IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 3, Issue 5, April 2023

Impact Factor: 7.301

Bank Locker Security System using Machine Learning with Face and Liveness Detection

Abhijeet Bade[1], Akash Munde[2], Sushant Hipparkar[3], Shubhangi Kharat[3], Prof. Sonali Sethi[5]

Student, Department of Computer Engineering[1,2,3,4]
Professor, Department of Computer Engineering[5]
NBN Sinhgad School of Engineering, Pune, Maharashtra, India

Abstract: *In today's day to day life, security plays an important role. Every person has accessories like gold, jewelry and cash. It is not enough to have these accessories, but security of this is important, for this security reason we keep them in bank lockers. for the bank locker security many tools are used in todays days some are fingerprint recogination, face detection, liveness detection ,password for lockers.In face to face detection Convolutional Neural Networks(CNN) algorithm features plays important role with more than 93% accuracy.*

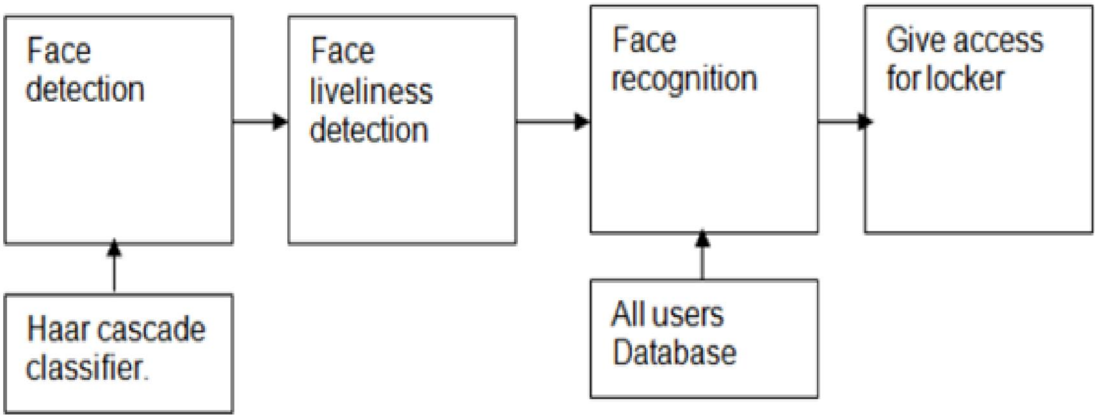
Keywords: Convolutional Neural Networks(CNN), Face Bank, automatic immigration control, Face-to-face comparison problem.

I. INTRODUCTION

The recognition performance of biometric system is these days satisfactory for several applications, a lot of works are necessary to allow secure and privacy-friendly systems. Liveness detection is very active topic in fingerprint recognition and iris recognition research 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. attackers 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 performance of biometric system security against spoofing. . It is an easy way to spoof face recognition systems by facial pictures such as portrait photograph on order to protect against such spoofing attacks , a secure system needs liveness detection to ensure the security of the system.

1.1 Model Framework

The proposed system that combines Face Net with liveness detection is shown in Figure1.

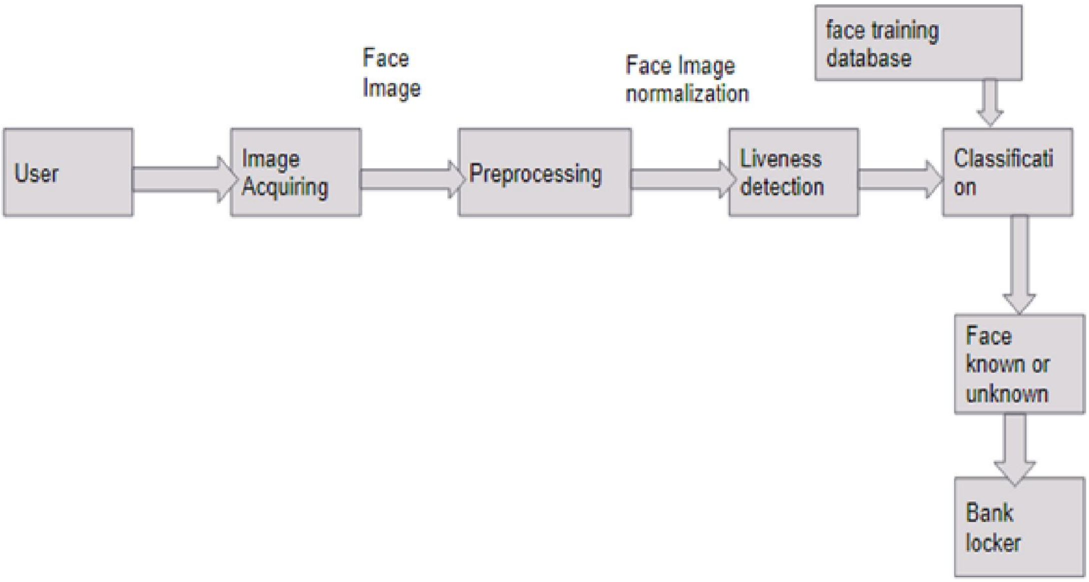


In diagram we tend to square measure visiting notice face mistreatment haar cascade classifier that algorithmic program for detection of face. once detection of face, system can decide the face is real or faux by mistreatment aliveness

DOI: 10.48175/IJARSCT-9331

detection technique. aliveness notice ion technique is that the act of differentiating the feature area into live and non-living In this method we wish the way to detect faces and eyes in period. therefore we tend to square measure mistreatment -cascade classifier to performs these tasks. Throughout this haar cascade classifier Cascade might be a machine learning object detection algorithmic program used to establish objects in an exceedingly image or video.

1.2 Architecture Diagram



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.

II. LITERATURE REVIEW

Gang Pan et al.[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 ar 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 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 ar 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].

DOI: 10.48175/IJARSCT-9331

III. CONCLUSION

In this paper, we do project on a machine learning based mostly face detection-recognition and aliveness detection for bank locker. it's reliable system to confirm the safety of our valuables resources.

This system provides a simple path for the future development of novel and more secured face liveliness detection approach for bank locker security.

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]. [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 HumanIdentification, 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.