IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Bank Locker Security System with Face Authentication

[1]Raghu K, [2]Hemanth Yadav H B, [3]Dushyanth J A, [4]Chiranth P R, [5]Akash Rajendra Sagar

[1]Assistant Professor, [2, 3, 4, 5]Student

[1,2,3,4,5]School of Electronics and Communication Engineering,

[1,2,3,4,5]REVA University, Bengaluru, India

***Abstract:*** This paper presents an advanced Bank locker security system based on Face Recognition. Traditional bank security locker systems in India often rely on keys and PIN codes for access control, which can be susceptible to theft, loss, or unauthorized access. To address these vulnerabilities, this paper presents a novel bank security locker system utilizing face authentication technology implemented through MATLAB, in conjunction with an Arduino-based hardware interface. The proposed system offers enhanced security by replacing conventional key and PIN-based authentication methods with biometric face recognition. Leveraging MATLAB's image processing and machine learning capabilities, the system extracts and analyses facial features for authentication, ensuring a reliable and secure access control mechanism. The integration of face authentication with MATLAB and Arduino enhances the security and usability of bank locker systems, providing a robust solution for safeguarding valuable assets. This Paper demonstrates the potential of leveraging advanced technologies to modernize and strengthen security measures in banking infrastructure, paving the way for more secure and user-friendly access control systems.

***Index Terms* - MATLAB, Arduino, Face Recognition.**

## I. INTRODUCTION

In a time of rapid technological development and growing security breach worries, it is now critical to protect valuables inside bank vaults. The integrity of these secure storage units can no longer be ensured by using outdated authentication techniques like passwords or keys. The idea of a High Protection Bank Locker Security System with Live Image Authentication appears as a clever response to this urgent demand. This innovative system integrates cutting-edge technologies to establish security, ensuring the utmost protection against unauthorized access. By using live image recognition, this system significantly enhances the authentication process, making it highly resistant to fraudulent attempts. The utilization of live image recognition involves capturing real-time images of individuals attempting to access the bank locker. These images are then analyzed using advanced algorithms to verify the identity of the user. High-resolution cameras placed at the locker entry point are used to take real-time pictures of the user's face to perform live image authentication. Subsequently, these photos undergo complex computer processing to extract distinct face traits, which are then cross-referenced with pre-registered templates to verify the user's identity. By using static pictures or masks, this strategy not only increases security but also removes the risk of fraudulent access. This technique reduces the dangers associated with traditional methods, such theft, forgeries, or unauthorized access through stolen credentials, by utilizing both visual and audible clues for verification. Furthermore, by enabling a prompt response to questionable activity or possible security breaches, the addition of Realtime monitoring capabilities strengthens security safeguards. All things considered, the High Protection Bank Locker Security System with Live Image Authentication is a noteworthy development in the field of bank security since it offers unmatched levels of security for priceless assets along with a smooth and intuitive authentication process. A breakthrough in the protection of valuable assets within financial organizations is the suggested high protection bank locker security system. For financial institutions and their clients, the system offers unmatched security, resilience, and convenience using live picture authentication technology. This paper will examine this novel security solution's technical details, implementation difficulties and possible uses in more detail to develop and deploy a robust bank security locker system using facial authentication technology integrated with MATLAB. The aim is to elevate the security standards for protecting financial assets by implementing a multi-layered approach that combines facial recognition. The system should accurately authenticate locker owners in real-time, ensuring only authorized individuals can access bank vaults. Overcoming the challenge involves designing a seamless and reliable system capable of capturing and analyzing live photos of users while maximizing security and operational efficiency.

## II. LITERATURE SURVEY

Face recognition technology has seen significant improvements in recent years, especially with the advent of deep learning techniques. The use of convolutional neural networks (CNNs) has enhanced the accuracy of face recognition systems, making them more reliable for security applications like bank locker systems. Studies have focused on improving the robustness of these systems under various conditions, such as low lighting, different facial expressions, and partial occlusions. CNN-based models have significantly outperformed traditional methods like PCA (Principal Component Analysis) and LDA (Linear Discriminant Analysis) in face recognition tasks [21]. Transfer learning techniques, where pre-trained models are fine-tuned for specific tasks, have been successfully applied to face recognition systems in bank locker scenarios [22].

Recent research highlights the integration of multiple biometric traits such as face, fingerprint, and iris recognition to enhance the security of bank lockers. Multi-modal biometric systems are more secure because they reduce the likelihood of unauthorized access by requiring multiple forms of authentication. Score-level and decision-level fusion techniques are commonly used to integrate data from different biometric modalities [23]. These systems provide higher accuracy and reliability compared to single-modal systems, especially in high-security environments like banks [24].

The practical application of face authentication systems in banking environments involves integrating these technologies with existing infrastructure. Studies have examined the challenges of deployment, such as the cost, user acceptance, and system maintenance. Successful implementations have been reported in pilot projects where face authentication was used for secure locker access. Banks have reported increased user satisfaction due to the convenience of face-based authentication compared to traditional methods [25], [26].

### The proposed work

As shown in the Fig 1, Arduino serves as the system’s main processing unit and is its fundamental component. It embeds the face recognition algorithms as well as external device communication. In the proposed system an LCD (Liquid Crystal Display) module is utilized to give a user interface with security system. It displays prompts authentication, status updates, and directions. The facial recognition is based on extracting the dominating features of a set of human faces stored in the database as shown in Figure 2 and performing mathematical operations on the values corresponding to them. Hence when a new image is fed into the system for recognition the main features are extracted and computed to find the distance between the input image and the stored images. Thus, some variations in the new face image to be recognized can be tolerated. When the new image of a person differs from the images of that person stored in the database, the system will be able to recognize the new face and identify who the person is after successful face recognition system unlocks the locker. If face didn’t match, a notification is sent to the bank manager through twillio messenger as a text message and an e-mail with the photo of unknown person’s face. The Proposed system also uses sensors like gas, fire sensors for locker safety. If smoke or fire is detected sprinkler automatically turns on for fire extinguish.

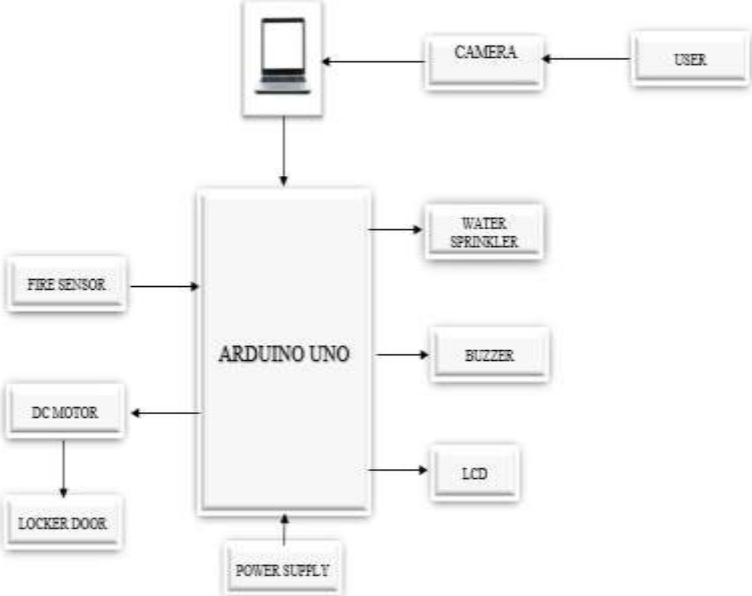

Figure 1 Block diagram of the Proposed model

Figure 3 outlines a face recognition system integrated with data processing and access control. When a user presents an input image, it undergoes facial recognition processing. If a match is found, a signal is sent to a DC motor to grant access to the locker. If no match is found, a message alert is sent to the owner. If the owner attempts to enter a password, access is denied unless the correct password is entered.

In Figure 4 a flowchart outlines a facial recognition process. If the camera is open, it reads an image, performs face detection, cuts and saves the detected face as grayscale, conducts face recognition, and then proceeds to read the next image. However, if the camera is not on, the process ends.

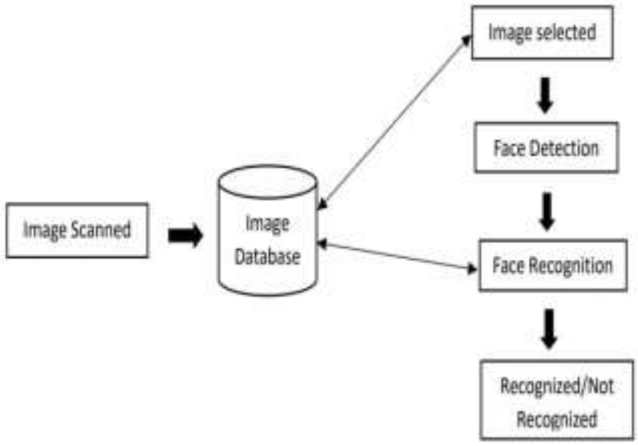

Figure 2: Face Recognition process

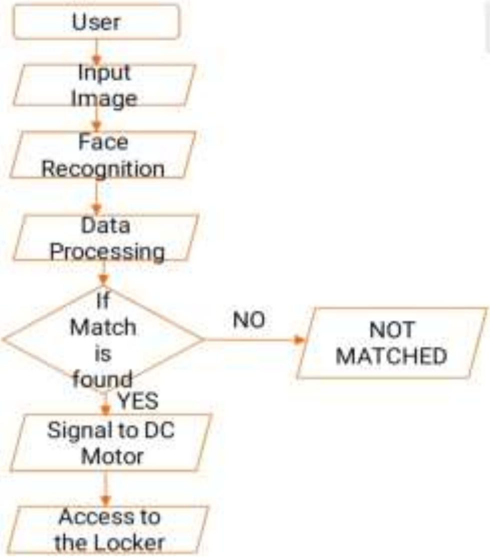

Figure 3: Flow diagram of the proposed system

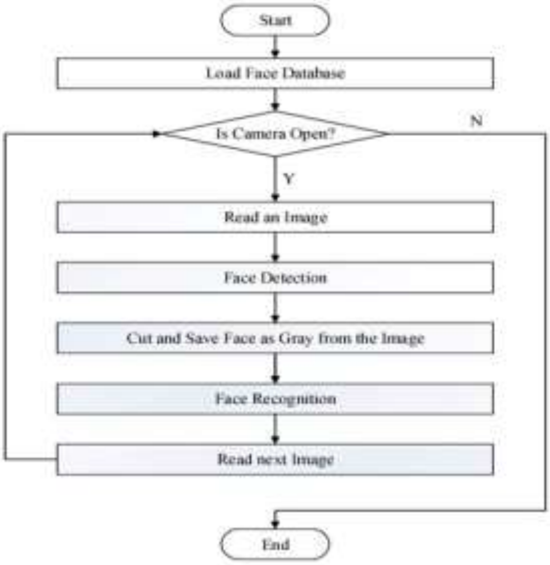

Figure 4: Flowchart of Face Recognition Process

The proposed system utilizes MATLAB-based image capturing techniques, where a camera is integrated with a PC running MATLAB software. This configuration is then connected to an Arduino via a cable interface. In the event of an unauthorized attempt to access the locker, the system automatically triggers an email notification, which includes a captured image of the intruder. Users are provided with the option of utilizing face recognition authentication, offering a flexible and robust security solution tailored to their needs. If there is a mismatch in the authentication process, an alert message is immediately dispatched to the user, ensuring real-time monitoring and enhancing the security of the locker system.

Figure 5 comprises the process that involves several steps for facial recognition. Initially, image resolution is set, followed by setting PCA dimensionality parameters. Training images are read, cropped, and saved. These images are then used to form a training data matrix along with their corresponding class labels. A PCA transformation matrix is calculated to reduce dimensionality, and feature vectors for training images are computed using this matrix. These vectors are stored for later use. Test faces are then read, cropped, and saved, and for each test face, its feature vector is calculated using the PCA transformation matrix. Distances between the test feature vector and all training vectors are computed and stored with their corresponding class labels. Error count is initialized, and for each test face, the person ID of the most similar training vector is determined using the distance data. If the found ID is not equal to the ID of the test image, the error count is incremented. Finally, the correct recognition accuracy is outputted based on the error count and the total number of test images.

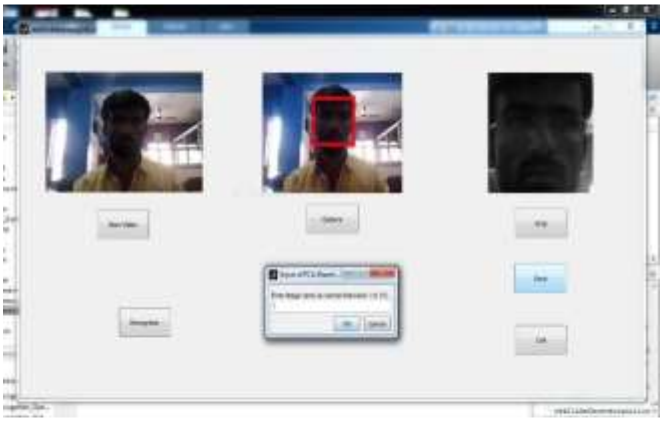

Figure 5: Image Capturing step

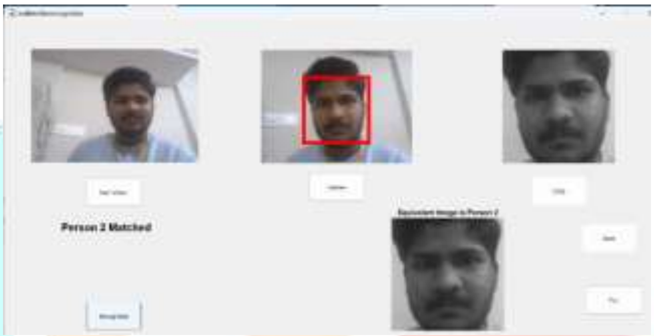

Figure 6: User Case 1

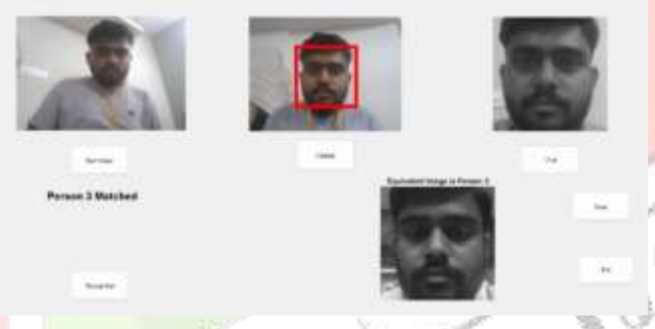

Figure 7: User Case 2

Figure 6 and Figure 7 demonstrate that the user's input data matches the data stored within the input data stored within the database. Figure 8 demonstrates that the input data does not match any data stored in the database and denies access to that person.

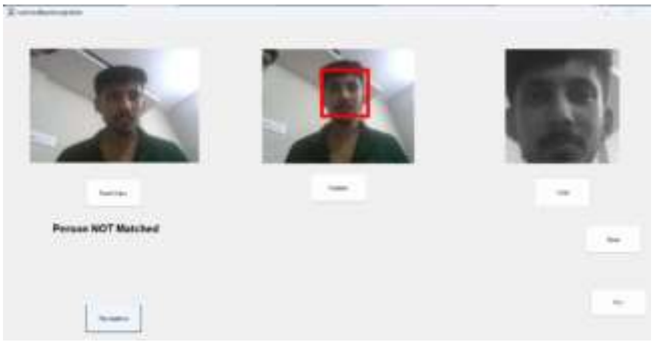

Figure 8: User Case 3

## IV. RESULTS AND DISCUSSION

Three metrics are used to assess the suggested system's performance: accuracy, speed, and reliability. The outcomes of the experiments show how well the picture authentication systems work to safely allow users to access bank lockers. The system is suited for real-world deployment since it maintains minimal latency while achieving high accuracy rates.

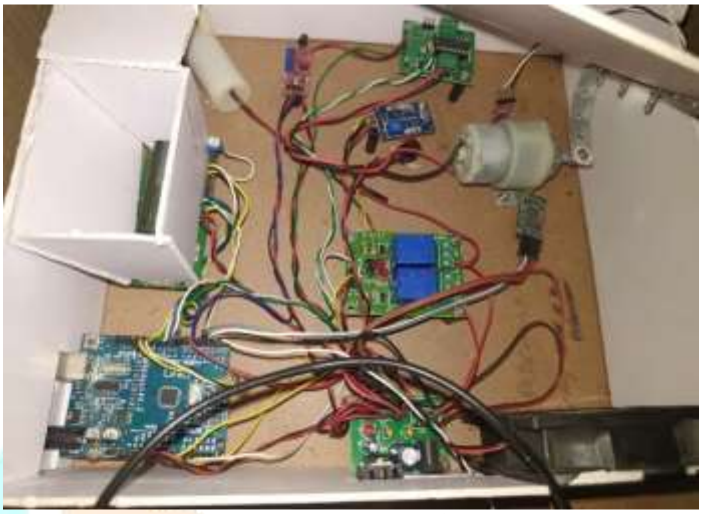

Figure 9: Final Product view of Proposed Model

Figure 6 shows a case of registered user, whose face's photo are present in the database with all possible different angles. When person 2 tries to access his bank locker, the real time face input image is matched with the database of that particular locker and access is granted. The output in Figure 6 is shown as "Person 2 Matched".

Similarly in Figure 7, it shows a case of another registered user, whose face's photo are present in the database with all possible different angles. When person 3 tries to access his bank locker, the real time face input image is matched with the database of that particular locker and access is granted. The output in Figure 7 is shown as "Person 3 Matched".

Figure 8 shows a case of person who is unauthorized for that particular locker and the output is shown as "Person NOT Matched".

## V. CONCLUSION AND FUTURE SCOPE

This paper demonstrated a very secure bank locker security system that uses live image authentication. In this paper, it is shown how to improve bank locker security in an economical and successful manner by utilizing MATLAB tool and Arduino UNO. To increase security, future development may concentrate on refining the system and investigating new biometric authentication methods. There are several ways in which the live picture authentication high-security bank locker security system might be improved in the future. Assuring regulatory compliance, addressing scalability issues for enterprise deployment, implementing real-time threat detection mechanisms, integrating blockchain technology for immutable audit trails, developing a user-friendly mobile application interface, integrating additional biometric modalities like fingerprint recognition and iris scanning, and emphasizing user education and training programs are just a few examples of what this entails. To ensure that the system is effective in protecting important assets in banking environments, these future research directions seek to improve the system's security, usability, scalability, and compliance while keeping up with developing technology and changing regulatory landscapes.

**Acknowledgment**

We sincerely thank REVA University, faculty and staff for extending their support in all aspects for the completion of this paper. We also thank our parents and the almighty for all the moral support and encouragement.

## References

[1] M.A. Turk, A.P. Pentland, “Face Recognition Using Eigenfaces,” IEEE Conference on Computer Vision and Pattern Recognition, pp.586--591, 1991.

[2] M. S. Nixon and A. S. Aguado, Image Processing and Feature Extraction. Publisher: Academic Press, 2019.

[3] Gulzar Kanza "Detection and recognition of human faces for automobile security," Conference Paper, June 2017.

[4] Moritoshi Yasunaga, Taro Nakamura, and Ikuo Yoshihara, “A Fault-tolerant Evolvable Face Identification Chip,” Proc. Int. Conf. on Neural Information Processing, pp.125-130, Perth, November 1999.

[5] Preeti Sharma and her colleagues present "Enhanced Security System for Bank Lockers Using Facial Recognition and IoT." 2020 International Conference on Informatics and Computer Communication (ICCCI). IEEE, 2020.

[6] P. N. Belhumeur, J. P. Hespanha, D. J. Kriegman, “Eigenfaces vs. Fisher faces Recognition using class specific linear projection,” IEEE Trans. Pattern Anal. Machine Intell., vol. 19, pp. 711–720, May 1997.

[7] M.S. Bartlett, J.R. Movellan, T.J. Sejnowski, “Face Recognition by Independent Component Analysis”, IEEE Trans. on Neural Networks, Vol. 13, No. 6, November 2002, pp. 1450-1464.

[8] "Enhanced Security for Bank Locker Using Biometric Authentication and Cryptography," Kumar, Amit, et al. Conference on Computing, Communication, and Intelligent Systems, International, 2021 (ICCCIS). IEEE, 2021.

[9] Singh, Pankaj, et al. "Deep Learning-Based Security System for Bank Lockers Using Facial Recognition." 2022: International Conference on Knowledge Economy and Computational Intelligence (ICCIKE). IEEE, 2022.

[10] Verma, Deepika, "Efficient Bank Locker Security System Using IoT and Biometric Authentication,", et al. The second international conference on advanced paradigms for computation and communication is scheduled for 2023 (ICACCP). IEEE, 2023.

[11] Abhilasha A Sayar1 , Dr. Sunil N Pawar2 , “Review of Bank Locker System Using Embedded System” , International Journal of Advanced Research in Computer and Communication Engineering .,Vol. 5, Issue 2, February 2016 .

[12] Bhalekar S.D., Kulkarni R.R., Lawande A.K., Patil V.V., “On line Ration card System by using RFID and Biometrics”, International journal of Advanced Research in Computer Science & Software engineering., Vol. 5, Issue 10, October 2015.

[13] Pramila D Kamble and Dr. Bharti W. Gawali “Fingerprint Verification of ATM Security System by Using Biometric and Hybridization” International Journal of Scientific and Research Publications, Volume 2, Issue 11, November 2012.

[14] Bhalekar S.D., Kulkarni R.R., Lawande A.K., Patil V.V., “On line Ration card System by using RFID and Biometrics”, International journal of Advanced Research in Computer Science & Software engineering., Vol. 5, Issue 10, October 2015.

[15] P. Sugapriya#1, K. Amsavalli#2, “Smart Banking Security System Using PatternAnalyzer”,International Journal of Innovative Research in Computer and Communication Engineering ,Vol.3, Special Issue 8, October 2015.

[16] Ashish M. Jaiswal andMahipBartere “Enhancing ATM Security Using Fingerprint And GSM Technology”, International Journal of Computing Science and Mobile Computing Vol. 3, Issue. 4, April 2014.

[17] Sagar S. Palsodkar*, Prof S.B. Patil , “Review: Biometric and GSM Security for Lockers” Int. Journal of Engineering Research and Applications , Vol. 4, Issue 12( Part 6), December 2014.

[18] 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, 2016.

[19] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, “DeepFace: Closing the Gap to Human-Level Performance in Face Verification,” *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2014.

[20] A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics*, Springer, 2006.

[21] N. Poh, T. Bourlai, and J. Kittler, “A Multimodal Biometric Test Bed for Quality-Dependent, Cost-Sensitive, and Client-Specific Score-Level Fusion Algorithms,” *IEEE Transactions on Systems, Man, and Cybernetics - Part B: Cybernetics*, vol. 40, no. 3, pp. 539–552, 2010.

[22] S. Bhattacharyya, S. Ranjan, A. Dasgupta, and A. Roy, “Biometric Authentication: A Review,” *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 4, no. 1, pp. 57–63, 2016.

[23] R. S. Chakraborty and S. Bhattacharya, “Face Recognition and Its Application to Forensic Investigation,” *Handbook of Statistics*, vol. 40, pp. 189–220, 2018.