3rd oNeScINTech

Volume 3 No 1 (2023)

Received : June 05,2023
Accepted : June 09, 2023
Published : August, 2023

Conference on Business, Social Sciences and Technology
https://journal.uib.ac.id/index.php/conescintech

Smart Door Lock System by Using Face Recognition

Amirah Syahirah Ariffin[1], Norharyati Harum[2]
amiraharff@gmail.com
[1,2]Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia

Abstract
Security is one of the main concerns to people who resides in a house as there is a lot of cases such as robbery. Thus, the safety of people is the utmost importance. However, people still use the traditional door lock to secure their home. Therefore, this paper presents the idea of using Face Recognition and Telegram application as part of the smart features to enhance the home security. Face Recognition methods that will be used are Local Binary Pattern Histogram (LBPH) which act as feature extraction under local appearance-based techniques and Haar Cascade as a classifier. Besides, the usage of Telegram application will also be utilised. As the output, the Face Recognition technology is being used to grant authorized user access to the house and the Telegram application is being used to remotely control the door lock without any keys. In conclusion, by implementing those advanced technologies it will strengthen the security of the home as well as the wellbeing of the people.

Keywords:
Security, Face Recognition, Telegram, Smart Features

Introduction
The Internet of Things (IoT) is a rapidly growing technology that has drastically contributed to the Industry 4.0 realization. IoT pursues to pervade our everyday environment and its objects, linking the physical to the digital world and allowing people and “things” to be connected anytime, anywhere, with anything and anyone ideally using any network and service. IoT is regarded as a dynamic and global network of interconnected “things” uniquely addressable, based on standard and interoperable communication protocols and with self-configuring capabilities. Despite still being at an early development, adoption and implementation stage, IoT can provide a multitude of contemporary solutions, applications and services according to the (Villamil, S., Hernández, C., & Tarazona, G., 2020).

Security plays a vital role in safeguarding individuals, organizations, and society as a whole. The sole importance of securing the home is to ensure the safety of people in the household. A secure home reduces the risk of physical harm to residents, unauthorized access and burglaries. This can provide people a peace of mind that can contribute to the comfortability and wellbeing of people. A secure house also can have a positive impact on the overall safety of the neighborhood.

The aim of this paper is to alleviate the security by integrating the smart features such as Face Recognition and Telegram application. Face recognition technology provides an additional layer of authentication beyond traditional methods like keys. By using biometric data, such as facial features, to grant access, it becomes more difficult for unauthorized individuals to gain entry. This helps prevent unauthorized access and strengthens home security. Additionally, by using platforms like Telegram, user can remotely monitor and control the door locks as well

as enabling them to manage access to the home even when the user is not physically present. This feature is beneficial for scenarios such as granting temporary access to trusted individuals or monitoring and controlling access from a distance

Literature Review

1. IoT Based on Home Security

Recent studies have focused on home security, which is crucial for keeping our homes safe. A research conducted by (Deepty et al., 2019) suggests using an IoT and Wi-Fi based door access control system using a mobile application. This system utilizes Wi-Fi to activate the door access control and allows owners to remotely control access through the mobile application. Visitors can also use the application, which has a biometric feature for fingerprint registration to become authorized and unlock the door. Additionally, the system compares the phone's IMEI number to the registered number on the cloud server for authentication.

Another study by (Giorgi et al., 2019) focuses on an Iris and Voice Recognition System for a Smart Doorbell. This system requires both iris and voice recognition to identify visitors. It comprises speaker identification and iris recognition blocks using specialized software and open-source platforms. The speaker identification block processes audio features and uses probabilistic models to compare against an enrolled persons' database. The iris recognition block locates eyes, extracts iris codes, and matches them with enrolled users.

(Ragade, 2017) proposes an Embedded Home Surveillance System with Pyroelectric Infrared Sensor Using Global System for Mobile Communication (GSM). This system utilizes ultrasonic and PIR sensors to detect motion and changes in temperature. When an unauthorized user is detected, the system activates a buzzer and sends an SMS to a predefined number. Additionally, the system captures images with a web camera and allows owners to view them on their mobile devices.

(Ganapathi Raju et al., 2018) describe a Smart Lock Controlled using Voice Call. This system employs a GSM module for call reception and user verification, an Arduino UNO for microcontroller functions, and a servo motor for gear control. Authorized users need to provide a 4-digit PIN code via SMS to unlock the door. Incorrect codes trigger an alert sent via SMS to authorized users.

(Javare et al., 2018) conducted research on Access Control Detection in a Door Lock System using Bluetooth Technology. This system utilizes Bluetooth and sensors for authorization and security. Vibration sensors detect attempts to break the door, while a motion sensor triggers if motion is observed. Upon arrival, the user's smartphone with Bluetooth sends a unique identifier to the system for verification and unlocking. If there is no match, the system captures the visitor's picture and sends it to the owner for access approval. The system also activates an alarm when an unauthorized user attempts to forcefully access the door.

(Park and Cheong, 2017) propose the IoT Smart Bell Notification System, which integrates smartphones and home network systems for home security. This system uses a webcam, Wi-Fi, and a smartphone, and the programming language employed is C++. When the doorbell is pressed, the system captures the visitor's picture and sends an SMS with the picture to the owner. Owners can monitor their homes by accessing a web page. In case of a break-in attempt, CCTV footage can be used as evidence for lodging a police report

(Pinjala and Gupta, 2020) propose a Remotely Accessible Smart Lock Security System with Essential Features. Apart from remote control and monitoring, this system includes an audio message feature. When the doorbell is pressed, the Raspberry Pi is activated, triggering the camera stream, and the owner receives a notification on their smartphone. The owner can remotely view the live camera feed and grant or deny access by entering a pre-set password. Furthermore, users can input text to convey audio messages to visitors.

(Andreas et al., 2019) propose a Door Security System for Home Monitoring Based on ESP32. This system utilizes an ESP32 microcontroller and MQTT cloud communication protocol with SSL encryption. It includes a PIR sensor for movement detection and a touch sensor for human hand detection. Messages from the MQTT Broker trigger various operations, such as unlocking or locking the door and managing the buzzer.

(Sataloff et al., 2018) researched an Integrated Smart House Security System Using Sensors and RFID. Instead of conventional methods, this system uses RFID and a keypad for door access and integrates with automated lighting systems. The Arduino Uno microcontroller connects with various sensors to detect PIR, RFID, LDR, and keypad inputs. Visitors must use an RFID card to unlock the door, and in case of an attempted break-in, the system activates a buzzer. Additionally, the system automates lighting based on motion detection.

(Pacheco and Miranda, 2020) propose an NFC Door Lock for a Smart Home System. This system utilizes an Arduino microcontroller and NFC technology to control the physical lock. Each user has their own NFC card or tag with a unique identification number. Scanning the NFC tag sends the information to the Arduino board for user authentication. If the user is authorized, the door unlocks otherwise, it remains locked.

2. Face Recognition Methods

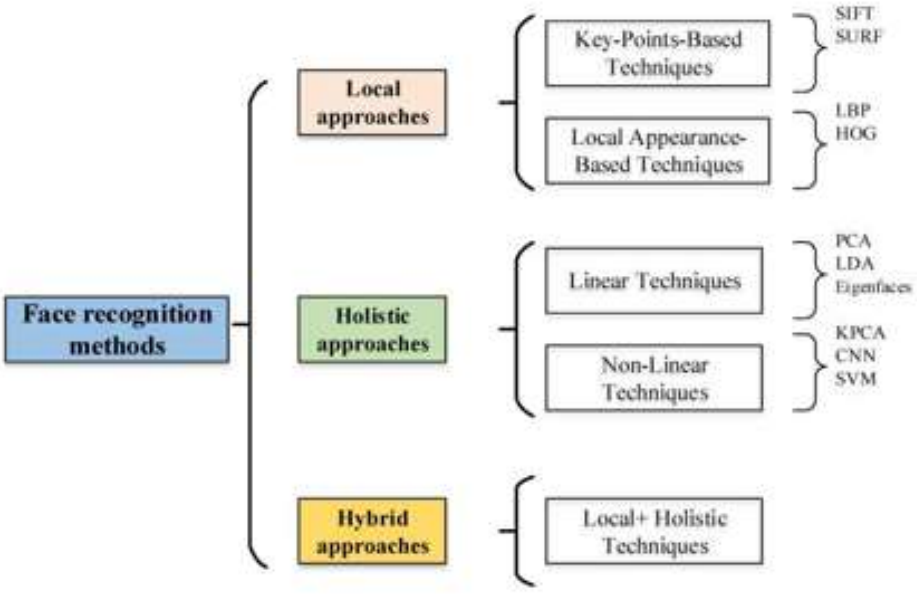


Figure 1. Face Recognition Methods

Face recognition methods will be focusing more into local approaches, centering on specific parts of facial features during feature extraction. There are two main categories within this framework which are Key-Points-Based Techniques and Local Appearance-Based Techniques. However, elaboration will be more on the Local Appearance-Based Techniques.

Local Appearance-Based Techniques also known as analytic, feature, or geometrical techniques, represent by a set of distinctive vectors with small regions or low dimensions of a face image. This technique focusses on critical points like the eyes, mouth, and nose, reducing the number of parameters. It offers the advantage of analyzing images in challenging real-time environments. Method that is chosen by this technique is Local Binary Pattern (LBP) or also known as Local Binary Patterns Histogram (LBPH).

LBP or LBPH extracts features by converting an image into an array of pixels and extracting histograms. It computes the variance between the central pixel and its neighbors, making it suitable for

general texture analysis. It provides better performance and computational simplicity. However, as the size of features and the number of neighbors increase, the computational complexity in space and time also increases.

Research Methods

Method that will be used in this project is prototyping model. In this model, prototype will be created, tested and modified until the final outcome of the project is achieved and fully developed.

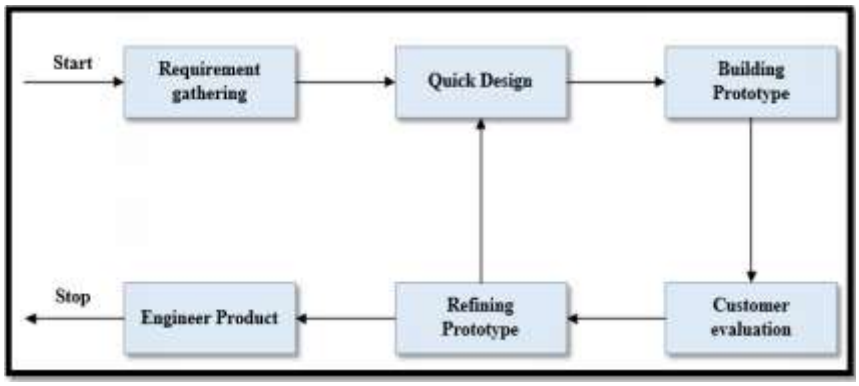


Figure 2. Prototyping Model

1. Requirement Gathering

In the first stage, requirement of the project will be defined. A detailed information of the project such as project background, project statement, objectives need to be gathered. This information will be a guideline in the completion of the project. Next, do a literature review that related to the project, analyze the data and make comparison.

2. Quick Design

In the second stage, the basic design of the project is made to give a quick view and concept of the project. There are also involve in few activities which is to determine what hardware and software to be used in the project. Next, do the requirement analysis. After that, design the project which includes flowchart.

(1) Face Recognition

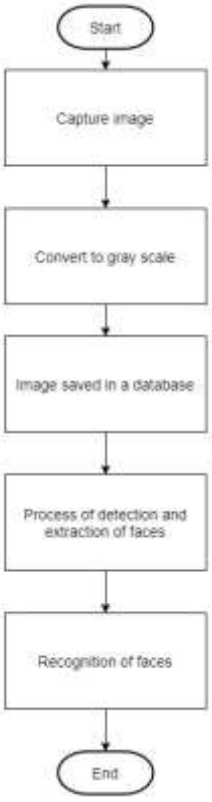


Figure 3. Flowchart of User Registeration

Figure 3 shows the system flowchart to register user. Firstly, the image of the user will be captured from a webcam and the ID number will be generated. Then, the sample of images will be converted to gray scale and it will be saved in a database with the name that assign to the ID. After that, the process of detection of faces using Haar cascade classifier and extraction of faces using LBPH will be performed. After the faces being detected, the image of the face will be divided into blocks. Then, histogram for each block will be calculated and it will combine the LBPH histogram to a single histogram. Lastly, the face image will be processed and it will recognize the faces.

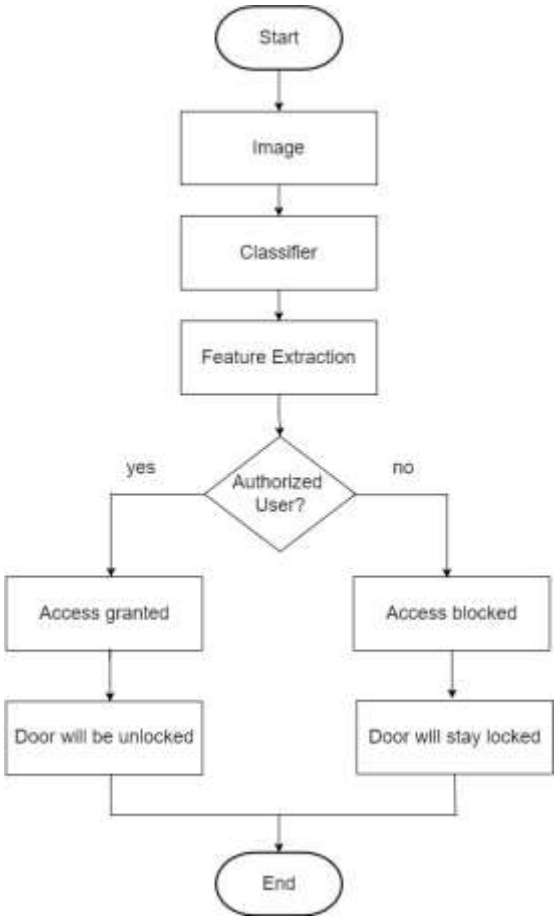


Figure 4. Flowchart of Overall Face Recognition System

Figure 4 shows the flowchart of overall system of Face Recognition. The system will be started by capturing the image from the webcam feed that will be processed. Then, the process of detection of the faces will be started by using Haar cascade classifier. After that, the process of face recognition which is to recognize people's face that match with the samples in a database of the system will be operated by is LBPH as a feature extraction. The LBPH features will be extracted in this step to detect if the person is an authorized or unauthorized user. If the user is an authorized user, access will be granted and the door will be unlocked whereas for unauthorized user, the access will be blocked and the door will stay locked.

(2) Telegram

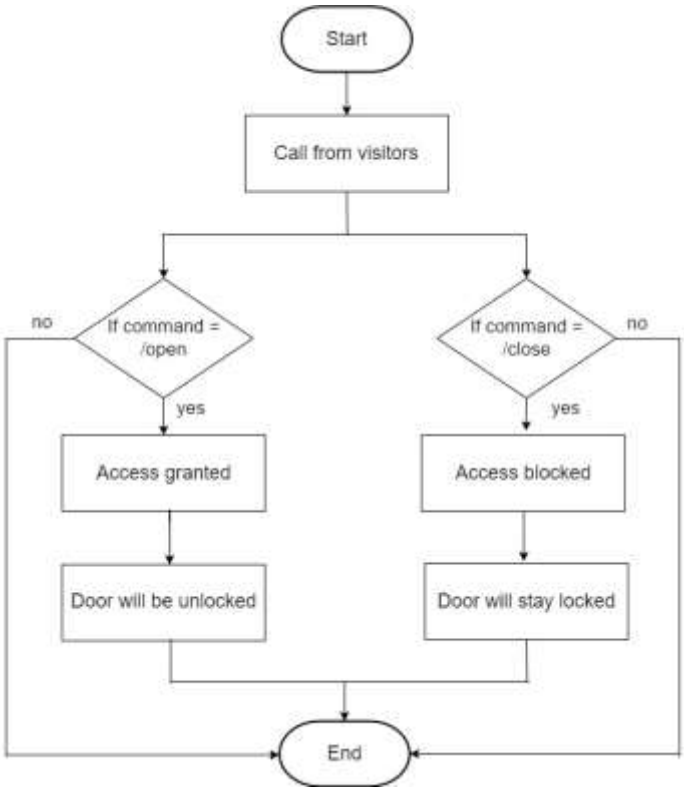


Figure 5. Flowchart of Overall Telegram System

Figure 5 shows the flowchart of overall system of Telegram. The system will be started by getting a call from visitors. Then, the owner will remotely control the door lock via Telegram. If the command /open, then the door will be unlocked whereas if the command /close, then the door will be locked.

3. Building Prototype

In the third stage, the prototype will be created based on the design. There are few activities that involve which are all the required hardware need to be setup. Then, required software need to be installed and configured.

Table 1. Hardware and Software

Hardware	Software
Raspberry Pi 4 Model B	Python 3.7
Webcam	OpenCV
Jumper Wires	Raspbian OS
LED	Telegram
Breadboard	BotFather

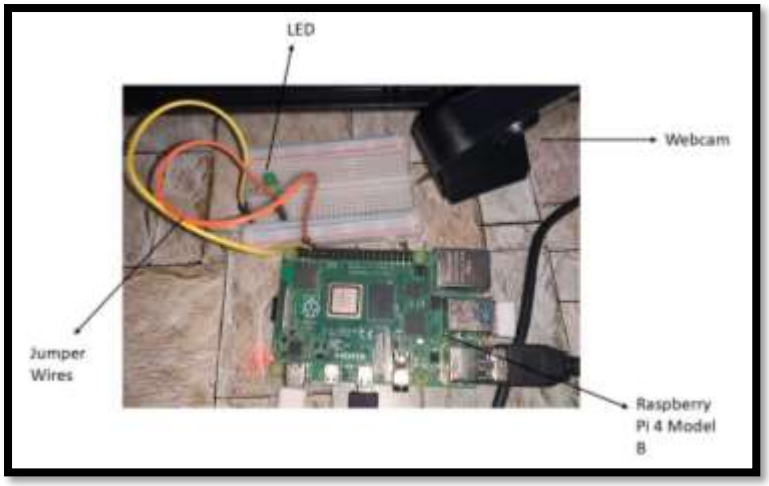


Figure 6. Hardware Setup for The Project

4. Customer evaluation

In the fourth stage, when the constructing of the prototype is done, testing process will be executed and then the person in charge will evaluate the prototype. They will point out on a few criteria such as its strengths, weakness and what element should be added or removed. The result of the assessment will be gathered and analyzed to make an improvement of the prototype.

5. Refining prototype

In the fifth stage, the modification of the prototype will be done according to the information gathered on the evaluation in the fourth stage. After the improvement has been made, it will go back to the quick design stage to correct the previous design and will be evaluated again to ensure the criteria has been met. Lastly, after all the criteria and objective of the project has been fulfilled and achieved, we will be moving on to the last stage which are engineer product.

6. Engineer product

For the last stage, the project will be developed based on the final prototype which has been tested and make changes for a better improvement. Then, the project conclusion that consist of project summarization of overall project need to be write it out.

Results and Discussion

In this section, the testing result wil be discussed. It will cover two tests which are Face Recognition and Telegram test. The LED represents the door lock. If the LED light up it indicates that the door is unlock whereas if the LED is not light up it indicates that the door is lock.

Table 2. The Functionaliy of The Face Recognition Test

Test Number	Action	Result	Outcome
1	User's face that is not registered in the system faced the webcam.	LED is not light up, door lock.	Success
2	User's face that is registered in the system faced the webcam.	LED is light up, door unlock.	Success

Table 3. The Functionality of The Telegram Test

Test Number	Action	Result	Outcome
1	Visitors will call owner and the owner will remotely grant access to lock or unlock the door.	LED is not light up, door lock. LED is light up, door unlock.	Success

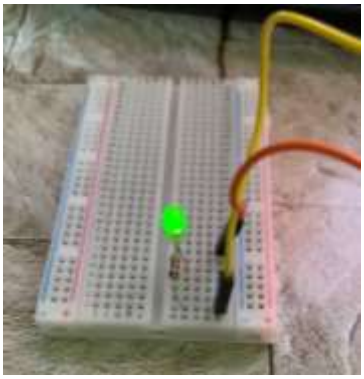
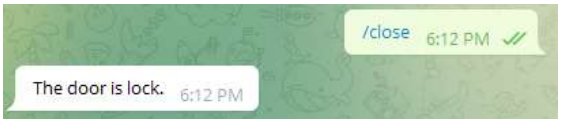


Figure 7. Command to Unlock the Door and LED Lights Up



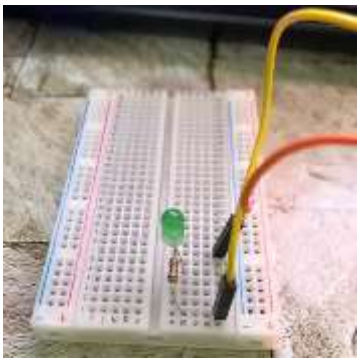


Figure 8. Command to Lock The Door and LED Does Not Lights Up

Conclusions

In this paper, the IoT based on home security has been discussed and the best technology has been implemented to enhance the home security which is by using the Face Recognition technology to grant access and the Telegram application to remotely control the door lock. Testing phase of the prototype has also been done to ensure the prototype has been executed and functioning well. This research can also be added up as for future advancements of other smart elements to make it more usable and secure.

References

Villamil, S., Hernández, C., & Tarazona, G. (2020). An overview of internet of things. *Telkomnika (Telecommunication Computing Electronics and Control)*, *18*(5), 2320-2327.

Andreas, Aldawira, C. R., Putra, H. W., Hanafiah, N., Surjarwo, S., & Wibisurya, A. (2019). Door security system for home monitoring based on ESp32. *Procedia Computer Science*, *157*, 673–682. https://doi.org/10.1016/j.procs.2019.08.218

Deepty, R. R., Alam, A., & Ezharul Islam, M. (2019). IoT and Wi-Fi Based Door Access Control System using Mobile Application. *2019 IEEE International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things, RAAICON 2019*, 21–24. https://doi.org/10.1109/RAAICON48939.2019.09

Ganapathi Raju, N. V., Vikas, J., Appaji, S. V., & Sai Hanuman, A. (2018). Smart lock controlled using voice call. *Proceedings of the International Conference on Smart Systems and Inventive Technology, ICSSIT 2018*, *Icssit 2018*, 97–103. https://doi.org/10.1109/ICSSIT.2018.8748770

Giorgi, R., Bettin, N., Ermini, S., Montefoschi, F., & Rizzo, A. (2019). An Iris+Voice Recognition System for a Smart Doorbell. *2019 8th Mediterranean Conference on Embedded Computing, MECO 2019 - Proceedings*, *June*, 8–11. https://doi.org/10.1109/MECO.2019.8760187

Javare, A., Ghayal, T., Dabhade, J., Shelar, A., & Gupta, A. (2018). Access control and intrusion detection in door lock system using Bluetooth technology. *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing, ICECDS 2017*, 2246–2251. https://doi.org/10.1109/ICECDS.2017.8389852

Pacheco, J., & Miranda, K. (2020). Design of a low-cost NFC door lock for a smart home system. *IEMTRONICS 2020 - International IOT, Electronics and Mechatronics Conference, Proceedings*. https://doi.org/10.1109/IEMTRONICS51293.2020.9216409

Park, W. H., & Cheong, Y. G. (2017). IoT smart bell notification system: Design and implementation. *International Conference on Advanced Communication Technology, ICACT*, 298–300. https://doi.org/10.23919/ICACT.2017.7890101

Pinjala, S. R., & Gupta, S. (2020). 2020 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2020. *2020 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2020*, 44–47.

Ragade, R. R. (2017). Embedded home surveillance system with pyroelectric infrared sensor using GSM. *Proceedings - 1st International Conference on Intelligent Systems and Information Management, ICISIM 2017*, *2017-Janua*, 321–324. https://doi.org/10.1109/ICISIM.2017.8122192

Sataloff, R. T., Johns, M. M., & Kost, K. M. (2018). Integrated Smart House Security System Using Sensors and RFID. *2018 4th International Conference on Wireless and Telematics (ICWT)*, 2–6.