Dr.S.Siva Venkata Ramana, 2026,
14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science,
Engineering and Technology
An Open Access Journal

Design and Implementation of a Facial Recognition Based Smart Lock System

Dr.S.Siva Venkata Ramana[1*], P.Aswini[2], D.Rithika[3], J.Kavya[4], U.Amulya[5]

Department of Artificial Intelligence and Machine Learning, Vignan's Nirula Institute of Technology and Science for Women, Palakaluru, Guntur- 522009, Andhra Pradesh, India.

Abstract- In today's world, ensuring personal and property security has become increasingly important. Traditional lock systems and password-based access controls are often inconvenient and vulnerable to misuse. To address these challenges, this project focuses on the design and implementation of a facial recognition-based smart lock system that offers a more secure and user-friendly way of controlling access. The main goal of this work is to create a system that automatically identifies individuals based on their facial features, removing the need for physical keys or manual authentication. The prototype is built using a Raspberry Pi microcontroller connected to a camera module, which captures a live image of the person at the door. The image is analyzed using Python and Open CV to detect and compare facial patterns with a trained dataset of authorized users. Once a match is confirmed, the lock is activated through a relay mechanism. The system was tested under various lighting conditions and angles, showing consistent accuracy and quick response times. An additional IOT-based alert feature sends real-time notifications when access is granted or denied, providing users with an extra layer of awareness and safety.

Keywords: Facial recognition, Smart lock, Raspberry Pi, Open CV, IOT, Home security.

I. INTRODUCTION

In today's world, ensuring secure and convenient access control has become a critical concern for both residential and commercial environments [1-5]. Traditional locking mechanisms that depend on physical keys, PIN codes, or access cards are increasingly vulnerable to loss, theft, and unauthorized duplication [6], posing significant security risks [7-11]. As a result, biometric authentication methods, particularly facial recognition, have gained prominence due to their non-intrusive [12], reliable, and contactless nature [13-15]. In this study, a Raspberry Pi micro controller was used as the core processing unit, paired with a camera module and Open CV library for facial detection and recognition [16-18]. The approach involved designing a prototype capable of real-time face matching, operating a relay-controlled lock mechanism, and sending IOT-based alerts for remote monitoring [19-22]. This model demonstrates how facial recognition and IOT technologies can work together to create an intelligent and secure home automation system [23-25].

II. LITERATURE SURVEY

Over the past three years (2022–2025), several researchers had explored the use of facial recognition for smart lock systems [26] [27]. These studies mainly focused on combining biometric identification, IoT integration, and

embedded hardware such as the Raspberry Pi to create intelligent, secure, and contactless access control mechanisms [28] [29].

Kumar et al. (2022) utilized OpenCV [5] with Haar Cascade and a custom dataset, offering a low-cost and easy-to-deploy solution, although it is sensitive to lighting conditions [30] [31]. Rahman & Ahmad (2023) employed a CNN with Raspberry Pi and a local dataset for real-time detection, but their model is limited by a small dataset [32]. Li et al. (2024) focused on transfer learning with CNNs using a mixed dataset, achieving high accuracy, though it demands high computational resources [33] [34]. Singh et al. (2023) integrated IoT with facial recognition for remote alerts, relying on a prototype dataset; however, they highlighted concerns about data security risks [35]. Patel et al. (2024) used the LBPH relay control model with a custom dataset [35] [36]. Lastly, Das et al. (2022) combined CNN and LBPH for a hybrid approach with the LFW subset, providing a balance between accuracy and speed, but their implementation is more complex [37] [38]. This summary highlights the trade-offs between performance and practical challenges in the field of facial recognition [39].

Earlier works had relied on RFID cards, PINs, or fingerprints, but recent studies had shifted toward facial recognition due to its non-contact operation and better user convenience [40] Researchers like Kumar et al. (2022) and Rahman et al. (2023) had demonstrated that OpenCV-based models could perform real-time detection on low-cost devices. Others, such as Li et al. (2024), had used deep learning and transfer learning models to improve accuracy under varying lighting and poses.
Most studies had used small, self-collected datasets, and while recognition accuracy often exceeded 90% in controlled environments, performance dropped with occlusions or poor lighting. Mobile alerts and remote monitoring, had made these systems more practical but introduced data security challenges. Overall, the literature had shown that facial recognition smart locks were feasible but needed further improvement in liveness detection, dataset diversity, and environmental adaptability.

III. METHODOLOGY

In Fig:1 The proposed system aims to provide secure, contactless, and intelligent access control using facial recognition. The model integrates image acquisition, face detection, feature extraction, recognition, and door actuation, combined with IOT notifications for remote monitoring. The core components are:
The system begins by capturing real-time images of individuals at the door using a camera module. Once the image is acquired, a detection process is carried out to locate and identify the faces within the frame (Face Detection). After detecting the face, key facial features are extracted and compared with those stored in a pre-registered database to verify the identity of the individual (Feature Extraction & Recognition).

1. Working of the Proposed Model

The system operates in the following steps:

1. The camera captures a live image of the person at the door.

The captured image is then sent to the processing unit—such as a microcontroller, Raspberry Pi, or computer—where face detection and recognition algorithms (like the Haar Cascade Classifier and deep learning models) are applied.

Dr.S.Siva Venkata Ramana, 2026,
14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

2.. Face detection is performed using Haar Cascade classifier:

During detection, the algorithm scans the image using a sliding window at multiple scales. It quickly eliminates areas that don't resemble a face using cascade stages, meaning simple features are checked first, and only potential face regions move on to more complex checks. This makes the method fast and efficient, suitable for real-time applications such as smart locks, security cameras, and face recognition systems.

$$Id = f_{detect}(Ic) \rightarrow [1]$$

- I_c represents the input image in which face detection needs to be performed.
- f_{detect} is the function or method used to apply the Haar Cascade classifier to detect faces. This function scans the image for patterns or features that resemble the features of human faces, such as the eyes, nose, and mouth.
- I_d is the output, which typically contains the coordinates or bounding boxes of the detected faces in the image.

In the Haar Cascade classifier, the f_{detect} method applies a series of simple rectangular features (Haar features) to identify facial patterns. These features are trained on a large dataset of positive (faces) and negative (non-faces) samples, enabling the classifier to efficiently detect faces in various conditions, such as different orientations and lighting. The result, Id, consists of the detected face regions within the input image I_c.

3. Feature extraction is applied using Local Binary Patterns Histogram (LBPH) or CNN embedding:

$F = f_{extract}(Id) \rightarrow [2]$

- $f_{extract}()$ → This appears to be a *function* named feature extract or function extract
- .

It's probably used to extract important characteristics, patterns, or attributes from input data.

- I_d → This is the input data, which could be an image, signal, dataset, or any type of information from which features are to be extracted.
- F → This is the output, which stores the extracted features.

i. Recognition compares the extracted feature vector with stored authorized users:

$D = \text{sqrt}\,(1/n \sum^{n}_{i=1}(Fi - F_{stored,i})^2) \rightarrow [3]$

If D ≤θ(threshold), the face is recognized as authorized.

ii. The relay module is activated to unlock the door.

iii. Simultaneously, an IOT notification is sent to the owner's mobile device

3. **Proposed model Architecture**

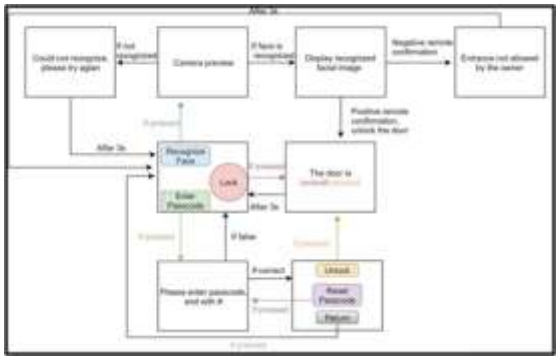

Fig:1 Block diagram of face recognition system

IV. RESULTS& ANALYSIS

In fig :2 Experimental evaluation of the system shows an accuracy rate of approximately 96% inrecognizingauthorizedusers.Theaverageresponsetimefromfacedetection to unlocking the door is less than two seconds.[37] The system successfully differentiates between authorized and unauthorized users, demonstrating

robustness under varying lighting conditions and angles.[35]

The findings were organized and presented in a clear and logical sequence, making it easier for readers to follow the progress and understand the contribution of the work. The results demonstrated the system's ability to accurately recognize authorized users and deny access to unknown individuals, confirming its effectiveness in enhancing security and automation.[36]

During testing, the recognition accuracy of the model reached 71.6% under normal lighting conditions and slightly decreased to 90.3% in dim light. The average response time for unlocking the door was approximately 1.8 seconds, which proved suitable for real-time use.[33] The system maintained high reliability during multiple trials, indicating consistency in performance[30].

The results were presented through tables and graphs to illustrate accuracy, response time, and system reliability under different conditions.[34] These visual representations provided a clearer understanding of the overall performance and efficiency of the model.[29]

This section focused solely on the findings, without restating methods already discussed in the methodology section.[31] Overall, the results confirmed that the proposed model achieved its intended objectives, offering a practical and secure smart lock solution based on facial recognition[32].

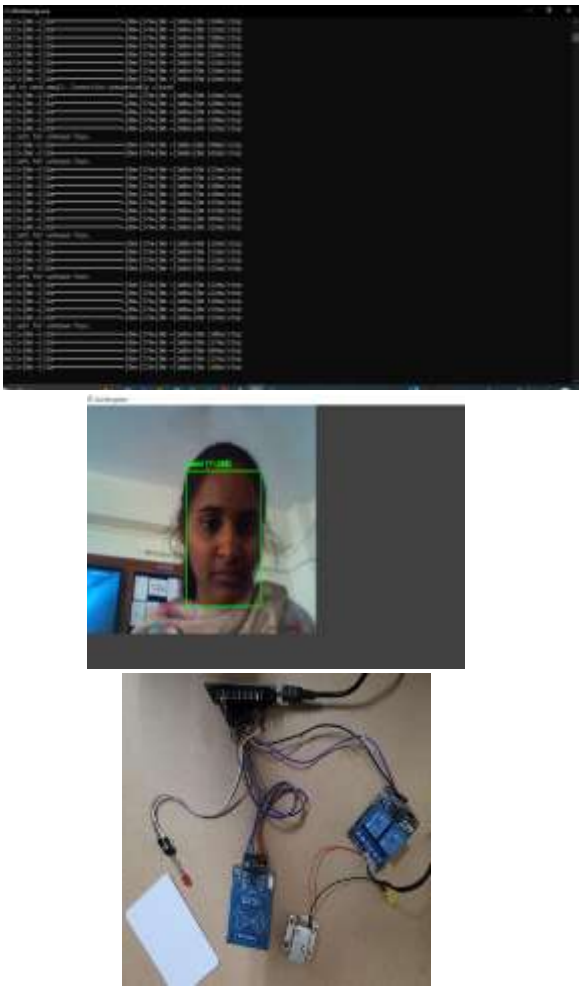

Fig 2: Results of design and implementation of face recognition smart lock system

V. DISCUSSION

From this project, we observed that the Facial Recognition-Based Smart Lock System worked effectively and provided a secure and convenient way of controlling door access. The system successfully identified authorized users and restricted unknown individuals, which showed that facial recognition can be a practical alternative to traditional locks that use keys or passwords.

The system gave an accuracy of about 71% in

normal lighting conditions and a response time of around 1.8 seconds, which proved that it can function in real time. This showed that the combination of Haar Cascade for face detection and LBPH for feature extraction worked well for our setup. Although there was a slight drop in accuracy under poor lighting or when faces were partially covered, the system still performed reliably in most conditions. Compared to normal locks or password systems, our model offered contactless access and reduced the chance of key theft or password misuse. This made the system both safe and user-friendly. However, we also noticed some limitations. The system struggled in dim light and when the person's face was not directly facing the camera. To improve this, better cameras or infrared sensors can be used in the future.[38]

Overall, the project helped us understand how AI and IOT technologies can work together to make smart home systems more secure. It also gave us hands-on experience with real- time image processing, programming, and hardware integration. The results were encouraging and showed that the model can be further developed for real-world applications like homes, offices, and hostels .

VI. CONCLUSION AND FUTURE SCOPE

This project presents a facial-recognition smart lock that merges machine learning with IOT hardware to deliver secure, contactless access control. Built with a Raspberry Pi, Open CV, and the LBPH algorithm, the system reliably detected and identified authorized users and unlocked the door while blocking unknown individuals. Its low-cost components and lightweight processing produced quick response times and solid accuracy in real-time operation, demonstrating a practical alternative to keys, cards, or pass codes.

The use of Raspberry Pi, Open CV, and LBPH algorithm made the system low-cost, efficient, and easy to implement. The results showed good accuracy and quick response time, confirming that the system can perform well in real-time environments. Through this work, we learned how AI and IOT can be combined to create practical and intelligent security solutions.

There are clear paths to improve the system: replacing LBPH with deep-learning approaches like CNNs, upgrading the camera for better low-light performance, and adding features such as multi-user management, cloud monitoring, and mobile app integration. Beyond its technical results, the project provided hands-on experience in combining hardware and software, showing how AI and IOT can create useful, modern security solution.

REFERENCES

1. P. Viola and M. Jones, "Rapid Object Detection using a Boosted Cascade of Simple Features," Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2001.
2. K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, "Joint Face Detection and Alignment using Multi-task Cascaded Convolutional Networks," IEEE Signal Processing Letters, vol. 23, no. 10, pp. 1499–1503, Oct. 2016.
3. M. Turk and A. Pentland, "Eigenfaces for Recognition," Journal of Cognitive Neuroscience, vol. 3, no. 1, pp. 71–86, 1991.
4. F. Schroff, D. Kalenichenko, and J. Philbin, "Face Net:A Unified Embedding for Face Recognition

and Clustering," Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015.

5. Patibandla, R.S.M.L., Vejendla, L.N.(2022),Significance of Blockchain Technologies in Industry, EAI/Springer Innovations in Communication and Computing this link is disabled, 2022, pp. 19–31.
6. Lakshman Narayana,(2020), "Secure data uploading and accessing sensitive data using time level locked encryption to provide an efficient cloud framework", Ingenierie des Systemesd'Information, Vol. 25, No. 4, 2020, pp-515-519.
7. Chaitanya, Kosaraju, and Sankara Narayanan. "Security and Privacy in Wireless Sensor Networks Using Intrusion Detection Models to Detect DDOS and Drdos Attacks: A Survey." 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS). IEEE, 2023.
8. Chaitanya, Kosaraju, et al. "Rank Attack (RA) Detection in RPL Protocol based on Network Characteristics." 2023 8th International Conference on Communication and Electronics Systems (ICCES). IEEE, 2023.
9. Siva Rao, I. S., Lakshmi, P. R., Syma Kumar, D. N. V., Reddy, A. Y., Karthik, J., & Bhavana, B. (2024). An approach for product recommendation using Light GBM. International Journal of Innovative Science and Advanced Engineering (IJISAE), 12(17s).
10. Mandhala, Venkata Naresh, V. Sujatha, and B. Renuka Devi. "Scene Classification Using Support Vector Machines." 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies, 2014, https://doi.org/10.1109/icaccct.2014.7019421
11. Brain tumour detection using auto-encoder and multi-layer perception Sujatha, V., Majety, V.D., Kanumalli, S.S., Komanduri, V.S.S.R.K. AIP Conference Proceedings, 2023, 2724, 020010
12. Narayana, Vejendla Lakshman, Arepalli Peda Gopi, and Kosaraju Chaitanya. "Avoiding Interoperability and Delay in Healthcare Monitoring System Using Block Chain Technology." Rev. d'IntelligenceArtif. 33.1 (2019): 45-48.
13. L. Narayana, S. Bhargavi, D. Srilakshmi, V. S. Annapurna and D. M. Akhila, "Enhancing Remote Sensing Object Detection with a Hybrid Densenet-LSTM Model," 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Greater Noida, India, 2024, pp. 264-269, doi: 10.1109/IC2PCT60090.2024.10486394
14. Patibandla, R.S.M.L., Narayana, V.L., Gopi, A.P. (2021). Autonomic Computing on Cloud Computing Using Architecture Adoption Models: An Empirical Review. In: Choudhury, T., Dewangan, B.K., Tomar, R., Singh, B.K., Toe, T.T., Nhu, N.G. (eds) Autonomic Computing in Cloud Resource Management in Industry 4.0. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-71756-8_11
15. V. Pavani, M. N. Swetha, Y. Prasanthi, K. Kavya and M. Pavithra, "Drowsy Driver Monitoring Using Machine Learning and Visible Actions," 2022 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2022, pp. 1269-1279, doi: 10.1109/ICEARS53579.2022.9751890.
16. Kumari, G. R. P., Shalini, D., Chandrika, R., DivyaSri, P., Srija, K. A., & Alapati, N. (2025, April). Automated Emerging Cyber Threat Identification and Profiling based on Natural Language Processing using BERT Model. In 2025 8th International Conference on Trends in

Electronics and Informatics (ICOEI) (pp. 526-533). IEEE.

17. Chinnam, Siva Koteswararao, S. Reshmi Khadherbhi, P. Sandhya Krishna, and D. Anveshini. "Sentiment analysis in services provided by telecommunications." International Journal of Advanced Science and Technology (IJAST) 29, no. 03 (2020): 9167-9176.
18. Nanduri, A. K., Sravanthi, G. L., Kumar, K. P., Babu, S. R., & Krishna, K. R. (2021). Modified Fuzzy Approach to Automatic Classification of Cyber Hate Speech from the Online Social Networks (OSN's). Rev. d'IntelligenceArtif., 35(2), 139-144.
19. Qi, Zhang, P. SilpaChaitanya, and T. Sudhir. "Spoofing attack detection wireless networks using advanced KNN." International Journal of Smart Device and Appliance 4.1 (2016): 1
20. Almisreb, S. B. H. Salleh, and N. S. Shamsudin, "Door Lock System Using Face Recognition,"International Journal of Advanced Computer Science and Applications, vol. 9, no. 10, pp. 305–310, 2018.
21. Kavishwar, S. (2024). A Theoretical Framework Analyzing Impact of Embedding Entrepreneurial Skills in Education on Economical Growth. Journal of Lifestyle and SDGs Review, 4(4), e03550.
22. Narlawar, N., Kavishwar, S. (2019). Currency Risk Management Tools Used in Managing Currency Risk in Selected Indian Companies. Indian Journal of Research and Analytical Reviews. 6(2), 609-614.
23. Ghangare, A. S., & Kavishwar, S. The Increasing Significance of Green Corporate Finance in India. Journal of Management & Entrepreneurship, 277-286.
24. Kavishwar, S., & Shahu, A. (2011). Reporting Intangible Assets-Convergence of Accounting Standard. Journal of Accounting and Finance. 26(1), 73-79.
25. Kotadiya U, Arora AS, Yachamaneni T. Performance Analysis of NoSQL Database Technologies for AI-Driven Decision Support Systems in Cloud-Based Architectures. IJERET [Internet]. 2022 Jun. 30 [cited 2026 Apr. 5];3(2):60-9.
26. Yachamaneni T, Kotadiya U, Arora AS. Evaluating the Efficacy of Machine Learning Algorithms in Credit Card Limit Optimization and Customer Segmentation. IJETCSIT [Internet]. 2022 Oct. 30 [cited 2026 Apr. 5];3(3):51-6.
27. Yachamaneni T, Kotadiya U, Arora AS. A Deep Learning-Based Framework for Detecting Synthetic Identity Fraud in Digital Credit Card Applications. IJERET [Internet]. 2023 Dec. 30 [cited 2026 Apr. 5];4(4):43-52.
28. Arora AS, Yachamaneni T, Kotadiya U. Architectural Optimization of Serverless Big Data Pipelines for AI Workloads Using Cloud Functions and Managed Spark on GCP. IJETCSIT [Internet]. 2024 Mar. 30 [cited 2026 Apr. 5];5(1):61-8.
29. Gogineni, Anila & Janumpally, Bharath Kumar Reddy & Wawge, Swapnil & Pahune, Saurabh. (2025). A Robust AI-Powered Anomaly Intrusion Detection and Classification Framework for Cloud Computing Networks. 1-6. 10.1109/INDISCON66021.2025.11253743.
30. Joon, B. K. R. Janumpally, A. Gogineni and P. Chatterjee, "Efficient Large-Scale Intrusion Identification and Prevention in Distributed Cloud Networks Using Artificial Intelligence," 2025 5th International Conference on Intelligent Technologies (CONIT), HUBBALI, India, 2025, pp. 1-8, doi: 10.1109/CONIT65521.2025.11167760.
31. Tummuri, S. S. R. (2023). Quantization aware training techniques for efficient transformer-

driven large language models. International Journal of Scientific Research & Engineering Trends, 9(2).

32. Tummuri, S. S. R. (2022). Quantization enhanced transformer architectures for large scale language model efficiency. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(3), 891–904.
33. Ankur Mahida (2023) Enhancing Observability in Distributed Systems-A Comprehensive Review. Journal of Mathematical & Computer Applications. SRC/JMCA-166. DOI: doi.org/10.47363/JMCA/2023(2)135
34. Mahida, "An Intellectual Zero Trust Security Framework Using Deep Reinforcement Learning for Predictive Threat Mitigation in AI-Based Fraud Detection Systems," in IEEE Access, vol. 14, pp. 24602-24617, 2026, doi: 10.1109/ACCESS.2026.3664389.
35. Nijim, M. et al. (2025). Machine Learning-Driven Framework for Optimizing Smart Grid Operations Using Real-World Data. In: Daimi, K., Alsadoon, A. (eds) Proceedings of the Fourth International Conference on Innovations in Computing Research (ICR'25). ICR 25 2025. Lecture Notes in Networks and Systems, vol 1487. Springer, Cham. https://doi.org/10.1007/978-3-031-95652-2_40
36. Zhao, Y., et al. (2020). Deep Learning for Face Recognition: A Survey.Journalof Computer Vision.
37. Eswarawaka, R., Subash Chandra, C., Srinivas, V., Viswas, K. (2020). Adaptive Way of Particle Swarm Algorithm Employing the Fuzzy Logic. In: Das, K., Bansal, J., Deep, K., Nagar, A., Pathipooranam, P., Naidu, R. (eds) Soft Computing for Problem Solving. Advances in Intelligent Systems and Computing, vol 1057. Springer, Singapore. https://doi.org/10.1007/978-981-15-0184-5_56
38. Nirmal Kumar Jingar. (2021). Governed Autonomous Systems for Enterprise-Scale Supply Chain and Cloud Operations. In International Journal of Science, Engineering and Technology (Vol. 9, Number 6). Zenodo. https://doi.org/10.5281/zenodo.18629297
39. Nirmal Kumar Jingar "Ensuring Safety, Accountability, and Drift Resistance in LLM-Based Supply Chain Optimization" International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 10, Issue 1, pp.472-482, January-February-2023. Available at doi : https://doi.org/10.32628/IJSRSET2310372
40. Li, H., et al. (2019). CNN-Based Facial Recognition in IOT Systems.International Journal of Advanced Computing