

# Face and liveness detection with criminal identification using machine learning and image processing techniques for security system

Pratibha Shinde<sup>1,2</sup>, Ajay R. Raundale<sup>3</sup>

<sup>1</sup>Department of Information Technology, Dr. Vithalrao Vikhe Patil College of Engineering, Ahmednagar, India

<sup>2</sup>Department of Computer Science and Engineering, Faculty of Department of Information Technology, Dr. Vithalrao Vikhe Patil College of Engineering, Ahmednagar, India

<sup>3</sup>Department of Computer Science and Engineering in Dr. A. P. J. Abdul Kalam University, Indore, India

## Article Info

### Article history:

Received Mar 23, 2023

Revised Aug 17, 2023

Accepted Oct 5, 2023

### Keywords:

Convolutional neural networks

Criminal identification

Face anti-spoofing

Face liveness detection

Machine learning

## ABSTRACT

In the past, real-world photos have been used to train classifiers for face liveness identification since the related face presentation attacks (PA) and real-world images have a high degree of overlap. The use of deep convolutional neural networks (CNN) and real-world face photos together to identify the liveness of a face, however, has received very little study. A face recognition system should be able to identify real faces as well as efforts at faking utilizing printed or digital presentations. A true spoofing avoidance method involves observing facial liveness, such as eye blinking and lip movement. However, this strategy is rendered useless when defending against replay assaults that use video. The anti-spoofing technique consists of two modules: the ConvNet classifier module and the blinking eye module, which measure lip and eye movement. The results of the testing demonstrate that the developed module is capable of identifying various face spoof assaults, including those made with the use of posters, masks, or smartphones. To assess the convolutional features in this study adaptively fused from deep CNN produced face pictures and convolutional layers learned from real-world identification. Extensive tests using intra-database and cross-database scenarios on cutting-edge face anti-spoofing databases including CASIA, OULU, NUAA and replay-attack dataset demonstrate that the proposed solution methods for face liveness detection. The algorithm has a 94.30% accuracy rate.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



## Corresponding Author:

Pratibha Shinde

Department of Information Technology

Dr. Vithalrao Vikhe Patil College of Engineering

Ahmednagar, Maharashtra, India

Email: ps21.shinde@gmail.com

## 1. 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].

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

Another technique for identifying real people is liveness detection, and Eye-blink detection is a highly accurate liveness detection evaluation. Natural blinking is an easy way to determine whether a face is alive or dead. A blink closes one's eyes for about 250-300 milliseconds. In [4] a typical person blinks 5-10 times per minute. Eye blink detection can be used to analyze face landmarks and calculate the surface area of the eyes. However, because modern technology makes it easy to attack video replays with devices like smartphones or tablets, relying on blinking eye detection is no longer sufficient [5].

By analyzing individual facial motions, the movement detection method attempts to recognize vital signs. Humans may be distinguished from inanimate items like images by this movement. Changes in face expression, blinking eyes, and lip motions are a few of the most often used motion detection methods [6]. Motion-based evaluation methods are typically adequate for preventing inactive representation strikes such as photo-spoofing, but they fail to prevent dynamic rendering attacks such as videos [7].

3D cameras or photoplethysmography [8] are the most reliable anti-spoofing methods. Because we can distinguish between a face and a flat object, pixel depth advice may provide high precision against demonstration attacks [9], [10]. Cameras, on the other hand, continue to be one of the most reliable anti-spoofing methods available. Furthermore, even though customers have access to cameras, few have them on their computers, and it is not suitable for use on mobile devices such as smartphones [11].

This system is intended to assist any investigation department in identifying criminals. Images of criminals are stored in our database alongside their details in this system, and these images are then segmented into four slices-foreheads, eyes, nose, and lips. These images are then saved in a different database record to help with identification. The slices that appear on the screen will be chosen by eyewitnesses, and we will use them to retrieve the image of the face from the database. As a result, if the criminal's record is found in the database, this system provides a very friendly environment in which both the operator and the eyewitness can easily identify the criminal [12].

Deep learning and convolutional neural networks (CNN) are two other anti-spoofing technologies. The system could train CNN to distinguish between genuine and spoofed images. However, there is one problem. The convolutional network sees and understands no consistent set of features [13]. The entire model was built on the hope that the system would detect what our eyes couldn't see. As a result, I believe it is critical to combine detection methods for signs of life, such as blinking or lip movements, with CNN analysis methods. To limit the scope of our face liveness detection, we will use blink detection and lip movement detection because these two signs are the most common and simple to detect.

As a result, this study looks into an advanced face liveness detection method and CNN for telling the difference between fake and real faces. It is straightforward, and, more importantly, it is more resistant to environmental changes and various attack methods. The significant contributions of the work are listed: i) the proposed procedure is completely accurate because it uses CNN and deep transfer learning to learn signs that reflect both real and fake face characteristics; ii) the proposed method is simple to implement and does not necessitate the purchase of any additional hardware; and iii) the proposed anti-spoofing scheme is strong and detects spoofing in real time. In complex real-world indoor and outdoor scenarios, it can deal with various spoofing attacks (print, replay, and mask).

In this research, we will assess how well deep CNN produced face pictures and convolutional layers' adaptive learning of convolutional features from real-world face photos can identify the liveness of a face. In addition, a layer for balancing the merging of convolutional features from both deep CNN produced face pictures and convolutional features from real-world face images is presented. The suggested technique outperforms state-of-the-art algorithms on face liveness detection, according to extensive trials on cutting-edge face anti-spoofing databases including CASIA, OULU, and Replay-Attack, with both intra-database and cross-database situations [14]-[17].

## 2. LITERATURE REVIEW

Yuan *et al.* [1] 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. However, extensive research indicates that obtaining high performance detection requires a certain minimum number of MLP. For the first time, we used FLD to resolve the conflict known as the deep residual network in this paper (DRN). Then, to eliminate interference from incorrect portions of given photos, an extraction algorithm (ROI) is proposed. 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.

The study in [2] a “desktop anti-spoofing application” is proposed in this paper. To determine whether a face is living, this programme counts the number of eyes blinking. Face detection and identification are the application’s primary stages, 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. The webcam captures the user’s image at regular intervals. The image is checked for liveness after it has passed the authentication process. In the event of a security breach, countermeasures are put in place. This includes photographing an adversary and logging off or exiting the system.

Killioglu *et al.* [3] concentrated on liveness detection for spoofing facial recognition systems with artificial face motion. A modest piece of hardware was used by the authors to create a pupil direction observation system for face recognition systems. The first step is to extract the eye area from a real-time camera using a specifically trained eye region recognition classifier and the haar-cascade classifier. Feature points were extracted and traced using the Kanade-Lucas-Tomasi (KLT) algorithm to minimize a person head movements and obtain a stable eye region. The real-time camera frame is chopped and rotated to stabilize the eye region. Then, using a new, enhanced method, the pupils are retrieved from the eye region.

Li *et al.* [4] face recognition is a popular biometric technology due to its ease of use; however, It is susceptible to spoofing attacks from fake faces, such as those in a real user’s picture or video. An essential technique for confirming that the input face belongs to a real person is face liveness detection. Traditional liveness detection methods, such as texture analysis and motion detection, remain extremely difficult. The objective of this study is to provide a framework that is effective at dealing with face liveness detection and identification as well as a multifunctional feature descriptor. This framework employs a multiscale directional transform to define new feature descriptors (shearlet transform). Then, to detect the liveness of a face and identify the person, stacked auto-encoders and a softmax classifier are combined. The authors tested this approach using the CASIA face anti-spoofing database, and the results show that when tested using the database’s evaluation protocols, our approach outperforms state-of-the-art techniques, indicating that it is possible to significantly improve the security of face recognition biometric systems.

Peng and Chan [5] a typical adversarial approach in facial recognition is spoofing, in which the attacker presents the user’s photos or videos in front of the camera while pretending to be them. In order to maintain the security of the system, face liveness detection is employed to separate photographs taken from a live face from those taken from a faked face. In this study, the authors provide a face liveness detection approach based on the high frequency descriptor to counter spoofing assaults. By revealing more hair and skin features and creating a shine on the flat surface, more lighting may both boost and drop the energy of high frequency components of a genuine face.

Cai and Quan, [6] facial anti-spoofing is a small part of face recognition systems, which are necessary for access control and financial payment systems. By merging convolutional neural network with brightness equalisation, an unique approach is proposed that overcomes the issues of unstable face alignment, complicated lighting, and complex face anti-spoofing detection network structure. A multi-task convolutional neural network (MTCNN) built on a cascade of three CNNs, P-net, R-net, and O-net, is employed first to obtain precise face positioning, and the identified face bounding box is cropped by a predetermined multiple.

Mohamed *et al.* [7] face recognition is one of the most frequently utilised biometric techniques. Numerous applications make use of face recognition. The authentication of mobile devices is one of these areas. Mobile security is becoming necessary as more people use mobile devices every year. Face recognition, on the other hand, is susceptible to deceptive face spoofing. Using facial images that have been derived from pictures or movies, this trick is used to fool face recognition software. Other cheats dress in official uniforms to make it appear as though they are authorised personnel to the recognition camera. For scope of identifying face spoofing, liveness detection is a crucial study area.

Hadiprakoso *et al.* [8] biometrics based on facial recognition are now widely used. A face identification system should be able to recognise not only people’s faces, but also attempts at spoofing using printed faces or digital presentations. Examining liveness of the face, such as eye blinking and lip movement, is an effective spoofing prevention strategy. Nonetheless, when dealing with video-based replay attacks, this approach is rendered ineffective. As a result, this paper proposes a method for detecting the liveness of a face using a CNN classifier. The blinking eye module, which assesses eye opening and lip movement, and the ConvNet classifier module make up the anti-spoofing approach. Data from a number of freely accessible sources may be used to train our CNN classification system.

Kumar *et al.* [9] biometrics is now one of the most widely used security applications. Face recognition is the most widely used method due to its uniqueness. To grant access to confidential resources, authors must ensure that only genuine live face images are used. Hackers, on the other hand, undermine this system by impersonating genuine users through photo attacks, video replay attacks, and 3-D attacks. To deter these impostors, many deterrent mechanisms have been devised. As a result, a neural network-based detection method for spoofed faces is proposed. The architecture of the convolutional network is intended to prevent spoofed faces from gaining access in the name of legitimate users.

Singh *et al.* [10] face anti-spoofing is critical for keeping face recognition systems secure. Deep learning approaches have previously treated face anti-spoofing as a binary classification problem. Many of them struggle to understand appropriate spoofing cues and make incorrect generalizations. The authors argue in this paper that auxiliary supervision is critical for guiding learning toward discriminative and generalizable cues. A CNN-RNN model is trained with pixel-by-pixel supervision to estimate face depth and rPPG signals with sequence-by-sequence supervision. To distinguish between live and spoof faces, the estimated depth and rPPG are combined.

### 3. 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.

Finally, concentrate on the third approach, which is a criminal identification module that will detect face recognition input during face anti-spoofing detection. If a real face is found in the face anti-spoofing detection module, this face provides input to the criminal identification module, which determines whether the face is normal or criminal [18]–[20]. The methodology we propose is made up of several general steps. The steps to develop the CNN classifier modules are: data collection, data pre-processing, model training, model evaluation, and testing.

The life sign (liveness) detection module on the face has two sub-modules: blink detection and lips motion detection. The lip-movement-net module [21] 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 [22]. Figure 1 shows proposed system architecture details flow.

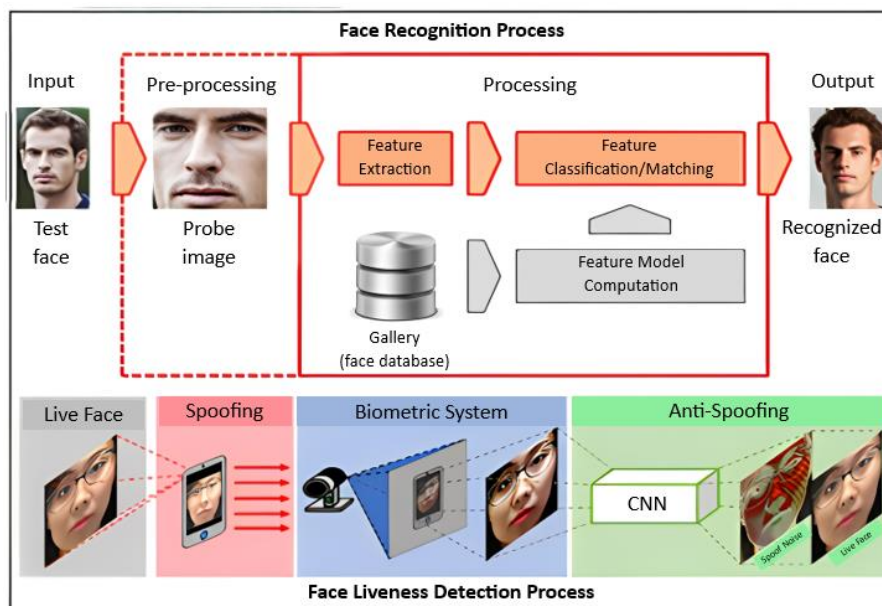


Figure 1. Proposed system architecture diagram

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 [23].

### 3.1. 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. Applications for it include facial recognition in attendance systems, purchases, and mobile device authentication [1]. In forensics and security access, it is also utilised [2]. Face faking is one of the problems that developers have while putting in place a face recognition system. Attackers who attempt to trick facial recognition software are said to engage in face spoofing. The most well-known face spoofing techniques are printed photos, films, and 3D masks, as illustrated in Figure 2. These techniques let an attacker contact a target without their permission and get around a face recognition system.

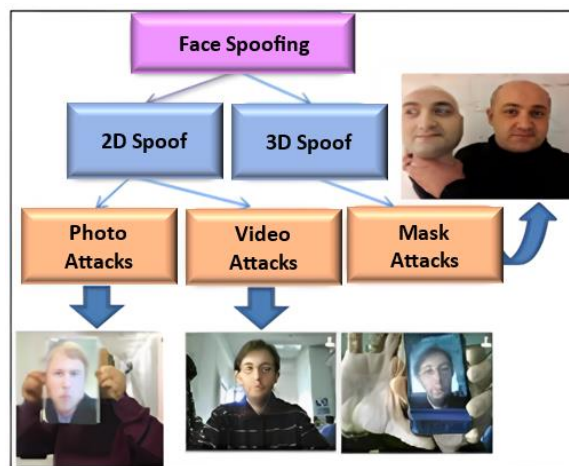


Figure 2. Face spoofing types

One of several techniques used to prevent face spoofing attacks is face liveness detection. Sensing face liveness is a relatively new technology, as fingerprints and passwords are the most commonly used security methods. However, many businesses require face spoofing detection to prevent unauthorised access to their systems. The use of a projected picture (or video) or 3D mask of a real person in front of a security camera allows cheaters to get unauthorised access. Access to the faces of live individuals is one of the security system's functions. In order to stop face spoofing assaults, it will be essential to detect face liveness.

### 3.2. Face recognition system

Using real users' photographs, videos, and 3D face masks, certain unlawful intruders are now able to execute spoof face assaults against systems. Face recognition can only identify the identity of a face; therefore, it cannot shield users from attacks from non-living faces like spoof faces, which are a serious security risk to the system. Face recognition simply detects the identity of the face; hence it cannot protect against attacks from non-living faces like spoof faces. Face anti-spoofing detection technology is mostly used to distinguish between actual and fake faces in order to stop spoof attacks. It is crucial to create a face anti-spoofing strategy with high detection accuracy and great generalisation capacity to support the face recognition and authentication system against malicious assaults since face anti-spoofing is a crucial security defensive mechanism in face recognition systems [24]. Face recognition system illustrate in Figure 3.

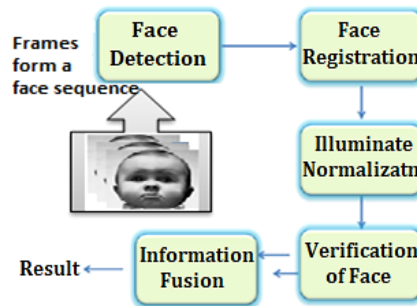


Figure 3. Face recognition system

### 3.3. Criminal identification

There has been an unusual increase in the crime rate, as well as an increase in the number of criminals, raising serious concerns about security. The primary issues confronting police personnel are crime prevention and criminal identification, Police are primarily concerned with protecting property and lives, yet there aren't many officers available to fight crime. An automated facial recognition system for a criminal database was suggested in this paper using a well-known CNN classifier. This technology will enable real-time face detection and identification of criminal which shown in Figure.4. Accurately identifying the face is still challenging. To locate faces and other objects in a picture, researchers frequently employ the Viola-Jones framework. With open communities like OpenCV, face detection classifiers are shared [25]. With a full solution for image-based face identification and recognition with improved accuracy, a higher response rate, and as a first step towards video surveillance, this system aims to assess face detection and recognition methods.

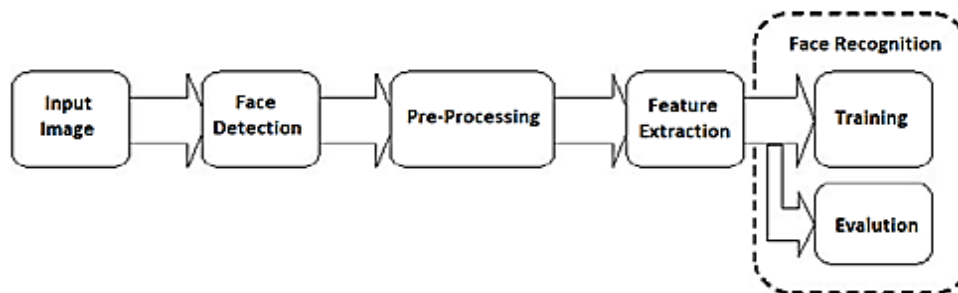


Figure 4. Structure of criminal identification using face recognition system

### 3.4. Deep convolutional neural network

One of the most significant subcategories of image categorization and recognition is CNN. CNNs are frequently employed in a broad range of tasks, including as object identification, face and emotion recognition, among others. 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: The system receives a dataset that includes reference frames and object pictures.
- Step 2: Import the necessary libraries now, then construct the model.
- Step 3: In order to extract picture features, the convolutional neural network is employed, pixel by pixel.
- Step 4: The retrieved pixels are subjected to matrix factorization.  $M*N$  makes up the matrix.
- Step 5: This matrix is subjected to max pooling, where the largest value is chosen and added to the matrix once again.
- Step 6: The process of normalization involves converting every negative number to zero.
- Step 7: Rectified linear units are used to convert values to zero, with each value being filtered and the negative value being set to 0.
- Step 8: The weights are assigned to the input values from the visible layers after determining maximum likelihood in the hidden layers.



#### 4. RESULTS AND DISCUSSION OF PROPOSED WORK

The main contribution of the proposed framework is:

- i) The objective of this study is to evaluate face liveness, including eye blinking and lip movement, as a defence against spoofing. Nevertheless, this tactic is worthless when facing attacks based on replay videos. This provides a method that combines facial liveness detection with CNN classifier.
- ii) We'll provide you a thorough performance study of the recommended system's handling of the anti-spoofing problem in both intra- and cross-database scenarios in this part. Also covered are the placement of an adaptive convolutional-feature fusion layer in a CNN network and how that affects the efficiency of face liveness detection in general.
- iii) It is necessary to build and create a system for criminal identification in the third module of the CNN module employing a facial recognition method to crime prevention.
- iv) To enhance the efficiency and precision of suggested algorithms.
- v) To use a deep CNN network with an adaptive convolutional-feature fusion layer to combine convolutional features learned from real-world face photographs with deep CNN-based auto-encoder produced (DNG) face images in a weighted manner.

#### 5. CONCLUSION

Provide 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 reliability of the face recognition application is increased by the detection of liveness through eye-blink and lip movement. The suggested strategy is a multi-platform programme that will increase the security of a business, governmental, or banking system. This is an inexpensive, automated solution that runs without user input. Application testing is done on real data in challenging environments to show how reliable and effective the suggested work is. Using the ORL, OULU, and CASIA datasets, the performance evaluation of the increased functionality utilising CNN as a classifier provided results that were adequate.




#### REFERENCES

- [1] C. Yuan, Z. Xia, X. Sun, and Q. M. J. Wu, "Deep residual network with adaptive learning framework for fingerprint liveness detection," *IEEE Transactions on Cognitive and Developmental Systems*, vol. 12, no. 3, pp. 461–473, Sep. 2020, doi: 10.1109/TCDS.2019.2920364.
- [2] A. Nema, "Ameliorated anti-spoofing application for PCs with users' liveness detection using blink count," in *2020 International Conference on Computational Performance Evaluation, ComPE 2020*, Jul. 2020, pp. 311–315, doi: 10.1109/ComPE49325.2020.9200166.
- [3] M. Killioğlu, M. Taşkıran, and N. Kahraman, "Anti-spoofing in face recognition with liveness detection using pupil tracking," in *SAMI 2017-IEEE 15th International Symposium on Applied Machine Intelligence and Informatics, Proceedings*, Jan. 2017, pp. 87–92, doi: 10.1109/SAMI.2017.7880281.
- [4] Y. Li, L. M. Po, X. Xu, L. Feng, and F. Yuan, "Face liveness detection and recognition using shearlet based feature descriptors," in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing-Proceedings*, Mar. 2016, pp. 874–877, doi: 10.1109/ICASSP.2016.7471800.
- [5] J. Peng and P. K. Chan, "Face liveness detection for combating the spoofing attack in face recognition," in *International Conference on Wavelet Analysis and Pattern Recognition*, Jul. 2014, pp. 176–181, doi: 10.1109/ICWAPR.2014.6961311.
- [6] P. Cai and H. min Quan, "Face anti-spoofing algorithm combined with CNN and brightness equalization," *Journal of Central South University*, vol. 28, no. 1, pp. 194–204, Jan. 2021, doi: 10.1007/s11771-021-4596-y.
- [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," in *2021 IEEE 11th Annual Computing and Communication Workshop and Conference, CCWC 2021*, Jan. 2021, pp. 1483–1488, doi: 10.1109/CCWC51732.2021.9376030.
- [8] R. B. Hadiprakoso, H. Setiawan, and Girinoto, "Face anti-spoofing using CNN classifier face liveness detection," in *2020 3rd International Conference on Information and Communications Technology, ICOIACT 2020*, Nov. 2020, pp. 143–147, doi: 10.1109/ICOIACT50329.2020.9331977.
- [9] L. A. Kumar, J. R. Basiriya, M. S. Rahavarthinie, and R. Sindhuja, "Face anti-spoofing using neural networks," *International Journal of Applied Engineering Research*, vol. 14, pp. 1183–1186, 2019.
- [10] A. K. Singh, P. Joshi, and G. C. Nandi, "Face recognition with liveness detection using eye and mouth movement," in *2014 International Conference on Signal Propagation and Computer Technology, ICSPCT 2014*, Jul. 2014, pp. 592–597, doi: 10.1109/ICSPCT.2014.6884911.
- [11] Y. Liu, A. Jourabloo, and X. Liu, "Learning deep models for face anti-spoofing: Binary or auxiliary supervision," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, Jun. 2018, pp. 389–398, doi: 10.1109/CVPR.2018.00048.
- [12] Y. Moon, I. Ryoo, and S. Kim, "Face antispoofing method using color texture segmentation on FPGA," *Security and Communication Networks*, pp. 1–11, May 2021, doi: 10.1155/2021/9939232.
- [13] Y. A. U. Rehman, L. M. Po, M. Liu, Z. Zou, W. Ou, and Y. Zhao, "Face liveness detection using convolutional-features fusion of real and deep network generated face images," *Journal of Visual Communication and Image Representation*, vol. 59, pp. 574–582, Feb. 2019, doi: 10.1016/j.jvcir.2019.02.014.




- [14] E. Park, X. Cui, T. H. B. Nguyen, and H. Kim, "Presentation attack detection using a tiny fully convolutional network," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 11, pp. 3016–3025, Nov. 2019, doi: 10.1109/TIFS.2019.2907184.
- [15] M. Zhang, K. Zeng, and J. Wang, "A survey on face anti-spoofing algorithms," *Journal of Information Hiding and Privacy Protection*, vol. 2, no. 1, pp. 21–34, 2020, doi: 10.32604/jihpp.2020.010467.
- [16] L. Li, Z. Xia, L. Li, X. Jiang, X. Feng, and F. Roli, "Face anti-spoofing via hybrid convolutional neural network," in *Conference Proceedings-2017 International Conference on the Frontiers and Advances in Data Science, FADS 2017*, Oct. 2017, pp. 120–124, doi: 10.1109/FADS.2017.8253209.
- [17] M. Alshaikhli, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Face-fake-net: the deep learning method for image face anti-spoofing detection : 45," in *Proceedings-European Workshop on Visual Information Processing, EUVIP*, Jun. 2021, vol. 2021-June, doi: 10.1109/EUVIP50544.2021.9484023.
- [18] P. Zhang *et al.*, "FeatherNets: Convolutional neural networks as light as feather for face anti-spoofing," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, Jun. 2019, pp. 1574–1583, doi: 10.1109/CVPRW.2019.00199.
- [19] S. Fatemifar, M. Awais, S. R. Arashloo, and J. Kittler, "Combining multiple one-class classifiers for anomaly based face spoofing attack detection," Jun. 2019, doi: 10.1109/ICB45273.2019.8987326.
- [20] B. Ahuja and V. P. Vishwakarma, "Local binary pattern based feature extraction with KELM for face identification," in *2020 6th International Conference on Signal Processing and Communication, ICSC 2020*, Mar. 2020, pp. 91–95, doi: 10.1109/ICSC48311.2020.9182760.
- [21] F. Ullah *et al.*, "Cyber security threats detection in internet of things using deep learning approach," *IEEE Access*, vol. 7, pp. 124379–124389, 2019, doi: 10.1109/ACCESS.2019.2937347.
- [22] T. K. A. Kumar, R. Vinayakumar, V. V. S. Variyar, V. Sowmya, and K. P. Soman, "Convolutional neural networks for fingerprint liveness detection system," in *2019 International Conference on Intelligent Computing and Control Systems, ICCS 2019*, May 2019, pp. 243–246, doi: 10.1109/ICCS45141.2019.9065713.
- [23] T. Alipourfard, H. Arefi, and S. Mahmoudi, "A novel deep learning framework by combination of subspace-based feature extraction and convolutional neural networks for hyperspectral images classification," in *International Geoscience and Remote Sensing Symposium (IGARSS)*, Jul. 2018, pp. 4780–4783, doi: 10.1109/IGARSS.2018.8518956.
- [24] W. Jian, Y. Zhou, and H. Liu, "Densely connected convolutional network optimized by genetic algorithm for fingerprint liveness detection," *IEEE Access*, vol. 9, pp. 2229–2243, 2021, doi: 10.1109/ACCESS.2020.3047723.
- [25] H. Y. Jung, Y. S. Heo, and S. Lee, "Fingerprint liveness detection by a template-probe convolutional neural network," *IEEE Access*, vol. 7, pp. 118986–118993, 2019, doi: 10.1109/ACCESS.2019.2936890.

## BIOGRAPHIES OF AUTHORS



**Pratibha Shinde**    received the B.E degree in information technology from North Maharashtra University, Jalgaon in 2011. And also received the M. Tech degree in Computer Science and Engineering from Jawaharlal Nehru Technological University, Hyderabad in 2014, where she is currently pursuing the Ph.D. degree. She is currently working as assist. Prof. with Department of Information Technology, Dr. Vithalrao Vikhe Patil Foundation's Dr. Vithalrao Vikhe Patil College of Engineering, Ahmednagar. Where she is also a member of the Institution of Engineers (India). Her current research interests include machine learning, image processing, artificial intelligence. She can be contacted at email: ps21.shinde@gmail.com.



**Ajay R. Raundale**    currently holds the position of Assistant Professor in the Department of Computer Science Engineering at Dr. A. P. J. Abdul Kalam University in Indore, India. With over a decade of experience in teaching and the educational corporate sector, he has achieved significant milestones. He holds a Ph.D. in Computer Science and Engineering, an M. Tech in Digital Communications, and a BE in Electronics and Telecommunications. Dr. Raundale's research interests primarily revolve around machine learning and data mining. He has an impressive publication record, with over 15 papers published in renowned international journals and conferences. Additionally, he serves as an editorial board member for four international journals. Demonstrating his commitment to advancing research and development, Dr. Raundale holds a directorial position at Advance Research and Development, India (ARD INDIA). He can be contacted at email: arraundale@gmail.com.