International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 01 | January - 2023 Impact Factor: 7.185 ISSN: 2582-3930

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

Prof. Sunil M. Kale
(Project Guide)
Sandip Institute of Technology and Research Centre
Savitribai Phule Pune University
Nashik, Maharashtra, India

Anuja Nair
Sandip Institute of Technology and Research Centre
Savitribai Phule Pune University
Nashik, Maharashtra, India

Manasi Pagar
Sandip Institute of Technology and Research Centre
Savitribai Phule Pune University
Nashik, Maharashtra, India

Kiran Pagar
Sandip Institute of Technology and Research Centre
Savitribai Phule Pune University
Nashik, Maharashtra, India

Esha Kamble
Sandip Institute of Technology and Research Centre
Savitribai Phule Pune University
Nashik, Maharashtra, India

ABSTRACT

One of the main problems that financial systems are currently facing is ensuring the security of transactions. Banks from all over the world spend a significant amount of money using biometric authentication of consumers because it is convenient and widely used. Particularly in offline settings where digital selfies and ID document facial photos are matched. In reality, nowadays, more extensive programs like automatic immigration control also use selfie-ID comparisons. Limiting the discrepancies between comparative facial photos given their various origins is the procedure's greatest challenge. We suggest a unique architecture based on deep features derived by two well-referenced convolutional neural networks for the cross-domain matching problem (CNN). The results from the data collection, known as Face Bank, show that the proposed face-to-face comparison problem is strong and should be included into actual banking security systems with more than 93% accuracy.

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

1.INTRODUCTION

Although the recognition performance of biometric systems is now quite satisfactory for a variety of applications, much work remains to be done in order to design systems that are convenient, secure, and privacy-friendly. An equivalent previous attack strategy in face recognition is also classified into many classes. The concept of classifying is dependent on what verification proof is provided to the face verification system, such as a stolen icon, stolen face photos, recorded video, 3D face models with the ability to blink and move their lips, 3D face models with various expressions, and so on. Throughout this paper, we have projected some method of live face detection to resist the attack using a photograph. Face verification system is given verification proof in the form of a stolen icon, stolen face photos, recorded video, 3D face models with the ability to blink and move their lips, 3D face models with various expressions, and so on.

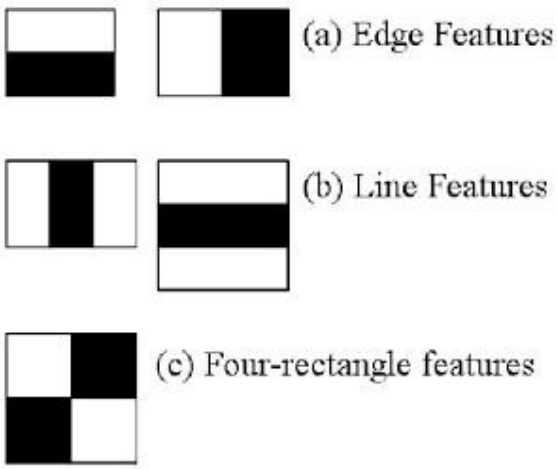
We tend to project a method of live face detection

to resist the attack using a photograph throughout this paper. Our formula is based on the movement of facial parts, particularly the eyes, in subsequent images. Typically, there are very few variations in the shape of the face and facial parts in subsequent face pictures. However, eyes have a lot more variation in shape because we constantly blink and move the pupils unconsciously. As a result, we tend to observe eyes in subsequent face pictures and compare the shape of each eye region to determine whether the input face image is a true face or a photograph.

Haar Cascade Classifier

In their 2001 publication, "Rapid Object Recognition with a Boosted Cascade of Simple Features," Paul Viola and Michael Jones proposed an efficient object detection technique that uses Haar feature-based cascade classifiers. A cascade function is trained using a large number of both positive and negative images in this machine learning-based approach. Object detection in other photos is then performed using it.

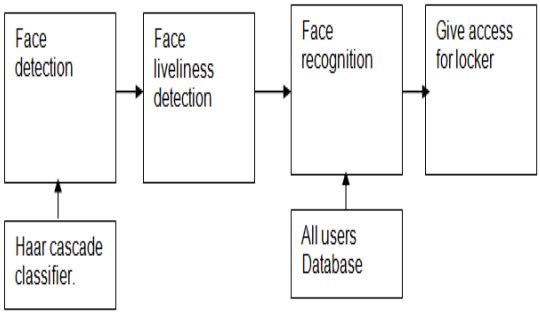
Here, facial detection will be used. The classifier must first be trained using a large number of positive images (images of faces) and negative images (images without faces). After that, we must extract its features. This uses the haar features indicated in the image below. They are a perfect match for our Convolutional kernel. A single feature makes up each.



A) Problem Framework

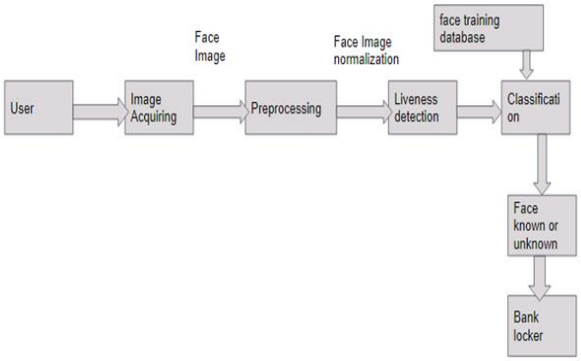
Due to the popularity of facial recognition, thieves may choose to attack the system, and aliveness detection has grown to be a crucial component of the authentication process. Among these aliveness detection algorithms, machine learning was supported. We will therefore use this methodology throughout the entire study.

B) Model framework



We tend to notice face abuse using a haar cascade classifier, an algorithmic program for face detection, in the diagram up top. Once a face is detected, the system can determine if it is real or fake by using an aliveness detection algorithm. Differentiating the feature region into living and non-living is the aliveness detection approach. With this technique, we want to be able to recognize faces and eyes over time. As a result, we frequently use a cascade classifier to carry out these jobs. This haar cascade classifier across Cascade is a machine learning approach that can be used to identify items in an extremely large image or video.

C) Architecture diagram



This diagram shows how the LBPH algorithmic software will be used to achieve eye-blink detection and face identification. The algorithmic program displays the person's name while operating in real time through a digital camera. This is how the program operates:

1. Take note of faces in every digital camera frame.
2. Look at the eyes for every face you can find.
3. Check to see if the face is alive by observing whether or not the eyes are blinking.
4. Identify yourself and enter the user's valued locker.

2.LITERATURE REVIEW

Gang Pan et al. [1] present a spoofing against photograph in face recognition using real-time physiological property detection via spontaneous eye blinking. To avoid spoofing attacks in a nonintrusive manner, this methodology requires only a generic camera and no other hardware. Eye blinking is a physical process that opens and closes the lids in a flash. Again and again in an extremely brief period of time. Generic cameras capture fifteen frames per second and provide two frames of faces that can be used as a clue against spoofing attacks. Two captured frames in sequence are considered freelance. HMM generates options based on a finite state set. A typical blinking activity exploiting the HMM feature detects a spoofing attack. Anjos et al. [2] planned how to use foreground or background motion correlation to test a user's physiological properties. This methodology is categorized as motion detection. This methodology is based on the correlation between the user's head rotation and the background. The author employs fine-grained motion direction to search for correlation. Optical flow is used to determine motion direction. This method is simple, but it requires multiple frames to check physiological properties, so the user must be cooperative. Face physiological property detection [3] is being developed to improve the dependability and security of the face recognition system. The fake faces are distinguished from the thousands by employing completely different classification techniques. We propose an image-based faux face detection methodology supported by frequency and texture analyses for distinguishing 2-D paper masks from live faces in this paper. For the frequency analysis, we used a power spectrum-based methodology [4] that makes use of not only low frequency information but also information from high frequency regions. Furthermore, native Binary Pattern (LBP) is widely used [5]. Quality attack strategies in face recognition can even be classified into several classes. The classification strategy is based on the verification evidence provided to the face verification system, such as a stolen image, stolen face images, recorded video, 3D face models with the ability to blink and move their lips, 3D face models with a variety of expressions, and so on [6]. The main objective of this article is to design and put into practice a bank locker security system that uses RFID and GSM technology that may be installed in banks, secure offices, and private residences. Using this technique, only the real individual can retrieve money from a bank safe. The microcontroller receives the passwords entered by the keypad and received from the documented mobile range after the RFID reader reads the identification range from the passive tag. If the identification range is valid, the microcontroller sends an SMS request to the documented person's mobile range for the primary countersign to open the bank locker. If these two passwords match, the locker will be unlocked; otherwise, it will remain in the bolted position [7]. Initial datasets for the pattern flow unit of measurement were gathered and kept on the bank agent server. The device has a camera to record the user's pattern of movement, which is then sent to be compared with the logic's method choices and the user identified. In addition to user authentication, there is another technique to identify users before RFID little long-term quantity checking is necessary. For an additional layer of security, the image approach is utilised and information data input device identification is necessary. Future banks may use this method of authentication, and this project's results demonstrate that it can be done efficiently and securely without the use of credit cards for all bank accounts [8]. Access control systems are an extremely crucial link in a chain of security. The security system with fingerprint-based identification described here is an access

system that only allows people who have been granted permission to enter a restricted home. We have put in place a locker security system that uses GSM, fingerprint, and identity technologies with a door lockup system that can instantly activate, verify, and activate the user. According to them, protecting restricted access systems from malicious attacks is possibly the most crucial application of accurate personal identity. Due to the lengthy history of fingerprints and their extensive usage in forensics, fingerprint identification systems have attracted the most interest among all currently used biometric approaches. In order to create a system that meets essential standards in performance and accuracy, it can be challenging to choose an optimal formula for matching fingerprints [10].

3.CONCLUSION

In this research, we provide a face detection-recognition and aliveness detection system for bank lockers that is based on machine learning. It is an incredibly trustworthy way to verify the security of our possessions.

4.REFERENCE

[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 International Conf. Comput. Vis. (ICCV), Oct. 2007, pp. 1-8.
[2] Anjos et al., "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 are the authors of this work. "Detecting face liveness with a monocular camera by combining eyeblink and scene context." Telecommunication Systems, vol. 47, no. 3-4, pp. 215-225, 2011.
[4] H. S. Choi, R. C. Kang, K.T. Choi, A. T. B. Jin, and J.H. Kim are the authors of this paper. Multiple Static Features are used to detect fake fingerprints. 48(4), Optical Engineering, 2009.
[5] A. Pietikainen, T. Ojala, and A. Local Binary Patterns for Multiresolution Gray-Scale and Rotation-Invariant Texture Classification. Pattern Analysis and Machine Intelligence in IEEE Transactions, 24
[6] "Live face detection based on the study of fourier spectra," in Biometric Technology for Human Identification, SPIE vol. 5404, pp. 296-303, 2004. J. Li, Y. Wang, T. Tan, and A. K. Jain.
[7] Person identification using lip texture analysis, International Conference on Digital Signal Processing, DSP, 2017, pp. 472-476. [7] Z. Lu, X. Wu, and R. He
[8] 3D convolutional neural network based on face anti-spoofing, Gan, J.Y., Li, S.L., Zhai, Y.K., and Liu, C.Y. pp. 1–5 in IEEE: Piscataway, NJ, USA, 2017, Proceedings of the International Conference on Multimedia and Image Processing, Wuhan, China, 17–19 March 2017.
[9] Li, L., Feng, X.Y., Jiang, X.Y., Xia, Z.Q., and A. Hadid. Deep local binary patterns are used for face antispoofing. IEEE International Conference on Image Processing, Beijing, China, September 17-20, 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 101-105.

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