

# International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: [www.ijirset.com](http://www.ijirset.com)

Vol. 6, Issue 9, September 2017

## Multimodal Biometric Authentication for High Security System using Raspberry Pi

Alsa Thomas<sup>1</sup> Anitta Thomas<sup>2</sup>

M.Tech Student, Department of ECE, Viswajyothi College of Engineering & Technology, Vazhakulam, Kerala, India<sup>1</sup>

Asst. Professor, Department of ECE, Viswajyothi College of Engineering & Technology, Vazhakulam, Kerala, India<sup>2</sup>

**ABSTRACT:** Biometric is a process of identifying a person using physiological or behavioral characteristics. Since the unimodal biometric systems have several tradeoffs like noisy data, intra-class variations, restricted degrees of freedom, non-universality, spoof attacks, and unacceptable error rates, this paper focusing into multimodal biometric systems. A new approach using various multimodal options like fingerprint, Face, vein pattern, iris to improve the authentication is proposed. Each biometric module captures the relevant traits of an individual, extracts feature sets, compares those features against the same user's pre-stored trait templates in a database and passes its decision. The outputs from each biometric module are checked to generate a final decision to either grant or deny access to a user who is in the process of authentication. The proposed system is simulated using MATLAB and implemented in Raspberry Pi. The system was tested with 30 different persons in real time implementation. The accuracy obtained after implementing the system is 86.66%.

**KEYWORDS:** Accuracy, Multimodal, Unimodal, Universality.

### I. INTRODUCTION

As technology advances, information and intellectual properties are wanted by many unauthorized personnel. As a result, many organizations have been searching ways for more secure authentication methods for user access. Furthermore, security has always been an important concern to many people. From Immigration and Naturalization Service (INS) to banks, industrial, military systems, and personal are typical fields where security is highly valued. It is soon realized by many, that traditional security and identification are not sufficient enough; people need to find a new authentic system in the face of new technological reality. Conventional security and identification systems are either knowledge based – like a social security number or a password, or token based – such as keys, ID cards [9]. The conventional systems can be easily breached by others, ID cards and passwords can be lost, stolen or can be duplicated. In other words, it is not unique and not necessary represent the rightful user. Therefore, biometric systems are developing intensively and many researches are going on. Biometric authentication is an automated method of recognizing a person. Biometric authentication can be classified into unimodal and multimodal biometric systems [2].

Unimodal systems that use single biometric trait for recognition purposes; and suffers a several practical problems like non-universality, noisy sensor data, intra-class variation, restricted degree of freedom, unacceptable error rate, failure-to-enrol and spoof attacks. So, the performance of single biometric system needs to be improved. The techniques of multimodal biometric system can offer a feasible method to solve the problems coming from unimodal biometric system. Multimodal biometric system makes use of different biometric traits simultaneously to authenticate a person's identity. Robustness and high security of authentication can be achieved by using the multimodal biometric systems.

### II. RELATED WORK

Multimodal biometrics has been proposed by Ross and Jain in 2003[1]. The concept of biometric multimodalities fusion is introduced with different fusion strategies and various levels of fusion are also presented [2]. Fusion of iris and fingerprint has attracted a lot of attention and researchers have presented variety of approaches. The conventional fusion methods [4] use the same weight for each single biometric trait, but some biometric traits are more precise than the other ones; they have more stability and resistance to attacks. So in our approach, iris trait has more

# International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: [www.ijirset.com](http://www.ijirset.com)

Vol. 6, Issue 9, September 2017

weight in fusion with fingerprint. Weight here is not a number assigned to the matching score, but a decision with intermediate values related to the matching distance.

## III.SYSTEM ARCHITECTURE

The whole system is composed by following parts: an image capturing camera, Raspberry Pi board to run image recognition programs on it. Monitors also connected with this system during initial stages to preview the captured images and give the user indication. The system block diagram is shown in Fig 1.

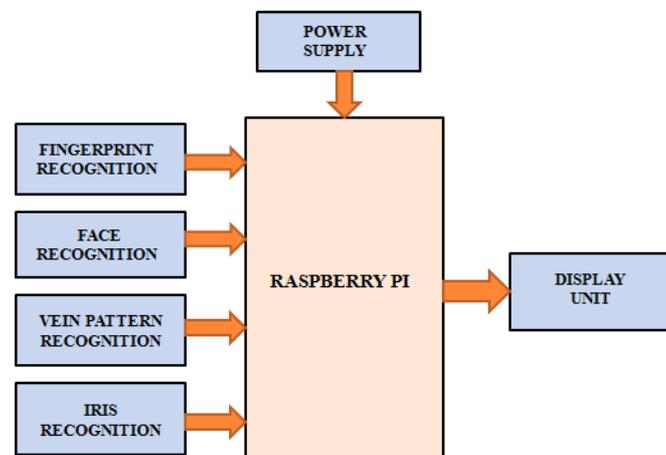


Fig.1. System Block Diagram

The working consists of two phases, i.e. enrolment phase and verification phases. The purpose of the enrolment model is to register all the authority users to access control and save the biometrics features in a database. The verification (or authentication) model used for verifies the claimed identify of person. This model consists of four stages: the first one for the fingerprint, the second for the face, third as vein pattern and last for iris recognition.

### A. Fingerprint Recognition

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify an individual and verify their identity. Because of their uniqueness and consistency over time, fingerprints have been used for over a century, more recently becoming automated (i.e. a biometric) due to advancement in computing capabilities. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and their established use and collections by law enforcement and immigration.

This system registered the users that consider as authority to access control in the enrolment. Each user in this stage will take the ID number that save in the database. This proposed system is implemented in a Linux based GUI application, with the intention of using this to demonstrate the functionality of the finger print device along with raspberry pi embedded computer. It offers an interface for enrolling fingers and deleting enrolment data for previously enrolled .it also verify a specific finger and identify a finger from a selection of previously enrolled fingerprint data.

#### 1. Software- Algorithm

- Step 1: Initialize IP address in Putty.
- Step 2: Connect the fingerprint module.
- Step 3: Enroll the fingerprint.
- Step 4: Create the database with particular ID.
- Step 5: Created ID is stored in Raspberry pi.
- Step 6: Test the system with a new input.

# International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: [www.ijirset.com](http://www.ijirset.com)

Vol. 6, Issue 9, September 2017

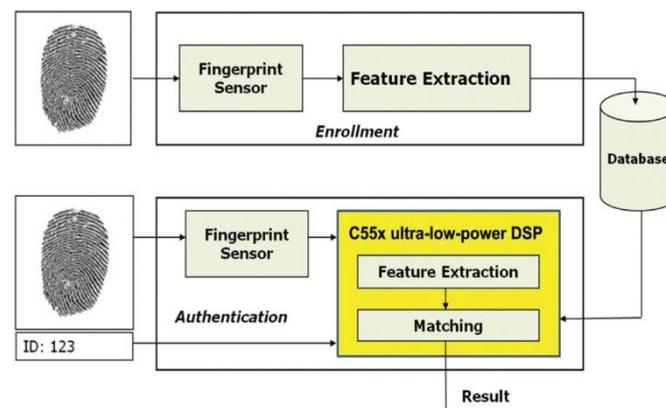


Fig.2. Block Diagram of Fingerprint Recognition System

Each module has a different ID number. You can make your system remember this ID number, so that each time before use your system will read Module ID number to check if the module matches. There is user flash in the module, where user can write some related user info to be distinguished from other modules. If the testing person is an authorized one, he can access the system, otherwise system cannot be accessed.

## B. Face Recognition

The input can be recorded as video using a web camera. From this video, face is detected and saved. A pre-processing module marks the eye position and also looks after the surrounding lighting condition and color variance. After the face is detection, localization and normalization are carried out. The appearance of the face can change considerably during speech and due to facial expressions. Principal component analysis (PCA) was invented in 1901 by Karl Pearson. PCA is a variable reduction procedure and useful when obtained data have some redundancy. This will result into reduction of variables into smaller number of variables which are called Principal Components which will account for the most of the variance in the observed variable. Problems arise when we wish to perform recognition in a high-dimensional space. Goal of PCA is to reduce the dimensionality of the data by retaining as much as variation possible in our original data set. On the other hand dimensionality reduction implies information loss. The best low-dimensional space can be determined by best principal components. The major advantage of PCA is using it in eigenface approach which helps in reducing the size of the database for recognition of a test images. The images are stored as their feature vectors in the database which are found out projecting each and every trained image to the set of Eigen faces obtained. PCA is applied on Eigen face approach to reduce the dimensionality of a large data set. Calculate the Euclidian distance between the weights of the unknown image and the database images. If the distance is less than the threshold then test image is considered to be in the database and hence authorized, otherwise unauthorized.

## C. Vein Pattern Recognition

Palm vein technology is used to identifying the vein patterns in a person's palm. Vein pattern identification uses an infrared light source to scan for hemoglobin within the blood. Once a user's hand is kept over a sensing device, a near infrared light from the sensing device maps the position of the veins. The backs of hands and palms have more complex vascular patterns than fingers and provide a lot of distinct features for pattern matching and authentication. Images suffer from quality degradation due to transmission of limited range of light, low contrast and blurred image due to quality of light and diminishing color. The performance of an image filtering system depends on its ability to detect the presence of noisy pixels in the image. Different techniques are available in the literature for improving the images, as the filtering methods remove noise from the image; contrast enhancement tends to enhance the contrast of the image and segmentation method to extract the foreground image from the background.

## International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: [www.ijirset.com](http://www.ijirset.com)

Vol. 6, Issue 9, September 2017

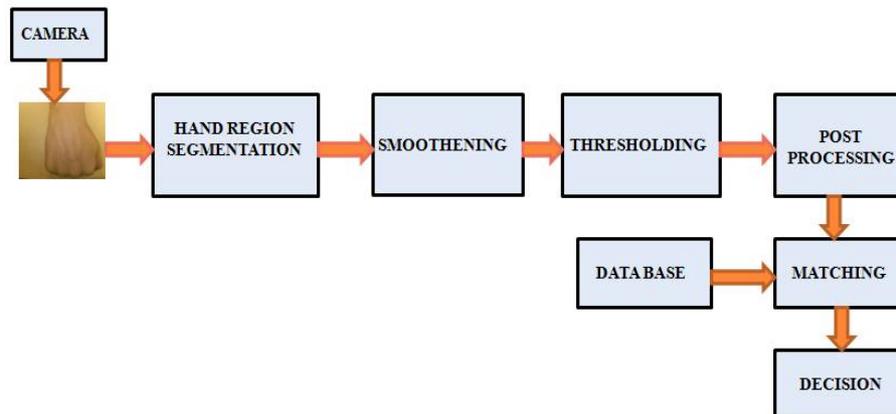


Fig.3. Proposed System for Hand Vein Pattern

The processing of image captured is performed in this module. The image captured by the image acquisition module will be in RGB so it has to be converted into gray scale image for further processing. This module is responsible for removing noises, contrast enhancements in patterns from raw image of the back of the hand.

Training Phase includes:

- Step 1: Capture an image
- Step 2: Convert the image to grayscale
- Step 3: Crop the needed region
- Step 4: Paste the cropped image into a black frame
- Step 5: Apply Smoothing operation
- Step 6: Apply Morphological operation
- Step 7: Convert image to binary
- Step 8: Save it to a database

Testing Phase includes:

- Step 1: Repeat the same steps done in training phase.
- Step 2: Compare the testing template with the database file. If the result is within the limit then the access is granted.

1. RGB to Gray scale conversion: The images obtaining from the image acquisition module are in RGB format. For further processing we need to convert it into gray scale.
2. Hand Region Segmentation: Segmenting the image into two levels; object (hand region) and background; the object segment which is the region of interest (ROI) and the background segment.

3. ROI Extraction: Selecting an optimal threshold, which is used to segment the image into two distinct parts; hand and background? Then translate the greyscale hand region to the centre of the image after assigning the background area to zero value pixels. Thus we can completely localize, separate and centred the hand region for subsequent processing.

4. Smoothing and Noise Reduction: In order to remove the hand traces from the acquired image a median filter of 5\*5 masks can be used. The median replaces each pixel by the median or middle pixel (as opposed to the mean pixel) value in a square neighbourhood around the centre pixel.

5. Subtraction: After estimating the vein pattern background the morphologically transformed image is subtracted from median filtered image. By median filtering the vein patterns get preserved, and by morphological transformation we get estimated background. So by subtracting both, the vein patterns are extracted. This subtraction process extracts the vein

# International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: [www.ijirset.com](http://www.ijirset.com)

Vol. 6, Issue 9, September 2017

patterns from the image.

6. Thresholding: This is a binarization process for converting the gray scale vein pattern obtained after the subtraction process to a binary image. In this process, an optimal threshold value is selected and each pixel value is compared with this threshold value. The values greater or lower when compared with this threshold are converted to 1's (white) and 0's (black) respectively.

## **D. Iris Recognition**

Unlike face recognition, close-up photographing is required to obtain appropriate resolution of the eye image since an eye is smaller than a face. For recognition/authentication of a person, the eye image is captured using infrared (IR) camera. The infrared rays used to capture the iris image have low intensity, and are known to be non-harmful to humans.

### 1. Segmentation

#### a) Basic Pupil Detection

Pupil Detection will be the basis of eye tracker. The pupil is just a black circle, but this might not always be true as in the circle does not always have to be completely black (in case we have some glints) and might not be a circle (if we're looking at the pupil under an angle).

#### b) Basic Iris Detection

Iris detection is significantly more difficult than pupil. Mostly because it is not so well defined, pupil is just a black disk essentially as far as a gray scale image is concerned, but the outer edge of the iris is not nearly as sharp as the outer edge of the pupil is. Also, there is a much higher probability of glints and reflections in the iris, since it is larger than the pupil and this can complicate the detection further. And on top of all that the upper and lower eyelids often cover up portions of the iris, which means that detecting the iris as a circle is going to be either difficult or impossible. Smooth down the image using median filter.

Steps for normalizing Iris image includes first of Daugman's rubber sheet model. Second step is representing Cartesian to polar coordinates. Next step is output normalization. Consider small part of iris section for further processing. As iris should be isolated and stored as separate image because of its limits such as occluded iris part or iris covered with eyelashes and also observe that possibility of pupil dilating and appearing in terms of different size of pupil for different images. So, need to change the coordinate system by unwrap the iris and then mapping is performed in all the points within the boundary of the iris into their polar equivalent using Daugman's rubber sheet model. Unwrapping the image from a circular pattern to form rectangular one. Extract a 3D RGB color histogram from the image and the histogram value is stored.

### 2. Matching

Compare the histogram value using phase correlation. If the number of correlation coefficients between the detected corners of the two images is greater than a threshold value then the candidate accepted by the system.

## **IV.RESULTS AND DISCUSSION**

The hardware implementation of the finger print recognition, face recognition, vein pattern recognition and iris recognition is done in Raspberry Pi and software used for implementation is Python. The system is implemented in Raspberry Pi and is tested in real time. The system uses database of 2 persons in each stage.

# International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: [www.ijirset.com](http://www.ijirset.com)

Vol. 6, Issue 9, September 2017

```

Press 1 for scanning
  2 for storing
  3 to stop the the scanning
  4 to exit from the loop
enter ur input: 2
Enter the loction you want to store: 1
Enter the name: alsa
Found OK
READY
Store OK
#1%

Press 1 for scanning
  2 for storing
  3 to stop the the scanning
  4 to exit from the loop
enter ur input1
Scanning started.....
Found OK
|
READY
#2%
#2%
#2%
alsaYour Fingerprint is recognized
You are authorized
please show your face for authentication
please pose for a photo
  
```

(a) (b)  
Fig.4. Fingerprint Recognition Results (a) Database Creation (b) Testing Result

At the first location with a particular ID the corresponding fingerprint is saved. During testing if a person access the system the module checks whether the person is authorized or not. If an authorized person accesses the system the ID will be returned. Otherwise no ID will be returned. Once an authorized person is identified and login to check the next face recognition system.

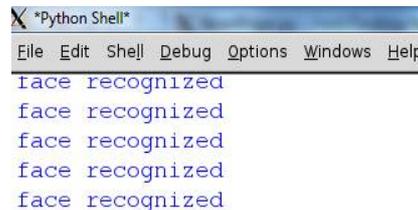


Fig.5. Face Recognition Result

Once the face is recognized move on to check the vein pattern recognition system. The database for face recognition is created by faces with different illumination and poses variations. This system uses database of 2 persons and each person's 10 images. The database for vein pattern recognition is created by vein of 2 persons and each person's 5 images.

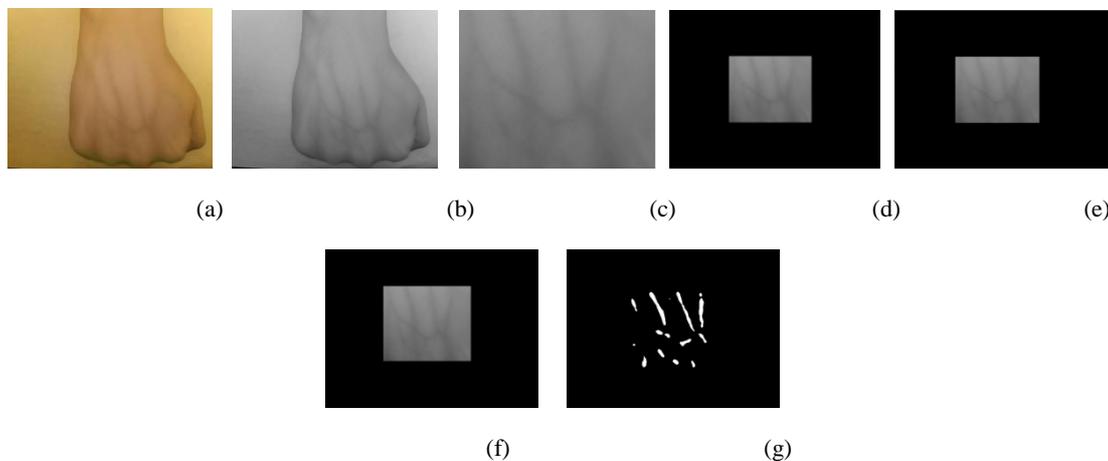


Fig.6. Vein Pattern Recognition Results. (a)Captured Image (b) Grey Scale Image (c) Cropped Image (d) Roi Image (e) After Smoothing (f) After Morphological Operation (g) Vein Pattern

## International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: [www.ijirset.com](http://www.ijirset.com)

Vol. 6, Issue 9, September 2017

The database for vein pattern recognition is created by vein of 2 persons and each person's 5 images. Once the vein pattern is recognized move on to check the next iris recognition system.

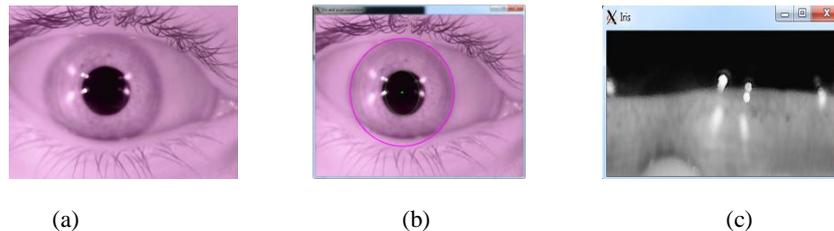


Fig.7. Iris Recognition Results (a) Testing, (b) iris and pupil detection, (c) iris template  
The database for iris recognition is created by iris of 2 persons and each person's 5 images.

### V. CONCLUSIONS

This project implements a multimodal biometric authentication for high security system using fingerprint, face, vein pattern and iris in Raspberry Pi. The system was evaluated using the database collected by fingerprint module and camera. The outputs from each biometric module are checked to generate a final decision to either grant or deny access to a user who is in the process of authentication. From the experimental results, the proposed multimodal personal authentication approach worked well and significantly improved authentication performance over the methods that use a single biometric trait. Using the multi-layer biometric system in combination with the optimum tested threshold value, will create a secure, optimal, artificially intelligent system. Thus, in practical applications, impostors attempting to use the device can be prevented. In future it would be necessary to measure the performance of the suggested approaches with a larger dataset, containing more individuals and also investigating further methods for evaluating the quality of the testing data.

### REFERENCES

- [1] Fingerprint Recognition using image segmentation by Dravider Kaur, Dario Maio, Anil K. Jain & Salil Prabhakar.
- [2] Fingerprint Recognition, Paper by WUZHILI (Department of Computer Science & Engineering, Hong Kong Baptist University) 2002.
- [3] Fingerprint Classification and Matching by Anil Jain (Department of Computer Science & Engineering, Michigan State University) & Sharath Pankanti (Exploratory Computer Vision Group IBM T. J. Watson Research Centre) 2000 .
- [4] Fingerprint database - FVC2002 (Fingerprint Verification Competition 2002) Jain, R. Bolle, and S. Pankanti, "Biometrics Personal Identification in Networked Society", Kluwer Academic Publishers New York, Boston, Dordrecht, London, Moscow, pp. 1-64, 2002.
- [5] A. K. Jain, F. Patrick, A. Arun, "Handbook of Biometrics", Springer science+Business Media, LLC, 1st edition, pp. 1-42, 2008.
- [6] D. Maio, and D. Maltoni, "Direct gray-scale minutiae detection in fingerprints", IEEE Transactions Pattern Analysis and Machine Intelligence, vol. 19(1), pp. 27-40, 1997.
- [7] Organism Information Visualization Technology Editing Committee Edition: Organism Information Visualization Technology. (in Japanese), Corona Publication Co., Ltd., p.235 (1997).
- [8] The Federation of Bankers Associations of Japan: Statistics from the Questionnaire on the Number of Withdrawals and the Amount of Money Withdrawn Using Stolen Passbooks.
- [9] An embedded real-time finger-vein recognition system for mobile devices, Zhi Liu Sch. of Inf. Sci. & Eng., Shandong Univ., Jinan, China Shangling Song published in: Consumer Electronics, IEEE transactions on (Volume:58 , Issue: 2).
- [10] A.M. Badawi, —Hand Vein Biometric Verification Prototype: A Testing Performance and Patterns Similarity In Proceedings of the 2006 International Conference on Image Processing, Computer Vision, and Pattern Recognition (ICCV'06: June 26-29, 2006, Las Vegas, USA.

### BIOGRAPHY



**Aisa Thomas** was born in KSA. She took her B.Tech in Electronics and Communication Engineering from Sree Narayana Gurukulam College of Engineering, Kadayiruppu(2015). She is doing her M.Tech in VLSI and Embedded System at Viswajyothi College of Engineering & Technology, Vazhakulam. Her fields of interest include VLSI, Embedded System and Digital System Design.

## International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

Website: [www.ijirset.com](http://www.ijirset.com)

Vol. 6, Issue 9, September 2017



**Anitta Thomas** was born in Kerala, India. She took her B.Tech in Electronics and Communication from Mahatma Gandhi University College of Engineering, Thodupuzha(2004) and M.Tech from Model Engineering College, Thrikkakkara (2010).She is currently working as Assistant Professor in Viswajyothi College of Engineering and Technology, Vazhakulam for the last 12 years. Her fields of interest include VLSI and Embedded Systems. She is a life-time member of 'Indian Society for Technical Education' (Life Membership Card No: LM 100967).