Archives available at journals.mriindia.com

International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2278-5140
Volume 14 Issue 01, 2025

Smart Bank Locker Using Finger Print Scanning

Ms. Sneha Bankar[1], Shubham Sutar[2], Siddheshwar kadam[3], Omkar Navsupe[4], Pandurang More[5]

Assistant Professor, U.G. Student, Department of Artificial Intelligence and Data Science, Dr. D. Y. Patil College of Engineering and Innovation

Peer Review Information

Submission: 21 Feb 2025
Revision: 25 March 2025
Acceptance: 30 April 2025

Keywords

Biometric
KNN
CNN
SVM
Bank Locker
Authorised Person

Abstract

In the banking industry, security is a top priority, particularly when it comes to protecting personal lockers. Conventional techniques that use keys or PINs are becoming more and more susceptible to hacking and theft. This study examines the use of biometric fingerprint identification as a reliable substitute, examining current systems, their architectures, benefits, and drawbacks. Banks are implementing biometric authentication systems in response to the increase in security breaches. The distinctiveness and simplicity of fingerprint recognition make it stand out. The use of fingerprint-based methods to improve locker security is examined in this research .The conventional key-based bank locker system has been improved with the fingerprint-based method .Nowadays, security is crucial everywhere. Security is the top priority, particularly in banks. Conventional keys are easily copied. We have so many smart lockers available in market, but all they are very expensive. Here we are providing system to solve this. The name the system is bank locker system using finger print security.

INTRODUCTION

Safe deposit boxes are the safest place to store valuables like jewelry, cash, vital documents, etc. since in the real world, people are more worried about their safety. Users can now operate high security systems with electronic identification alternatives thanks to the introduction of quickly expanding technology.These identity technologies, which are unfortunately not secure against hacker attacks, theft, and forgotten passwords, include safe deposit boxes, automated teller machines, other smart cards, user IDs, and password-based systems, among others. These systems still have all of these flaws, failures, malfunctions, and breakdowns, but the most effective and dependable way to ensure stringent security is through biometric or fingerprint verification. Biometrics measures a person's unique physical characteristics to recognize or authenticate their. Raghu Ram.Gangi (2013) and others have given a proposal for fingerprint verification of the security system of automatic teller machines using biometrics with hybridization. The fingerprint function was selected because to its great precision, dependability, and availability. The
identification of the fingerprint. Physical traits include signatures, voice keystroke patterns, and fingerprints of the hand, face, iris, etc. Both identification and verification modes are used by biometric systems. In verification mode, the system compares the biometric template that was collected and previously stored in the system database to confirm an individual's identity. In the conventional locker security identification mode, the system identifies a user by looking through the whole template database for matches. It then makes one of several comparisons to ascertain the user's identity, or it fails if the user is not the one registered with the

system. Therefore, in order to increase the security of traditional lockers, our project uses a fingerprint security method.

LITERATURE SURVEY

Gender classification using the same iris code used for identification **(J. Tapia, C. Perez**). The initial step in this investigation was to reliably establish gender using the binary iris code that could be utilized for identification. The author claims that rather than being concentrated in discrete concentric rings, the data used to predict gender is distributed throughout the iris. They discovered that utilizing features that only represent a section of the iris region improves accuracy when compared to using features that represent the entire iris region. The author 3 chose iris code bits to be used as gender characteristics by employing mutual information measures as a guiding prediction. This technique, along with person-disjoint training and testing evaluation, can accurately predict gender by combining the best elements of the iris codes from the left and right eyes.

A. Verma: A Bank Security System with Multiple Layers One way to verify, monitor, and control the security at bank storage rooms is with a multi-layer bank security system. Nowadays, a lot of banks employ the approved access control strategy to prevent unwanted entry to the changing area. The most dependable, multi-level, and efficient locker room security system has been created thanks to this effort. The system includes a biometric component that controls the security of the front door to the locker room using devices like an iris scanner and a fingerprint reader. It also features an RFID system that restricts access to the dressing room area to approved individuals only. Unauthorized visits are monitored in the locker room area using a stationary passive infrared monitor.

In the event of any unauthorized motion, the camera's picture will be mailed to security authorities, and the alarms will sound to notify local security.

"Using Face Recognition, Iris Scanner, and Palm Vein Technology to Enhance Bank Security System," by **R. Gusain, H. Jain, and S. Pratap.** This article's goal is to create a bank locker security system that protects valuables by utilizing facial recognition, iris scanning, and palm vein technology (PVR). Facial recognition systems employ MATLAB software to recognize and verify the authorized user's image. The camera captures images of anyone entering an unrestricted area, and a computer program compares those images to a database of approved individuals. The iris detecting technology utilizes the unique physical characteristics of humans. This technique is used for biometric authentication in a number of locations, such as ATMs, immigration and border control, public safety, hospitality, and tourism. A method known as palm vein recognition (PVR) analyses a user's palm vein pattern and compares it to information kept in a database in order to confirm their identity.

Based on quadrature discriminant analysis, **D. Akila, S. Jayalakshmi, R. Jaya Karthik, S. Mathivilasini**, and **G. Suseendran** conducted a study on biometric authentication using finger vein images. Biometric authentication has long been utilized in high-security applications such as private places and bank lockers. Here, analysis of a person's iris, finger print, etc., can provide information about their physiological traits. The innovative method for four biometric recognitions includes finger vein identification. Here, a user can be authenticated for access to high-security apps using the vein patterns on their fingers. The purpose of this study is to use quadrature discriminant analysis to locate veins in the fingers. Pretreatment techniques are applied to finger vein pictures in order to improve the image's stability for subsequent processing. The Minimal Distance Classifier was used after the QDA procedure.

A. Natarajan and N. Shanthi: An Overview of Template Protection and Multimodal Biometric Authentication. The market for security systems is dominated by biometric systems. The majority of applications, including as attendance and locker restrictions at establishments like banks and hospitals, utilize biometric technology. In addition to the authentication that these biometric systems offer, the templates that are kept there also need to be secured. This paper gives an overview of many biometrics, including fingerprints, faces, hand veins, iris, and signatures, as well as authentication, fusion, and template protection techniques. Several characteristics and behaviours are examined in order to determine the most unique and useful approaches for biometric identification and template protection. This study also includes a comparison of the unimodal and multimodal biometric systems.

Secure biometric-based access to the bank safety lockers was verified by **S. Sridharan**. The main goal of this paper is to provide a safe, reliable, and easy-to-use system for bank customers who own lockers as well as the branch head's participation in all activities related to the safety lockers. This paper's main objective is to offer a solution for a comprehensive biometric-based authentication system for safety locker operation. With the use of two separate keys—one belonging to the branch head and the other to

the user—all lockers currently operate. This solution aims to improve that situation. It is suggested that the present paradigm, which mostly depends on the user's key, be improved in order to support the locker's operation using biometrics and a secret code (password). The two-level authentication—one by the branch head and one by the user for their identities—secure individual authentication using their biometrics, and granting access to their safety lockers exclusively to the relevant individuals are the primary aspects of the new system. The central regional office of that bank assigns the branch head in charge of managing the safety deposits on a daily basis.

METHODOLOGY

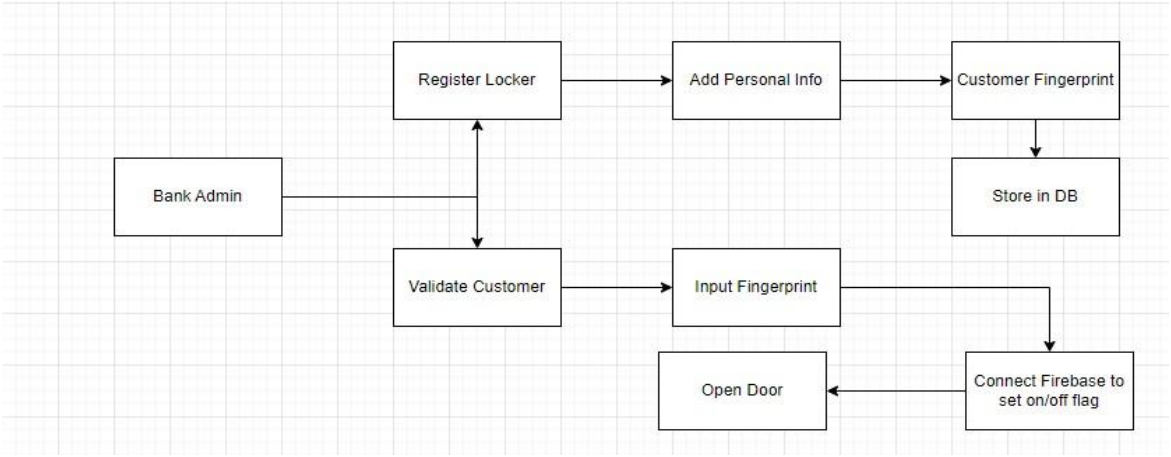


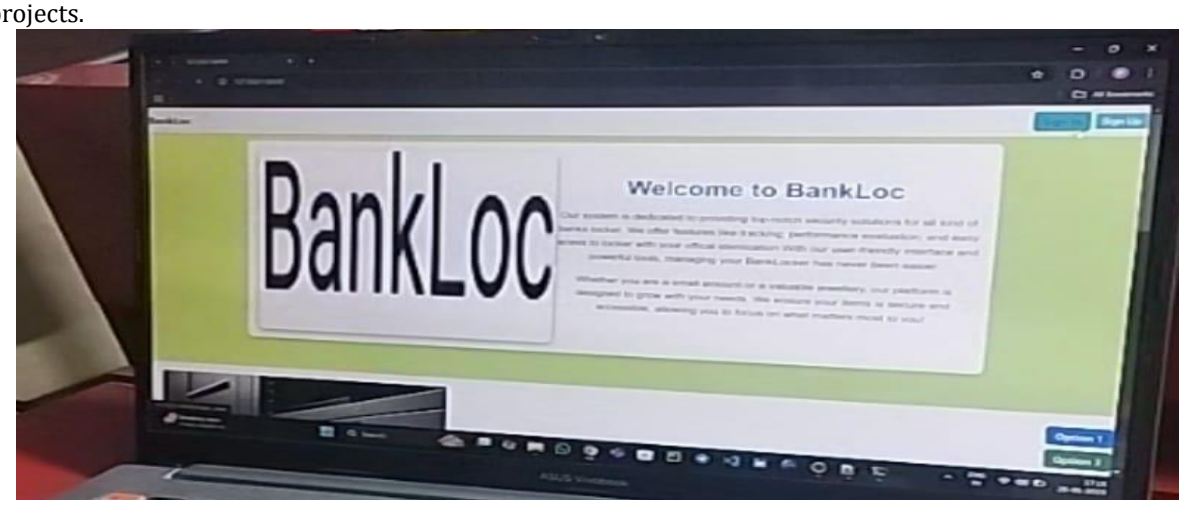
Fig 1. Methodology Diagram

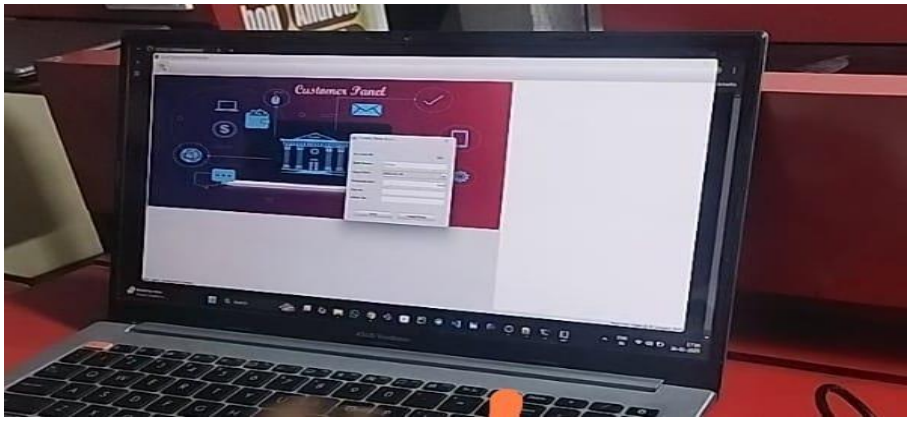
We will implement
Module 1: User Registration and Login will be implemented. Module 2: View or update the record Module 3: Fingerprint Matching. Set a flag on Firebase if it matches.
Module 4: If a fingerprint matches, the user's door will open.
The bank administrator will register the user and fill out personal data. We'll use your fingerprint as input. The user's fingerprint will be inserted whenever they wish to access a door.
A minute-based technique will be used; if the fingerprints match, a firebase flag will be set to open. Every time the status is set to open, the hardware will sense the firebase continually and open the door.
Only those with permission can use their fingerprints to enter the bank locker door in these projects.

First, we must click the enroll button to save our finger prints in the module. The user must hold down their finger while accessing the module and then hit the identification button. The door will be open for authorized finger prints. The door will be closed if the same fingerprint is found there again.

EXPERIMENTAL RESULTS

The purpose of this project In order to address the security issues that arise from using a single security system, the goal of this project is to provide a high-level security system that uses a fingerprint sensor in the locker. Additionally, the system will be designed to be more costeffective, efficient, and secure.





CONCLUSION

A very safe and practical replacement to traditional key-based systems are biometric bank lockers. They offer quicker access and improved fraud prevention while removing the dangers of misplaced keys and forgotten PINs. To guarantee dependability and consumer confidence, however, issues like exorbitant prices, privacy issues, and technological malfunctions must be resolved.

The future of biometric lockers is bright despite these limitations, particularly with developments in multi-factor authentication, AI-driven security, and encrypted biometric storage. Biometric technology has the potential to transform bank security and improve consumer satisfaction with the correct protections.

References

M. Bertalmio, G. Sapiro, V. Caselles, and C. Ballester, “Image inpainting”, in Proc. SIGGRAPH, pp. 417–424, 2000.

A. Criminisi, P. Perez, and K. Toyama, “Region filling and object removal by exemplar-based image inpainting.”, IEEE Transactions on Image Processing, vol. 13, no.9, pp. 1200–1212, 2004.

Marcelo Bertalmio, Luminita Vese, Guillermo Sapiro, Stanley Osher, “Simultaneous Structure and Texture Image Inpainting”, IEEE Transactions On Image Processing, vol. 12, No. 8, 2003

.

Yassin M. Y. Hasan and Lina J. Karam, “Morphological Text Extraction from Images”, IEEE Transactions On Image Processing, vol. 9, No. 11, 2000

Eftychios A. Pnevmatikakis, Petros Maragos “An Inpainting System For Automatic Image Structure-Texture Restoration With Text Removal”, IEEE trans. 978-1-4244-1764, 2008

S.Bhuvaneswari, T.S.Subashini, “Automatic Detection and Inpainting of Text Images”, International Journal of Computer Applications (0975 – 8887) Volume 61– No.7, 2013

Aria Pezeshk and Richard L. Tutwiler, “Automatic Feature Extraction and Text Recognition from Scanned Topographic Maps”, IEEE Transactions on geosciences and remote sensing, VOL. 49, NO. 12, 2011

Xiaoqing Liu and Jagath Samarabandu, “Multiscale Edge-Based Text Extraction From Complex Images”, IEEE Trans., 1424403677, 2006

Nobuo Ezaki, Marius Bulacu Lambert , Schomaker , “Text Detection from Natural Scene Images: Towards a System for Visually Impaired Persons”

, Proc. of 17th Int. Conf. on Pattern Recognition (ICPR), IEEE Computer Society, pp. 683-686, vol. II, 2004

Mr. Rajesh H. Davda1, Mr. Noor Mohammed, " Text Detection, Removal and Region Filling Using Image Inpainting", International Journal of Futuristic Science Engineering and Technology, vol. 1 Issue 2, ISSN 2320 – 4486, 2013

Uday Modha, Preeti Dave, " Image Inpainting-Automatic Detection and Removal of Text From Images", International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622 Vol. 2, Issue 2, 2012

Muthukumar S, Dr.Krishnan .N, Pasupathi.P, Deepa. S, "Analysis of Image Inpainting Techniques with Exemplar, Poisson, Successive Elimination and 8 Pixel Neighborhood Methods", International Journal of Computer Applications (0975 – 8887), Volume 9, No.11, 2010