

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

Mr. Aditya Todkar¹

Ms. Pranita Shetty²

Ms. Ayesha Shaikh³

Ms. Mukta Tawale⁴

Students, Department of Computer Engineering

Prof. Ganesh Wayal⁵

HOD, 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 of 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.

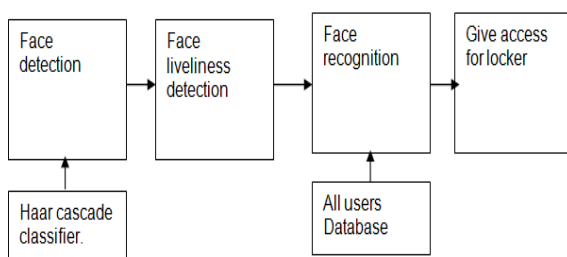
Project Scope

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 face detection and live detection to improve bank locker security.

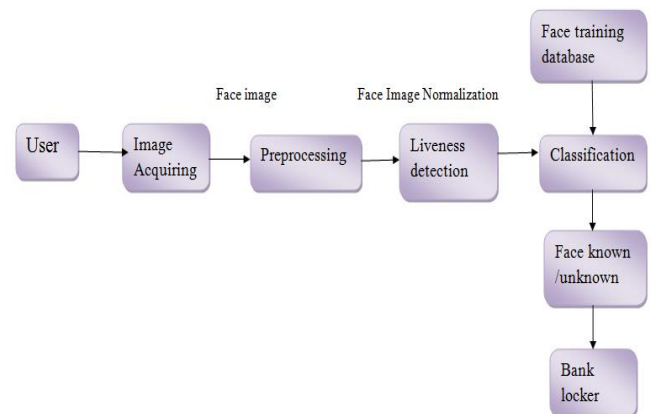
Proposed System



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. I

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 liveness 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

Step 1: First face is detected using HAAR Cascade classifier.

Step 2: For face recognition first data set is created then it trained, using this dataset we recognized face.

Step 3: Then for face liveness detection we used face landmark detection database is used. In that dataset eye blink is detected ,then we calculated aspect ratio of eye blink using eye blink value means if eye is opened what value we get and if eye is closed then what value get based that aspect ratio value.

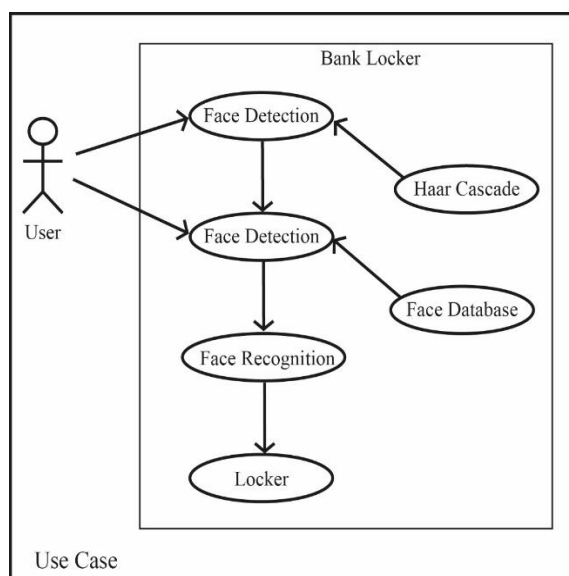
Step 4: In liveness detection three times aspect value is calculated if eye is blinked means liveness is detected.

Step5: Then we created web application in that we checked camera live stream .finally we all merged based on camera output we face and liveness is detected .

3.2 Local Binary Pattern Histogram

- Step 1: Convert the image into grayscale space.
- Step 2: For each pixel in the image, select the P neighborhoods that surround the central pixel.
- Step 3: Take the center pixel and set it as a threshold for its P neighbors.
- Step 4: Set to 1 if the value of the adjacent pixel is greater than or equal to the value of the center pixel, 0 otherwise.
- Step 5: Now compute the LBP value: Sequentially counterclockwise, write a binary number consisting of digits adjacent to the center pixel. This binary number (or it's decimal equivalent) is called LBP-central pixel code and, further, is used as a characteristic selected local texture.

3.3 Use Case Diagram

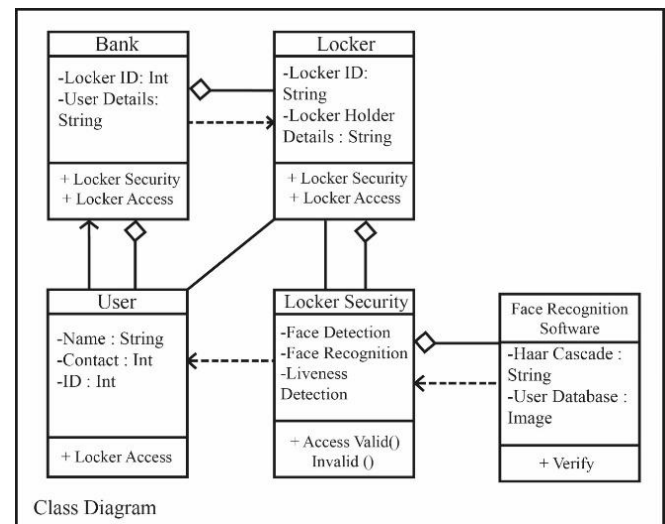


A use case diagram is used to represent the dynamic behaviour of a system. It encapsulates system functionality by incorporating use cases, actors and

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.



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. Experimental setup

1. Choose a suitable hardware setup: You will need a camera with good resolution and a processing unit such as a computer or a Raspberry Pi to process the data. You may also need additional sensors such as infrared sensors or microphones depending on your requirements.
2. Install and configure the necessary software: You will need to install software for face detection

and recognition, as well as liveness detection. You may also need to develop custom algorithms depending on your specific needs. Some popular software packages for face detection and recognition include OpenCV, Dlib, and FaceNet.

3. Collect a dataset: You will need to collect a dataset of faces to train your system. This dataset should include a diverse range of faces from different genders, ages, and ethnicities.
4. Train the system: You will need to use the collected dataset to train the face detection and recognition system. You will also need to train the liveness detection system to detect if the face is a real person and not a photograph or a video.
5. Test the system: Once the system is trained, you will need to test it with a set of test data. This data should include both real and fake faces to evaluate the accuracy and robustness of the system.
6. Deploy the system: Once the system is tested and validated, you can deploy it in the bank safe. The system should be integrated with the safe's locking mechanism so that only authorized personnel with a verified face can access it.
7. Evaluate the system: Once the system is deployed, you should evaluate its performance periodically to ensure that it is still accurate and robust. You should also make any necessary adjustments or upgrades to improve its performance.

6. Test Cases

1. Positive face recognition: A genuine bank employee approaches the safe and the system correctly recognizes their face and grants access.
2. Negative face recognition: An unauthorized person approaches the safe and the system correctly identifies their face as not being authorized, and denies access.
3. Face recognition with masks: The system is tested with individuals wearing different types of masks (cloth, surgical, N95), and the system correctly recognizes their face despite the masks.

4. Face recognition with accessories: The system is tested with individuals wearing different types of accessories such as hats, glasses, or scarves, and the system correctly recognizes their face despite the accessories.
5. Liveness detection: The system is tested with different types of spoofing attacks, such as using a photograph, a video, or a mask, and the system should correctly detect and deny access to the safe.
6. Lighting conditions: The system is tested in different lighting conditions, such as bright, dim, or backlit, and the system should still correctly recognize faces and grant or deny access as appropriate.
7. Environmental noise: The system is tested in noisy environments, such as with people talking or machinery running, and the system should still correctly recognize faces and grant or deny access as appropriate.
8. System performance: The system's response time and accuracy are measured, and the results are compared to the system's specifications to ensure that it is meeting the requirements.
9. System reliability: The system is run for an extended period, and the number of false positives and false negatives is measured to ensure that the system is reliable.

6.1 Testing Strategy

1. Functional Testing: This type of testing verifies the functional requirements of the system. In this case, it would include testing the face detection and liveness detection functionalities to ensure they work as expected.
2. Integration Testing: Integration testing checks how the system integrates with other systems, such as the bank's existing security system. It ensures that data is exchanged correctly between systems and that there are no compatibility issues.
3. Performance Testing: Performance testing evaluates the system's ability to perform under

expected loads and stress levels. It tests how quickly the system responds to user requests and ensures that it can handle multiple requests simultaneously.

4. **Security Testing:** Security testing checks the system's ability to prevent unauthorized access to the bank's assets. It includes testing the system's ability to detect and prevent fraud, such as using photographs or videos of authorized personnel to gain access to the safe.

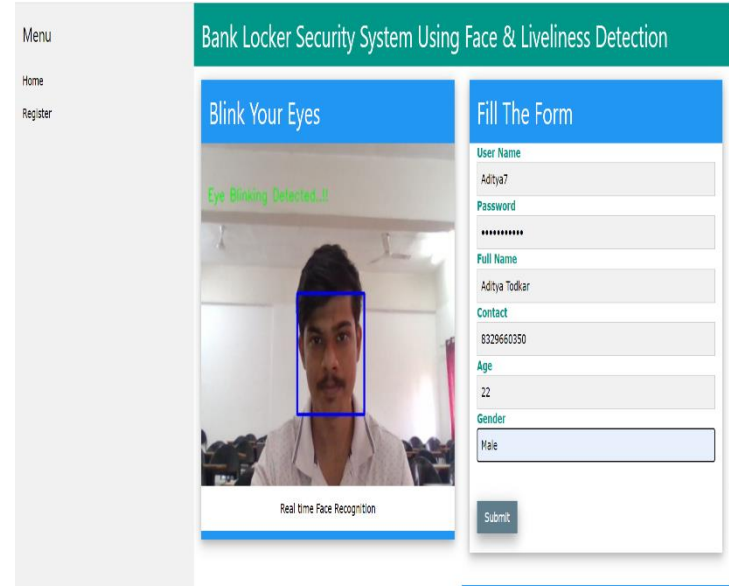
6.2 Test Report

Test case	Description	Expected Result	Actual Result	Pass/Fail
Face Detection	Capture an image of an authorized personnel's face and compare it with the authorized personnel's data base.	System should allow access to the safe	System should allow access to the safe	Pass
	Capture an image of an unauthorized person's face and compare it with the authorized personnel's data base.	System should deny access to the safe	System should deny access to the safe	Pass
Liveliness Detection	Ask an authorized personnel to blink their eyes, move their head, or speak a specific phrase.	System should allow access to the safe if the actions are performed correctly.	System should allow access to the safe if the actions are performed correctly.	Pass
	Ask an authorized personnel to blink their eyes, move their head or speak a specific phrase.	System should deny access to the safe	System should deny access to the safe	Pass
	Ask an authorized personnel to blink their eyes, move their head or speak a specific phrase.	System should deny access to the safe	System should deny access to the safe	Pass
Integration	Integrate the system with the banks.	The system should work seamlessly.	The system should work seamlessly.	Pass
	Add an authorized personnel to the system.	The system should allow newly authorized	The system should allow newly authorized	Pass

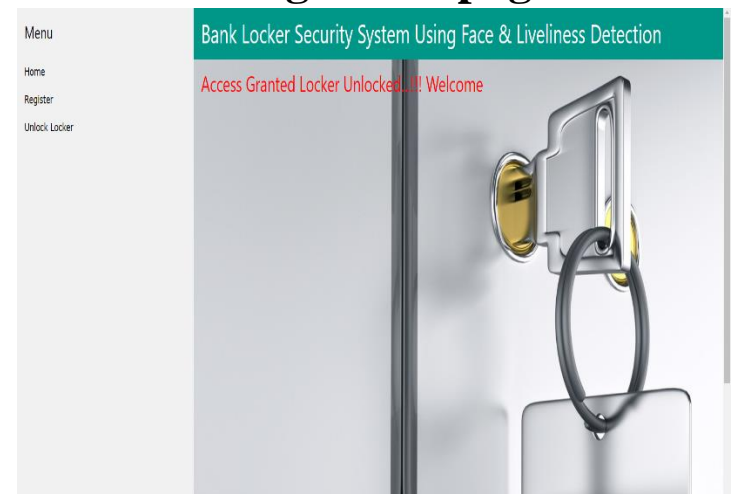
		personnel to the access the safe.	personnel to the access the safe.	
	Remove an authorized personnel from the system.	The system should deny access to the safe of the removed personnel.	The system should deny access to the safe of the removed personnel.	Pass
Security Alert	Attempt unauthorized access to the safe	The system should alert security personnel of the attempted unauthorized access.	The system should alert security personnel of the attempted unauthorized access.	Pass

7. Project Demonstration

Login Page



Access granted page



8. 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.

9. 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.

10. 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.

11. 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

12. References

- [1] G. Kim, S. Eum, J. K. Suhr, D. I. Kim, K. R. Park, and J. Kim, Facial liveliness 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.