STM JOURNALS

International Journal of
VLSI Circuit Design & Technology

Volume 2, Issue 1, 2024
DOI (Journal): 10.37591/IJVCDT
(Jan-June)

https://journals.stmjournals.com/ijvcdt

Review IJVCDT

Bank Locker Security System Using Machine Learning

Prajakta Medhekar[1], Mandar Shahane[2], Karan Rajiwade[3,*], Rohit Gadhave[4], B.M. Borhade[5]

Abstract

The Bank Locker Security System integrates cutting-edge technology solutions to strengthen the security of bank locker facilities. This system uses biometric identification techniques, such as facial recognition and fingerprint scanning, to confirm users' identities before granting them access to the lockers. Furthermore, access control techniques based on RFID technology are employed to augment security protocols. The locker area is equipped with real-time monitoring and alerting tools that enable fast detection of any unauthorized access attempts or suspicious actions. The Bank Locker Security System uses these technologies to reduce the possibility of theft or unauthorized entry while offering clients a quick and safe way to access their goods kept in bank lockers. With this method, consumers' assets are protected and their confidence in financial services is increased overall. It is a huge breakthrough in bank security measures.

Keywords: Machine Learning, user authentication, bank locker, Rfid, biometric.

INTRODUCTION

Even while biometric systems are becoming more and more common and perform pretty well for many applications, a great deal of work is still required to enable the design of practical, safe, and private systems. The same earlier attack methods in face recognition are additionally divided into multiple groups. The idea of classification is based on the verification evidence provided to the face verification system, such as different types of stolen icons, images of stolen faces, recorded videos, 3D face models with expressive lips and blinking, and 3D face models with a range of expressions. The idea behind classification is based on the verification evidence provided to the face verification system, which includes a range of stolen icons, images of stolen faces, recorded videos, 3D face models with expressive lips and blinking, 3D face models with different expressions, and so forth. In order to fend off the attack using a photo, we will be projecting live face detection techniques throughout this work. Regarding the types of verification proof that the face verification system offers, these include a range of stolen icons, images of stolen faces, recorded videos, 3D face models with expressive lips and blinking, and 3D face models with a range of expressions. The idea behind classification is based on the verification evidence provided to the face verification system: completely distinct expressions akin to a pilfered icon, pilfered face photos, recorded videos, 3D face models possessing the ability to move their lips and blink, 3D face models with a variety of expressions, and so forth. Due to QR codes' benefits over barcodes, they are now widely used worldwide. Compared to barcodes, QR codes have the advantage of being able to store enormous amounts of data. The QR code contains data that may be accessed both vertically and horizontally. QR code error correction makes it possible to read data that has been damaged. Data may be read in all directions thanks to pattern recognition, which is in each of the QR code's three corners. There are various QR code variants, ranging from V1 to V40.

***Author for Correspondence**
Karan Rajiwade
E-mail: karanrajiwade1020@gmail.com

[1-4]Student, Department of Computer Engineering, RD' Shri Chhatrpati Shivajiraje College of Engineering, Dhangwadi, Bhor, Pune, Maharashtra, India
[5]HOD, Department of Computer Engineering, RD' Shri Chhatrpati Shivajiraje College of Engineering, Dhangwadi, Bhor, Pune, Maharashtra, India

Received Date: June 19, 2024
Accepted Date: June 25, 2024
Published Date: July 03, 2024

Citation: Prajakta Medhekar, Mandar Shahane, Karan Rajiwade, Rohit Gadhave, B.M. Borhade. Bank Locker Security System Using Machine Learning. International Journal of VLSI Circuit Design & Technology. 2024; 2(1): 16–20p.

The module size of version V40 is 177×177, while version V1 has a module size of 21×21. The type of data and the amount of data that needs to be encoded define which version of the QR code is utilized in the application. While there are several security requirements for QR codes, there are very few for 2L QR codes. The ability to recover private messages and the possibility of authentication attacks are drawbacks of the current standards [1, 2]. We presented a method in this work that guards against authentication and message recovery attacks on private messages. The Bank Locker Security System was created in response to the pressing requirement that financial establishments strengthen security protocols, particularly about protecting valuables stored in lockers at banks. Because security threats are becoming more sophisticated, previous methods of securing lockers are no longer sufficient, necessitating the use of cutting-edge technical solutions. This system aims to solve these problems by utilizing cutting-edge technologies like biometric authentication, RFID-based access management, and real-time monitoring. By putting these components in place, the Bank Locker Security System hopes to provide a robust barrier against theft, fraud, and unauthorized entry attempts. Furthermore, the system aims to enhance consumers' overall satisfaction and confidence in banking services by offering a seamless and user-friendly locker access experience. To ensure the privacy and security of valuables stored on bank property, security systems for bank lockers are crucial. These systems guard the contents of the lockers against theft, unlawful entry, and environmental dangers using a variety of technologies and protocols [3].

A bank locker security system's core elements are often robust physical components like premium steel vaults, reinforced doors, and tamper-resistant locking systems. Modern systems have advanced electronic security mechanisms built in to give even greater security.

Banks can efficiently monitor and regulate who has access to lockers by implementing electronic access control systems. This means keeping track of entry and exit hours and implementing dual-key access policies that require multiple authorizations before unlocking lockers [4].

Furthermore, advances in machine learning and artificial intelligence have made it possible for banks to employ anomaly detection algorithms and predictive analytics, which enhances the security of locker facilities.

LITERATURE SURVEY

Arvasu Chikara [6] et al. have developed a smart locker designed for the banking sector. A key feature of this innovation is its capability to track the time, date, and frequency of locker accesses by bank users. The system incorporates biometric scanning equipment, addressing potential issues related to false positives or negatives during the authentication process.

Raj Gusain [7] et al. aim to develop a sophisticated bank locker security system that ensures asset security through the use of MATLAB software, Face Recognition, Iris Scanner, and Palm Vein Technology (PVR). The system employs the image of an authorized user for authentication. During the face recognition process, achieving proper lighting and positioning is essential for accurate scanning and identification.

Abdelrahamn Ashraf Mohamed [8] et al. explore facial recognition as a prominent biometric technique widely adopted across various fields, including mobile device authentication. Their study utilizes CNN technology, which, while effective for face liveness detection, demands significant processing power and computational resources.

Ajay Kumar [9] et al. aim to develop a robust security system for bank lockers, enabling remote monitoring of events and capturing critical frames as needed, facilitated by sensors. The implementation involves leveraging the Internet of Things (IoT), acknowledging potential technological challenges and system failures that may arise.

Yogesh Jadhav [10] et al. highlight face recognition as a straightforward method for distinguishing someone's identity based on their facial features. This personal identification technique utilizes machine learning technology to analyze unique facial characteristics. However, the system may encounter challenges such as misidentifying someone as unauthorized or failing to recognize an authorized person due to variations in facial expressions, lighting conditions, or obstructions like masks or spectacles.

PROPOSED SYSTEM

This suggested technique leverages the human face to recognize various facial expressions. There are several ways to identify the face image. Real-time systems can simply be integrated with this technology. The system briefly displays face detection, image processing, and webcam picture capturing methods. A small number of outcomes are identified.

The proposed machine learning (ML) bank locker security system will make use of proactive anomaly detection, continuous learning algorithms, and personalized authentication in an effort to upgrade security procedures. By employing real-time suspicious activity detection, restricting locker access to authorized users through sophisticated biometric verification, and adapting to evolving security threats, the system's incorporation of machine learning (ML) will increase security. This dynamic approach guarantees consumers that valuables stored in bank lockers will be adequately safeguarded by putting in place efficient and seamless access methods. When considered as a whole, the proposed system represents a significant advancement in bank locker security due to its dependable, adaptable, and user-focused solutions.

Application

Only one authenticated user may access the lockers because faces are kept on file to maintain each person's distinct identity.

It is feasible to add more banking services to the System. System Architecture is Shown in Figure 1 You can improve security by blocking unauthorized access by doing this.

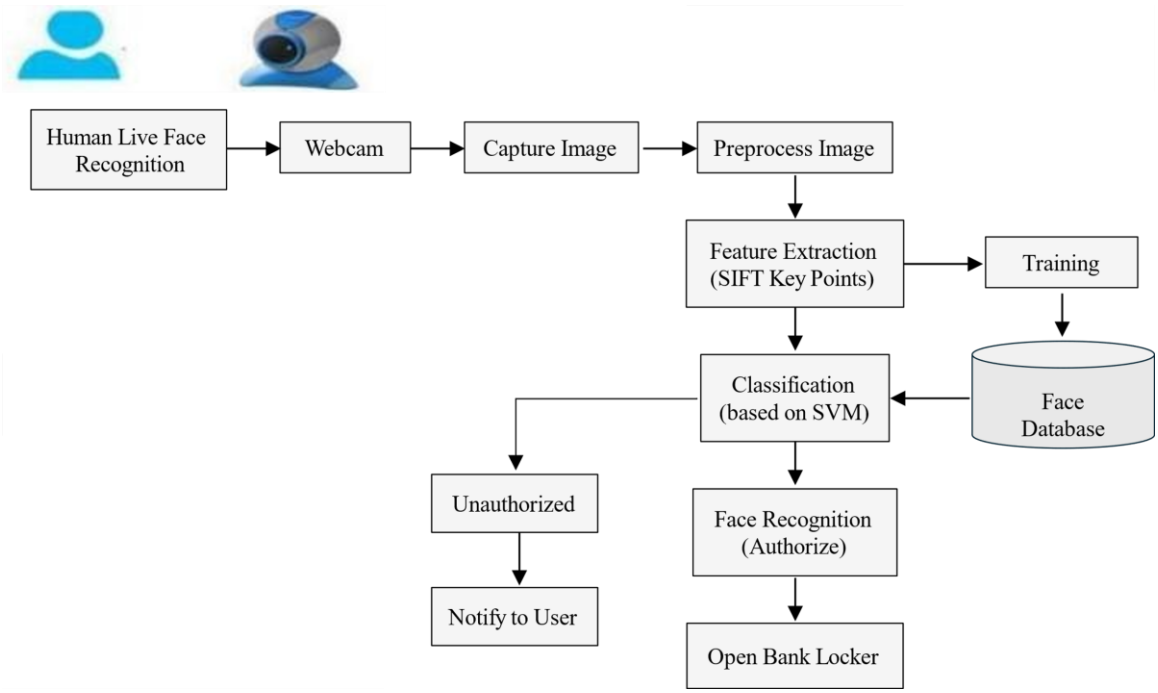

Figure 1. System Architecture.

System Architecture

ALGORITHM

Harr cascade Algorithm

The Haar cascade algorithm, also known as the Haar cascade classifier, is a machine learning-based object detection method. It is frequently used to recognize objects—especially faces—in pictures or video feeds. The approach works by using a set of pre-trained classifiers, which are essentially a set of fundamental Haar-like qualities. These attributes can be used to find patterns in the image that correspond to the specified object. The precision and efficacy of the Harassed method in object recognition are well known in real-time applications.

The technique primarily relies on machine learning, wherein a vast array of both positive and negative images is utilized to educate a cascade function. The training data is then utilized to identify the objects in the remaining images. Huge, distinct.xml files, each with a large feature set and corresponding to a certain use case type, are used to achieve this. We will try to recognize faces in this use-case by employing the haarcascade frontal face. We have shrunk the photo from its original, extremely huge proportions to get better results.

MATHEMATICAL MODEL

Let S be the Whole System S= {I, P, O}

In this context, S represents the entire system, which consists of three main components: I, P, and O

I = Input

P = Procedure O = Output Where,

I = This component represents the input or data that is provided to the system. It could be any information or variables that the system needs to process or analyze.

P = This component represents the processing, or operations performed on the input data. It involves applying algorithms, mathematical models, or any other techniques to transform the input into meaningful output.

O = This component represents the output, or results generated by the system. It could be any information, analysis, or conclusions derived from the processing step.

Input (I)
I = {Face Data}

Procedure (P)
P = {Apply Harcascade Algorithm for Face Recognition} Output (O)

O = {Detect Person is authentic or not}

CONCLUSION

In conclusion, the use of machine learning into bank locker security systems has ushered in a new era of proactive and adaptive protection. Machine learning (ML) enhances the effectiveness of security measures using intricate algorithms for continuous learning, individualized authentication, and anomaly detection. By streamlining access processes, this strategy improves user experiences while fortifying defenses against new threats. Security systems will always be able to adapt to new threats and provide strong protection for valuables kept in bank vaults since machine learning is dynamic. Applying machine learning is therefore a big step toward providing banks and customers with more security and comfort. Predictive analytics and machine learning (ML) have the potential to be used to bank locker security systems for proactive threat reduction and anomaly identification. Machine learning approaches will improve biometric authentication by including sophisticated

elements such as gait analysis and face dynamics. To reduce false positives and maximize security measures, ML-powered systems will also provide customized security rules based on user behavior patterns. In addition to improving user experiences via seamless access control methods, ongoing education and machine learning model modification will ensure that protection against possible threats advances. Machine learning (ML) has the potential to drastically change bank locker security because of its proactive, adaptable, and user-focused solutions.

REFERENCES

1. Lin WH, Wu BH, Huang QH. A face-recognition approach based on secret sharing for user authentication in public-transportation security. In2018 IEEE international conference on applied system invention (ICASI) 2018 Apr 13 (pp. 1350-1353). IEEE.
2. Gusain R, Jain H, Pratap S. Enhancing bank security system using face recognition, Iris scanner and palm vein technology. In 2018 3rd international conference on internet of things: smart innovation and usages (IoT-SIU) 2018 Feb 23 (pp. 1-5). IEEE.
3. Wijaya IG, Husodo AY, Arimbawa IW. Real time face recognition based on face descriptor and its application. TELKOMNIKA (Telecommunication computing Electronics and control). 2018 Apr 1;16(2):739-46.
4. Liu X, Lu R, Liu W. Face liveness detection based on enhanced local binary patterns. In2017 Chinese Automation Congress (CAC) 2017 Oct 20 (pp. 6301-6305). IEEE.
5. Chikara A, Choudekar P, Asija D. Smart bank locker using fingerprint scanning and image processing. In2020 6th international conference on advanced computing and communication systems (ICACCS) 2020 Mar 6 (pp. 725-728). IEEE.
6. Gusain R, Jain H, Pratap S. Enhancing bank security system using face recognition, Iris scanner and palm vein technology. In2018 3rd international conference on internet of things: smart innovation and usages (IoT-SIU) 2018 Feb 23 (pp. 1-5). IEEE. Abdelrahamn Ashraf Mohamed, "Face Liveness Detection Using a sequential CNN technique" [2021].
7. Kumar A, Sood P, Gupta U. Internet of things (IoT) for bank locker security system. In2020 6th International Conference on Signal Processing and Communication (ICSC) 2020 Mar 5 (pp. 315-318). IEEE.
8. Vishwakarma M, Gite R, Katyare B, Kokane P, Sabale RP. Bank Locker Protection with Liveness Detection Using Machine Learning.
9. Tiwari S. An introduction to QR code technology. In 2016 international conference on information technology (ICIT) 2016 Dec 22 (pp. 39-44). IEEE.
10. Tkachenko I, Puech W, Destruel C, Strauss O, Gaudin JM, Guichard C. Two-level QR code for private message sharing and document authentication. IEEE Transactions on Information Forensics and Security. 2015 Dec 8;11(3):571-83.

