International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 04 | April - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Face and Liveliness Detection based Bank Locker Security System

Prof. Sunil M. Kale
(Project Guide)
Sandip Institute of Technology and Research Centre
Savitribai Phule Pune University
Nashik, Maharashtra, India

Anuja Nair
Sandip Institute of Technology and Research Centre
Savitribai Phule Pune University
Nashik, Maharashtra, India

Kiran Pagar
Sandip Institute of Technology and Research Centre
Savitribai Phule Pune University
Nashik, Maharashtra, India

Manasi Pagar
Sandip Institute of Technology and Research Centre
Savitribai Phule Pune University
Nashik, Maharashtra, India

Esha Kamble
Sandip Institute of Technology and Research Centre
Savitribai Phule Pune University
Nashik, Maharashtra, India

ABSTRACT

Ensuring transaction security is one of the biggest challenges for banking systems today. The use of biometrics by users has attracted huge sums of money from banks around the world due to its convenience and acceptability. Especially in offline environments where facial images on ID documents are matched to digital selfies. In fact, comparing selfies and ID cards is also used in some more widespread programs these days such as in Automated Immigration Control. A major difficulty with such methods is narrowing down the differences between comparative facial images from different origins. We propose a new architecture for cross-domain matching problems based on deep features extracted from two well-referenced convolutional neural networks (CNNs). Results obtained from the collected data, called Face Bank, demonstrated the power of the proposed face-to-face comparison problem and its incorporation into real bank security systems, with an accuracy of over 93%.

Keywords*: *Face Bank, Convolutional Neural Networks (CNN), automatic immigration control, digital selfies, face to face comparison problem, spoofing.

1.INTRODUCTION

Security is vital in the contemporary world. Everybody possesses priceless items like gold, jewellery, or cash. It is not enough to just possess these things; rather, their protection is crucial, thus we store them in bank lockers. Even yet, we frequently read or hear in the news that a phoney individual gained entry to someone else's locker and stole money. The verification of the user who wants to access the locker is crucial in order to combat this form of fraud.

Although most applications can already recognize people using biometric systems rather well, more effort is still needed to enable the construction of systems that are practical, secure, and privacy-friendly. The typical assault techniques in face recognition may be divided into a few different groups. Classification is based on the verification evidence that is provided to the face verification system, such as a stolen photo, stolen face photos, recorded video, 3D face models with the ability to blink and move their lips, 3D face models with different emotions, and so on.

In this article, we proposed a live facial recognition method to resist attacks using photos. Our algorithm is based on analyzing facial components, especially eye movements, in consecutive frames. In general, sequential face images show little change in face shape or face components. But we are constantly blinking and unconsciously moving our pupils, which makes our eyes much larger. Therefore, it detects eyes from consecutive facial images and compares the shape of each eye region to determine whether the input facial image is a real face or a photograph.

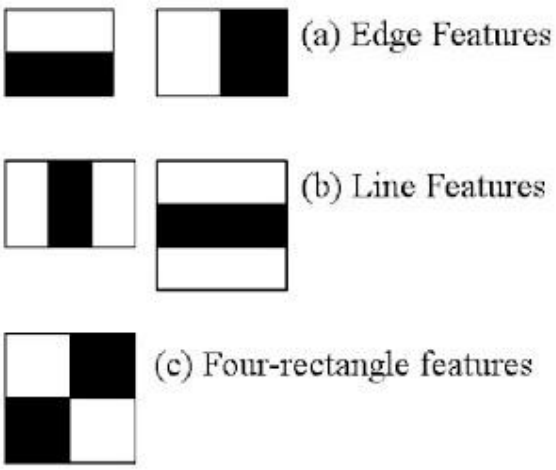
Nowadays, liveness detection has been a very

active study area in the fingerprint and iris recognition fields. However, there are very few techniques to tackling the challenge of face recognition. The act of discriminating between living and non-living functional areas is referred to as aliveness. Scammers attempt to inject a large number of bogus biometrics into the system. The use of live detection improves the performance of biometric systems. It is a critical and difficult topic that affects the security and dependability of biometric systems against spoofing.

Haar Cascade Classifier

In their 2001 paper "Rapid Object Recognition with a Boosted Cascade of Simple Features," Paul Viola and Michael Jones suggested an effective object detection approach based on Haar feature-based cascade classifiers. In this machine learning-based technique, a cascade function is learned using a large number of both positive and negative pictures. It is then used to detect objects in other photographs.

In this case, face recognition will be employed. The classifier must first be trained using a large number of positive and negative pictures (with and without faces). Then we must extract its characteristics. This makes use of the haar characteristics shown in the figure below. They are ideal for our Convolutional kernel. Each is made up of a single feature.



2.LITERATURE REVIEW

Gang Pan et al. [1] present a spoofing against photograph in face recognition using real-time physiological property detection via spontaneous eye blinking. To avoid spoofing attacks in a nonintrusive manner, this methodology requires only a generic camera and no other hardware. Eye blinking is a physical process that opens and closes the lids in a flash. Again and again in an extremely brief period of time. Generic cameras capture fifteen frames per second and provide two frames of faces that can be used as a clue against spoofing attacks. Two captured frames in sequence are considered freelance. HMM generates options based on a finite state set. A typical blinking activity exploiting the HMM feature detects a spoofing attack. Anjos et al. [2] planned how to use foreground or background motion correlation to test a user's physiological properties. This methodology is categorized as motion detection. This methodology is based on the correlation between the user's head rotation and the background. The author employs fine-grained motion direction to search for correlation. Optical flow is used to determine motion direction. This method is simple, but it requires multiple frames to check physiological properties, so the user must be cooperative. Face physiological property detection [3] is being developed to improve the dependability and security of the face recognition system. The fake faces are distinguished from the thousands by employing completely different classification techniques. We propose an image-based faux face detection methodology supported by frequency and texture analyses for distinguishing 2-D paper masks from live faces in this paper. For the frequency analysis, we used a power spectrum-based methodology [4] that makes use of not only low frequency information but also information from high frequency regions. Furthermore, native Binary Pattern (LBP) is widely used [5]. Quality attack strategies in face recognition can even be classified into several classes. The classification strategy is based on the verification evidence provided to the face verification system, such as a stolen image, stolen face images, recorded video, 3D face models with the ability to blink and move

their lips, 3D face models with a variety of expressions, and so on [6]. The main objective of this article is to design and put into practice a bank locker security system that uses RFID and GSM technology that may be installed in banks, secure offices, and private residences. Using this technique, only the real individual can retrieve money from a bank safe. The microcontroller receives the passwords entered by the keypad and received from the documented mobile range after the RFID reader reads the identification range from the passive tag. If the identification range is valid, the microcontroller sends an SMS request to the documented person's mobile range for the primary countersign to open the bank locker. If these two passwords match, the locker will be unlocked; otherwise, it will remain in the bolted position [7].

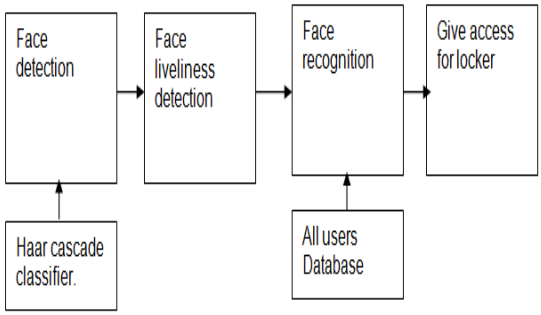
Initial datasets for the pattern flow unit of measurement were gathered and kept on the bank agent server. The device has a camera to record the user's pattern of movement, which is then sent to be compared with the logic's method choices and the user identified. In addition to user authentication, there is another technique to identify users before RFID little long-term quantity checking is necessary. For an additional layer of security, the image approach is utilized and information data input device identification is necessary. Future banks may use this method of authentication, and this project's results demonstrate that it can be done efficiently and securely without the use of credit cards for all bank accounts [8]. Access control systems are an extremely crucial link in a chain of security. The security system with fingerprint-based identification described here is an access system that only allows people who have been granted permission to enter a restricted home. We have put in place a locker security system that uses GSM, fingerprint, and identity technologies with a door lockup system that can instantly activate, verify, and activate the user. According to them, protecting restricted access systems from malicious attacks is possibly the most crucial application of accurate personal identity. Due to the lengthy history of fingerprints and their extensive usage in forensics, fingerprint identification systems have attracted the most interest among all currently used biometric approaches. In order to create a system that meets essential standards in performance and accuracy, it can be challenging to choose an optimal formula for matching fingerprints [10].

3. PROJECT OVERVIEW

A) Problem Framework

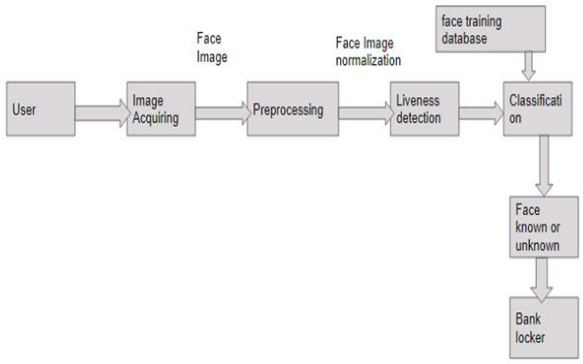
Due to the popularity of facial recognition, thieves may choose to attack the system, and aliveness detection has grown to be a crucial component of the authentication process. Among these aliveness detection algorithms, machine learning was supported. We will therefore use this methodology throughout the entire study.

B) Model framework



We tend to notice face abuse using a haar cascade classifier, an algorithmic program for face detection, in the diagram up top. Once a face is detected, the system can determine if it is real or fake by using an aliveness detection algorithm. Differentiating the feature region into living and non-living is the aliveness detection approach. With this technique, we want to be able to recognize faces and eyes over time. As a result, we frequently use a cascade classifier to carry out these jobs. This haar cascade classifier across Cascade is a machine learning approach that can be used to identify items in an extremely large image or video.

C) Architecture diagram



This diagram shows how the LBPH algorithmic software will be used to achieve eye-blink detection and face identification. The algorithmic program displays the person's name while operating in real time through a digital camera. This is how the program operates:

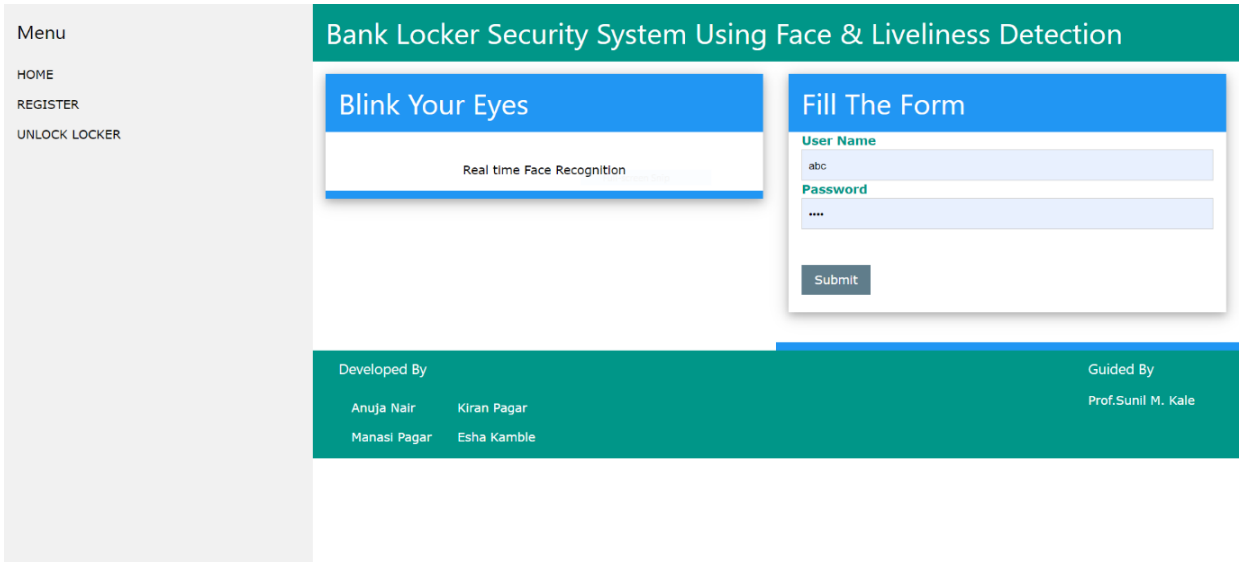
1. Take note of faces in every digital camera frame.
2. Look at the eyes for every face you can find.
3. Check to see if the face is alive by observing whether or not the eyes are blinking.
4. Identify yourself and enter the user's valued locker.

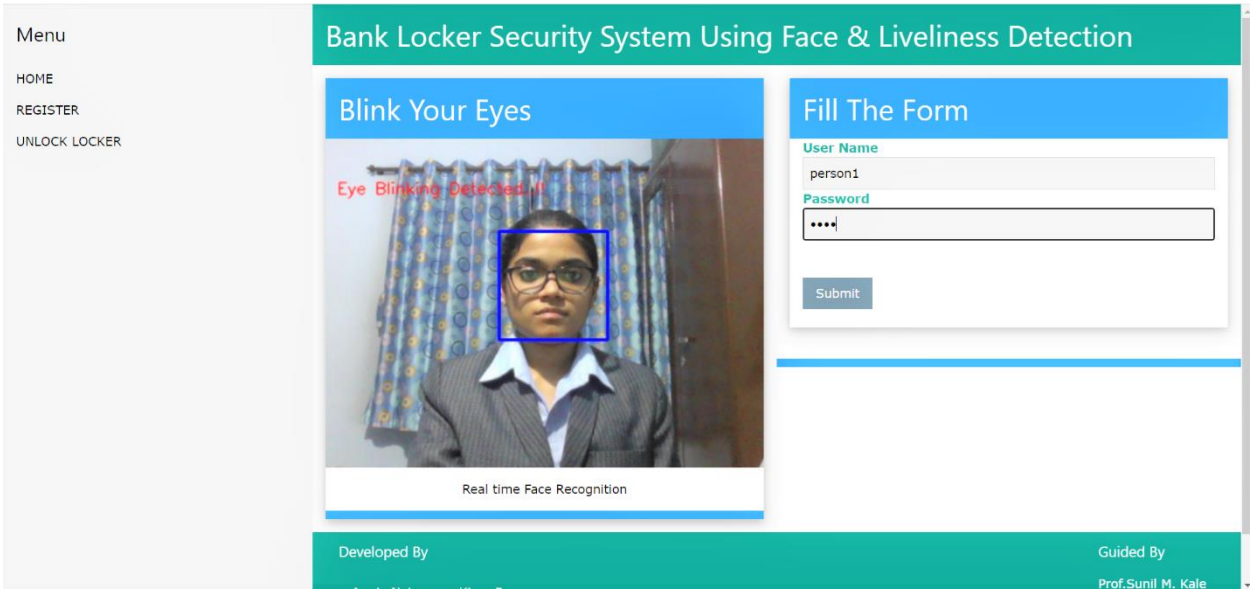
D) Modules

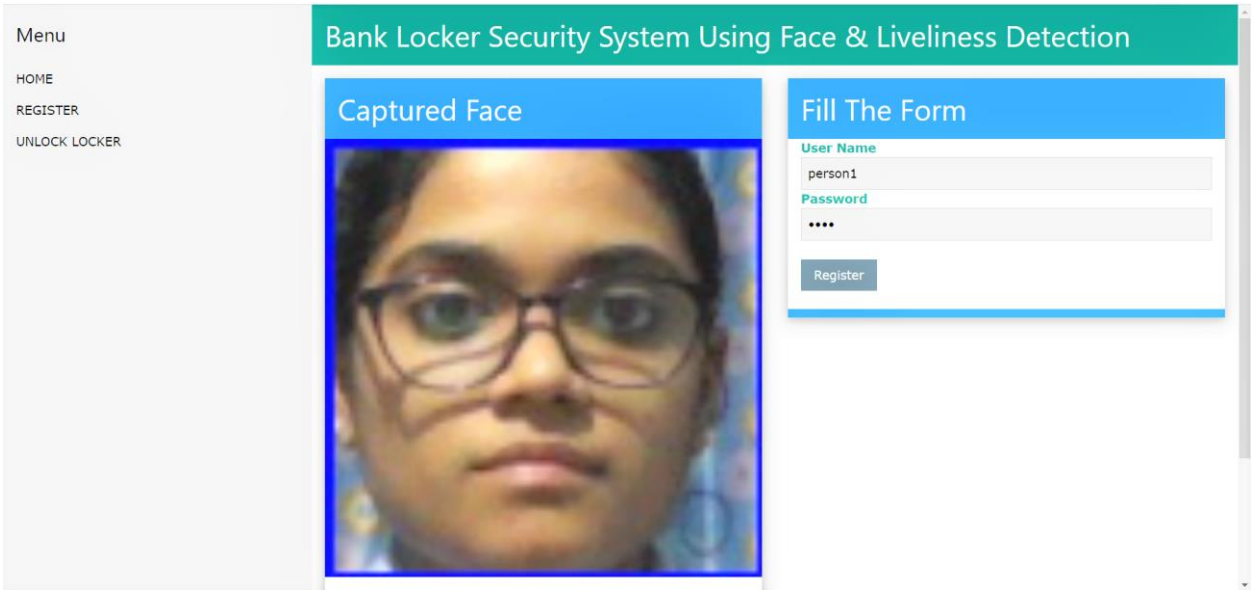
- Image Acquisition:
  - The camera will be interfaced to locker which will be controlled by python interface
- Face Detection:
  - Facial Landmarks can be used to detect Face of person
- Face Recognition:
  - Neural Network can be trained to recognize faces of user
- Liveliness Detection:
  - Eye blink detection algorithm can be used to detect liveliness
- Access Control:
  - Finally access control is achieved based on face & liveliness Detection

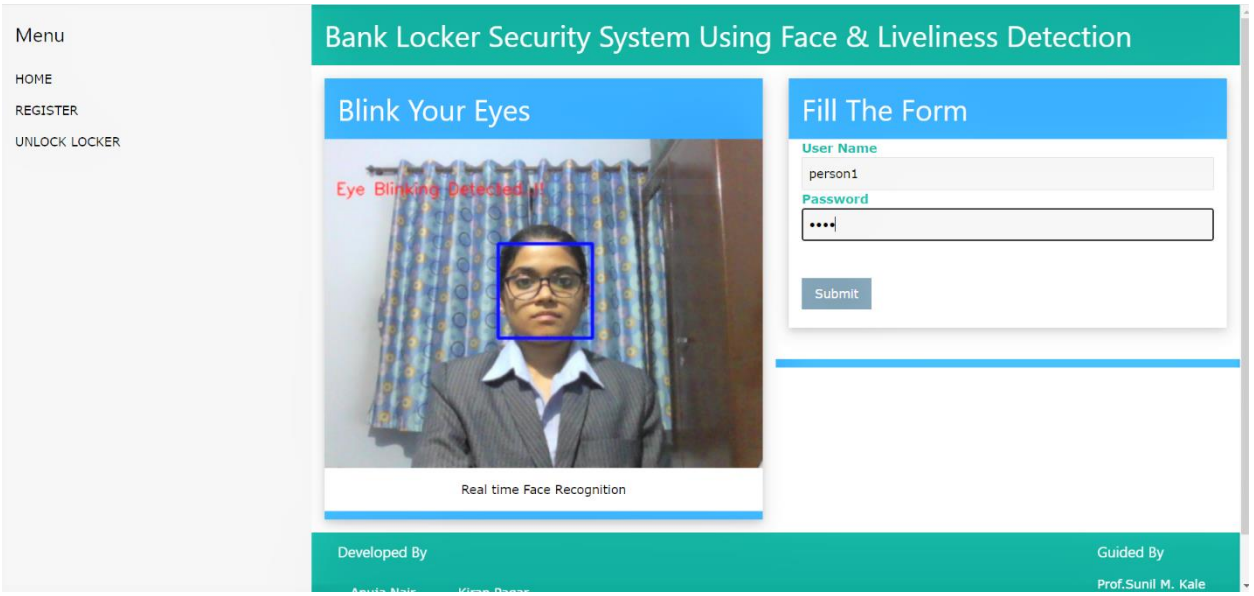
4.IMPLEMENTATION RESULTS

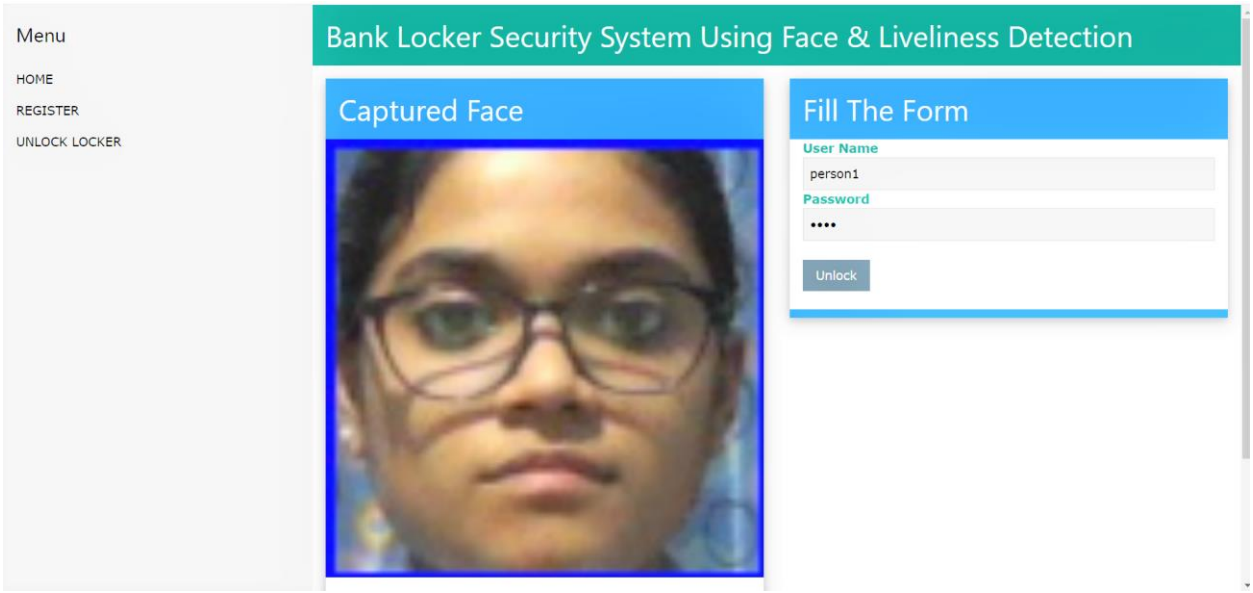
a) Home page


Menu
HOME
REGISTER
UNLOCK LOCKER
Bank Locker Security System Using Face & Liveliness Detection
Blink Your Eyes
Real time Face Recognition
Fill The Form
User Name
abc
Password
Submit
Developed By
Anuja Nair
Kiran Pagar
Manasi Pagar
Esha Kamble
Guided By
Prof.Sunil M. Kale


Menu
HOME
REGISTER
UNLOCK LOCKER
Bank Locker Security System Using Face & Liveliness Detection
Blink Your Eyes
Eye Blinking Detected !!
Real time Face Recognition
Fill The Form
User Name
person1
Password
Submit
Developed By
Guided By
Prof.Sunil M. Kale


Menu
HOME
REGISTER
UNLOCK LOCKER
Bank Locker Security System Using Face & Liveliness Detection
Captured Face
Fill The Form
User Name
person1
Password
Register


Menu
HOME
REGISTER
UNLOCK LOCKER
Bank Locker Security System Using Face & Liveliness Detection
Blink Your Eyes
Eye Blinking Detected..!!
Real time Face Recognition
Fill The Form
User Name
person1
Password
Submit
Developed By
Guided By
Prof.Sunil M. Kale


Menu
HOME
REGISTER
UNLOCK LOCKER
Bank Locker Security System Using Face & Liveliness Detection
Captured Face
Fill The Form
User Name
person1
Password
Unlock


Menu
HOME
REGISTER
UNLOCK LOCKER
Bank Locker Security System Using Face & Liveliness Detection
Access Granted Locker Unlocked..!!!

5.FUTURE SCOPE

This project has the potential to be developed further . Face liveness identification, will aid in comprehending various spoof assault scenarios and their relationship to the established remedies. The very following day, popular technology is no longer relevant. The method might be improved further to maintain the abstract of technological advancements. Even though, it will get better with more improvements. To make it even better, we can update it with new changes such as adding fingerprint sensing/recognition, iris scanning, voice recognition etc. As a result, the project can always be upgraded with improved features.

1.The System can be implemented in embedded processors such as raspberry PI.

2. The System can be further extended to other banking services.

3.It can be used in attendance system in school or college, home security, ATM security etc.

6.CONCLUSION

In this research paper, we provide a face detection-recognition and aliveness detection system for bank lockers that is based on machine learning. To further ensure the security we used an additional sms API (Twilio) to send message at the times of invalid logins directly to your phone. Hence, it is an incredibly trustworthy way to verify the security of our possessions.

7.REFERENCES

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

[2] Anjos et al., "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 are the authors of this work. "Detecting face liveness with a monocular camera by combining eyeblink and scene context." Telecommunication Systems, vol. 47, no. 3-4, pp. 215-225, 2011.

[4] H. S. Choi, R. C. Kang, K.T. Choi, A. T. B. Jin, and J.H. Kim are the authors of this paper. Multiple Static Features are used to detect fake fingerprints. 48(4), Optical Engineering, 2009.

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

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

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

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

[9] Li, L., Feng, X.Y., Jiang, X.Y., Xia, Z.Q., and A. Hadid. Deep local binary patterns are used for face antispoofing. IEEE International Conference on Image Processing, Beijing, China, September 17-20, 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 101-105.

[10] Wang, S.Y., Yang, S.H., Chen, Y.P., and Huang, J.W. Face liveness detection using skin blood flow analysis. 305, Symmetry 2017.