International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 5 Volume No.6 Aug-Sept – 2022
DOI:10.46647/ijetms.2022.v06i05.055 ISSN: 2581-4621

A systematic review on face spoofing detection methods

Anu Joseph[1], Gigi Joseph[2]
[1] *Assistant Professor, Kristu Jyoti College of Management and Technology*
[2] *Assistant Professor, Kristu Jyoti College of Management and Technology*

ABSTRACT
Face biometric researchers have had a lot of success over the past 62 years. Face recognition technology has been widely employed in both commercial and governmental applications, including mobile, banking, and surveillance systems. Though, the facial recognition system's ability to survive an uninvited attacker is a crucial issue. Face recognition software is susceptible to fake images and video attacks. Anti-spoofing solutions are useful in these situations for thwarting these attacks. The biometric community as a whole, including researchers, developers, and retailers, has spent the last ten years working on difficult projects to create a more precise defence against spoofing attacks. Despite numerous face anti-spoofing or liveness detection techniques being put out, the problem has not been addressed since it is challenging to identify the features and techniques for spoof assaults. This paper's objective is to present a thorough analysis of antispoofing techniques. The study came to the conclusion that in order to increase the system's security, computational efficiency, and dependability, it is necessary to provide more generalized methods for the detection of unanticipated spoofing assaults.
Keywords— face spoof, detection, machine learning

1. Introduction

Despite significant advancements in recent years, 2D face biometrics remains an important field of study. Face identification can be difficult due to a wide variety of views, occlusions, ageing of participants, and complicated outdoor illumination. Although there are many articles addressing these problems, face biometric systems' susceptibility to spoofing assaults is frequently disregarded. Face recognition, however, is frequently vulnerable to many kinds of attacks. Print and video/replay assaults are examples of presentation attacks. In a print attack, the attacker makes use of a legitimate user's photo that is displayed on a digital device or printed on paper. In a video/replay assault, the attacker mimics the normal human gestures of a real user who has been captured on camera. To detect spoof faces, a wide range of hardware and software techniques have been created. The liveness properties, such as textures, structural data, liveness sign, and image quality, are analysed by software-based approaches. All of these techniques are quite susceptible to environmental sounds, such as dim lighting. To get the result, extensive computation is required. The use of texture-based approaches makes use of the target's surface's ability to reflect light. A screen or plain paper will reflect light differently from human skin. The visual and tactile characteristics of the actual and fake faces differ, which is how spoof attack detection is done. While visual texture creates the perception of surface quality, tactile texture indicates how smooth or rough a surface is.

In this article, we explore six alternative face spoofing attack detection strategies. The article is divided into four sections: section 2, which covers the models chosen, the methodology employed, and an analysis of each model; section 3, which gives a summary of the whole study; and section 4, which wraps up the paper.

2. Face Spoof Attacks

The biometric system is deceived into accepting the attackers' fake identification in a spoofing attack, which is nothing more than a false acceptance. It is quite easy for the spoofing system to create such an assault due to how easily photographs and videos of the person may be found on social

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 5 Volume No.6 Aug-Sept – 2022
DOI:10.46647/ijetms.2022.v06i05.055 ISSN: 2581-4621

networking sites or recorded from a distance. An attacker can access the system by displaying pictures and recorded videos that they illegally got.

There are two methods for face spoofing: 2D spoofing and 3D spoofing. Both spoofings can be further subdivided into many types of attacks, such as picture attacks, video attacks, and 3D mask attacks, as shown in Fig. 2. Online social networking services have made images and movies widely accessible. Another option is to simply take videos with a mobile phone or other digital device. Today, 3D masks are widely available on the market. These assaults are all directed towards the face.

The term "photo attack" refers to a 2D spoof attack in which an attacker uses a photograph to access a system using a biometric method, such as the screen of a mobile phone, tablet, or laptop. This picture might have been downloaded from Facebook, Twitter, or Instagram or captured with a digital camera[8]. Photographic masks, the most advanced type of photo-attack, are created by morphing high-resolution prints of the lips and eyes. During the attack, the impostor is placed in the back so that certain facial expressions, including blinking eyes, can be replicated.

Video assaults are a more advanced version of photo assaults[9]. In this assault, the perpetrator uses a mobile phone, tablet, digital camera, etc. to film a video of the actual victim. The attacker then plays the video while facial recognition is in operation, gaining access to the biometric system because the face portion of the video moves naturally. These attacks are therefore harder to identify or prevent.[10-12]

The 3-D mask assault is a more advanced version of the video and photo attacks due to the depth components in the facial characteristics. It is more difficult to design a defence against spoofing in a 3D mask attack since the offenders make a 3D mask of the real person being impersonated. These attacks are less common than those in the other groups. 3D masks are typically made from materials including paper, polymers, silicon, and other things[13-14].

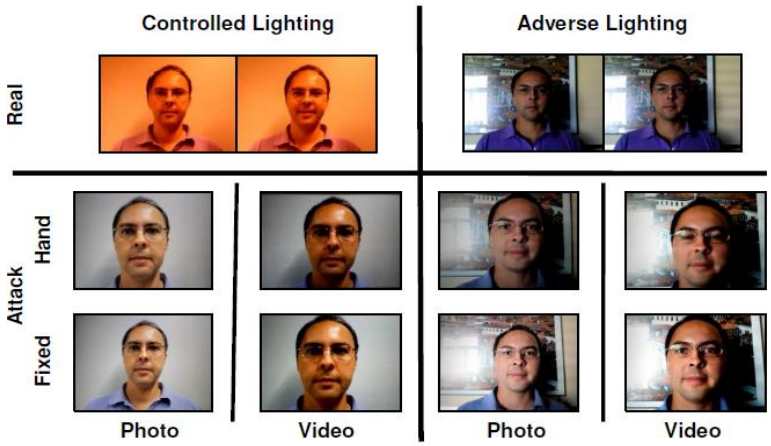

Figure 1. Few video frames from the Replay Attack database [4] illustrating photo (print) and video (replay) attacks.

3. Classification of antispoofing techniques

To detect spoof faces, a wide range of hardware and software techniques have been created. The liveness features, including textures, structure data, the liveness sign, and image quality, are analysed by software-based approaches. All of these techniques are quite susceptible to environmental sounds, such as dim lighting. To get the result, extensive computation is required. Antispoofing techniques for 2-D face recognition can be loosely categorised as motion, texture, and liveness based on the indicators employed for attack detection. Techniques for motion analysis make use of the fact that planar things move very differently from 3-D items like actual human faces.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 5 Volume No.6 Aug-Sept – 2022
DOI:10.46647/ijetms.2022.v06i05.055 ISSN: 2581-4621

Texture analysis approaches use observable texture patterns to identify threats, such as printing errors and general image blur. The use of texture-based approaches makes use of the target's surface's ability to reflect light. A screen or plain paper will reflect light differently from human skin. The visual and tactile characteristics of the actual and fake faces differ, which is how spoof attack detection is done. While visual texture creates the appearance of surface quality, tactile texture describes how smooth or rough a surface is. Local binary pattern (LBP), Fourier analysis, and Color Texture Analysis are the algorithms utilised for texture-based methodologies. This approach is more sensitive to background noises. The structural distinctions between 2-D plain surfaces and 3-D surfaces are captured by structure-based approaches. When light hits 3-D surfaces, it diffuses more gradually than it does on 2-D surfaces. Non-uniform light distribution on the 3-D surface is the cause of the diffusion delay. It takes longer to detect it. Attacks are categorised using liveness detection, which looks for life-signs like lip and eye movement. The users' cooperation is also necessary. When it comes to video/replay attacks, this kind of spoof detection is ineffective. The method of picture quality analysis finds the level of the image's quality that was employed for detection. These types of analytic techniques can pass higher resolution photos. Hardware-based approaches produce very accurate findings but are expensive since they require additional hardware like infrared cameras and several 2-D cameras.

4. Dataset

Various biometric databases were used for the investigation. The PRINT-ATTACK biometric (facial) database is one example of such a database. 200 films of actual accesses and 200 videos of attempted attacks by 50 distinct identities make up the database. Real access video sequences are recorded at a resolution of 320 by 240 pixels (QVGA), with a frame rate of 25 frames per second, and for a total of 15 seconds per sequence. These real-access films were captured under two different lighting and background settings. Attack attempts are recorded for up to nine seconds at the same resolution and frame rate with the same background and lighting. Attacks are recorded using hard copies of digital photos produced on standard A4 paper using a colour laser printer. Two separate support mechanisms are mounted in front of the acquisition system's input camera for attacks. The supports employed are fixed-support and hand-based, where the client's print is affixed to the wall and the attacker holds it in his hands.

Other datasets used for face spoof detection training and testing include bespoke datasets, the Replay Attack Database, the CASIA Face Antispoofing Database, and real and spoof photographs from the NUAA photographic imposter dataset.

Figure 1. Samples from NUAA dataset [8]

Figure 2. Samples from Custom dataset

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 5 Volume No.6 Aug-Sept – 2022
DOI:10.46647/ijetms.2022.v06i05.055 ISSN: 2581-4621

5. (Description of Models) Literature Review

A real-time liveness detection system for photo spoofing was presented by Gang Pan et al.[2] in 2006. This method can detect unintentional eye blinking. The only additional hardware needed for this strategy is a webcam. For eye blinking detection, Adaboost classifier and HMM approaches are utilised, which provides good accuracy with a 3 percent error.

Anjos et.al[3] proposed a method to verify faces by countermeasures based on texture and motion. Texture quality is analysed by using local binary patterns (LBP). Correlation analysis (Motion based) is used to calculate the correlations between the head movements and the background. The input video frames are divided into N frames window. Each frame is then analysed based on the motion and micro-texture. The local binary patterns (LBP) face description is computed only for the last frame based on the motion analysis of whole-time window. The classifier used is Linear Discriminant Analysis (LDA).

A texture feature algorithm using the Local Binary Pattern (LBP) technique was proposed by Ivana Chingovska et al.[7] Replay Attack Database, NUAA Photograph Imposter Database, Public Database, and CASIA Face Antispoofing Database were the four databases used for the experiments. During studies conducted on several databases, this LBP generating an error of around 16% of the total.

A 3D mask spoofing face recognition method by Nesli Erdogmus et al.[5]. To distinguish between a fake and real user using a biometric modality, the author used Modified Local Binary Pattern (MLBP), Linear Discriminant Analysis (LDA), and Support Vector Machine (SVM). The trials were carried out using the newly released 3D Mask databases and the Morpho database. The experiment showed a 3 percent error rate in line with the suggested strategy.

A visual dynamics strategy was proposed by Santosh Tirunagari et al. (2015)[4]. The author suggested a classification pipeline made up of the following: Support Vector Machine (SVM), Principal Component Analysis (PCA), Local Binary Pattern (LBP), and Dynamic Mode Decomposition (DMD). All of these categorization technique combinations produced findings that were more precise in identifying the spoofing assault. Three well-known databases that are freely accessible to the public—the Print Attack Database, Replay Attack Database, and CASIA-FASD Database—were used to illustrate this concept. The experiment shows a 9.55 percent error rate.

Techniques for fusing several descriptors were proposed by Shervin Rahimzadeh et al. (2015)[6]. A quick kernel discriminant analysis served as the foundation for our kernel fusion technique (KDA). A different publicly accessible database was used for the experiment. Multiscale, dynamic, binarized statistical picture characteristics were applied in this method. With an error rate of 1.67 percent, the authors tested the algorithm on the CASIA, Replay Attack, Cross, NUAA Photograph Imposter, and databases. In comparison to previous techniques, the results obtained show an advantage in identifying various spoof assaults.

Soft biometric methods based on neural networks and principal component analysis were described by Mihai Gavrilescu et al.(2015)[1]. The inventors of this video-based face recognition technology used the many expressions that people's faces made in various frames. The findings showed that this methodology has an error rate of 5.7%.

Related Works	Method/ Algorithm	Dataset	Domain Used	Error Rate (%)
Gang Pan et al.	Adaboost classifier and HMM	Public Database NUAA Photograph Imposter Database	Unintentional eye blinking	3%
Anjos et.al.	Local Binary Pattern (LBP) Linear Discriminant Analysis (LDA)	Public Database Print Attack Database	Texture quality Motion analysis	11%

DOI:10.46647/ijetms.2022.v06i05.055 ISSN: 2581-4621

Ivana Chingovska et al.	Local Binary Pattern (LBP)	Replay Attack Database NUAA Photograph Imposter Database Public Database CASIA Face Antispoofing Database	Texture quality	16%
Nesli Erdogmus et al.	Modified Local Binary Pattern (MLBP) Linear Discriminant Analysis (LDA) Support Vector Machine (SVM)	3D Mask database Morpho database	3D mask spoofing face recognition	3%
Santosh Tirunagari et al.	Support Vector Machine (SVM) Principal Component Analysis (PCA) Local Binary Pattern (LBP) Dynamic Mode Decomposition (DMD)	Print Attack Database Replay Attack Database CASIA-FASD Database	Visual dynamics	9.55%
Shervin Rahimzadeh et al.	Kernel Discriminant Analysis (KDA)	CASIA Replay Attack Cross NUAA Photograph Imposter databases	Multiscale, dynamic, binarized statistical picture characteristics	1.67%
Mihai Gavrilescu et al.	Neural Networks and Principal Component Analysis	Honda/UCSD Video Database Youtube Faces Database	Soft biometric methods (video-based face recognition technology)	5.7%

6. Conclusion

In terms of biometrics, the human face is the most accurate due to its distinctive feature. It has been applied on a massive scale to identify millions of real users. Recently, research has been conducted in the area of face spoofing, which presents a difficulty in face identification, as a result of the rising need for biometric technologies based on the human face. The academic community has focused increasingly on identifying false and real face samples in recent years. The suggested liveness and replay attack detection techniques, however, function on well-known spoof materials. Therefore, it is necessary to construct universal liveness algorithms for spoofing assaults that are unanticipated and undetected. To make the system more secure and computationally efficient for unforeseen and unanticipated spoof attacks, it is necessary to consider the vulnerability of features against spoofing attacks.

References

[1]Gavrilescu, Mihai. "Study on using individual differences in facial expressions for a face recognition system immune to spoofing attacks." IET Biometrics, vol. 5, no. 3, pp. 236-242, 2016.

DOI:10.46647/ijetms.2022.v06i05.055 ISSN: 2581-4621

[2]Pan, Gang, Lin Sun, Zhaohui Wu, and Shihong Lao. "Eyeblink-based anti-spoofing in face recognition from a generic web camera." In 11th IEEE International Conference on Computer Vision, pp. 1-8, 2007.
[3]Anjos, André, and Sébastien Marcel. "Counter-measures to photo attacks in face recognition: a public database and a baseline." In IEEE International Joint Conference on Biometrics (IJCB), pp. 1-7, 2011.
[4]Tirunagari, Santosh, Norman Poh, David Windridge, Alamo Iorliam, Nik Suki, and Anthony TS Ho. "Detection of face spoofing using visual dynamics." IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 762-777, 2015.
[5]Erdogmus, Nesli, and Sebastien Marcel. "Spoofing face recognition with 3D masks." IEEE Transactions on Information Forensics and Security, vol. 9, no. 7, pp. 1084-1097, 2014.
[6]Arashloo, Shervin Rahimzadeh, Josef Kittler, and William Christmas. "Face spoofing detection based on multiple descriptor fusion using multiscale dynamic binarized statistical image features." IEEE Transactions on Information Forensics and Security, vol. 10, no. 11, pp. 2396-2407, 2015.
[7]Chingovska, Ivana, André Anjos, and Sébastien Marcel. "On the effectiveness of local binary patterns in face anti-spoofing." In IEEE Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG), pp. 1-7, 2012.
[8] Yang, Jianwei, Zhen Lei, Dong Yi, and Stan Z. Li. "Person-specific face antispoofing with subject domain adaptation." IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 797-809, 2015.
[9] Pinto, Allan, William Robson Schwartz, Helio Pedrini, and Anderson de Rezende Rocha. "Using visual rhythms for detecting video-based facial spoof attacks." IEEE Transactions on Information Forensics and Security, vol 10, no. 5, pp. 1025-1038, 2015.
[10] Poh, Norman, Chi Ho Chan, Josef Kittler, Sébastien Marcel, Christopher Mc Cool, Enrique Argones Rúa, José Luis Alba Castro et al. "An evaluation of video-to-video face verification." IEEE Transactions on Information Forensics and Security, vol. 5, no. 4, pp 781-801, 2010.
[11] Evans, Nicholas, Stan Z. Li, Sebastien Marcel, and Arun Ross. "Guest editorial: Special issue on biometric spoofing and countermeasures." IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 699-702, 2015.
[12] Wen, Di, Hu Han, and Anil K. Jain. "Face spoof detection with image distortion analysis." IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 746-761, 2015.
[13] Galbally, Javier, and Riccardo Satta. "Three-dimensional and two-and-a half dimensional face recognition spoofing using three-dimensional printed models." IET Biometrics, vol. 5, no. 2, pp. 83-91, 2015.
[14] Pan, Gang, Lin Sun, Zhaohui Wu, and Shihong Lao. "Eyeblink-based anti-spoofing in face recognition from a generic web camera." In 11th IEEE International Conference on Computer Vision, pp. 1-8, 2007.