iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.82757

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Bank Locker Security System with Face and Liveness Detection

Dr. Nikita Kulkarni[1], Prof. Ashwini Kamble[2], Sanket Morde[3], Omkar Somwanshi[4], Aditya Konda[5], Rahul Shingade[6]
[1,2]*Assistant Professor, Department of Computer Engineering*
[3, 4, 5, 6]*K.J. College of Engineering & Management Research, Pune, India*

Abstract: ***This paper proposes a secure bank locker system using face recognition technology with liveness detection to avoid spoofing attacks. In the proposed system, a Convolutional Neural Network (CNN) is used for face recognition to verify the identity of the user. Blink detection and texture analysis are also used to confirm the presence of a live user. The Raspberry Pi is used for the implementation of the electronic lock mechanism.***
Keywords: Face recognition, Liveness detection, Deep learning, LBPH, HAAR CASCADE, CNN, Anti-spoofing.

I. INTRODUCTION

Safeguarding valuables in bank lockers is a top security concern for financial institutions and their customers. Traditional access methods, such as physical keys, passwords, and magnetic cards, can be lost, duplicated, stolen, or misused. More importantly, these methods do not confirm if the person using the credential is the rightful owner of the locker.

Biometric authentication provides a better option by verifying unique human traits. Among the different biometric methods, facial recognition is well-suited for locker systems because it operates without contact, is easy for users, and works with affordable camera technology.

However, standalone face recognition systems can fall victim to presentation attacks. In these attacks, unauthorized people try to gain access using printed photos, recorded videos, or realistic masks. To tackle this problem, liveness detection techniques are added to confirm that a real user is physically present. Research shows that combining texture-based analysis with short-term motion cues, such as eye blinking and subtle facial movements, greatly enhances resistance to spoofing while still being efficient for embedded platforms.

This work suggests a modular and privacy-focused bank locker security system. It integrates deep learning-based facial embeddings with active liveness verification. The system records a short video at the locker, detects and aligns the face, and creates feature embeddings using a Convolutional Neural Network (CNN) for identity checks. At the same time, a liveness module assesses texture and motion traits to confirm authenticity. Access is granted only when both identity and liveness requirements are met.

The entire system runs locally on embedded hardware like a Raspberry Pi that connects to an electronic solenoid lock. Security is strengthened through encrypted local logging, with optional cloud sync for auditing. Experiments on both custom and publicly available datasets show that this solution effectively balances recognition accuracy, spoof resistance, response time, and user privacy. The rest of this paper is organized as follows: Section II problem definition, Section III represents objective, Section IV describes literature review, Section V represents proposed system, Section VI represents system architecture, Section VII describes system workflow, Section VIII advantages of the proposed system, Section IX show methodologies and implementations, Section X discusses result, Section XI conclude and Section XII shows references.

II. PROBLEM DEFINITION

The traditional method of locking and unlocking the bank lockers using physical keys, PIN codes, or basic biological identification methods is no longer safe and secure from the current security attacks and threats. The physical keys may be duplicated, the PIN code may be compromised or guessed, and the traditional facial identification method may be tricked using printed pictures or videos. This makes the system vulnerable to unauthorized access, financial losses, and loss of customer confidence in the security systems employed by the banks.

There is a need to develop an intelligent system that not only authenticates the user identity but also checks the physical presence of the legitimate user holding the bank account. This problem is being addressed in the current study by developing a smart system for the security of the bank lockers using facial identification and liveness detection methods. This would not only improve the level of security but also prevent spoofing attacks during the identification and access control process.

III. OBJECTIVE

The primary aim of this project is to develop a secure and intelligent bank locker system that integrates facial recognition with liveness detection to ensure access is granted only to authenticated and physically present users. The specific objectives are outlined as follows:

To design and implement a robust face recognition module capable of accurately identifying authorized users across varying environmental and lighting conditions. To develop an efficient liveness detection mechanism that distinguishes genuine human presence from spoofing attempts involving photographs, recorded videos, or masks.To seamlessly integrate the recognition and liveness modules with the electronic locking system for real-time and automated authentication.To assess system performance based on recognition accuracy, processing time, False Acceptance Rate (FAR), and False Rejection Rate (FRR).To improve overall locker security and user convenience by replacing traditional key- or PIN-based methods with a smart biometric solution.To establish a scalable and cost-effective framework adaptable to other high-security access control applications.

IV. LITERATURE REVIEW

Face recognition has emerged as one of the most reliable biometric authentication techniques due to its non-intrusive nature and high applicability in security systems. Early work by Li and Jain [1] presented comprehensive foundations of face recognition technologies, covering feature extraction, classification methods, and practical security applications. Their work established the importance of biometric authentication in access control and surveillance systems.

Traditional face detection methods were significantly improved by Viola and Jones [6], who introduced a robust real-time face detection framework using Haar-like features and AdaBoost classifiers. This method became widely adopted because of its computational efficiency and real-time performance. However, traditional approaches faced limitations under varying lighting conditions, pose variations, and spoofing attacks.

To overcome these limitations, deep learning-based techniques were introduced. Zhang et al. [3] proposed the Multitask Cascaded Convolutional Neural Network (MTCNN), which jointly performs face detection and alignment with high accuracy. The approach improved robustness in unconstrained environments and became a standard preprocessing method for modern facial recognition systems.

With the increasing use of facial authentication in security applications, presentation attacks such as printed photos, replay videos, and masks became major concerns. Galbally et al. [8] conducted a detailed survey of biometric anti-spoofing methods and highlighted the vulnerabilities of face recognition systems to spoofing attacks. Their study emphasized the necessity of integrating liveness detection mechanisms into biometric systems.

Further advancements in anti-spoofing were achieved through deep learning techniques. Liu et al. [5] proposed a deep learning framework for face anti-spoofing using auxiliary supervision instead of simple binary classification. Their method improved the detection of spoofing attacks by learning depth and temporal information from facial images. Similarly, George and Marcel [2] utilized convolutional neural networks (CNNs) for presentation attack detection and demonstrated significant improvements in detecting fake facial inputs under diverse attack scenarios.

Recent studies have focused on integrating facial recognition with Internet of Things (IoT) technologies for smart security systems. Patel et al. [4] developed an IoT-based smart locker system that uses facial recognition for authentication. Their system demonstrated enhanced automation and remote monitoring capabilities. Mohanty et al. [7] further improved smart locker security by combining facial recognition with IoT-enabled communication modules, enabling real-time alerts and remote access management.

Deep learning has also contributed to improving the reliability of biometric authentication systems. D'Souza [9] discussed the application of deep learning models in secure biometric systems and highlighted their effectiveness in feature extraction and recognition accuracy. The study emphasized that deep neural networks outperform traditional machine learning methods in large-scale biometric applications.

In addition, Sanderson and Lovell [10] introduced multi-region probabilistic histogram techniques for robust identity inference. Their approach improved recognition accuracy by analyzing multiple facial regions independently, making the system more scalable and resilient to partial occlusions.

V. PROPOSED SYSTEM

In the end, a Bank locker system based on facial recognition fused with liveness check provides a secure and contactless solution. This will require the authorized users to be physically present, thus eliminating the inefficiencies of using key-, PIN-, or single-biometric systems. Security, convenience, and real-time performance remain the focus of the system for practical use in banking environments.

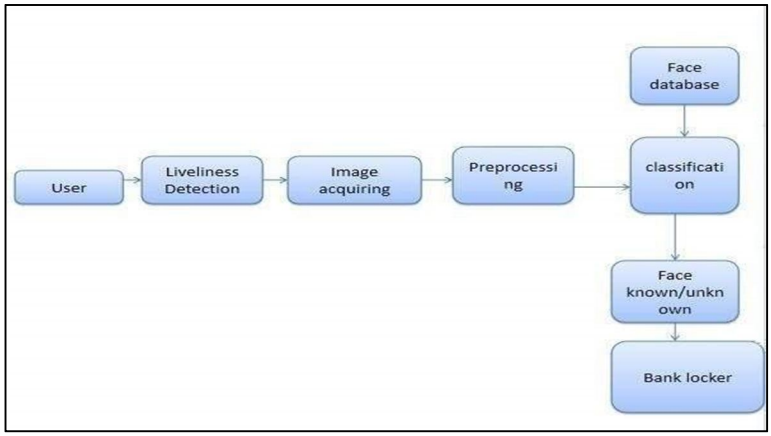
VI. SYSTEM ARCHITECTURE

Its architecture includes three interconnected modules:

1) Face Recognition Module - A camera takes a real-time image of the user's face, which is then processed through a Convolutional Neural Network (CNN) to produce unique feature vectors. These vectors are then matched against a database of enrolled users in a secure manner. It has been made robust against variations in illumination, facial pose, and facial expressions.

2) Liveness Detection Module - To prevent spoofing attempts using printed images, videos, or 3D masks, the liveness module considers behavioral and texture cues. These include checking for eye blinks, detecting facial micro movements, and analyzing motion patterns. Further access processing is only allowed when the system detects a living human face.

3) Locker Control Module - Locker Control Module After the verification of identity and liveness, the control unit activates the electronic solenoid lock to grant access. All failed authentication attempts are logged securely, and security alerts can be optionally initiated to notify the bank staff. The resulting integrated design offers automated and real-time locker control while maintaining high-security intelligence against unauthorized access.



VII. SYSTEM WORKFLOW

The operation of the proposed bank locker security system is done through a clear stepwise procedure of ensuring both identity and liveness confirmation.

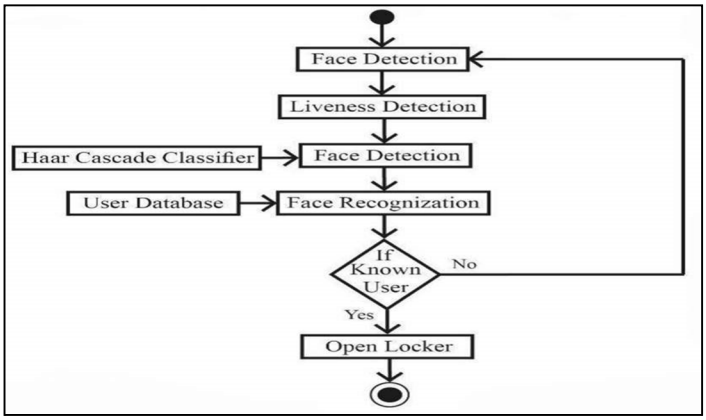
1) User Interaction: The user walks up to the locker and puts their face in front of the camera.

2) Facial Recognition: The system first takes a facial image and then extracts the feature embeddings using a CNN and search the probability against the enrolled user in the database to verify identity.

3) Liveness Verification: At the same time, the liveness detection module assesses behavioral and texture information such as blinking and fine facial movements to verify that the user is physically present.

4) Access Decision: Finally, if the two checks succeed, electronic locks are activated to grant physical access; otherwise, access is denied, the attempt is logged, and optional security alerts are raised for administrative actions.

This workflow guarantees that only live, verified users can operate the locker, thereby providing an access control system that is robust and automated.



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

VIII. METHODOLOGY AND IMPLEMENTATION

The proposed security system for the bank lockers guarantees safe and secure access control using the facial recognition and liveness detection methods. The framework effectively utilizes classical image processing and machine learning methods to improve the accuracy and security of the system against spoofing attacks. The proposed workflow includes four stages in the system implementation.

A. Data Acquisition

Facial images of the users are acquired using a high-resolution camera installed at the terminal of the lockers. Multiple images per user are acquired under varying lighting conditions and with different head poses and facial expressions to improve the accuracy of the system. Additional images, such as printed photos and video replays, are also acquired to improve the liveness detection system.

B. Image Preprocessing

Facial regions are detected using a cascade-based detector that recognizes the important features of the faces in real time. The acquired images are then preprocessed by resizing the images, converting them to grayscale, and normalizing the images to reduce the effect of varying lighting conditions.

C. Feature Extraction and Analysis

The system uses a dual feature approach to perform the recognition task:
Local Binary Pattern Histogram (LBPH): This method is used to extract efficient features for fast comparisons.
Convolutional Neural Network (CNN): This method is used to extract deep spatial features, resulting in compact representations that enhance the accuracy of the system.
The liveness detection module analyzes the minute behavioral and texture changes of the individual in a series of images, including eye blinking, natural head movements, and changes in skin texture. This module uses a CNN classifier to differentiate between a genuine and fake attempt by a user to perform the liveness detection.

D. Hardware Integration and Real-Time Control

After the successful authentication of the individual and their liveness, the microcontroller (Raspberry Pi or Arduino) commands the electronic solenoid lock to allow the individual to pass. In the case of a failed authentication, the system logs the failure and can send security alerts to prevent the individual from entering the system.

E. Performance Evaluation

The system is evaluated using parameters such as the accuracy of the system, False Acceptance Rate (FAR), False Rejection Rate (FRR), and the average response time of the system.

IX. RESULTS AND DISCUSSION

The effectiveness of the proposed security system for bank locker systems was examined under practical working conditions. The results of the experiment are discussed below:

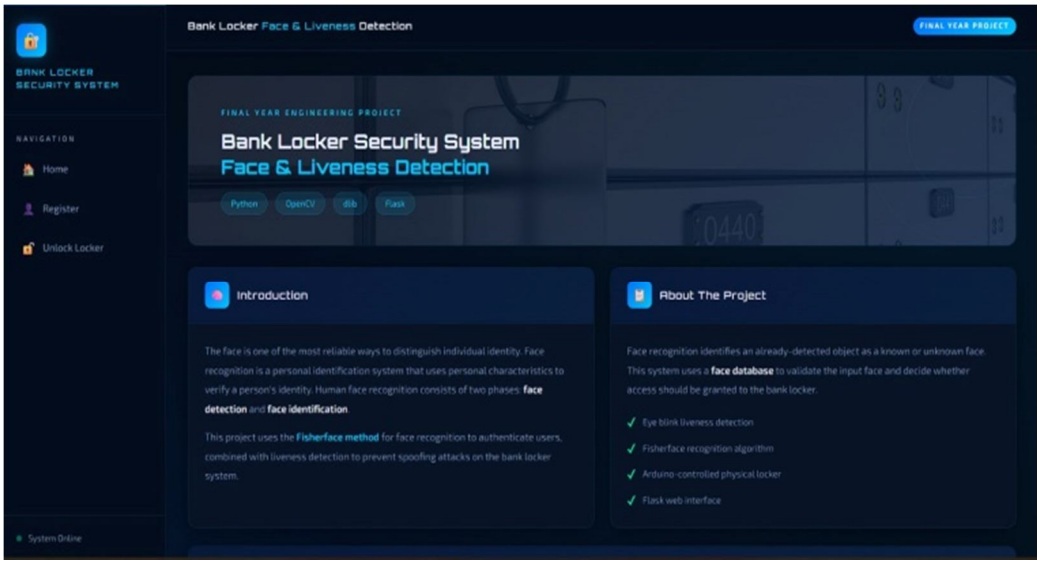
1) User Recognition Accuracy: The facial recognition module was observed to correctly recognize authorized users, even under varying lighting conditions, facial expressions, and head positions. The accuracy of the system was significantly enhanced with the use of deep learning-based feature extraction.
2) Liveness Detection Effectiveness: The effectiveness of the liveness verification module was also examined. It was observed that the module was successful in detecting genuine users and preventing spoofing attacks, including photographs, videos, and 3D masks. The effectiveness of the module was examined using True Positive Rate (TPR) and True Negative Rate (TNR), which showed that the module was successful in verifying live users.
3) Real-Time Responsiveness: The total time taken by the system was observed to be low, which shows that the system can operate in real time.
4) Error Rates (FAR & FRR): The False Acceptance Rate (FAR) and False Rejection Rate (FRR) analysis revealed that the proposed system strikes an excellent balance between security and usability, thereby reducing unauthorized access as well as inconvenience to genuine users.

5) Environmental Adaptability: The proposed system was also evaluated under different illumination conditions, facial orientations, and expressions. The robustness of the proposed system was validated as it performed satisfactorily even under moderate variations of environmental conditions. The recognition and liveness detection module performed well under varying conditions.

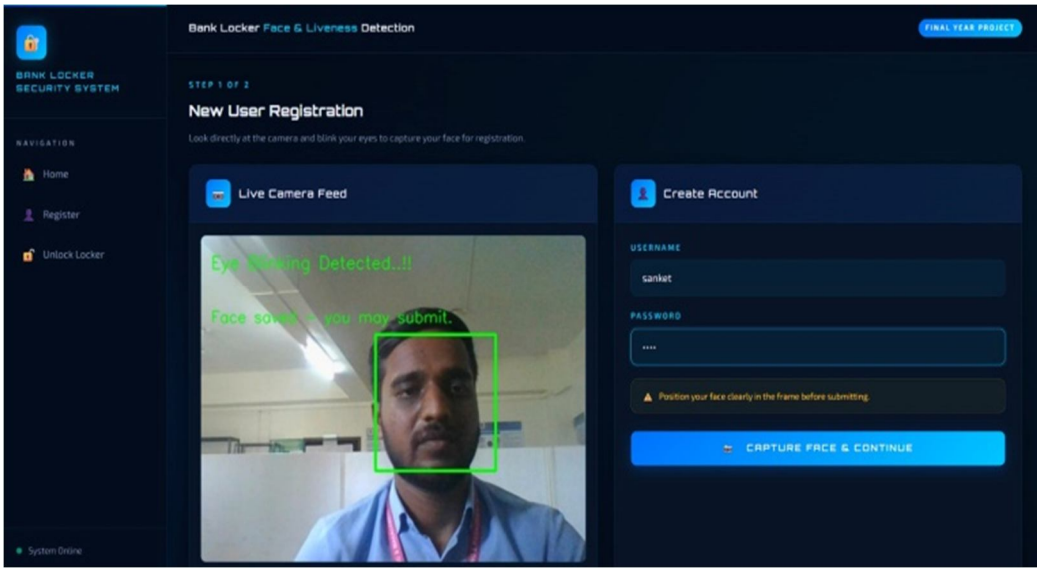
6) Comparative Performance: The proposed system was compared with other conventional approaches used to access bank lockers, such as keys, PINs, and facial recognition. The proposed system outperformed other approaches by a significant margin. The liveness detection feature of the proposed system ensured that it was more secure than other approaches. The proposed system was more trustworthy for access control to bank lockers.

A. Results Snapshots

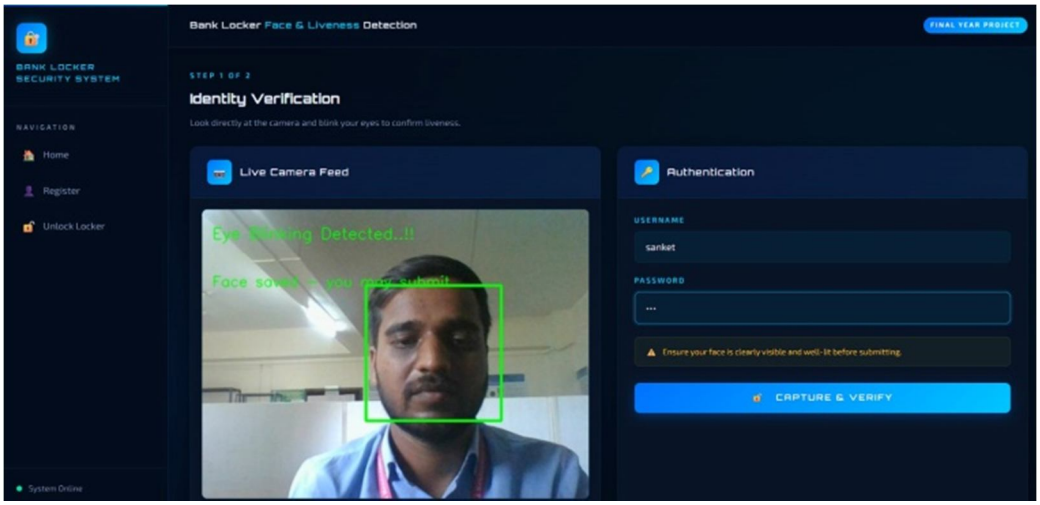
1) Home Page



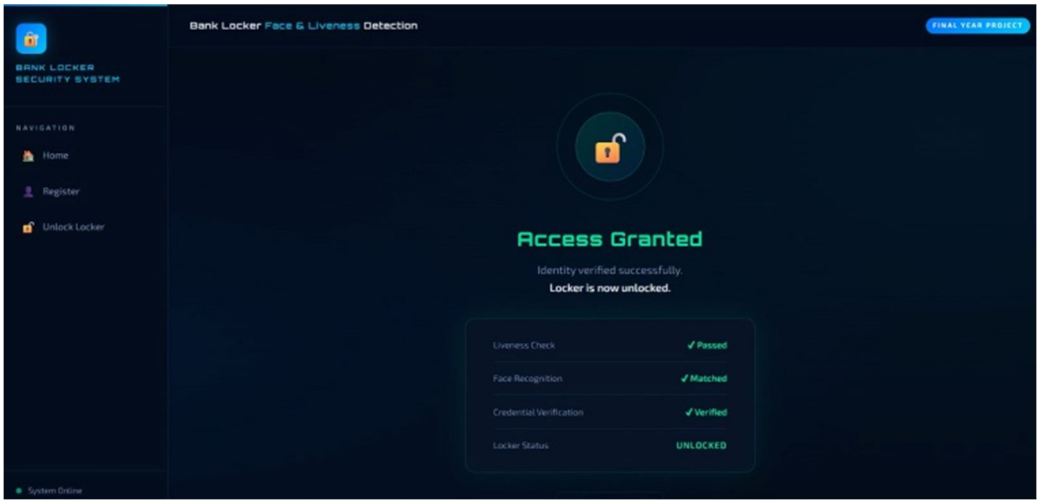
2) Registration Page



3) Identity Verification



4) Locker Unlock



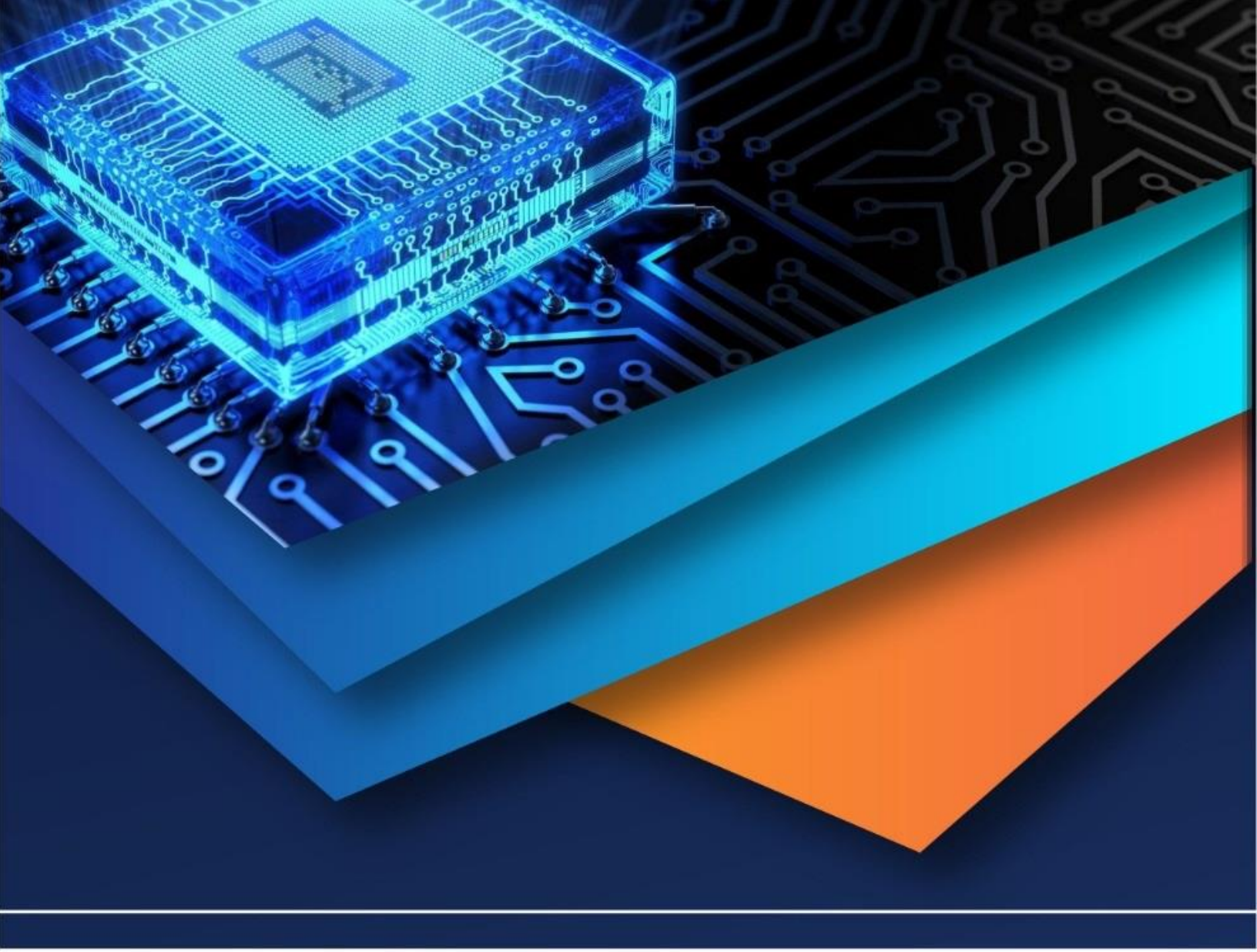
X. CONCLUSION

The integrated face recognition and liveness detection system offers high accuracy, security, and practical real-time performance. Performance metrics indicate that the system is suitable for use in bank lockers and other high-security physical access applications. The Bank Locker Security System with Face and Liveness Detection, as proposed, offers secure and contactless access through an integration of face recognition technology, which uses deep learning, and liveness detection.

REFERENCES

[1] S. Z. Li and A. K. Jain, Handbook of Face Recognition, 2nd ed. London, U.K.: Springer, 2011.
[2] A. George and S. Marcel, “Presentation attack detection using convolutional neural networks,” IEEE Transactions on Information Forensics and Security, vol. 14, no. 8, pp. 2147–2160, Aug. 2019.
[3] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, “Joint face detection and alignment using multitask cascaded convolutional networks,” IEEE Signal Processing Letters, vol. 23, no. 10, pp. 1499–1503, Oct. 2016.
[4] N. Patel, P. Sharma, and R. Singh, “IoT-based smart locker system using facial recognition,” International Journal of Innovative Research in Computer and Communication Engineering, vol. 8, no. 6, pp. 5632–5638, 2020.
[5] Y. Liu, A. Jourabloo, and X. Liu, “Learning deep models for face anti-spoofing: Binary or auxiliary supervision,” in Proc. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018, pp. 389–398.
[6] P. Viola and M. J. Jones, “Robust real-time face detection,” International Journal of Computer Vision, vol. 57, no. 2, pp. 137–154, 2004.

[7] J. Galbally, S. Marcel, and J. Fierrez, "Biometric antispoofing methods: A survey in face recognition," IEEE Access, vol. 2, pp. 1530–1552, 2014.
[8] S. S. D'Souza, "Deep learning for secure biometric authentication systems," International Journal of Computer Applications, vol. 176, no. 38, pp. 1–6, 2020.
[9] M. Sanderson and B. C. Lovell, "Multi-region probabilistic histograms for robust and scalable identity inference," in Proc. International Conference on Biometrics: Theory, Applications, and Systems (BTAS), 2009, pp. 1–8.
[10] A. Mohanty, S. B. Ghosh, and R. K. Sharma, "Design and implementation of an enhanced security locker system using facial recognition and IoT," International Journal of Advanced Research in Computer and Communication Engineering, vol. 9, no. 3, pp. 45–49, Mar. 2020.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY