

BANK LOCKER SECURITY SYSTEM USING MACHINE LEARNING WITH FACE & LIVENESS DETECTION

Nikhil Yeole, Rohan Alhat, Sushant Thorve, Vaibhav Shinde, Prof.Tushar Phadtare

Computer Department ,JSPM's BSIOTR, Wagholi, Pune, Maharashtra

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 due to their convenience and acceptance. Especially in offline environments, where face images from ID documents are matched to digital selfies. In fact, comparisons of selfies with IDs have also been used in some broader programs these days, such as automatic immigration control. The great difficulty of such a process lies in limiting the differences between comparative facial images given their different origins. we propose a novel architecture for cross-domain matching problem based on deep features extracted by two well-referenced Convolutional Neural Networks(CNN). The results obtained from the data collected, called Face Bank, with more than 93% accuracy, indicate the strength of the proposed face-to-face comparison problem and its inclusion in real banking security systems.

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

1. INTRODUCTION:

Although the recognition performance of biometric system is nowadays quite satisfactory for most applications, much work is still necessary to allow convenient, secure and privacy-friendly systems to be designed. In face recognition, the usual attack methods may be classified into several categories. The idea of classifying is based on what verification proof is provide to face verification system, such as a stolen photo, stolen face photos, recorded video, 3D face models with the abilities of blinking and lip moving, 3D face models with various expressions and so on.

The idea of classifying is based on what verification proof is provide to face verification system, such as a stolen photo, stolen face photos, recorded video, 3D face models with the abilities of blinking and lip moving, 3D face models with various expressions and so on. In this paper, we proposed a method of live face detection to resist the attack using a

photograph. on what verification proof is provide to face verification system, such as a stolen photo, stolen face photos, recorded video, 3D face models with the abilities of blinking and lip moving, 3D face models with various expressions and so on. The idea of classifying is based on what verification proof is provide to face verification system, such as a stolen photo, stolen face photos, recorded video, 3D face models with the abilities of blinking and lip moving, 3D face models with various expressions and so on. In this paper, we proposed a method of live face detection to resist the attack using a photograph. Our algorithm is based on analysis of movement of facial components, especially eyes, in sequential images. Generally in sequential face images there are very little variations in shape of face and facial components. But eyes have much larger variation in shape because we always blink and move the pupils unconsciously. So we detect eyes in sequential face images and compare the shape of each eye region to decide whether the input face image is a real face or a photograph.

1.2 MOTIVATION-

Liveness detection has been a very active research topic in fingerprint recognition and iris recognition communities in recent years. But in face recognition, approaches are very much limited to deal with this problem. Liveness is the act of differentiating the feature space into live and non-living. Imposters will try to introduce a large number of spoofed biometrics into system. With the help of liveness detection, the performance of a biometric system will improve. It is an important and challenging issue which determines the trustworthiness of biometric system security against spoofing.

2. Methodology

A.Problem statements-

With the popularity of face recognition, criminals will try to attack the face recognition system, for which liveness detection has become an important part of the authentication system. Among the current liveness detection algorithms, methods based on machine learning. Therefore, we proposed this method in this paper.

B.Model framework-

The proposed framework that combines Face Net with liveness detection is shown in

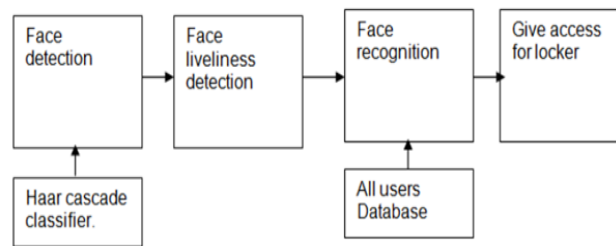


Figure1. Model framework

In above block diagram we are going to detect face using haar cascade classifier which algorithm for detection of face. After detection of face, system will decide the face is real or fake by using liveness detection technique. Liveness detection technique is the act of differentiating the feature space into live and non-living.

In this system we need a way to detect faces and eyes in real-time. So we are using - cascade classifier to performs these tasks. In this haar cascade classifier Cascade is a machine learning object detection algorithm used to identify objects in an image or video.

C.Architecture diagram-

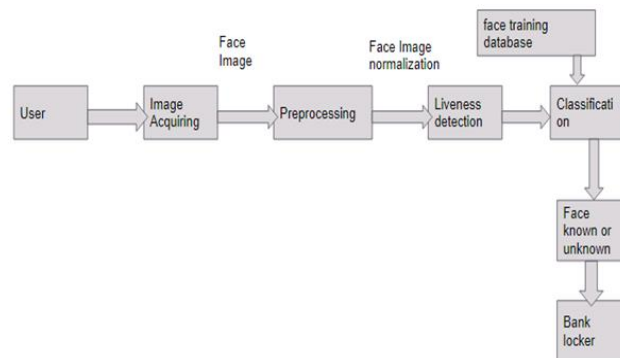


Figure 2: Architecture diagram

In this diagram we are going to implement eye-blink detection & face recognition Based on LBPH algorithm. The algorithm works in real time through a webcam and displays the person's name. The program runs as follows:

1. Detect faces in each frame generated by the webcam.
2. For each detected face, detect eyes.
3. Detect liveness of the face i.e. eyes are blinking or not

4. Recognize face and access the respected locker of the user.

E. Hardware and Software Requirement-

1) Software Requirement:

Python idle/pycharm development environment for Python coding.

Sublime for html and css coding.

2) Hardware requirement

Pc/Laptop (4gb Ram/ above i3 processor)

F. Algorithm Used:

1.CNN Algorithm-

- It is used to determine the local features in the face.
- It works by using basic LBP operator. in a matrix originally of size 3×3, the values are compared by the value of the centre pixel, then binary pattern code is produced.

The LBP code is obtained by converting the binary code into decimal one

example		
6	5	2
7	6	1
9	8	7

thresholded		
1	0	0
1	0	0
1	1	1

weights		
1	2	4
128	0	8
64	32	16

Pattern = **11110001**

LBP = $1 + 16 + 32 + 64 + 128 =$ **241**

C = $(6+7+8+9+7)/5 - (5+2+1)/3 =$ **4.7**

2. LBP Histograms (Local Binary Pattern)-

Each pixel of an image is labeled with an LBP code. First it will divide the image to several blocks. Then it will start calculating the LBP histogram for each block after that it will combine every LBP histogram for that image then you will get all the LBP histograms into one vector

Flowchart of LPBH

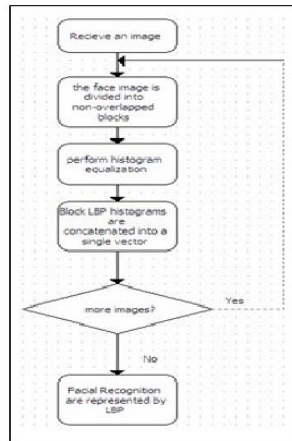


Figure 3-2-3: Flowchart of LBP Process

- 1) Capture an image then store it.
- 2) The process will divide the image to several blocks.
- 3) Histograms will be calculated for each block, then a histogram will be concentrated into a single vector.
- 4) As a result, the facial recognition is represented by LBP and the shape of the face is obtained by concentration of different local histograms.

3. Application

1. It can be used in attendance system in school or college.
2. Home security.
3. ATM security.

4. Conclusion

In this paper, we have proposed a machine learning based face detection-recognition and liveness detection for bank locker. In this project user will use bank locker by using face detection and liveness technique. This face detected locker is much better than traditional locker because it does not require any traditional key to unlock the locker. It is highly reliable system to ensure the security of our valuables.

5. Future scope

1. The System can be implemented in embedded processors such as raspberry PI.
2. Additional Securities can be used such as fingerprint recognition.
3. The System can be further extended to other banking services.

REFERENCES

- [1] G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink -based anti-spoofing in face recognition from a generic webcam," 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 eye blink 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.