I.J. Wireless and Microwave Technologies, **2022, 2, 40-50**
Published Online April 2022 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2022.02.04

Smart Home Security Using Facial Authentication and Mobile Application

Khandaker Mohammad Mohi Uddin
Department of Computer Science and Engineering (CSE), Dhaka International University (DIU), Dhaka-1205, Bangladesh
E-mail: jilanicsejnu@gmail.com

Shohelee Afrin Shahela, Naimur Rahman, Rafid Mostafiz, Md. Mahbubur Rahman
Department of Computer Science and Engineering (CSE), Dhaka International University (DIU), Dhaka-1205, Bangladesh
E-mail: {shohele.afrin, nrd.durjoy65, rafid.dka, mahbub.shimulbd}@gmail.com

Received: 18 December 2021; Revised: 20 January 2022; Accepted: 20 February 2022; Published: 08 April 2022

Abstract: In this fast-paced technological world, individuals want to access all their electronic equipment remotely, which requires devices to connect over a network via the Internet. However, it raises quite a lot of critical security concerns. This paper presented a home automation security system that employs the Internet of Things (IoT) for remote access to one's home through an Android application, as well as Artificial Intelligence (AI) to ensure the home's security. Face recognition is utilized to control door entry in a highly efficient security system. In the event of a technical failure, an additional security PIN is set up that is only accessible by the owner. Although a home automation system may be used for various tasks, the cost is prohibitive for many customers. Hence, the objective of this paper is to provide a budget and user-friendly system, ensuring access to the application and home attributes by using multi-modal security. Using Haar Cascade and LBPH the system achieved 92.86% accuracy while recognizing face.

Index Terms: Smart home security, Internet of Things (IoT), Artificial Intelligence (AI), Face recognition, door access, Android application.

1. Introduction

Technology has advanced beyond our wildest dreams, bringing a new era of AI-powered electronics. Over the last decade, the demand for IoT-enabled home automation has skyrocketed. IoT is a technology that links gadgets over a network and allows users to control all aspects of their house remotely [1, 2]. Home automation aids in the monitoring and management of many aspects of the home in order to give a better living. Home automation allows you to monitor and control many aspects of your home to improve your living. The majority of countries are gradually implementing a smart security system. The most important aspect of any security system is precisely identifying inhabitants in order to provide access. Face recognition is likely one of the most logical methods of human authentication.

As the need for home automation grows, so does the number of security breaches. Burglary has long been a source of concern to Bangladeshis, and it is rather widespread in both urban and rural areas. Over 4,500 house burglaries occur every day in the United States, accounting for 77 percent of all offenses. Intruders utilize the front entrance of the property around 34% of the time, and 25% of homeowners who try to oppose the thief become victims of violence. Three out of every four residences will be broken into during the next two decades [3]. Despite the fact that the United States is a developed country, the rate of property crime is relatively high, making Bangladesh more vulnerable to property crime due to its underdevelopment and overcrowding. As a result, a safe home automation system is a must in Bangladesh, where crime is on the rise.

The face recognition scheme is one of several biometric security approaches that may be utilized in a home automation system. It's a type of physiological biometric technology that's used to identify and authenticate people. The input for the recognition procedure is gathered from video frames in the instance of a probable crime scene. The procedure is carried out with the aid of artificial intelligence (AI), utilizing data that has been previously trained.

The proposed approach in this work utilizes AI and IoT to construct a home automation system with security features to assist homeowners in monitoring their home 24/7. In addition, ObSpy, a mobile application, has been developed to allow owners to effectively monitor and securely manage home characteristics from anywhere at any time. The key contributions of this paper are given as follows:

- The integration system is based-on Internet of things (IoT), and mobile application.
- The structural design established through IoT mechanism along with the Raspberry PI.
- The security system is developed by using face detection and recognition.
- Developed mobile application helps to get the notification of unauthorized users.

This paper presents the related works in **Section 2**. **Section 3** talks about the proposed system, **Section 4** discusses the methodology, **Section 5** gives the results and analysis, and lastly, the conclusion of the project is in **Section 6.**

2. Related Works

There are a lot of research papers in the fields of home security using IoT and AI, all with a common goal to make life easier. Ibrahim et al. [1] presented a framework for a biometric door lock for home protection, in which they examine security concerns and solutions. A fingerprint scanner is used in the system to automate the identification and authentication of a person. Tiwari et al. [2] proposed an intelligent security system that uses a remote-controlled door lock with a pre-programmed application. The homeowner may use the app to open and close doors, as well as allow visitors inside the house or leave the entrance unlocked if the visitor is unknown.

Khattar et al. [4] proposed utilizing the Raspberry Pi to create a smart house with a virtual assistant (Olivia). If the individual is unknown, Olivia approaches them and asks for their name, as well as permission to leave a note if necessary. Deepty et al. [5] proposed a biometric door access control system with an android phone to validate authorized users. Pawar et al. [6] developed a smart home system that included sensors and employed facial recognition. The door will unlock if the face is recognized; otherwise, the doorbell will automatically ring.

Maheshwari et al. [7] presented a Microsoft face API-based smart door with face recognition. They utilize an HD camera on the front entrance that is connected to a display monitor to keep track of who is standing there. Gunawan et al. [8] proposed utilizing a Raspberry Pi to manage door entry using a facial recognition security system. The door in their system locks/unlocks based on their facial recognition algorithm, which is implemented in Python and OpenCV.

Manjunatha et al. [9] proposed a system where the face recognition process is implemented by the PCA approach. Their system includes auto Police e-Complaint registration that sends a security alert e-mail to the nearby police station. Balaprasad et al. [10] suggested a facial recognition security solution based on the SIFT (Scale Invariant Feature Transform) method. Face recognition, door entry, and SMS sending are the three components of the system. A command from the ARM7 processor causes the door to open automatically for a recognized individual. If the individual is unknown, however, an alert will sound and an SMS will be sent to the control centre.

Deshmukh et al. [11] presented a system that, once the bell is rung, enables real-time face recognition. The taken image is evaluated, and if a match is discovered, the door is opened; however, if the face is not matched, the captured image is forwarded to the owner's e-mail address through SMTP (Simple Mail Transfer Protocol). The system then waits for the owner to respond within a certain amount of time. Door access will be given or refused based on the returned response. Sahini et al. [12] developed a system that can be used on the web as well as on a GSM platform. For facial recognition, they employed the PCA method, and customers may monitor real-time actions via web services/SMS. Face-recognition based attendance system has been developed by Uddin et al. [13] to take the real time attendance.

Shah et al. [14] presented a home automation system based on the Internet of Things and a mobile app. The authors performed research on how smart software applications linked with hardware may be used to automate household appliances. Mostakim et al. [15] created an intelligent home automation and environmental solution, as well as a sensor module architecture. This proposed system includes a biometric fingerprint scanner and an electronic lock with password verification. These sensors guarantee that illegal access to the system is prevented.

3. Proposed System Architecture

This study presents an enhanced secured smart home system to remotely regulate house characteristics and monitor door entry in order to overcome the faults of existing systems. A multimodal security system and a mobile phone app for regulating house features, such as door locks, are the core components of the system.

Fig 1. depicts the outline of the proposed paper. The security system ensures that the house, particularly the front, is safe from prospective intruders. Furthermore, smart home gives consumers complete control over their home features, which are linked to the Android platform.

3.1. Proposed System

This paper proposes a smart home security system, as it is a massive concern for residents. The system uses Raspberry Pi as the primary control device, since its components are embedded into a single chip [16]. Raspberry Pi consists of all the program codes, which can be remotely controlled via Android application with the help of IoT. The system architecture is divided into three modules are given as follows and shown in Fig.2.

I. *Android Application Module*: The app consists of an admin panel that allows the owner to add/remove face ids and home attributes. Additionally, owners can remotely monitor the house and decide whether to grant door access or to trigger the alarm system, after receiving a notification showing an image of the person.
II. *Data Processor Module*: It consists of the facial database and the program codes of the proposed system.
III. *Data Generator Module:* In this category, all home attributes including the door lock are implemented with the Raspberry Pi.

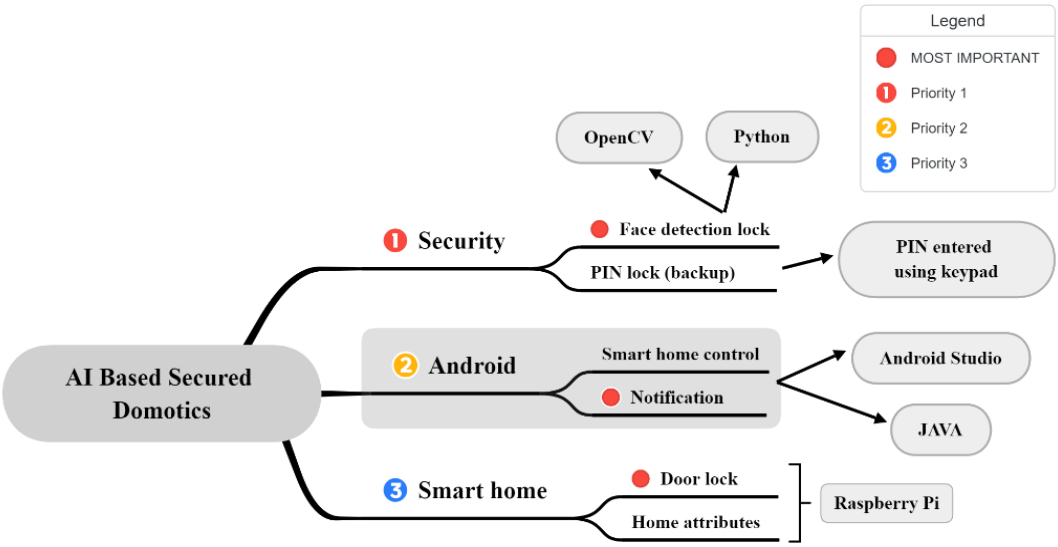

Fig. 1. Overview of our proposed system

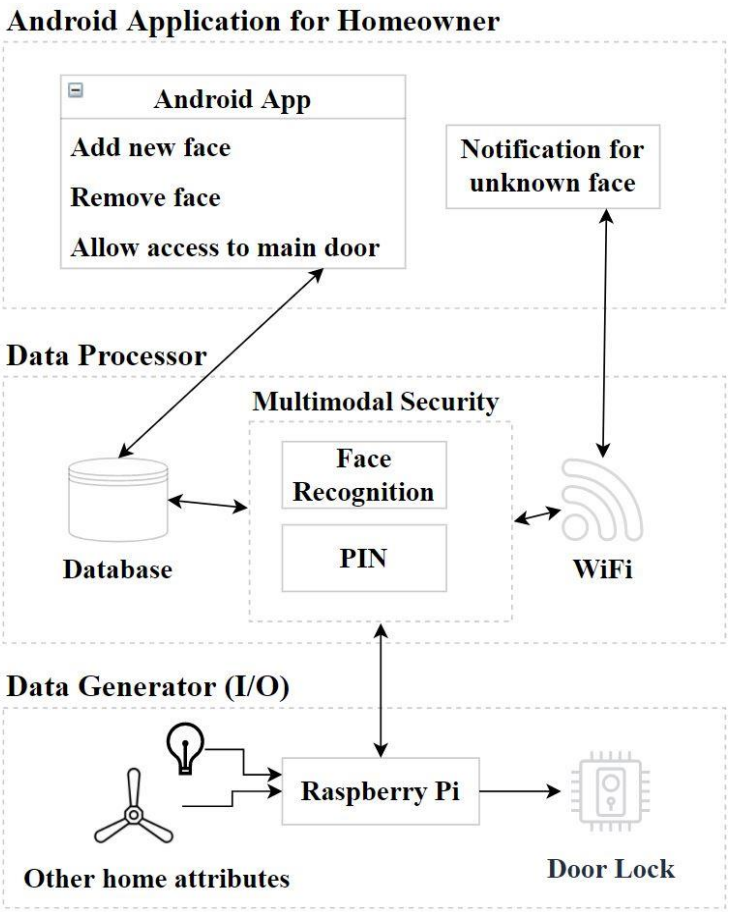

Fig. 2. The system architecture of our proposed system

3.2. Hardware and Software Requirements

The most vital hardware is the Raspberry Pi, which bears the maximum cost of the system. All the hardware (shown in Fig.3) used was chosen carefully to keep the system as budget-friendly as possible. ***Raspberry Pi 3 model b+*** has is used to implement the security system. A red ***LED*** is used on the main door to signal the user in case of a failure in face detection after system initiation.

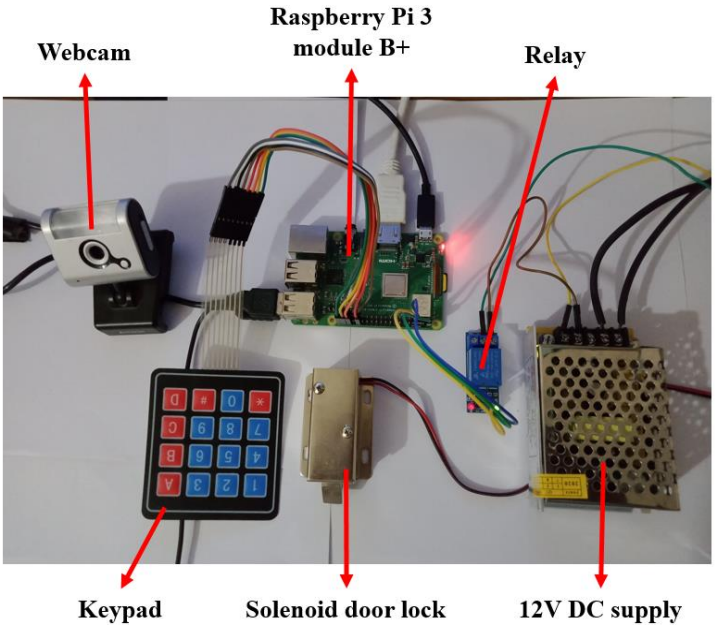

Fig. 3. The hardware setup of the proposed model

The system uses various software to make it fully functional. Here, **Raspbian OS** is used to configure the Raspberry Pi. **Python IDLE** (version 3.8) provides an environment for coding in Python language [17]. Face recognition and keypad are implemented using **PyCharm**, which requires the IDLE to execute. **OpenCV** (version 4.4) is a programming library used for real-time computer vision [18]. **Android Studio** (version 4.4.1) is used to design and implement the mobile application with JAVA programming language. **Firebase** acts as an online database for mobile/web applications [2], which is used to create a connection between the home attributes and the mobile application. It allows this system to push notifications in the mobile app when a person is not recognized.

4. Methodology

The proposed system enhances the user experience and efficiency by pairing IoT with AI. To secure the system, Haar Cascade classifier is used for face detection and Local Binary Pattern Histogram (LBPH) text operator for face recognition.

The design and implementation for the mobile application are done using Android Studio 4.4.1. Fig 4. depicts the processes of the suggested model's security mechanism. To detect a face, the security system first captures pictures from video frames. Face recognition is carried out by comparing data to a previously trained facial dataset. The door lock unlocks if the face is classed as "known," and it automatically locks after 10 seconds of closing the door. Even if the face is classed as "unknown," a 4 PIN code can be input. The door unlocks when the right PIN is entered. The alarm system will immediately activate if the erroneous PIN is entered. The alarm may be turned off with the use of the mobile app. The keypad lock is a backup security option with a PIN code that only the owner knows. In the event of a power outage, low illumination, or other technical challenges with the face recognition approach, this non-biometric option is retained.

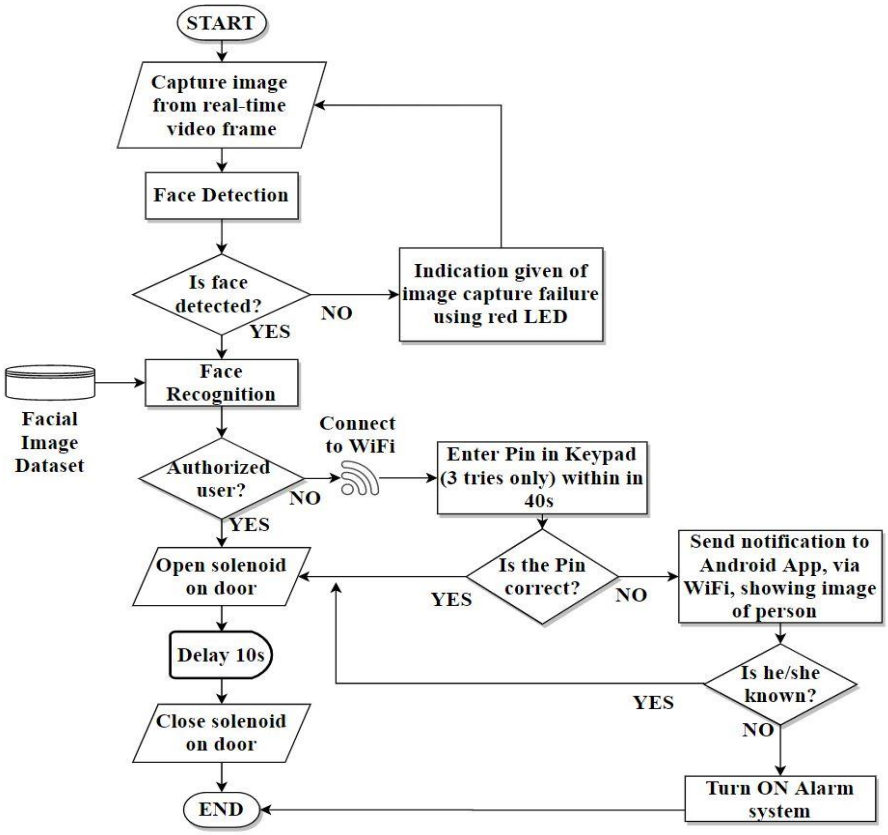

Fig. 4. Flowchart of the security system

4.1. Face Recognition

Face recognition image processing (shown in Fig. 5) begins with an input image from the video frame. An algorithm is then used to detect the face. The facial picture is normalized, improved, and cropped as part of the preprocessing procedure. The bit patterns are digitized once the features are extracted. For verification and identification, they are compared to an existing face dataset. Finally, a choice is made to recognize the face based on the match.

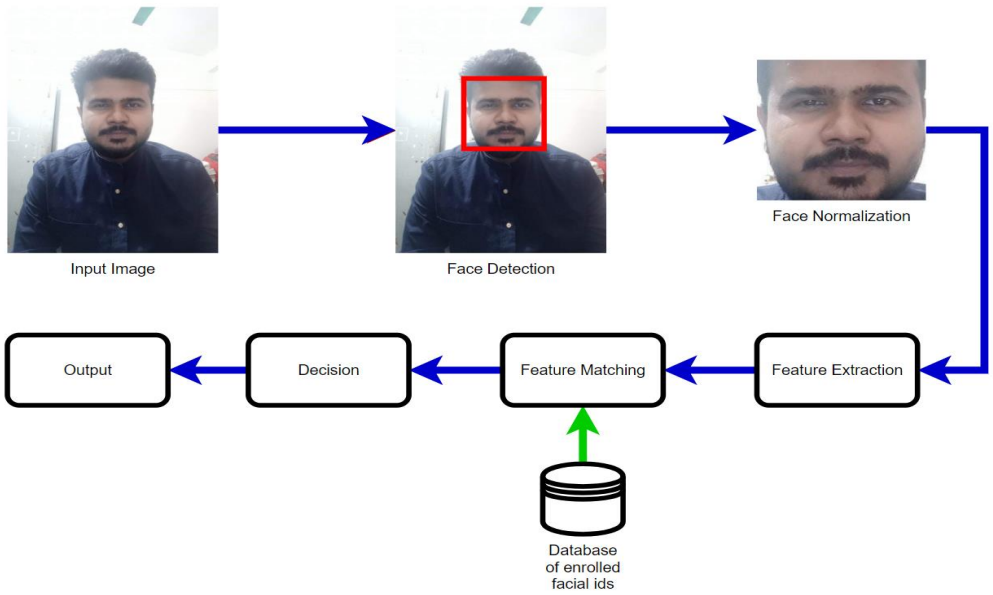

Fig. 5. Image processing steps of face recognition

4.2. Haar Cascade

The Haar Cascade is a machine learning technique that can handle a huge database. Positive (i.e. images containing faces) and negative (i.e. images without faces) images are used to train the classifier (i.e. images without face). The Haar Cascade feature takes into account nearby regions at a specified place in the source picture, allowing the total of rectangular areas to be calculated using the following equation [19],

$$sum = I(C) + I(A) - I(B) - I(D) \quad (1)$$

Where points A, B, C and D belong to the integral image I, as shown in Fig.6.

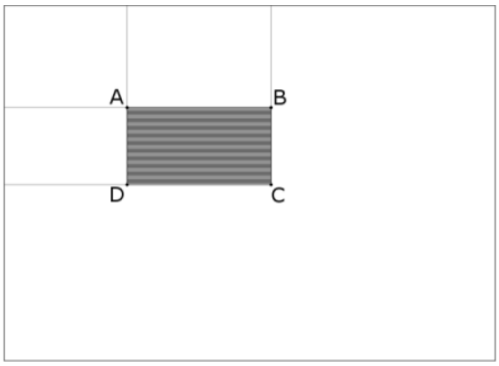

Fig. 6. Determining the sum of shaded rectangular area

4.3. Local Binary Pattern Histogram

LBPH has an improved recognition performance due to histogram combined which provides a data vector. LBPH operator works by taking an input of the captured image. The face is divided into 3*3 blocks where the histogram of each block is calculated. Later, image processing is done on the image to determine a result. The workflow diagram of LBPH is shown in Fig. 7.

During face recognition, several approaches can be used to compare the histograms, e.g. Euclidean distance, chi-square. Here Euclidean distance can be used based on the following equation [20],

$$D = \sqrt{\sum_{i=1}^{n}(hist1_i - hist2_i)^2} \quad (2)$$

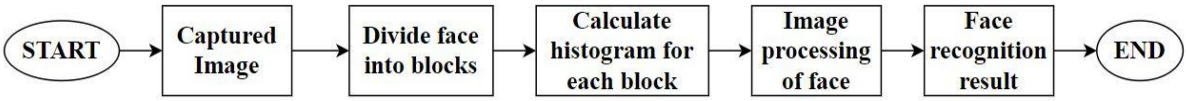

Fig. 7. Workflow diagram of LBPH operator

5. Result Analysis

The proposed system uses Raspberry Pi as the primary control device for its cost-effectiveness and reliability. It stores the Face Recognition algorithm along with all other required codes. The mobile application was developed using JAVA and Android Studio, and Firebase is used to push a notification to the application, which will contain an image of an unknown person. The interfaces – login panel, home panel and admin panel – are shown in Fig.8.

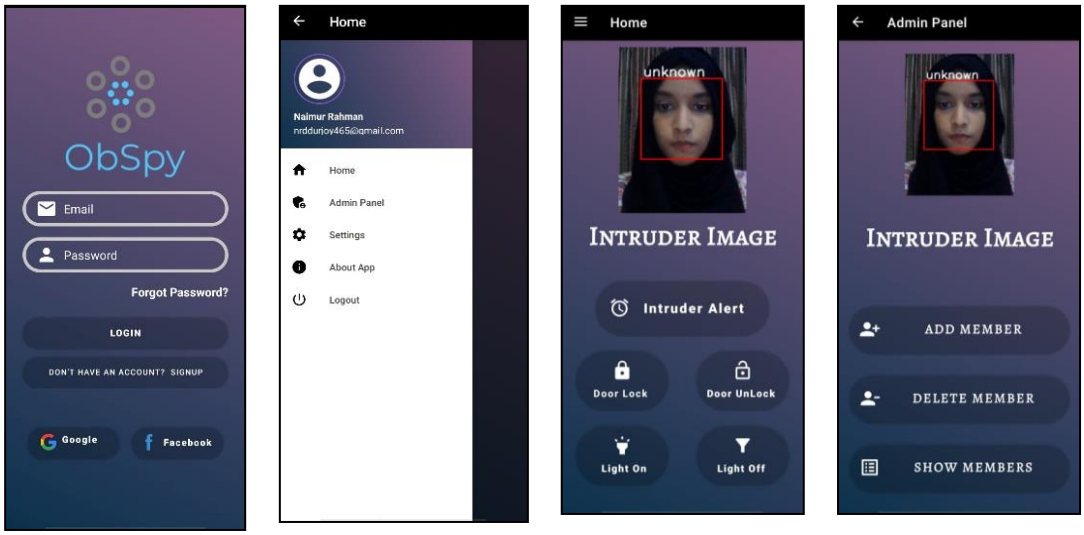

Fig. 8. User interface of the mobile app 'ObSpy'

Fig. 9 shows the control of a light using the mobile application. Upon pressing the Light ON and OFF button, the light turns on and off, respectively. Other home attributes can be controlled in the same manner.

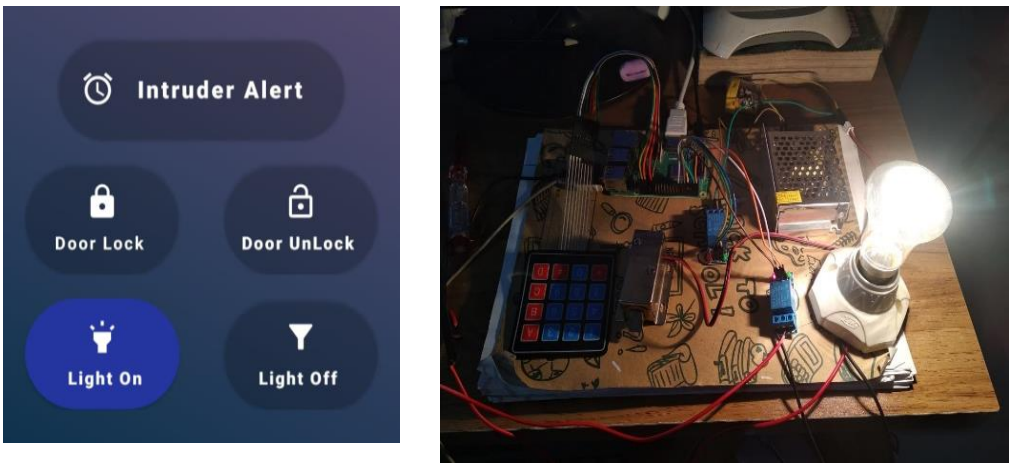

Fig. 9. Controlling home attribute (on the right side) with the mobile application (on the left side)

The confidence level is set at 80% for face recognition, which means a face will only be detected when confidence is 80 or higher. This system, on average, has a confidence of 85% as shown in Fig.10.

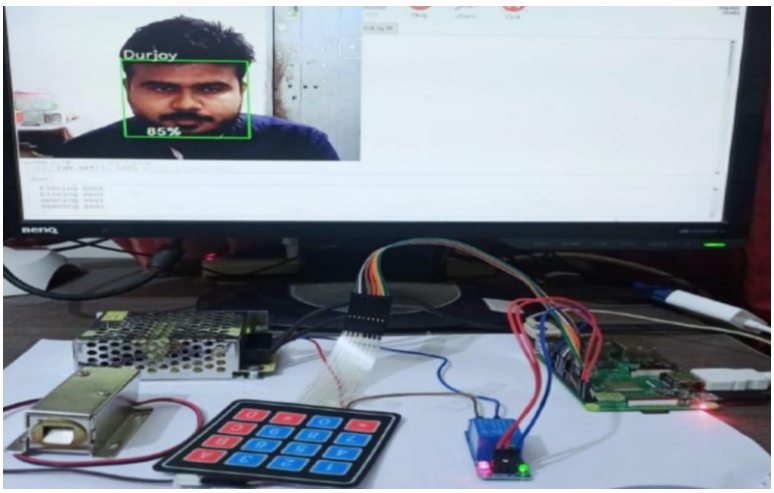

Fig. 10. Output of face recognition

5.1. Success rate of face recognition

Table 1 shows the test results of face recognition where 7 participants were taken to perform the test to find out the success rate. 10 trails were carried out per person. The test was conducted on 5 known participants, including the owner, and 2 unknown participants.

Table 1. Test results for face recognition using 7 participants

Participants	**Number of Trials**	**Success Rate (%)**
User 1 [Owner]	10	100
User 2	10	100
User 3	10	80
User 4	10	80
User 5	10	90
Unknown 1	10	100
Unknown 2	10	100

To find the success rate,

$$Success\ rate = \frac{No.of\ correct\ output}{No.of\ trails} \times 100$$

The average success rate is,

$$Average\ success\ rate = \frac{\sum Success\ rate\ of\ each\ participant}{No.of\ participants}$$
$$= \frac{100 + 100 + 80 + 80 + 90 + 100 + 100}{7} = 92.86\%$$

5.2. Test Results

The dataset is trained using 100 samples of each face. The accuracy of this system is compared with some other research papers in Table 2. The cost for building this project is approximately BDT. 6,750, which is tremendously lower than others.

Table 2. Comparison of system accuracy with other research papers

Research Papers	Algorithm	System Accuracy (%)
Pawar et al. [6]	LBP	80
Gunawan et al. [8]	PCA, Eigenface	90
Dhobale et al. [21]	LBP	80-90
Our system	Haar Cascade, LBPH	92.86

The table below gives the testing result of the proposed system. Tests were carried out several times during the development of the project, some of the test results are given in Table 3.

Table 3. Test results of the proposed system

Test measures	Expected Result	Actual Result		
		1	2	3
System boot	The system starts up without any malfunction.	Fail	Success	Success
Face ID modification	Adding/Removing a face ID using the mobile application.	Success	Success	Success
Face detection	Detecting a face	Success	Success	Success
Face recognition	Displaying the name of a known person while displaying "Unknown" for an unidentified person.	Success	Fail	Success
LED	A red LED will illuminate if the face is not detected.	Success	Success	Success
PIN lock	The door unlocks after entering a PIN.	Success	Fail	Success
Sending mobile notification	The owner is alerted via the mobile, which consists of the image of the unidentified person.	Fail	Success	Success
Regulating home attributes	Remotely controlling all home attributes using the mobile application.	Success	Success	Success

5.3. Features comparison with other works

The proposed system stands out since it is a mixture and enhanced version of all the papers mentioned earlier, as shown in Table 4 where the features are compared between this system and other research papers. It can be safely stated, after comparing, that this system is an ideal solution to home automation as it has biometric non-contact lock mechanism, making it suitable for situation like COVID-19 and also makes the entry process a whole lot faster than contact locks.

The system consists of a backup lock and all the home attributes are connected with the mobile application via firebase over the Internet (i.e. Wi-Fi or Mobile Data), hence allowing remote control and monitoring of all the attributes.

Table 4. Feature comparison between our proposed system and other research papers

Research Papers	Biometric Lock	PIN Lock	Wi-Fi	Mobile-based	Appliance Control
Ibrahim et al. [1]	✓	✓	×	×	×
Khattar et al. [4]	✓	×	×	×	×
Deepty et al. [5]	✓	×	✓	✓	✓
Pawar et al. [6]	✓	×	✓	✓	×
Gunawan et al. [8]	✓	×	✓	×	×
Balaprasad et al. [10]	✓	×	✓	✓	×
Deshmukh et al. [11]	✓	✓	✓	✓	×
Our Proposed system	✓	✓	✓	✓	✓

6. Conclusion

To summarize, the major aim is to ensure that users' property is secure. We designed a mobile application that allows the owner to remotely operate gadgets at home and monitor home qualities and activities around the house, as well as a PIN lock and facial recognition in Raspberry Pi, which can successfully lock/unlock a door. As a result of the information gathered, it can be concluded that the suggested system is both cost-effective and precise. As a consequence, it will aid in the reduction of property crimes. . The biometric approach will be upgraded in the future by including blockchain for PIN lock and employing Neural Networks to increase security. This will make any cyber-attack on the system impossible once it goes live.

References

[1] S. Ibrahim, V. K. Shukla, R. Bathla, Security Enhancement in Smart Home Management Through Multimodal Biometric and Passcode., 2020 International Conference on Intelligent Engineering and Management, IEEE, London, United Kingdom, 2020, pp. 420-424.

[2] S. Tiwari, S. Thakur, D. Shetty, A. Pandey, Smart Security: Remotely Controllable Doorlock, 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), IEEE, Coimbatore, India, 2018, pp. 979-984.

[3] P. Christo,SPENDMENOT Burglary Statistics, https://spendmenot.com/blog/burglary-statistics/,Last accessed 2021/07/08.

[4] S. Khattar, Sachdeva, A., R., Kumar, R., Gupta, Smart Home With Virtual Assistant Using Raspberry Pi, 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), IEEE, Noida, India, 2019, pp. 576-579.

[5] R.. R. Deepty, A. Alam, M. E. Islam, IOT and Wi-Fi Based Door Access Control System Using Mobile Application, 2019 IEEE International Conference on Robotics, Automation, Artificial-Intelligence-of-Things, IEEE, Dhaka, Bangladesh, 2019, pp. 21-24.

[6] S. Pawar, V. Kithani, S. Ahuja, S. Sahu, Smart Home Security using IoT and Face Recognition, 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), IEEE, Pune, India, 2018, pp. 1-6.

[7] K. Maheshwari, N. Nalini, Facial Recognition Enabled Smart Door Using Microsoft Face API, International Journal of Engineering Trends and Applications (IJETA),Volume 4 Issue 3, (2017) 1-4.

[8] T. S. Gunawan, M. H. H. Gani, F. D. A. Rahman, M. Kartiwi, Development of Face Recognition on Raspberry Pi for Enhancement of Smart Home Security, Indonesian Journal of Electrical Engineering and Informatics (IJEEI), Journal 5(4), (2017) 317-325.

[9] R. Manjunatha, R. Nagaraja, Home Security System and Door Access Control Based on Face Recognition, International Research Journal of Engineering and Technology (IRJET), Journal 4(3), (2017) 438-442.

[10] T. Balaprasad, R. V. V. Krishna, Face Recognition Based Security System Using Sift Algorithm, International Journal of Science Engineering and Advance Technology, Journal 3(11), (2015) 969-973.

[11] A. D. Deshmukh, M. G. Nakrani, D. L. Bhuyar, U. B. Shinde, Face Recognition Using OpenCv Based On IoT for Smart Door, International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Jaipur-India, 2019, pp. 1066-1073.

[12] M. Sahani, S. Subudhi, M. N. Mohanty, Design of Face Recognition based Embedded Home Security System, KSII Transactions on Internet and Information Systems (TIIS), Journal 10(4), (2016) 1751-1767.

[13] K. M. M. Uddin, A. Chakraborty, M. A. Hadi, M. A. Uddin, & S. K. Dey, Artificial Intelligence Based Real-Time Attendance System Using Face Recognition. In 2021 5th International Conference on Electrical Engineering and Information & Communication Technology (ICEEICT) (pp. 1-6). IEEE, November 2021.

[14] S. K. A. Shah, & W. Mahmood. Smart home automation using IOT and its low cost implementation. International Journal of Engineering and Manufacturing (IJEM), 10(5), 28-36, 2020.

[15] M. N. Mostakim, S. Mahmud, M. K. H. Jewel, M. K. Rahman, & M. S. Ali, Design and development of an intelligent home with automated environmental control. IJIGSP, 12(4), 1-14, 2020.

[16] Raspberry Pi Foundation, About Us, https://www.raspberrypi.org/about/, Last accessed 2020/09/23.

[17] K. M. M. Uddin, S. K. Dey, G. U. Parvez, et al. MirrorME: implementation of an IoT based smart mirror through facial recognition and personalized information recommendation algorithm. Int. j. inf. tecnol. 13, (2021) 2313–2322.

[18] K. Pulli, et al., Real-time computer vision with OpenCV, *Communications of the ACM* 55.6 (2012): 61-69.

[19] L. Cuimei, Q., Zhiliang, J. Nan, et al. Human face detection algorithm via Haar cascade classifier combined with three additional classifiers, 13th IEEE International Conference on Electronic Measurement & Instruments (ICEMI), IEEE, 2017, pp. 483-487.

[20] A. M. Jagtap, et al., A Study of LBPH, Eigenface, Fisherface and Haar-like features for Face recognition using OpenCV, International Conference on Intelligent Sustainable Systems, IEEE, 2019, pp. 219-224.

[21] M. R. Dhobale, R. Y. Biradar, R. R. Pawar, S. A. Awatade, Smart Home Security System using IoT, Face Recognition and Raspberry Pi, International Journal of Computer Applications, Journal 176(13), (2020) 45-47.

Authors' Profiles

Khandaker Mohammad Mohi Uddin is an academic researcher and an Assistant Professor in the Department of Computer Science and Engineering at Dhaka International University. He has done his B.Sc. and MSc. (Research) in Computer Science and Engineering from the Jagannath University. His research interests in the field of Wireless Networking, Software Defined Networking, Computer Vision and Image Processing, Machine Learning/Deep Learning, and IoT.

Shohelee Afrin Shahela graduated from Dhaka International University and attained B.Sc. in Computer Science and Engineering. Her research involves Artificial Intelligence, Machine learning, and the Internet of Things. She gained experience working as an analyst for a year.

Naimur Rahman, currently an Analyst, holds a B.Sc. in Computer Science and Engineering from Dhaka International University. His research explores Artificial Intelligence, Machine learning, and the Internet of Things. He plans to execute his studies in M.Sc. soon.

Rafid Mostafiz is working as an Assistant Professor at Dhaka International University in the Computer Science and Engineering department. He has completed his Master's (MSc.) and Bachelor's (BSc.) Degree in Computer Science and Engineering from Mawlana Bhashani Science and Technology University, Bangladesh. Rafid does research in Computer Vision and Image Processing, Medical Imaging, Deep Learning, Artificial Neural networks, Software Defined Networking and Algorithms.

Md. Mahbubur Rahman is a smart sensing-based researcher at the Department of Computer Science and Engineering, Dhaka International University. He has completed his B.Sc. (Eng.) and M.Sc. (Research) degree from the department of computer science and engineering, Mawlana Bhashani Science and Technology University, Tangail, Bangladesh. His research interests are in the field of Artificial Intelligence, Internet of Thing (IoT), Machine Learning and Smart Sensing. Now Mr. Rahman serves as a faculty member at Dhaka International University in the Department of Computer Science and Engineering.

How to cite this paper: Khandaker Mohammad Mohi Uddin, Shohelee Afrin Shahela, Naimur Rahman, Rafid Mostafiz, Md. Mahbubur Rahman, " Smart Home Security Using Facial Authentication and Mobile Application", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.12, No.2, pp. 40-50, 2022.DOI: 10.5815/ijwmt.2022.02.04