IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 10, October 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 10, October 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1010010 |

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

Adam Ussamuddin Mir[1], Atharva Dahotre[2], Om Chougule[3], Bhavesh Dhobe[4], Prajwalita Dongare[5]

Student, Department of Computer Engineering, Sinhgad Academy of Engineering, Pune, India[1,2,3,4]

Professor, Department of Computer Engineering, Sinhgad Academy of Engineering, Pune, India[5]

ABSTRACT: Ensuring the security of deals is presently one of the biggest challenges facing banking systems. The use of biometric authentication of drugs attracts huge sums of money from banks around the world due to their convenience and acceptance. Especially in offline surroundings, 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, similar to automatic immigration control. The great difficulty of such a process lies in limiting the differences between relative facial images given their different origins. We propose a new armature for cross-domain matching problems grounded on deep features uprooted by two well- substantiated Convolutional Neural Networks(CNN). The results obtained from the data collected, called Face Bank, with further than 93 delicacies, indicate the strength of the proposed face- to-face comparison problem and its addition in real banking security systems.

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

I. INTRODUCTION

Although the recognition performance of biometric systems is these days quite satisfactory for several applications, a lot of work remains necessary to allow convenient, secure and privacy-friendly systems to be designed. In face recognition, an equivalent previous attack strategy is additionally classified into many classes. The idea of classifying depends on what verification proof is given to the face verification system, sort of a purloined icon, purloined face photos, recorded video, 3D face models with the skills of blinking and lip moving, 3D face models with varied expressions thus on. The thought of classifying depends on what verification proof is given to the face verification system, sort of a purloined icon, purloined face photos, recorded video, 3D face models with the skills of blinking and lip moving, 3D face models with varied expressions and so on. throughout this paper, we tend to projected some way of live face detection to resist the attack using a photograph on what verification proof is give to face verification system, sort of a purloined icon, purloined face photos, recorded video, 3D face models with the skills of blinking and lip moving, 3D face models with varied expressions thus on. The thought of classifying depends on what verification proof is given to the face verification system, completely different expression variety of a purloined icon, purloined face photos, recorded video, 3D face models with the skills of blinking and lip moving, 3D face models with varied expressions and so on. Throughout this paper, we tend to project a way of live face detection to resist the attack using a photograph. Our formula relies on analysis of movement of facial parts, particularly eyes, in sequent pictures. Usually in sequential face pictures there are very little variations in form of face and facial parts. However, eyes have a lot of larger variation in form as a result of which we tend to continually blink and move the pupils unconsciously. Thus we tend to observe eyes in sequent face pictures and compare the shape of each eye region to create a call whether or not the input face image can be a true face or a photograph.

A. Problem statement

With the popularity of face recognition, criminals can decide to attack the face recognition system, that aliveness detection has become an important part of the authentication system. Among these aliveness detection algorithms, ways supported machine learning. Therefore, we tend to project this methodology throughout this paper.

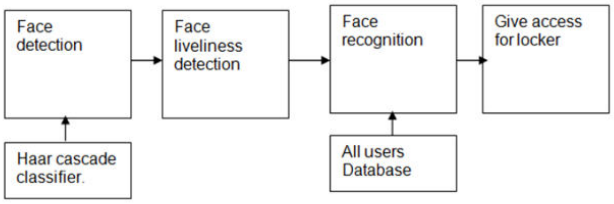
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 10, October 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1010010 |

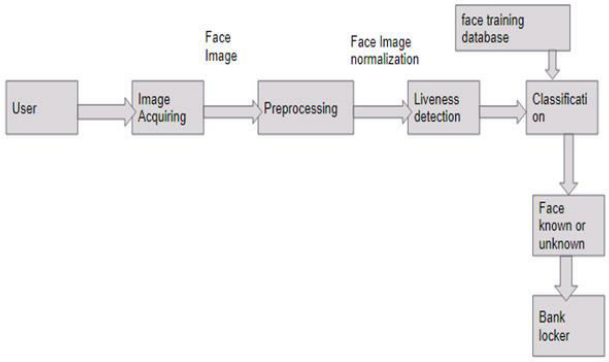
B. Model framework

The proposed frame that combines Face Net with liveness discovery is shown in Figure1.



On top of illustration we tend to square measure visiting notice face mistreatment haar waterfall classifier that algorithmic program for discovery of face. formerly discovery of face, system can decide the face is real or dummy by mistreatment aliveness discovery fashion. Aliveness notice in fashion is the act of discerning the point area into live and non-living In this system we wish to describe faces and eyes in period. Thus we tend to square measure mistreatment- waterfall classifiers to perform these tasks. Throughout this haar waterfall classifier Cascade might be a machine learning object discovery algorithmic program used to establish objects in an exceedingly large image or videotape.

C. Architecture diagram



In this diagram we tend to square measure attending to implement eye-blink detection & face recognition supported LBPH algorithmic programs. 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) give a spoofing against snap in face recognition exploitation real time physiological property discovery exploitation robotic eye blinking. This methodology needs solely a general camera, no different tackle to avoid spoofing attack in non intrusive manner. Eye blinking is a physical system that in a flash opens and closes lids Again and formerly more in an exceedingly} veritably nanosecond. The general camera captures fifteen frames per seconds, it provides 2 frames of faces that are used as indication against spoofing attack. 2 captured frames in sequence are allowed - about as freelance. HMM produces options from a finite state set. Typical blinking exertion exploitation HMM point finds spoofing attack. Anjos et al.(2) planned how to support focus or background stir correlation for checking physiological properties of stoners. This methodology is classified in stir discovery. This methodology works on correlation between head gyration of a stoner and its background. To go looking out for correlation the author uses fine grained stir direction. optic inflow is used to hunt out the direction of stir. This approach is an easy system that still needs multiple frames to check physiological properties, therefore stoner ought to be united. Face physiological property discovery(3) has been planned to support the responsibility and security of face recognition systems. The

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 10, October 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1010010 |

dummy faces are distinguished from the 000 bones exploitation in completely different bracket ways. During this paper, we tend to propose one image- grounded dummy face discovery methodology supported frequency and texture analyses for differencing 2- D paper masks from the live faces. For the frequency analysis, we've got applied power diapason primarily grounded methodology(4) that exploits not solely the low frequency word but still jointly the word abiding among the high frequency regions. also, widely used native Binary Pattern(LBP)(5). In face recognition, the quality attack strategies may indeed be classified into numerous classes. the idea of classifying depends on what verification evidence is give to face verification system, kind of a purloined picture, purloined face prints, recorded videotape, 3D face models with the capacities of blinking and lip moving, 3D face models with multitudinous expressions and so on(6). The best thing of this paper is to vogue and apply a bank locker security system supported RFID and GSM technology which could be organized in banks, secured services and homes. Throughout this system a solely authentic person recovers cash from a bank locker. The RFID anthology reads the id range from unresistant label and shoot to the microcontroller, if the id range is valid also microcontroller shoot the SMS request to the proved person mobile range, for the primary password to open the bank locker, if the person shoot the password to the microcontroller, which may corroborate the watchwords entered by the crucial board and entered from proved mobile. if these 2 watchwords are matched the locker is opened else it's going to stay in bolted position(7). originally pattern inflow unit of dimension collected as datasets and maintained in bank agent garçon. The machine includes a camera to capture the pattern inflow of stoner and transferred for system choices of the sense were compared and stoner where honoured. Also to the authentication of stoner there is another system to spot the stoner before that RFID little indefinite volume checking is needed. Image system is used and information data input device identification is needed for a fresh position of security. An unborn bank can apply this kind of authentication chance for banking and from this design shows that everyone's bank accounts are penetrated whereas not exercise cards through this face recognition with effectiveness and safely(8). Access system forms a vital important} link during a} terribly veritably security chain. The point associated identification grounded security system given then AN access system that enables simply authorized persons to pierce a confined house. We have enforced a locker security system supporting point identification and GSM technology containing a door lockup system which might spark, evidence and validate the stoner and unlock the door in real time for locker secure(9). They say maybe the foremost veritably important operation of correct particular identification is securing defined access systems from vicious attacks. Among all the presently utilised biometric techniques, point identification systems have entered the foremost attention due to the long history of fingerprints and their ferocious use in forensics. This paper deals with the difficulty of selecting an associated optimum formula for point matching, therefore in vogue a system that matches needed specifications in performance and delicacy(10).

III. CONCLUSION

In this paper, we've got a machine learning project based mostly on face detection-recognition and aliveness detection for bank lockers. It's an extremely reliable system to confirm the safety of our valuables.

REFERENCES

[1] G. Pan, L. Sun, Z. Wu, and S. Lao, “Eyeblink -based anti-spoofing in face recognition from a generic web camera,” 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.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 10, October 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1010010 |

[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 anti spoofing 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.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details