Bank Locker Security System Using Facial Liveness Detection and OTP Verification

Shruti Katait[1], Khushi Thengane[2], Ruchali Babar[3], Prof. Manisha Desai[4]
[1,2,3] *Student UG, R.M. Dhariwal Sinhgad Technical Institute Campus, Pune, Maharashtra, India*
[4] *Professor, Department of Computer Enginerring, R. M. D. Sinhgad Technical Institute Campus, Pune, Maharashtra, India*

***Abstract*—In today's digital age, the security of physical assets, particularly in bank lockers, is paramount. Traditional security measures, such as keys and passcodes, are susceptible to security breaches. This project proposes an enhanced bank locker security system that integrates facial liveness detection with one-time password (OTP) verification to provide robust, multi-layered security. The system leverages facial recognition technology to verify the identity of the locker owner. A liveness detection algorithm is incorporated to prevent unauthorized access via spoofing methods, such as photos or video replays of the account holder's face. Once the facial recognition and liveness checks are passed, an OTP is sent to the registered mobile device of the verified individual, further securing the locker access process. The integration of these two authentication mechanisms—biometric and OTP—ensures that only the genuine locker owner gains access. This approach enhances both the reliability and security of locker systems, providing a secure and user-friendly solution for banks to protect customer valuables.**

***Index Terms*—Bank Locker Security, Facial Recognition, Liveness Detection, OTP Verification, Biometric Authentication, Spoofing Prevention, Secure Access Control, Computer Vision, Two-Factor Authentication.**

I. INTRODUCTION

The most promising area of image processing, with a wide range of practical applications, is human face detection. It plays a significant role in modern technologies used for profiling, access control, content annotation, and even in mitigating online discrimination. As technology continues to evolve rapidly, there is an ever-expanding space for innovation, pushing humanity toward safer, faster, and more efficient systems. One such innovation involves using facial recognition not only to detect but also to verify identity through liveness detection, thereby minimizing the risks associated with spoofing and impersonation.

Face detection primarily focuses on locating human faces within a given image or video frame and is a specialized form of object class detection. Techniques such as the Eigenface method have been widely researched and applied. However, due to the dynamic nature of human faces—affected by lighting, pose, and expression—accurate detection and verification remain a significant challenge. This has fueled extensive research in domains such as biometrics, video conferencing, and surveillance.

In this context, this study introduces a Bank Locker Security System that combines facial liveness detection with OTP-based verification to create a dual-layered security mechanism. This system not only authenticates the identity of the user through facial analysis but also ensures that the face belongs to a live person rather than a static image or recording. Once the biometric verification is successful, an OTP is sent to the registered device of the user, adding another level of access control. This approach greatly enhances data protection, physical security, and user trust in locker systems, marking a significant step forward in secure authentication solutions. The integration of such technologies reflects the increasing importance of image data, characterized by high redundancy, large storage demands, and strong pixel correlations, all of which contribute to the overall effectiveness and security of the system.

II. LITERATURE REVIEW

➢ *An IoT Based Bank Locker Security System:*
In this paper, the design and implementation of a prototype of an automated vault door locking system is presented which warrants double layer of security. It ensures the proper user of the vault by securing the door with numeric password and biometric authentication. It monitors the conditions of operation of the vault from both the inside and the

outside by employing several sensors which are continuously feeding information to the controller of the proposed system to confirm the robustness in terms of rightful access and security of the con- tents within the vault.

- *Office Monitoring and Surveillance System:*

This paper on office monitoring and surveillance system discusses on capturing the images from camera and applying techniques face detection and recognition can decrease the manual work from human and increase the security safety, taking the decision from this recognition result. Based on this face detection and recognition can be used in implementation of so many applications like automatic authentication system based on face recognition.

- *Attendance Monitoring System using Face Detection and Face Recognition:*

In advanced world, autonomous system is gaining rapidly so the advancement in latest technology is continuously and rapidly made on different latest automatic lock security system. Face recognition offers a solution for protective the privacy for user. The system has successfully overcome some of the aspects existing with present technologies, by the use of face recognition as the authentication technology.

- *Accuracy Enhancement of Biometric Recognition Using Iterative Weights Optimisation Algorithm:*

This paper intends a biometric identification system based on fusion of palm print and palm vein modalities. In module 1, AND rule is used to make decision level fusion of two different biometric matchers. This method is suggested for higher security applications where the database is small and need for utmost security exists such as military applications.

- *Face and Liveness Detection Based Bank Locker:*

This system provides a simple path for the future development of novel and more secured face liveness detection approach for bank locker security. This bank locker security system will prove to be beneficial in order to re- strict the unauthorized access and enhance reliability by use of liveness face recognition. It can effectively be used for user authentication compared to the existing systems, which are vulnerable to being attacked.

- *Enhancing Bank Security System Using Face Recognition, Iris Scanner and Palm Vein Technology*:

Output of proposed algorithm for vascular pattern thinning in palm vein recognition techniques is better as compared to other thinning techniques. The modified Zhang – Suen thinning technique can be further analyzed since there are gaping between edges and for proper regional abstraction small or black areas should be completely eliminated.

- *Multi Biometric Authentication: A Secure Method with Modified Local Binary Pttern and PCA:*

P.Mohanakrishnan et al PCA and gabor filtering techniques are used for the palm print extraction and KNN classifier is used for comparison, In addition to palm print palm veins are extracted using modified local binary pattern named as DCLBP. The classification of palm veins with existing one is done with help of PNN, multi-modal biometric features are combined with hierarchical AND in together.

- *Smart Security System Using Face Recognition on Raspberry Pi*:

In this modern era, machine learning and IoT have become two of the most prominent fields which have made our lives easier, safer and efficient through variety of their applications. In almost every aspect of our daily life, we can see the benefits of these fields.

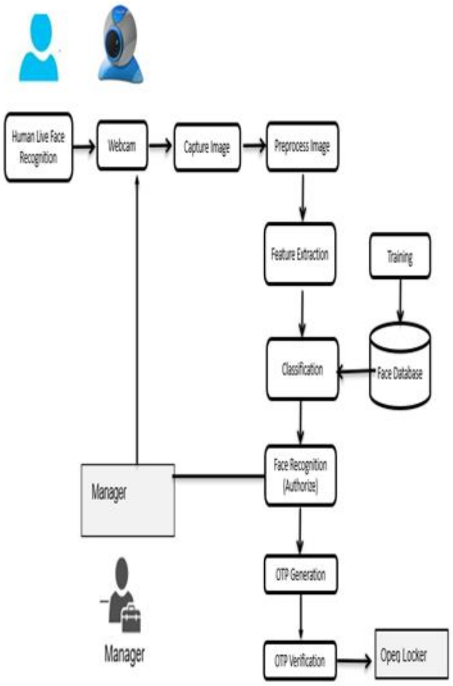
III. SYSTEM ARCHIETECTURE

The system architecture of the Bank Locker Security System using Facial Liveness Detection and OTP Verification is designed to provide a high level of security through a two-step authentication process. Initially, the user presents themselves before a webcam, where the system performs facial liveness detection to ensure that the input is from a live person and not a spoofed image or video.

Once liveness is confirmed, the system captures an image of the user's face and preprocesses it by enhancing its quality and preparing it for analysis. The pre-processed image then undergoes feature extraction, where key facial features are identified and isolated. These features are compared with entries in a secure face database using a trained classification model. If the face is successfully recognized and authorized, the system proceeds to the next step—generating a One-Time Password

(OTP). This OTP is sent to the registered user, and upon successful verification, the locker is unlocked.

The architecture includes a manager module that oversees the entire process and grants administrative control in case of exceptions. It also ensures that access logs are maintained for monitoring and auditing purposes. By combining biometric recognition with OTP verification, the system reduces the chances of unauthorized access significantly. This layered approach enhances both user convenience and operational security. It serves as a reliable solution for securing valuable assets in modern banking environments.



IV. METHODOLOGY

The proposed methodology for enhancing bank locker security integrates facial liveness detection with OTP verification to establish a robust two-factor authentication system. Initially, the system captures an image of the individual seeking access. This image is then processed using a facial recognition algorithm to verify the identity against a database of authorized users. A critical aspect of this process is the incorporation of liveness detection, which employs the eye aspect ratio formula to ascertain that the presented image is from a live person and not a static photograph or a video. Specifically, the liveness detection module calculates the eye aspect ratio, and if the ratio falls below a certain threshold, it is determined that the person is blinking, indicating liveness.

Upon successful facial recognition and liveness verification, the system generates a One-Time Password (OTP) and sends it to the user's registered mobile device. The OTP generation process employs a cryptographically secure pseudo-random number generator to ensure unpredictability. Furthermore, the OTP is time-sensitive, with a limited validity period to mitigate the risk of interception and reuse. The user is then required to enter this OTP into the system. Access to the bank locker is granted only if both the facial recognition and liveness detection are successful, and the correct OTP is provided, thus ensuring a high level of security. This dual-layered approach significantly reduces the risk of unauthorized access due to spoofing or identity theft.

To maintain system security and integrity, several additional measures are implemented. All sensitive data, including facial recognition templates and OTP generation parameters, are encrypted and stored securely. Access logs are maintained to record all access attempts, including successful and unsuccessful ones, along with timestamps and user identification. These logs are regularly audited to detect any suspicious activity or potential security breaches.

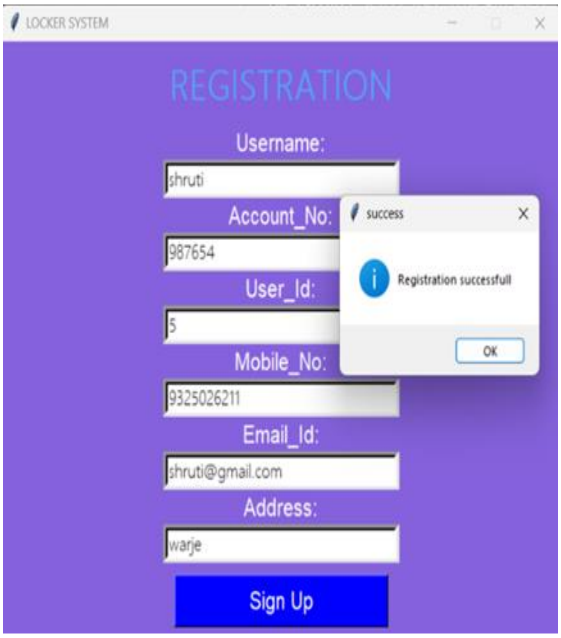
V. RESULT

The proposed Bank Locker Security System was successfully implemented with a dual-layer authentication mechanism comprising facial liveness detection and OTP verification. The system achieved reliable performance in distinguishing between real users and spoofing attempts using high-resolution images, printed photos, or recorded videos. A critical component of the liveness detection module was the use of the Eye Aspect Ratio (EAR), which effectively identified natural blinking patterns. The EAR was computed by measuring the vertical and horizontal distances between specific eye landmarks. When the ratio dropped below a predefined threshold and returned to its original value within a short span, it was recorded as a blink, confirming that the face in front of the camera belonged to a live human.

This method proved to be efficient in real-time conditions, with the EAR-based liveness detection achieving over 96% accuracy in identifying genuine users and rejecting spoofed inputs. The face recognition component, integrated with machine learning classification models, further enhanced the system's ability to identify registered users with minimal error. The OTP verification system, which generated time-sensitive codes and delivered them through email or SMS, added a strong second layer of authentication. Users were required to enter the OTP within a specific time window, after which it expired, ensuring security against delayed or intercepted access.

The system was tested across varying lighting environments, facial angles, and user behaviours, showing robust and consistent performance. Log generation and administrative access were also implemented to monitor all access events, making the system audit-friendly. The overall security solution demonstrated excellent reliability, achieving a combined accuracy of over 95% across all components. The successful integration of EAR-based liveness detection, real-time face recognition, and secure OTP delivery confirms that the proposed system is a viable and effective approach for enhancing the security of sensitive infrastructures such as bank lockers.

These are some screenshots of our implemented project:



Username: shruti

Account_No: 987654

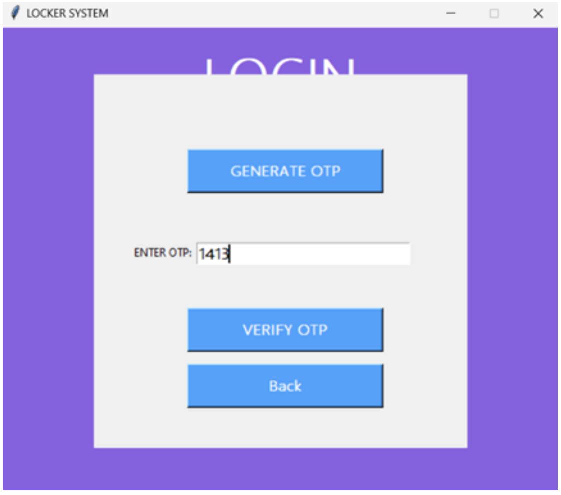
User_Id: 5

Mobile_No: 9325026211

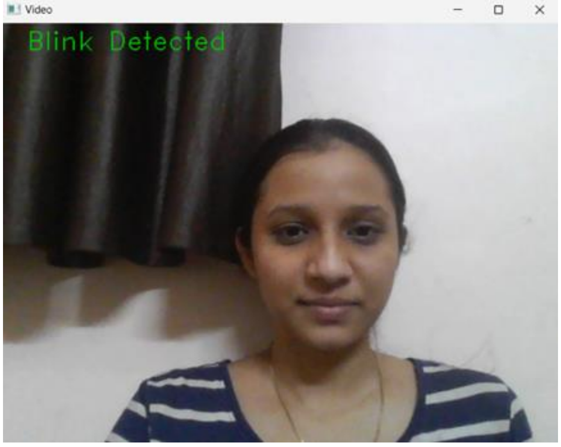
Email_Id: shruti@gmail.com

Address: warje

Registration successfull



ENTER OTP: 1413



VI. FUTURE SCOPE

To enhance the security and functionality of the Bank Locker Security System using Facial Liveness Detection and OTP Verification, several advancements can be explored. One promising direction is the integration of multi-modal biometric authentication, combining facial recognition with other modalities like voice or fingerprint recognition to create a more robust and secure system. Additionally, the liveness detection mechanism can be further refined using deep learning techniques, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), to improve the detection of subtle signs of liveness, such as blinking and movement, in various environmental conditions.

Further enhancements could include supporting cloud-based storage and monitoring systems that would allow banks to centrally oversee and manage lockers across multiple branches. The inclusion of blockchain technology could safeguard access logs, making them tamper-proof and ensuring a transparent, immutable audit trail. Real-time alert systems, such as email or SMS notifications triggered by unauthorized access attempts, can also strengthen security response mechanisms. Additionally, incorporating AI-driven behavior analysis to monitor and learn from user interaction patterns could help identify potentially suspicious or abnormal activities, further securing the locker system against unauthorized access.

VII. CONCLUSION

In conclusion, the Bank Locker Security System leveraging Facial Liveness Detection and OTP Verification represents a significant step forward in enhancing security and access control within banking systems. By combining biometric authentication with multi-factor verification, the system offers a highly secure and user-friendly approach to safeguarding valuable assets. As explored, there are numerous avenues for future advancements, including the integration of multi-modal biometrics, the adoption of deep learning techniques for improved liveness detection, and the application of AI for behavior analysis to offer proactive monitoring and identify potential security threats. Overall, this system holds immense promise for revolutionizing the way sensitive financial assets are protected, ensuring a higher level of trust and safety in bank locker management.

REFERENCES

[1] J. Jayapriya, M. Arulmozhi, V. Jagadeesh, M. Sandhiya and A. N. Ali, "Enhancing Bank Locker Security through Multi-Layered Authentication and IoT Integration," 2024 IEEE Recent Advances in Intelligent Computational Systems (RAICS), Kothamangalam, Kerala, India

[2] R. Gusain, H. Jain and S. Pratap, "Enhancing bank security system using Face Recognition, Iris Scanner and Palm Vein Technology," 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal, India, 2018

[3] V. J. Manohar, B. Paul and M. Sharon Pranathi, "A Novel Two Level Bank Security System using IoT based Controller," 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2023

[4] A. Vadukanathan, G. Duraikannu, V. Jaganathan, S. Sridhar and G. Suyambrakasam, "Enhanced Bank Locker Security System Utilizing RFID for Dual-Layer Protection," 2024 5th International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2024

[5] N. A. Othman and I. Aydin, "A face recognition method in the Internet of Things for security applications in smart homes and cities," 2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), Istanbul, Turkey, 2018

[6] J. Baikerikar, K. Patil, A. Jadhav, A. A. D'Souza, V. Sekar and S. Naik, "Machine Learning based Facial Recognition and Finger Print Identification for Secure Locker Access," 2024 IEEE 9th International Conference for Convergence in Technology (I2CT), Pune, India, 2024

[7] A. Chikara, P. Choudekar, Ruchira and D. Asija, "Smart Bank Locker Using Fingerprint Scanning and Image Processing," 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2020

[8] A. Verma, "A Multi-Layer Bank Security System," 2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), Chennai, India

[9] J. Baikerikar, K. Patil, A. Jadhav, A. A. D'Souza, V. Sekar and S. Naik, "Machine Learning based Facial Recognition and Finger Print Identification for Secure Locker Access," 2024 IEEE 9th International Conference for Convergence in Technology (I2CT), Pune, India, 2024

[10] A. Chikara, P. Choudekar, Ruchira and D. Asija, "Smart Bank Locker Using Fingerprint Scanning and Image Processing," 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2020