International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET23103101

Implementation of Bank Locker Authentication System Using Facial Recognition

Prof. A.B. Gadewar[1], Yash D Satre[2], Saurabh Y Girme[3], Sagar Walunj[4]

Information Technology Department, Savitribai Phule Pune University, PDEA's College of Engineering Manjari (Bk), Pune, Maharashtra, India

ARTICLEINFO

Article History:

Accepted: 10 May 2023

Published: 29 May 2023

Publication Issue

Volume 10, Issue 3

May-June-2023

Page Number

286-291

ABSTRACT

Security and Authentication of individuals is necessary for our daily lives especially in Bank lockers. A smart digital door lock system for bank automation is equipment that uses digital information such as a user's data and face recognition as the method for authentication in the system. In this system the bank will collect the face imprints of each person for accessing the lockers. Only authenticated people can recover the money, documents from the lockers as faces are stored for the individual identity of a person. For facial recognition, this project uses the CNN algorithm. In this project, only authenticated user can access the lockers as faces are stored for the individual identity of a person. Facial recognition alone cannot determine whether the person is real or not. Therefore, liveness detection is implemented. In liveness detection, the system detects if it interacts with a real person or a spoof artefact used by other person such as a face photo. To detect whether the person is live or not the project uses eye blink detection. In this system the owner of a particular locker needs to authenticate his/her identity by verifying their face following with an One Time Password authentication feature. Here the person will receive an OTP received on their registered mobile number, proceeding with it; the valid one will allow the owner to access the particular locker whilst incorrect will not.

Keywords : Authentication System, Facial Landmarks, Convolutional Neural Networks

I. INTRODUCTION

Although the popularity performance of biometric system is nowadays quite satisfactory for many applications, much work continues to be necessary to permit convenient, secure and privacy-friendly systems to be designed. In face recognition, the same old attack methods could also be classified into several categories. The thought of classifying relies on what verification proof is provided to face verification system. In this paper, we have proposed a technique of live face detection to resist the attack employing artefacts like a stolen photo, stolen face photos, recorded video, 3D face models. Liveness detection has been a really active research topic in fingerprint recognition and iris recognition communities in recent years. It is that the act of differentiating the feature space into live and non-living. But in face recognition, approaches are pretty much limited to cope with this problem. Imposters will attempt to introduce an oversized number of spoofed biometrics into system

In banking sector most, advanced technologies are not being used. Bank safety is an important issue at present. Our money is not safe in bank lockers when people cheat and misuse bank account and take unauthorized access to bank account. For safety purpose locks or alarms are installed in the bank lockers. For the safety of bank lockers latest technologies are used. Designing of our prototype, involves the image comparing technique. Also, manpower used in managing these lockers is vast in banks whereas there are less people to attend to the consumers, banks can deploy more employees instead of wasting manpower in locker management system as our project will automate the locker system in banks.

II. LITERATURE SURVEY

The security of bank lockers is of utmost importance to ensure the protection and integrity of valuable assets entrusted by customers. Traditional security systems relying on physical keys or access codes have their limitations, making them susceptible to theft or unauthorized access. However, the advent of facial recognition technology has brought about a promising solution to enhance bank locker security. This literature survey aims to delve into existing research and advancements pertaining to bank locker security systems utilizing facial recognition. By exploring the benefits, challenges, and best practices in implementation, this survey will shed light on the potential of facial recognition technology in bolstering bank locker security.

A. FACIAL RECOGNITION TECHNOLOGY IN SECURITY SYSTEMS:

This section will provide a comprehensive overview of facial recognition technology and its applications within security systems. It will delve into the fundamental principles underlying facial recognition, including face detection, feature extraction, and matching algorithms. Moreover, it will critically evaluate the advantages and imitations associated with facial recognition technology as it pertains to bank locker security.

B.BIOMETRIC AUTHENTICATION FOR BANK LOCKER SECURITY:

Focusing specifically on biometric authentication, this section will delve into the use of facial recognition technology for bank locker security. It will compare and contrast facial recognition with other biometric modalities such as fingerprint or iris recognition, assessing its efficacy in this context. Furthermore, the section will examine the reliability and accuracy of facial recognition systems, considering factors such as varying lighting conditions, pose variations, and potential vulnerabilities to spoofing attacks.

C.CASE STUDIES AND IMPLEMENTATION:

This section will extensively review various case studies and real-world implementations of bank locker security systems incorporating facial recognition. It will provide insights into deployment strategies, challenges encountered during implementation, and the outcomes of these systems in terms of enhanced security and customer satisfaction. The section will highlight successful deployments and draw valuable lessons from past experiences.

D. PRIVACY AND ETHICAL CONSIDERATIONS:

The use of facial recognition technology raises significant privacy and ethical concerns. In this section, the privacy implications associated with the implementation of facial recognition for bank locker security will be examined. It will emphasize the importance of obtaining user consent, ensuring secure storage of facial data, and complying with relevant privacy regulations. Additionally, ethical considerations such as potential biases within facial recognition algorithms and the responsible use of facial data will be thoroughly addressed.

Integration with Existing Bank Systems:

This section will explore the integration of facial recognition systems with pre-existing bank infrastructure. It will discuss the technical considerations involved, including interoperability with access control systems, and potential challenges associated with seamlessly integrating facial recognition technology into the bank's overall security ecosystem. Best practices and recommendations for successful integration will be provided.

III. FUTURE TRENDS AND RESEARCH DIRECTIONS

The final section will explore emerging trends and research directions in the field of bank locker security systems employing facial recognition. It will delve into advancements in facial recognition algorithms, hardware improvements, and the potential integration of complementary technologies such as machine learning and artificial intelligence. Furthermore, this section will identify promising areas for further research and development in order to advance the capabilities and effectiveness of bank locker security systems using facial recognition technology.

IV. METHODOLOGY

Present-day bank security systems use the mechanical key method in which one key was given to the user and the other one was kept by the bank. That's why a more secure system with image capturing facility that activates, authenticates, and validates the user and only then unlocks the locker.

Step 1: Data Collection

- Here we gather a diverse and representative dataset of facial images with privacy regulations and obtain appropriate consent from individuals whose facial data will be collected.

Step 2: Data Pre-processing

- Then we Implement pre-processing techniques to enhance the quality and consistency of the collected facial images, including noise reduction, alignment, and normalization

Step 3: Facial Recognition Model Selection and Training

- Here we consider factors such as accuracy, speed, robustness to variations in lighting and facial expressions, and compatibility with the available hardware resources.
- Train the selected model using the pre-processed facial images, via CNN algorithm to optimize performance.

Step 4: Building the software

When we first built the facial recognition system for the bank locker security, we followed these steps to integrate it with the locker management system seamlessly and ensure data protection:

i. Identify Integration Points:

We closely analysed the locker management system to determine where the facial recognition system needed to connect with it. This included identifying the stages where authentication and access control processes occur.

ii. Establish seamless database connectivity:

To enable smooth communication between the facial recognition system, the locker management system and the database we developed optimal codebase for minimum to zero downtime.

iii. System Testing and Validation:

Testing and validation were crucial to ensure the integration worked flawlessly. We conducted extensive testing, simulating different scenarios like heavy user loads and network interruptions. This aided us to verify the reliability of the integration and ensure that the facial recognition system accurately identified users and granted them access to lockers as intended.

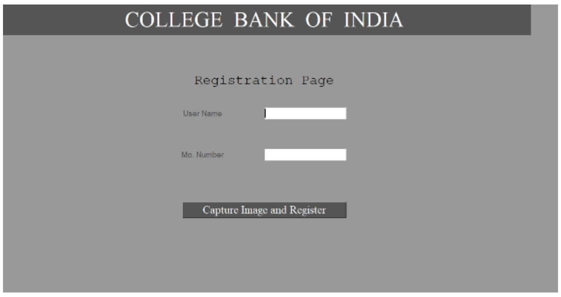
V. SOFTWARE DESCRIPTION

I. The client’s first interaction with the application is during the registration

With the name and his/her mobile number followed by the image capturing step.

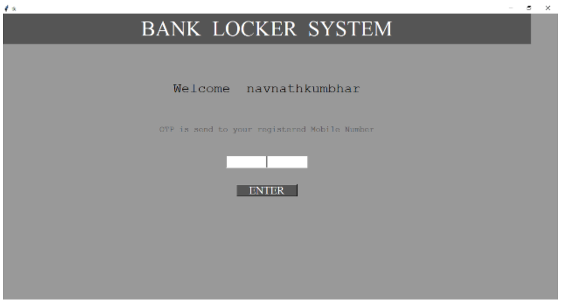
II. In this particular step an OTP is sent on the registered mobile number.

III. Based on this OTP it is decided whether the person is the righteous authority to access the locker or not.



COLLEGE BANK OF INDIA

Registration Page



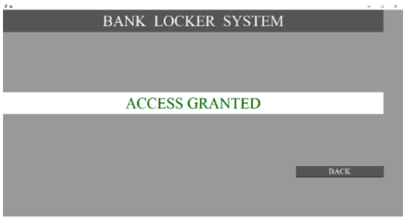
BANK LOCKER SYSTEM

Welcome navnathkumbhar

OTP is send to your registered Mobile Number

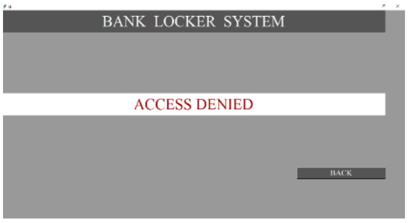
I. In this particular step an OTP is sent on the registered mobile number.

II. Based on this OTP it is decided whether the person is the righteous authority to access the locker or not.



BANK LOCKER SYSTEM

ACCESS GRANTED



BANK LOCKER SYSTEM

ACCESS DENIED

VI. CONCLUSION

In conclusion, the implementation of the bank locker security system using facial recognition technology has proven to be a significant advancement in enhancing the security and convenience of bank lockers. The successful integration of facial recognition technology with the existing locker management system has provided a robust and reliable solution that surpasses traditional authentication methods.

The facial recognition system has demonstrated exceptional accuracy in identifying and verifying customers, granting them secure access to their lockers. By leveraging advanced algorithms and training techniques, the system has effectively adapted to various lighting conditions, angles, and facial expressions, ensuring a seamless user experience.

Looking ahead, ongoing monitoring and maintenance of the facial recognition system will be crucial to ensure its continued effectiveness and adaptability to emerging security challenges. Regular updates and advancements in facial recognition technology should be embraced to further enhance the system's performance and resilience against evolving threats.

VII. REFERENCES

[1]. Kumar, Ajay; Sood, Priyan; Gupta, Utkarsh, “Internet of Things (IoT) for Bank Locker Security System”, (2020) 6th International Conference on Signal Processing and Communication (ICSC), 315–318. doi:10.1109/ICSC48311.2020.9182713

[2]. Chikara, Arvasu, Choudekar, Pallavi; Ruchira, Asija, Divya, “Smart Bank Locker Using Fingerprint Scanning and Image Processing”, (2020) 6th International Conference on Advanced Computing and Communication Systems (ICACCS), (), 725– 728. doi:10.1109/ICACCS48705.2020.9074482

[3]. Sandip Dutta1 Nitin Pandey2 Sunil Kumar Khatri, “Microcontroller Based Bank Locker Security System Using IRIS Scanner and Vein Scanner”, Proceedings of the International Conference on Inventive Research in Computing Applications (ICIRCA 2018) IEEE Xplore Compliant Part Number:CFP18N67-ART; ISBN:978-1-5386-2456-2

[4]. Gusain, Raj; Jain, Hemant; Pratap, Shivendra, “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) -. , (), 1–5. doi:10.1109/IoT-SIU.2018.8519850

[5]. Hossain, Shafayet; Ahmed, Mazid Ishtique; Niaz Mostakim, Md, “A Prototype of Automated Vault Locker Solution for Industrial Application”, (2019) 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT), (), 1– 6. doi:10.1109/ICASERT.2019.8934754

[6]. Nallapa Reddy, Anusha & Sai, A & Srikar, B. (2022). Locker Security System Using Facial Recognition and One Time Password (OTP).

[7]. 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, pp. 1-5, doi: 10.1109/IoT-SIU.2018.8519850.

Cite this article as :

Prof. A .B. Gadewar, Yash D Satre, Saurabh Y Girme, Sagar Walunj, "Bank Locker Authentication System using Facial Recognition", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 3, pp. 286-291, May-June 2023. Available at doi : https://doi.org/10.32628/IJSRSET23103101
Journal URL : https://ijsrset.com/IJSRSET23103101