# A Study on Face Recognition and Face Spoofing Detection Techniques

Khyati Jash Desai
Research Scholar
School of Information Technology
Auro University, Surat

Sunil Kumar, PhD
Assistant Professor
School of Information Technology
Auro University, Surat

## ABSTRACT
Security has become major concern in early years. For security purpose, Face recognition is used. The security of this technique can be compromised by various attacks. "Face spoofing is one of the attacks where non-original image of valid user's face presented to the camera to access the system [15]" So the present study attempts to explore the face spoofing detection techniques through a comparative analysis. The present study has three main objectives. 1. To identify and explain the component of face spoofing techniques. 2. To do the comparative analysis on different face spoofing techniques. 3. To develop or modify an efficient technique to find face spoofing. This study is quantitative in nature. This study aims to discover the best method for detecting face spoofing. Identify component like face recognition, effective factors etc. from different techniques. Also this study aims to identify best dataset for detecting face spoofing. This study presents one comparative analyses. It helps one to select a technique for their future work based on its advantages and disadvantages and the dataset used, which helps one to identify the most suitable dataset. At the end this study reviewd some effective techniques for someone who wants to use that technique into their study or work.

## Keywords
Face Recognition; Face Spoofing; Face Spoofing Techniques; Comparative Analysis

## 1. INTRODUCTION
"Face spoofing is one of the attacks where non-original image of valid user's face presented to the camera to access the system [15]." Face spoofing is also known as "Identity Spoofing". As the most commonly used biometric parameter, the face has been used for personal and commercial purposes, such as accessing laptops, personal computers, automatic teller machines (ATMs), online banking, airports, and border control. Face spoofing is one of the most common and low budget methods to perform biometric authentication that's why almost all business sector use this anti-face spoofing technique for their security purpose. By using this method ones can secure them account, data and identity. So there is less chance of fraud. Face recognition systems have been extensively used in government as well as commercial applications such as mobile, banking and surveillance systems etc. [13].

Anti-spoofing is a technique that involves minimizing the potential ability of fraud to happen, with respect to facial recognition systems and associated technology. In 1992, for the first time, Hoogsteden suggested that the face spoofing can be a potent threat for biometric modalities. After that, Stephanie A. C. Schuckers in 2002 gave a detailed study of spoofing and anti-spoofing [13].

In this early age, security has become a major concern. Face recognition is one of the techniques for security. These methods become insecure due to different types of attacks, such as photo attacks, video attacks and 3D masks [8]. The current study aims to explore the detection techniques of face spoofing.

In this study, different approaches to face spoofing detection have been examined. Finally, this study presents the techniques with their advantages and disadvantages. Also the study presents the databases which have been used with its techniques.

As a part of this research, this review paper read different journals, conference papers and review papers about this topic to gain some knowledge about it.

### 1.1 Face Spoof Detection Application
The concept of face spoofing is using a person's fake images to simulate their facial biometrics. There are various methods and techniques to detect this fake image. One needs to perform certain steps to detect the fake face.

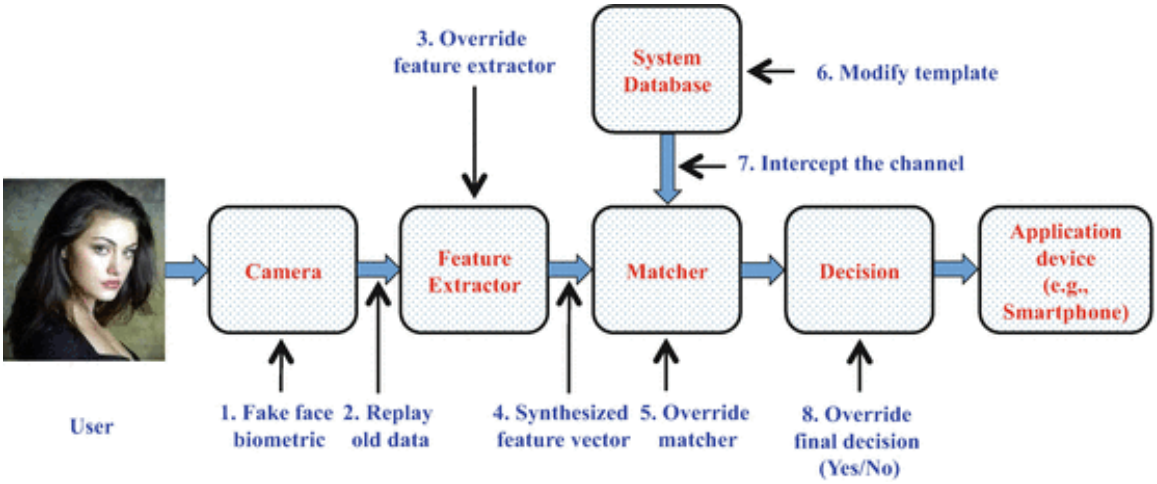


**Fig 1: Work of Anti Face-Spoofing Application [19]**

In above figure how anti face-spoofing application works that id describe. In this application ones photo can be captured. Then from database data are replayed to compare the original face image. Then different types of features like face curve, eye portion, flash light ratio are extracted then technique is use to match the database image and feature extracted image. Then one decision comes that if that image is real or fake. On application devices such as smartphones, laptops, etc., that output is displayed on the screen with a message.

## 1.2 Types of Attack

In order to gain authentication, attackers submit fake evidence to biometric system called as spoofing attack. In fact, a spoofing system can easily generate such an attack since images and videos of that person can easily be found online on social networks or captured remotely. In order to access the system, the attacker must display pictures and videos obtained from unauthorized sources onto the device. Fig. 2 shows different types of attack in spoofing.

Basically spoofing is divided into 2 parts 2D attack and 3D attack. 2D face spoofing is performed with the help of photographs and videos. 3 D face spoofing is performed with a 3D mask which needs more cost [3].

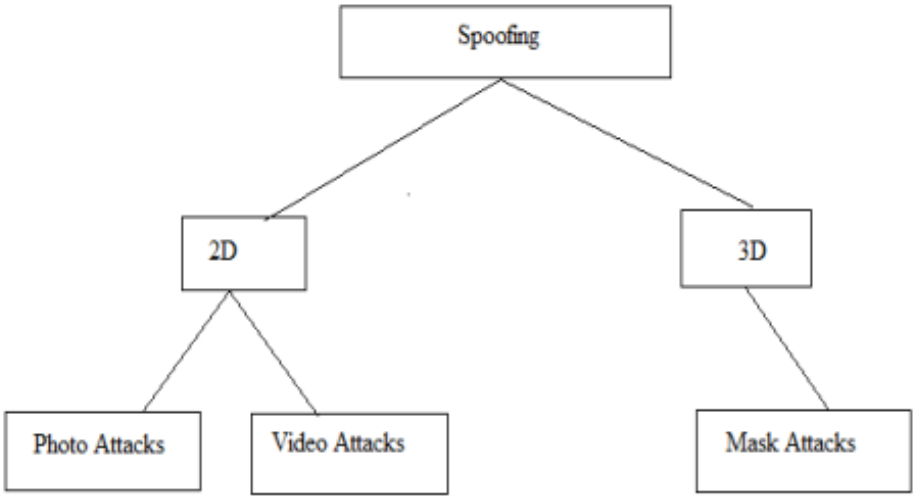


**Fig 2: Type of Attack [8]**

### *1.2.1 Photo Attack*

The photo attack is a type of biometric spoofing in which the attacker simulates the identity of another using his or her fake image. An attacker can either capture the pictures from a digital device such as a camera or a mobile from a distance without taking his/her permission [8].

### *1.2.2 Video attack*

An attack using video can also be used in face-spoofing. Here, the attackers try to spoof the users biometric by playing the video. A video appears more natural than a print image to the face recognition system [8].

### *1.2.3 Mask attack*

Mask attack can be broadly categorized into paper cut masks and wearable masks [8]. The wearable mask attacks are more effective at simulating some other user's biometric data.

## 2. RELATED WORKS

### 2.1 Color Distortion technique

In article [4] proposed the color distortion technique for face spoof detection. In their previous work, they added an element called the "Recapturing process". Then they applied their proposed method to three different databases that is Replay-Attack, MSU and CASIA. They experiment their proposed method on that three databases. In first database that is Replay-Attack they found BPCER@APCER1% = 0% to BPCER@APCER1% = 5% compared to the default evaluation setting (the same illumination for enrolment and evaluation) results. In second database that MSU, they found Poor performance is achieved with BPCER@APCER1% = 65% and BPCER@APCER1% = 85% in both experiments, respectively. and in third database that is CASIA, they found BPCER@APCER1% = 80% and BPCER@APCER1% = 66.7% in both experiments using the medium quality sensor and low quality sensor, respectively. Finally, they conclude that using recapturing process this proposed method gave them the best result on those three main databases. And they also give two main limitations of this proposed method [mentioned in Table 1].

### 2.2 Texture and local shape feature based technique

In [9] they proposed texture and local shape feature based techniques for face spoof detection. The proposed approach analyzes the texture and gradient structure of facial images using low-level feature descriptors, fast linear classification and score level fusion. Low-level feature descriptors include edges and blobs of an image. And it is based on image processing techniques. In Fast linear classification only be used to classify data that is linearly separable. In score-level fusion the match scores output by multiple biometric matchers are consolidated in order to render a decision about the identity of an individual. This work is based on three different databases that is NUAA Photograph Imposter Database, Yale Recaptured Database and Print-Attack Database. In NUAA database, their proposed method gives 0.999 AUC. On second database their proposed method give 100% Accuracy result. and on third database, their proposed method give excellent result. Lastly, they conclude that their proposed work also be extended to detect spoofing attack using mask or 3D model.

### 2.3 Color texture based technique

[15] in their article used color texture based face spoof technique to face recognition. In their proposed work they use two-stage face detection and face verification. Then they use two algorithms viola-jones algorithm and histogram of oriented gradients algorithm to detect the face in an image. Among them, they conclude that HOG (Histogram) algorithm was more accurate. They achive 91.29% accuracy. They also said that this system can be implemented to secure the accounts and device from spoof-attack.

### 2.4 CNN model

[18] in their article they proposed to use CNN. On this CNN model, they try different data augmentation strategies. And they find that their proposed method makes a significant improvement. They use two datasets for this REPLAY-ATTACK and CASIA dataset. CASIA stands for Chinese Academy of Sciences (CASIA)The Replay-Attack Database for face spoofing consists of 1300 video clips of photo and video attack attempts to 50 clients, under different lighting conditions. After their experiment they achive 97% accuracy on both database.And lastly, they suggest integrating this proposed method with the motion and shape-based methods.

### 2.5 End-to-End CNN architecture

An end-to-end approach is a technaiue where the model leanrs all the steps between the initial input phase and the final output result. [12] in their article they develop an end-to-end CNN architecture for face anti-spoofing application. Then they perform an extensive evaluation on CASIA-FASD dataset. CASIA-FASD dataset is a small face anti-spoofing dataset containing 50 subjects. They got 85% accuracy and 7% EER on this database by using their proposed architecture. Lastly, they conclude that their proposed CNN architecture was effective on both top-1 percentage accuracy[1] and traditional performance evaluation metrics. And it also provides the platform to assess further the capabilities of various CNN paradigms using an end-to-end approach.

### 2.6 Deep CNN

[2] in their article present deep CNN based approach. In this article, they used an SVM(Support Vector Machine) classifier and two networks namely AlexNet and ResNet-50 to test a pre-trained CNN networks. AlexNet is a Convolutional neural network that is 8 layer deep. ResNet-50 is also a Convolutional neural network that is 50 layer depp. They use two approaches 1. Applying pre-trained CNN for extracting features using AlexNet with SVM and ResNet-50 with SVM classifier. 2. Applying transfer learning from the AlexNet model for extracting features. They got best result of 100% on YTF database.

### 2.7 Light CNN using Biometric Quality Assessment

[7] in their article present light CNN based approach using biometric quality assessment(BQA) method. This method id used to monitor the video surveillance cameras and also used to evaluate the visual quality of a face image. In this approach three database were used namely CASIA-wabface, LFW and YouTubeFace. In this light CNN model was trained in CASIA database. CASIA-webface is a one kind of dataset contains 4,94,414 face images of 10.575 real identities collected from web-source. LFW stands for Labeled Faces in the Wild and contains 13,233 images of faces collected from web source. YouTubeFace dataset desinged for studying the problem of unconstrained face recognition in video and having 3425 videos of 1595 different people. And another two database

[1] Top-1 percentage accuracy
- This method considers only the output class that has the highest probability.
- Classes are arranged sequentially at the output of a CNN in such a way that the index of a class corresponds to the label of that class.
- It counts a true positive or true negative if the index of the class, which has maximum probability among other classes, matches the corresponding true label, otherwise it counts a 0.

were used for testing this model. Last conclusion was that their BQA model can precisely predict the quality of a face image.

## 2.8 Deep Learning Methods

[10] in their aertical they used different models like ResNet50, ResNet152, VggNet15, VggNet19, DensNet121, DensNet169, MobileNet and EfficientNetB0 to test. They used 2 parameter namely recall and precision. And at the end they give accuracy of all these models.

## 2.9 Securing Face recognition using Blockchain

[14] in their article they present blockchain to secure the data for face recognition. They used VGGFace CNN for feature extraction and face recognition. and to secure data Blockchain is used. Three database ORL, LFW, FEI used. and they got heighest accuracy that is above 95% on ORL dataset.

## 2.10 Other Techniques

Kanika kalihal (2019) in their article they reviewed on different face spoof detection techniques in the biometric system. Firstly, they classify three types of such as attack photo, video and mask. Then they broadly reviewed two techniques such as hardware based technique and feature based technique. In feature based again, three types namely frequency based, texture based and motion based. Then they describe five parameters to evaluate the system FAR, FRR, HTER, accuracy and EER.

A FAR stand for False Acceptance Ratio and it is a unit to measure the average number of false acceptance within a biometric security system. A FRR is stands for False Rejection Rate and it is described as the percentage of identification instances in which authorized users are incorrectly rejected. HTER stands for Half Total Error Rate and it is an average of both FAR and FRR error rates. Accuracy means how accurate the system is. And EER stands for Equal Error Rate and it inherently references to an Algorithmic approach of Error margin, where ones equalize false rejections and false acceptances.

[3] in their article presents different type of attack and review on latest works regarding face spoofing detection techniques. In this paper, three attacks were presented, namely Printed photo attack, replay video attack and 3D mask attack. In printed photo attack attacker use printed photo to gain the access of the system. Replay video attack is a form of network attack in which valid data transmission is maliciously or fraudulently repeated or delayed. In 3D mask tack attacker wear 3D mask of different material and try to access the system. And lastly paper presents different approaches, namely texture based, motion based, image quality based, frequency based and some others. Then they give one summary table with the technique used type of attack, the database used and its performance.

# 3. COMPARISON OF DIFFERENT TECHNIQUES

Table 1 gives a comparative analysis of different method reviewed above with databases used to implement that technique. By studying this one can get a brief idea about the databases which are used to implement a particular technique.

**Table 1. Different techniques and used databases**

| Sr. No. | Technique Used | Database Used | Advantages | Disadvantages |
|---|---|---|---|---|
| 1. | Color Distortion Technique [4] | Replay attack, CASIA and MSU public database | By using “Recapturing Process” this technique give a more efficient result. | One disadvantage was it can be bypassed quite easily if there is video feedback. And the second one was it has difficulty distinguishing color distortions due to unknown variations. |
| 2. | texture and local shape feature based technique [9] | NUAA Photograph Imposter, Yale Recaptured, Print-Attack | This technique gives excellent result for several real and fake faces. Compare to other technique, this technique was robust, fast and no requirement of any user-cooperation. | In this technique, the excellent results suggest also that more complex databases with various types of high-quality spoofing attacks and proper protocol are needed for future development. |
| 3. | Face liveness detection using flash [3] | flash | Advantages of this method include low installation cost of flash and no user cooperation required. . Also the use of flash successfully improves face liveness detection in terms of accuracy, robustness and running time. (Patrick, Weiwen, Daniel, Fei, Xizhao and Chien, 2017) | Not applicable to 3D spoofing attacks, for instance, rigid 3D mask and 3D face models with various expressions. (Patrick, Weiwen, Daniel, Fei, Xizhao and Chien, 2017) |
| 4. | Anomaly detection based approach - one class. [3] | CASIA MSU Replay Attack | It was demonstrated that the anomaly-based formulation is not inferior as compared with the conventional two-class approach. (Shervin, Josef and William, 2017) | Accordingly, both formulations (one-class and two-class) did not perform well and more research was needed to improve the detection rates. (Shervin, Josef and William, 2017) |

| | | | | |
|---|---|---|---|---|
| 5. | Dynamic texture using CVLBC. Feature descriptor. [3] | Print Attack, CASIA FASD. Replay Attack | This method shows good performance. Thus, the proposed method is able to distinguish between valid users' facial videos and those of impostors by distinguishing their motions and their appearances. (Xiaochao, Yaping and Janne, 2017) | NA |
| 6. | Deep texture feature extraction using CNN +LBP [3] | NUAA spoofing Database | This technique shows great result in NUAA dataset. Also this method are more efficient than other state-of-the-art techniques. (Gustavo, Daniel, Rafael, Aparecido and João, 2017) | NA |
| 7. | Unsupervised domain adaptation method. [3] | CASIA attack, Replay Attack MSU Rose- You tu | As compared with the straightforward learning approach without domain adaptation, the results show that domain adaptation achieves an average 20% improvement in generalization ability. (Haoliang, Wen, Hong, Shiqi, Feiyue and Alex, 2018) | More research can be done by using this method to gain more accurate result. (Haoliang, Wen, Hong, Shiqi, Feiyue and Alex, 2018) |
| 9. | Color Texture Based Technique [15] | VGG7 architecture | CNN used in classifying, is more advantageous and produce better accurate result than that of other Machine learning and classifying techniques. | It failed to predict the faces properly under certain improper light conditions |
| 10. | End-to-End architecture [12] | CASIA-FASD | Accurate and Excellent Result | Need to improve by using some different databases. |
| 11. | CNN model [18] | REPLAY-ATTACK, CASIA | Compare to other technique give good result. | Due to different capturing conditions not getting a more efficient result. |
| 12. | Deep CNN [2] | AlexNet, ResNet-50 | This technique gives 94% to 100% accuracy in given all the databases. ResNet-50 with SVM took less time than other networks with all datasets. | To train the data model more datasets need to be included. So classification and recognition accuracy improved. |
| 13. | BQA method [7] | CASIA-webface, LFW and YouTubeface | This approach precisely predicts the quality of a face image. And this approach can also be embedded into face recognition system. | This proposed BQA model shows inferior performance for several distortion categories. And also critical to detect whether a face image is falsified. |
| 14. | Deep Learning methods [10] | AlexNet, VGGNet, ResNet, MobileNet, DensNet and EfficientNet | In this approch EfficientNetB0 method give better result compare to other. | Only EfficientNetB0, MobileNet and DensNet169 models are more efficient and have acceptable accuracy for this application. |
| 15. | Securing Face recognition with Blockchain. [14] | ORL, LFW and FEI | Blockchain give excellent security to the data. VGGFace deep neural network was used for feature extraction and logistic regression as a classifier which resulted in increased accuracy in less time. | NA |

(CVLBC – Volume Local Binary Count, CNN – Convolutional Neural Network, LBP – Local Binary Pattern, BQA – Biometric Quality Assessment, CASIA FASD - Institute of Automation, Chinese Academy of Sciences, NUAA - Nanjing University of Aeronautics and Astronautics, MSU – Montana State University, VGG – Visual Geometric Group, LFW – Labeled Faces in the Wild )

## 4. DISCUSSION AND CONCLUSION

Face spoofing is substantial challenge in face recognition systems. Face spoofing detection techniques have been proposed, but none is without limitations, such as lack of generalization to unseen attack types and environmental factors. Despite advances in face recognition technology, spoofing attacks remain as a significant security threat.

In this paper, many techniques are reviewed and discussed. Furthermore, one comparative studies based on techniques have been performed on this paper. The Techniques re

compared based on databases used and their advantages / disadvantages. After reviewing these all techniques this paper concludes that no techniques have that much accuracy rate to find spoof face accurately. By studying this paper, one can get the knowledge about the different techniques available. Also one can get the knowledge that till now some particular database were already used with technique. And he\she can implement some another database to perform the technique. Also by using this paper one can easily found different techniques advantages/disadvantages. So that ones can easily get that which method he\she wants to implement for their work.

The purpose of this paper is to provide new comers in the face spoofing field with a review of different types of attacks and recent techniques of detecting face spoofing among with the database used and advantages disadvantages.

## 5. REFERENCES

[1] Electronic IDentification. (2021, July 5). Retrieved from electronicid: https://www.electronicid.eu/en/blog/post/facial-spoofing-what-it-is-how-to-prevent-it-and-spoofing-detection-solutions/en

[2] Almabdy, S., & & Elrefaei, L. (2019, October 17). Deep Convolutional Neural Network-Based Approaches for Face Recognition. Applied Science, 9(20), 1-21.

[3] Daniel N., A. A. (2018). A Study on Recent Trends in Face Spoofing Detection Techniques. nternational Conference on Inventive Computation Technologies (ICICT) (pp. 583-586). Coimbatore, India: IEEE.

[4] Edmunds, T. &., & Caplier, A. (2018). Face Spoofing detection based on colour distortions. IET biometrics, 7(1), 27-38.

[5] Gustavo, B., Daniel, F., Rafael, G., Aparecido, N., & João, P. (2017, October 20). Deep Texture Features for Robust Face Spoofing Detection. IEEE Transactions on Circuits and Systems II: Express Briefs, 64(12), 1397-1401.

[6] Haoliang, L., Wen, L., Hong, C., Shiqi, W., Feiyue, H., & Alex, K. (2018, February 02). Unsupervised Domain Adaptation for Face Anti-Spoofing. IEEE Transactions on Information Forensics and Security, 13(7), 1794-1809.

[7] Jun, Y., Kejia, S., Fei, G., & Suguo, Z. (2018, May 3). Face Biometric Quality Assessment via Light CNN. Pettern Recognition Letters, 107, 25-32.

[8] Kanika kalihal, J. K. (2019, Mar-Apr). A Review on Different Face Spoof Detection Techniques. International Journal of Scientific Research & Engineering Trends , 5(2), 609-611.

[9] Määttä J., H. A. (2012, March). Face spoofing detection from single images using texture and local shape analysis. IET biometrics, 1(1), 3-10.

[10] Nader, E., Mustafa, A., & Banu, A. (2022, Jun 7). Liveness control in face recognition with deep learning methods. The European Journal of Research and Development(Vol. 2 No. 2 (2022): The European Journal of Research and Development), 92-101.

[11] Patrick, C., Weiwen, L., Daniel, Y., Fei, Z., Xizhao, W., & Chien, H. (2017, October 02). Face Liveness Detection Using a Flash Against 2D Spoofing Attack. IEEE Transactions on Information Forensics and Security, 13(2), 521-534.

[12] Rehman, Y. A. (September, 2017). Deep learning for face anti-spoofing: An end-to-end approach. Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA) (pp. 195-200). Poland: IEEE.

[13] Sandeep, K., Sukhwinder, S., & Jagdish, K. (2017). A comparative study on face spoofing attacks. 2017 International Conference on Computing, Communication and Automation (ICCCA) (pp. 1104-1108). Greater Noida: IEEE.

[14] Saumya, S., Jitendra, M., & Poonam, S. (2020). Securing Face Recognition System Using Blockchain Technology. Second International Conference, MIND. 2, pp. 449-460. Silchar,India: Springer.

[15] Shatish, B., & Kumar, S. (May 2019). FACE-SPOOF DETECTION SYSTEM USING CONVOLUTIONAL NEURAL. nternational Conference on Recent trends in Electronics, Computing and Communication Engineering (p. 6). chennai: Conference.

[16] Shervin, R., Josef, K., & William, C. (2017, July 19). An Anomaly Detection Approach to Face Spoofing Detection: A New Formulation and Evaluation Protocol. IEEE Access, 5, 13868 - 13882.

[17] Xiaochao, Z., Yaping, L., & Janne, H. (2017, September 08). Dynamic Texture Recognition Using Volume Local Binary Count Patterns With an Application to 2D Face Spoofing Detection. IEEE Transactions on Multimedia , 20(3), 552-566.

[18] Yang, J., Lei, Z., & Li, S. Z. (2014, Aug). Learn convolutional neural network for face anti-spoofing. arXiv preprint arXiv, 2, 1-8.

[19] Zinelabidine Boulkenafet, Z. A. (2016, December 24). Springer Link. Retrieved February 2, 2022, from springer.com: https://link.springer.com/chapter/10.1007/978-3-319-47301-7_13