www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 05, May 2023, pp : 352-357

e-ISSN : 2583-1062

Impact Factor : 5.725

BANK LOCKER PROTECTION WITH LIVENESS DETECTION USING MACHINE LEARNING

Monika Vishwakarma[1], Rutuja Gite[2], Bhavana Katyare[3], Pooja Kokane[4], Prof. R. P. Sabale[5]

[1,2,3,4,5]Department of Computer engineering, Sir Visvesvaraya Institute of Technology,Chincholi, Nashik, India.

DOI : https://www.doi.org/10.56726/IRJMETS31174

ABSTRACT

The security plays a vital role in the banking sector, it uses different security method such as biometric and Documentation, etc. These are done physically in the presence of the customer, but now Everything is getting evolved into digitalization. Face recognition is an effective, digital and successful security technique, It alone cannot determine whether the person is real or fake, A liveness detection is added to make it more secure. The bank locker security is based on liveliness detection. In liveness detection, the system detects, it interacts with a real person or it can be spoof artefact used by other person such as a face photo. Therefore, To detect whether the person is live or not, it uses eye blink(iris) detection and motion. The system identifies whether the user is authentic or not. If not then, the locker will not open instead it will send a text SMS to the admin and customer that somebody is trying to open respective locker. If the person is not available and others from their family members wants to access the locker then Customer have their Nominee in the system, they can access the locker. These enhanced security features are enough to make consumers feel safer and more confident to keep their precious things in locker.

Keywords: liveness(iris) detection, Nominee.

1. INTRODUCTION

Although the popularity performance of biometric system is lately quite satisfactory for many applications, heaps of labour remains necessary to permit convenient, secure and privacy-friendly systems to be designed. In face recognition, the same previous attack ways are in addition classified into several categories. the concept of classifying depends on what verification proof is offer to face verification system, variety of a stolen icon, stolen face photos, recorded video, 3D face models with the talents of blinking and lip moving, 3D face models with varied expressions so on. the thought of classifying depends on what verification proof is offer to face verification system, variety of a stolen icon, stolen face photos, recorded video, 3D face models with the talents of blinking and lip moving, 3D face models with varied expressions and then on. throughout this paper, we tend to tend to project how of live face detection to resist the attack employing a photograph. On what verification proof is offer to face verification system, variety of a stolen icon, stolen face photos, recorded video, 3D face models with the talents of blinking and lip moving, 3D face models with varied expressions so on. the thought of classifying depends on what verification proof is offer to face verification system, utterly totally different expression sort of a stolen icon, stolen face photos, recorded video, 3D face models with the talents of blinking and lip moving, 3D face models with varied expressions and then on. Throughout this paper, we tend to tend to project the way of live face detection to resist the attack employing a photograph. Our formula depends on analysis of movement of facial components, significantly eyes, in sequent photos. typically, in sequent face photos there are little or no variations in sort of face and facial components. but eyes have heaps of larger variation in kind as a result of we tend to tend to repeatedly blink and move the pupils unconsciously. so, we tend to tend to watch eyes in sequent face photos and compare the form of every eye region to decide whether or not or not the input face image will be a real face or a photograph. If the person is not available and others from their family members wants to access the locker Then Customer have their Nominee in the system, they can access the locker. These enhanced security features are enough to make consumers feel safer and more confident to keep their precisions things in locker.

2. ITERATURE REVIEW

Gang Pan etal.[1] gift a spoofing against photograph in face recognition exploitation real time physiological property detection exploitation spontaneous eye blinking. This methodology needs solely a generic camera no different hardware to avoid spoofing attack in nonintrusive manner. Eye blinking is physical method that in a flash opens and closes lids Again and once more in an exceedingly} very minute. Generic camera captures fifteen frames per seconds, it provides 2 frames of faces that used as clue against spoofing attack. 2 captured frames in sequence are thought-about as freelance. HMM produces options from finite state set. Typical blinking activity exploitation HMM feature finds spoofing attack. Anjos et al. [2] planned how supported foreground or background motion correlation for

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 05, May 2023, pp : 352-357

e-ISSN : 2583-1062

Impact Factor : 5.725

checking physiological property of user. This methodology classified in motion detection. This methodology works on correlation between head rotation of user and its background. to go looking out correlation author uses fine grained motion direction. Optical flow is used to hunt out the direction of motion. This approach is easy method however need multiple frames to check physiological property, thus user ought to be co-operative. Face physiological property detection [3] has been planned to reinforce the dependability and security of face recognition system. The faux faces are distinguished from the 000 ones exploitation totally different classification techniques. during this paper, we tend to propose one image-based faux face detection methodology supported frequency and texture analyses for discriminating 2-D paper masks from the live faces. For the frequency analysis, we have got applied power spectrum primarily based methodology [4] that exploits not solely the low frequency info however conjointly the info residing among the high frequency regions. Moreover, wide used native Binary Pattern (LBP) [5]. In face recognition, the quality attack strategies may even be classified into many classes. the idea of classifying depends on what verification proof is give to face verification system, sort of a purloined picture, purloined face photos, recorded video, 3D face models with the abilities of blinking and lip moving, 3D face models with numerous expressions and so on [6]. the most goal of this paper is to vogue and implement a bank locker security system supported RFID and GSM technology which could be organized in bank, secured offices and homes. throughout this method solely authentic person is recovered cash from bank locker. The RFID reader reads the id range from passive tag and send to the microcontroller, if the id range is valid then microcontroller send the SMS request to the documented person mobile range, for the primary countersign to open the bank locker, if the person send the countersign to the microcontroller, which may verify the passwords entered by the key board and received from documented mobile. if these 2 passwords are matched the locker are opened otherwise it's going to be stay in bolted position[7].Initially pattern flow unit of measurement collected as datasets and maintained in bank agent server. The machine includes a camera to capture the pattern flow of user and sent for method choices of the logic were compared and user where recognized. additionally to the authentication of user there's another system to spot the user before that RFID little indefinite quantity checking is required. Image method is used and information data input device identification is required for an additional level of security. In future bank can implement this sort of authentication chance for banking and from this project shows that everyone the bank accounts is accessed whereas not practice cards through this face recognition with efficiency and safely [8]. Access system forms a vital important} link during a} terribly very security chain. The Fingerprint associated identification-based security system given here is AN access system that enables exclusively authorized persons to access a restricted house. we've implemented a locker security system supported fingerprint, identification and GSM technology containing door lockup system which might activate, proof and validate the user and unlock the door in real time for locker secure[9]. They says perhaps the foremost very important application of correct personal identification is securing restricted access systems from malicious attacks. Among all the presently utilized biometric techniques, fingerprint identification systems have received the foremost attention due to the long history of fingerprints and their intensive use in forensics. This paper deals with the difficulty of selection of associate optimum formula for fingerprint matching thus on vogue a system that matches required specifications in performance and accuracy[10].

3. AIMS AND OBJECTIVES

1. To study existing bank locker's method.
2. To design the system architecture for proposed system.
3. To implement the proposed system using machine learning.
4. To analyse and evaluate the design module

4. SYSTEM ARCHITECTURE

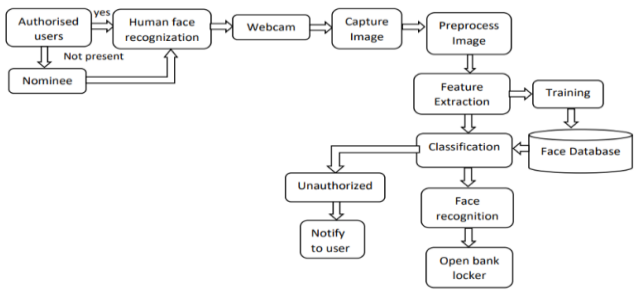


Fig1. System Architecture Of Bank Locker Protection with Liveness Detection

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 05, May 2023, pp : 352-357

e-ISSN : 2583-1062

Impact Factor : 5.725

In this diagram we tend to square measure attending to implement eye-blink detection & face recognition supported LBPH algorithmic program. The algorithmic program works in real time through a digital camera and displays the person's name. The program runs as follows: 1. notice faces in every frame generated by the digital camera. 2. For every detected face, notice eyes. 3. Notice aliveness of the face i.e. eyes square measure blinking or not 4. Acknowledge face and access the revered locker of the user.

5. ALGORITHM

Convolutional Neural Network(CNN)

A Convolutional Neural Network (CNN) is a type of machine learning algorithm that is particularly well-suited for image recognition and processing tasks. It is made up of multiple layers, including convolutional layers, pooling layers, and fully connected layers. The convolutional layers are the key component of a CNN, where filters are applied to the input image to extract features such as edges, textures, and shapes. The output of the convolutional layers is then passed through pooling layers, which are used to down-sample the feature maps, reducing the spatial dimensions while retaining the most important information. The output of the pooling layers is then passed through one or more fully connected layers, which are used to make a prediction or classify the image.

Haar Cascade

Haar Cascade is a feature-based object detection algorithm to detect objects from images. A cascade function is trained on lots of positive and negative images for detection. The algorithm does not require extensive computation and can run in real-time. We can train our own cascade function for custom objects like animals, cars, bikes, etc. Haar Cascade can't be used for face recognition since it only identifies the matching shape and size. Haar cascade uses the cascade function and cascading window. It tries to calculate features for every window and classify positive and negative. If the window could be a part of an object, then positive, else, negative.

6. USED TECHNOLOGY

The Bank Locker Protection with Liveness Detection System is developed using a various of technologies to enable its various features and functionalities. Some of the key technologies used in the system are:

PYTHON: The system is developed using the Python programming language, which is a popular language used for Artificial Intelligence and Machine Learning projects with the help of libraries like TensorFlow, Keras, Pandas and scikit-learn etc.the system/model is developed .

SQL: SQL is used to communicate with a database. The SQL statements are used to perform tasks such as update delete and retrieve data from a database of the users.

JAVASCRIPT: JavaScript is a scripting language which helps to create dynamically updating content, control multimedia, textfields, and various buttons.

HTML/CSS: The system's user interface is built using HTML and CSS, which is the standard languages used for creating webpages

7. ADVANTAGES

1. Provides high security.
2. No hack or crack to system.
3. Easy to use.
4. Fully automatic system.
5. Theft protection and alert.

8. APPLICATIONS

1. In offices.
2. In Bank Lockers.
3. In identification.
4. In Jewellery shops
5. All that places when unique identity & high security is required.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 05, May 2023, pp : 352-357

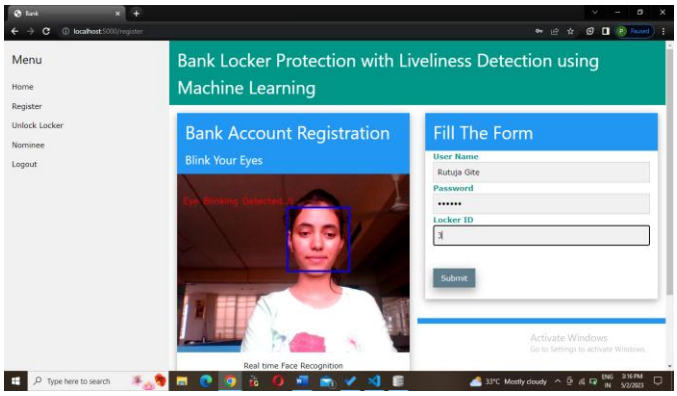
e-ISSN : 2583-1062

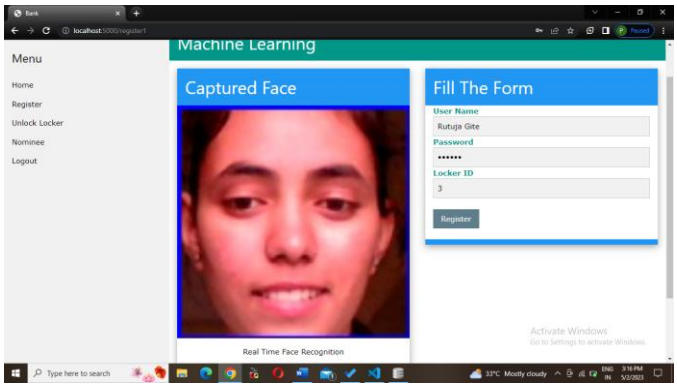
Impact Factor : 5.725

9. MODULES AND RESULTS

1. REGISTER

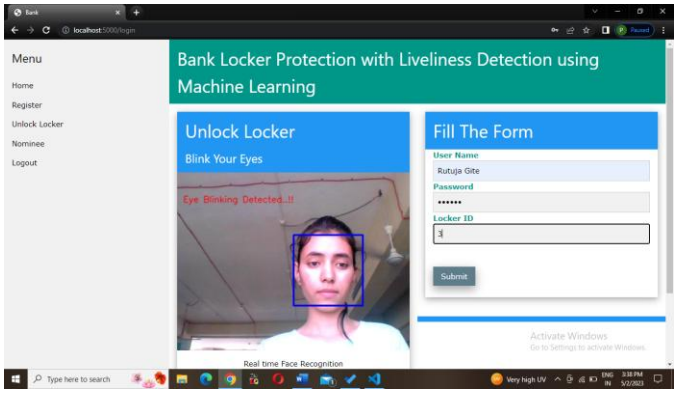
User have to do Registeration with liveness detection to have an access of locker in the System.



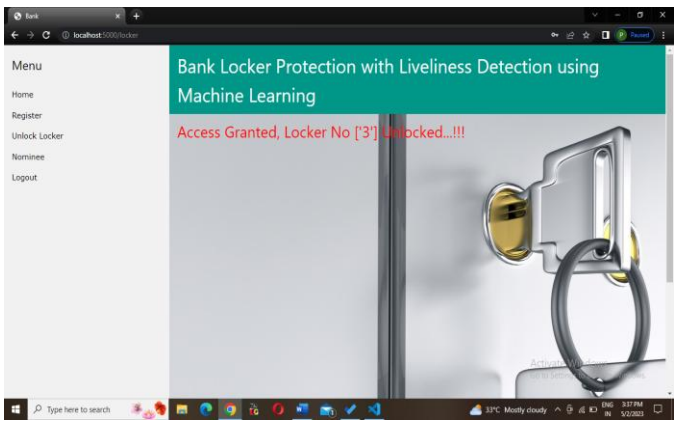


2. UNLOCK LOCKER :

The locker will unlock when liveness of the valid user is detected through eyeblink and moments.



Access to Respective Locker



INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

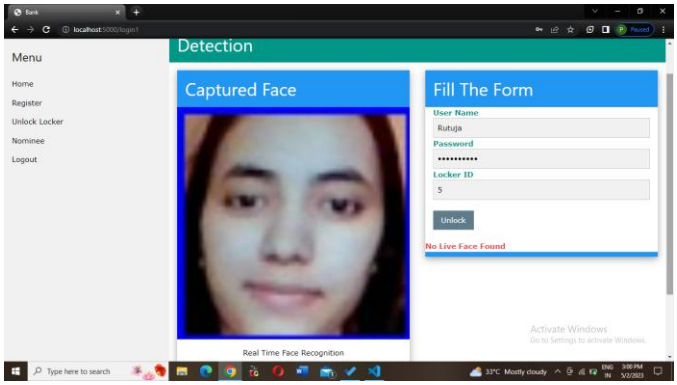
Vol. 03, Issue 05, May 2023, pp : 352-357

e-ISSN : 2583-1062

Impact Factor : 5.725

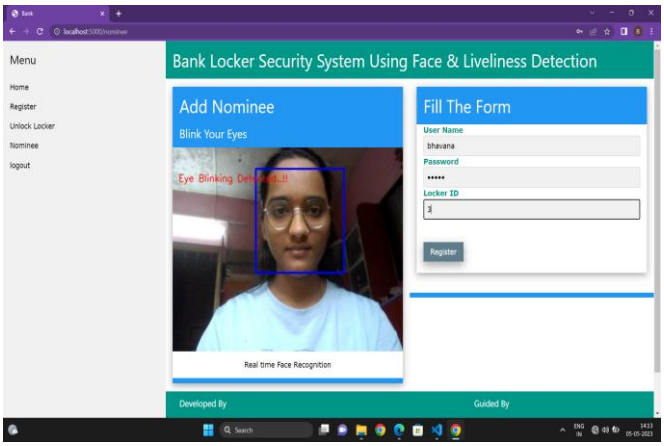
No Liveness Detected :

If person is trying to do spoofing, it will display an error and text-message will be send to respective locker holder (user).

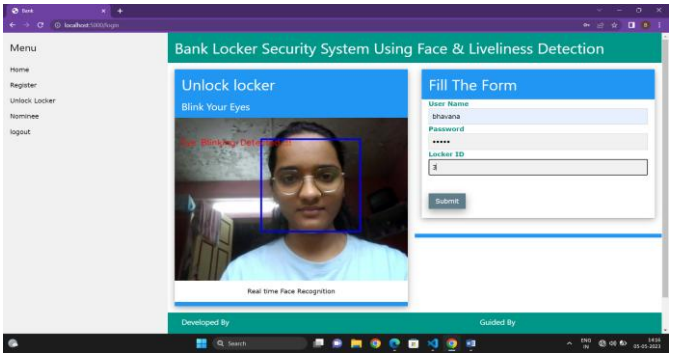


3. ADD NOMINEE :

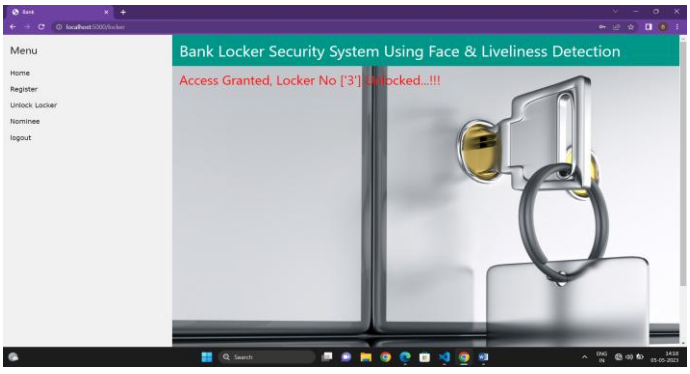
A user have to add nominee with different username password but same locker id.



Unlock Locker by Nominee **:**



Access of Locker to Nominee **:**



10. CONCLUSION

The Theft and spoofing have increased due to which many losses are taking place. Therefore we've projected a Machine Learning technique based on Face Detection-Recognition and a liveness detection for bank locker System which helps to avoid spoofing and provide high security. It's extremely reliable system to confirm the safety and security of the valuables things.

11. REFERENCES

[1] G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink -based anti-spoofing in face recognition from a generic webcamera," in Proc. IEEE 11th Int. Conf. Comput. Vis. (ICCV), Oct. 2007, pp. 1–8.

[2] Anjos, M. M. Chakka, and S. Marcel, "Motion-based countermeasures to photo attacks in face recognition," IET Biometrics, vol. 3, no. 3, pp. 147–158, Sep. 2014.

[3] Pan, Gang, Lin Sun, Zhaohui Wu, and Yueming Wang. "Monocular camera-based face liveness detection by combining eyeblink and scene context." Telecommunication Systems 47, no. 3-4 (2011): 215-225.

[4] H. S. Choi, R. C. Kang, K.T. Choi, A. T. B. Jin, and J.H. Kim. Fake-Fingerprint Detection using Multiple Static Features. Optical Engineering, 48(4), 2009.

[5] T. Ojala, and M. Pietikainen. Multiresolution Gray-Scale and Rotation Invariant Texture Classification with Local Binary Patterns. IEEE Transactions on Pattern Analysis and Machine Intelligence, 24

[6] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of fourier spectra," In Biometric Technology for Human Identification, SPIE vol. 5404, pp. 296-303, 2004.

[7] Z. Lu, X. Wu, and R. He, "Person identification from lip texture analysis," in International Conference on Digital Signal Processing, DSP, 2017, pp. 472–476.

[8] Gan, J.Y.; Li, S.L.; Zhai, Y.K.; Liu, C.Y. 3D convolutional neural network based on face anti-spoofing. In Proceedings of the International Conference on Multimedia and Image Processing, Wuhan, China, 17–19 March 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–5.

[9] Li, L.; Feng, X.Y.; Jiang, X.Y.; Xia, Z.Q.; Hadid, A. Face anti spoofing via deep local binary patterns. In Proceedings of the IEEE International Conference on Image Processing, Beijing, China, 17–20 September 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 101–105.

[10] Bank locker protection with liveness detection using machine learning"||R.P.Sabale, Monika Vishwakarma, Rutuja Gite , Bhavana katyare, Pooja Kokane IRJMETS/vol.04,issue11 2022.