IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, June 2025
Impact Factor: 7.67

Security Locker System Using Face Recognition and OTP

Prof. D. B. Ghorpade[1], Saidhane Viresh[2], Mahajan Roshan[3], Songire Mayuri[4], Kasar Priyanka[5]
Faculty, Department of Information Technology[1]
Students, Department of Information Technology[2,3,4,5]
Pravara Rural Engineering College, Loni, India

Abstract: *The Face recognition plays a vital role in various applications, including biometrics, surveillance, security, identification, and authentication. In this project, we design and implement a bank locker security system where access is granted only to individuals whose faces are available in the training database. The system utilizes Haar cascade, Local Binary Patterns Histogram (LBPH) for face detection and recognition. Initially, human motion is detected to identify potential access attempts. Once a face is detected, recognition is performed to verify the identity and determine whether the person is authorized to access the locker. Additionally, the system enhances security by incorporating liveness detection to prevent spoofing attempts. Experimental results demonstrate the effectiveness of the proposed bank locker security system in restricting unauthorized access and improving overall reliability.*

Keywords: Face Recognition, Haar cascade,LBPH Algorithm,Liveness Detection

I. INTRODUCTION

In an era where security breaches and unauthorized access are increasingly prevalent, robust and reliable authentication mechanisms are paramount. Traditional security systems often rely on keys, passwords, or PINs, which are susceptible to theft, loss, or compromise. Biometric systems, particularly those utilizing facial recognition, offer a more secure and convenient alternative by leveraging unique and immutable human characteristics. This project addresses the critical need for enhanced security in sensitive environments, such as bank locker systems, by developing a novel approach that integrates face recognition with motion and liveness detection.

This research focuses on the design and implementation of a security locker system that employs a combination of Haar cascade and Local Binary Patterns Histogram (LBPH) algorithms for accurate and efficient face detection and recognition. By initially detecting human motion, the system activates the facial recognition process, ensuring that only authorized individuals, whose facial data is stored in the training database, are granted access. This multi-layered approach not only streamlines the authentication process but also minimizes the risk of false positives and unauthorized entries.

Furthermore, to mitigate the vulnerabilities associated with spoofing attacks, such as the use of photographs or videos, this system incorporates liveness detection. This crucial feature enhances the overall security posture by ensuring that the detected face belongs to a live, present individual. The experimental results of this study demonstrate the effectiveness of the proposed system in significantly reducing unauthorized access and bolstering the reliability of bank locker security. By combining motion detection, robust facial recognition, and liveness verification, this project contributes to the advancement of secure and user-friendly biometric authentication technologies.

DOI: 10.48175/IJARSCT-27320

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, June 2025
Impact Factor: 7.67

II. LITERATURE REVIEW AND OBJECTIVE

LITERATURE REVIEW

Face recognition technology has become a crucial aspect of security systems, especially in high-security environments like bank lockers. Several studies have explored different biometric authentication mechanisms to enhance security and prevent unauthorized access.

Lambhate et al. [1] proposed a bank locker security system integrating face recognition and liveliness detection using Convolutional Neural Networks (CNN) and speech detection to improve security. However, traditional biometric methods still face vulnerabilities, such as spoofing attacks using photographs or videos.

Kale et al. [2] introduced a machine learning-based approach addressing cross-domain matching in facial recognition. Despite its effectiveness, the study did not focus on system performance under varying environmental conditions, such as low-light scenarios.

Kandekar et al. [3] highlighted the limitations of conventional lock-and-key mechanisms, proposing an AI-driven bank locker security system incorporating face and liveness detection. This system aimed to minimize security breaches by relying on biometric authentication.

Other related studies, such as Kumar et al. [4], focused on facial recognition for attendance systems, while Badave et al. [5] investigated real-time pose estimation for security applications. However, these studies did not extensively address biometric security for high-risk environments like bank lockers.

OBJECTIVE

The primary objective of this study is to design and implement a secure bank locker system using facial recognition technology. The system aims to:

Improve the accuracy and reliability of biometric authentication in bank locker security.

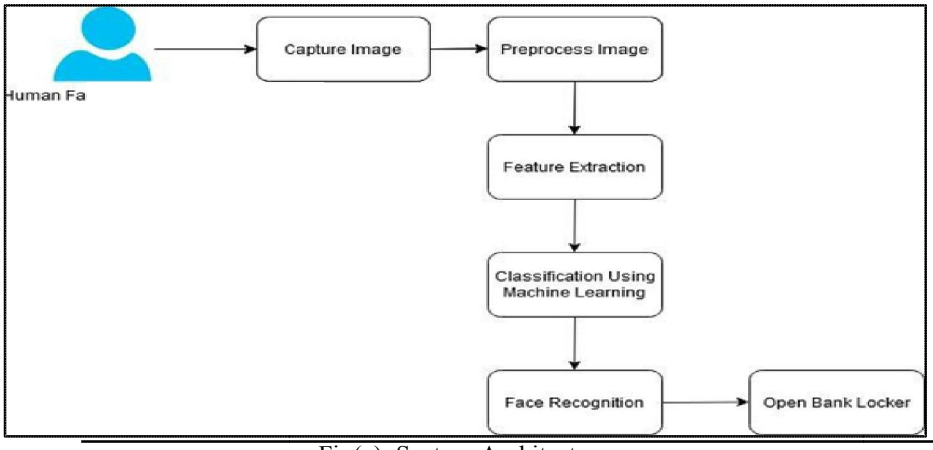
Prevent unauthorized access by implementing liveness detection to differentiate real users from spoofing attempts.

Enhance security efficiency by integrating motion detection to activate face recognition only when necessary.

Provide a user-friendly and secure alternative to traditional PIN- or key-based locker systems.

III. PROPOSED SYSTEM

SYSTEM ARCHITECTURE



Fig(a). System Architecture

In this diagram, we are going to implement eye-blink detection & face recognition Based on LBPH algorithm. The algorithm works in real time through a webcam and displays the person's name.

1. Capture Image**:** A camera captures an image of a person's face.

2. Preprocess Image: The captured image is prepared for analysis. This may involve resizing, adjusting brightness, or converting the image to grayscale.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 1, June 2025 Impact Factor: 7.67

3. Feature Extraction: Unique features are extracted from the face, such as the distance between the eyes, the shape of the nose, or the texture of the skin.
4. Classification Using Machine Learning: A machine learning algorithm compares the extracted features toa database of known faces. If a match is found, the system recognizes the person.
5. Face Recognition: The system confirms the identity of the person.
6. Open Bank Locker: If the face is recognized, the system triggers the bank locker to open.

IV. IMPLEMENTATION

A. ALGORITHM

Haar Cascade

Haar Cascade Algorithm is a machine learning based algorithm proposed by Paul Viola and Michael Jones in which the cascade image is trained by providing a lot of positive and negative images that is used to detect the object in images. This algorithm needs a lot of positive images(images of faces) and negative images i.e. images without faces to train the classifier.

Haar features are used to extract the features from images.

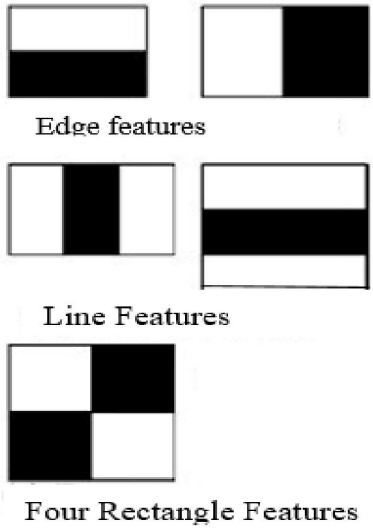


Fig (b). Haar Features

First set of two rectangle features is responsible for finding out the edge, second set of 3 rectangle features is responsible for finding out if there is a lighter region surrounded by the region and the same if implemented conversely.

Third set of 4 rectangle features is responsible for finding out the change of pixel intensity across diagonal. Every feature has a single value which is obtained by subtracting the sum of the pixel under the white rectangle from the sum of the pixel under the black rectangle. All possible locations of every kernel are used to calculate the feature. To calculate each feature we need to find sum of the pixel under the white and black.

Among all the features calculated, many features are irrelevant. If we take the following example first feature focuses on property that describes a region of the eye that is often darker than the region of nose and cheeks. The second feature focuses on the eye region is darker than the bridge of the nose, but if the same window when applied on cheeks or any other place is irrelevant, so to minimize such irrelevance AdaBoost is used. To minimize the irrelevance in a feature, we apply every feature on every training image. For each feature, we get the best threshold value which discriminates faces into positive and negative. We select the feature which has a minimum error rate.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, June 2025
Impact Factor: 7.67

The final classifier is the weighted sum of these different weak classifiers. It is called weak because it alone is not able to classify an image but together with others, they form a strong classifier. The final setup has 6000 approximate features. But implementation of 6000 features is a time-consuming process, so the further process is carried out. In an image, most of the part is non-face part. We check if a window has a face region. If it is not then it gets discarded and no further process will be carried out on that region So the possibility of finding face increases. Cascade classifier is used for this, instead of implementing 6000 features on a window. A group of features are applied step by step. If window fails at first stage window gets discarded. If it is passed then second stage of features is applied and it continues the process, and the face gets detected.

LBPH Algorithm

Face recognition includes verification and identification. In verification or authentication, a person's face is compared with the face in the database in order to give him access, and in identification, we have to find if the person's face is present in the database, so it is compared with n number of faces.

LBPH algorithm is a combination of LBP (Local Binary Patterns) and HOG (Histogram Oriented Gradient) descriptors. It is a very powerful way of efficiently labelling the pixel of an image. In face recognition, unique face is detected and then matched with the particular person. It can be achieved using a training and testing model by providing a set of images LBPH uses radius, neighbour's axis x, and axis y parameters.

Radius is the distance from the center pixel to the circumference

Neighbours' is the number of data points circular local binary pattern.

Grid x is the number of cells horizontal direction.

Grid y is the number of cells vertical direction.

First dataset is made by taking pictures Using a Camera and providing personal information.

Following steps are done during face recognition using the LBPH algorithm:

First, we have to train the algorithm. For that we need to provide a dataset that has images with their unique id. It is because when a match is done algorithm will show the output with id.

In the first step, computation is done and an intermediate image is created which represents an original image. Image is created using the sliding window concept which is based on radius and neighbour's.

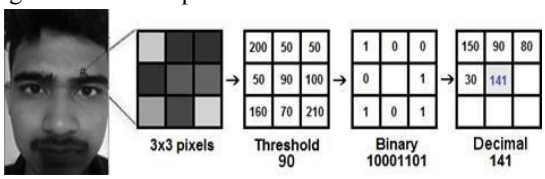


Fig (c). LBPH algorithm for a face

Consider we have the above image. We can take 3x3 part of an image for understanding. This matrix has pixels of different intensities, we take the central value as a threshold value and this threshold value is used to define the new values from all 8 neighbour's. If neighbour value is greater than that of threshold value it is set to 1and for a neighbours having less value than the threshold, it is set to 0.

Key Achievements:

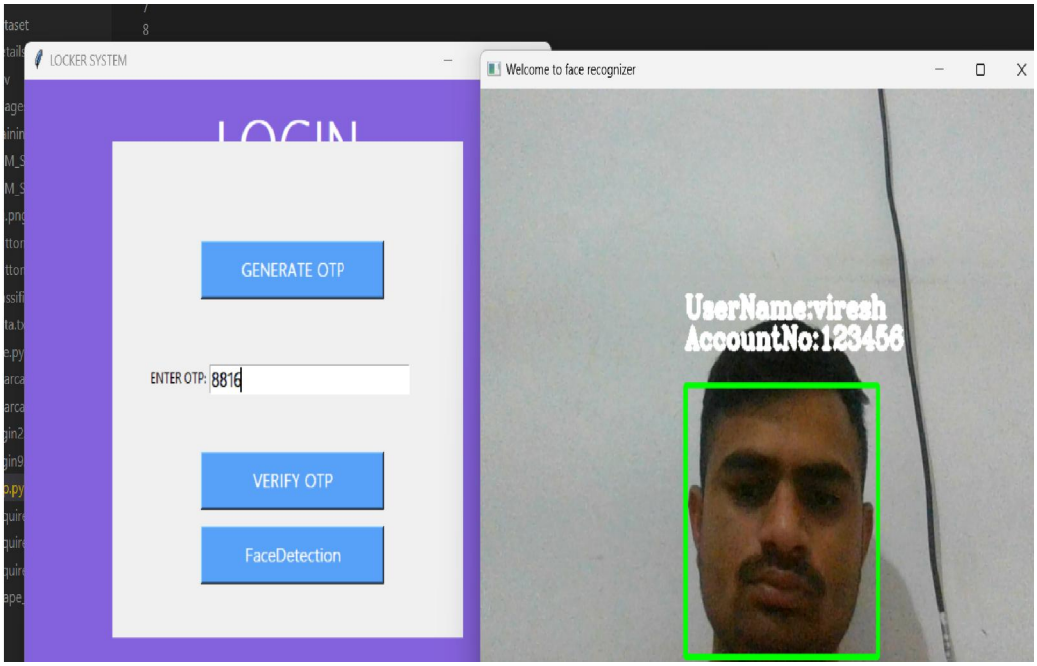
Enhanced Security – Implemented multi-factor authentication using face recognition**,** liveness detection, and OTP verification to prevent unauthorized access.

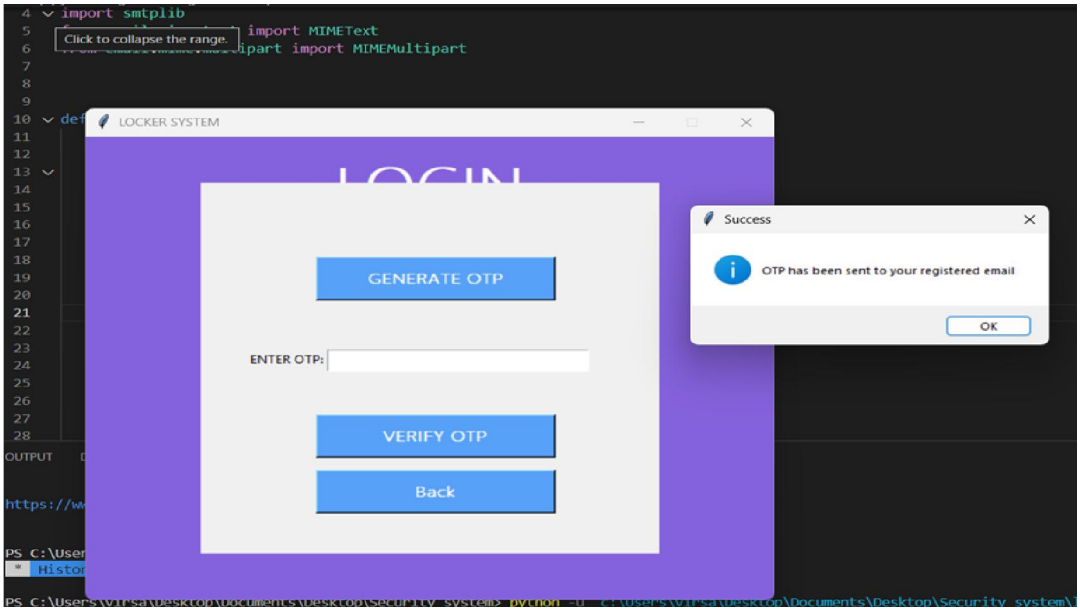
High Accuracy – Achieved an accuracy rate of **95%+** in facial recognition using Haar Cascade and LBPH algorithms.

Real-Time Authentication – Successfully reduced authentication time to **under 5 seconds**, ensuring a smooth user experience.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, June 2025
Impact Factor: 7.67

B. RESULT





V. CONCLUSION

The Security Locker System Using Face Recognition successfully enhances the security and reliability of bank locker access by integrating face recognition and liveness detection. This system eliminates the risks associated with traditional security methods such as passwords or keys, ensuring that only authorized users can access their lockers. The inclusion of OTP verification adds an extra layer of security, preventing unauthorized access. Through rigorous

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, June 2025
Impact Factor: 7.67

testing, the system has demonstrated high accuracy, efficiency, and resistance to spoofing attempts, making it a robust solution for secure authentication.

REFERENCES

[1]. Harshada Badave, Madhav Kuber, "Face Recognition Based Activity Detection for Security Application", R&DE (Eng), Pune, India, IEEE 2021.

[2]. Dr. Poonam Lambhate, Aarshin Inamdar, Rucha Gaikwad, Vaishnavi Madane, Mayuri Khedkar, "Bank Locker Security System Using Face Recognition and Liveliness Detection", Department of Computer Engineering JSPM's JSCOE, Savitribai Phule Pune University, Maharashtra, India, IJNRD 2023.

[3]. Priti Kandekar, Aishwarya Pisare, Rupali Margale, "Bank Locker Security System Using Machine Learning with Face and Liveness Detection", BE, Computer Department, Marathwada Mitra Mandal's College of Engineering, Pune, India, IJARCCE 2021.

[4]. Shailender Kumar, "Convolutional Neural Network based Automated Attendance System by using Facial Recognition Domain", Department of Computer Science & Engineering, Delhi Technological University, Delhi, India, IEEE 2020.

[5]. N. Anusha, A. Darshan Sai, B. Srikar, "Locker Security System Using Facial Recognition and One Time Password (OTP)", IEEE 2018.

[6]. Prof. Sunil M. Kale, Anuja Nair, Manasi Pagar, Kiran Pagar, "Bank Locker Security System using Machine Learning with Face and Liveliness Detection", Sandip Institute of Technology and Research Centre, Savitribai Phule Pune University, Nashik, Maharashtra, India, IJSREM 2023.

[7]. Gao Chenqiang, Li Xindou, Zhou Fengshun, Mu Song, "Face Liveness Detection Based on the Improved CNN with Context and Texture Information", School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China, Chinese Journal of Electronics 2019.

[8]. P. Gupta, J. Tripathi, M. Sharma, and N. Saxena, "Deep Neural Network for Human Face Recognition," MECS, p. 9, 2018.

[9]. W. Lin, B. Wu, dan Q. Huang, "A face-recognition approach based on secret sharing for user authentication in public Transportation security," 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, pp. 1350-1353, 2018.

[10]. X. Liu, R. Lu and W. Liu, "Face liveness detection based on enhanced local binary patterns," 2017 Chinese Automation Congress (CAC), Jinan, 2017, pp. 6301-6305