Journal of Innovative Engineering and Research (JIER)
Vol.- 6, Issue -2, October 2023, pp. 19-25 (6 pages)

Face Anti-Spoofing and Criminal Detection of Real and Valid Face Images With Face Liveness Detection Using Novel Convolutional Neural Network

PRATIBHA SHINDE[1] and DR. AJAY R. RAUNDALE[2]

[1,2] *Department of Computer Science and Engineering, Dr. A. P. J. Abdul Kalam University, Indore 452010, India*
Corresponding Author Email: pratibha.gayke@gmail.com

***Abstract*— Conventionally, classifiers designed for face liveness detection are trained on real-world images, where real-face images and corresponding face presentation attacks (PA) are very much overlapped. However, a little research has been carried out in utilization of the combination of real-world face images and face images generated by deep novel convolutional neural networks (NCNN) for face liveness detection. The biometrics with facial recognition is now widely used. A face identification system should identify not only someone's faces but also detect spoofing attempts with printed face or digital presentations. A sincere spoofing prevention approach is to examine face liveness, such as eye blinking and lips movement. Nevertheless, this approach is helpless when dealing with video-based replay attacks. For this reason, this system proposes a combined method of face liveness detection and NCNN (Novel Convolutional Neural Network) classifier. The anti-spoofing method is designed with two modules, the blinking eye module that evaluates eye openness and lip movement, and the NCNN classifier module. The dataset for training our NCNN classification can be from a variety of publicly available sources.**

We combined these two modules sequentially and implemented them into a simple facial recognition application using the Python. The test results show that the module created can recognize various kinds of facial spoof attacks, such as using posters, masks, or smart-phones. In this research work, we evaluate the adaptive fusion of convolutional-features learned by convolutional layers from real-world face images and deep NCNN generated face images for face liveness detection. Additionally, we propose an adaptive convolutional-features fusion layer that adaptively balance the fusion of convolutional-features of real-world face images and face images generated by deep NCNN during training. Our extensive experiments on the state-of-the-art face anti-spoofing databases, i.e., CASIA, OULU and Replay-Attack face anti-spoofing databases with both intra-database and cross-database scenarios indicate promising performance of the proposed method on face liveness detection compared to state-of-the-art methods.

Index terms: Image Processing, Face Anti-Spoofing, Face Liveness Detection, Facial Spoof Attacks, Artificial Intelligence (AI), Machine Learning, Novel Convolution Neural Networks (NCNN), and Classifiers, etc.

I. INTRODUCTION

Biometrics is one of the most widely used authentication technologies nowadays. Face recognition technology is one of them, and it is frequently utilized due to its ease and accuracy. Face recognition technology is now being used in a variety of facial spoof attacks, such as on smartphones, tablets, and laptops. We can recognize other people using face recognition technology. This facial recognition application works by taking images of a person's face using a camera, then processing the image with a specific algorithm to determine whether the face is recognized from a database or not [1]. Nonetheless, there is a weakness in the facial recognition strategy, called spoofing attacks. Facial recognition systems cannot distinguish between real faces and spoofing attacks such as masks, videos, or photos. As a result, these flaws open the door for someone to deceive the machine. Furthermore, someone's face is much easier to obtain than other biometrics such as fingerprints. Someone's face can be easily obtained by using social media or a profile photo. [2].

Face spoofing attacks are classified as static or dynamic [3]. Static 2D demonstration spoofing attacks use photos or masks, whereas dynamic attacks use video replays or a large number of photos in a sequence. Static 3D demonstration attacks can make use of 3D sculptures, prints, or even masks, whereas animated versions make use of complex robots to mimic expressions, complete with cosmetics.

Here another technique for real person identification is that liveness detection, in that Eye-blink detection is a highly accurate liveness detection evaluation. Natural blinking is a simple way to tell if a face is alive or dead. A blink closes the eyes for approximately 250-300 milliseconds. [4] The average person blinks 5-10 times per minute. We can use eye blink detection to analyze face landmarks and calculate the

surface area of the eyes. However, because current technology makes it simple to attack video replays with devices such as smartphones or tablets, relying on blinking eye detection is no longer sufficient.

Challenges and responses are yet another effective anti-spoofing technique. This method makes use of a one-of-a-kind action known as a challenge. The machine's purpose is to confirm a challenge that occurred during a video sequence. A challenge-response system relies on a series of questions to confirm someone's identity [5]. Nonetheless, while successful, this procedure necessitates additional input and may have a significant impact on the user experience.

The movement detection method seeks to recognize vital signs by analyzing individual facial motions. This motion distinguishes people from inanimate objects such as photographs. A change in facial expressions, blinking eyes, and lip motions are among the most commonly used motion detection techniques [6]. Motion-based evaluation methods are usually adequate for preventing inactive representation strikes such as photo-spoofing, but they become ineffective when dealing with dynamic rendering attacks such as videos [7].

The most dependable method of anti-spoofing would be 3D cameras or photoplethysmography [8]. Because we can tell the difference between a face and a flat object, specific pixel depth advice may offer high precision against demonstration attacks. Cameras, on the other hand, remain one of the most dependable anti-spoofing techniques available. Furthermore, despite having access to cameras, few customers have them on their computers, and it is not suitable for use on mobile devices such as smartphones.

Different texture patterns can be found in both real and fake facial images. The simple truth is that reconstructing faces from camera photographs degrades the quality of facial expressions and creates gaps in reflectivity [9]. Several previous studies attempted to capture the difference using engineered colour texture characteristics, such as RGB (Red Green Blue) or LBP (Local Binary Pattern) variations [10]. Classification algorithms such as support vector machines or nearest neighbors have also been used in similar studies [11]. The weakness of this texture analysis system, on the other hand, is its reliance on room light conditions. In specific room conditions, such as dimly lit rooms, the initial facial texture using imitations will be hard to differentiate.

This system is designed to help any investigation department identify criminals. In this system, images of criminals are stored in our database along with their details, and these images are then segmented into four slices-foreheads, eyes, nose, and lips. These images are then saved in another database record to aid in the identification process. Eyewitnesses will choose the slices that appear on the screen, and we will use them to retrieve the image of the face from the database. Thus, if the criminal's record exists in the database, this system provides a very friendly environment for both the operator and the eyewitness to easily identify the criminal.

Deep learning and convolutional neural networks (CNN) are two additional anti-spoofing solutions. System could train CNN to recognize which photos are genuine and which are spoofed. There is, however, one issue. There is no consistent set of features that the convolutional network sees and understands [13]. The entire model was based on the hope that the system would detect what we couldn't see with our eyes. As a result, to believe it is critical to use a combination of detection methods for signs of life, such as blinking or lip movements, in conjunction with CNN analysis methods. For limit the scope of our face liveness detection by using blinks detection and lip movement detection because these two signs are the most common and easy to detect.

As a result, this research work investigates an advanced face liveness detection method and CNN for distinguishing between fake and real faces. It is simple, and most importantly, it is more resistant to environmental changes and various attack methods. The work's significant contributions are listed below.

(1) The proposed procedure is completely accurate because it employs CNN and deep transfer learning to learn signs that reflect the characteristics of both real and fake faces. (2) Proposed method is simple to implement and does not require any additional hardware. (3) Proposed face anti-spoofing scheme is robust and detects spoofing in real time. It can deal with various spoofing attacks (print, replay, and mask) in complex real-world indoor and outdoor scenarios.

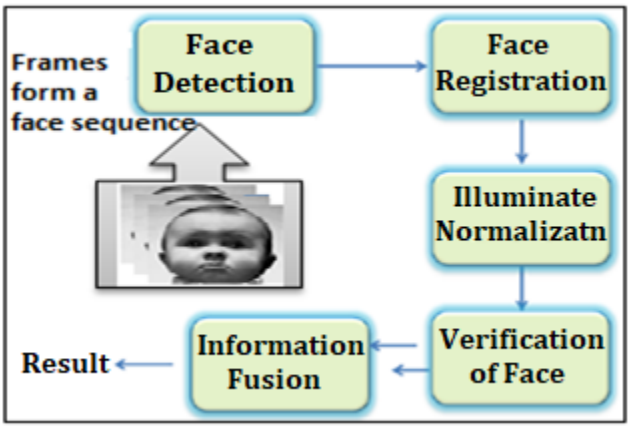


Fig.1: System Overview

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 the use of a combination of real-world face images and face images generated by deep novel convolutional neural networks (NCNN) for face liveness detection. Facial recognition biometrics is now widely used. A face identification system should be able to recognize not only people's faces, but also spoofing attempts using printed faces or digital presentations. Examining face liveness is a genuine spoofing prevention strategy, such as eye blinking and lips movement. 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 NCNN (Novel 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 NCNN classifier module. The dataset used to train our NCNN classification algorithm can come from a variety of publicly available sources. For 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 using posters, masks, or smart-phones.

To evaluate the adaptive fusion of convolutional-features learned by convolutional layers from real-world face images and deep NCNN generated face images for face liveness detection in this research work. Furthermore, now propose an adaptive convolutional-features fusion layer that balances the fusion of convolutional-features from real-world face images and deep NCNN generated face images during training. Extensive experiments on state-of-the-art face anti-spoofing databases, such as CASIA, OULU, and Replay-Attack, with intra-database and cross-database scenarios, show that the proposed method performs well on face liveness detection compared to state-of-the-art methods.

II. RELATED WORK

- Arpita Nema, [2] this paper proposes a "desktop anti-spoofing application." To detect liveness, this application employs a face recognition approach as well as an eye-blink count. The application's main phases are face detection and recognition, as well as determining the user's liveness status. Liveness detection has been shown to prevent video playback attacks and the use of printed photographs to compromise security. The user's image is captured by the webcam at regular intervals. After passing the authentication process, the image is checked for liveness. Countermeasures are implemented in the event of a security breach. This includes capturing an adversary's image and logging off or exiting the system.

- A. A. Mohamed, M. M. Nagah, M. G. Abdelmonem, M. Y. Ahmed, Mahmou, [7] Face recognition is one of the most widely used biometric approaches. Face recognition is used in a variety of fields. Mobile device authentication is one of these fields. While the number of mobile device users grows year after year, so does the need for mobile security. Face recognition, on the other hand, is vulnerable to malicious face spoofing. This is done to fool the face recognition system with facial images obtained from images or videos. Other cheaters wear an authorized person's mask to fool the recognition camera into thinking they are a real person. To detect face spoofing, liveness detection is an important research topic.

- Raden B. Hadiprakoso, Hermawan Setiawan, Girinoto, [8] Facial recognition biometrics are now widely used. A face identification system should be able to recognize not only people's faces, but also 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 paper proposes a method that combines face liveness detection with a CNN (Convolutional Neural Network) classifier. The anti-spoofing method is composed of two modules: the blinking eye module, which assesses eye openness and lip movement, and the CCN classifier module. The dataset used to train our CNN classification algorithm can come from a variety of publicly available sources.

- AK. Singh, Pi. Joshi, G. C. Nandi, [10] The issue of face spoofing, which can bypass the authentication system by placing a photo/video/mask of the enrolled person in front of the camera, is discussed in recent literature on face recognition technology. This issue could be mitigated by detecting the person's liveness. As a result, we propose a robust liveness detection scheme based on a challenge and response method in this paper. Before the face recognition module, the liveness module is added as an extra layer of security. The Liveness module makes use of face macro features, particularly eye and mouth movements, to generate random challenges and observe the user's response on account of this. The dependability of the liveness module is tested by deploying various types of spoofing attacks via various means, such as photographs, videos, and so on.

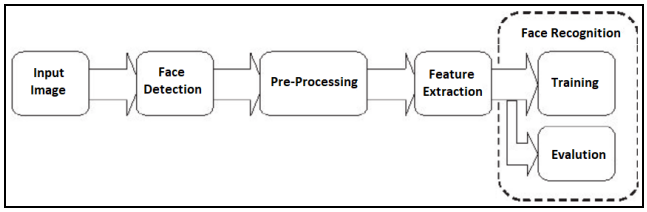
J. Yaojie Liu, Amin Jourabloo, Xiaoming Liu, [11] Face anti-spoofing is critical for preventing a security breach in face recognition systems. Face anti-spoofing has previously been treated as a binary classification problem in deep learning approaches. Many of them struggle to understand appropriate spoofing cues and generalize incorrectly. In this paper, authors argue that auxiliary supervision is essential for guiding learning toward discriminative and generalizable cues. A CNN-RNN model is trained to estimate face depth with pixel-by-pixel supervision and rPPG signals with sequence-by-sequence supervision. The estimated depth and rPPG are combined to distinguish between live and spoof faces.

III. PROPOSED SYSTEM

In this research work propose building an anti-spoofing model with three major modules: face anti-spoofing detection, a liveness detector and a criminal identification using NCNN classifier.

In proposed work the input will be processed by the face anti-spoofing module, which will detect photos, posters, masks, or Smartphone's. If a face is detected, the input is routed to the NCNN classifier module, which determines whether the face is fake or real. Next input will be processed for the liveness detection module, which will detect eye blinks and lip movements. If the input passes through both modules, it is declared a real face. Finally, focus on third approach which is criminal identification module, which will detect face recognition input at the time of face anti-spoofing detection. In face anti-spoofing detection module if real face is found then this face gives input for criminal identification module and to found the face is normal valid person or criminal.

There are two sub-modules inside the life sign (liveness) detection module on the face: blink detection and lip motion detection represent in fig.1. This module detects lip motion using the lip-movement-net module [14]. As part of the module, 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. You can run the detector module on a video file or camera output in real-time. This module detects lip movement by creating a filter to determine the locations of the upper and lower lips and then calculating the lips separation distance.



IV. SYSTEM MODULES

A. *Face Anti-Spoofing:*

Facial anti-spoofing is the task of preventing false facial verification by using a photo, video, mask or a different substitute for an authorized person's face.
Some examples of attacks: Print attack: The attacker uses someone's photo. The image is printed or displayed on a digital device.

B. *Liveness Detection:*

In biometrics, Liveness Detection is a computer's ability to determine that it is interfacing with a physically present human being and not an inanimate spoof artifact or injected video/data. Remember: It's not "Liveliness". Don't make that rookie mistake!
"With the increasing use of facial recognition, the risk for spoofing-attacks rises".

C. *Face Recognition Systems:*

Face Recognition System is an application that mechanically identifies a person from a digital image or a video outline from a video source. One of the behaviors to do this method is by matching chosen facial features from a facial database and the image. In this system, with appropriate lightning and robust learning. Further a positive visual match would cause the live image to be stored in the database so that future transactions would have broader base from which to compare if the original account image fails to provide a match –thereby decreasing false negatives.

In an increasingly digital world, protecting confidential information from hackers and unauthorized individuals is becoming more difficult and the need for robust security is paramount.

As a result, Biometric spoofing is a growing concern as biometric traits are vulnerable to attacks. Biometric spoofing is the ability to fool a biometric system into recognizing a fake user as a genuine user by means of presenting a synthetic forged version of the original biometric trait to the system. Specific countermeasures that allow biometric system to detect fake artifacts and to reject them need to be developed.

D. *Criminal Identification System:*

This system is designed to help any investigation department identify criminals.
In this system, focus on third approach which is criminal identification module, which will detect face recognition input at the time of face anti-spoofing detection. In face anti-spoofing detection module if real face is found then this face gives input for criminal identification module and to found the face is normal valid person or criminal.

V. ALGORITHM DETAILS

E. *NCNN Algorithm:*

NCNN is one of the most common image recognition and classification algorithms. NCNNs are frequently employed in domains like emotion recognition, facial recognition, object detection, and so on. Then image classification algorithm i.e. NCNN can takes an input image, to pre-process that image, and categorizes it into different groups of emotions (joyful, terror, sad, surprise, angry, disgust, and neutral). A NCNN is a neural network algorithm with more than one convolutional and pooling layer [14].

- **Step 1:** The machine is fed a data set containing images and reference emotions. Face Emotion Recognition (FER) is the name of the dataset, and that is publicly-available data collection that was formed publically freely accessible on Kaggle Dataset.
- **Step 2:** Here you may build the model by importing the necessary libraries.
- **Step 3:** The image features are extracted pixel by pixel using a convolution neural network.
- **Step 4:** The retrieved pixels are subjected to matrix factorization. The matrix is m x n in size.
- **Step 5:** This matrix is subjected to maximum pooling, which involves selecting the highest value and re-inserting it into the matrix.
- **Step 6:** Every negative value is turned to zero as part of the normalization process.
- **Step 7:** Rectified linear units are used to convert values to zero, with each value filtered and the negative value converted to zero.

Step 8: After computing maximum probability, the hidden layers apply weights to the input values from the visible layers.

VI. RESULTS AND DISCUSSION

In this section results are formed as a implementation of ML and IP based application and results is generated on any web browsers for social community users to prevent various health and mental stress issues of patients as well as user's in his daily life and social interaction time. The analysis results of the proposed system are carried out according to the following parameters:

- Time consumption = A
- Response Time = B
- Computation Cost = C
- Performance accuracy = D
- Scalable & User Friendly = E

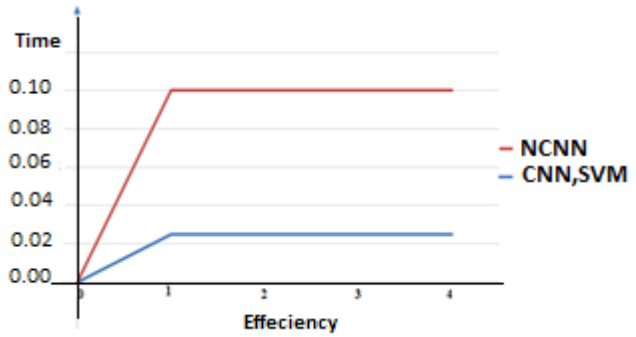


Fig.3: Time and Efficiency Chart

In this context, the whole system has taken many more input attributes, but the main focus is on system performance and time. We will obtain the following analytical results for our proposed system based on some attributes and above mentioned parameters is as follows:

Parameter	Existing	Proposed
A	10	4
B	10	5
C	8	8
D	10	3
E	8	2

Table 1: Result Table

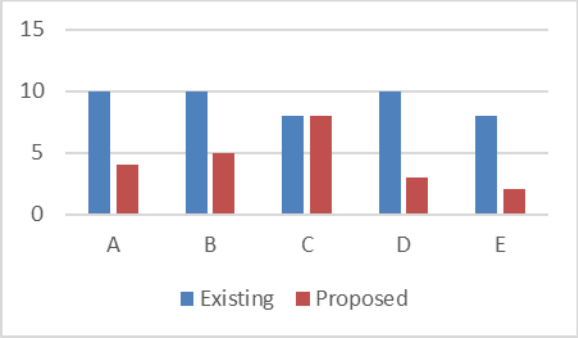


Fig.4: Time line chart of Result Analysis

VII. CONCLUSION

This paper focuses on with so many devices using facial recognition biometric authentication, the need for face anti-spoof is an absolute must. This paper proposes using the NCNN analysis model for image input combined with the face liveness detection module and criminal identification. Based on the results of module testing shows excellent results to prevent various types of face spoof attacks. We test various spoof face attacks tested included static attacks such as masks, photo posters or digital photos, and dynamic attacks such as video replays. Further research can explore parallel programming techniques that can speed up the time for facial recognition programs [15]. We ran our tests on datasets that were freely available online. Our tests revealed that our NCNN-based models outperformed NCNN-based models. Models with improved embeddings were able to keep their generalization capabilities while maintaining performance.

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] Y. Liu, A. Jourabloo and X. Liu, "Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision," 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, (Salt Lake City, UT, USA, June 2018), pp. 389-398

[12] Youngjun Moon, Intae Ryoo, and Seokhoon Kim, "Face Anti-spoofing Method Using Color Texture Segmentation on FPGA," Hindawi Security and Communication Networks, Vol. 2021, pp. 1-11, May 2021.

[13] Yasar Abbas Ur Rehman, Lai-Man Po, Mengyang Liu, Zijie Zou, Weifeng Ou, Yuzhi Zhao, "Face liveness detection using convolutional-features fusion of real and deep network generated face images". February 2019, Journal of Visual Communication and Image Representation, Vol. 59, Page. 574-582, February 2019.

[14] A. Kumar T.K., R. Vinayakumar, S. Variyar V.V., V. Sowmya and K. P. Soman, "Convolutional Neural Networks for Fingerprint Liveness Detection System," 2019 International Conference on Intelligent Computing and Control Systems (ICCS), (Madurai, India, Ma 2019), pp. 243-246

[15] Meigui Zhang, Kehui Zeng and Jinwei Wang, "A Survey on Face Anti-Spoofing Algorithms". Journal of Information Hiding and Privacy Protection, Vol.2, No.1, pp.21-34, June 2020.