Face Spoofing Attacks And Detection: A Review

Lokesh M.Giripunje[1], Om Dandade[2], Poorvi K.Kulkarni[3], Pranita H.Kulkarni[4]
[1]Assistant Professor, Dept of Electronics and Telecommunication
[2, 3, 4]Dept of Electronics and Telecommunication
[1, 2, 3, 4] Dr. D Y PatilInstitute of Engineering, Management and Research, Akurdi, Pune - 44, Maharashtra, India

Abstract- *Recently, face recognition systems have become popular and are being used heavily in mobile devices and surveillance systems due to the convenience they provide. Face biometric provides a convenient, contactless, accurate, and instruction-less way for authentication when compared to other biometrics like fingerprint and voice recognition. As the technology is evolving, face recognition is being even accurate and safer. But it's well known there are always two sides, unluckily they are even unsafe due to how easy it is to do presentation attacks like photos, videos of currently 3D prints of a registered user. And capturing photos and videos without consent makes it even easier. A lot of research is already been done for the development of a face anti-spoof system. In this paper, the authors have reviewed various face spoofing detection methods proposed by several researchers. This paper covers popular approaches made in the development of face anti-spoof systems and gives a comparative study of the same by comparing the popular methods those cover 2D (print and replay) attack detection, 3D (3D printed mask, etc) attack detection, and attempts to breach such anti-spoofing systems.*

Keywords- Face recognition, Face Spoofing, 3D prints, Anti-spoofing, Spoof detection

I. INTRODUCTION

A generic face recognition system extracts facial characteristics and features from input data (photo, video, or 3D data) to compare it with the database of already registered faces to find a match.[18][19] Facial recognition is considered one of the strongest authentications because of the number of data points that can be collected from a face leading to a password which has more than billions of permutations and combinations, and a variety of facial features across individuals and. When compared to other faces biometric is the most convenient and instruction-less as it needs a user to only make his/her face visible to the sensor. Also, being contactless authentication makes it more advantageous in a pandemic situation where disease spreads through touches [17].

Lately, face recognition is being extensively used in mobile devices like Smartphones, Tablets, and Laptops. Only some of them use a sensor that can detect the contour of the face in real-time and others only use 2D data from cameras they have. Comparing the methods of authentication fig 1.1 show the possibility of the same being breached.

SMARTPHONE UNLOCK METHOD	TOTAL POSSIBLE COMBINATIONS	APPROX FALSE ACCEPTANCE RATE
ANDROID 9 PIN PATTERN	389,112	0.0003%
iOS 6 DIGIT PIN	1,000,000	0.0001%
ANDROID 2D FACE UNLOCK	1000	0.1%
CAPACITIVE FINGERPRINT	50,000	0.002%
iOS FACE-ID	1,000,000	0.0001%
ANDROID 6X6 GRID	≅100,000,000	≅0.0000001%

Fig 1.1 comparison of authentication methods in mobile devices [3]

The probability of false input getting accepted is calculated based on possible combinations the method provides. Face recognition is very secure yet convenient.

Also, if there is a lock there is always a key-maker, unfortunately, face recognition also can be fooled by someone who is pretending to be someone else. And this high accuracy comes with the disadvantage of more vulnerabilities which is been discussed below[1].

II. FACE SPOOFING ATTACKS

A spoofing attack is nothing but a false acceptance in which attackers submit fake evidence to the biometric system to gain authentication [1] [2]. Is easy to such an attack because one can capture someone's phots/video from a distance without their consent and can also get it from social media websites. Fig. 2.1 represents a simple face spoof attack using a photo of a registered user.

Fig. 2.1 Simple face spoof attack using a photo [4]

These attacks can be categorized as 1. 2D attacks and 2. 3D attacks [1][20].

1. 2D attacks

2D attacks where the attacker can fool a camera sensor by using a high-resolution image or playing video facing directly to the camera. These are also known as print and replay attacks, fig 2.2 represents an example of prints and replay attacks. These can easily breach a face recognition system that only relies on the camera and doesn't use any anti-spoofing technique. Some of the examples include using a high-resolution photo, using a monitor, using any mobile display like a smartphone, tablet, etc.

Fig. 2.2 Example of print and replay attack [4]

2. 3D attacks

Where 3D is where the attacker tries to mimic the original person's facial contours as a false input. Now as the attacker have a detailed 3D face copy of a registered person it can easily breach a camera-based system and 3D sensing systems too. It can be done using a detailed 3D printed face model or a face mask. Fig 2.3 provides an example of the same.

Fig. 2.3 Hyper-realistic 3D printed face model [16]

Currently, 3D printers are already available and use materials like plastic, polycarbonate, and some UV-sensitive materials providing great details.

III. LITERATURE REVIEW

In the past 50+ years, face recognition has developed vigorously and achieved great success. For the past 10-15 years researchers have been working on anti-spoofing techniques, but in this area of research new problems had kept coming and so does the research. Fig 3.1 shows a block diagram of a generic anti-spoofing system. The techniques that have been used for anti-spoofing systems can be classified on basis of attack type i.e., 2D attacks and 3D attacks. The following literature survey compares the popular methods that have been used.

3.1 Methodologies for prints and replay attacks

Using CNN Classifier

This anti-spoofing method is comprised of two parts, detection of blinking of the eye which asses openness of eyes and then movements of the lip, and the CCN classifier module. Databases like NUAA photo imposter, CASIA-SURF, Siw, CSMAD, MSU USAA were used. It predicts the output using trained class for positive inputs. Print and replay attacks were detected with an accuracy of 93.52 % [5].

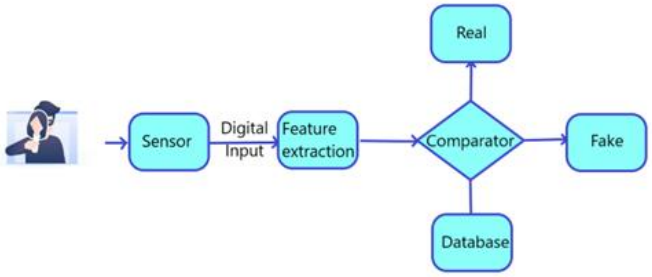

Fig 3.1 Generic anti-spoofing system

Detection with Flash

The main motive of the research was to propose an efficient face spoofing attack detection approach that requires nominal hardware and uses a small database. Using a single visible light camera, the proposed approach captures two photos face, one with and the other without the flash. For prediction of spoofi) specular reflections from the eye-ball and ii) diffuse reflections from the other contours of the face were considered. It covers Print and replay attacks and was tested on mobile devices i.e., iPhone7 (A1779), iPhone XR (A2106), and iPad Pro (A1876), and MacBook Pro and found to have Lesser computational time for tested mobile devices [6].

Micro-Texture Analysis

By evaluating the quality of the image, printing artifacts, their characterization, and differences in reflection, the spoofing detection was done from a texture analysis point of view [21][22]. This approach evaluates the texture present in the images using multi-scale local binary patterns (LBP) and sup-port vector machine (SVM). For print and replay attacks it was accurate 99% of the time, which is more than previous using the same database [7].

Motion Magnification

In this approach, the author enhances the complex expressions captured in video using Eulerian motion magnification and these expression/micro-expressions were considered as a feature. Next, feature extraction was done in two ways: (i) By configuring LBP which was computationally more efficient than other texture-based approaches and (ii) estimation of motion using HOOF descriptor. For Print Attack and Replay Attack, the proposed approach had shown improved performance; including HOOF descriptor giving a total error rate of 0% and 1.25% respectively [8]

Anomaly Detection

Unlike two-class recognition problems where relevant features of both positive (real access) and negative samples (spoofing attempts) are utilized to train the system, the Model was trained to detect spoofs using one class only i.e., positive class and anomaly detection was to distinguish spoofing attacks. And was claimed to cover all prints, replay, and unseen attacks.The performance of both formulations (one-class and two-class) was not adequate [9].

Table 3.1 gives a quick overview of the methods discussed above.

Table 3.1 Comparison of proposed methods and techniques for Print and Replay attacks

Sr. No.	Method	Main principles and working	Attack covered	Conclusion	Author and Year of publication
1	Using image data and CNN	1. Input images were preprocessed to extract more information 2. CNN was to predict based on trained data	Print and replay attacks	Print and replay attacks were distinguished with precision of 93.52%	Raden BudiartoHadiprakoso 2020 [5]
2	Detection with Flash	1. Utilizing one monocular visible-light camera 2. Prediction of liveliness using i) specular reflections from the iris region ii) diffuse reflections from the entire	Print and replay attacks	Lesser computational time and tested on mobile devices	Akinori F. Ebihara, Kazuyuki Sakurai, Hitoshi Imaoka 2021 [6]
3	Micro-Texture Analysis	1. Analyzing texture using printing defects, specular reflections and shadows. 2. Done using multi-scale local binary patterns (LBP) and 3. support vector machine (SVM)	Print and replay attacks	Was accurate for 99% of the time, which is more than previous using same database	Jukka Maatta, Abdenour Hadid, Matti Pietikäinen 2011 [7]
4	Motion Magnification	1. LBP for texture analysis 2. Motion estimation approach using HOOF descriptor.	Print and replay attacks	Total error rate of 0 % and 1.25% was achieved	Samarth Bharadwaj, Tejas I. Dhamecha, Mayank Vatsa and Richa Singh 2013 [8]
5	Anomaly Detection	1. Spoofing detection using anomaly detection 2. One-class classification 3. The local binary pattern (LBP)	Print and replay attacks	Performance of both formulations (one-class and two-class) was not adequate	Shervin RahimzadehArashloo, Josef Kittler, William Christma 2017 [9]

3.2 Methodologies for 3D printed attacks

3D Face shape analysis using a 3D scanner

Using Vectra 3D CRT system, based on the 3D structure of the face, is proposed. The ability to process the 3D contour of the face allows the biometric system to distinguish between a live face and a flat image. Considering this as a feature for 3D and 2D recognition systems, latter insituations where 3D data could be computed from two or more 2Dimages captured by the sensor. Can be used for 3D printed attacks to some extent [10].So, by creating super realistic 3D masks and matching the resolution of the scanner, such systems can be spoofed.

rPPG based spoofing detection

Remote photoplethysmograph (rPPG) signal is a recently developed liveness clue for face-spoof detection [23][24].Uses domain-specific Efficient Net as the classification method. The performance of this approach was experimented with and evaluated using databases named3DMAD and HKBU-Mars V2exhibiting superior performance over state-of-the-art rPPG-based face anti-spoofing algorithms. And it shows that the proposed approach surpasses the performance of already rPPG-based methods significantly and consistently [11].

Texture-based methods

In this approach, the author tracked unusual textures present on face masks like askew figures and reflected articles [25].On the CASIA FASD and the MSU MFSD, analyzing the

color textures presents on the face over HSV and YCbCrcolor spaces the proposed method outperformed existing methods. while exhibiting superior performance for Replay-Attack Database i.e., CASIA FASD and the MSU MFSD[12]. When it comes to hyper-realistic 3D prints texture-based analysis usually has deficient generalization ability.

Motion-based methods

By recognizing micro-expression on the human face this approach can differentiate between the 3D mask and the human face. The human face can create complex micro-expressions thanks to dense facial muscles present on a human face, which make it nearly impossible to mimic[14]. By jointly learning the channel discriminability and spatial-discriminability, more discriminative deepdynamic textures are further emphasized in the joint discriminative learning model Proposed method had good generalization ability, which is more applicable in real-world scenarios.

Table 3.2gives a quick overview of the methods discussed above.

Table 3.2 Comparison of proposed methods and techniques for 3D printed attacks

Sr. No.	Method	Main principles and working	Attack covered	Conclusion	Author and Year of publication
1	3D Face shape analysis using a 3D scanner	1. Vectra 3D CRT system was used to take input 2. The shape of the face was analyzed	Print and replay and 3D masks	Scanning and collecting data using a CRT scanner were not enough due super-realistic face mask.	Andrea Lagorio, Massimo Tistarelli 2013 [10]
2	rPPG based spoofing detection	1. rPPG signal was used as the feature for liveliness detection 2. This approach surpasses the already existing rPPG-based methods	Print and replay and 3D masks	This method works flawlessly despite processing of rPPG becomes the real problem as it is prone to have a lot of noise	Changlin Yao, Shihe Wang 2021 [11]
3	Texture-based methods	1. The spoof was detected using abnormalities in the texture of spoof face 2. Analysis of color texture in HSV and YCbCr color space	Print and replay and 3D masks	Good performance was achieved on Replay-Attacks. Cannot withstand hyper-realistic 3D prints.	Z. Boulkenaf et, J. Komulainen 2016 [12]
4	Motion-based methods	1. Micro expression from human face was used as feature/characteristic	Print and replay and 3D masks	The human face has so many facial muscles which can create expressions that are hard to mimic. So have great generalization ability.	Y. Tang and L. Chen 2017 [14]

3.3 Spoofing attacks on anti-spoofing systems

Nesli Erdogmus and Sébastien Marcel in their research studied the potential and limit of anti-spoofing systems using 3D facial masks for different systems [13]. The various approaches towards the anti-spoofing system were assessed by using 2D, 2.D, and 3D masks against them. Both 2D and 2.5D masks were used against texture-based countermeasures, a parallel study with comprehensive experiments was performed. The evaluation of performance was done on two databases namely Morpho and 3DMAD, which had differing protocols used in them.

The following points were concluded [13]:

1) Spoof detection is better for 2D attacks than 2.5D.
2) The approaches with extraction based on LBP improved classification rates, significantly for 2D presentation.
3) While all classifiers are performing well the SVM and LDAare mostly drawn ahead.
4) Modified LBP exhibited the best performance than extended LBP for all scenarios.
5) Using linear kernels was found to be helpful For SVM classifiers.

IV. CONCLUSION

In today's generation where the digital security system is used in large numbers, spoofing attacks are causing high-security threats for biometric recognition systems. When identifying a face, it is easy and obvious to fool an unprotected recognition system. A lot of successful research is already been done to overcome these drawbacks. However, creating and using 3D masks for face spoofing attacks has become easier. Using 3D masks has become not only easy but also cheap thanks to ever-evolving 3D printing techniques.

The review shows that, Because of evolving 3D reconstruction technology, there's a lot of scope for the research on 3D spoof detection. As most of the anti-spoofing techniques are based on the attacks done in past it is difficult to catch an impostor with a new idea of spoofing. And also discussed new clues that can be used for training and recognition while having minimal hardware requirements

REFERENCES

[1] Sandeep Kumar, Sukhwinder Singh, Jagdish Kumar. “A Comparative Study on Face Spoofing Attacks”. ISBN: 978-1-5090-6471-7/17/, 2017 IEEE.
[2] Galbally, Javier, Sébastien Marcel, and Julian Fierrez. "Biometric antispoofing methods: A survey in face recognition." IEEE Access, vol. 2, pp. 1530-1552, 2014.
[3] Arun Maini. “How secure your Android Unlock Pattern ACTUALLY is”. YouTube.
[4] Shervin Arashloo, Josef Kittler, William Christma. “An Anomaly Detection Approach to Face Spoofing Detection: A New Formulation and Evaluation Protocol”. IEEE Access 10.1109/ACCESS.2017.2729161
[5] Raden BudiartoHadiprakoso, Hermawan Setiawan, Girinoto. “Face anti-spoofing Using CNN classifier and liveness detection”. 3rd International conference, IEEE 2020
[6] Akinori F. Ebihara, Kazuyuki Sakurai, Hitoshi Imaoka. “Efficient Face Spoofing Detection with Flash”. IEEE

Transactions on Biometrics, Behaviour, and Identity Science, 2021.

[7] Jukka Maatta, Abdenour Hadid, Matti Pietikäinen. "Face Spoofing Detection from Single Images Using Micro-Texture Analysis". 978-1-4577-1359-0111 2011 IEEE

[8] Samarth Bharadwaj, Tejas I. Dhamecha, Mayank Vatsa and Richa Singh. "Computationally Efficient Face Spoofing Detection with Motion Magnification" IEEE Conference on Computer Vision and Pattern Recognition Workshops 2013

[9] Shervin RahimzadehArashloo, Josef Kittler, William Christma. "An Anomaly Detection Approach to Face Spoofing Detection: A New Formulation and Evaluation Protocol" IEEE Access vol 5, 2017

[10] Andrea Lagorio, Massimo Tistarelli, MarinellaCadoni, Clinton Fookes, Sridha Sridharan. "Liveliness detection based on 3D face analysis", 978-1-4673-4989-5/13/ IEEE 2013

[11] Chenglin Yao, Shihe Wang, Jialu Zhang, Wentao He, Heshan Du, Jianfeng Ren, Ruibin Bai, and Jiang Liu. "rPPG-Based spoofing detection for face mask attack using efficient net on weighted spatial weighted spatial-temporal representation", IEEE Xplore 2021.

[12] Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face anti-spoofing based on color texture analysis," in IEEE International Conference on Image Processing (ICIP). Vol 6, IEEE, 2016.

[13] N. Erdogmus and S. Marcel, "Spoofing face recognition with 3D masks," IEEE Transactions on Information

[14] Forensics and Security (TIFS), vol. 9, no. 7, pp. 1084–1097, 2014.

[15] Y. Tang and L. Chen, "3D facial geometric attributes based anti-spoofing approach against mask attacks," in IEEE International Conference on Automatic Face Gesture Recognition (FG, pp. 589–595), 2017)

[16] Daniel Rodriguez, Jing Wang, Changzhi Li. "Spoofing Attacks to Radar Motion Sensors with Portable RF Devices"

[17] Article published on www.thejakartapost.com (ShuheiOkawara, 30, owner of mask shop KamenyaOmote, holds a super-realistic face mask based on his real face, made by using 3D printing technology, in Tokyo, Japan, on December 16, 2020.) (REUTERS/Issei Kato)

[18] Mr. LokeshM.Giripunje,Mr. Prasad Khajone,Mr.Yogesh Sudrik,Mr.Akash Range,"Review Paper on Automatic Vehicle Number Plate Detection and Recognition Using Image Processing", "International Journal of Advance Engineering and ResearchDevelopment, pp.673-677.

[19] O. De Vel,S.Aeberhard, "Line-based face recognition under varying pose", IEEE Transactions on Pattern Analysis and Machine Intelligence 1999

[20] Rajat Bhati, Shubham Saraff, Chhandak Bagchi, V. Vijayarajan, "Critical Decision Making Using Neural Networks", International Journal of Engineering & Technology 2018

[21] Azim Zaliha Abd Aziz, "Effects of Visible and Near Infrared Polarized Lights on Spoofing Face", Journal of Computer Science 2019

[22] LitongFeng,Lai-Man Po,YumingLi,Fang Yuan, "Face liveness detection using shearlet-based feature descriptors", Journal of Electronic Imaging 2016

[23] Yan Wang, Fudong Nian, TengLi,ZhijunMeng, Kongqiao Wang, "Robust face anti-spoofing with depth information", Journal of Visual Communication and Image Representation 2017

[24] Maneet Singh, Richa Singh,Arun Ross, "A comprehensive overview of biometric fusion", Information Fusion 2019

[25] Mikhail Artemyev, Marina Churikova, Mikhail Grinenko, Olga Perepelkina, "Robust algorithm for remote photoplethysmography in realistic conditions", Digital Signal Processing 2020

[26] Zinelabidine Boulkenafet, Jukka Komulainen, Abdenour Hadid, "Face Spoofing Detection Using Colour Texture Analysis", IEEE Transactions on Information Forensics and Security 2016