

# **BANK SAFE SECURITY SYSTEM USING MACHINE LEARNING WITH FACE AND LIVE DETECTION**

**Mr.Aditya Todkar<sup>1</sup>**

**Ms.Pranita Shetty<sup>2</sup>**

**Ms.Ayesha Shaikh<sup>3</sup>**

**Ms.Mukta Tawale<sup>4</sup>**

Student, Department of Computer Engineering Padmabhooshan Vasantdada Patil Institute of Technology,  
Bavdhan SPPU Pune

## **Abstract**

Ensuring the security of transactions is currently one of the biggest challenges facing banking systems. The use of biometric authentication of users attracts huge sums money from banks around the world thanks to their convenience and acceptance. Especially in an offline environment where face images from ID documents are compared to digital ones selfie. The selfie vs. id comparison has actually been used in some broader areas as well programs today, such as automatic immigration screening. The great difficulty of such the process is to limit the differences between the comparison face images given their different origins. We propose a new architecture for the cross-domain matching problem based on deep features extracted by two well-referenced convolutional neurons Network (CNN). The results obtained from the collected data, called Face Bank, with more accuracy of more than 93%, indicate the power of the proposed head-to-head comparison problem and its integration into real banking security systems.

## **Index Terms**

Convolutional Neural Networks (CNN), Face Bank, Automatic Immigration control, Digital selfie, Face-to-face comparison problem.

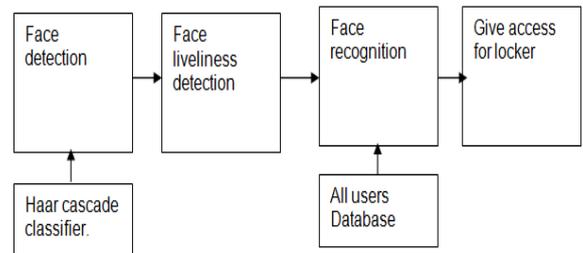
## **1. Introduction**

Although the recognition performance of the biometric system is quite sufficient these days suitable for most applications, much work is still needed to make it comfortable and safe and design Privacy-friendly systems. In facial recognition, common attack methods can be divided into several categories. The idea of classification is based on what verification evidence is provided to verify the faces system such as stolen photo, stolen face photo, recorded video, 3D face models with blink and lip movement abilities, 3D face models with different expressions and so on. In this paper, we proposed a live face detection method to resist the attack using a photo for which a verification document is provided Face authentication system like stolen photo, stolen face photo, recorded video, 3D face

Models with blink and lip movement capabilities, 3D face models with various expressions and so on. The idea of classification is based on what verification evidence is provided face authentication system like stolen photo, stolen face photo, recorded video, 3D face models with blink and lip movement capabilities, 3D face models with various expressions and so on. In this paper, we proposed a live face detection method to defend photo attack. Our algorithm is based on facial motion analysis components, especially eyes, in sequential images. Generally in face sequential display there is very little variation in the shape of the face and facial components. But they have a lot of eyes greater variation in shape because we are always unconsciously blinking and moving our pupils. So we detect eyes in sequential face images and compare the shape of each eye region with decide whether the input face image is a real face or a photo.

face detection and live detection to improve bank locker security.

**Proposed System**



In the above block diagram we will detect face using HAAR cascade classifier which Algorithm for face detection. After detecting the face, the system decides that the face is real or fake using a liveness detection technique. The liveness detection technique is an act distinguishing feature space into animate and inanimate.

In this system, we need a way to detect faces and eyes in real time. So we use -cascade classifier to perform these tasks. In this HAAR Cascade classifier, an Object detection machine learning algorithm used to identify objects in an image or video.

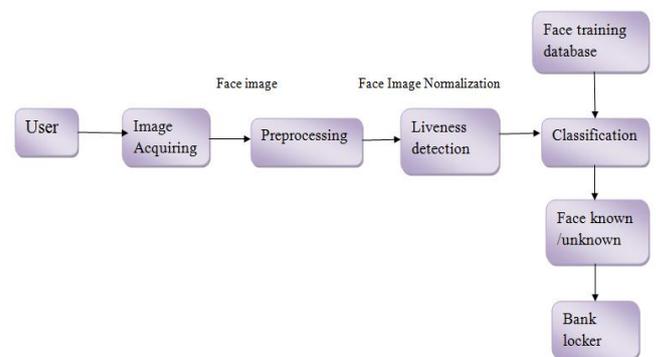
**Project Scope**

To provide a clear path for the future development of safer, more user-friendly and efficient approaches to facial liveness detection. Facial liveness detection to help understand different phishing attack scenarios and their relationship to the developed solutions.

**2. Problem Statement**

This project aims to design and implement a bank locker security system using machine learning with

**3. System Architecture**



In this diagram, we will implement eye blink detection and face recognition Based on the LBPH algorithm. The algorithm works in real time via a webcam and will display the person's name.

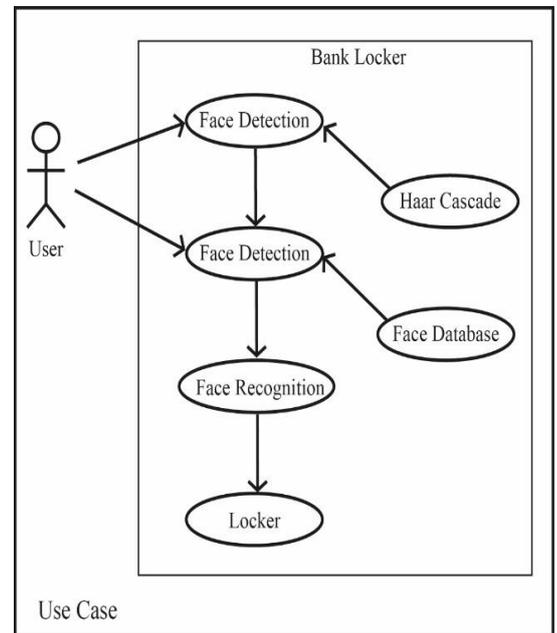
The program runs as follows:

1. Detect faces in every image generated by the web camera.
2. For each detected face, detect the eyes.
3. Detect the liveliness of the face, i.e. the eyes are blinking or not.
4. Recognize the face and gain access to the user's respected locker.

### 3.1 HAAR Cascade Classifier

An efficient object is object detection using cascaded classifiers based on HAAR elements detection method proposed by Paul Viola and Michael Jones in their article “Rapid Object Detection using a Boosted Cascade of Simple Features” in 2001. This is machine learning based approach where a cascading function is trained from many positives and negatives images. It is then used to detect objects in other images. Here we will work with face detection. At first, the algorithm needs a lot of positive images (images of faces) and negative images (images without faces) for training the classifier. Then we need to extract features from it.

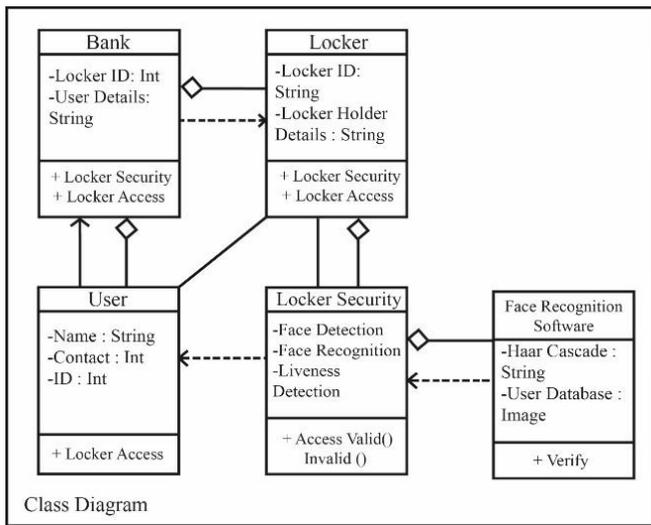
### 3.2 Use Case Diagram



A use case diagram is used to represent the dynamic behaviour of a system. It encapsulates system functionality by incorporating use cases, actors and their relationships. It models the tasks, services and functions required by the application system/subsystem. It shows the high level functionality of the system and also tells how the user handles the system.

### 3.3 Class Diagram

A class diagram represents a static view of an application. It represents the types of objects residing in the system and the relationships between them. A class consists of its objects and can also inherit from other classes. A class diagram is used to visualize, describe, document various different aspects of a system, and also to construct executable software code.



#### 4. System Requirements

- Software Requirements :
  - PyCharm development environment for Python coding.
  - Sublime for HTML and CSS coding.
- Hardware requirements :
  - Desktop/Laptop
  - 4GB Ram & above i3 processor

#### 5. Applications

1. It can be used in school or college attendance system.
2. Home security.
3. Security of ATMs.
4. Door security.
5. Bank Locker security.

#### 6. Advantages

1. It provides high security.
2. There is no doubt about hacking or cracking the system.

3. No need to remember username/password.
4. Easy to use.
5. Fully automatic system.
6. Theft protection and alerts.

#### 7. Conclusion

In this paper, we proposed machine learning based face recognition and recognition live detection for bank locker. In this project user will use bank locker using face detection and live technique. This facial recognition locker is much better than the traditional one locker because it doesn't need any traditional key to unlock the locker. Its high a reliable system to ensure the safety of our valuables.

#### 8. Future Scope

Here we cover several aspects when it comes to getting better and updated results our research system. We may add more features in the future. More country data can be watched for international investment and multinational banking. Mutual funds can too be monitored and suggestion regarding mutual fund investments may be provided. Every activity, effective decisions at national level and decision makers can be tracked early forecast

#### 9. References

[1] G. Kim, S. Eum, J. K. Suhr, D. I. Kim, K. R. Park, and J, Kim, Facial liveness detection based on textures and frequency analyses, 5th IAPR International Conference on Biometrics (ICB), New Delhi, India. pp. 67-72, March 2012.

[2] J. Maatta, A. Hadid, M. Pietikainen, Face Spoofing Detection from Single images Using Micro Texture Analysis, Proc. International Joint Conference on Biometrics (UCB 2011), and Washington, D.C., USA.

[3] sooyeon Kim, Sunjin Yu, Kwangtaek Kim, Yuseok Ban, Sangyoun Lee, face vividness detection using variable focusing, Biometrics (ICB), 2013 International Conference on, On page(s): 1 – 6, 2013.

[4] H. K. Jee, S. U. Jung, and J. H. Yoo, Liveness detection for integrated face recognition system, International Journal of Biological and Medical Sciences, vol. 1(4), pp. 235-238, 2006.

[5] Wei Bao, Hong Li, Nan Li, and Wei Jiang, A face liveliness detection method optical flow field-based recognition, In Image Analysis and Signal Processing, 2009, IASP 2009, International Conference on, pages 233 – 236, April 2009.

[6] W. Yin, Y. Ming, and L. Tian, "An Optical Flow-Based Face Anti-Spoofing Method field," in International Conference on Signal Processing Proceedings, ICSP, 2017, pp. 1333–1337.

[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 facial 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.