Finger Vein Biometric based Secure Access Control in Smart Home Automation

R.Sarala, E.Yoghalakshmi, V.Ishwarya

Abstract**: *Smart home automation has become popular with the advent of IoT technology. Smart home automation systems suffer from a number of security issues due to the vulnerabilities that exist in the different devices and the interconnection network. Providing user authentication for smart homes is an important security requirement for preventing intruders from attacking a smart home automation system. Biometric based authentication systems have been used in many applications since they provide high security than the smart cards and password based authentication systems. Finger vein recognition is a biometric authentication technique that applies pattern recognition on the images of human finger vein present beneath the skin's surface. The advantage of using finger vein authentication is that, it is difficult to forge and also provides high accuracy as the external deformities like rashes, cracks and rough epidermis do not have an impact on the matching and recognition process. This paper deals with the implementation of a secure smart home automation system that uses finger vein biometric for the authentication mechanism. The algorithm used for authentication uses K Means Segmentation and canny edge detection for feature extraction. SVM classifier is used for the matching process. The authentication system is then incorporated into the smart home automation system that can be used to monitor and control the devices connected to it. The proposed approach shows better performance than the existing methods used in literature for authentication, monitoring and control of smart home automation systems.***

Index Terms**: *Smart home automation; User authentication; Finger vein biometric; K-means segmentation; Canny edge detection; Raspberry pi.***

I. INTRODUCTION

The smart home automation is an application of the Internet of Things (IoT) which is an interconnection of devices with features for sending and receiving data. Using IoT devices such electronic appliances, security systems, thermostats, cars, alarm clocks, speaker systems and mobile phones can be connected by means of sensors and interconnection network [1]. Automation is popular nowadays because it provides ease of use, security and efficiency. Home automation refers to handling and controlling home appliances by using a micro-controller [2]. Even if the user is far away from home, the home appliances can be controlled by switching the devices on/off.

The smart home automation has many advantages, since devices are used only when they are required, help handicapped and aged people control the devices from where they stay, save time and allow for appliance control when out of town [3]. The IoT environment which is crowded with data from billions of sensors, smart phones, other mobile devices, and cloud-based services face threats from every direction. Therefore providing security for smart home systems is very much required [4]. Providing user authentication for smart homes is an important security requirement for preventing intruders from attacking a smart home automation system Biometric based automatic personal identification systems use physiological or behavioral characteristics such as fingerprint, iris, face, palm print, retina, gait and voice [5]. They are susceptible to forgery since they are exposed outside the human body. In case of a fingerprint, the condition of the finger surface namely dryness, sweat and skin distortion can degrade the recognition accuracy [6]. The fingerprints biometric devices can also be cheated by a dummy finger fitted with a copied fingerprint. The accuracy of face recognition systems depend hugely on the facial expressions and illuminations, which can change by occlusions or face-lifts. The Iris pattern recognition systems also require high-cost position adjustment mechanisms for the accurate recognition. The Finger Vein recognition technology, offers a promising solution to these challenges due the following characteristics:

- Similar to unique fingerprints all individuals have unique finger vein images and they remain unchanged despite ageing.
- Palm and finger vein detection methods do not create any known negative impact on body health.
- The condition of the epidermis does not affect the result of vein detection.
- Vein features are difficult to be forged and changed even with surgery.

These desirable properties make finger vein recognition a highly reliable authentication method. The proposed system tries to implement a secure authentication mechanism for smart home access control using finger vein biometric. Also, it enables to control the home appliances using automation through IoT technology.

II. RELATED WORK

Plenty of work has been carried out by researchers on the use of finger vein biometric during the past decade**.**

Revised Manuscript Received on October 30, 2019.
* Correspondence Author

R.Sarala, Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India.
E.Yoghalakshmi, Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India.
V.Ishwarya, Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India.

Retrieval Number F8044088619 /2019©BEIESP
DOI: 10.35940/ijeat.F8044.088619

A gradient correlation algorithm that uses histogram statistics recognizes whether the given input is a valid finger vein image [7]. Then, a matched filter based on the maximum curvature model is adopted to extract the gradient image of the finger vein. A cross-correlation between the two gradient images helps to estimate their similarity. The maximal correlation with threshold method is used to decide whether there is a matching or not. This algorithm makes the finger vein identification inaccurate. Repeated line tracking and gradient correlation reduces the recognition rate because the captured vein images are not always clear. An effective algorithm based on support vector machine for finger vein recognition is proposed for an Automated Teller Machine environment [8]. Here, the local binary pattern and wavelet transform methods are used to extract the finger vein features and support vector machine is used for the image classification. In this approach, the equal error rate and the processing time are reduced when compared to other methods. But the only drawback is that it moves the problem of over-fitting from optimizing the parameters to model selection. A method for calculating the local maximum curvatures in cross-sectional profiles of a vein image to robustly extract the precise details of the depicted veins is proposed in [9]. This method can extract the centerlines of the veins consistently without being affected by the fluctuations in vein width and brightness. Even though this pattern matching method is highly accurate than the existing conventional methods it cannot extract vein patterns that are narrower/wider than the assumed widths, which degrades the accuracy of the personal identification. [10] developed a much secured remote control system by telephone based on PIC. The designed circuit is isolated both optically and electrically. Therefore, it does not create any effect on the telephone line. With the pin check system, non-authorized people cannot connect to or use this system. But the drawback is that Pin check Algorithm was used to implement in the system only where it was connected with cable network but not in wireless communication. In recent years, wireless systems have become more and more common as they provide increased efficiency, easy access, availability and flexibility. Hence they are suitable to build home networking and home control automation systems. A Home Automation system using Intel Galileo kit that employs the integration of cloud networking is proposed in [11] and [12] focuses on the advantages of using Raspberry pi in Home automation. They used the messaging API in Raspberry pi, which sends text messages to the user about the changes in the home environment, with the help of a text to speech plug-in. The difference between [11], [12] and the proposed system is that the proposed system also considers adding finger vein biometric authentication over smart home automation since secure authentication is required to overcome physical threats to smart home security. Biometric characteristics never change with time or age and especially finger vein biometric is not easy to replicate or spoof. All these qualities give it an edge over traditional methods of identification.

III. PROPOSED WORK

The overall architecture of the proposed system is shown in fig 1. The system implements secure smart home automation using finger vein biometric authentication. It also monitors and controls the home appliances using IoT technology.

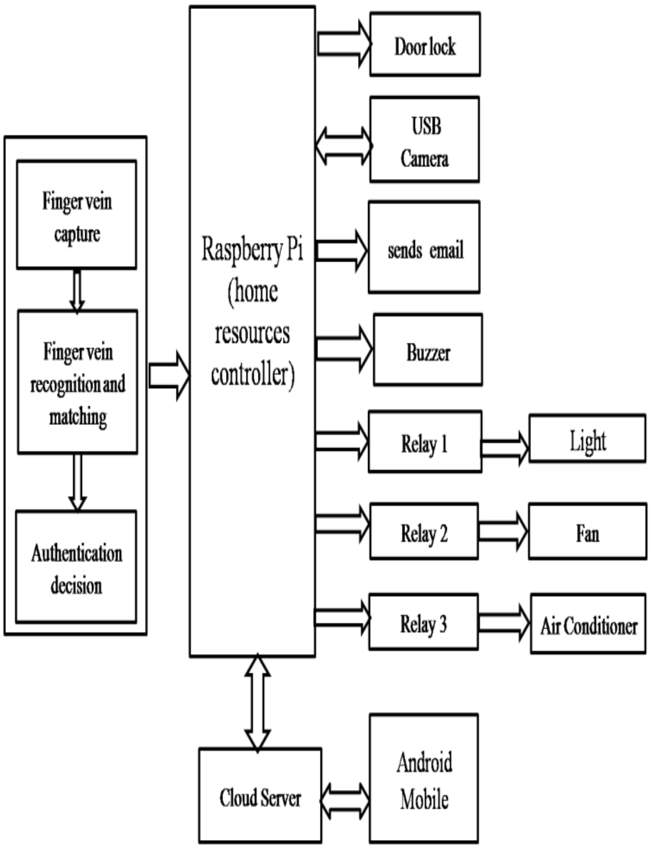


Fig 1 System architecture

The proposed system has two major components. They are finger vein authenticator and home resources monitoring and control unit. The flow diagram of finger vein authentication process is shown in fig 2.

A. Finger Vein Biometric based Authentication

This module involves image acquisition, pre-processing, feature extraction, and matching. The results of the matching process are sent to the raspberry pi kit. The input to the authenticator module is the dataset of 100 captured images of 10 fingers. Pre-processing consists of RGB to gray scale conversion, image resizing and filtering. Gray scale conversion converts the true color RGB image to the grayscale intensity image. The rgb2gray function converts RGB images to grayscale by eliminating the hue and saturation information while retaining the luminance. Image resizing is done to convert the image to the required new width and height to achieve image processing accuracy. K-Means segmentation [13] is a least-squares partitioning method that divides a collection of objects into K groups. It is used to separate the finger vein image from the background. The key points are identified from the finger vein image and the clusters are initialized with the key points. The centroid of each cluster is computed and then the distance between the keys points and the centroid is found. Based on this distance, the points with minimum distance are assigned to the clusters and this is repeated. In the k-means image segmentation the captured image is divided into multiple parts which make it easier to analyze and extract features that are required to calculate inclination value for the matching purpose.

Based on the inclination value, the output is decided as a ‘0’ or ‘1’ and sent to the home resources controller; i.e. the Raspberry PI kit.

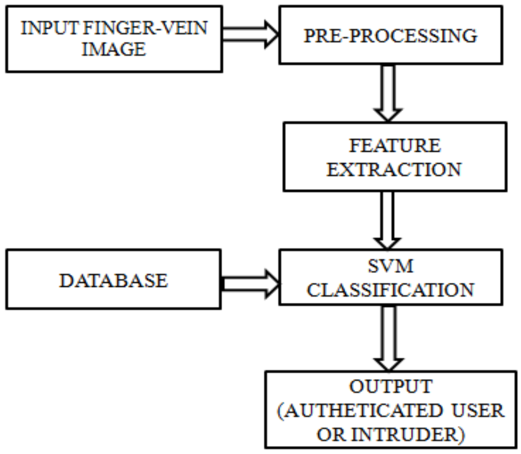


Fig 2 Finger vein authentication process

After segmentation of the image filtering is done to remove noise from the segmented image. The gaussian filter is used for noise removal. Edge detection is an image processing technique for finding the boundaries of objects within the images. In this paper, the canny edge detection algorithm [13] is used to detect the edges of the vein. Thinning technique helps to reduce the width of the vein pattern. After thinning the input image irregularities such as small branches and holes found in the vein pattern are removed using the smoothing technique. The features extracted from the input image include vein width, length, position and intersection points of vein. These are stored as feature vectors. The SVM classifier is fed with the feature vector which classifies the image as a valid user or not by comparing it with the stored features of authorized users. The output value of the SVM is represented by a continuous value. A value that is close to 1 represents an authorized user and a value that is close to 0 represents an imposter.

B. Home resources monitoring and control unit

An IoT based home automation system is one that uses personal computers or portable devices to control basic functionalities of home appliances automatically through the internet at anytime and from anywhere around the world. The Raspberry Pi model B+ is used as the home resources controller. It provides the user with remote control of various appliances such as lights, fans and also the opening of the door. This system can be accessed from the web browser on any local PC on the same LAN connection using server IP, or remotely from any portable device connected to the internet.

For interaction, the user initially has to establish a connection between the android application on the mobile and the deployed IoT manages the communication between raspberry pi and android device. The relay is used to switch the electrical appliances like light, fan, etc. The user can also monitor the status of the home appliances through the internet via web server. If the lights or any electrical appliances are left on in a hurry it can be turned off remotely through the android application. A maximum of eight appliances can be connected using the android application.

IV. EXPERIMENTAL SETUP AND RESULTS

The implemented system is shown in fig 3. The finger vein biometric authentication is simulated in MATLAB R2017b. The database used consists of training and testing images.

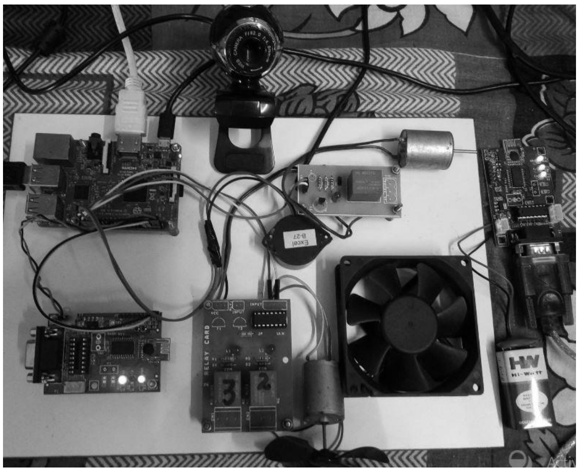


Fig 3 Implemented system

The given RGB input image is converted into a grayscale image as shown in fig 4.

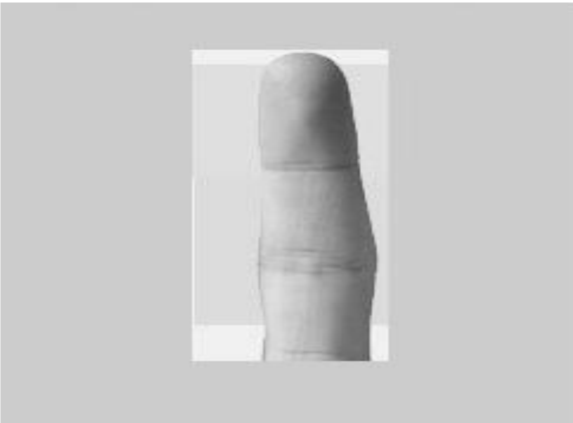


Fig 4 RGB to gray scale conversion

The features extracted from grayscale image are shown in fig 5.

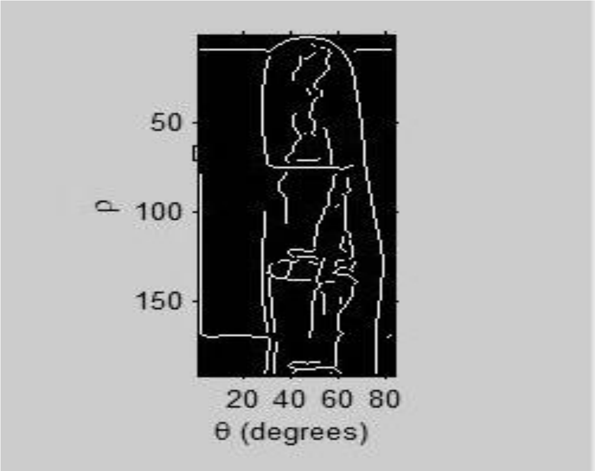


Fig 5 Gray scale feature extraction

The features extracted for the matching purpose is shown in fig 6. Raspberry Pi is used to control the relay and also acts as interface to the android application. The server running on the raspberry pi device is written in python.

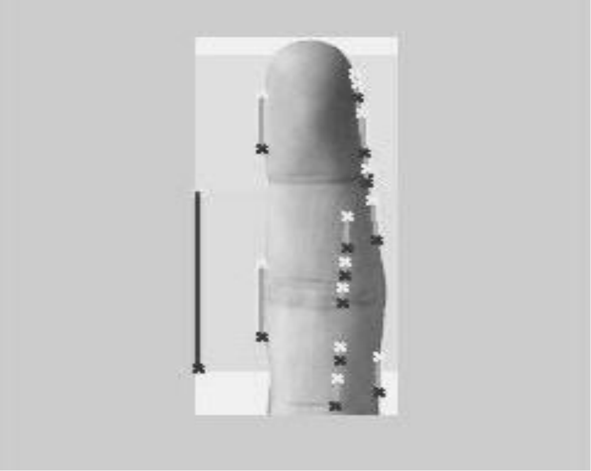
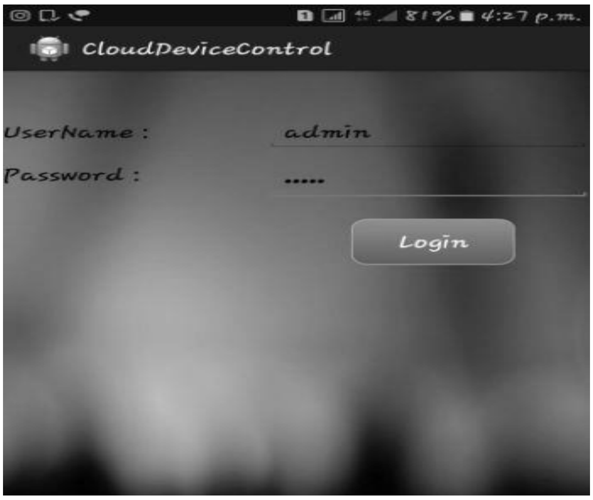


Fig 6 Extracted features

The login page of the device control app is shown in fig 7 and user interface for controlling appliances is shown in fig 8.



CloudDeviceControl

UserName : admin

Password : .....

Fig 7 Login page

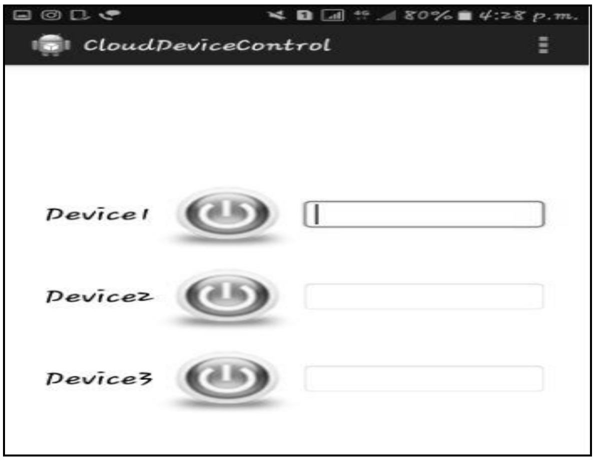


Fig 8 Device control page

In the proposed system users will be able to control a maximum of eight appliances using the android application. The controlling operation on three devices is shown in table I.

Table I Device Control Operation

8-bit data	Operation
00000000	All 3 devices OFF
11100000	All 3 devices ON
10000000	Device 1 ON, Devices 2 and 3 OFF
01000000	Device 2 ON, Devices 1 and 3 OFF
00100000	Device 3 ON, Devices 1 and 2 OFF
11000000	Devices 1 and 2 ON, Device 3 OFF
01100000	Devices 2 and 3 ON, Device 1 OFF
10100000	Devices 1 and 3 ON, Device 2 OFF

Device 1 indicates light, device 2 indicates fan and the device 3 indicates air conditioner. The finger vein biometric is used to recognize whether the person who tries to open the door is authorized or not. When the recognition is successful the door will be made open. Otherwise an error message is displayed and the theft buzzer rings. Also, the camera which is fixed at outside of the home captures the image of unknown person and sends it to the owner's mail id. The performance evaluation of the finger vein biometric based authentication system is measured using the false acceptance rate (FAR) and false rejection rate (FRR) parameters. FAR is defined as the ratio of the number of false acceptances to the number of identification attempts. i.e. it measures the acceptance of unauthorized users by the biometric system. The FRR is the metric that a biometric authentication system will falsely reject an access attempt by an authenticated user. FRR is the ratio of the number of false rejections to the number of identification attempts. The formulas for computing the FAR and FRR are shown in (1) and (2). From the experimental results for 100 images of 10 fingers, the obtained FAR and FRR values is given in table II. The EER is calculated as 0.01%. From the observation, EER of the recognition process using proposed method is less and thus the proposed method provides better accuracy.

$$FAR = \frac{Total\_successful\_fradulent\_attempts}{Total\_verification\_attempts} \quad (1)$$

$$FRR = \frac{Total\_false\_rejection\_attempts}{Total\_verification\_attempts} \quad (2)$$

Table II Obtained FRR and FAR values

No. of users	No. of images	FAR%	FRR%	EER%
10	100	2.72	4.66	0.015

V. CONCLUSION

Smart homes have become a reality for common people to easily monitor and manage their homes. Apart from the network based threats, smart homes need to be protected from intruders and burglars.

This paper proposes a finger vein based biometric authentication system that verifies the users before granting them access to smart homes. The finger vein features are extracted using K means segmentation and Canny edge detection algorithm and matched with the stored features using SVM classifier. The output of the authentication process is given as input to the Raspberry PI Kit which is used to implement the smart home automation system Experimental results have proven that this authentication system has a lower EER, FAR and FRR values when compared with the existing systems. Finger vein biometric systems also suffer from presentation attack. As a future enhancement, mitigation of this attack can be done to improve the smart home automation system.

REFERENCES

1. J. Gubbia, R. Buyyab, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions", International Journal on Future Generation Computer Systems, Elsevier, Vol. 29, Issue 7, 2013, pp. 1645-1660.
2. A.R.Al-Ali and M. AL-Rousan, "Java-based Home Automation System", IEEE Transactions on Consumer Electronics, Vol. 50, Issue 2, 2004, pp. 498-504.
3. A.Z.Alkar and U. Buhur, "An Internet Based Wireless Home Automation System for Multifunctional Devices", IEEE Transactions on Consumer Electronics, Vol. 51, Issue 4, 2005, pp. 1169-1174.
4. Y. Lu, S. Wu, Z. Fang , N. Xiong, S. Yoon, D.S. Park, "Exploring finger vein based personal authentication for secure IoT", International Journal of Future Generation Computer Systems, Elsevier, Vol. 77, Issue C, 2017, pp.149–160.
5. B. Miller, "Vital signs of identity [biometrics]", IEEE Spectrum , Vol. 31, Issue 2 , 1994, pp. 22-30.
6. R.R. Tallam, S.S. Temgire, R.M. Zirange, "Finger Vein Recognition System using Image Processing", International Journal of Electrical, Electronics and Data Communication, Vol. 2, Issue-5, 2014.
7. L.Chunyi, L. Mingzhong and S. Xiao, "A Finger Vein Recognition Algorithm Based on Gradient Correlation", AASRI Conference on Computational Intelligence and Bioinformatics, Elsevier Procedia, Vol.1, 2012, pp. 40–45.
8. T.Thilagavathy and K. Siruba, "Personal Verification through Finger Vein Pattern Recognition using Support Vector Machine", International Journal of Applied Sciences & Engineering, Vol.2, Issue 1, 2014, pp. 13-20.
9. N. Miura, A. Nagasaka and T. Miyatake, "Extraction of Finger-Vein Patterns Using Maximum Curvature Points in Image Profiles", IEICE Transactions on Information and Systems, Vol. E90-D, Issue 8, 2007, pp.1185-1194.
10. Y. Erol, H.H. Balik, S. Inal and D. Karabulut, "Safe and Secure PIC Based Remote Control Application for Intelligent Home", International Journal of Computer Science and Network Security, Vol.7 No.5, 2007, pp. 179-182.
11. N.Sangle, S. Sanap, M. Salunke and S.Patil, "Smart Home System based on IoT", International Journal of Emerging Technology and Advanced Engineering, Vol. 6, Issue 9, 2016, pp. 168-170.
12. A.D'mello, G. Deshmukh, M. Murudkar and G. Tripathi, "Home Automation using Raspberry Pi 2", International Journal of Current Engineering and Technology ,Vol.6, Issue 3, 2016, pp. 750-754.
13. N. Dhanachandra, K. Manglem, Y.J. Chanu "Image Segmentation Using K -means Clustering Algorithm and Subtractive Clustering Algorithm", Procedia Computer Science,Vol. 54, 2015, pp. 764-771.
14. J.Canny, "A Computational Approach to Edge Detection", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 8, Issue 6, 1986, pp. 679–698.

AUTHORS PROFILE

R.Sarala has completed her Ph.D in Computer Science and Engineering at Pondicherry Engineering College, Pondicherry, India. Her research interests include Machine learning, Information Security and Soft Computing. She is a life member of Indian Society of Technical Education.

E.Yoghalakshmi has completed B.Tech Computer Science and Engineering, at Pondicherry Engineering College, Pondicherry, India.

V.Ishwarya has completed B.Tech Computer Science and Engineering, at Pondicherry Engineering College, Pondicherry, India.