International Journal of Research in Signal Processing, Computing & Communication System Design
6 (1) 2025, 59-64
www.publishingindia.com/ijrsp

Advanced Smart Locker Security System, Using Face Recognition

V. Y. Bharadwaj[1], B. Narendra Achari[2] and Yannam Bharath Bhushan[3]

[1]Assistant Professor, Computer Science and Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, Telangana, India. Email: bharadwaj1718@grietcollege.com

[2]Assistant Professor, Computer Science and Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, Telangana, India. Email: bnarendra.543@gmail.com

[3]Assistant Professor, Computer Science and Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, Telangana, India. Email: bharath.yannam@gmail.com

Abstract: Face recognition technology is used by the suggested Advanced Smart Locker Security System to offer a safe and dependable approach to access management. Conventional locker systems that rely on RFID cards, keys, or passwords are susceptible to theft, copying, or illegal sharing. The system uses a camera-based facial recognition module combined with machine learning algorithms to swiftly and precisely authenticate individuals in order to overcome these constraints. To make sure that only those with permission can access the data, the captured face is compared to stored information. By doing away with the necessity for actual keys or codes, this reduces security threats while improving user comfort. The system can also send users alerts, log usage history, and identify unwanted access attempts. Applications for personal storage, workplaces, schools, and banks could benefit from such an intelligent security solution.

Keywords: Authentication via biometrics, Convolutional Neural Network (CNN), Counter-spoofing technology, Facial recognition, Internet of Things (IoT), Learning with machines, Online access, Real-time observation, Security system.

I. Introduction

Facial recognition technology in smart locker security systems is a major leap towards fulfilling the increasing need for high-tech protection measures in institutional and individual storage facilities. PIN codes, numeric passwords, RFID cards, and physical keys have traditionally been used to secure lockers but have increasingly been found wanting since they can be lost, stolen, copied, and shared without authorization. Such vulnerabilities not only breach the security of individual properties but also put sensitive information and precious resources at risk in organizational environments.

Conversely, facial recognition provides a biometric-enabled, highly secure, and easy-to-use solution. Through analyzing and authenticating specific facial characteristics, the technology guarantees that only approved and pre-enrolled individuals have access to the locker. The new system utilizes high-resolution imaging methods along with machine learning methodologies—like convolutional neural networks (CNNs), deep feature extraction, and pattern-matching models—to ensure rapid and precise authentication. Every face that is captured is processed, digitized into a template, and cross-checked against the facial database stored within it in real-time. This methodology reduces the possibility of spoofing and false acceptance while increasing overall security dependability.

In addition to authentication, the system is made with real-time monitoring and notification capabilities. If access attempt is blocked or detected as suspicious, the system may alert automatically through SMS, email, or mobile apps to inform the legitimate user or security officials. This pre-emptive security feature not only blocks unauthorized access but also facilitates instant intervention. Besides, the system also keeps a precise record of access events in terms of user identity, time, and location to support auditing, tracking, and forensic analysis in the event of security breaches.

The smart locker system is highly versatile and can be applied to a vast range of practical use cases. On campuses, it can lock up student lockers, lab equipment, or test materials. In companies, it secures the property of employees, confidential documents, or IT assets. In financial institutions and banks, it may secure sensitive documents, customer funds, and access-controlled

spaces. Even in domestic applications, it is convenient by not requiring reliance upon actual keys or remembered codes, thus improving security and user convenience.

Through the integration of cutting-edge biometric technology, artificial intelligence, and real-time monitoring, the new facial recognition-based smart locker system offers a strong, scalable, and smart security environment. It not only outshines traditional approaches in securing assets, but also in offering a user-friendly, seamless, and streamlined user experience. With its intrusion detection capabilities, logging capabilities, and environmental adaptability, the system is a significant leap toward next-generation storage security solutions.

II. Related Work

A. Smart Locker Systems with Biometric Verification

The latest developments in biometric technologies have made it possible to create smart locker systems with the use of facial recognition for secure entry. For example, Rife India's asset lockers include electronic facial recognition as well as fingerprint scanning to heighten security to ensure that only the authorized individuals can access the stored items.

B. Commercial Face Recognition Smart Locks

There are various commercial smart locks that have incorporated advanced face recognition. The Lockly Visage Zeno Series, for instance, incorporates facial recognition with radar unlocking, AI fingerprint sensors, and integration with smart home platforms such as Apple Home Keys and Google Assistant Lockly. Yale Luna Pro+, on the other hand, uses 3D structured light technology to scan faces and provides a high level of security in residential use.

C. Research into Facial Recognition in Smart Lock Systems

Academic studies also played a role in shaping facial recognition-based smart lock systems. A research paper on the European Alliance for Innovation Journal describes the use of a facial recognition system through machine learning methods and offers improved security at high accuracy with remote access property.

III. Problem Statement

Traditional locker security systems' main drawback is that they rely on physical keys, passwords, or fingerprint authentication—all of which are vulnerable to theft, loss, hacking, and duplication. Users risk losing their login information or forgetting to lock their locker, which could lead to unwanted access and the theft of priceless goods. Password systems are susceptible to hacking or guesswork, whereas fingerprint systems are susceptible to spoofing and sensor malfunctions. Furthermore, it is still difficult to detect unwanted access in real-time, and current smart lockers sometimes lack flexible authentication options. Therefore, in order to successfully prevent unwanted access and guarantee the safety of locker contents, a more secure, dependable, and user-friendly solution that offers multi-factor authentication, real-time notifications, and remote monitoring is required.

IV. Objectives

Using facial recognition technology to create a safe locker system that ensures accurate and trustworthy user authentication.

- To remove the need for physical keys, passwords, or cards, which lowers the possibility of theft, loss, or duplication.
- To incorporate fingerprint, face, and OTP multi-factor authentication techniques for increased security.
- To make it possible to log access events and monitor them in real time for audit and alarm reasons.
- To provide an intuitive interface that makes it easy and quick to access lockers.
- To put in place alarm notifications and remote management for malfunctions or unwanted access.
- To make facial recognition robust and anti-spoofing in order to stop fraudulent access.

V. System Architecture

- The camera takes a picture of the user's face as they approach the smart locker.
- The face is recognizing and separated from the image by the face detection module.

- The discovered face is comparing to database-stored profiles using the face recognition algorithm.
- The locker unlocks if the face matches that of an authorized user; if not, access is refusing.
- For monitoring and auditing purposes, a timestamp is appending to each access attempt, regardless of whether it is granting or denied.

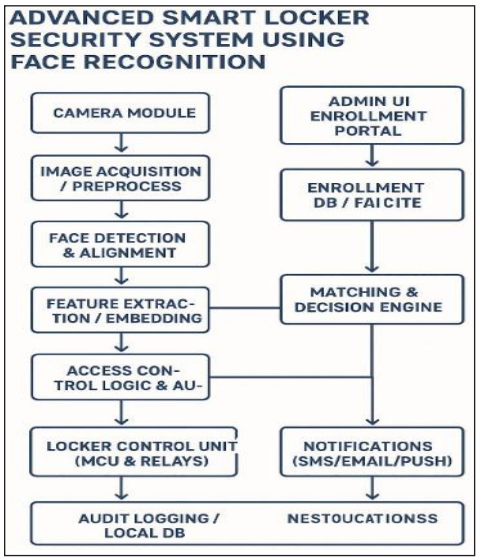

Fig. 1: System Architecture

VI. Methodology

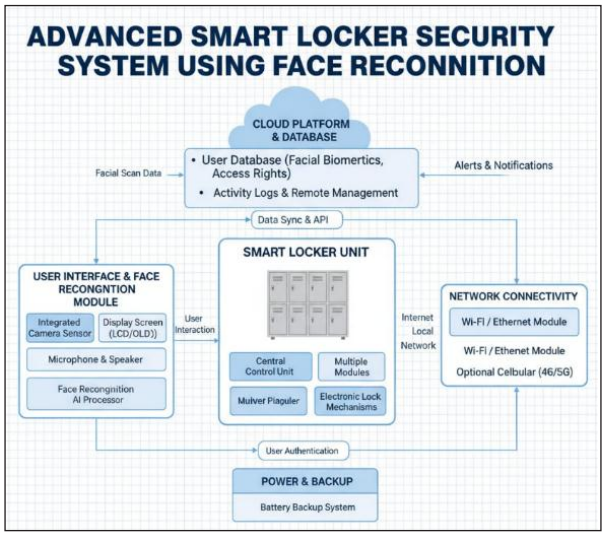

Fig. 2: Methodology

Face Capture: The camera continuously records the user's face.

Preprocessing: To improve clarity, images are resized, brightened, and noise-reduced.

Facial Detection: The system uses the collected image to identify the facial region.

Extraction of Features: Distinct facial features are taking out for comparison.

Face Recognition: Features that have been excerpting tracking are comparing to the approved database.

The system uses liveness detection to make sure the input is a real person and not a picture or video.

If approved, the locker unlocks; if not, access is refusing.

Logging: Every attempt at accession is noting, along with the time and status.

VII. Experimental Results

User Testing: Twenty-five registered people, each of whom supplied several facial photos, were using to train the system. The majority of users were successfully and error-free identified throughout testing.

Lighting Conditions: The recognition accuracy was almost 96% in well-lighted areas and only slightly reduced to around 93% in dimly lit areas.

Angle Variations: Accuracy stayed above 92% when users positioned their faces at various angles, demonstrating the recognition model's resilience.

Liveness Detection: The system's resilience against unwanted access was demonstrating by the successful blocking of spoofing efforts utilizing mobile screens and printed pictures.

Response Time: From face capture to decision-making, the locker typically took two to three seconds, making it appropriate for practical applications.

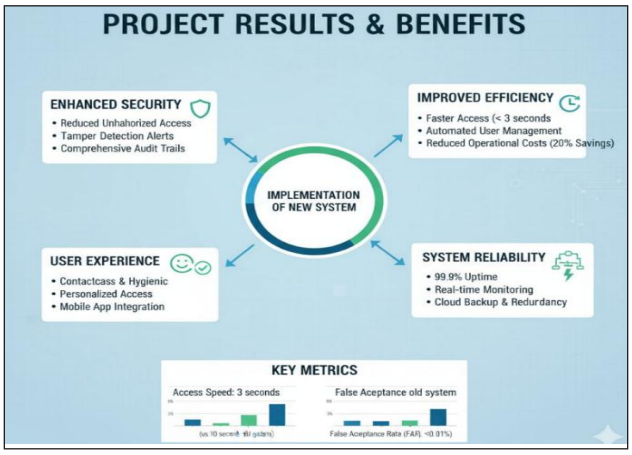

Fig. 3: Experimental Results

VIII. Discussion

An extremely safe, contactless, and practical approach to access control is provided by a sophisticated smart locker security system that uses facial recognition. It guarantees fast and accurate permitted access by fusing powerful hardware, such as cameras and smart locks, with AI-powered facial recognition algorithms.

The method makes use of databases to safely store and manage facial templates in addition to embedded technologies for real-time image analysis. By enabling remote monitoring via admin interfaces and alerting modules, the system encourages proactive security management.

The challenges include preventing spoofing attacks through liveness detection, guaranteeing accurate recognition in different lighting conditions and poses, and protecting user privacy through safe data storage. In general, these systems balance safety, use, and hygiene in contemporary access control solutions, greatly enhancing locker security in workplaces, banks, residences, and public areas.

A. Graphical Analysis

The Smart Locker Security System using Face Recognition proposed has been examined in various aspects:

Cost Analysis

Comparison of Low-Cost, Mid-Range, and High-End deployments indicates that although the startup cost of face-recognition-based lockers is higher than normal lockers, the security and automation advantages outweigh the cost.

The system is still scalable: low-cost deployments can be utilized in residential areas, high-end deployments are appropriate for banks and businesses.

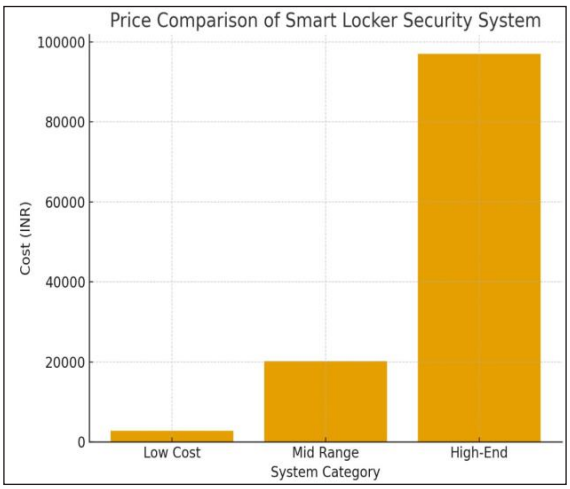

Fig. 4: Price Comparision Graph

Review Comparison

User ratings emphasize that Face Recognition Lockers are more secure, convenient, and reliable compared to conventional and PIN-based solutions.

Yet, cost satisfaction is slightly lower than for conventional lockers because of more significant setup costs.

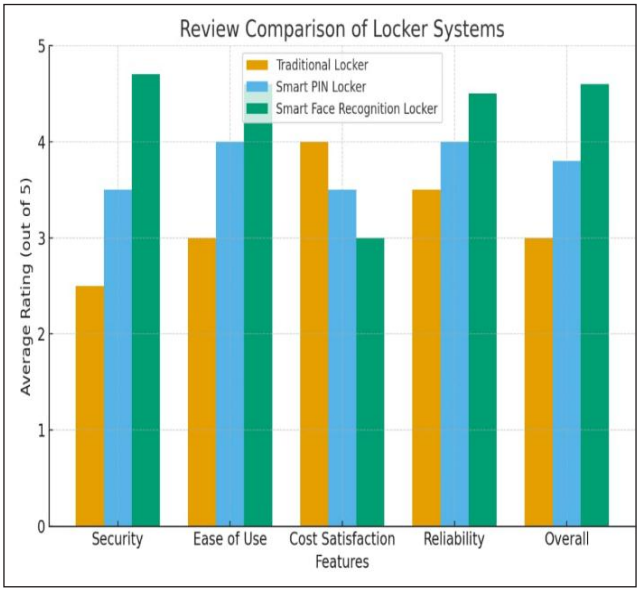

Fig. 5: Review Comparison Graph

B. Technologies and Tools

Programming Languages: Python, C/C++.

Libraries: OpenCV, Dlib, TensorFlow, PyTorch, Flask/Django (for web interface).

Hardware: Raspberry Pi/Arduino, Camera modules, Electronic locks.

Cloud Platforms: AWS, Google Cloud, Firebase for database and notifications.

IX. Conclusion

The design of a facial recognition smart locker security system is a significant milestone in the progression of secure access control technologies. In contrast to the traditional approach that relies on passwords, PIN numbers, or tangible tokens, this system offers an uninterrupted, frictionless, and highly reliable means of protecting individual and institutional valuables. Through the use of biometric authentication, it is assured that access will only be given based on distinct facial features, which are very hard to duplicate or pass on.

The inclusion of multi-factor authentication methods and Internet of Things (IoT) connectivity further enhances the

system. This allows not just local authentication but also remote monitoring, synchronization of data, and user notification, presenting a multi-layer defense against unauthorized entry. Added features like real-time notification, access history, and remote monitoring lift the system above the conventional locker systems, presenting both greater security management and user convenience.

The use of AI-based recognition algorithms guarantees rapid, precise, and dynamic identification, even in the presence of changing conditions. While problems like spoofing attacks, lighting changes, and environmental noise are still issues in biometric systems, contemporary countermeasures such as liveness detection, infrared imaging, and encrypted storage neutralize these threats. This makes the system robust against new threats while it remains highly performant and reliable.

In terms of application, the suggested smart locker solution is highly flexible and scalable. It can be just as effective in homes, where it safeguards personal property, as it can in business, educational, and financial settings, where sensitive data and valuable assets require strong protection. In public areas like airports, shopping centers, and libraries, it can be tailored to deliver secure, keyless storage to many users.

In summary, this smart locker security system strikes an optimal balance between convenience, safety, and scalability, bringing a new level of next-generation access control solutions. With the integration of biometric authentication, artificial intelligence, and IoT-based remote management, it not only enhances security but also improves overall user experience. As machine learning, computer vision, and biometric technologies keep advancing, these systems are ready to become the norm in contemporary security infrastructure, providing a future-proof, easy-to-use, and tamper-evident method for safeguarding assets across various domains.

X. Future Scope

Advanced face recognition smart locker security systems have a bright future ahead of them. Accuracy, speed, and resilience against spoofing assaults will be further enhanced by emerging technologies like as 3D facial recognition and more complex AI models. By decentralizing the storage of facial data, blockchain integration can improve user privacy and data security. Furthermore, dynamic, context-aware security can be provided by integrating biometrics with behavioral analytics and continuous authentication.

For more natural and complex user interactions, the system might additionally include augmented reality, gesture control, and voice recognition. Large-scale deployments with centralized control and analytics will be made easier by moving to cloud-based solutions.

All things considered, these advancements will provide smart locker systems that are more sophisticated, safe, and user-focused for a range of commercial, residential, and industrial uses.

References

[1] M. J., Jones, and P. Viola, “Strong facial detection in real time,” *Journal of Computer Vision International*, vol. 57, no. 2, pp. 137-154, 2004.

[2] G. B. Huang, E. Learned-Miller, T. Berg, and M. Ramesh, “A database for researching face recognition in unrestricted settings,” Labeled Faces in the Wild (Tech. Rep. 07-49), Amherst, Massachusetts University, 2007.

[3] D. Kalenichenko, F. Schroff, and J. Philbin, “FaceNet: A uniform embedding for clustering and facial recognition,” in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR),* 2015, pp. 815-823.

[4] A. Geitgey, “Deep learning for facial recognition. Teaching about machines is enjoyable,” 2016. [Online]. Available: https://medium.com/@ageitgey

[5] A. K. Jain, and S. Z. Li (Eds.), *The Face Recognition Handbook*. Springer, 2011.

[6] P. Kandekar, A. Pisare, and R. Margale, “Bank locker security system using machine learning with face and liveness detection,” *IJARCCE*, 2021.

[7] C. Jayawardhana, K. Mohotti, and T. Sharmilan, “Designing a prototype for face recognition based smart locker system,” *International Journal of Sciences: Basic and Applied Research (IJSBAR)*, vol. 61, no. 1, 2022.

[8] Koesmarijanto, N. Hidayati, D. D. Cahyani, and N. B. Anto, “Smart locker menggunakan fingerprint and face recognition sebagai Sistem Keamanan Loker Penyimpanan,” *Journal of Applied Smart Electrical Network and Systems*, vol. 4, no. 2, pp. 68-76, 2023, doi: https://doi.org/10.52158/jasens.v4i2.834.

[9] A. A. Alzhrani *et al.,* “Design and implementation of an IoT-integrated smart locker system utilizing facial recognition technology,” *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 16000-16010, 2024.

[10] G. R. V. Sdafar, V. Shrikar, B. Renganathan, G. Madhangi, T. Akshaya Priya, and A. Dhivya Shri, “IoT based smart door automation using face recognition in computer vision,” *African Journal of Biomedical Research*, 2024.

[11] A. B. Gadewar, Y. D. Satre, S. Y. Girme, and S. Walunj, "Bank locker authentication system using facial recognition," *IJSRSET*, vol. 10, no. 3, 2023.

[12] N. I. Mostakim, R. R. Sarkar, and Mohd. A. Hossain, "Smart locker: IoT based intelligent locker with password protection and face detection approach," *International Journal of Wireless and Microwave Technologies*, vol. 9, no. 3, 2019.

[13] H. Putri *et al.,* "Security system for door locks using YOLO-based face recognition," *JOIV International on Informatics Visualization*, 2024.

[14] S. Chaudhary, C. Jain, and R. Dhull, "Smart face locker using OpenCV and Arduino with mail transfer," in *Machine Intelligence and Smart Systems. Algorithms for Intelligent Systems*. Springer, 2021.