First International Conference on Computer Engineering
International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
Volume 5 Issue 8, November-December-2020

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

Akash Mote[1], Kanhaiya Patil[1], Akshay Chavan[1], Mrunal Saraf[1], Prof. Ashwini Pandagale[2]
[1]Department of Computer Engineering, Dr. D. Y. Patil School of Engineering, Lohegaon, Maharashtra India
[2]Professor, Department of Computer Engineering, Dr. D. Y. Patil School of Engineering, Lohegaon, Maharashtra India

ABSTRACT

Ensuring the security of transactions is currently the biggest threat 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. Based on deep features extracted by two well-referenced Convolutional Neural Networks(CNN).we suggest a novel architecture for cross-domain matching problem . 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.

I. INTRODUCTION

Much work is still necessary to allow convenient, secure and friendly systems to be designed.the recognition performance of biometric system is satisfactory for most applications, In face recognition, the usual attack methods may be classified into certain categories.

The concept of classifying is placed on what verification proof is equip to face verification system, such as a lifted photo, lifted face photos, recorded video, 3D face models with the skills of blinking and lip moving, 3D face models with various expressions and so on. The concept of classifying is placed on what verification proof is provide to face verification system, like a stolen photo, stolen face photos, recorded video, 3D face models with the skills 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 lifted photo, lifted face photos, recorded video, 3D face

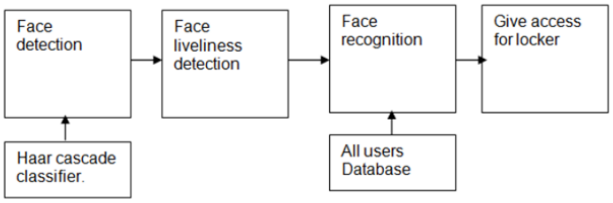
models with the skills of blinking and lip moving, 3D face models with various expressions and so on. The concept of classifying is placed on what verification proof is provide to face verification system, such as a stolen photo, lifted face photos, recorded video, 3D face models with the skills of blinking and lip moving, 3D face models with various expressions and so on. In this paper, to resist the attack using a photograph we proposed a method of live face detection Our algorithm is placed on analysis of movement of facial components, especially eyes, in sequential images.In sequential face images there are very small variations in shape of face and facial elements. But eyes have larger variation in shape because we always blink,move the pupils unconsciously. So we spot 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.

A. Problem Statement

With the demand of face recognition, criminals will try to attack the face recognition system, for which liveness detection has become an crucial 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

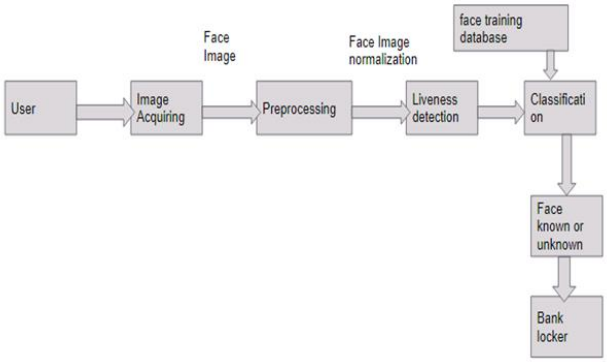
The proposed framework that combines Face Net with liveness detection is shown in the figure.



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



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 human'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.

II. LITERATURE REVIEW

Gang Pan et al.[1] present a spoofing against photograph in face recognition using real time liveness detection using spontaneous eye blinking. This method requires only a generic camera no other hardware to avoid spoofing attack in nonintrusive manner. Eye blinking is physical process which instantaneously opens and closes lids many times in a minute. Generic camera captures 15 frames per seconds, it gives two frames of faces which used as clue against spoofing attack. Two captured frames in multiple frames to check liveness, so user should be co-operative.

Face liveness detection [3] has been proposed to improve the reliability and security of face recognition system. The fake faces are distinguished from the real ones using different classification techniques.

In this paper, we propose a single image-based fake face detection method based on frequency and texture analyses for discriminating 2-D paper masks from the live faces. For the frequency analysis, we have carried out power spectrum based method [4] which exploits not only the low frequency information but also the information residing in the high frequency regions. Moreover, widely used Local Binary Pattern (LBP) [5]. In face recognition, the usual attack methods may be classified into various different types. The basic ideology of classifying is based on what verification proof is provided to face verification system, such as a stolen face photos, recorded video, 3D face models, fake photos with the abilities of blinking and lip moving, 3D face models with various expressions and many more to mention[6].

The main goal of our paper is to design and implement a bank locker security system solely based on RFID and GSM technology which has to be organized in the bank, secured offices and homes. In our system only authentic person can be the one recovering the money from the bank locker. The sequence are considered as independent. HMM produces features from finite state set. Typical eye blink activity using HMM feature finds spoofing attack.

Anjos et al. [2] proposed a method based on foreground or background motion correlation for checking liveness of user. This method classified in motion detection. This method works on correlation between head rotation of user and its background. To find correlation author uses fine grained motion direction. Optical flow is used to find the direction of motion. This approach is easy process but require RFID reader reads the identification number from passive tag and sends it to the microcontroller, if the identification number is valid then microcontroller sends the SMS request to the authenticated person mobile number, for the original password to open the bank locker, if the person enters the password to the microcontroller which will verify the passwords entered by the key board and received from authenticated mobile number . If these two passwords are matched the locker will be opened otherwise it will be remain in locked position[7].

Initially pattern flow are collected as the datasets are maintained in bank agent server. The device has a camera to capture the pattern flow of user and sends it for processing, features of the logic were compared and user was recognized. In addition to the authentication of user there is another system to identify the user before that RFID tag checking is needed. Image processing is used and the keypad password is needed for another level of security. In future bank can implement this type of authentication option for banking and from this project it shows that all the bank accounts can be accessed without using cards through this face recognition efficiently and safely [8].

Access control system forms a essential link in a security chain. The biometric password and pattern based security system presented here is an access control system that allows only the authorized persons to access a restricted area. We have implemented a locker security system based on fingerprint, password and GSM technology

containing door locking system which can activate, authenticate and validate the user and unlock the door in real time for locker secure[9].

They say perhaps the most important application of accurate personal identification is acquiring limited access systems from malicious attacks. Among all the presently employed biometric techniques, biometric identification systems have received the most attention due to the long history of fingerprints and their extensive use in forensics. Our paper deals with the issue of selection of an optimal algorithm for biometric suiting in order to design a system that matches required specifications in performance and accuracy[10].

III. CONCLUSION

In this paper, we have proposed a machine learning based face detection-recognition and liveness detection for bank locker. It is highly reliable system to ensure the security of our valuables.

IV. 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]. 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.

[9]. Li, L.; Feng, X.Y.; Jiang, X.Y.; Xia, Z.Q.; Hadid, A. Face antispoofing via deep local binary patterns. In Proceedings of the IEEE International Conference on Image Processing, Beijing, China, 17 20 September 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 101 105.

[10]. Wang, S.Y.; Yang, S.H.; Chen Y, P.; Huang, J.W. Face liveness detection based on skin blood flow analysis. Symmetry 2017, 9, 305.