Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Enhancing Smart Home Security System with HOG Algorithm

Muhammad Aiman Irfan Shahrel[1], Raihani Mohamed[1,*], Sufri Muhammad[2], Ade Candra[3], Muhammad Noorazlan Shah Zainudin[4]

[1] Intelligent Computing Research Group, Department of Computer Science, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia
[2] Department of Software Engineering Information System, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia
[3] Department of Computer Science, Faculty of Computer Science and Information Technology, Universitas Sumatera Utara, 20155 Indonesia
[4] Universiti Teknikal Malaysia Melaka, Durian Tunggal, 76100 Melaka, Malaysia

ARTICLE INFO

Keywords:
Internet-of-things; face recognition; HOG algorithm; smart environment; smart door lock system

ABSTRACT

The escalating global concern over burglary incidents, particularly by the economic repercussions of the 2020 pandemic, necessitates innovative solutions to fortify residential security. Traditional locks, once presumed as the primary defence against intruders, have proven inadequate against modern burglary techniques. This work proposes the development and implementation of a "Smart Home Security System" to address the imperative need for improved home security. By implementing technologies such as the Internet of Things (IoT), artificial intelligence (AI), and mobile applications, the proposed system aims to establish multiple layers of protection against unauthorized entry. The objectives of this study revolve around the integration of various components, including smart locks employing solenoid locking mechanisms, ultrasonic sensors, video surveillance, and mobile application-based access control. The system offers diverse methods for unlocking, encompassing passcodes, face recognition utilizing the HOG (Histogram of Oriented Gradients) algorithm, mobile applications, and physical button switches. Leveraging Firebase for database management enhances system reliability and accessibility. Additionally, the Smart Home Security System incorporates important features such as real-time monitoring of the front door and image capture capabilities. Furthermore, a burglary detection system, facilitated by ultrasonic sensors, serves as a proactive measure against unauthorized access attempts. A key goal of the proposed Smart Home Security System is to offer homeowners an advanced and comprehensive security solution at a lower cost, while maintaining functionality superior to existing systems on the market. By integrating cutting-edge technology and cost-effective components, this system provides a robust and accessible defense mechanism, empowering homeowners with enhanced protection against contemporary burglary threats.

* *Corresponding author.*
E-mail address: raihanimohamed@upm.edu.my

https://doi.org/10.37934/araset.64.4.187200

1. Introduction

In recent years, the alarming rise in burglary cases has become a significant concern for homeowners worldwide. This surge can be attributed, in part, to the economic repercussions of the 2020 pandemic, which has left many individuals unemployed and desperate for alternatives such as financial income [1]. During the post Covid 19, the criminal case for burglary increased up to 6% compared to pandemic Covid 19 [26]. Consequently, traditional locks have been proven inadequate in safeguarding houses against burglary attacks [2]. To address this pressing issue, this project proposes the development and implementation of a state-of-the-art smart home security system, aimed at fortifying home security and providing homeowners with enhanced protection. Motivated by the growing need to safeguard houses and restore homeowners' peace of mind, this project sets out to develop by integrating advanced technologies such as artificial intelligence, Internet of Things (IoT), and smart devices [3-5]. The proposed system aims to revolutionize house security measures. It seeks to establish multiple layers of defense against unauthorized entry, leveraging components such as smart locks, motion sensors, video surveillance, and remote access controls. The author stated that the conventional lock systems currently in use lack important modern security features, such as a video surveillance camera, home pin passcode and notification alert to mobile application functionality. These features are crucial in enhancing the overall security of a premises [2]. The absence of a video surveillance camera denies users the ability to visually monitor the area surrounding the lock, making it difficult to identify potential threats or intruders. Furthermore, the lack of a home pin passcode feature reducing the flexibility and convenience of accessing the locked area. The absence of a notification alert to mobile application fails to provide immediate notifications in case of unauthorized access attempts. Existing smart home security systems often lack efficient remote monitoring capabilities, relying heavily on manual interventions for security assessment, which can be cumbersome and inefficient [6]. This limitation not only compromises the timeliness of response to potential security breaches but also hinders the ability to ensure the safety of occupants within the premises, particularly vulnerable individuals like children.

Therefore, the proposed research aims to address these challenges by designing a smart home security system that enables comprehensive remote monitoring via intuitive mobile applications. By integrating features such as real-time burglar alerts system and enhanced lock door lock mechanism will empower users to monitor their homes from anywhere at any time. This advancement will not only enhance the overall security posture of smart homes but also provide homeowners with peace of mind knowing that their loved ones and belongings are well-protected.

This paper makes a two-fold contribution. Firstly, it aims to design and develop a smart home security system with smart home security features such as solenoid lock, keypad, and ultrasonic sensor. Secondly, to include smart security functions such as control lock and burglary detection with HOG algorithm. The rest of this paper is organized as follows. Section 2 explores the previous related work. Meanwhile, Section 3 explains the system and methodology proposed in this study. Section 4 presents the results and discussions. Section 5 clarifies the conclusion of the overall studies.

2. Related Work

There are critical elements requisite for the advancement of developing smart home security systems components encompass a face recognition system, motion detection facilitated by ultrasonic sensors, user alert mechanisms, keypad-based door lock functionality, real-time door status display via LCD interfaces, solenoid lock mechanisms, and application management protocols within the system framework [7]. Face recognition is one of the important features in smart home security

system. This is because by using the face of the user, it allows the door can be unlock by using facial. This help to reducing time taken to unlock the door while providing better security system. The raspberry pi 3 was used for handling the process of facial recognition. The ultrasonic sensor was used to determine the distance of the user and the front door [8-11]. The system will check the distance between user and camera by using ultrasonic sensor. The distance between user and camera must be at least within 240cm. If satisfied, the image will be captured and processed. If the image matches the database, the door will unlock [2].

Face recognition as door lock as a best solution compared to other methods such as RFID and password pin. This is because RFID keys can be lost, and password pin code might be forgotten by the users. Face recognition also does not require physical touch [12]. The system works by capturing the face of the person standing in front of the camera [13]. Then it will be compared with the database. If it is matched with the database, the door will open. Else the system will lock the door. The author does not disclose the algorithm used for facial recognition. Based on the picture in the journal itself, it is believed that this algorithm is a pre-built library within the ESP32CAM library on Arduino IDE [14]. Based on the previous works of these authors, the popular algorithm used for face recognition are Histogram of Oriented Gradient (HOG) and Local Binary Pattern (LBP). Face recognition is very important for this project to provide enhance smart home security system [15,16].

Motion sensing serves as a principal element due to its pivotal role in detecting human presence. This capability is essential for initiating various actions such as triggering notification alerts or commencing the facial recognition process [17-20]. The ultrasonic sensors are employed to detect human presence in proximity to the door. When a user approaches the front door within the optimal range for face recognition, their facial features are captured, thus prompting the initiation of the facial recognition process to facilitate door unlocking [2]. Alert notification functionality serves as a critical feature aimed at informing users of any unusual occurrences. This capability is typically realized through the transmission of alerts via email using the Simple Mail Transfer Protocol (SMTP) and mobile applications [21]. In the event of a mismatch and the absence of the homeowner, the system sends both an email and SMS to alert the owner. Conversely, if the owner is present, the system activates an audible alert within the premises. Additionally, attempts to breach the door trigger an alarm notification [2]. Other work utilizes Passive Infrared (PIR) motion sensors as triggers for alert notifications. Upon detecting intruders attempting to access the door, the system captures the event via camera and promptly sends email alerts to the user. Simultaneously, a buzzer is activated to alert neighboring residents [22,23]. The features expanded using mobile apps triggers alerts in response to door openings, instances of jamming, or attempted breaches of the lock mechanism [24].

3. Material and Method

3.1 System Design and Architecture

The system design and architecture of enhance smart home security system consists of several major parts. In this architecture as in Figure 1, the major of three parts was consisted of door lock system, burglary detection system, and face recognition. Firstly, on the door lock system it serves the purpose to control the locking mechanism in order to control the door status whether to open or close the door. The main microcontroller used for this part is ESP32. Keypad and Button were used to open door solenoid locks. LCD display is used for displaying the status of the door and the passcode entered to the system. Secondly, the burglary detection system serves the purpose for detecting any intruder that may try to enter the house from vulnerable spots inside the house such as the kitchen window. If there is any motion that tripped on the sensor, it sends the alert to the user in real time

thru Firebase. The main microcontroller used for this part is ESP32. The sensor used to detect the motion is an ultrasonic sensor. When the sensor reading below a certain threshold, it is indicated that the sensor has been tripped with anybody part of the intruder. The main reason to use ultrasonic sensors compared to PIR motion sensors is when the temperature is too hot or too cold. It can randomly trigger the sensor during the testing phase. This produces false detection. Thus, an ultrasonic sensor is the best option. Lastly, the face recognition serves the purpose for detecting the user facial to unlock the door via facial recognition. This offers another alternative layer of security to unlock doors. The main microcontroller used in this part is ESP32CAM and Raspberry Pi 4. The ESP32CAM uses protocol RTSP to send the live stream smartphone and Raspberry Pi 4. The smartphone is only able to capture the picture of livestream and control the flash of ESP32CAM. While on Raspberry Pi 4 it used the livestream for facial recognition matching with the database. If it is matching, it sends the signal to Firebase to unlock the Door for 5 seconds. Otherwise, the system just returns an "Unknown" user.

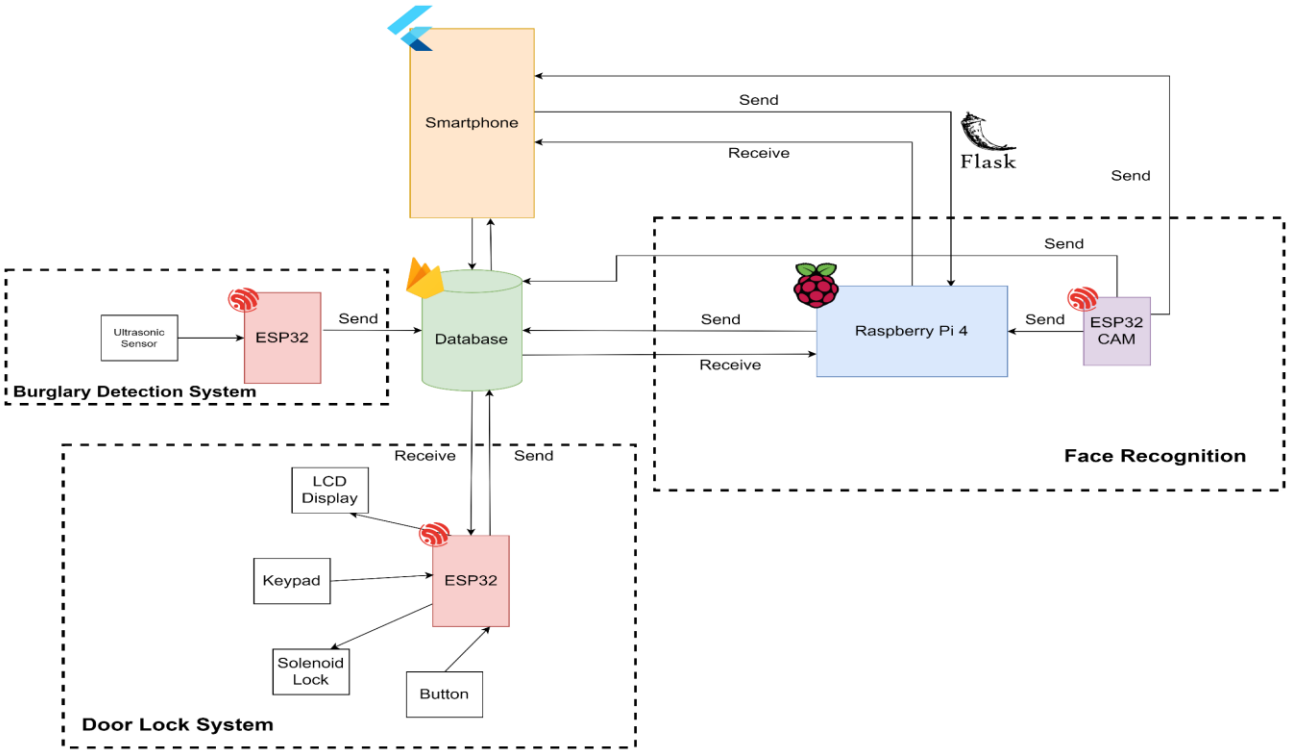


Fig. 1. Design of proposed system architecture

3.2 Flowchart Diagram

In this project there are several scenarios to enhance system security for smart home such as unlocking the door via pin code, face recognition, mobile application, and button. Within the app also there are options to manage the pin code, manage the users for the face recognition system, monitoring the front door and burglary detection system management. The flowchart diagram as shown in Figure 2 provides a general explanation of how the smart home security system works. Sensors will be turned on simultaneously and connected to the designated Firebase when it starts. The first part is unlocking the door via keypad. The ESP32 will retrieve a new passcode for every four seconds. Users insert the passcode via keypad and confirmed it with "#" button.

After the user confirms the passcode, the ESP32 will make a comparison between the user entered passcode and the passcode that retrieved from Firebase. If the passcode is matching, it will

display the message “Door Opened” on the LCD display for 5 seconds then it will lock it back. Otherwise, the LCD displays “Wrong Passcode” and the door will be locked. Another method to unlock the door is via face recognition. On the Raspberry Pi 4, it reads the user’s face model that has been trained. Then it gets the image livestream of ESP32CAM via real-time streaming protocol (RTSP) to scan the user face in real time.

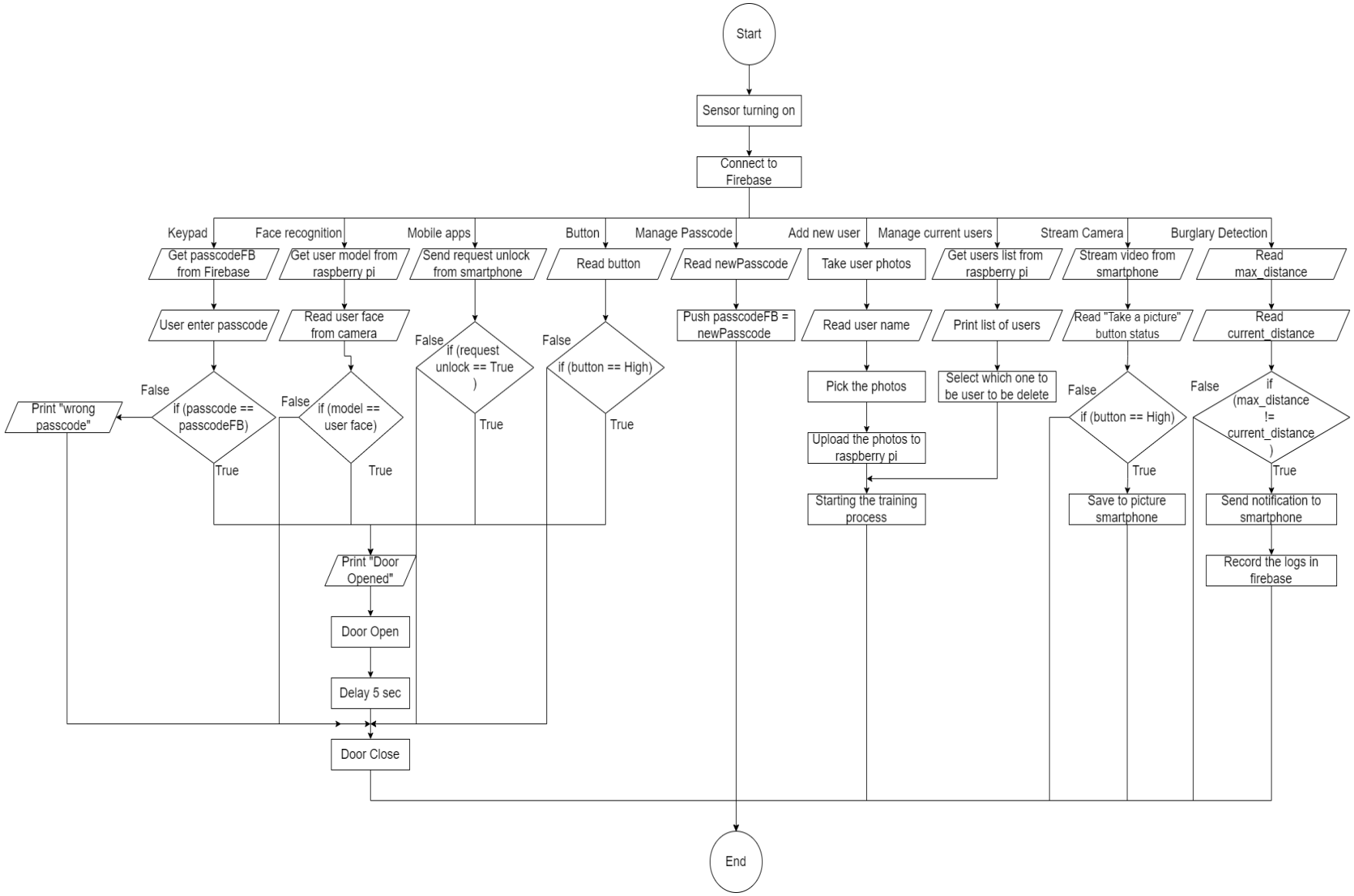


Fig. 2. Flowchart of the designed system

3.3 Hardware and Software Requirements

Details specification and requirements for hardware and software and its function as indicated in Table 1.

Table 1
Hardware and software specifications and its functions

Hardware Specification & Function	
2x ESP-Wroom-32 Board	ESP32 has WiFi and Bluetooth connection that will be useful to connect to Firebase. These microcontrollers are used in Door Lock System and Burglary Detection System.
ESP32CAM	This microcontroller has camera features prebuilt within it. This camera is used to provide livestream to mobile applications and face recognition processes.
Raspberry Pi 4	This microprocessor has performance like a conventional computer, but it is smaller. It is used for handling face recognition.
Ultrasonic sensor	It calculates the distance between the sensor and wall. By using this distance, the distance will be shorter compared to the original distance when being tripped by an intruder. The difference in length is used to alert the user about the intruder.
Solenoid lock	This is the lock mechanism used to control the door whether to unlock or close the door.
Software Specification & Function	
Arduino IDE:	Mainly used to program ESP32 and ESP32Cam microcontrollers. The language it uses is C++.
Visual Code Studio:	Mainly using Dart language and using Flutter framework.
Terminal	It used to run python code. The python code is used for face recognition with the Flask framework to receive users' selfies.
Database – Firebase	Database to store the information and data from the microcontroller and the mobile application. The language it uses is NoSQL.

3.4 Face Recognition with Histogram of Gradient (HOG) Algorithm

HOG algorithm functions by quantifying the occurrences of gradient orientations within localized segments of an image. Initially, the image undergoes conversion to grayscale, following which it is resized to dimensions of 128x64 pixels to alleviate computational complexity, as delineated in Figure 3.

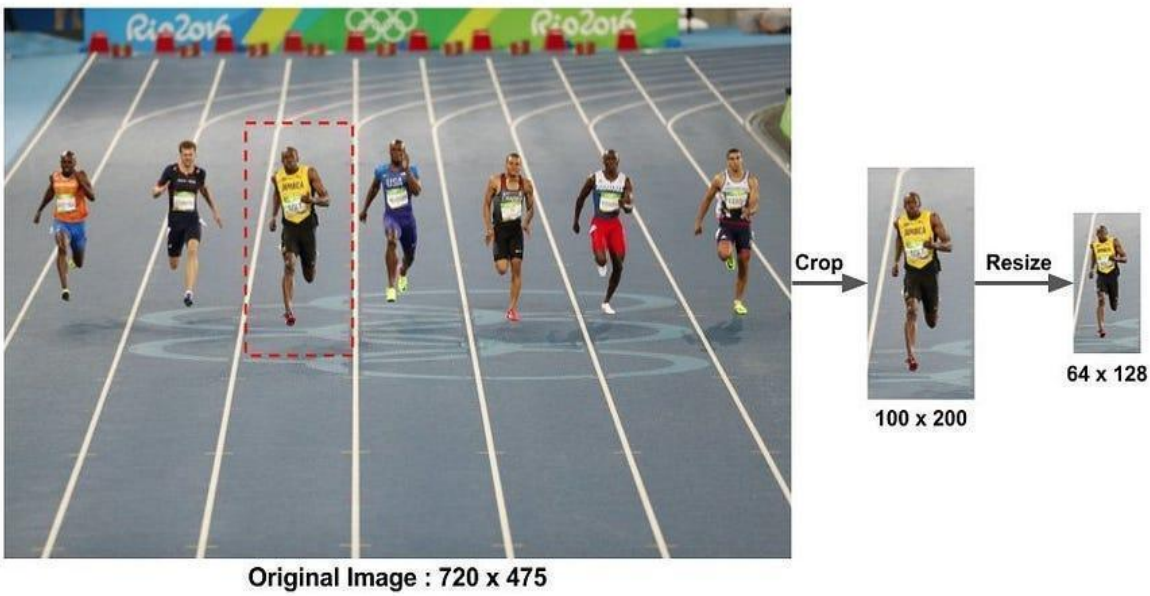


Fig. 3. Shows the image has been resized using HOG algorithm

Upon preprocessing, gradient computation ensues. This entails the determination of gradients through the amalgamation of magnitude and angle information extracted from the image [15]. The initial gradients, Gx and Gy, are computed employing the formulas depicted in Eq. (1). Subsequently, the magnitude and angle of each pixel are derived utilizing the formulas elucidated in Eq. (2).

$$G_x(r,c) = I(r,c+1) - I(r,c-1) \quad G_y(r,c) = I(r-1,c) - I(r+1,c) \tag{1}$$

$$Magnitude(\mu) = \sqrt{G_x^2 + G_y^2} \;\; Angle(\theta) = |tan^{-1}(\frac{G_y}{G_x}) \tag{2}$$

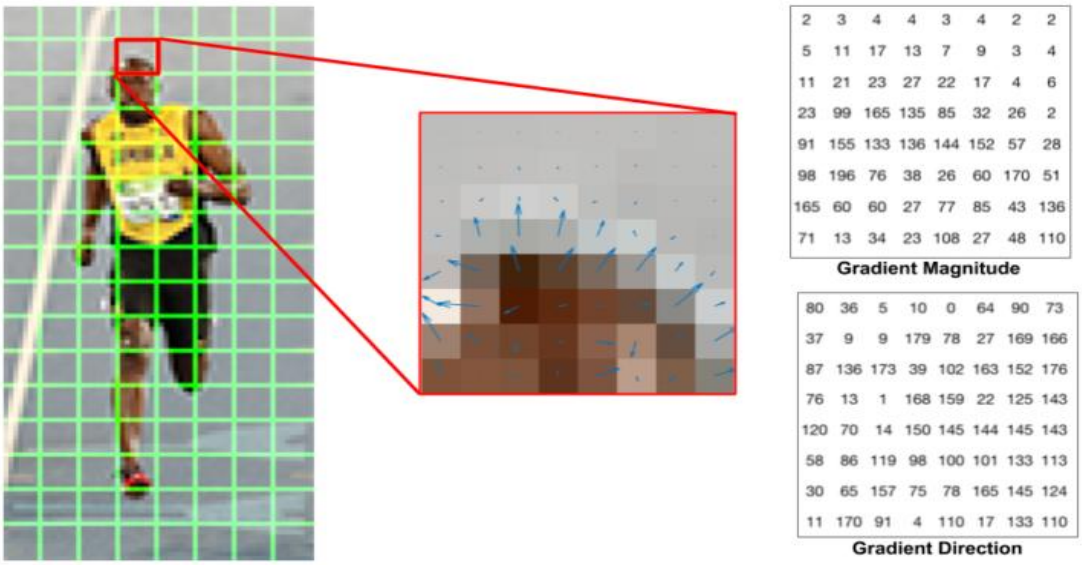


Fig. 4. The result of gradient magnitude and gradient angle

Further processing involves the segmentation of gradient matrices into discrete blocks of 8x8 cells. Within each block, a 9-bin histogram is generated, encapsulating the gradient distribution. This histogram comprises bins accommodating gradients across 20-degree intervals. Notably, the resulting 9-bin histograms are representative of gradient intensity distributions within their respective blocks, exemplified in Figure 4.

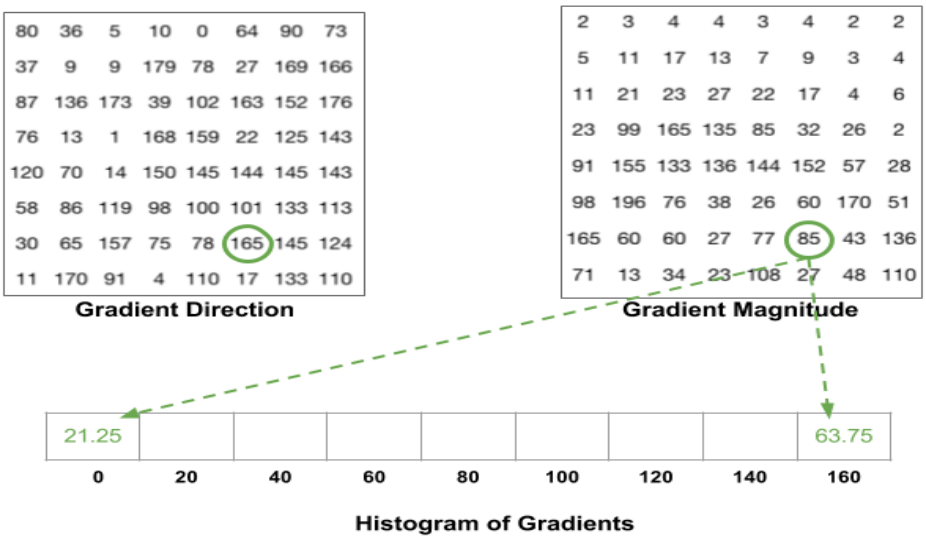


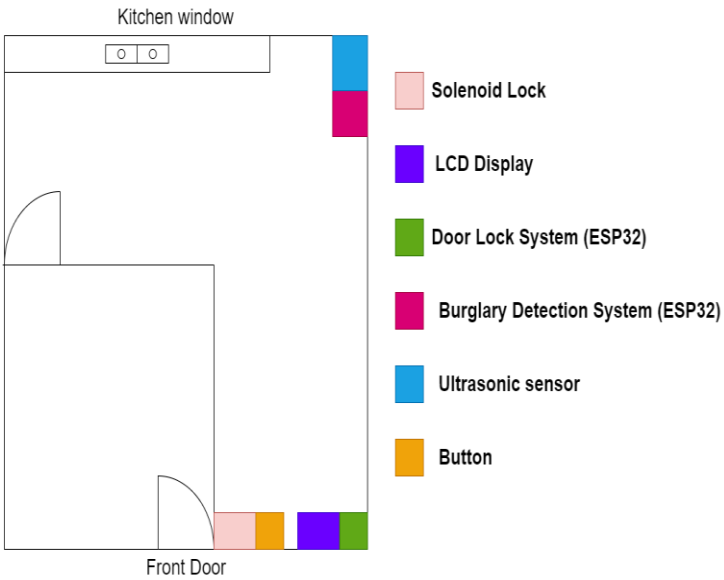
Fig. 5. The pixel in the bins depending on their direction and magnitude

The bin assignment process is contingent upon the chosen direction, with bin values determined by the associated gradient magnitudes. Noteworthy is the consideration that pixels residing between bin boundaries apportion their magnitudes proportionately to the adjacent bins. After this procedure, a cumulative histogram emerges, wherein bins with maximal weights signify predominant gradient orientations, as illustrated in Figure 5.

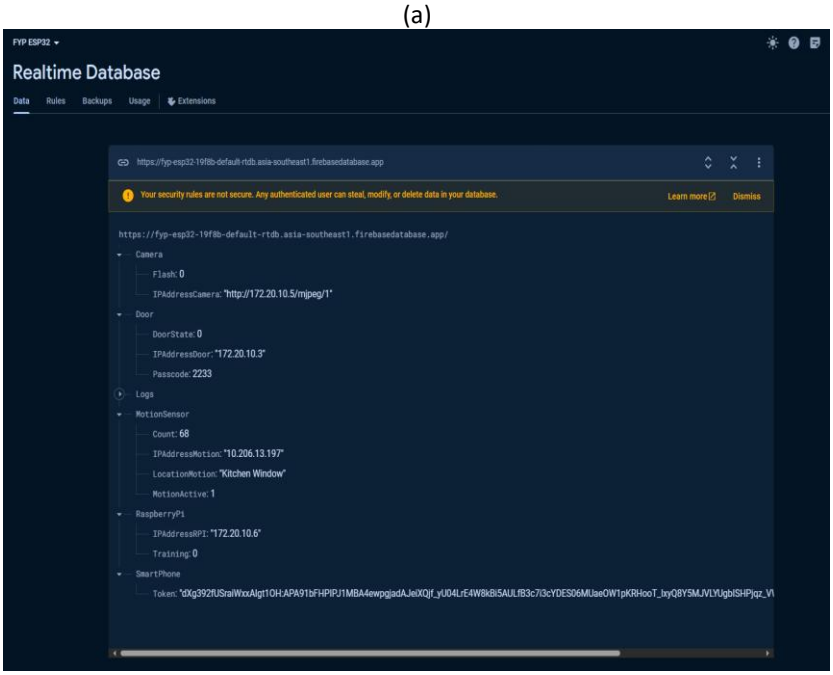
4. Project Implementation and Model Development

4.1 Smart Home Security System Layout

Figure 6(a) is the representation of the layout of the sensor that will be placed inside the house. The area it covers are the front door and the kitchen at the window. This project uses ultrasonic sensors to detect the burglary and solenoid lock for controlling the locking mechanism.



(a)



(b)

Fig. 6. The layout of the sensor inside the house (a) Sensor layout for the smart home (b) Database (Firebase)

Meanwhile Figure 6(b) indicates the firebase used as the database for this project. In this project primarily use real-time database for storing all the data such as door state, passcode, flash state, motion sensor state, IP Address, etc. The ESP32, ESP32CAM, Raspberry Pi 4, and mobile applications will use this database to communicate with each other and store data.

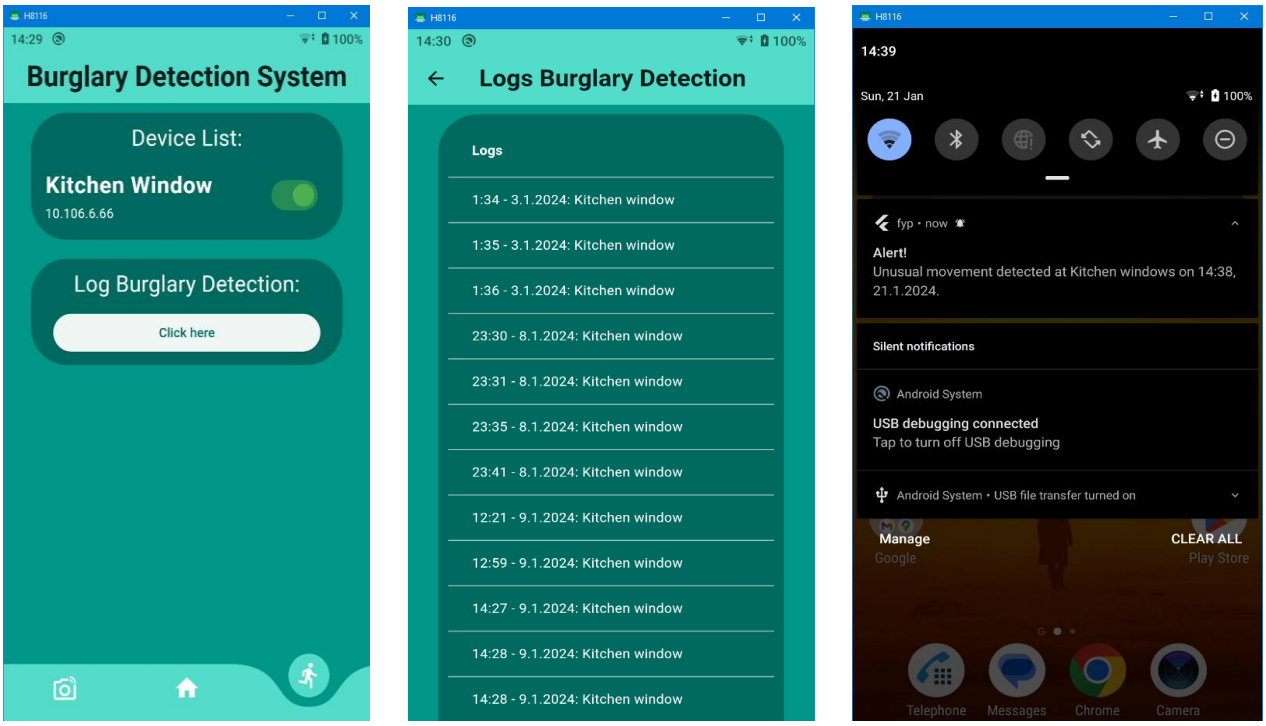
4.1.1 Features of smart home security system

4.1.1.1 Door lock system

There are many ways implemented to unlock the door such as using passcode, via face recognition in mobile apps and via button for users inside the house to unlock the door. Hence, managing passcode is important for the user to change and update the passcode. The new passcode can be changed to any kind of numeric value as long the minimum characters are 4 and maximum characters are 6. Users can press the button "Update" to confirm the changes of passcode. The passcode will be pushed to Firebase and on the Door Lock System, the ESP32 fetches the passcode for every four seconds from the Firebase.

4.1.1.2 Burglary detection alert system

Alert notification will be sent to the owner when there is abnormality detected from the triggered sensors. The owner can check notifications from the logs retrieved from the real-time database as in Figure 7.



(a) (b) (c)

Fig. 7. Mobile apps user interface used for burglary detection alert system (a) List of abnormalities detection triggered by the sensors (b) Logs of abnormalities appeared from the real-time database (c) Notification sends to the phone owner

4.1.1.3 Other smart features

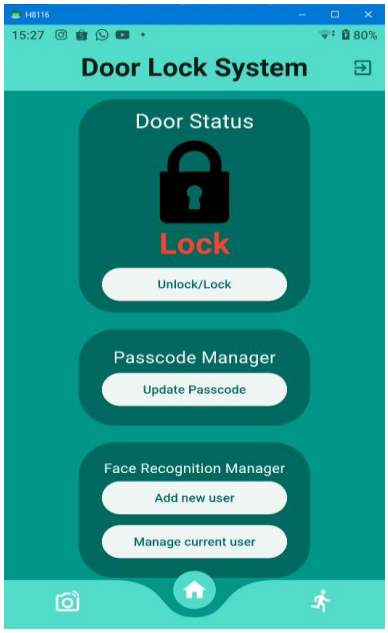
Other features for the mobile apps including manage current users so that the admin user can select which user can be deleted from using facial recognition as shown in Figure 8. For add new user, user's face will be capture by using front camera and to 20 pictures will be taken. The user enters the desired name to be registered into system. meanwhile, for door monitoring, user can monitor the person in front of the door in real time. User also can capture it as a picture and saved it in internal storage and have ability to enable or disable the flashlight.

4.2 Face Detection with HOG algorithm

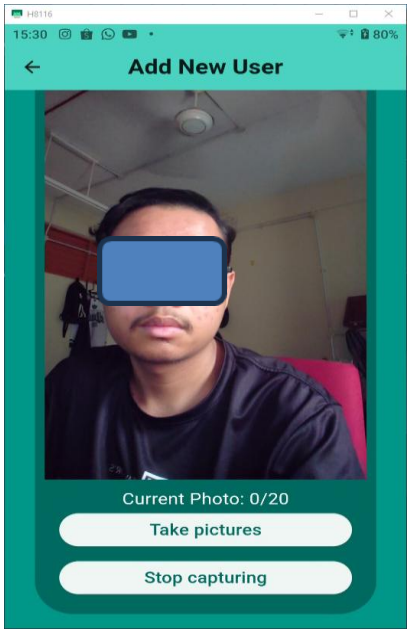
In the phase of building the machine learning model using HOG algorithm, user-provided selfies served as the primary training dataset, with approximately 20 images per user. These images were utilized to train a singular model, subsequently stored using pickle serialization. The employed machine learning algorithms comprised Histogram of Oriented Gradient (HOG) and Local Binary Pattern (LBP), were developed using Python library face-recognition, Dlib, imutils, pickle, and OpenCV. During the livestream recognition, the video from the livestream ESP32CAM converted into multiple frames by using imutils to resize the image by width = 500. This helps to reduce the complexity of computing in the next section. The use of OpenCV is to convert the frame from BGR to grayscale for face detection and the same frame also will be converted from BGR to RGB for face recognition. Thus, for 1 frame will have 2 types of images. The images of grayscale are used to detect the face and draw the box for that region. By using the face-recognition library, it uses the draw boxed image and the RGB image to bound the box for each face that is named as encodings. This encoding will be used to compare with the trained model if there is matching with the trained model. It updates the door state in Firebase to "open". If it is not matching, there is nothing changed on the door state in Firebase.

4.2.1 Face recognition for smart home security system

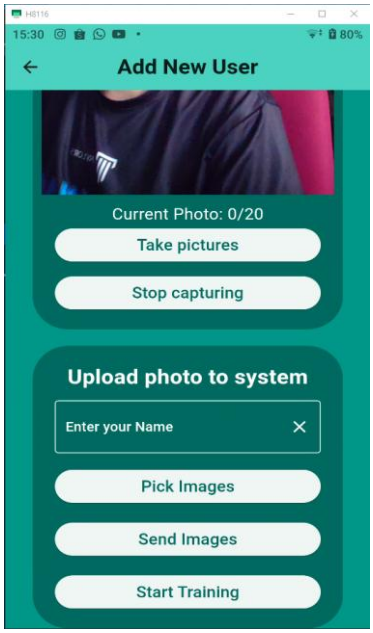
Face recognition is one of the main features in this project to provide options to the users to unlock the door without sacrificing the security. Figure 8(a) presents the system capturing the user's face for registration of new user and Figure 8(b) for other features.



Shows the user interface that is used for managing users.

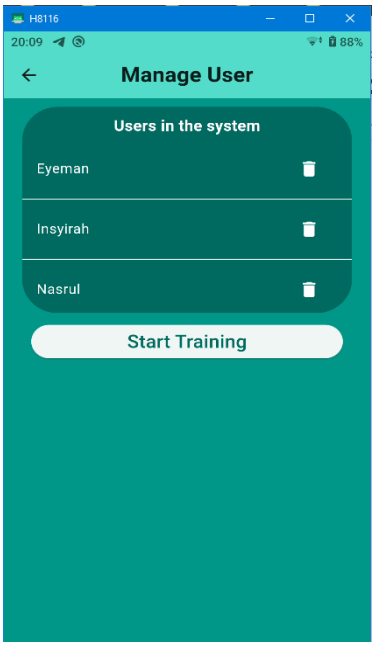


Shows the user interface that is used for taking user selfies.



Shows the user interface that is used for taking user selfies and uploading the selfie photos to the system.

(a)



Shows the user interface that is used for managing the users.

User interface that is used for monitoring the front door.

(b)

Fig. 8. User interface in mobile apps for user's face recognition (a) Add new user and manage current user interface (b) Other features

The accuracy of this algorithm was performed thrice, involving ten users, each contributing 20 photos. The initial test yielded an accuracy of 88.89%, followed by 92.49% in the second test, and 91.83% in the third. The average accuracy across all tests stood at 91.07%. Regarding the time required for facial recognition, the fastest recorded time was 0.96 seconds, while the slowest was 1.00 second, with an average recognition time of 0.98 seconds.

5. Conclusion and Future Work

In conclusion, the smart home security system has been enhanced with security features with face recognition in mobile apps and other IoT sensors such as solenoid, ultrasonic, ESP32CAM and PIR motion sensors have been installed in the environment. This project successfully achieved the high accuracy of the face recognition which is on average 91.07% during the test. Also, it is able to achieve faster response time from the sensor to Firebase to the mobile application within below 5 seconds with average 3 seconds to receive the alert notification. Face recognition model using HOG algorithm offers a sophisticated security layer, its reliance solely on camera-based recognition without 3D imaging technology. Some limitations were obtained from the system implementation; hence improvements need to be rectified for future study. Currently, the face recognition system relies on 2D image-based authentication, which presents a significant limitation in distinguishing between real 3D human faces and 2D representations, such as photographs. To address this vulnerability, future enhancements could incorporate 3D scanning technology, such as dot projection, to capture the depth and contours of a face, providing a more accurate and secure method of authentication that was similar to the approach used by Apple's Face ID. The system also can be improved in terms of centralized server architecture to optimize ESP32 software to minimize mobile app door control delays to rectify central server task offloading. With the improvement that can be implemented, this introduces more opportunities that can potentially be adapted for other security systems, such as office buildings, industrial environments, or public surveillance systems. The use of HOG for feature detection could also apply to areas like autonomous vehicles, robotics, or healthcare monitoring systems, where accurate object or human detection is essential. Other than that, the algorithms can be enhanced for face recognition with 3D scanning to detect unauthorized access, especially for identical twins.

Acknowledgement
This work has been sponsored by Faculty of Computer Science and Information Technology (FCSIT) of Universiti Putra Malaysia funded by Malaysian Ministry of Higher Education.

References
[1] Lambovska, Maya, Bogusława Sardinha, and Jaroslav Belas Jr. "Impact of the COVID-19 pandemic on youth unemployment in the European Union." *Ekonomicko-manazerske spektrum* 15, no. 1 (2021): 55-63. https://doi.org/10.26552/ems.2021.1.55-63

[2] Pawar, Suraj, Vipul Kithani, Sagar Ahuja, and Sunita Sahu. "Smart home security using IoT and face recognition." In *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, pp. 1-6. IEEE, 2018. https://doi.org/10.1109/ICCUBEA.2018.8697695

[3] Khalaf, A. O. A. H., Raihani Mohamed, and Abdul Rafiez Abdul Raziff. "Detection model for ambiguous intrusion using smote and lstm for network security." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 39, no. 2 (2024): 191-203. https://doi.org/10.37934/araset.39.2.191203

[4] Hussin, Muhammad, Jamaludin Jalani, Muhammad Powdzi, Sujana Rejab, and Mohamad Khairi Ishak. "Smart Robot Cleaner Using Internet of Things." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 46 (2024): 175-186. https://doi.org/10.37934/araset.46.1.175186

[5] Guixia, Xiao, Normalia Samian, Muhammad Faiz Mohd Faizal, Muhammad Alif Zakwan Mohd, Muhammad Firdaus Mohamad Fadzil As'ad, Azizol Abdullah, Winston Khoon Guah Seah, Mastura Ishak, and Irman Hermadi. "A framework for blockchain and internet of things integration in improving food security in the food supply chain." *J. Adv. Res. Appl. Sci. Eng. Technol* 34, no. 1 (2024): 24-37. https://doi.org/10.37934/araset.34.1.2437

[6] Kumar, Sushant, and S. S. Solanki. "Remote home surveillance system." In *2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA)(Spring)*, pp. 1-4. IEEE, 2016. https://doi.org/10.1109/ICACCA.2016.7578890

[7] Mohamed, Raihani, Mohammad Noorazlan Shah Zainudin, Md Nasir Sulaiman, Thinagaran Perumal, and Norwati Mustapha. "Multi-label classification for physical activity recognition from various accelerometer sensor

positions." *Journal of Information and Communication Technology* 17, no. 2 (2018): 209-231. https://doi.org/10.32890/jict2018.17.2.3

[8] Jiang, Ning, Wenxin Yu, Shaopeng Tang, and Satoshi Goto. "A cascade detector for rapid face detection." In *2011 IEEE 7th International Colloquium on Signal Processing and its Applications*, pp. 155-158. IEEE, 2011. https://doi.org/10.1109/CSPA.2011.5759863

[9] Pss, Srivignessh, and M. Bhaskar. "RFID and pose invariant face verification based automated classroom attendance system." In *2016 International Conference on Microelectronics, Computing and Communications (MicroCom)*, pp. 1-6. IEEE, 2016. https://doi.org/10.1109/MicroCom.2016.7522434

[10] Samet, Refik, and Muhammed Tanriverdi. "Face recognition-based mobile automatic classroom attendance management system." In *2017 International conference on cyberworlds (CW)*, pp. 253-256. IEEE, 2017. https://doi.org/10.1109/CW.2017.34

[11] Pranav, K. B., and J. Manikandan. "Design and evaluation of a real-time face recognition system using convolutional neural networks." *Procedia Computer Science* 171 (2020): 1651-1659. https://doi.org/10.1016/j.procs.2020.04.177

[12] Mohamed, Raihani, Jaffrina Umaira Jafni, and Siti Nurulain Mohd Rum. "Real-Time Face Recognition System in Smart Classroom using Haar Cascade and Local Binary Pattern Model." In *2022 International Conference on Advanced Creative Networks and Intelligent Systems (ICACNIS)*, pp. 1-6. IEEE, 2022. https://doi.org/10.1109/ICACNIS57039.2022.10054833

[13] Gu, Jie, and Shan Lu. "An effective intrusion detection approach using SVM with naïve Bayes feature embedding." *Computers & Security* 103 (2021): 102158. https://doi.org/10.1016/j.cose.2020.102158

[14] Bagchi, Trinanjana, Ankita Mahapatra, Dipesh Yadav, Daiwik Mishra, Anish Pandey, P. Chandrasekhar, and Ashwani Kumar. "Intelligent security system based on face recognition and IoT." *Materials Today: Proceedings* 62 (2022): 2133-2137. https://doi.org/10.1016/j.matpr.2022.03.353

[15] Déniz, Oscar, Gloria Bueno, Jesús Salido, and Fernando De la Torre. "Face recognition using histograms of oriented gradients." *Pattern recognition letters* 32, no. 12 (2011): 1598-1603. https://doi.org/10.1016/j.patrec.2011.01.004

[16] Ahonen, Timo, Abdenour Hadid, and Matti Pietikäinen. "Face recognition with local binary patterns." In *Computer Vision-ECCV 2004: 8th European Conference on Computer Vision, Prague, Czech Republic, May 11-14, 2004. Proceedings, Part I 8*, pp. 469-481. Springer Berlin Heidelberg, 2004. https://doi.org/10.1007/978-3-540-24670-1_36

[17] Chen, Lei, Yun-Hong Wang, Yi-Ding Wang, and Di Huang. "Face recognition with statistical local binary patterns." In *2009 International Conference on Machine Learning and Cybernetics*, vol. 4, pp. 2433-2439. IEEE, 2009. https://doi.org/10.1109/ICMLC.2009.5212189

[18] Zhu, Xiaobo, Dong Ren, Zhenyu Jing, Lin Yan, and Shuanghui Lei. "Comparative research of the common face detection methods." In *Proceedings of 2012 2nd International Conference on Computer Science and Network Technology*, pp. 1528-1533. IEEE, 2012. https://doi.org/10.1109/ICCSNT.2012.6526210

[19] Alhanaee, Khawla, Mitha Alhammadi, Nahla Almenhali, and Maad Shatnawi. "Face recognition smart attendance system using deep transfer learning." *Procedia Computer Science* 192 (2021): 4093-4102. https://doi.org/10.1016/j.procs.2021.09.184

[20] Masupha, Lerato, Tranos Zuva, Seleman Ngwira, and Omobayo Esan. "Face recognition techniques, their advantages, disadvantages and performance evaluation." In *2015 International Conference on Computing, Communication and Security (ICCCS)*, pp. 1-5. IEEE, 2015. https://doi.org/10.1109/CCCS.2015.7374154

[21] Hardhienata, Medria Kusuma Dewi, Karlisa Priandana, Daffa Rangga Putra, Mamiek Sriatun, Agus Buono Wulandari, and Raihani Mohamed. "Modification of the Ant Colony Optimization Algorithm for Solving Multi-Agent Task Allocation Problem in Agricultural Application." *Optimization (ACO)* 34, no. 1 (2024): 90-105. https://doi.org/10.37934/araset.34.1.90105

[22] Chandra, ML Ravi, B. Varun Kumar, and B. Suresh Babu. "IoT enabled home with smart security." In *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, pp. 1193-1197. IEEE, 2017. https://doi.org/10.1109/ICECDS.2017.8389630

[23] Khattar, Shubhang, Anisha Sachdeva, Rishi Kumar, and Richa Gupta. "Smart home with virtual assistant using raspberry pi." In *2019 9th International conference on cloud computing, data science & engineering (Confluence)*, pp. 576-579. IEEE, 2019. https://doi.org/10.1109/CONFLUENCE.2019.8776918

[24] Bao, Zhipeng, and Peidong Zhuang. "Smart Door Lock System Based on STM32." In *International Conference in Communications, Signal Processing, and Systems*, pp. 381-388. Singapore: Springer Nature Singapore, 2023. https://doi.org/10.1007/978-981-99-7502-0_42