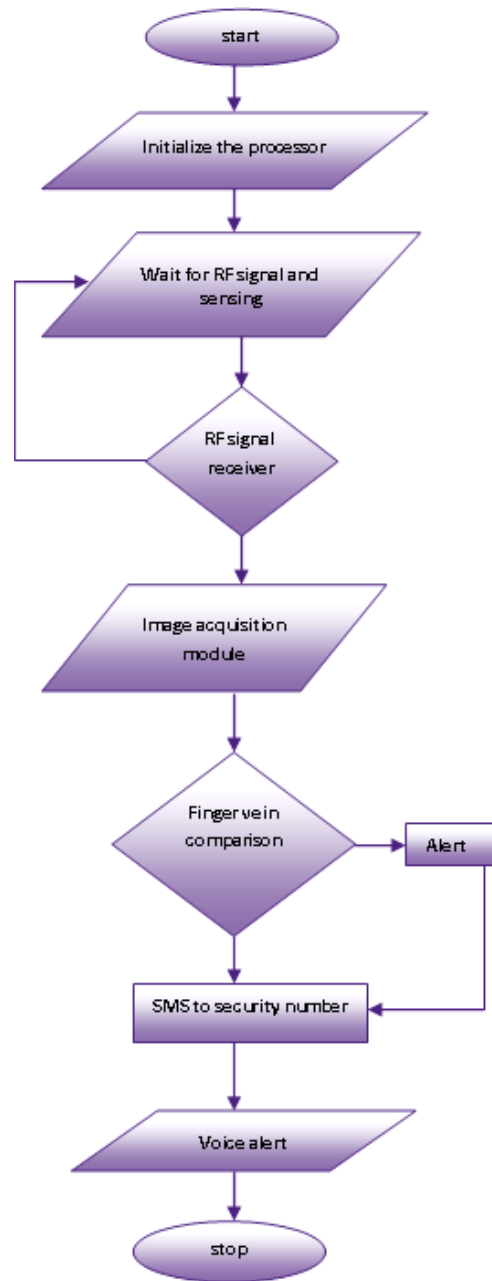


Figure 3: Flow diagram of FVRS

CONCLUSION

Security is becoming essential in all kind of application. This project is implemented in a way to improve the security level. As the finger-vein is a promising biometric pattern for personal identification in terms of its security and convenience. Also the vein is hidden inside the body and is mostly invisible to human eyes, so it is difficult to forge or steal. The non-invasive and contactless

capture of finger-veins ensures both convenience and hygiene for the user, and is thus more acceptable. So this system is more hopeful in improving the security level.

REFERENCES

- [1] A. K. Jain, S. Pankanti, S. Prabhakar, H. Lin, and A. Ross, "Biometrics: a grand challenge", *Proceedings of the 17th International Conference on Pattern Recognition (ICPR)*, vol. 2, pp. 935-942, 2004.
- [2] P. Corcoran and A. Cucos, "Techniques for securing multimedia content in consumer electronic appliances using biometric signatures," *IEEE Transactions on Consumer Electronics*, vol 51, no. 2, pp. 545-551, May 2005
- [3] P. J. Phillips, A. Martin C. L. Wilson and M. Przybocki, "An Introduction to Evaluating Biometric Systems," *IEEE Computer*, Vol.33, No.2, Feb. 2000, pp. 56-63.
- [4] S. Pankanti, R. M. Bolle and A. Jain, "Biometrics: The Future of Identification," *IEEE Computer*, Vol.33, No.2, Feb. 2000, pp. 46-49.
- [5] H. Lee, S. Lee, T. Kim, and Hyokyung Bahn, "Secure user identification for consumer electronics devices," *IEEE Transactions on Consumer Electronics*, vol.54, no.4, pp.1798-1802, Nov. 2008.
- [6] D. Wang, J. Li, and G. Memik, "User identification based on finger vein patterns for consumer electronics devices", *IEEE Transactions on Consumer Electronics*, vol. 56, no. 2, pp. 799-804, 2010.
- [7] D. Mulyono and S. J. Horng, "A study of finger vein biometric for personal identification", *Proceedings of the International Symposium Biometrics and Security Technologies*, pp. 134-141, 2008.
- [8] Y. G. Dai and B. N. Huang, "A method for capturing the finger-vein image using nonuniform intensity infrared light", *Image and Signal Processing*, vol.4, pp.27-30, 2008
- [9] X. Sun, C. Lin, M. Li, H. Lin, and Q. Chen, "A DSP-based finger vein authentication system", *Proceedings of the Fourth International Conference on Intelligent Computation Technology and Automation*, pp.333-336, 2011.
- [10] D. D. Hwang and I. Verbauehede, "Design of portable biometric authenticators - energy, performance, and security tradeoffs," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 4, pp. 1222-1231, Nov. 2004.
- [11] N. Miura, A. Nagasaka, and T. Miyatake, "Feature extraction of finger vein patterns based on repeated line tracking and its application to personal identification", *Machine Vision Application*, vol. 15, no.4, pp.194-203, 2004.
- [12] W. Song, T. Kim, H. C. Kim, J. H. Choi, H. Kong and S. Lee, "A finger-vein verification system using mean curvature", *Pattern Recognition Letters*, vol. 32, no.11, pp. 1541-1547, 2011.