I.J. Intelligent Systems and Applications, **2023, 3, 44-55**
Published Online on June 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijisa.2023.03.04

Artificial Intelligence Based Domotics Using Multimodal Security

Khandaker Mohammad Mohi Uddin*
Department of Computer Science and Engineering (CSE), Dhaka International University (DIU), Dhaka-1205, Bangladesh
E-mail: jilanicsejnu@gmail.com
ORCID iD: https://orcid.org/0000-0002-5401-0437
*Corresponding Author

Naimur Rahman
Department of Computer Science and Engineering (CSE), Dhaka International University (DIU), Dhaka-1205, Bangladesh
E-mail: nrd.durjoy65@gmail.com
ORCID iD: https://orcid.org/0000-0002-4015-2741

Md. Mahbubur Rahman
Department of Computer Science and Engineering (CSE), Dhaka International University (DIU), Dhaka-1205, Bangladesh
E-mail: mahbub.shimulbd@gmail.com
ORCID iD: https://orcid.org/0000-0003-2502-4634

Samrat Kumar Dey
School of Science and Technology (SST), Bangladesh Open University (BOU), Gazipur 1705, Bangladesh
E-mail: samrat.sst@bou.ac.bd
ORCID iD: https://orcid.org/0000-0002-7999-8576

Received: 03 December 2022; Revised: 04 January 2023; Accepted: 15 March 2023; Published: 08 June 2023

Abstract: All electronic devices in our cutting-edge technology world must be networked together via the Internet if users want to have remote access to them. As a result, it may raise a variety of serious security issues. This study suggests a remote access home automation security system that incorporates utilizing the Internet of Things (IoT), and Artificial Intelligence (AI) for ensuring the security of the house. For a highly efficient security system, Face recognition has been used to maneuver the door access. In case of power outage or for any technical issues, an alternative security PIN has been added which is only accessible by the owner. Moreover, individuals are able to monitor and control the door access along with other attributes of the house using an application. In this work, Face detection is performed using the Haar Cascade classifier, while face recognition is performed using the Local Binary Pattern Histogram (LBPH). 95.7% accuracy in recognizing faces has been achieved after evaluating the proposed system.

Index Terms: Internet of Things, Automation, Face Recognition, Multi-modal Security.

1. Introduction

The evolution of technology is beyond imagination which led to an era of gadgets that use Artificial Intelligence (AI) to operate. The demand for home automation has abruptly increased over the past decade, which uses IoT. With the help of the Internet of Things (IoT), homeowners may remotely manage all aspects of their homes [1, 2]. Home automation helps monitor and control home attributes to provide a better lifestyle. A large number of countries are progressively converting to intelligent security systems. Any security system's primary purpose is to precisely identify the residents in order to grant them access. One of the most obvious methods to accomplish human authentication is possibly face recognition [3]. Home security is becoming a serious issue in our society, where anyone can be a victim even in his own house. Older security systems cannot tackle situations like system failure and lack of intelligence.

The number of IoT devices in the smart home is growing day by day. Cvitić et. al. [4] suggested a machine learning method to classify the IoT devices and that research used 41 IoT devices. Using 13 network traffic a multiclass classification model is developed by the authors and 99.79% accuracy is obtained on the traffic flow features of such devices. Precision, True Positive Ratio, False Positive Ratio, Kappa coefficient, and F-measure are used to calculate the model performance.

Due to the rise of home automation demands, security breaches are on the increase as well In Bangladesh, burglary has been a serious concern amongst people in the long run and is relatively common both in urban and rural dwellings. In the US, there are over 4,500 house burglaries on a daily basis, making 77% of the crimes being property crimes. A whopping 34% of burglars enter through the front door, and 26% of residents who attempt to fight back suffer assault. In the next two decades, it can be said that three out of four houses will be burgled [5]. Although being a civilized country, the US has a relatively high rate of property offenses, making Bangladesh more susceptible because it is a less civilized country and has a densely populated area. Thereby, a secured home automation system is a necessity in Bangladesh as the crimes are on the rise. The face detection system is one of several biometric authentication techniques that may be implemented in an automated home [6, 7]. It utilizes physiologic biometrics for identification and authentication. In case of a potential crime scene, input is taken from video frames for recognition process to occur. Data that has been trained in advance is used in the process with the support of Artificial Intelligence. The proposed solution implements a monitoring and control system with security mechanisms to assist residents in monitoring their homes around-the-clock using IoT and AI. Besides, using TKinter graphical interface, a user interface is developed to allow the owners to successfully control home attributes, and the system uses e-mail notification to alert the homeowner upon face recognition known and unknown. This work's major goal is to stop all types of property crimes by creating a security system with a dual security door lock.

This system has been taken into accounts since in recent years, despite having automation systems, either the security scheme of the systems is still an alarming issue or the cost of them are beyond reach for a handful of people. Hence, this system has been implemented for the following reasons.

- A budget-friendly system due to usage of low-cost equipment.
- Provides security for unauthorized access as it uses a multimodal security method – face recognition and keypad door lock.
- E-mail can be sent to the homeowner, keeping him/her alert of any potential door access.

2. Related Works

Researches on home security are quite massively hyped in this face paced world. As a result, many related research articles employing IoT and AI have the same objective of making living easier and safer. Table 1 below includes a few of the related works from which some suggestions for enhancing the home security system were derived.

Table 1. Related Works Based on Smart Home Security

Serial	Existing Work	Steps used
1	Ibrahim et al. [8]	Developed a plan for a fingerprint door panel intended for home protection, in which they talk about safety concerns and related precautions. The technology uses a fingerprint scanner to automatically recognize and verify a person.
2	Tiwari et al. [9]	Presented a remote-controlled security door that operates with a pre-configured software as part of a smart access control. The owner can use the application to open and close door and can permit visitors to enter the home or keep the door unlocked in case the person is unknown.
3	Khattar et al. [10]	Proposed a smart home using a virtual assistant, called Olivia. In their system, they integrated Olivia and a camera into the door lock. The camera is used to capture images for face recognition process. If the face detected is unknown, while the homeowner is not at home, Olivia interacts with the person asking him/her for their name and also asks them to drop a message if required.
4	Deepty et al. [11]	Presented an Android phone-based home entry monitoring system with biometric features. To verify legitimate access, the phone employs a cloud-based server.
5	Pawar et al. [12]	Proposed home automation system using face recognition, where they use sensors such as PIR (Passive Information) and ultrasonic sensor. The sensors are used for motion detection, to capture image when motion is detected. The door will autonomously open if the face matches the dataset; else, the buzzer will ring.
6	Maheshwari et al. [13]	Proposed a face recognition enabled home automation system using Microsoft API. To keep an eye on those who are standing at the entrance door, the Posed system deploys a high-definition camera that is mounted there and connected to a display monitor.
7	Gunawan et al. [14]	The proposed security system utilizes a Raspberry Pi to manage door entry with facial recognition. The system uses Python and OpenCV to implement their facial recognition technology, which controls how the door locks and opens.
8	Manjunatha et al. [15]	The proposed system uses the PCA technique to perform the face detection and recognition method. Their system has an application form for electronic auto police complaints, which alerts the nearby police station about the security breach.

9	Balaprasad et al. [16]	Introduced a face-based security system that relies on the SIFT (Scale Invariant Feature Transform) algorithm. Facial recognition, a door control system, and messaging are the three major components of the system. A command from the ARM7 processor causes the door to automatically open for a known individual. However, if the individual is unidentified, an alert will sound and an SMS will be sent to the command center.
10	Deshmukh et al. [17]	In a suggested system, once the bell has rung, it offers real-time facial recognition. If the face does not match, the taken image is delivered through SMTP to the owner's email, and if it does, door access should be permitted. After that, the system waits for the owner to respond within a certain period of time. Depending on the response, access to the door will either be granted or denied.
11	Sahani et al. [18]	They developed a system for tracking and authenticating that operates on both the web and the GSM channel. They employed an electro-magnetic security door and the PCA technique to recognize faces. This makes it easier for the owner to keep an eye on current events via text or web applications.
12	Deshmukh et al. [19]	Introduced an IoT-based smart door that uses the Local Binary Pattern Histograms (LBPH) method for identifying the facial expression. This proposed system used a dataset to compare the captured image and while the captured picture is matched with the dataset then the door opens. If the captured image does not match then the process sends an email with the captured image to the owner using SMTP. Raspberry pi is used by the author to process the capture and control of the entire system.
13	Sourav Roy et al. [20]	Designed a smart lock system using the face recognition technique where authors used Haar cascade classifier Algorithm (HCCA) for face recognition. They also used raspberry pi3 to control and execute the whole system. The proposed application used pi camera to take the input image and the unknown person’s image is sent to the owner using SMTP. Using SMTP and IMAP their wireless communication is achieved. The main goal of their application is to create a low-cost face recognition-based secure system.

3. Methodology

In contemplation to overcome the flaws of other systems this paper proposes an amplified secured home automation system to remotely control home attributes and monitor the door access. The system mainly consists of a multimodal security system and an interface for controlling home attributes, including door lock. The outline of the proposed paper is shown in Fig. 1. The security scheme helps ensure that the home is protected from potential invasions, especially through the front doors. Moreover, smart home adds the opportunity for users to have full control over their home attributes using a TKinter graphical interface. Given that all of the system parts are integrated onto a single chip, the Raspberry Pi [21, 22] serves as the main central controller in the suggested architecture. All the software instructions are contained on the Raspberry Pi, and the visual user interface allows for remote control.

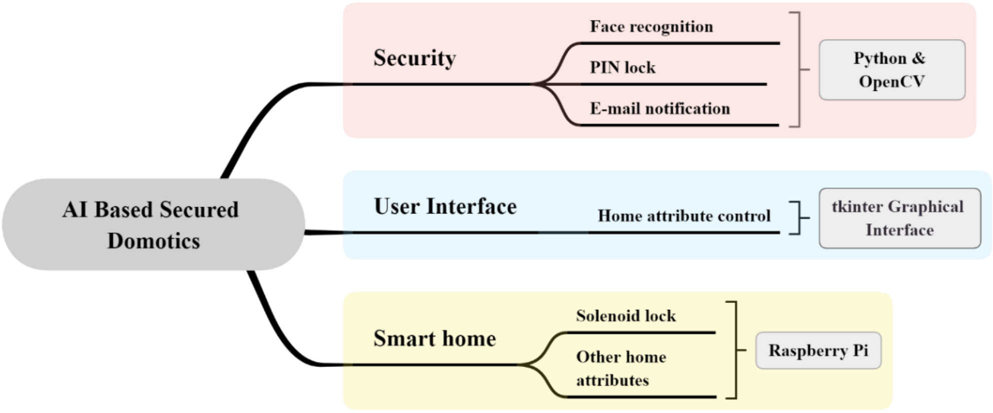


Fig.1. Overview of the proposed system

3.1. *Security of the Proposed System*

The steps of the security system of the proposed mode are shown in Fig. 2. The security system initiates by capturing image from the video frames to detect a face. The face recognition process proceeds by matching data with previously trained facial dataset. If the face is classified as “known”, the door lock opens and after 10 to 12 seconds of shutting the gate it automatically locks. A password consisting of 4 keys can still be entered even if the person's face is categorized as "unknown". The door opens if the right password is provided. When the incorrect PIN is entered, the alarm system will instantly go off. and a notification containing the image of the visitor will be sent to the owner’s email. The alarm can be stopped using the GUI.

The homeowner alone is aware of the PIN number for the passcode locking, which serves as a supplementary security measure. In the event of power failure, poor illumination, or any other operational problems with the face recognition system, this non-biometric technique is still in operation. Algorithm-1 illustrates the security system of the suggested method.

Algorithm 1: Algorithm of the proposed security system

```
Start
Input: HF = Capture image from the video frame
if  HF match with the database
    DoorOpen();
    Delay();
    CloseDoor();
else
    AskForThePIN()
    ImageSentToOwner();
        if PIN is equal to the registered PIN
          DoorOpen();
          Delay();
          CloseDoor();
        else
          AlarmON();
        End if
End if
End
```

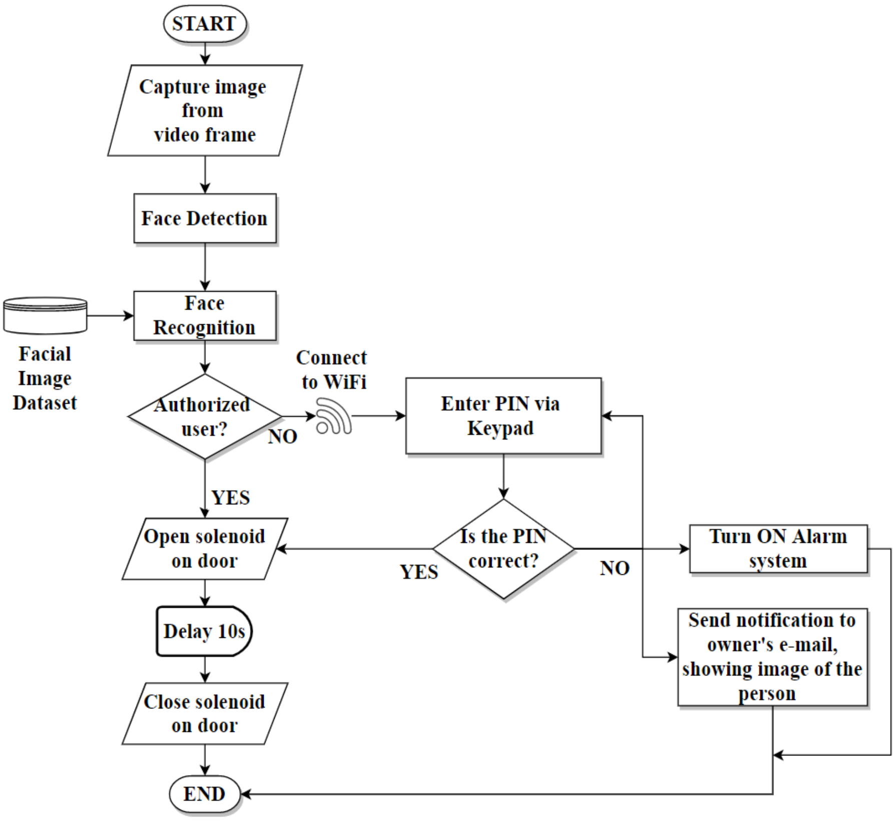


Fig.2. Flowchart of the security system

3.2. *System Architecture*

The four components that make up the structure of the system are shown in Fig. 3 and discussed as follows:

- *E-mail alert Module:* The homeowner receives an e-mail consisting of an image of known/unknown person whenever they try to go near the front door.
- *Data Processing Module:* It includes all of the suggested scheme's source codes and face information.
- *Data Generating Module:* In this area, the Raspberry Pi is used to integrate all dwelling features, along with the door lock and an alert. An alarm is implemented with the Raspberry Pi.
- *User Interface Module:* The homeowner can control the home attributes remotely, which was developed using the TKinter graphical interface.

3.3. Hardware Requirement

The Raspberry Pi, which accounts for the majority of the system's overall cost, is the system's key piece of hardware. To keep the system as cost-effective as possible, all of the hardware was carefully picked. This design allows use of Raspberry Pi 3 module B+ hardware, Solenoid Door Lock, Keypad, Relay Module, Camera, Power Supply and Buzzer, Wires, and LED Light and SD card.

Raspberry Pi is used to implement the home automation system since it is a cheap mini-computer, but it is efficient and has a powerful computing speed enough to run the entire system. A solenoid door lock is a small electromagnetic lock that is interfaced with the Raspberry Pi for remotely controlling the lock and it also responds to the command put in the program for face recognition. A 4x4 matrix keypad is used to take inputs. It is used as a backup security in this project. The home attributes (i.e., solenoid lock, keypad, etc.) are connected to the Raspberry Pi via a 5V DC relay module since Raspberry Pi is not capable of providing the required power supply directly. The relay channels can be chosen, depending on the number of attributes connected to the system. In this work, a 1 channel relay modules are used. The A4 tech webcam of model PK-331F is used to input images for training the system and also for the face recognition process. The specifications of the webcam are as follows:

- Video resolution: 2MP
- Image resolution: 16MP

The 12V power supply is used to power the relays and solenoid door lock. The buzzer is utilized as an alarm system. Jumper wires are just cables with connector pins on either side that can be utilized to link two places without soldering. The LED lights are used for indicating different activities of the system. A SD card is used in this project to store data.

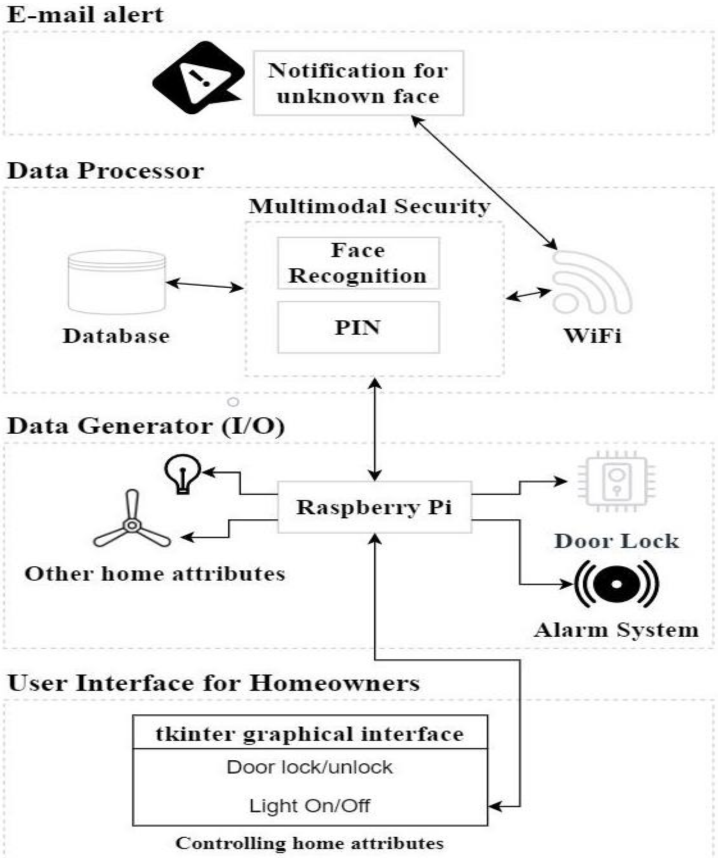


Fig.3. System architecture of the proposed model

3.4. Software Requirement

To interact with the hardware the system uses a number of softwires like Raspbian OS, Python IDLE, PyCharm, OpenCV and Thonny are used in this proposed system. The Raspbian OS is a Debian-based operating system, which is quite similar to a Linux OS, and is utilized to set up the Raspberry Pi. Python IDLEs are integrated development environments that offer a framework for writing Python script. This project uses the version 3.8. In this Work, face recognition, keypad and e-mail notification are implemented using PyCharm. PyCharm supports Python 2.7 and Python

3.6 to 3.10. This project uses PyCharm 2020.1.2.

An open-source computer vision and machine learning software library called OpenCV was developed to speed up the usage of artificial intelligence in commercial products and to offer a standard foundation for application areas [23]. This project uses OpenCV 4.4.1. Thonny is an IDE for Python is used in this work as a coding environment, directly in the Raspberry Pi.

3.5. Face Detection and Recognition

IoT and AI are used in the suggested solution to improve customer experience and effectiveness [24]. Local Binary Pattern Histogram (LBPH) text operator and Haar Cascade filter were both employed to protect the platform for face identification and recognition. Using a huge database is supported by the machine learning method known as Haar Cascade [25]. LBP combined with the histogram, which is a data vector, improves the recognition performance. For configuring the keypad, the pad4pi package was installed before beginning the program code. The image processing steps of face recognition is shown in Fig. 4, below.

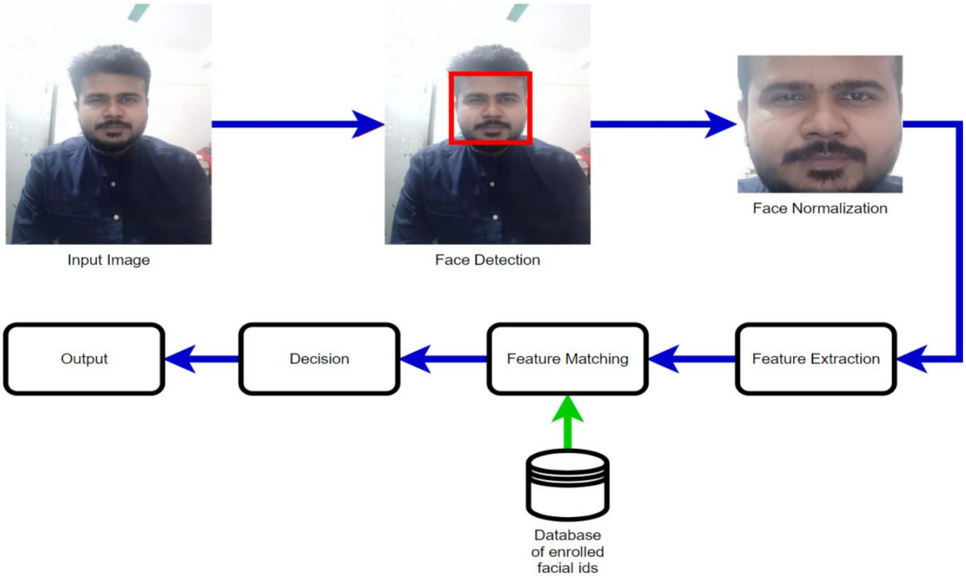


Fig.4. Image processing steps of face recognition

The procedure is stated below.

- An image is snapped from the source image sequence.
- Face is detected using an algorithm
- The facial image undergoes preprocessing where the image is normalized, enhanced, cropped, etc.
- Features from the image are extracted and the bit patterns are digitized
- The patterns are matched with the enrolled facial dataset for verification or identification.
- A decision is taken based on the match and the face is recognized

A. Haar Cascade Classifier

A machine learning object identification technique is called the Haar Cascade. Positive images (facial images) and negative images (images without a face) are used to train the classifier. At a certain point in the detection window, the Haar Cascade feature takes nearby rectangular areas into consideration. The sum of the pixels in the original image's top-left corner makes up each integral image. This enables the equation [26] to be used to compute the total of the image's rectangular regions. Where points X, Y, Z and L belong to the integral image I.

$$sum = I(Z) + I(X) - I(Y) - I(L) \qquad (1)$$

B. Local Binary Pattern Histogram (LBPH)

LBPH [27, 28] is a binary text operator which is more accurate than LBP alone, since LPB combined with histogram provides a better result due to data vectors. The flowchart of LBPH is shown in Fig. 5. LBPH is easy to use and understand and is less sensitive to light conditions.

The Fig. 6 shows how LBPH operator works. Firstly, the captured image is taken as input. Secondly, a 3*3 block of the face is formed, and the histogram for every section is computed. The image is processed in the end to produce the final product regions. LBPH uses 4 parameters such as radius, neighbors, grid X and grid Y.

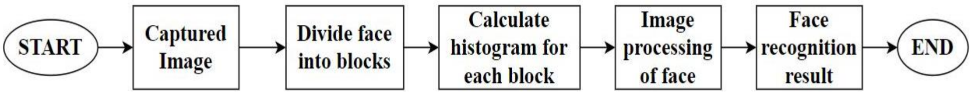
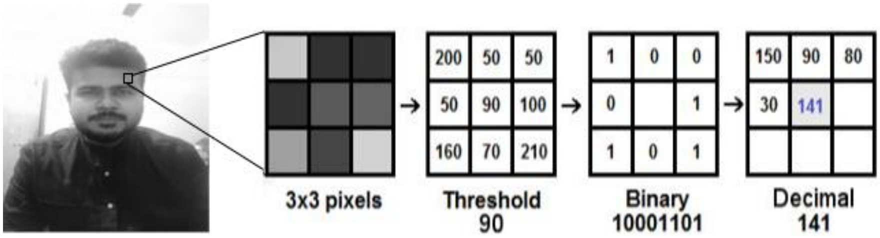


Fig.5. Workflow diagram of LBPH operator



200	50	50
50	90	100
160	70	210

1	0	0
0		1
1	0	1

150	90	80
30	141	

Fig.6. Procedure of LBP

In LBHP, a part of a gray-scaled image is taken in a window of 3*3 pixels, it may be seen as a 3*3 matrix with an intensity range of 0 to 255 for each pixel [29]. Thresholding is performed on the matrix's center value, and for each of the value's neighbors, a new binary value is computed. Values are assigned to 1 for readings that are equal to or more than the threshold, and to 0 for readings that are less than the threshold. The binary values are concatenated in a clockwise direction and then converted into decimal values. The final result has a new image that has a better representation of the original image. Now, using the new image, grids X and Y are used to divide the image into several grids. Various methods, such as Euclidean distance, absolute value, chi-square, etc., can be utilized to analyze the histograms while face identification is being performed. This system uses the Euclidean method.

4. Implementation of the Proposed System

This section discusses the proposed system's formulation and construction. Fig. 7, shows the circuit setup for the entire system. The figure shown in Fig. 8 is the final setup for this system.

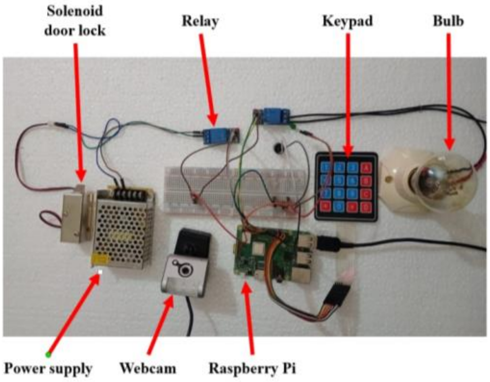


Fig.7. Hardware circuit setup of the proposed system

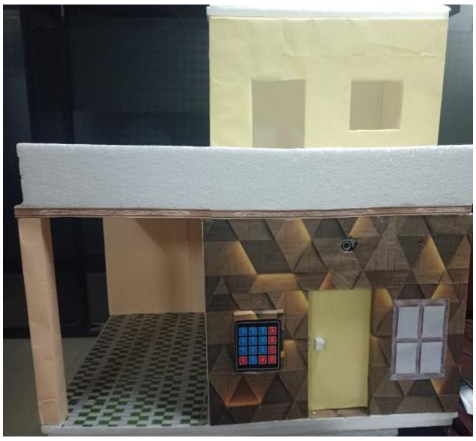


Fig.8. Final set up of the proposed model

In this system, TKinter graphical user interface (GUI), as shown in Fig 9, is used to create a user interface with which the owner can control all home attributes. This user interface is created using Python language. It allows the addition of multiple attributes. The interface can be operated in a mobile phone by connecting it to the VNC server. VNC uses a protocol to remotely control another computer, by connecting to the IP address of the Raspberry Pi to the mobile phone.

Fig. 10 shows the control of light using a TKinter GUI, which can be used in a mobile phone. Other home attributes can also be controlled, and more devices can be added in the GUI. The GUI can be used in mobile phone, as mentions previously, to remotely control the home attributes.

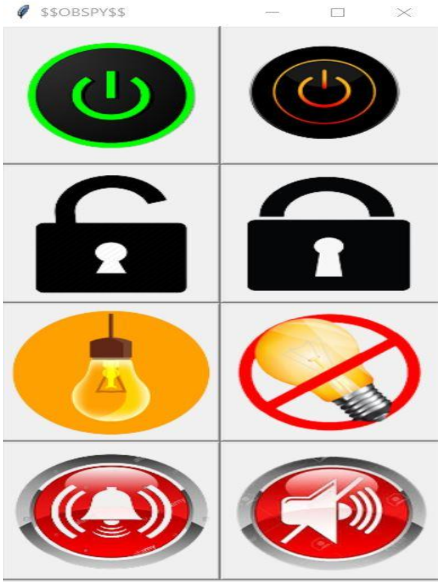


Fig.9. TKinter GUI

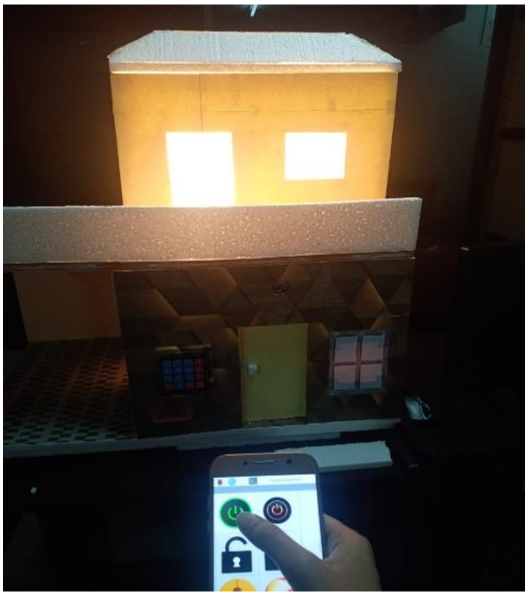


Fig.10. Remotely controlling a light – Light ON

5. Result and Discussion

Based on the experiment in this section testing results are talked about. This research was conducted at Dhaka International University's Machine Insights Laboratory (MINTEL).

5.1. Testing System

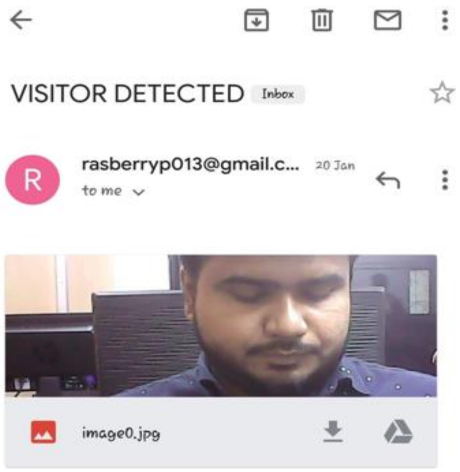
Several tests were conducted during the journey of this project's development, and a few of the outcomes are listed in Table 2.

Table 2. Test results of the system

Testing measures	**Expected Results**	**Actual Result**		
		1	2	3
Booting the system	The system boots without any signs of crashes	Fail	Success	Success
Face detection	Detect a face	Success	Success	Success
Face recognition	• Categorize faces into “known” and “unknown” classes • Show name of the known user	Success	Fail	Success
LED	LED lights up if face is not detected	Success	Success	Success
Buzzer	• Starts ringing when wrong PIN is entered • It can only be stopped by entering the correct PIN	Fail	Success	Success
Solenoid door lock	Door locks/unlocks using face recognition process and TKinter GUI	Fail	Success	Success
PIN lock	Door lock opens upon entering PIN code	Success	Fail	Success
Sending e-mail notification	When an unknown person is detected, a notification is sent consisting of the image of that person	Success	Success	Success
Controlling home attributes	Being able to control all home attributes using the TKinter graphics interface	Success	Success	Success

5.2. Testing of Face Recognition

For face recognition, the confidence level was set to 70%, which means a face will only be categorized as a known person when the percentage is 70 or higher. The degree of confidence in this approach is 73%, on average. Fig. 11 shows the mail with the visitor’s image to the homeowner. The confidence level of this project ranges from 70 to 80%, depending on the lighting conditions and the training of dataset.



VISITOR DETECTED Inbox

rasberryp013@gmail.c... 20 Jan

to me

image0.jpg

Fig.11. Face detection mail sent to the owner

5.3. Success Rate

The Table 3 shows the confusion matrix of face recognition, from which the accuracy, recall and precision rate can be calculated. A total of 70 cases were considered.

Table 3. Confusion Matrix

N = 70		**Prediction**	
		Known	**Unknown**
Actual	**Known**	47	3
	Unknown	0	20

The confusion matrix above has two predicted classes – Known and Unknown. 7 participants were used to test the system, where 5 were known and 2 were unknown and a total of 10 trails were done on each person, making it a total of 70 cases. Out of the total 70 cases, the classifier predicted “Known” 47 time and “Unknown” 20 times. 50 cases were of the known-class, out of which the classifier predicted “Known” 47 times and “Unknown” 3 times. 20 cases were of the unknown-class, out of which 20 of them were predicted as “Unknown” and none were predicted as “Known”.

Predicting known as unknown can be improved by training the dataset with more images of the person, but as the classifier did not predict a single unknown face as known is a great advantage for the system. Hence, The Accuracy rate is 95.7%, the Recall rate is 94.0% and the Precision rate is 100%. 100 observations of each sample (face) were used in the training of the dataset. Table 4 compares the accuracy of our system to several previous study articles. The design was implemented for about BDT 7,500, which is a really affordable price compared to others.

Table 4. Accuracy of the system is compared to other research articles

Research Articles	Algorithm	Accuracy (%)
Pawar et al. [8]	LBP	80
Gunawan et al. [10]	PCA, Eigenface	90
Balaprasad et al. [12]	SIFT	70
Dhobale et al. [20]	LBP	80-90
Our proposed system	Haar Cascade, LBPH	95.7

5.4. Comparison Features with Related Works

The properties of the developed framework are contrasted with those of other research articles in Table 5, which highlights how it is a combination and improved version of all the publications previously discussed. After comparing the related systems, it is reasonable to say that this system is a perfect choice for home automation. Since it features a non-contact biometric lock mechanism, that makes it appropriate for circumstances like COVID-19 and speeds up access considerably more than touch locks like thumbprint. The system includes a secondary safeguard, which is covered in more detail later on in the research article. Since the TKinter visual API is used to handle every aspect of the house, all elements may be tracked and managed remotely.

Table 5. Feature comparison between this project and other research papers

Research Articles	**Biometric Lock**	**Security PIN**	**E-mail/SMS**	**Mobile Control**	**Appliance Control**
Ibrahim et al. [8]	✓	✓			
Tiwari et al. [9]	✓			✓	
Khattar et al. [10]	✓				
Deepty et al. [11]	✓			✓	✓
Pawar et al. [12]	✓			✓	
Maheshwari et al. [13]	✓				
Gunawan et al. [14]	✓				
Manjunatha et al. [15]	✓		✓	✓	
Balaprasad et al. [16]	✓		✓	✓	
Deshmukh et al. [17]	✓	✓	✓	✓	
Sahani et al. [18]	✓		✓	✓	
Proposed System	✓	✓	✓	✓	✓

6. Conclusions

All in all, the main focus is to ensure home security for users. We have completely implemented the security lock and facial recognition, allowing it to lock and open the door, and we have developed a mobile application, which allows owners to remotely control devices at home using TKinter GUI. To make it easier for homeowners, e-mail is sent to their addresses, which consists of an image of the person who gets recognized either as "known" or "unknown." This project uses low-cost equipment. Therefore, from the data collected, we can say that our system is indeed budget-friendly and fairly accurate, and will be of great help to decrease property crimes. In the near future, using Neural Networks, the biometric scheme can be further improved. In addition, biometric methods can be emphasized in order to boost the security level and also include blockchain for PIN lock to make it secure from cyber-attacks.

Funding

No funding received.

Conflict of Interest

All authors declare no competing interest.

Availability of Data and Materials

Not Applicable.

Ethics Approval

All procedures performed in studies involving human participants were in accordance with the ethical standards of the committee of Dhaka International University (DIU) research cell and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards.

Consent to Participate

Informed consent was obtained from all individual participants included in the study.

References

[1] N. Amraoui, and B. Zouari, Securing the operation of Smart Home Systems: A literature review. Journal of Reliable Intelligent Environments, 8(1), pp.67-74, 2022.

[2] 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

[3] S. V. Chippa, Dr. R. R. Dube, “AWS EC2 based Home Security System using Face Recognition”, International Journal of Engineering Research & Technology (IJERT), vol.8, no.08, pp. 397-400 (2019).

[4] I. Cvitić, D. Peraković, M. Periša, & B. Gupta, “Ensemble machine learning approach for classification of IoT devices in smart home,” International Journal of Machine Learning and Cybernetics, 1-24, 2021.

[5] P. Christo, “Spendmenot Burglary Statistics”, https://spendmenot.com/blog/burglary-statistics/, Last accessed 2020/12/12

[6] F. Wang, Practical Research on Artificial Intelligence and Internet of Things in Smart Home. In Innovative Computing (pp. 1793-1798). Springer, Singapore,2022.

[7] N. Amraoui, and B. Zouari, Securing the operation of Smart Home Systems: A literature review. Journal of Reliable Intelligent Environments, 8(1), pp.67-74, 2022.

[8] 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 (ICIEM), pp. 420-424, IEEE, London, United Kingdom (2020)

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

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

[11] 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 (RAAICON), pp. 21-24, IEEE, Dhaka, Bangladesh (2019).

[12] 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), pp. 1-6, IEEE, Pune, India (2018).

[13] 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, 1-4 (2017).

[14] 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), 5(4), 317-325, (2017).

[15] R. Manjunatha, R. Nagaraja, “Home Security System and Door Access Control Based on Face Recognition”, International Research Journal of Engineering and Technology (IRJET), 4(03), (2017).

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

[17] A. D. Deshmukh, M. G. Nakrani, D. L. Bhuyar, U. B. Shinde, “Face Recognition Using OpenCv Based on IoT for Smart Door”, In Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India, (2019).

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

[19] D. Deshmukh, A., G. Nakrani, M., L. Bhuyar, D., & B. Shinde, “Face Recognition Using OpenCv Based on IoT for Smart Door”, SSRN Electronic Journal, 2019.

[20] S. Roy, M. N. Uddin, M. Z. Haque, & M. J. Kabir, “Design and implementation of the smart door lock system with face recognition method using the linux platform raspberry Pi,” IJCSN-International Journal of Computer Science and Network, 7(6), 2018.

[21] E. Upton, & G. Halfacree, "Raspberry Pi user guide", John Wiley & Sons, (2014).

[22] K. Pulli, A. Baksheev, K. Kornyakov, & V. Eruhimov " Real-time computer vision with OpenCV", Communications of the ACM, 55(6), 61-69, (2012).

[23] K.M.M. Uddin, A. Chakraborty, M.A. Hadi, M.A. Uddin, and S.K. Dey, November. 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, 2021.

[24] 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, 975, p.8887, (2020).

[25] K.M.M. Uddin, S.K. Dey, G.U. Parvez, A.S. Mukta, and U.K. Acharjee, "MirrorME: implementation of an IoT based smart mirror through facial recognition and personalized information recommendation algorithm," International Journal of Information Technology, 13(6), pp.2313-2322, 2021.

[26] A. Kasinski, and A. Schmidt, "The architecture and performance of the face and eyes detection system based on the Haar cascade classifiers," Pattern Analysis and Applications, 13(2), pp.197-211, 2010.

[27] C. Shan, Learning local binary patterns for gender classification on real-world face images. Pattern recognition letters, 33(4), pp.431-437, 2012.

[28] R.Ogla, A. A. Saeid, and S. H. Shaker, Technique for recognizing faces using a hybrid of moments and a local binary pattern histogram. International Journal of Electrical and Computer Engineering, 12(3), p.2571, 2022.

[29] S. Karanwal, Improved Local Binary Pattern for Face Recognition. In International Conference on Deep Learning, Artificial Intelligence and Robotics (pp. 86-96). Springer, Cham, 2022.

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 M.Sc. (Research) in Computer Science and Engineering from Jagannath University. His research interests are in the field of Machine Learning/Deep Learning, Wireless Networking, Computer Vision and Image Processing, and IoT.

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.

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.

Samrat Kumar Dey is a faculty member in the School of Science and Technology (SST), Bangladesh Open University (BOU). He has completed his Bachelors and Masters in Computer Science and Engineering (CSE) from Patuakhali Science and Technology University (PSTU) and Military Institute of Science and Technology (MIST) respectively. His research interest mainly focuses on Data Science, Visual Data Analytics, Human-Computer Interaction (HCI), Usability and UX analysis, Machine Learning/Deep Learning and Network Security.

How to cite this paper: Khandaker Mohammad Mohi Uddin, Naimur Rahman, Md. Mahbubur Rahman, Samrat Kumar Dey, "Artificial Intelligence Based Domotics Using Multimodal Security", International Journal of Intelligent Systems and Applications(IJISA), Vol.15, No.3, pp.44-55, 2023. DOI:10.5815/ijisa.2023.03.04