IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2024

DOI: 10.17148/IJARCCE.2024.13925

Smart Bank Locker Using Finger Print Scanning

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

Department of Artificial Intelligence & Data Science,

Dr. D. Y. Patil College of Engineering and Innovation[1-5]

Abstract: The fingerprint based bank locker system is an enhancement to the traditional bank locker system that uses keys. Now a day security is very important in everywhere. Especially in Banks security is primary concern. Traditional keys can easily copy. We have so many smart lockers available in market, but all those are very expensive. Here we are providing system to solve this. The name the system is bank locker system using finger print security.

Keywords: Biometric,KNN,CNN,SVM,Bank Locker,Authorised Person.

I.INTRODUCTION

In the real world, people are more concerned about the safety of their valuable things like jewelry, money, important documents, etc. which is why safe deposit boxes are the safest place to keep them. The advent of rapidly growing technologies enables users to operate high security systems with electronic identification options .These identification technologies include safe deposit boxes and ATMs as well as other smart cards, user IDs and password-based systems etc., which are unfortunately not protected against hacker attacks, theft and forgotten passwords. All of these failures or faults and malfunctions or crashes of these systems still exist; However, identification based on biometric or fingerprint authentication is the most efficient and reliable solution for strict security. 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 is chosen for its availability, reliability and high precision. The fingerprint identity. The physical characteristics are fingerprints of the hand, face, iris, etc., signature, voice keystroke patterns, etc. Biometric systems operate in verification mode or in identification mode. In verification mode, the system validates a person's identity by comparing the captured biometric template previously saved in the system database. In the traditional locker security identification mode, the system recognizes a person by searching the entire template database for matches, and the system performs one of many comparisons to determine the person's identity or fails if the person is not as the system is registered. Our project therefore use a fingerprint security system to improve the security of conventional lockers

II. LITERATURE SURVEY

J. Tapia, C. Perez - Gender Classification from the same iris code used for recognition. In this study, the binary iris code that could be used for identification was first applied to accurately determine gender. The information for gender prediction, according to the author, is dispersed throughout the iris as opposed to being localized in distinct concentric rings. They found that, in comparison to using features that represent the complete iris region, using features that only represent a portion of the iris region increases accuracy. By using measurements of mutual information as a guidance prediction, the author 3 selected iris code bits to use as gender characteristics. 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 Multi-Layer Bank Security System**, A multi-layer bank security system is a method for validating, supervising, and managing the security at bank storage rooms. To stop unauthorized access to the changing area, many banks today use the authorized access control approach. This work has developed the most effective, multi-level, and extremely reliable protection system for locker rooms. The system has a biometric component that uses gadgets like a fingerprint reader and an iris scanner to manage the security of the locker room's front entrance. Additionally, it has an RFID system that only permits authorized people to enter the dressing room area. Using a stationary passive infrared monitor in the locker room area, unauthorized visitors are kept an eye on. 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.

R. Gusain, H. Jain and S. Pratap -"Enhancing bank security system using Face Recognition, Iris Scanner and Palm Vein Technology. The purpose of this article is to design a bank locker security system that uses palm vein technology (PVR), iris scanning, and facial recognition to safeguard valuable items. MATLAB software is used by facial recognition systems to identify and validate the authorized user's picture. When someone enters an area that isn't restricted, the camera takes pictures of them, and a computer program matches those photos to a database of authorized

DOI: 10.17148/IJARCCE.2024.13925

people. The iris detection technology makes use of the kind human physical traits. Several places, including ATMs, immigration and border control, public safety, hospitality, and tourism, use this technology for biometric authentication. This research provides recommendations on how to modify the vascular pattern thinning algorithm to enhance the capability of palm vein recognition systems. 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.

D. Akila, S. Jayalakshmi, R. Jaya Karthik, S. Mathivilasini and G. Suseendran - Biometric Authentication with Finger Vein Images Based on Quadrature Discriminant Analysis. For a very long time, high-security apps like bank lockers and private locations have used biometric authentication. Here, examination of a person's finger print, iris, etc. can reveal study on their physiological characteristics. Finger vein identification is part of the novel approach to 4 biometric recognitions. Here, a person's finger vein patterns can be used to authenticate them for entry to high-security apps. This research aims to identify finger veins using a quadrature discriminant analysis approach. Finger vein images are pretreated using methods to increase the image's stability for processing later. The QDA process was followed before using the Minimal Distance Classifier.

A.Natarajan and N. Shanthi - A Survey on Multimodal Biometrics Authentication and Template Protection. Biometric systems occupy a large portion of the security system market. Most applications use biometric technology, including locker and attendance controls at institutions like banks and hospitals. The templates that are stored there must be protected in addition to the authentication that these biometric systems provide. An overview of numerous biometrics, such as authentication, fusion, and template protection methods, as well as biometrics including fingerprints, faces, hand veins, iris, signatures, etc., is provided in this paper. In order to identify the most distinctive and practical methods for biometric identification and template protection, several traits and practices are investigated. A comparison of the unimodal and multimodal biometric systems is also included in this study. The various unimodal and multimodal biometric systems are assessed using metrics like the Genuine Acceptance Rate, Equal Error Rate, False Acceptance Rate, and False Reject Rate.

S. Sridharan-Authenticated secure biometric based access to the bank safety lockers. This paper focuses on providing a secure, authentic, and user-friendly mechanism for both the customers of the bank holding a locker and the branch head's involvement in all the operations pertaining to the safety lockers. The primary aim of this paper is to provide a solution towards a complete biometric based authentication mechanism for operating the safety lockers. This system rests on improving the current fact that all the lockers that operates currently operates only with the help of two different keys - one the branch head's key and other the user key. Improvement towards the current model that relies heavily on the key of the user is proposed which helps in the functioning of the locker with bio-metric and secret code (password). The main features that are proposed in the new mechanism is the two-level authentication - one by the branch head and one by the user for their identities, secure individual authentication with their bio-metrics and the access only to the concerned individuals for their safety lockers. The branch head responsible for the operation of the safety deposits is assigned in a daily basis by the central regional office of that bank.

III.PROBLEM DEFINITION

The existing security system either based on key or PIN number. Key alone has some failure for security system because it can be fake. In case of PIN number-based security system, same PIN number is used again and again. Anybody can hack the PIN number or guess.

IV. PROPOSED METHODOLOGY

The purpose of this project is to provide a high-level security system using the finger print sensor in the Locker which need high security using in money transform or high security information to fulfill the security gabs resulted from using just individual security system considering that system will design to be efficient, more secure, and with less cost.

k-nearest neighbours algorithm

In pattern recognition, the k-nearest neighbors algorithm (k-NN) is a non-parametric method used for classification and regression. In both cases, the input consists of the k closest training examples in the feature space. The output depends on whether k-NN is used for classification or regression.

Algorithm:

The K-NN working can be explained on the basis of the below algorithm:

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2024

DOI: 10.17148/IJARCCE.2024.13925

Step-1: Select the number K of the neighbors
Step-2: Calculate the Euclidean distance of K number of neighbors
Step-3: Take the K nearest neighbors as per the calculated Euclidean distance.
Step-4: Among these k neighbors, count the number of the data points in each category.
Step-5: Assign the new data points to that category for which the number of the neighbor is maximum.
Step-6: Our model is ready.
Suppose we have a new data point and we need to put it in the required category. Consider the below image:

K-Nearest Neighbor(KNN) Algorithm for Machine Learning
Firstly, we will choose the number of neighbors, so we will choose the k=5.
Next, we will calculate the Euclidean distance between the data points. The Euclidean distance is the distance between two points, which we have already studied in geometry. It can be calculated as:
K-Nearest Neighbor(KNN) Algorithm for Machine Learning
By calculating the Euclidean distance we got the nearest neighbors, as three nearest neighbors in category A and two nearest neighbors in category B. Consider the below image:
K-Nearest Neighbor(KNN) Algorithm for Machine Learning
As we can see the 3 nearest neighbors are from category A, hence this new data point must belong to category A.
How to select the value of K in the K-NN Algorithm?
Below are some points to remember while selecting the value of K in the K-NN algorithm:

There is no particular way to determine the best value for "K", so we need to try some values to find the best out of them. The most preferred value for K is 5.
A very low value for K such as K=1 or K=2, can be noisy and lead to the effects of outliers in the model.
Large values for K are good, but it may find some difficulties.

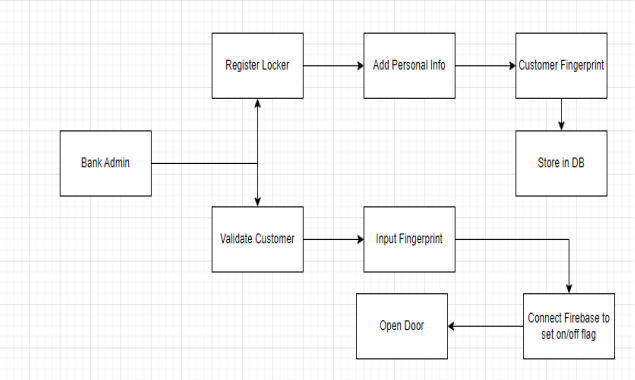

Fig 1. System Architecture

Module 1: Registration and Login for patient and Doctor
Module 2: Update Record or view record
Module 3: Fingerprint Matching
Module 4: Report Generation
.

V.MATHEMATICAL MODEL

Euclidean distance formula.

Here's the formula: $\sqrt{(X_2-X_1)^2+(Y_2-Y_1)^2}$

Where:

X_2 = New entry's brightness (20).
X_1= Existing entry's brightness.
Y_2 = New entry's saturation (35).
Y_1 = Existing entry's saturation.

$$\text{distance}(x, X_i) = \sqrt{\sum_{j=1}^{d}(x_j - X_{i_j})^2]}$$

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2024

DOI: 10.17148/IJARCCE.2024.13925

VI. CONCLUSION

The fingerprint device based system for securing the transactions of the user and providing the security for the User and even more for the Account verification using a finger print scanner has been followed.

REFERENCES

[1]. Janhavi Baikerikar “Machine Learning based Facial Recognition and Finger Print Identification for Secure Locker Access” 2024 IEEE 9th International Conference

[2]. Devi, M. J. Therese and G. Premalatha, "Cloud Computing based Intelligent Bank Locker System", *Journal of Physics: Conference Series*, vol. 1717, no. 1, pp. 012020, Jan. 2021.

[3]. Kumar, P. Sood and U. Gupta, "Internet of Things (IoT) for Bank Locker Security System", *2020 6th International Conference on Signal Processing and Communication (ICSC)*, pp. 315-318, 2020.

[4]. G. Charitha Reddy, K. Akhil and C.H. Meghanath Reddy, "Bank safety locker system with image identification by using email", *Journal of Engineering Science*, vol. 11, no. 4, pp. 1165-1169, April 2020.

[5]. 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)*, pp. 725-728, 2020.

[6]. G. Charitha Reddy, K. Akhil and C.H. Meghanath Reddy, "Bank safety locker system with image identification by using email", *Journal of Engineering Science*, vol. 11, no. 4, pp. 1165-1169, April 2020.