MULTIMEDIA UNIVERSITY

TRIMESTER 2, SESSION 2023/2024

FYP Research Proposal

Raspberry Pi-based Face Recognition Door Lock System

APM6168 – PROJECT

Name	Student ID	Faculty
Seifeldin Sherif Elnozahy	1191102388	FOE

Supervisor: Dr. Chinnaiyan Senthilpari

ABSTRACT

This project proposes the development of a Raspberry Pi-based Face Recognition Door Lock System, integrating machine learning, AI, and OpenCV. By leveraging facial recognition technology and Raspberry Pi microcomputing, the system aims to enhance security and convenience in various environments. Hardware components such as Raspberry Pi, camera module, relay module, and lock mechanism are integrated with software components including OpenCV for real-time image processing and machine learning algorithms for facial recognition. The system will be trained to accurately detect, recognize, and authenticate authorized individuals based on their facial features. The affordability and accessibility of hardware components, coupled with the scalability of open-source software libraries like OpenCV, ensure widespread adoption potential. This study helps to advance smart security systems by providing a potential alternative to solve the constraints of standard door locks and enable safer and more convenient access control methods.

TABLE OF CONTENTS

INTRODUCTION

In today's culture, the importance of security measures has reached new heights, as concerns about unauthorized access and security breaches spread across all industries. The use of traditional key-based or keypad-based door locks, while widespread, has become more unworkable in the face of rising security threats and weaknesses. While traditional locking systems have long been used to provide security, they have inherent limitations that restrict their effectiveness in guaranteeing strong access control.

The ongoing dangers of misplaced or stolen keys, unauthorized replication, and the logistical difficulties involved with key management are crucial among these restrictions. Accidental key loss or illegal duplication of physical key copies pose serious threats to people, property, and assets in addition to compromising the integrity of security procedures. Furthermore, the tedious character of key management—which is typified by the requirement for thorough administration and oversight—imposes substantial operational overheads and logistical difficulties, which reduces the overall effectiveness of security measures.

Given these obstacles, there is a strong need to investigate and adopt cutting-edge solutions that can outperform conventional door locks and strengthen access control systems against modern security risks. Facial recognition technology has become a bright spot in the world of sophisticated security solutions, providing a powerful combination of accuracy, ease of use, and non-intrusiveness when it comes to access management and authentication.

Through the utilization of machine learning algorithms and biometric data, facial recognition systems have shown to be remarkably effective at precisely recognizing and verifying individuals based on their distinct facial characteristics. Without requiring tangible keys or committed passcodes, facial recognition technology provides a smooth and effortless method of access management, eliminating the risks and administrative hassles related to traditional locking systems.

The combination of Raspberry Pi microcomputing's versatility and computational power with facial recognition technology marks a new frontier in the security systems space. Through the utilization of open-source software libraries like OpenCV and the computational efficiencies and extensibility provided by Raspberry Pi platforms, developers can create complex and scalable face recognition systems that are not only dependable and durable but also affordable.

In light of this, the current project aims to investigate the viability and effectiveness of creating a face recognition door lock system based on a Raspberry Pi. This project aims to provide an advanced yet user-friendly replacement for conventional door locks by carefully integrating machine learning, artificial intelligence, and facial recognition technology. With its unmatched security, ease of use, and mental stability, this cutting-edge system has the potential to revolutionize access control techniques in a variety of contexts and uses.

PROBLEM STATEMENT

Robust access control mechanisms are a major barrier for traditional key-based or keypad-based door locks in the quickly changing security landscape of today. Despite their widespread use, these systems have built-in flaws that make it harder for them to keep people safe in a variety of situations.

Traditional door locks come with a number of security problems since they rely on physical keys or passcodes that must be remembered. Security risks include instances of misplaced or stolen keys, unauthorized replication, and the laborious process of key management. These vulnerabilities put properties, assets, and people at risk of harm from unauthorized entry and impair the integrity of access control measures.

Moreover, conventional door locks frequently aren't strong enough to withstand contemporary security risks like hacking and manipulation. The increasing frequency of digital attacks and the spread of advanced incursion tactics highlight how inadequate traditional locking systems are at offering complete safety. Innovative solutions that can effectively minimize the risks caused by contemporary security threats and adjust to the ever-evolving threat landscape are therefore desperately needed.

The rise of these difficulties underscores the pressing need for novel solutions that can improve security, efficiency, and user-friendliness while addressing the deficiencies of current door lock systems. Both individuals and organizations need to make proactive investments in technologies that can protect their privacy, secure their assets, and lessen the possible repercussions of security breaches. As a result, there is a strong need to investigate and apply cutting-edge technologies, like artificial intelligence, machine learning, and facial recognition, to transform access control systems and raise security standards in line with modern digital needs.

MOTIVATION AND OBJECTIVES

The project's motivation comes from the potential advantages it presents in a number of contexts, such as residential, commercial, and institutional settings. A face recognition-based door lock system can provide users with enhanced security, more efficient access control, and a better overall experience. Furthermore, this system is very scalable and environmentally flexible because to the accessibility and affordability of Raspberry Pi hardware and the adaptability of open-source software libraries like OpenCV. The main goal of this project is to create a Face Recognition Door Lock System based on a Raspberry Pi that addresses the drawbacks of conventional door locks and improves convenience and security at the same time. It is a technologically advanced yet approachable replacement.

LITERATURE REVIEW

“A Face Recognition Method In Machine Learning (ML) For Enhancing Security In Smart Home”

The paper titled "A Face Recognition Method In Machine Learning (ML) For Enhancing Security In Smart Home" [1] by M. Alshar’e, M. R. Al Nasar, R. Kumar, M. Sharma, Prof. D. Dharamvir, and V. Tripathi explores the utilization of ML, specifically Convolutional Neural Networks (CNN), to enhance security in smart homes. By leveraging CNN, the system empowers prediction without explicit programming, leading to the automation of security processes. Moreover, the use of CNN Mobilenet and CNN Alexnet techniques contributes to the high accuracy in recognizing faces, a crucial aspect in ensuring the effectiveness of security measures.

However, the adoption of machine learning for face recognition is not without its challenges. One major obstacle lies in the significant data preparation required for training the models effectively. Additionally, the computational complexity associated with ML algorithms can pose implementation challenges, especially in resource-constrained environments such as smart home devices. Moreover, privacy concerns surrounding facial recognition technology remain a prominent issue, necessitating careful consideration of data handling and storage practices.

Despite these challenges, the benefits of employing machine learning for face recognition in smart homes are substantial. The automation of security processes and the deployment of efficient image recognition systems contribute to improving overall security systems' effectiveness. Furthermore, the successful implementation of facial recognition systems on devices like the Raspberry Pi showcases the practicality and feasibility of integrating ML techniques into real-world applications for enhanced security.

In conclusion, the integration of machine learning techniques, particularly CNN, holds promise for enhancing security in smart homes through advanced facial recognition technology. While challenges such as data preparation, computational complexity, and privacy concerns persist, the benefits of automation and improved security outcomes justify continued research and development in this field. Successful implementation and deployment of ML-based facial recognition systems signify a significant step towards achieving robust security measures in smart home environments.

LITERATURE REVIEW

“Raspberry Pi-Powered Door Lock with Facial Recognition”

The paper titled “Raspberry Pi-Powered Door Lock with Facial Recognition” [2] by A. Jha, R. Bulbule, N. Nagrale, T. Belambe, presented at the 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), presents a novel approach to secure access control using facial recognition technology integrated with Raspberry Pi. This section reviews relevant literature in the field, focusing on computer vision, OpenCV, and the Haar cascade algorithm.

Computer vision, an interdisciplinary field that enables computers to interpret and understand visual information from the real world, plays a crucial role in facial recognition systems. OpenCV, an open-source computer vision library, provides essential tools for image and video analysis, including face detection and recognition. The paper leverage OpenCV for processing and displaying camera images, highlighting its importance in facilitating facial recognition tasks.

The Haar cascade algorithm, a machine learning-based approach, is utilized for face detection in images. This algorithm employs a cascade of simple classifiers to efficiently identify objects of interest, making it suitable for real-time applications such as security systems. The literature supports the effectiveness of the Haar cascade algorithm in detecting faces accurately and reliably, contributing to the robustness of the proposed system.

Facial recognition systems typically involve dataset creation and training to develop accurate recognition models. The paper emphasize the importance of collecting facial data images for creating a dataset and training the recognition algorithm. This process may require significant processing power and time, as highlighted in the literature. However, efficient data processing techniques and algorithm training methods can mitigate these challenges, ensuring the reliability and effectiveness of the facial recognition system.

Evaluation of face recognition performance under different conditions is crucial for assessing system reliability and effectiveness. Testing was conducted to validate the functionality of their system, including user identification, lock/unlock functions, and message notifications. The literature emphasizes the importance of comprehensive testing to identify and address potential issues, ensuring the system's robustness in real-world scenarios.

In conclusion, the paper presents a valuable contribution to the field of facial recognition-based security systems. By leveraging computer vision techniques, OpenCV, and the Haar cascade algorithm, the proposed system offers a reliable and efficient solution for secure access control. The literature review highlights the significance of these technologies in advancing facial recognition.

LITERATURE REVIEW

“Face Recognition Door Lock System Using Raspberry PI”

The paper titled " Face Recognition Door Lock System Using Raspberry PI" [3] by A. D. Singh, B. S. Jangra, R. Singh, present a novel approach to secure door access using facial recognition integrated with Raspberry Pi. This section reviews relevant literature in the field, focusing on the Haar Cascade Classifier, OpenCV, and the implementation of face recognition systems using Raspberry Pi.

The Haar Cascade Classifier, a machine learning-based approach, is utilized for accurate face detection in images. This algorithm is known for its effectiveness in detecting objects with high accuracy and efficiency. However, the literature suggests that the performance of the Haar Cascade Classifier may vary under different lighting conditions and facial orientations, highlighting the importance of optimizing parameters for reliable detection.

OpenCV, an open-source computer vision library, plays a crucial role in processing and analyzing images captured by the Raspberry Pi camera. They leverage OpenCV for image processing tasks such as converting images to grayscale, defining regions of interest, and applying thresholding techniques. The literature supports the versatility and effectiveness of OpenCV in various computer vision applications, including facial recognition.

The integration of Raspberry Pi, a low-cost, single-board computer, with face recognition technology offers a cost-effective solution for access control systems. They utilize Raspberry Pi for processing image data, controlling access devices such as solenoid door locks, and implementing remote access functionalities. While Raspberry Pi provides a convenient platform for system implementation, the literature highlights the importance of ensuring reliable internet connectivity for remote access functionalities.

Overall, the paper presents a valuable contribution to the field of access control systems using facial recognition technology. By leveraging the Haar Cascade Classifier, OpenCV, and Raspberry Pi, the proposed system offers improved security and convenience in access control applications. The literature review underscores the significance of optimizing algorithms and hardware configurations for reliable face detection and recognition in real-world scenarios.

LITERATURE REVIEW

“Face Recognition Door Lock System Using Raspberry Pi”

The paper titled " Face Recognition Door Lock System Using Raspberry Pi " [4] by F. N. Nwukor, presents that Face recognition technology has garnered significant attention in the domain of security systems owing to its potential for effective authentication and access control. Among the various techniques employed in face recognition, Principal Component Analysis (PCA) stands out as a statistical approach for simplifying large high-dimensional datasets. By leveraging mathematical tools such as eigenvectors and eigenfaces, PCA extracts essential features from images, facilitating accurate face recognition.

The integration of PCA with OpenCV and Raspberry Pi in face recognition systems offers a cost-effective solution for enhancing home security. Raspberry Pi, a credit card-sized computer, serves as a versatile platform for controlling servo motors and other sensors, enabling automated door access control. This setup offers benefits such as lower power consumption, compact design, and ease of application development on Linux-based operating systems.

However, challenges persist in face recognition systems, particularly in low-light environments where recognition accuracy may be limited. Additionally, reliance on reliable internet connectivity for remote access functionalities poses a constraint in certain scenarios. Despite these challenges, the implementation of face recognition systems using Raspberry Pi and PCA holds promise for enhancing home security and convenience through automated door access control.

The application of Haar Cascade Classifier and Raspberry Pi in this context demonstrates the feasibility of integrating hardware and software components for implementing face recognition technology. By leveraging PCA for data simplification and Raspberry Pi for system control, this approach offers a robust solution for access control in residential settings.

LITERATURE REVIEW

“Home Security System Based On Facial Recognition”

The paper titled " Home Security System Based On Facial Recognition " [5] by D. G. Padhan, M. Divya, S. N. Varma, S. Manasa, V. C., and B. Pakkiraiah, presents a comprehensive approach to enhancing home security through the utilization of facial recognition technology. The authors highlight the growing concern regarding traditional home security systems' vulnerabilities and the need for more advanced and efficient solutions. They argue that facial recognition technology offers a promising avenue for improving security due to its accuracy and reliability.

One of the key contributions of the proposed system is the integration of Facial Recognition with Artificial Intelligence (AI) and Machine Learning (ML) techniques. Specifically, the authors employ the Histograms of Oriented Gradients (HOG) algorithm for facial recognition, which is known for its high precision and efficiency across various lighting conditions. This choice of algorithm underscores the importance of accuracy in facial recognition systems, particularly in the context of home security where reliability is paramount.

Furthermore, the paper emphasizes the role of the Internet of Things (IoT) and Global System for Mobile Communications (GSM) in enhancing the system's functionality. By incorporating IoT and GSM capabilities, the system enables remote access and control, allowing homeowners to monitor and manage their security systems from anywhere. However, it is important to note the potential dependency on reliable internet connectivity for seamless remote access functionalities, which could pose challenges in certain environments.

Moreover, the authors address practical considerations such as low-light conditions, which can impact facial recognition accuracy. While the HOG algorithm is known for its robustness, optimizing performance in challenging lighting environments remains an area of ongoing research and development.

Overall, the paper underscores the significance of facial recognition technology in modern home security systems. By leveraging advanced algorithms and integrating with IoT and GSM technologies, the proposed system offers enhanced security and convenience for homeowners. However, further research may be needed to address challenges such as low-light conditions .

DESIGN METHOD

Main Hardware Components:

1. Raspberry Pi 3: Serves as the core computing platform for running the facial recognition algorithms and controlling the access mechanism.

2. Raspberry Pi Camera Module v2: Captures live video feed for facial detection and recognition processes. Its high resolution and compatibility with Raspberry Pi make it ideal for this application.

3. Relay Module 2 Channel (5V): Controls the solenoid lock mechanism based on the recognition results obtained from the facial recognition module. It interfaces with the Raspberry Pi GPIO pins to actuate the lock.

4. Solenoid Lock (12V): Secures the door and controls access based on the recognition results. The solenoid lock is engaged or disengaged by the relay module under the control of the Raspberry Pi.

5. Jumper Wires: Provide electrical connections between the Raspberry Pi, relay module, solenoid lock, and other components, ensuring proper signal transmission and power distribution.

6. Micro SD Card: Stores the operating system, software libraries, and program code for the Raspberry Pi, facilitating seamless operation of the system.

7. Official Raspberry Pi Power Supply (USB-C Plug): Powers the Raspberry Pi and its peripherals, ensuring stable and reliable operation.

Software:

1. OpenCV (Open Source Computer Vision Library): Used for implementing facial recognition algorithms, facial detection, feature extraction, and recognition tasks. OpenCV provides robust functionalities for image processing and computer vision tasks, making it suitable for real-time facial recognition applications.

2. Python: Chosen as the primary programming language for its simplicity, versatility, and compatibility with Raspberry Pi. Python facilitates the implementation of facial recognition algorithms, system control logic, and integration with other software components.

3. VNC Viewer: Enables remote access and monitoring of the Raspberry Pi-based system, facilitating configuration, troubleshooting, and maintenance tasks from a remote location. VNC Viewer enhances the accessibility and management capabilities of the system.

Design Principles:

In designing the Face Recognition Door Lock System, key principles are followed to ensure effectiveness, reliability, and seamless integration:

1. Efficiency: The system is designed to efficiently execute facial recognition tasks, minimizing delay in access control decisions.

2. Compatibility: Strict adherence to compatibility standards ensures seamless integration with Raspberry Pi hardware and peripherals, facilitating easy deployment and scalability.

3. Machine Learning Integration: Leveraging machine learning algorithms implemented with OpenCV to train and deploy the facial recognition model, enabling accurate identification of authorized individuals.

Modular Design Approach:

The system architecture follows a modular approach, dividing the functionality into distinct modules:

1. Facial Recognition Module: Implements machine learning algorithms for facial detection, feature extraction, and recognition using OpenCV.

2. Access Control Module: Controls the relay module to actuate the solenoid lock based on the recognition results obtained from the facial recognition module.

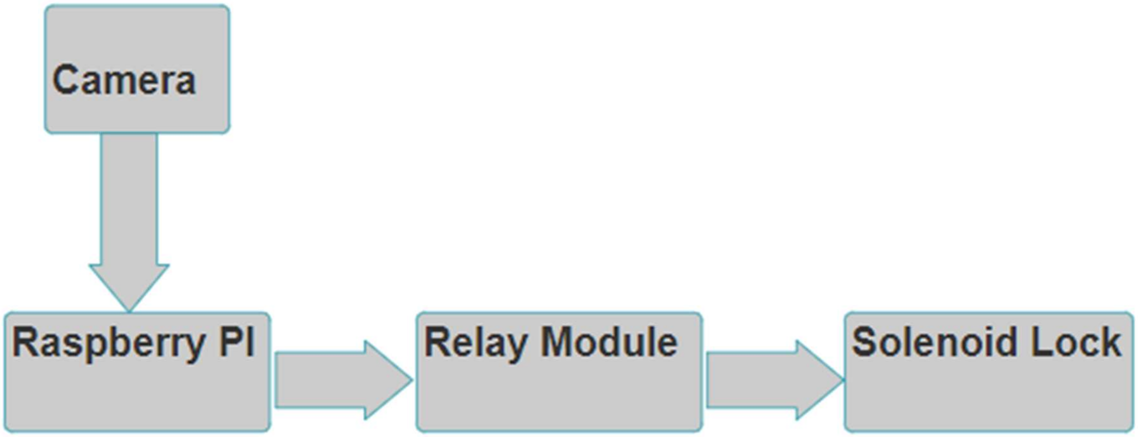

Figure 1: Block diagram of the system

Hardware and Software Description:

Python is chosen as the primary programming language for its versatility and compatibility with the Raspberry Pi platform. OpenCV is utilized for implementing facial recognition algorithms and image processing tasks. VNC Viewer software facilitates remote access and monitoring of the system. These software components are integrated with the hardware components to realize the Face Recognition Door Lock System.

By adhering to these design principles and methodologies, the goal is to develop a robust and reliable system that enhances security and access control in various environments, leveraging the capabilities of Raspberry Pi, OpenCV, and VNC Viewer.

Synthesis and Simulation:

The synthesis and simulation steps are crucial for validating the system design and preparing it for deployment:

Synthesis: Using Python development tools and Raspberry Pi SDK to convert the codebase into executable binaries, ensuring compatibility with Raspberry Pi hardware.

Simulation: Conducting thorough simulations to verify the functionality of the system under various scenarios, ensuring accuracy and reliability of the facial recognition and access control processes.

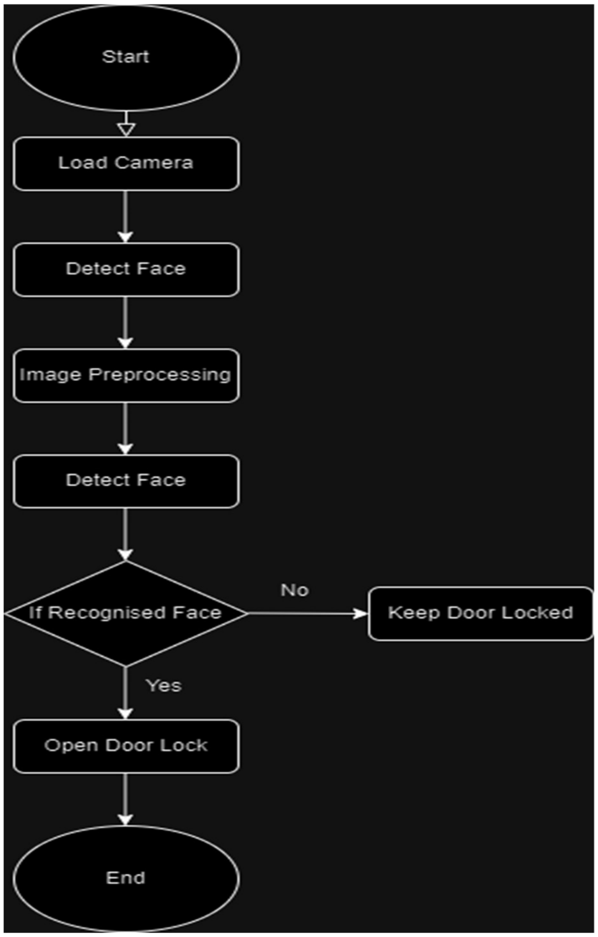

Figure 2: Flowchart of the system

Testing:

The testing phase is pivotal for verifying the functionality and correctness of the system design:

Scenario Testing: Simulating various scenarios to verify the system's response to different lighting conditions, facial poses, and environmental factors, ensuring robust performance in real-world scenarios.

Performance Metrics:

Performance metrics are established to quantitatively assess the effectiveness and efficiency of the system:

Speed: Evaluating the system's response time in processing facial recognition tasks and actuating the solenoid lock, ensuring minimal delay in granting access to authorized individuals.

Accuracy: Measuring the system's accuracy in recognizing authorized individuals and rejecting unauthorized individuals, ensuring reliable access control.

Resource Utilization: Assessing the efficient use of Raspberry Pi hardware resources, including CPU and memory, to optimize for performance and scalability.

Optimization:

The system undergoes iterative optimization to enhance performance and efficiency:

Algorithm Optimization: Fine-tuning machine learning algorithms and facial recognition models to improve accuracy and speed, ensuring reliable recognition of authorized individuals.

Resource Optimization: Optimizing resource utilization to ensure efficient use of Raspberry Pi hardware resources and minimize power consumption, maximizing system performance and reliability.

EXPECTED RESULTS

Upon successful implementation and deployment of the Raspberry Pi-based Face Recognition Door Lock System, the following outcomes are anticipated:

1. Accurate Facial Recognition: The system is expected to accurately detect and recognize authorized individuals based on their facial features, minimizing false positives and false negatives.

2. Efficient Access Control: Authorized users should experience seamless and swift access to the secured area, with minimal delay between facial recognition and door unlocking.

3. Improved Security: By replacing traditional key-based or keypad-based door locks with a facial recognition-based system, the overall security of the premises is expected to be significantly enhanced. Unauthorized access attempts should be effectively thwarted, reducing the risk of security breaches.

4. Convenience and User Experience: The system aims to provide a user-friendly experience, allowing authorized individuals to access the secured area without the need for physical keys or passcodes. This enhances convenience and reduces the likelihood of user errors or security vulnerabilities associated with traditional access control mechanisms.

5. Scalability and Adaptability: The modular design approach and use of open-source software libraries such as OpenCV ensure that the system is highly scalable and adaptable to different environments and use cases. As the need arises, additional functionalities or security features can be integrated into the system without significant architectural changes.

6. Reliability and Stability: The system is expected to demonstrate robustness and stability in its operation, with minimal downtime or system failures. Proper testing and validation procedures are conducted to ensure that the system performs reliably under various conditions, including changes in lighting, facial poses, and environmental factors.

CONCLUSION

In conclusion, the development of the Raspberry Pi-based Face Recognition Door Lock System represents a significant advancement in access control technology, offering a modern and efficient solution to enhance security in various environments. Through the integration of machine learning algorithms, facilitated by OpenCV, and the versatility of the Raspberry Pi platform, the system achieves accurate and reliable facial recognition capabilities, mitigating the vulnerabilities associated with traditional key-based or keypad-based door locks.

The proposed system not only improves security by preventing unauthorized access but also enhances user experience by eliminating the need for physical keys or passcodes, the system provides convenience and accessibility for authorized individuals while maintaining robust security measures.

The modular design approach ensures scalability and adaptability, allowing for easy integration of additional functionalities or security features as needed. Moreover, the system's reliability and stability are upheld through rigorous testing and validation procedures, ensuring consistent performance under diverse conditions.

Overall, the Raspberry Pi-based Face Recognition Door Lock System presents a compelling solution to the evolving security challenges faced by residential, commercial, and institutional settings. Its successful implementation promises to enhance security, streamline access control processes, and provide peace of mind for users, making it a valuable addition to any security infrastructure.

REFERENCES

[1] M. Alshar'e, M. R. Al Nasar, R. Kumar, M. Sharma, Prof. D. Dharamvir, and V. Tripathi, "A Face Recognition Method In Machine Learning (ML) For Enhancing Security In Smart Home," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Muscat, Oman, Dubai, UAE, and Noida, India, 2022, pp. 1081-1084. https://doi.org/10.1109/ICACITE53722.2022.9823833.

[2] A. Jha, R. Bulbule, N. Nagrale, T. Belambe, "Raspberry Pi-Powered Door Lock with Facial Recognition," 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), 2024, pp. 1-6. DOI: 10.1109/SCEECS61402.2024.10481920.

[3] A. D. Singh, B. S. Jangra, R. Singh, "Face Recognition Door Lock System Using Raspberry PI," 2022 International Journal for Research in Applied Science & Engineering Technology (IJRASET), vol. 10, no. V, May 2022. Available: https://doi.org/10.22214/ijraset.2022.42663.

[4] F. N. Nwukor, "Face Recognition Door Lock System Using Raspberry Pi," 2022 Global Scientific Journal (GSJ), vol. 10, no. 8, pp. 1390-1393, Aug. 2022. Available: www.globalscientificjournal.com.

[5] D. G. Padhan, M. Divya, S. N. Varma, S. Manasa, V. C., and B. Pakkiraiah, "Home Security System Based On Facial Recognition," 2023 IEEE 3rd International Conference on Sustainable Energy and Future Electric Transportation (SEFET), 2023, pp. 979-8-3503-1997-2/23/$31.00 ©2023 IEEE, DOI: 10.1109/SEFET57834.2023.10244798.