

A Prototype based Multibiometric Authentication System for Smart House Door System using Arduino

Balraj E.^{1*}, Abirami T.²

¹Assistant Professor, Department of Information Technology, M.Kumarasamy College of Engineering, Karur, Tamil Nadu, India. Email: balraje.it@mkce.ac.in

²Associate Professor, Department of Information Technology, Kongu Engineering College, Perundurai, Tamil Nadu, India. Email: abiananthmca@gmail.com

Abstract. In recent days, Biometrics becomes essential part of our life. Because it provides more security than other properties. People can apply biometric authentication in any field such as online exam, door access control, banking, identifying people, intelligent agent. The intelligent house becomes standard for the past few years. It will give a security and cozy to the house owner. However, the protection is incredibly necessary, it should be determining the house owner accurately and forestall the system to create an error for identification. Our proposed frameworks use finger print, facial recognition to make a system just like the security to create a identity and observation the protection of building.

Keywords: finger print, face recognition, smart home door, multi biometric, intelligent house.

II. INTRODUCTION

Labour productivity has a major impact on cost, time and in today's busy world, security may be a major concern and everybody can rummage around for reliable ways in which to ensure safety. The old ways that of securing our homes and belongings was victimization key and lock systems which is kind of inefficient as keys are duplicated. Later consecutive level of protection was provided by fashionable technologies with PIN and passwords. fashionable systems are quite economical however it also can be hacked and gain access. so as to achieve high accuracy and responsibility, biometric authentication technology has been introduced that uses physical or

behavioral characteristics to verify a private. the most reason to settle on biometric identification technology over ancient methodology of identification is that ancient identification techniques are vulnerable to security, not reliable and insecure. Majority of developed biometric systems use single biometric technology for identification and verification. These unimodal systems are unable to satisfy a number of the challenges like enrolling large populations, high performance etc. Later a complicated biometric authentication technology with better performance and high accuracy rate referred to as multimodal biometric recognition system is being introduced. Multimodal systems are capable of victimization 2 or additional physical or behavioral characteristics of humans to enroll, verify and supply call. Multimodal biometric systems additionally mix 2 or additional identification. Technologies like fingerprint systems and iris recognition systems with multiple sensors and provides decision by combining results from every system. once victimization multimodal biometric systems if one sensing element or system fails to perform identification the opposite systems is wont to create call. Multimodal systems can be utilized in varied areas like in homes for biometric based mostly door locks to stop felony, in hospitals to record patients details, in package firms and academic establishments to keep up attending, in banks for secure and safe process of payment, biometric alarm systems just in case of information security in varied sectors. Multimodal systems are additional advantageous and overcomes all the constraints of unimodal systems with increased security, high accuracy and liveliness.

II. WHY BIOMETRIC?

The traditional methods are used to create and believe that one thing is secure and personal is that the use of passwords, keys and locks that are available in varied modes and functionalities locomote from automatically manual to electronically automatic. However, the keys and passwords we tend to purchase and build have the chance to be lost or forgotten, relatively easily. Biometric systems eliminate such hazards and risks, create the optimum use of what we've integrated among our own body as our organs and components. It becomes easier to grasp the Significant want for biometric once a personal loses her/his word that sometimes can't be retrieved. As per the Article of PBworks, "Aside from what is called "logical" use—using a finger scanning or another sort of technology to determine if a user is allowed to access information—biometrics can even offer appropriate folks access to a faculty building or space. biometric is not just for within walls, either. Banks are observing the technology to interchange cards and PINs at ATMs.

There's potential for victimization biometry to verify payment in on-line purchases. "Moreover, PBworks defines the gravity of the necessity of biometry with a awfully practical example through a probe conducted among the scholars and also the academics in a faculty in national capital. specializing in the matter of word remembrance and also the exchange of user names and passwords by students, Kvarnby faculty enforced a finger print work system for each users that in total is numbered to 450. This had made the login method safer and easier and additionally verified to avoid wasting five hundredth room time of a 40-minute lecture. [6]As mentioned on top of, it's not solely the benefit of use that's the aim of biometry, it is also the elimination of pricey (some word creation, configuration and maintenance company has their value limit to \$350) and overwhelming passwords (every folks World Health Organization use on-line services, and digital devices has over 5-10 passwords, and it becomes more durable and more durable to recollect and verify the security of passwords themselves) has become inevitable because the variety of forgery, fraud and villainous activities increase on a daily basis. The overwhelming variety of passwords

will eventually lead a personal to put in writing the word to another devices which might be intercepted or hacked, or perhaps the passwords typically are written in papers that has a high likelihood to be purloined or lost. Biometrics, in some level eliminates the employment of paper whereas saving the passwords and aids in minimizing the access use of papers.

Along with these advantages, biometry helps in increasing money responsibility, physical security like any quite possessions, building entrances is controlled and keep the flow as desired by the owner.

Since a identification system uses the computer code of AN electronically hold on unique and specific biological, physiological or activity characteristics referred to as biometric templet, of a personal, that is later compared with the templates gift in every and each individual whereas work in or requesting for AN access, it cannot fall prey to hackers and/or be lost, guessed by anyone, or be shared by anyone else.

III. LITERATURE REVIEW

[2] Bregman proposed the HI nodule, as delineate for the universal implementation model for the smart intelligent home. Because of the quality of good home systems and devices, their numerous areas of management and supervision, the variability of knowledge technologies and learning mechanisms, and the reasoning capabilities utilized in change the knowledge system, developers, suppliers and users should get together. Moreover, all devices and systems should be compatible with common standards supported the universal model. This info will then be analyzed and used for AI learning and to boost the system's reasoning mechanisms.

[3]Vijay Srinivasan et all proposed methodology tend to measure the utilization of height for identification of residents, by mounting inaudible distance sensors on top of the doorways in an exceedingly home. Height sensors are low cost, convenient for the residents, easy to put in in associate degree existing home, and looked as if it would be less invasive than cameras or microphones. Height is usually solely a weak biometric, however we tend to show that it's like minded for distinguishing among some residents with in the home, and might probably be improved by victimization the history of height measurements at

multiple doorways in an exceedingly following approach.

[4]Kamer visi proposed a completely unique multimodal identity verification approach fusing iris and fingerprint traits at score-level. we tend to chiefly explore the fusion of iris and fingerprint biometry and their potential application as biometric identifiers. The individual comparison scores obtained from the iris and fingerprints area unit combined at score-level employing a 3 score standardization techniques (Min-Max, Z-Score, Hyperbolic Tangent) and 4 score fusion approaches (Minimum Score, most Score easy total and User Weighting).

IV. PROPOSED SYSTEM

A. Hardware Implementation

1)Arduino UNO

Arduino UNO is used here to control the operations involved in Intelligent Home. There are 4 operations are involved in this prototype: Register, Verify, Delete, Reset. Arduino is very flexible to code and use, code and also supports to include more no of module.

2)Fingerprint sensor

R307 is AN optical fingerprint scanner that is an upgraded version of R305. R307 has its own info which may store a thousand templates. Security level for R307 is from 1-5. This module has less false error rate, quick looking out process, high speed processor, easy to work with finger print templates.

3)ESP32

It is less expensive development board with a very small size camera with a micro card SD. It is used to store the images. It has in build wifi, Bluetooth, high-performance 32-bit LX6 CPUs, 7-stage pipeline architecture.

4)Buzzer

It is used to give the alert tones for the user when the scanning of the finger print and face is getting delayed.

5)LCD Display

It is used to display the output of the authorization process, If finger print and face are matches with the database then access will be granted otherwise the access will be denied

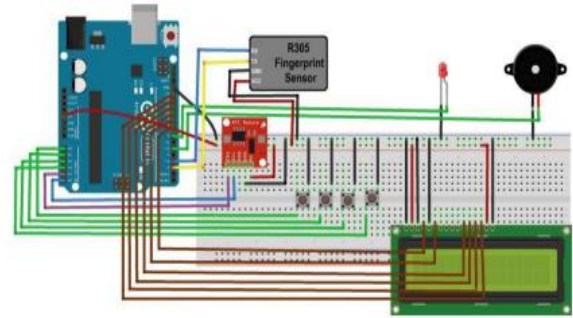


Figure 1 - Hardware View

B. Software Description

1)Arduino IDE

It is used to write the program logic for the Arduino UNO.

2) Adafruit Fingerprint Sensor Library

It is special library used to read and verify the finger prints of the house owner. Initially system was trained with more than one finger print images (same finger) of the user. During the authentication process, captured images will matched with templates available in the library.

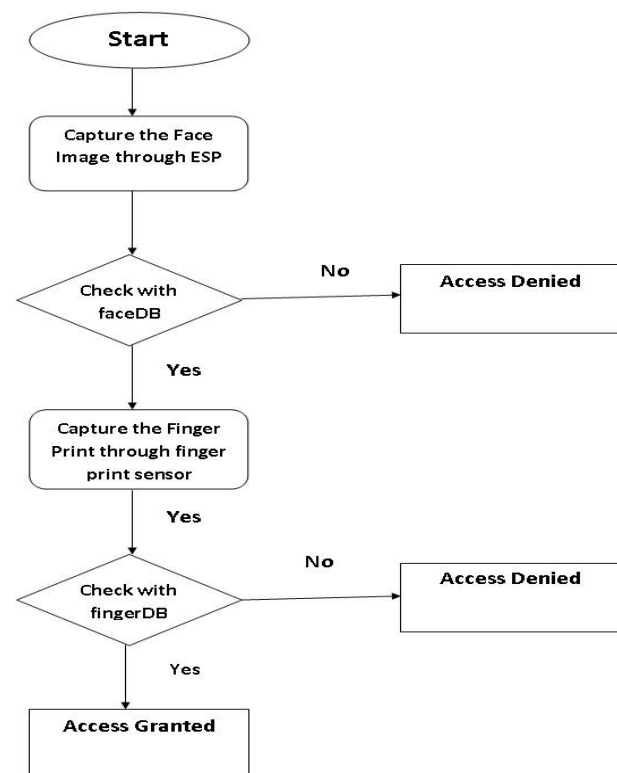


Figure 2 – Flow Diagram of Proposed System

V. QUALITY METRICS

The effectiveness of any biometric authentication system was measured with 4 attributes.

- False Acceptance Rate
- False Rejection Rate
- True Positive Rate
- False Negative Rate

a) False Acceptance Rate (FAR):

It is used to measure the number of incorrect samples was accepted by the system.

$$FAR = \frac{\text{No of Incorrect Samples accepted}}{\text{No of attempts}}$$

b) False Rejection Rate (FRR):

It is used to measure the number of correct samples was rejected by the system.

$$FRR = \frac{\text{No of correct Samples Rejected}}{\text{No of attempts}}$$

c) True Positive Rate (TPR)

It is used to measure the number of correct samples was accepted by the system.

$$TPR = \frac{\text{No of correct Samples accepted}}{\text{No of attempts}}$$

d) False Negative Rate (FNR):

It is used to measure the number of incorrect samples was rejected by the system.

$$FNR = \frac{\text{No of incorrect Samples Rejected}}{\text{No of attempts}}$$

VI. EXPERIMENTAL RESULTS

Our proposed system use with database images which consists of the 100 members finger print & face images. For every person, we have taken 5 finger print images, 5 face images. The implementation of the prototype was done using Arduino.

Table 1 – Performance Analysis on Proposed Method

Factors	Only Face	Only Fingerprint	Both
TPR	96.40%	96.80%	98.60%
FAR	0.04	0.05	0.03
FRR	0.03	0.02	0.01

True positive Rate will take into consideration for the number of correct users accepted by our proposed method. TPR will be high for our proposed method when it compares to single biometric authentication (Only Face, Only Fingerprint).

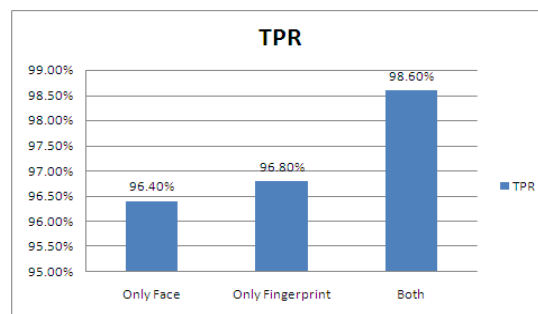


Figure 3 Performance Analysis on TPR

False Acceptance Rate will take into consideration for the number of incorrect users accepted by our proposed method. FAR is less in our proposed method when it compares to single biometric authentication (Only Face, Only Fingerprint).

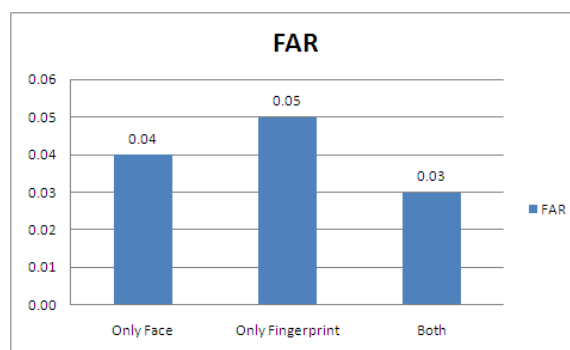


Figure 4 Performance Analysis on FAR

False Rejection Rate will take into consideration for the number of correct users rejected by our proposed method. FRR is less in our proposed method when it compares to single biometric authentication (Only Face, Only Fingerprint).

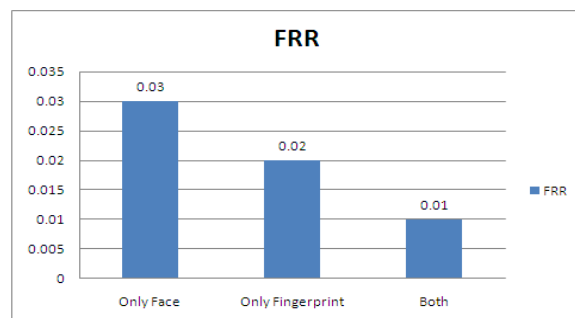


Figure 5 Performance Analysis on FRR

Any biometric authentication system TPR is high and FAR, FRR is less than that system will produce effective result.

Based on the above three results, our biometric authentication system TPR is high and FAR, FRR is less. So our proposed methodologies will effective result in biometric authentication.

VII. CONCLUSION

The proposed work achieved high accuracy than other methods. When we are using single biometric authentication system for smart house door, there is high number of chances are there correct users may not be given permission to access door for few times. But in the case of multi biometric authentication system, authentication is being based on the two factors. So when the acceptance rate of one system is low and another system gives high acceptance rate (Based on threshold factor), The correct user is having less number of chances for rejection to access the door. Multi biometric authentication system will give you better result than single biometric authentication. The above prototype was developed with the help of Arduino board, Finger Print Sensor, ESP32. There are 500 samples were taken and considered for the model. Based on our work, when we are fusing the finger print along with face recognition will give the better result compare to existing authentication systems It is also cost effective method to implement and also our proposed method gives accuracy 98.60% (Based on the 100 user's samples).

REFERENCES

[1]. ISHENGOMA, FREDRICK. (2014). AUTHENTICATION SYSTEM FOR SMART HOMES BASED ON ARM7TDMI-S AND IRIS-FINGERPRINT RECOGNITION TECHNOLOGIES. CIIT INTERNATIONAL JOURNAL OF PROGRAMMABLE DEVICE CIRCUITS AND SYSTEMS. 6. 162 – 167. 10.5815/IJIEEB.2014.06.08.

[2]. D. Bregman, "Smart Home intelligence – The eHome that Learns", International Journal of Smart Home, Vol.4, No.4, 2010.

[3]. Vijay Srinivasan, John Stankovic, Kamin Whitehouse, "Using Height Sensors for Biometric Identification in Multi-Resident Homes", Pervasive Computing, 8th International Conference, Pervasive

2010, pp. 337-354, Helsinki, Finland, 2010.

[4]. Rishi, Kamer & Yildirim Yayilgan, Sule. (2013). "Multimodal Biometric Authentication Using Fingerprint and Iris Recognition in Identity Management". 334-341. 10.1109/IIH-MSP.2013.91.

[5]. M. M. Monwar and M. L. Gavrilova, "Multimodal biometric system using rank-level fusion approach, "IEEE Trans. Syst., Man, Cybern. B, Cybern., vol. 39, no. 4, pp. 867878, Aug. 2009.

[6]. P. Paul, M. L. Gavrilova, and R. Alhajj, "Decision fusion for multimodal biometrics using social network analysis," IEEE Trans. Syst., Man, Cybern., Syst., vol. 44, no. 11, pp. 15221533, Nov. 2014.

[7]. Funsho Tosin Enahoro, Sudhasini Raman Kutty, "Biometrics Based Security System Using Arduino" International Journal of Information System and Engineering, Vol. 8 (No 1.), April, 2020. pp30-51.

[8]. Magdin, Martin & Koprda, Stefan & Eubor, Ferenczy. (2018). Biometrics Authentication of Fingerprint with Using Fingerprint Reader and Microcontroller Arduino. Telkomnika (Telecommunication Computing Electronics and Control). 16. 755-765. 10.12928/TELKOMNIKA.v16i2.7572.

[9]. Meenakshi, N & Monish, M & Dikshit, K & Bharath, S. (2019). Arduino Based Smart Fingerprint Authentication System. 1-7. 10.1109/ICIICT1.2019.8741459.

[10]. Mahesh Bhanushali,, Manish Bhanushali,, Darpan Bhanushali, Archana Chaugule, Manish Bhelade, " Biometric Authentication System using Arduino" Journal of Advancement in Parallel Computing Volume 3 Issue 3, PP1-5.

[11]. E.Balraj, T.Dinesh, S.Deepan, N.Nattuduraj, "CNN Based Multimodel Biometric Authentication System Using Face And Fingerprint", International Journal of Future Generation Communication and Networking, Volume 13, Issue 02, PP 1536 – 1539.

[12]. Dr.T.Abirami E.Balraj, "A Multibiometric Authentication System Using Fusion Level Techniques" , International Journal Of Scientific & Technology, Volume 09, Issue 01, PP - 3332-3335.