BIOMETRIC AUTHENTICATION FOR SAFE LOCKER SYSTEM

Rajil Jackson.L[1], Prithi.S[2], J. Priyadarshini[3], G.Vijayalakshmi[4]

[1] *Student, Department of ECE, Prince Shri Venkateshwara Padmavathy Engineering College, Tamil Nadu, India*
[2]*Assistant Professor, Department of ECE, Prince Shri Venkateshwara Padmavathy Engineering College, Tamil Nadu, India*
[3]*Assistant Professor, Department of ECE, Prince Shri Venkateshwara Padmavathy Engineering College, Tamil Nadu, India*
[4]*Assistant Professor, Department of ECE, Prince Shri Venkateshwara Padmavathy Engineering College, Tamil Nadu, India*

ABSTRACT

The most vital requirement in today's world of spoofing attacks is the high security. The development in consumer electronics demands for high security with high accuracy and high speed of authentication. Human behavioral and physiological features in biometrics have the large scope as a solution for security issues. However, the existing biometric systems are highly complex in terms of time or space or both, and thus not suitable in very high security. Thus, an embedded finger-vein recognition system for authentication is proposed. The biometric system is used for identification based on person's unique vein pattern. The system is to be implemented using gradient boost algorithm for feature extraction. Median filter is used for filtering Gaussian, , Poisson and salt and pepper noise. Canny edge detection is used for obtaining the finger vein pattern in which the vein and the background are differentiated using a binary image. The authentication of the finger vein features is done using a svm classifier. The svm classifier compares the obtained finger vein features with the database in the system and provides the necessary results. Based on this analysis finger vein recognition becomes easier and reliable. And this proposed system can be highly trusted in case of security issues.

Keyword: - *Biometrics, Finger vein, Canny edge detection, Gradient boost*

1. INTRODUCTION

Authentication, authorization and accounting are essential components of security. A biometric system is a technological system that uses information about a person (or other biological organism) to identify the person. To achieve a better recognition performance and overcome same limitations produced by the uni-modal systems such as lack of uniqueness and non-universality, the multimodal biometric system, which fuses information from multiple biometric sources, is used. In this scheme, for improving the system performance; some finger types are combined to construct an efficiency multimodal system. This combination is performed at the feature extraction level. In finger vein authentication process the pattern of blood vessels is captured by transmitting near-infrared light at different angles through the finger, usually the middle finger. Even twins are said to have different finger vein patterns. Authentication cannot be forged with a severed finger, as the blood would flow out of a disconnected finger, making authentication impossible.

2. PROPOSED SYSTEM

Proposed system obtains the vein pattern and gradient boost algorithm is used to obtain the better features such as angle magnitude and gradient from which efficient authentication is made. Gradient boost is to obtain features i.e. vein features and also to boost those features to obtain results. Median filter is implemented to eliminate unwanted

noises. Canny edge detection is used to obtain the vein pattern from which features can be extracted. Additional security is provided by IR sensors and RFID.

3. BLOCK DIAGRAM OF SAFE LOCKER SYSTEM

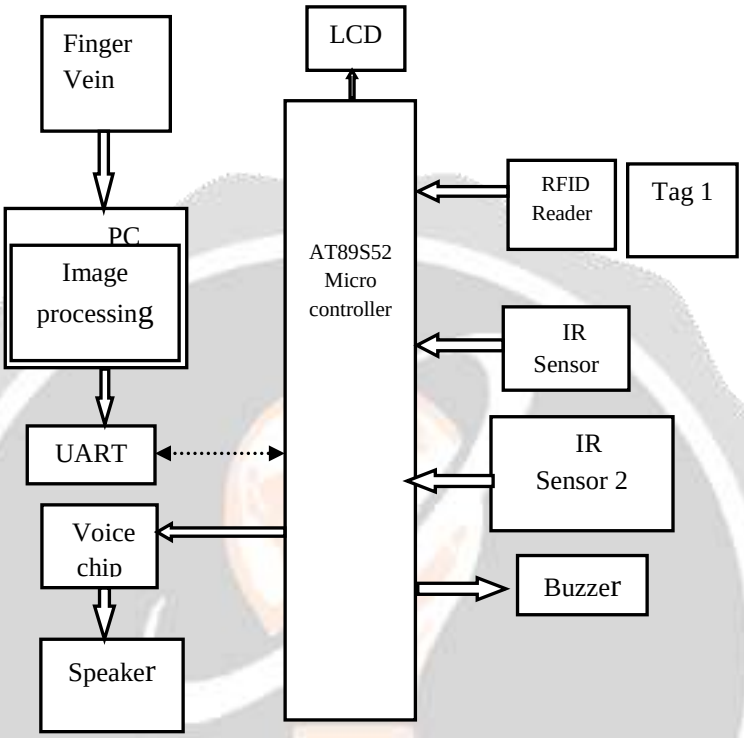

Fig -1: Block diagram of safe locker system

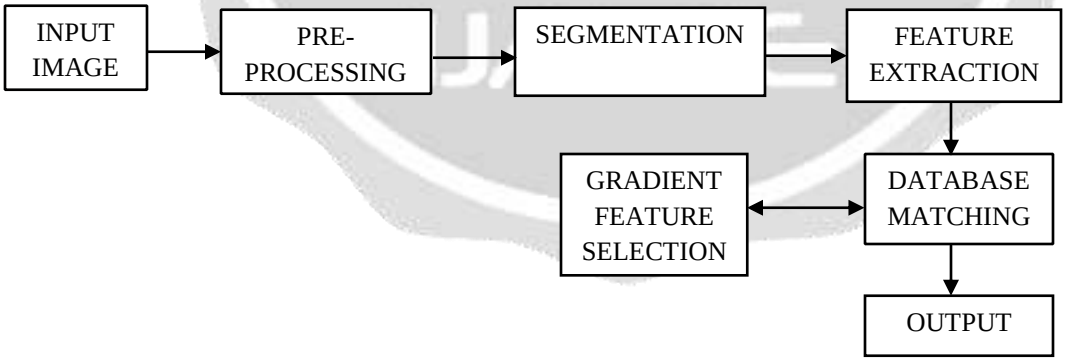

Fig-2 Block diagram of finger vein image processing

4. BLOCK DESCRIPTION OF SAFE LOCKER SYSTEM

Fig 1 presents the main hardware components of the safe locker system where authentication is done based on the finger vein pattern of individuals. The features that are extracted are compared with the system database using SVM classifier. The user first must keep his/her respective finger for vein authentication the image is captured and features are extracted through Image Processing. Image processing is done through MATLAB software. Microcontroller ATMEL 89S52 is used in this system. Programs are laden into the system using the software KEIL

compiler and coding is executed using embedded C. The reader energies the coil in the tag and information from the IC chip in the tag is transferred to the reader by RF waves, it compares the information with the database in the reader and decides the authenticated person. The reader checks the tag information present in the IC chip with its current database and then authenticates the person. Two IR sensors are used. One to determine the entry of the person and another is used to determine the exit of the person. Whether the person is authenticated or not can be seen from the LCD display. IR sensors performs counting when the persons enters into the locker each time. A voice chip along with a speaker is provided for better interaction. When more than one person intrudes into locker, buzzer becomes active and start to alert automatically.

5. BLOCK DESCRIPTION OF FINGER VEIN IMAGE PROCESSING

The figure 2 is the block diagram of MATLAB section. The input image is fed into the system. The input image is of size 320x240 and the image format is bitmap image. The preprocessing block enhances the image before further processing. It performs operations such as color conversion, resizing and filtering. The image is resized to 128x128 for easy computation. The color image is converted to gray scale image. Median filter is used to remove salt & pepper noise, Gaussian noise and Poisson noise. The segmentation block is used for separation of image for extracting the features. Edge detection is done using canny edge detection. Thresholding is applied along with edge detection so that the veins are obtained as white and the background is completely changed to black. Thus, the pattern of the veins is obtained from which the features can be extracted easily. In feature extraction, gradient boost algorithm is used which compares the features angle, magnitude and gradient. The obtained feature values are compared with the database. When the features that are obtained match with the database then the person is an authorized person else he is an unauthorized person and the locker will not open.

6. OVERALL CIRCUIT DIAGRAM

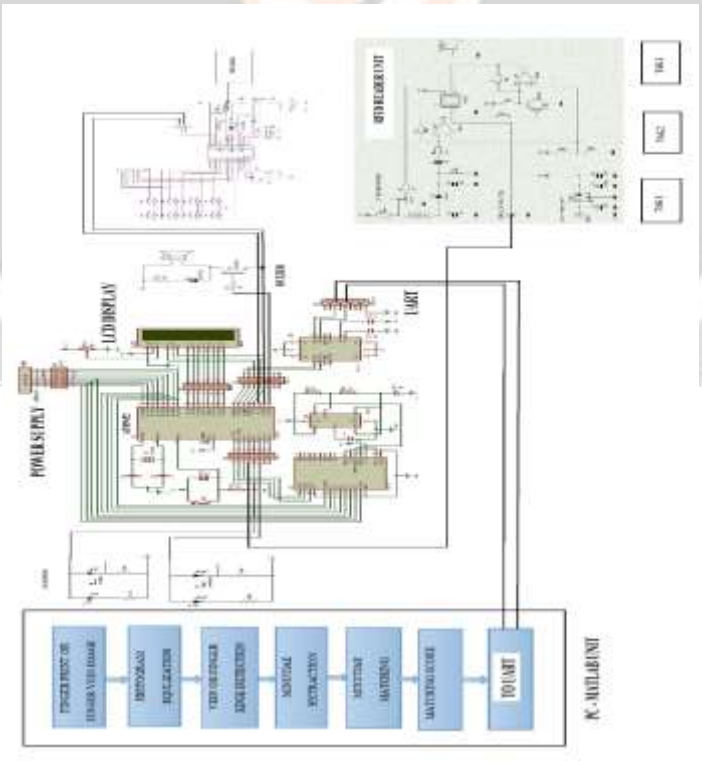

Fig -3: Interfacing circuit diagram for safe locker system

The figure 3 gives the overall circuit diagram of the safe locker hardware component. The PC performs the image processing and sends it to the UART to the microcontroller to port 3.0 and 3.1. The RFID reader is connected to the port 1.3 which authorizes the ID. The two IR sensors are connected to port 1.4 and 1.5. The IR sensors are used to

detect the entry of the person into the locker. The LCD display is used for interaction in which the data lines are connected to the entire port 2 pins and the control lines are connected to port 3.2, 3.3 and 3.4. Voice chip is used to indicate authentication the voice chip is connected to port 3.5 and 3.6. The buzzer is used for alarm and is connected to port 3.7. The table 1 describes the hardware components along with their specifications.

Table -1: Table of components

S.NO	HARDWARE COMPONENT	SPECIFICATION
1.	Microcontroller ATMEL	AT89S52
2.	LCD	16X2
3.	RFID Reader	-
4.	Voice Board	APR9600
5.	IR Sensor	-
6.	UART	RS232
7.	Speaker	-
8.	Buzzer	-
9.	Compiling tool	KEIL IDE

7. RESULTS

The results are expected to be obtained as follows. A real time image is captured and it is passed through the executable library to extract the required finger vein features and the output is obtained.

Fig -4: Loading database

The finger vein images that are to be authenticated are loaded into the database of the program as shown in the fig 4.

Fig -5: Selected finger vein image

After the database is fed one image is selected as the input image. Fig 5 shows the selected image from the given options.

Fig -6: Resized image

The input image is of size 320X240 this image is resized for easy computation. The resized image is of size 128X128 shown in fig 6.

Fig -7: Gray scale image

The image selected is tested for color model and conversion is performed for color image i.e., image is converted from RGB model to gray scale as shown in fig 7.

Fig -8: Filtered image

The image is filtered for reduction of noises such as salt and pepper noise, Gaussian noise and Poisson noise. Fig 8 shows the filtered image.

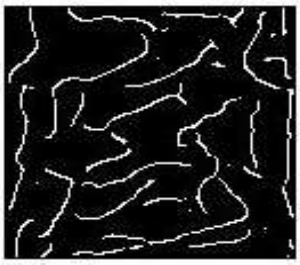

Fig -9: Finger vein pattern

The image is extracted for patterns of veins using canny edge detection technique. Thereby obtaining the pattern of the veins shown in fig 9.

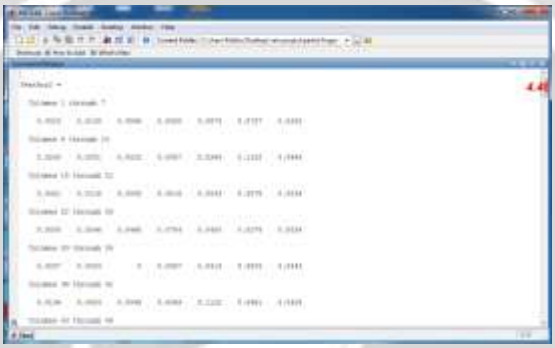

Fig -10: Obtained features

From the fig 9 the features are obtained for each block and each pixel as in fig 10.

Fig -11: Authenticated indication

Fig -12: Non-authentication indication

The obtained features are verified with the database in the computer for authentication when the person is authenticated fig 11 pops up or else fig 12 is displayed.

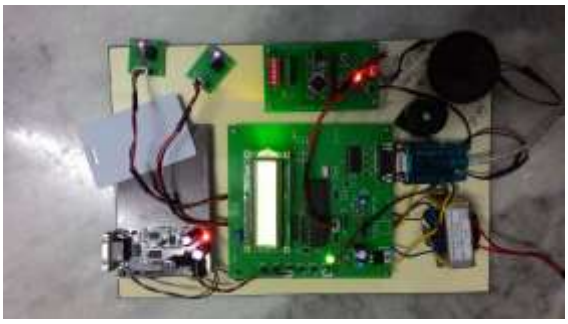

Fig -13: Hardware module for safe locker system

The fig 13 shows the hardware module for the safe locker system. The output from the MATLAB section is imported to the microcontroller part via the DB9 pin. The output thus obtained is displayed in the 16x2 LCD and speaker from the voice board also provides the authentication message. The RFID reader authenticates the tag and output is shown in LCD. The IR sensors are connected to the buzzer which provides alarm for false count.

8. CONCLUSIONS

The finger vein authentication for safe locker system is highly reliable and more secure than other biometric authentication systems. The power consumption is very low and the computation time is also low. The gradient boost algorithm used in image processing computes fast and obtains the features with low error rate. With the help of gradient boost algorithm efficiency is improved due to angle, magnitude and gradient features. RFID readers are more reliable than magnetic strip cards as data cannot be obtained easily from RFID tags. Thus, this system stands out for safety and security.

9. REFERENCES

[1]. R Ajay Kumar and Yingbo Zhou (2012) 'Human Identification using FingerImages', IEEE Transactions on Image Processing, Vol. 21, No. 4, pp.2228-2244.
[2]. R Desong Wang, Jianping Li and Gokhan Memik (2010) 'User Identification Based on Finger-vein Patterns for Consumer Electronics Devices', IEEE Transaction on Consumer Electronics, Vol.56, No.2, pp.799-804.
[3]. Hyejeong Lee, Sang-Ho Lee, Taeseok Kim and Hyokyung Bahn (2008) 'Secure User Identification for Consumer Electronics Devices', IEEE transactions on Consumer Electronics, Vol. 54, No. 4, pp. 1798-1802.
[4]. Manisha Sapkale and Prof Rajbhoj, S.M. (2016) 'A Finger Vein Recognition System',IEEE.
[5]. Mohamed Syed Ibrahim, M., Dr. Faris Salman Majeed Al Naimy, Dr. Rajaji, L. and Syed Amma, S. (2012) 'Biometric Recognition for safe Transaction using Vein Authentication System',IEEE.
[6]. Wonseok Song, Taejeong Kim, Hee Chan Kim, Joon Hwan Choi, HyounJoong Kong and Seung-Rae Lee (2011) 'A finger-vein verification system using mean curvature', Pattern Recognition Letters, 32, pp. 15411547.
[7]. Zhi Liu and Shangling Song (2012) 'An Embedded Real Time Finger Vein Recognition System for Mobile Devices', IEEE Transactions on Consumer Electronics, Vol. 58, No. 2, pp. 522-527.
[8]. Zhi Liu, YilongYin, HongjunWanga, ShanglingSong and QingliLi (2010) 'Finger vein recognition with manifold learning', Journal of Network and Computer Applications, 33, pp.275282.