Journal of Global Engineering Research & Science (J-GERS)
Vol. 04, No. 02, December 2025, pp. 56-66
ISSN: 2830-5906, *e*-ISSN: 2830-5418, DOI: 10.56904/j-gers.v4i2.162

Smart Keyless Locker Design Using Face Recognition Technology Based on the Internet of Things Jakarta Global University Classroom

Arizki Rahman[1], Legenda Prameswono Pratama[1*], Hamzah[1], Brainvendra Widi Dionova[1], Arisa Olivia Putri[1], Sinka Wilyanti[1], Safaa Najah Saud Al-Humairi[2]

[1*] Department of Electrical Engineering, Faculty of Engineering & Computer Science, Jakarta Global University, Indonesia, 16412
[2]Faculty of Information Sciences and Engineering, Management and Science University, Malaysia, 40100

Article Info

Article history:

Received August 29, 2025
Revised October 18, 2025
Accepted November 24, 2025

Keywords:

Smart Keyless Locker
Face Recognition
Internet of Things (IoT)
Biometric Authentication
OpenCV

ABSTRACT

This research presents the design and implementation of an Internet of Things (IoT)-based Smart Keyless Locker integrated with face recognition technology to enhance security and efficiency in classroom locker management at Jakarta Global University. The system replaces conventional mechanical keys with biometric authentication to minimize risks associated with key loss, duplication, and unauthorized access. The hardware architecture consists of a Raspberry Pi as the primary processing unit for facial recognition, an Arduino Mega for actuator control, a camera module for image acquisition, solenoid door locks as locking mechanisms, load cell sensors for locker status detection, and an IoT-based notification system integrated with WhatsApp for real-time monitoring. The facial recognition process utilizes the Haar Cascade Classifier for face detection and the Local Binary Patterns Histograms (LBPH) algorithm for feature extraction and matching. System performance was evaluated under various conditions, including differences in lighting intensity, facial orientation, distance, and face coverings. Experimental results indicate that the system achieved a recognition success rate of 50% under the tested conditions, particularly within a distance range of 40–70 cm and adequate lighting. The average verification time ranged from 1.4 to 2.1 seconds depending on facial angle, while the WhatsApp notification system demonstrated reliable message delivery with an average delay of 4.75 seconds. Although recognition performance decreases when facial features are partially obstructed or when lighting is insufficient, the proposed system demonstrates the feasibility of integrating biometric authentication with IoT technology for modern classroom locker management applications.

Corresponding Author:

Legenda Prameswono Pratama
Department of Electrical Engineering, Faculty of Engineering & Computer Science, Jakarta Global University, Indonesia, 16412
Email: legenda@jgu.ac.id

1. INTRODUCTION

While the last century has been defined by a breathtaking pace of technological advancement, locker security systems have remained curiously frozen in time [1]. Despite the digital revolution, many storage solutions still rely on stagnant, traditional mechanisms that feel increasingly out of sync with our hyper-connected world. Addressing this gap requires more than just a better lock; it demands the integration of the Internet of Things (IoT). By bridging the gap between physical hardware and digital networks, IoT transforms a passive storage box into an intelligent, responsive asset [2]. Ultimately, this shift enables real-time remote monitoring and seamless connectivity, offering a modern security framework that finally catches up to the demands of the 21st century.

© 2025 Published by Faculty of Engineering & Computer Science

Facial recognition technology has already become a cornerstone of modern surveillance, yet its application within locker security remains surprisingly limited, with many systems still tethered to vulnerable conventional keys [3]. To address this technological lag, this design introduces an innovative authentication unit powered by a Raspberry Pi, which cross-references real-time data against a trusted user database to automate locker access. By replacing physical hardware with biometric verification, the system offers a seamless, hands-free experience that eliminates the risks associated with lost or duplicated keys. This transition toward facial recognition represents a modern and adaptive approach to security, aligning perfectly with the increasing demand for intelligent, digital-first solutions in today's landscape.

The Smart Keyless Locker Security System specifically leverages facial recognition technology to eliminate the reliance on physical keys, providing a more robust and streamlined alternative to traditional locking mechanisms. This innovation serves as a direct response to the inherent vulnerabilities of conventional lockers, which remain susceptible to unauthorized access and the frequent loss of physical assets [4]. While earlier research focused heavily on Radio Frequency Identification (RFID) or alternative biometrics such as fingerprint scanning, the current system prioritizes facial recognition as a more flexible and secure access protocol. By utilizing real-time biometric markers to automate entry, it delivers a hands-free, high-security solution that effectively addresses the limitations of single-authentication methods in modern digital infrastructure. Accordingly, this study aims to develop a Smart Keyless Locker Design Using Face Recognition Technology Based on the Internet of Things to enhance security and accessibility within the Jakarta Global University Classroom.

2. METHOD

The development of this system follows a structured engineering approach designed to ensure the prototype effectively meets the specific security requirements of the Jakarta Global University classroom. The process began with a comprehensive requirements analysis, which identified the vulnerabilities of manual keys in a campus setting and established the need for a hands-free, biometric logging system. This led to the architectural design phase, where the system was mapped to integrate a Raspberry Pi microcontroller with a camera module, an OpenCV-based recognition algorithm, and a Telegram Bot for real-time IoT notifications. During the implementation phase, the physical prototype was constructed and subjected to rigorous experimentation, specifically testing facial verification accuracy across varying distances and angles to ensure operational reliability. Finally, the study concluded with the deployment of the system within the JGU classroom to evaluate its real-world performance and user acceptance, effectively bridging the gap between theoretical biometric security and practical educational infrastructure.

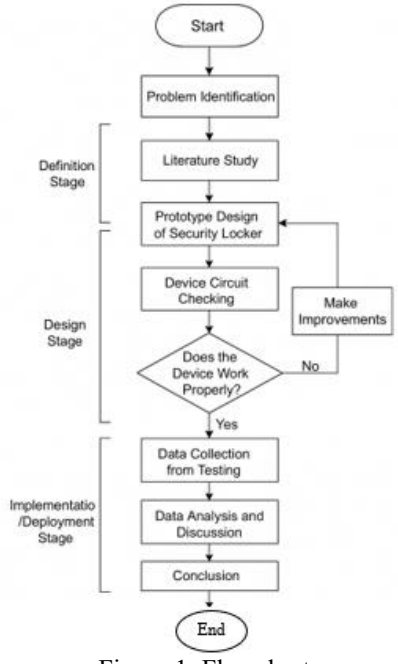

Figure 1. Flowchart

Recent literature has established several pathways for enhancing smart locker security and monitoring. Prior research primarily utilized Bluetooth Low Energy (BLE) technology, which restricted access to users

e-ISSN: 2830-5418, *p*-ISSN: 2830-5906

possessing authenticated hardware tokens, such as valid I-tags [5]. However, these systems often relied on secondary manual backups, such as a numeric keypad, to ensure access during power failures, a feature that introduces potential physical vulnerabilities. Further studies have suggested that security could be significantly strengthened by integrating biometric facial recognition with real-time mobile notifications. Specifically, the implementation of automated messaging via platforms like WhatsApp has been proposed as an effective method for monitoring key borrowing and tracking locker occupancy in real-time. By shifting toward these digital-first protocols, contemporary systems aim to eliminate the dependency on physical tokens and hardware-based entry.

2.1 Face Recognition

Face recognition in this study refers to a system that utilizes the Local Binary Patterns Histograms (LBPH) Face Recognizer algorithm implemented in OpenCV. The system employs a Haar Cascade classifier to detect faces by scanning image regions for specific patterns based on contrast differences between light and dark pixels. These patterns, known as Haar features, reflect the natural structural characteristics of human facial components such as the eyes, nose, and mouth. Once the face region is successfully detected and cropped (left image) in Figure 2, it is converted into a grayscale image to simplify intensity analysis. A 3×3 neighbourhood example is shown in Figure 2 to demonstrate how pixel intensity values are processed. The Local Binary Pattern (LBP) operator compares each neighbouring pixel value with the centre pixel. If the neighbouring value is greater than or equal to the centre pixel, it is assigned a value of 1; otherwise, it is assigned 0. This comparison generates a binary pattern that is then converted into a decimal value representing the local texture feature. The resulting LBP map (top right) in Figure 2 highlights facial texture characteristics. Finally, a histogram of LBP codes (0–255) is computed (bottom right) in Figure 2, representing the distribution of local texture features across the detected face. This histogram serves as the facial descriptor used by the LBPH algorithm for training and recognition

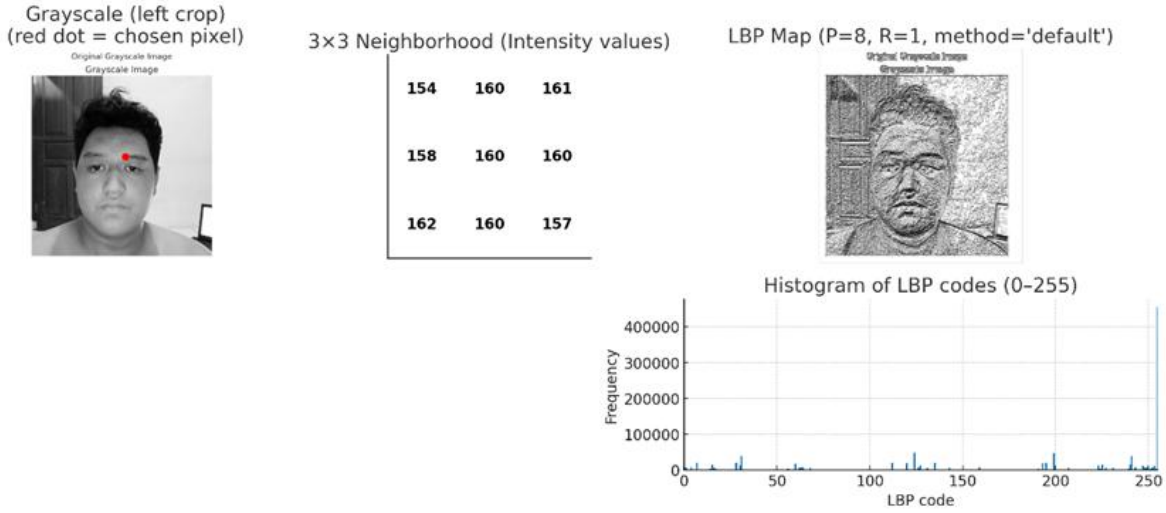

Figure 2. Face Recognition Analysis

In LBPH-based face recognition, the face with the smallest distance value between feature vectors is considered the best match, indicating the highest similarity between the test and stored faces. The LBPH algorithm has several key parameters: Radius, which defines the distance from the centre pixel to its neighbours (default: 1); Neighbours, the number of sample points around the centre pixel (default: 8); and Grid X and Grid Y, which specify the number of horizontal and vertical cells into which the image is divided (default: 8×8). Research has shown that facial recognition technology can enhance security and significantly reduce errors in attendance data collection and fraud detection by automating identity verification and minimizing human intervention errors. For example, a face recognition system based on LBPH has been successfully applied to automate attendance monitoring with high accuracy, demonstrating its practical viability in real-world educational environments [6]. Another study explored a multi-camera attendance solution that integrated LBPH with Haar Cascades to achieve reliable recognition even in challenging classroom scenarios [7]. Furthermore, facial recognition has been used to distinguish residents from non-residents in controlled access systems, showing its value beyond attendance into broader security applications.

2.2 Internet of Things

Gubbi et al. (2013) [8] explain that the term “Things” in the Internet of Things does not refer to all real-world objects, but specifically to physical entities that are identifiable, measurable, and capable of sensing and communication within a defined environment. In the IoT context, an object is defined relative to a target entity or environmental parameter; in this research, the target object is temperature [8]. Furthermore, a device is defined as an electronic component that directly interacts with the target unit, such as a transducer or sensor that converts environmental changes into electrical signals, which are then digitized using an analog-to-digital converter (ADC). IoT systems are generally composed of three main components: sensors, infrastructure (including hardware and communication protocols), and services. This conceptual framework is reflected in practical implementations, such as the study by Prayogo et al. (2025)[9], which developed a home security system based on Raspberry Pi and a PIR sensor integrated with WhatsApp Messenger notifications, demonstrating the integration of sensing devices, embedded processing units, and internet-based communication services. Moreover, as highlighted by Krawiec et al. (2025) [10], the rapid growth of IoT deployments leads to increased energy consumption, making the selection of efficient network communication protocols a critical factor in reducing power usage and improving overall system sustainability

2.3 Hardware

The first circuit consists of a Raspberry Pi connected to a display via an HDMI interface to output visual data and receive input from peripheral devices such as a keyboard, mouse, and webcam. The Raspberry Pi operates at a required supply voltage of 5 V, which is obtained by stepping down a 12 V DC power source to 5 V DC using a step-down converter directly connected to the power supply. In this system, the Raspberry Pi functions as the main control unit, serving as the central platform for issuing commands and receiving data from the Arduino Mega 2560. Additionally, it acts as the primary controller that manages and coordinates all connected components, including relays, servo motors, and load cells.

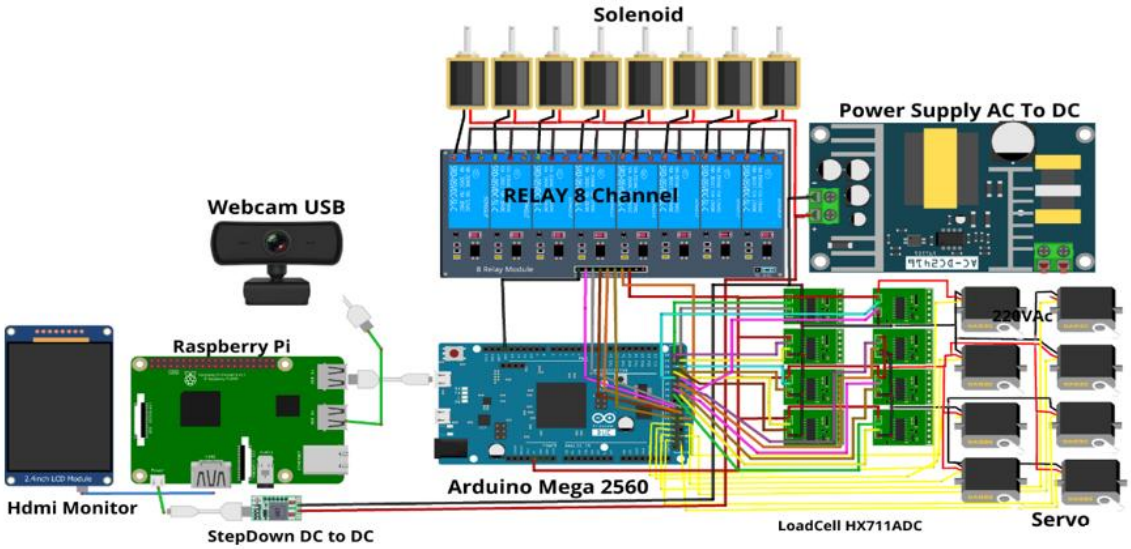

Figure 3. Circuit Diagram

The first circuit, shown in Figure 3, is centered on a Raspberry Pi connected to a display via an HDMI interface to output visual data and receive user input from peripheral devices, including a keyboard, mouse, and webcam. The system operates at a required voltage of 5 V, which is obtained by stepping down a 12 V DC power supply to 5 V DC using a step-down voltage regulator. The Raspberry Pi functions as the main processing unit, serving as the command and data exchange interface with the Arduino Mega 2560, and coordinating overall system operation. As illustrated in Figure 3, the Arduino Mega 2560 is responsible for controlling the peripheral hardware components. The servo motor circuits are connected to PWM pin group 1 (pins 30–37), with VCC and GND connected to the 5 V and GND pins of the Arduino. The relay circuits are connected to PWM pin group 2 (pins 40–47), with their VCC and GND similarly connected to the Arduino’s 5 V and GND outputs. The load cell modules, each equipped with SCK and DOUT pins, are interfaced with the Arduino Mega 2560 using dedicated digital pins, as shown in Figure 3. The SCK pins are connected to Arduino pins 23, 25, 27, 29, 39, 49, 51, and 53, while the DOUT pins are connected to pins 22, 24, 26, 28, 38,

39, 50, and 52. The VCC and GND connections for all load cells are supplied directly from the Arduino Mega 2560. Furthermore, in Figure 3, the solenoid actuator is powered by a 12 V DC supply, with its VCC connected directly to the 12 V power source. The GND connection is routed through the corresponding relay contacts, allowing the solenoid to be activated and deactivated via relay control.

2.4 Algorithm Face Recognition

The face recognition system employs a Haar Cascade classifier to detect faces by scanning image regions for specific patterns based on contrast differences between light and dark pixels [11]. These patterns, known as Haar features, reflect the natural structural characteristics of human facial components such as the eyes, nose, and mouth. Each Haar feature is computed using a mathematical formulation to evaluate intensity differences within defined rectangular regions (f)

$$f = \sum(white\ pixels) - \sum(black\ pixels)$$

To speed up the pixel count, the integral image formula is used

$$I(x,y) = \sum_{x' \le x, y' \le y} pixel(x', y')$$

This approach enables the total number of pixels within a rectangular region to be computed in constant time, O (1). The Local Binary Patterns Histograms (LBPH) Face Recognizer is a simple yet effective facial recognition algorithm, particularly robust under varying and unstable lighting conditions. The LBPH method operates by extracting local texture features from facial images using the Local Binary Pattern (LBP) operator and subsequently representing these features as histograms. These histograms are then compared to perform face recognition. The LBP computation is carried out as follows: for each pixel, the intensity value of the center pixel is compared with those of its eight surrounding neighbors. If a neighboring pixel has an intensity value greater than or equal to that of the center pixel, it is assigned a value of 1; otherwise, it is assigned a value of 0. The resulting sequence of binary values forms an 8-bit binary number, which is then converted into a decimal value to represent the local texture pattern. The formula is

$$LBP\ (x_c, y_c) = \sum_{p=0}^{P-1} s(\, i_p - i_c)\, .\, 2^p$$

i_p represents the intensity of the center pixel, while i_c denotes the intensity of the p-th neighboring pixel. The function $s(x)$ returns a value of 1 when x ≥ 0, and 0 when x < 0. The extracted Local Binary Pattern (LBP) features are first divided into several small image grids, for example, 8 × 8 blocks, to preserve the spatial distribution of facial textures. For each grid, a local histogram is generated by calculating the frequency of LBP values ranging from 0 to 255. These local histograms are then concatenated into a single feature vector that represents the overall facial characteristics. Face recognition is performed by comparing the input face feature vector with stored face data using the Euclidean distance metric, where the smallest distance indicates the highest similarity and the best matching identity.

$$d = \sqrt{\sum_{i=1}^{N} (H_1[i] - H_2[i])^2}$$

The Euclidean distance value obtained from this calculation represents the level of similarity between the input face image and each image stored in the database. A smaller distance indicates a higher degree of similarity, meaning that the extracted feature patterns are more closely matched. During the recognition process, the system computes the distance between the test image histogram and all stored histograms, then ranks them based on ascending distance values. The identity associated with the minimum distance is selected as the recognition result. This approach ensures a straightforward and computationally efficient classification process while maintaining reliable accuracy in distinguishing different facial patterns.

3. RESULTS AND DISCUSSION

This locker security system employs face recognition technology to enhance security in campus classroom locker management by ensuring that all users are properly recorded and authenticated. The borrowing process involves facial scanning along with the entry of the user's name and telephone number. To support timely returns, the system automatically sends WhatsApp reminder notifications to users before the return deadline. Each user is allowed to access only one locker at a time and cannot borrow another locker until the previously assigned key has been returned. Locker availability is determined by using a load cell sensor; if the detected return weight is less than 200 g or does not correspond to the recorded weight of the borrowed item, the system will reject the return and remain in return mode. The system is integrated with the Internet of Things (IoT) and is managed via a local dashboard that enables real-time monitoring of each locker's status and the weight of its contents. Once all required hardware components are prepared, the system design process continues with the fabrication of the frame and locker structures, which function as the testing platform for the developed system.

Figure 4. Complete design

Figure 4 illustrates the smart locker design, which was developed and adjusted from the initial design created using Tinker cad. The locker container and frame are constructed from 15-mm-thick wood. Each locker measures 20 × 20 cm and is arranged in four columns and two rows, resulting in a total of eight locker doors. In the present testing phase, only four locker doors are used. After the locker structure is completed, the designed electronic components are installed inside the locker system.

3.1. Locker Security

This locker security system utilizes facial recognition technology to enhance the security of campus classroom lockers by ensuring that all users are properly recorded. The borrowing process includes facial scanning, as well as the input of the user's name and telephone number. To ensure timely returns, the system automatically sends WhatsApp reminder notifications to users. Each user is permitted to use only one locker at a time and cannot borrow another locker until the previously assigned key has been returned. Locker availability is determined by using a load cell sensor. If the detected return weight is less than 200 g or does not match the recorded weight of the borrowed item, the system will reject the return and remain in return mode. The system is integrated with the Internet of Things (IoT) and is controlled through a local dashboard that enables real-time monitoring of each locker's status and weight.

3.2. Efficiency of Technology Implementation in Classroom Locker Key Access

The efficiency of the facial recognition system was evaluated as an access method for classroom locker keys. The evaluation was conducted comprehensively by considering multiple technical aspects as well as direct user interaction. Accordingly, a series of tests were performed based on several relevant indicators. The tests were carried out under various conditions, including recognition distances of 40–70 cm, straight and oblique facial orientations, and facial appearances with additional attributes such as glasses and masks. Under ideal conditions, the system achieved a 100% recognition rate. However, recognition performance decreased when the face was partially obscured or when the distance exceeded 100 cm.

e-ISSN: 2830-5418, *p*-ISSN: 2830-5906

Table 1. Testing With Light Variable Conditions

No	Respondent	Light Conditions	Distance (cm)	Intensity (Lux)	1st Verification Time (S)	2nd Verification Time (S)	3rd Verification Time (S)	Status Umum
1	User 1	Low Light	40	±52	-	-	-	Fail
2	User 1	Low Light	55	±51	-	-	-	Fail
3	User 1	Low Light	40	±312	2,1	2,0	1,9	Succeed
4	User 1	Medium Light	55	±283	2,3	2,0	2,1	Succeed
5	User 1	Medium Light	60	±322	2,2	2,1	2,0	Succeed
6	User 1	Bright Light	70	±346	2,0	1,9	2,1	Succeed
7	User 1	Low Light	40	±665	2,5	2,8	2,4	Succeed
8	User 1	Low Light	55	±689	1,8	1,6	1,6	Succeed
9	User 1	Medium Light	60	±569	1,7	1,6	1,5	Succeed
10	User 1	Bright Light	100	±711	1,6	1,5	1,6	Succeed

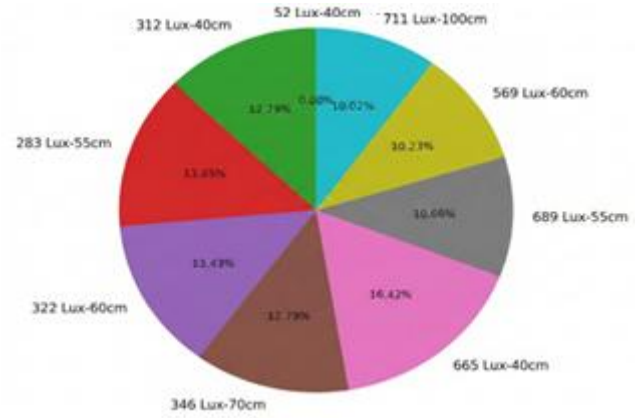

Figure 5. Face Recognition Verification

Based on Figure 5, lighting intensity has a significant effect on the speed and accuracy of the facial recognition system during the verification process. Three lighting conditions were evaluated: dim (approximately ±50 lux), medium (approximately ±300 lux), and bright (approximately ±700 lux), and the results varied noticeably across these conditions. Under dim lighting conditions (±50 lux), the system failed to perform facial verification. This failure occurred because the low light intensity prevented the camera from capturing facial features clearly, causing the Local Binary Pattern (LBP) algorithm to function improperly. As a result, key facial characteristics such as shape, skin texture, and contours could not be accurately extracted, leading to unsuccessful authentication. Consequently, the graph indicates failure for this condition, as the system was unable to produce valid verification results. In contrast, under medium lighting conditions (±300 lux), the system demonstrated stable and reliable performance. The average facial verification time was approximately 2.08 seconds, which is sufficiently fast for real-time applications. Overall, the system performs well under adequate to bright lighting conditions but experiences significant performance degradation in low-light environments. Therefore, for practical implementation, it is strongly recommended to provide stable and sufficiently bright artificial lighting in the facial recognition area to ensure optimal system performance.

3.3. System Reliability Testing

Tests were conducted under various conditions, including recognition distances of 40–70 cm, frontal and angled facial orientations, and facial appearances with additional attributes such as glasses and masks. Under these test conditions, the facial recognition system achieved a recognition success rate of 50%. This percentage was calculated based on 5 successful recognitions out of 10 total test cases. Successful recognitions occurred in test cases corresponding to rows 1, 2, 3, 4, and 9, while failures were observed in rows 5, 6, 7, 8, and 10. The results indicate that although the system performs adequately under certain conditions, its reliability decreases when variations in facial orientation, accessories, or other environmental factors are introduced. These findings suggest that further optimization is required to improve robustness and consistency across diverse real-world usage scenarios.

Table 2. Facial Recognition Results under Various Face Covering Conditions

No	Respondent	Face Condition	Distance (cm)	Intensity (lux)	Verification time (s)	Succeed/fail
1	User 1 Test 1	Normal Face	40	312	1,6	Succeed
2	User 1 Test 2	Wearing Glasses	55	283	2,0	Succeed
3	User 1 Test 3	Smiling Face	60	322	1,8	Succeed
4	User 1 Test 4	Sad Face	70	346	2,2	Succeed
5	User 1 Test 5	Wearing a Mask	50	665	-	Fail
6	User 1 Test 6	Angry Face	65	689	-	Fail
7	User 1 Test 7	Distance Too Far	100	569	-	Fail
8	User 1 Test 8	Face Not Registered	50	711	-	Fail
9	User 1 Test 9	Wearing Glasses	55	312	2,3	Succeed
10	User 1 Test 10	Wearing a Mask	40	283	-	Fail

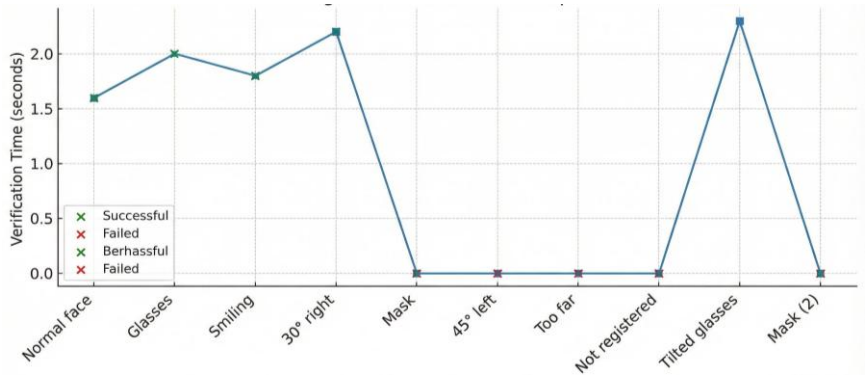

Figure 6. Facial Recognition and verification time

Figure 6 illustrates the facial recognition verification time under various test conditions. The results show that the system performs effectively when facial features are clearly visible and within an appropriate distance. Under normal facial conditions, the average verification time was approximately 1.6 seconds, indicating stable performance. Similar results were observed when users wore glasses, smiled, or slightly tilted their faces (30° to the right), with verification times ranging between 1.8 and 2.2 seconds. These results suggest that minor facial variations and common accessories such as glasses do not significantly degrade system performance when lighting and distance conditions are adequate. However, the system failed to perform verification under several challenging conditions, including when the user wore a mask, tilted the face at 45°, was positioned too far from the camera, or was not registered in the database. In these cases, the verification time was recorded as zero, indicating that the system was unable to process or authenticate the facial data. This failure can be attributed to insufficient facial feature extraction, as key facial landmarks required by the Local Binary Pattern (LBP) algorithm were either partially or entirely obscured. An interesting observation is that the system successfully verified users wearing tilted glasses, although the verification time increased to approximately 2.3 seconds. This indicates that while the system can tolerate certain visual distortions, increased processing time may be required to extract valid facial features. Overall, the results demonstrate that the facial recognition system performs reliably under controlled conditions but experiences significant limitations when facial features are obstructed or when the user deviates substantially from optimal positioning. These findings highlight the need for improved robustness, particularly for handling occlusions and non-ideal user positions in real-world applications.

3.4. Recognition success rate

The test was conducted using a single respondent at a fixed distance of 40 cm under adequate lighting conditions. The experimental variable was the facial tilt angle, which was varied from a frontal position (0°) to left and right orientations within a range of −45° to 35°. The observed parameters were the facial verification time (in seconds) and the recognition success rate. Based on the results presented in Table 3, the fastest verification time was achieved at a 0° angle, where the face was directly facing the camera, with an average time of 1.40 seconds. This result occurs because all key facial features, such as the eyes, nose, and mouth, are fully visible, allowing optimal feature extraction and matching. As the facial tilt angle increases to either side, the verification time also increases. For instance, at a −45° angle, the verification time rose to 2.10 seconds, while at a 35° angle, it reached 2.05 seconds. The increase in verification time can be attributed to the Local Binary Pattern Histogram (LBPH) algorithm requiring additional processing to match facial images that are partially visible. Consequently, the Euclidean distance (SDR) search process becomes more computationally

e-ISSN: 2830-5418, *p*-ISSN: 2830-5906

demanding. Overall, system performance decreases when the facial tilt angle exceeds ±25°, as some facial features are no longer fully captured by the camera.

Table 3. Face Recognition Success Rate

No	Respondent	Recognition Condition	Face Angle	Lighting	Distance	Recognition Status system	Verification time	Logically Conformity With experiment
1	User 1 Test 1	Normal face	-45°	Fairly bright	40	Success	2.1	Appropriate
2	User 1 Test 2	Normal face	-35°	Fairly bright	40	Success	1.95	Appropriate
3	User 1 Test 3	Normal face	-25°	Fairly bright	40	Success	1.8	Appropriate
4	User 1 Test 4	Normal face	-15°	Fairly bright	40	Success	1.65	Appropriate
5	User 1 Test 5	Normal face	-5°	Fairly bright	40	Success	1.55	Appropriate
6	User 1 Test 6	Normal face	0°	Fairly bright	40	Success	1.4	Appropriate
7	User 1 Test 7	Normal face	5°	Fairly bright	40	Success	1.5	Appropriate
8	User 1 Test 8	Normal face	15°	Fairly bright	40	Success	1.7	Appropriate
9	User 1 Test 9	Normal face	25°	Fairly bright	40	Success	1.92	Appropriate
10	User 1 Test 10	Normal face	35°	Fairly bright	40	Success	2.05	Appropriate

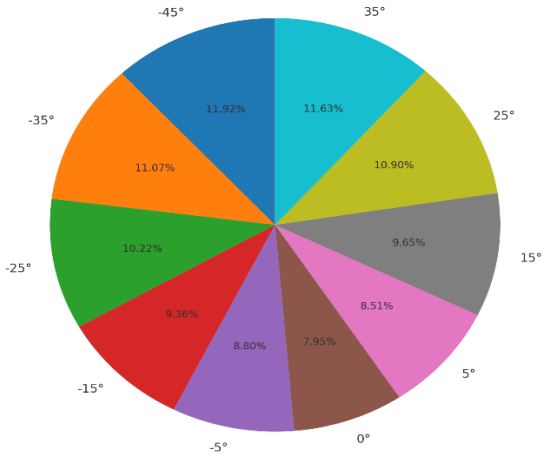

Figure 7. Average Percentage of Success Graph for Various Angles

3.5. Notification WhatsApp

Table 4 presents the results of WhatsApp notification testing for the locker system. The test was conducted to evaluate the reliability of message delivery and the time delay between the system-generated notification and the actual time the message was received by users. The results show that all notifications sent from the system were successfully delivered, as indicated by the "Success" recognition status and the "Sent" status for all tested lockers. The recorded delay times ranged from 3 to 7 seconds. Lockers 1 and 2 experienced the shortest delay of 3 seconds, while the longest delay of 7 seconds occurred for Locker 7. These variations in delay can be attributed to network conditions, server response time, and WhatsApp message routing processes. Despite these variations, the delay duration remains within an acceptable range for reminder notifications, as the messages are intended to inform users of return deadlines rather than requiring immediate action. Overall, the results demonstrate that the WhatsApp notification feature operates reliably and consistently across multiple lockers. The successful message delivery and relatively short delay times indicate that the system is suitable for real-time notification purposes in the locker management application. However, further testing under different network conditions and with a larger number of users is recommended to evaluate system performance scalability and robustness in real-world deployments.

Table 4. Testing Notifications WhatsApp

No	Locker	WhatsApp Number	Sent time	Real Time sent	Delay	Recognition Status System	Status Sent/Fail
1	Locker 1	08xxxxxxxxxx	15:59:00	15:59:03	3	Success	Sent
2	Locker 2	08xxxxxxxxxx	15:59:05	15:59:08	3	Success	Sent
3	Locker 3	08xxxxxxxxxx	15:59:10	15:59:15	5	Success	Sent
4	Locker 4	08xxxxxxxxxx	15:59:15	15:59:21	6	Success	Sent
5	Locker 5	08xxxxxxxxxx	15:59:20	15:59:23	3	Success	Sent
6	Locker 6	08xxxxxxxxxx	15:59:25	15:59:30	5	Success	Sent
7	Locker 7	08xxxxxxxxxx	15:59:30	15:59:37	7	Success	Sent
8	Locker 8	08xxxxxxxxxx	15:59:35	15:59:41	6	Success	Sent

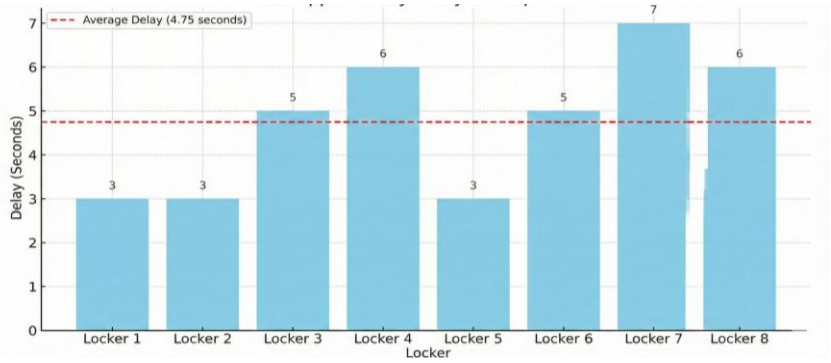

Figure 8. Notification Delivery Delay

Figure 8 illustrates the WhatsApp notification delay for each locker, highlighting the system's communication performance. The delay values range from 3 to 7 seconds across the eight tested lockers, with an average delay of approximately 4.75 seconds, as indicated by the dashed reference line. Lockers 1, 2, and 5 exhibited the shortest delays of 3 seconds, suggesting stable network connectivity and efficient message transmission during these instances. Moderate delays of around 5 seconds were observed for Lockers 3 and 6, while Lockers 4 and 8 experienced slightly higher delays of 6 seconds. The longest delay, 7 seconds, occurred at Locker 7, which may be attributed to temporary network latency or server-side processing variations during message delivery. Despite these differences, all recorded delays remain within a reasonable range for reminder-based notification systems, where immediate response is not critical. Overall, the results demonstrate that the WhatsApp notification feature operates reliably and consistently, with no message delivery failures observed. The relatively low and stable average delay indicates that the system is suitable for real-time locker return reminders. Nevertheless, further evaluation under varying network conditions and with increased system load is recommended to assess scalability and long-term reliability in real-world implementations.

4. CONCLUSION

Based on the design, implementation, and testing of the Smart Keyless Locker system using Internet of Things (IoT)–based face recognition technology, the following conclusions can be drawn:

1. The face recognition–based locker security system was successfully designed and implemented. A Raspberry Pi was used as the main processor for facial recognition, while an Arduino Mega was employed to control actuators, including relays and solenoid door locks.
2. The system was able to recognize users' faces with a success rate of 50% under the tested conditions, particularly at recognition distances of 40–70 cm. Recognition failures occurred when the user wore a mask, was positioned too far from the camera, or when the face was not registered in the system database.
3. Communication between the Raspberry Pi and the Arduino Mega was stable and reliable. All control commands transmitted from the Raspberry Pi were successfully executed by the Arduino, including relay switching and solenoid lock operation.

ACKNOWLEDGEMENTS

The authors thank the institution and laboratory staff for providing the facilities and technical support necessary for the successful implementation and testing of the Smart Keyless Locker system. Finally, appreciation is expressed to colleagues and peers for their valuable discussions and encouragement during the research process.

REFERENCES

[1] C. M. Shruthi, S. K. Bandari, C. K. Reddy Ala, and M. Reddy, "Locker Security System using Internet of Things," *E3S Web Conf.*, vol. 391, p. 01153, Jun. 2023, doi: 10.1051/e3sconf/202339101153.

[2] C. Bharatiraja, P. K. Chittoor, and Y. V. Bhargava, "An IoT based centralized smart locker using RFID technology," 2023, p. 020098. doi: 10.1063/5.0101139.

[3] A. A. Alzhrani, M. Balfaqih, F. Alsenani, M. Alharthi, A. Alshehri, and Z. Balfagih, "Design and Implementation of an IoT-Integrated Smart Locker System utilizing Facial Recognition Technology," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 4, pp. 16000–16010, Aug. 2024, doi: 10.48084/etasr.7737.

[4] R. Sudrajad, Achmad Fauzi, and Milli Alfhi Syari, "Development of a Dual Biometric Authentication System Based on IoT with Facial Recognition and Fingerprint for Safe Security," *J. Artif. Intell. Eng. Appl.*, vol. 5, no. 1, pp. 1529–1544, Oct. 2025, doi: 10.59934/jaiea.v5i1.1663.

[5] A. Lacava, V. Zottola, A. Bonaldo, F. Cuomo, and S. Basagni, "Securing Bluetooth Low Energy networking: An overview of security procedures and threats," *Comput. Networks*, vol. 211, p. 108953, Jul. 2022, doi: 10.1016/j.comnet.2022.108953.

[6] Nurhikma, Abdul Wahid, and Jumadi M Parenreng, "E-Presence and Monitoring System Based on Face Image Recognition

with Local Binnary Pattern Histogram (LBPH) Algorithm," *J. Embed. Syst. Secur. Intell. Syst.*, pp. 68–75, Mar. 2024, doi: 10.59562/jessi.v5i1.556.

[7] N. Habumugisha, J. Ngugi, and D. Sumbiri, "A Multi-Camera Automated Attendance System Using LBPH-Based Face Recognition," *J. Inf. Technol.*, vol. 5, no. 12, pp. 18–29, Nov. 2025, doi: 10.70619/vol5iss12pp18-29-694.

[8] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013, doi: 10.1016/j.future.2013.01.010.

[9] P. K. Prayogo, L. P. Pratama, and D. Junesco, "Home Security System Based on Raspberry Pi and PIR Sensor Using WhatsApp Messenger," *J. Glob. Eng. Res. Sci.*, vol. 4, no. 1, pp. 1–10, Jun. 2025, doi: 10.56904/j-gers.v4i1.134.

[10] J. Krawiec *et al.*, "Energy Footprint and Reliability of IoT Communication Protocols for Remote Sensor Networks," *Sensors*, vol. 25, no. 19, p. 6042, Oct. 2025, doi: 10.3390/s25196042.

[11] H. Kaur and A. Mirza, "Face Detection Using Haar Cascades Classifier," in *Proceedings of the 2nd International Conference on ICT for Digital, Smart, and Sustainable Development, ICIDSSD 2020, 27-28 February 2020, Jamia Hamdard, New Delhi, India*, EAI, 2021. doi: 10.4108/eai.27-2-2020.2303218.