IJIRCCE

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

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Special Issue 2, March 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

| International Conference on Recent Innovations in Engineering and Technology (ICRIET'23)|

| Sharadchandra Pawar College of Engineering, Pune, India |

|| Volume 11, Special Issue 2, March 2023 ||

Banking Security System using Face and Liveness Detection using Machine Learning and Image Processing

Tai Pawar[1], Dr. M.D.Rokade[2]

[1]PG Student, Sharadchandra Pawar College of Engineering, Dumbarwadi (Otur), Tal. Junnar, Savitribai Phule Pune University, Pune, India

[2]Asst. Professor, Department of Computer Engineering, Sharadchandra Pawar College of Engineering, Dumbarwadi (Otur), Tal. Junnar, Savitribai Phule Pune University, Pune, India

ABSTRACT: Classifiers designed for face liveness detection are traditionally trained on real-world images, where real-face images and corresponding face presentation attacks (PA) are highly overlapping. However, there has been little research into using a combination of real-world face images and face images generated by deep convolutional neural networks (CNN) to detect face liveness. Face recognition biometrics are now widely used. A face recognition system should not only recognize people's faces but also detect spoofing attempts using printed faces or digital presentations. Examining face liveness, such as eye blinking and lip movement, is a genuine spoofing prevention strategy. Nonetheless, this approach is rendered ineffective when dealing with video-based replay attacks. As a result, this system proposes a method of face liveness detection combined with a CNN (Convolutional Neural Network) classifier. The anti-spoofing method is comprised of two modules: the blinking eye module, which assesses eye openness and lip movement, and the ConvNet classifier module. Our CNN classification dataset can come from a variety of publicly available sources. We combined these two modules sequentially and used Python to create a simple facial recognition application. The results of the tests show that the created module can recognize various types of facial spoof attacks, such as those using posters, masks, or smart phones.

KEYWORDS:- Covid-19, Heart Rate Detection, Image processing, Machine Learning, Color Magnification (CM) Algorithm, Fast Fourier Transform (FFT) algorithm, Facial Video, etc.

I. INTRODUCTION

Nowadays, biometrics is one of the most widely used authentication technologies. Face recognition technology is one of them, and it is widely used due to its simplicity and accuracy. Face recognition technology is now being used in a wide range of facial spoof attacks, including those on smartphones, tablets, and laptop computers. Face recognition technology allows us to recognize other people. This facial recognition application works by photographing a person's face with a camera and then running the image through a specific algorithm to determine whether or not the face is recognized from a database [1]. Nonetheless, the facial recognition strategy has a flaw known as spoofing attacks. Facial recognition systems can't tell the difference between real faces and spoofing attacks like masks, videos, or photos. As a result, these flaws allow someone to deceive the machine. Furthermore, obtaining someone's face is far easier than obtaining other biometrics such as fingerprints. Using social media or a profile photo, you can easily obtain someone's face.[2].

II. RELATED WORK

- C. Yuan, Z. Xia, X. Sun and Q. M. J. Wu, [1] The authors of this article propose a system for dealing with this fingerprint animosity detection, as well as a workable anti-dismissal tool (FLD). Furthermore, the profound neural network (DCNN) based FLD methods were significantly different from most shallowness due to their quick operation, few parameters, and end-to-end self-learning. Methods for creating detailed features. Meanwhile, DCNN is confronted with two opposing challenges. On the one hand, multi-faceted perception (MLPs) continues to rise and is finally becoming stable. To increase the number of MLPs, the results will be reduced further. Then, adaptive DRNs are exploring ways to avoid the parameters learned falling into local optimization by automatically adjusting

the learning rate if such monitoring parameters (checking correctness) are stable. Finally, to improve the generalization of the model classifier, we propose improving the textures using the local gradient model method (LGP).

- Arpita Nema, [2] A "desktop anti-spoofing application" is proposed in this paper. This application uses a face recognition approach as well as an eye-blink count to detect liveness. The main phases of the application are face detection and recognition, as well as determining the user's liveness status. It has been demonstrated that liveness detection can prevent video playback attacks and the use of printed photographs to compromise security.

- M. Killioglu, M. Taskiran, N. Kahraman, [3] In this work, the authors focused on liveness detection for spoofing facial recognition systems using fake face movement. The authors developed a pupil direction observing system for anti-spoofing in face recognition systems using simple hardware. To begin, the eye region is extracted from a real-time camera using the Haar-Cascade Classifier with an eye region detection classifier that has been specially trained. Feature points were extracted and traced using the Kanade-Lucas-Tomasi (KLT) algorithm to minimize person head movements and obtain a stable eye region. The eye area is cropped from the real-time camera frame and rotated for stability. The pupils are then extracted from the eye area using a new improved algorithm.

III. PROPOSED WORK

This study proposes developing an anti-spoofing model with three major modules: face anti-spoofing detection, liveness detection, and criminal identification using CNN classifier. The operation scheme of this model is quite simple. The face anti-spoofing module will process the input and detect photos, posters, masks, or Smartphones. When a face is detected, the input is sent to the CNN classifier module, which determines whether the face is real or fake. The following input will be processed for the liveness detection module, which detects eye blinks and lip movements. If the input is processed by both modules, it is designated as a real face. The methodology we propose is made up of several general steps. The steps to develop the CNN classifier modules are:

I. Data collection,
II. Data pre-processing,
III. Model training,
IV. Model evaluation,
V. Testing

The life sign (liveness) detection module on the face has two sub-modules: blink detection and lip motion detection. The lip-movement-net module [22] is used in this module to detect lip motion. A simple Recurrent Neural Network (RNN)-based detector algorithm determines whether someone is speaking by analyzing their lip movements for 1 second of video using the Python programming language as part of the module. The detector module can be run in real-time on a video file or camera output. This module detects lip movement by first creating a filter to determine the upper and lower lip locations and then calculating the lips separation distance.

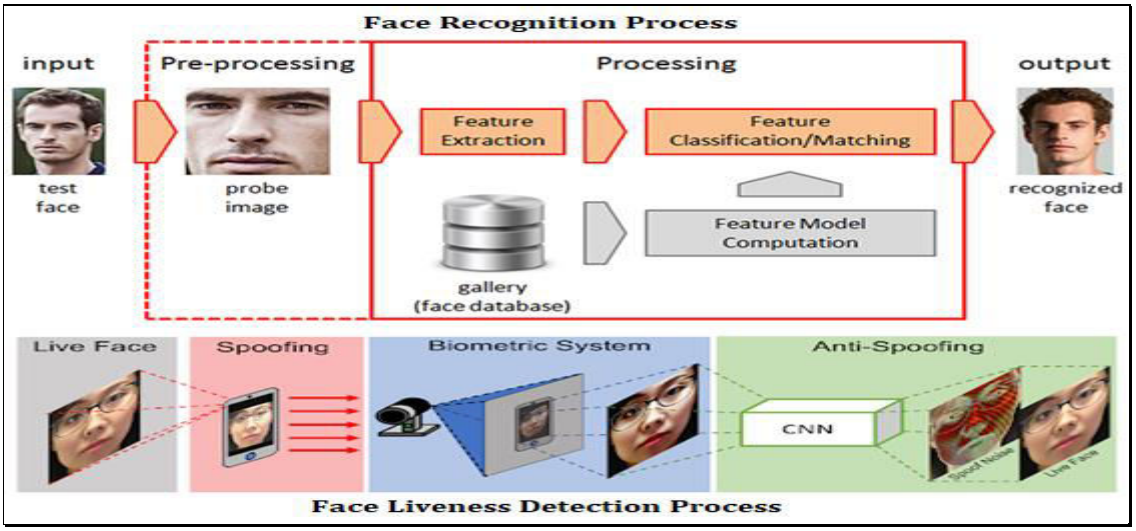

Fig.1: Proposed Research Architecture

To determine whether or not the eyes are blinking, a module developed in previous research [23] will be used. To determine whether or not the eyes are blinking, we use an eye area filter. The presence of the eye area in a person's face photo input can be detected by filters. The next step is to detect eye openness after capturing the eye area. This step employs the classification of eye openness. This classification produces a probability of opening the eye to the input image, which is then analyzed based on the value difference between the maximum and minimum eye openings. If the difference is significant, the eyes are blinking, which means that at least one transition between the eyes is open and closed. We prepared a dataset of faces with closed eyes and a dataset of faces with open eyes to create an eye classification module.

A. Face Liveness Detection:

Face recognition is a biometric system that compares data from people in a database of known faces to features extracted from someone's face. Researchers have developed a variety of methods for recognizing a person's face, overcoming challenges such as different facial expressions, different angles, and poor lighting. In the last decade, it has spread rapidly. It's been used in a variety of applications, including mobile device authentication [1, payments, and face recognition in attendance systems. It's also used in forensics and security access.

B. Face Recognition System:

Nowadays, some illegal intruders can launch spoof face attacks against systems using genuine users' photos, videos, and 3D face masks. Because face recognition only recognizes the identity of the face, it cannot prevent the attack of non-living faces, such as spoof face, which poses a significant threat to the system's security. Face recognition cannot prevent the attack of non-living faces, such as spoof faces, because it only recognizes the identity of the face. Face anti-spoofing detection technology is primarily used to differentiate between real and spoof faces in order to prevent spoof attacks. Face anti-spoofing is an important security defense mechanism in face recognition systems, so designing a face anti-spoofing approach with high detection accuracy and strong generalization ability to assist the face recognition and authentication system against malicious attacks is critical.

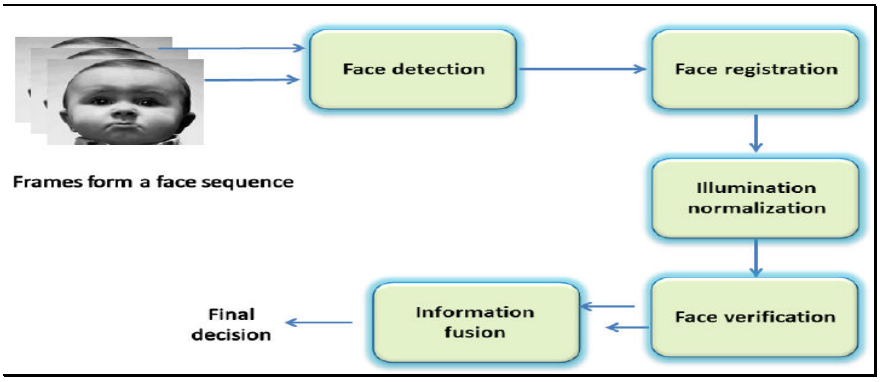

Fig.3: Face Recognition System

C. Deep Convolutional Neural Network:

CNN is one of the most important image recognition and classification categories. CNNs are widely used in a variety of applications, including object detection, face recognition, emotion recognition, and so on. CNN image classification processes and categorizes an input image. CNN is an abbreviation for a neural network with one or more convolutional layers.

CNN Algorithm Pseudo Code:

- **Step 1:** Dataset containing object images along with reference frames is fed into the System.
- **Step 2:** Now import the required libraries and build the model.
- **Step 3:** The convolutional neural network is used which extracts image features f pixel by pixel.
- **Step 4:** Matrix factorization is performed on the extracted pixels. The matrix is of m*n.
- **Step 5:** Max pooling is performed on this matrix where maximum value is selected and again fifixed into matrix.
- **Step 6:** Normalization is performed where the every negative value is converted to zero.
- **Step 7:** To convert values to zero rectifified linear units are used where each value is ffiltered and negative value is set to zero.
- **Step 8:** The hidden layers take the input values from the visible layers and assign the weights after calculating maximum probability.

IV. CONTRIBUTIONS OF PROPOSED WORK

The main contribution of the proposed framework is as follows:

1) In this research work spoofing prevention approach is to examine face liveness, such as eye blinking and lips movement. Although, this approach is helpless when dealing with video-based replay attacks. Hence proposes a combined method of face liveness detection and CNN classifier.

2) Here to provide detail performance analyses of the proposed system on face anti-spoofing problem in both intra-database and cross-database scenarios. Likewise, the placement of adaptive convolutional-feature fusion layer in a CNN network and its effects in general on face liveness detection performance.
3) To improve the performance and accuracy of proposed algorithms.
4) To utilize a deep CNN network with an adaptive convolutional-feature fusion layer that performs the weighted fusion between convolutional features learned by the convolutional layers from real-world face images and deep CNN based auto-encoder generated (DNG) face images.

V. CONCLUSION

In this research work Face identification and recognition is the process of comparing data from a camera to a database of known faces and finding the match. This general face recognition method has flaws. What if someone impersonates someone else or is a criminal? A liveness check overcomes this by distinguishing between a real face and a photograph. The detection of liveness via eye-blink and lip movement improves the reliability of the face recognition application. The proposed approach is a multi-platform application to improve the security of a banking, corporate, or government

system. This is a low-cost, automatic solution that does not require user participation. Application testing is carried out under adverse conditions on authentic data to demonstrate the sturdiness and efficacy of the proposed work. The performance evaluation of the improved functionality on the ORL, OULU and CASIA datasets using CNN as a classifier produced satisfactory results.

REFERENCES

[1] C. Yuan, Z. Xia, X. Sun and Q. M. J. Wu, "Deep Residual Network With Adaptive Learning Framework for Fingerprint Liveness Detection," in IEEE Transactions on Cognitive and Developmental Systems, Vol. 12, Issue 3, pp. 461-473, September 2020.

[2] A. Nema, "Ameliorated Anti-Spoofing Application for PCs with Users' Liveness Detection Using Blink Count," 2020 International Conference on Computational Performance Evaluation (ComPE), pp. 311-315, July 2020.

[3] M. Killioğlu, M. Taşkiran and N. Kahraman, "Anti-Spoofing in Face Recognition with Liveness Detection using Pupil Tracking," 2017 IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI), pp. 000087-000092, January 2017.

[4] Y. Li, L. Po, X. Xu, L. Feng and F. Yuan, "Face liveness detection and recognition using shearlet based feature descriptors," 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), (Shanghai, China, March 2016), pp. 874-877.

[5] J. Peng and P. P. K. Chan, "Face liveness detection for combating the spoofing attack in face recognition," 2014 International Conference on Wavelet Analysis and Pattern Recognition, (Lanzhou, China, July 2014), pp. 176-181.

[6] CAI Pei, QUAN Hui-min, "Face anti-spoofing algorithm combined with CNN and brightness equalization," Journal of Central South University, Vol. 28, pp. 194-204 June 2021.

[7] A. A. Mohamed, M. M. Nagah, M. G. Abdelmonem, M. Y. Ahmed, M. El-Sahhar and F. H. Ismail, "Face Liveness Detection Using a sequential CNN technique," 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), (NV, USA, January 2021), pp. 1483-1488

[8] R. B. Hadiprakoso, H. Setiawan and Girinoto, "Face Anti-Spoofing Using CNN Classifier & Face liveness Detection," 2020 3rd International Conference on Information and Communications Technology (ICOIACT), (Yogyakarta, Indonesia November 2020), pp. 143-147

[9] L. Ashok kumar, J. Rabiyathul Basiriya, M. S. Rahavarthinie, R. Sindhuja, "Face Anti-spoofing using Neural Networks," International Journal of Applied Engineering Research ISSN 0973-4562 Vol. 14, Number 6, 2019.

[10] A. K. Singh, P. Joshi and G. C. Nandi, "Face recognition with liveness detection using eye and mouth movement," 2014 International Conference on Signal Propagation and Computer Technology (ICSPCT 2014), (Ajmer, India, July 2014), pp. 592-597

[11] Monika D.Rokade ,Dr.Yogesh kumar Sharma,"Deep and machine learning approaches for anomaly-based intrusion detection of imbalanced network traffic."IOSR Journal of Engineering (IOSR JEN),ISSN (e): 2250-3021, ISSN (p): 2278-8719

[12] Monika D.Rokade ,Dr.Yogesh kumar Sharma"MLIDS: A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset", 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), IEEE

[13] Monika D.Rokade, Dr. Yogesh Kumar Sharma. (2020). Identification of Malicious Activity for Network Packet using Deep Learning. *International Journal of Advanced Science and Technology*, *29*(9s), 2324 - 2331.

[14] Sunil S.Khatal ,Dr.Yogesh kumar Sharma, "Health Care Patient Monitoring using IoT and Machine Learning.", IOSR Journal of Engineering (IOSR JEN), ISSN (e): 2250-3021, ISSN (p): 2278-8719

[15] Monika D. Rokade;Sunil S. Khatal"Detection of Malicious Activities and Connections for Network Security using Deep Learning",2022 IEEE Pune Section International Conference (PuneCon),Year: 2022 | Conference Paper | Publisher: IEEE

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

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