International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 04 | Apr 2022 www.irjet.net p-ISSN: 2395-0072

A Case Study on Face Spoof Detection

Aarohi Verma[1], Himanshu Awasthi[2], Ruchi Kumari[3], Shashank Pal[4], Megha Agarwal[5]

[1]*UG Student- SRM Institute of Science and Technology, Ghaziabad, India*

[2]*UG Student- SRM Institute of Science and Technology, Ghaziabad, India*

[3]*UG Student- SRM Institute of Science and Technology, Ghaziabad, India*

[4]*UG Student- SRM Institute of Science and Technology, Ghaziabad, India*

[5]*Asst. Professor, Dept. of Computer Science & Engg, SRM Institute of Science and Technology, Ghaziabad, India*

Abstract- *User authentication is a vital step in protecting information, and facial bio metrics might assist in this regard. Face bio metrics seems to be more natural, simple to use, and less intrusive to humans. Unfortunately, emerging research has revealed that face bio metrics are extremely sensitive to spoofing assaults. A spoofing attack occurs when a person tries to masquerade as someone else by falsifying data and thereby gaining illegitimate access. Inspired by image quality assessment, characterization of printing artifacts, and differences in light reflection, we propose to approach the problem of spoofing detection from texture analysis point of view. This report discusses many types of assaults against visual spectrum facial recognition systems. We propose comprehensive data sets for assessing the susceptibility of recognition systems and the effectiveness of countermeasures. Finally, we give a brief overview of anti-spoofing strategies for visual spectrum face identification, as well as a viewpoint on difficulties that remain unresolved.*

Key Words: **Biometrics; Facial Recognition; Facial Anti-Spoofing; Facial Presentation Attack Detection (PAD); RGB camera-based anti- spoofing methods; Computer Vision; Pattern Recognition**

1. INTRODUCTION

Biometrics is a multidisciplinary field concerned with measuring and mapping specific biological traits, such as fingerprints, faces, palm veins, and so on, in order to use them as an individualised recognition code[1].

Face recognition systems are utilised in many domains, such as pattern recognition, computer vision, and image processing, for various purposes.

Biometric traits are divided into two categories: physical traits and behavioural traits like signatures, voices, and keystrokes. Biometrics is critical for a wide range of technologies.

There has been widespread knowledge for a long time that face recognition systems have weak resistance to presentation attacks and are easily spoofed with photographs, videos, or 3D models of the enrolled person's face. The human eye is quite effective at detecting counterfeits, but this seems not to apply to face verification systems. Therefore, face recognition systems should be treated as a first priority before they are implemented unsupervised as a replacement for user credentials

Currently, biometric systems are being deployed in a variety of environments such as airports, laptops, and mobile phones, and the number of users is becoming more familiar with day-to-day life, so security is becoming increasingly important. As a result, this paper attempts to evaluate the various methods available in the various stages of this identification technique, as well as the various classification methods available. This technological advancement has allowed biometrics to be used in a wide range of applications, including forensics, access control, surveillance, and border security.

Recent advances in the field of facial biometrics have rekindled interest in liveness detection as a solution to spoofing attack problems. The goal of this paper is to review recent research efforts and map them into a cohesive taxonomy based on liveness indicators, as well as to provide a further classification on face anti spoofing techniques. Various components of a face recognition process are shown in Fig. 1 [2].

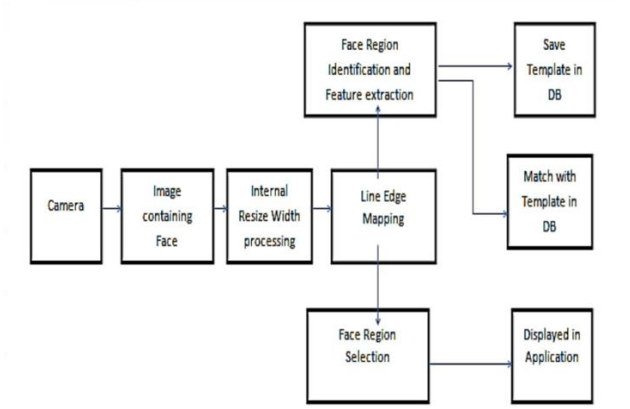

Fig 1: Components of Face Recognition System

2. ATTACKS TO FACE RECOGNITION SYSTEMS

There are two types of biometric system attacks: indirect and direct. [3] Figure 2 depicts a flow diagram of a typical biometric recognition system, with numbered points indicating potential attack points.

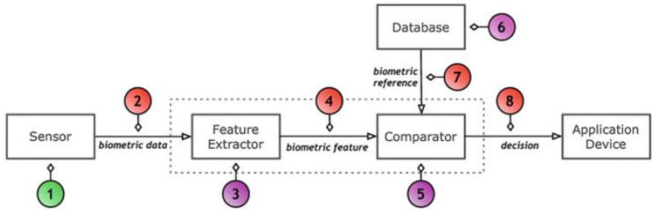

Fig. 2: Possible attack points in a generic biometric system

Indirect attacks are launched from within the recognition system, requiring intruders to first gain access to the system's internals. Once inside, indirect attackers can tamper with feature extractors or comparators, manipulate biometric references, or exploit potential flaws in communication channels. Indirect attacks can be mitigated by increasing the security of communication channels and restricting access to the internals of recognition systems so that cyber-criminals do not exploit them. Direct, presentation, or spoofing attacks are carried out at the sensor level [4] (shown as attack type 1 in Fig.2), which is beyond the biometric system manufacturer's control. In such cases, the attacker attempts to directly fool the sensor, and thus no physical protection mechanisms are available. In a direct attack, also known as a presentation attack, a person attempts to impersonate another person by falsifying their biometric characteristics in order to gain an unfair advantage. As input sensors for face recognition systems, standard image cameras are used. These devices can be used to record single or multiple photos or video sequences of users attempting to gain access to protected resources. Figure 3 depicts an ideal static configuration for a face authentication system. In these cases, the camera is embedded in a laptop that has been pre-programmed with a face recognition system.

Users position themselves so that the camera can capture their faces for as long as the system requires. The environmental conditions during data acquisition are an important consideration during the recognition process. It is a well-known fact that poor lighting conditions, pose, and ageing, among other factors, can significantly impair one's ability to recognise people[5].

In a more modern configuration, users may use a mobile phone to access protected resources on the phone itself, or as a terminal for other applications. Mobile devices can also be used to identify other people in forensics or surveillance applications. The environmental acquisition conditions in such cases can vary greatly[6].

Fig. 3. Example setup of a face recognition system

3. ATTACKS INVENTORY

In recent years, there have been numerous studies in the subject of spoofing detection systems. This section provides an overview of some of the techniques employed in this sector. The quantity of research articles, conferences, and journals with fresh ideas has substantially increased in the last ten years, promoting spoofing bio- metric security.

One of the early studies on face spoof detection, according to our knowledge, was published in 2004

by Li et al.[7] Face recognition for access control has grown in prominence in recent years, and this area has gotten a lot of attention from researchers in the last five years. The general classification of spoofing is shown in Figure 4, which can be divided into two categories: 2D[8] image spoofing and 3D image spoofing[9].

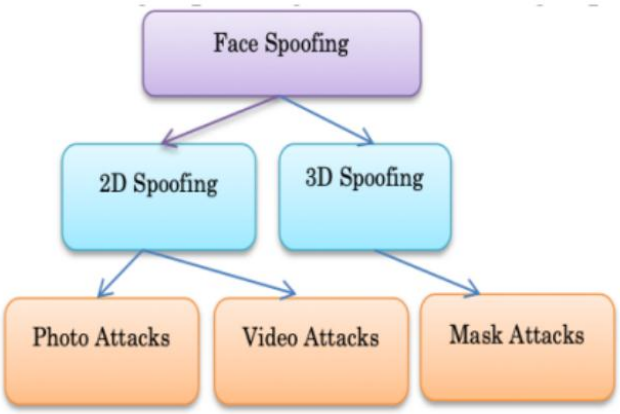

Fig 4: Types of Spoofing Attacks

3.1 Photo Attacks:

The primary premise of this form of fraudulent ac- cess attempt is to offer a recognition system with a photograph of a legitimate user. The photographs are taken from social networking sites or a digital camera by the attackers. The attacks might be on printed graphics on paper or images projected on a screen, such as a mobile phone or tablet. Photographic masks are a more advanced sort of attack in the photograph[10]. These are the masks made from high-quality photo-cut material. During attacks, an imposter is placed behind the attacker so that specific facial expressions, such as eye blinks, can be replicated.

3.2 Video Attacks:

Replay attacks are the name for these types of attacks. These are the more advanced spoofs of this shot. In this attack, instead of using still photos, the client's video from a digital device is utilised. In this attack, instead of using still photos, the client's video from a digital device is utilised. Some videos from mobile phones and computers are targeted, and they are more difficult to detect not just because to their texture, but also due to their dynamics[11].

3.3 Mask Attacks:

The client's face or a 3D[12] mask of the client's face is used as a spoofing artefact in this attack. It is quite difficult to develop a defence against such mask attacks. The face's 3D structure is hidden, and the face is mimicked here. Photo and video attacks can be mitigated with depth cues, whereas mask attacks require only mask attacks clues. Although the idea of fooling a biometric system by wearing a mask that imitates the face of another user has been floating around for a while.

Fig 5: Showing Photo Attack, Video Attack, and Mask Attack from Left to Right respectively.

4. Literature Survey

Kant et al. proposed a method that combined a camera and a thermal sensor. Both the camera and the thermal sensor capture the users for detection, and each frame is compared to a thermal image from the thermal sensor, which distinguishes the face skin from the 2-D surface. Using thermal face recognition, they achieved a 98 percent accuracy[13].

Jukka et al. proposed a method that involves passing the input image through a face detector and an upper body detector. After detecting the upper body, the image is subjected to a spoofing medium detector for further classification of real and spoof faces. They obtained an EER of 6.8 percent by combining the CASIA and NUAA datasets[14].

Face spoofing detection research has been going on for over many years. Since then, several methods for detecting face spoofing have been proposed, including print attacks, replay attacks, and 3D mask attacks. We provide a brief summary and analysis of published 2D face spoof detection methods because our focus is on 2D face spoof attack detection (on smartphones). The methods that have been published can be divided into six categories: (i) face motion analysis, (ii) face texture analysis, (iii) face 3D depth analysis, (iv) image quality analysis, (v) frequency domain analysis,

Face motion analysis-based spoofing detection methods extract behavioural characteristics of the face, such as eye blinks and lip or head movement. To localise the facial components, these methods require accurate face and landmark detection. In order to estimate the facial motions, multiple frames must be used. Because these methods are designed to detect print attacks, they cannot handle video replay attacks with facial motions.

Spoofing detection methods based on face texture analysis capture texture differences (due to different reflection properties of the live face and spoof material) between face images captured from live faces and face images captured from different spoof mediums (e.g., paper and digital screen). These methods can detect spoofs based on a single face image and thus have a relatively quick response time. However, when using small training sets with a limited number of subjects and spoofing scenarios, face texture analysis-based methods may have poor generalizability.

Spoofing detection methods based on 3D depth analysis estimate a face's 3D depth to distinguish between a 3D live face and a 2D spoof face. Spoof faces presented on a 2D planar medium are 2D, whereas live faces are 3D objects. As a result, if the 3D depth information of a face can be reliably estimated, these methods can be quite effective in identifying 2D face spoof attacks. Face 3D depth analysis methods typically rely on multiple frames to estimate a face's depth or 3D shape information.

Image quality differences between live and spoof face images are used by spoofing detection methods based on image quality analysis. Because spoof face images and videos are created by recapturing live face images and videos in photographs or on screens, there will be colour, reflection, and blurriness degradations in the spoof face images compared to the live face images and videos. These methods have been found to be very generalizable to a variety of scenarios. However, research on face spoofing detection using image quality analysis is limited.

Anti-spoofing methods based on frequency domain analyse noise signals in captured video to distinguish between live and spoof face access. There is a decrease in low frequency components and an increase in high frequency components during the recapture of printed photos or video replays.

While many of the published methods in the five categories listed above produce positive results for intra-database testing, their effectiveness in cross-database testing scenarios has not been thoroughly evaluated. The few publications that did conduct cross-database testing have generally reported poor results. Consider fusion of multiple physiological or behavioural cues to improve the robustness of face spoof detection methods in cross-database testing scenarios.

5. SPOOFING DATASETS

5.1 NUAA Photo Imposter Database

The database was created using an unspecified generic webcam that recorded photo attacks and real accesses to 15 different identities[15]. As shown in Fig. 6, the database is divided into three sessions with varying lighting conditions. Because not all subjects participated in the three acquisition campaigns, the amount of data collected across sessions is unbalanced. Participants in all sessions were asked to look frontally at the web camera, maintaining a neutral expression and avoiding eye blinks or head movements as much as possible. The webcam would then record for approximately 25 seconds at 20 frames per second, from which a set of frames would be hand-picked for the database. The database does not include the original video sequence.

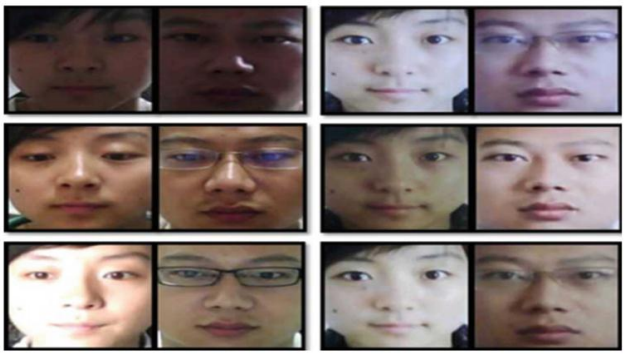

Fig.6 Samples from the NUAA Photo Imposter Database

5.2 The Replay-Attack Database Family

The Replay-Attack Database and its subsets (the Print-Attack Database[16] and the Photo-Attack Database[17]) are face anti-spoofing databases made up of short video recordings (about 10 seconds) of both real access and spoofing attacks on a face recognition system. This was the first database designed to aid in the research of motion-based anti-spoofing techniques. This database was used in the Competition on Countermeasures to 2D Facial Spoofing Attacks in 2011 and 2013.

Samples were taken from 50 different people. The entire database contains spoofing attempts from three major categories of the most obvious attacks on face recognition systems:

- Print attacks: attacks with photographs printed on a paper
- Photo attacks: digital photographs displayed on a screen of an electronic device
- Video attacks: video clips replayed on a screen of an electronic device

5.3 The CASIA Face Anti-spoofing Database

The CASIA Face Anti-spoofing Database (CASIA-FASD) introduces face attacks of varying imaging quality. It is a database that, like the NUAA Photo, treats spoofing detection as a binary classification task. In contrast to the latter, this database contains video files that can be used to experiment with texture, motion, or fusion techniques for anti-spoofing[16].

The CASIA-FASD data can be used in seven different anti-spoofing protocols, which are divided into two subsets for training and testing spoofing classifiers. There is no development set available for fine-tuning countermeasures. In total, 12 videos of about 10 seconds each are available for each identity: three real accesses, three warped photo attacks, three cut photo attacks, and three video attacks produced using each of the previously described devices with variable quality.

6. METHODS

Without ant spoofing measures, most cutting-edge facial biometric systems are vulnerable to attacks, because they try to maximise identity discrimination rather than determining whether the presented trait originates from a living legitimate client. Due to the pressing need to improve the security and robustness of face biometrics, a number of spoofing detection schemes have been proposed to address the problem of presentation attacks.

6.1 Liveness Detection

A common anti-spoofing countermeasure is liveness detection, which detects physiological signs of life such as eye blinking, facial expression changes, and mouth movements. To provide more evidence of life, Eulerian motion magnification[18] was used to enhance subtle changes in the face region[19] that would otherwise go unnoticed without a closer inspection. Within the context of the second competition on 2D facial spoofing countermeasures. However, the algorithm needs to be improved in order to perform better in more difficult and adversarial acquisition conditions.

6.2 Motion Analysis

Other motion cues can be used for face ant spoofing in addition to the facial motion used in liveness detection. It can be assumed, for example, that the movement of planar objects, such as video displays and photographs, differs significantly from that of real human faces, which are complex nonrigid 3D objects. If a face spoof is not tightly cropped around the targeted face or has an incorporated background scene, scenic fake face, stationary face recognition systems should be able to observe a high correlation between the overall motion of the face and the background regions. However, while being recognised, it can become confused between a fixed support photo-attack and a motionless person.

6.3 Contextual Information

Face images captured from face spoofs may visually resemble images captured from live faces; thus, detecting face spoofing is difficult based on a single face image or a relatively short video sequence. Depending on the imaging and fake face quality, it is nearly impossible for humans like us to tell the difference between a genuine and a fake face without any scene information or unnatural motion or facial texture patterns. However, we can immediately detect anything suspicious in the view, such as someone holding a video display or a photograph in front of the camera. Contextual information is a very important visual cue for face spoofing detection, according to the

experiments conducted by the CASIA Face Anti-spoofing Database and the NUAA Photograph Impostor Database.

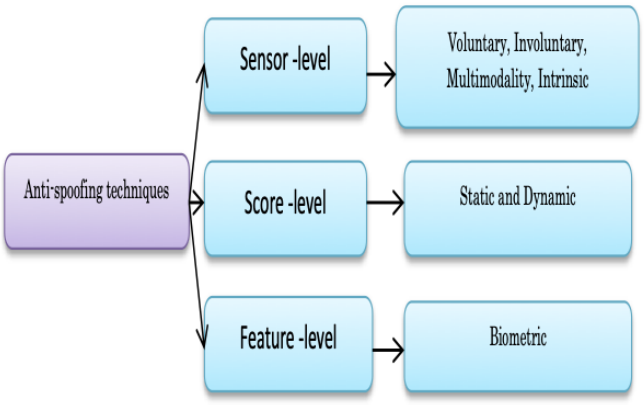

Figure 7: Various Anti-spoofing techniques

7. EVALUATION PARAMETERS (LIVENESS DETECTION)

FRR (False Rejection Rate), FAR (False Acceptance Rate, number of zero-effort impostor access attempts wrongly accepted), and SFAR are the three most commonly used metrics for evaluating liveness detection metrics (Spoofing False Acceptance Rate, corresponding to the number of spoofing attacks wrongly accepted). The true threat posed by a spoofing database to a specific recognition system can thus be determined.

8. CONCLUSION

Spoofing (i.e., direct) attacks are among the tangible threats and vulnerabilities that current face recognition systems face. Spoofing a face recognition system is possible by presenting a photograph, a video, or a three-dimensional shaped mask of a targeted identity to the input camera. This research problem has recently received increased attention (i.e., face spoofing attacks). This is evidenced by the increasing number of articles and competitions that have begun to appear in major biometric forums. In this chapter, we revealed the threats of face spoofing, presented the evolution of the available databases and protocols for evaluating face spoofing and anti spoofing based on visual information, and thoroughly discussed the various approaches proposed in the literature thus far.

Most cutting-edge facial biometric systems are vulnerable to spoofing attacks in the absence of spoofing countermeasures, because they strive to maximise discriminability between identities regardless of whether the presented trait originates from a living legitimate client or not. The proposed anti spoofing methods in the literature have shown very promising results on individual databases, but they may lack generalisation to the varying nature of spoofing attacks encountered in real-world applications. This implies that a network of attack-specific spoofing detectors may be required to combat various spoofing attacks. The existing databases for spoofing and anti-spoofing analysis have been and continue to be useful for studying spoofing problems, but it is impossible to anticipate and cover all possible attack scenarios in databases.

9. REFERENCES

1. Bledsoe, W. W. The model method in facial recognition, Panoramic Research Inc., Palo Alto. CA, Technical Report, Technical Report PRI: 15, 1964.
2. Dhawanpatil, T., & Joglekar, B. , “Face Spoofing Detection using Multiscale Local Binary Pattern Approach”, IEEE, International Conference on Computing, Communication, Control and Automation, 2017, pp. 1-5.
3. Ratha, N.K., Connell, J.H., Bolle, R.M.: An analysis of minutiae matching strength. In: Proceedings of the International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA), pp. 223–228. Springer-Verlag (2001).
4. Jain,A.K.,Flynn,P.,Ross,A.A.(eds.):HandbookofBiometrics.Springer-Verlag(2008).
5. Li,S.Z.,Jain,A.K.(eds.):Hand book of Face Recognition. Springer-Verlag(2011).
6. McCool C, Marcel S, Hadid,A., Pietikainen,M., MatejkaP, Cernocky, J Poh N,Kittler J, Larcher, A., Levy, C., Matrouf, D., Bonastre, J.F. Tresadern, P Cootes T: Bi-modal person recognition on a mobile phone: using mobile phone data. In: IEEE ICME Workshop on Hot Topics in Mobile Multimedia (2012).
7. Li, Jiangwei, Yunhong Wang, Tieniu Tan, and Anil K. Jain. "Live face detection based on the analysis of fourier spectra." In Biometric Technology for Human Identification, vol. 5404, pp. 296-304. International Society for Optics and Photonics, 2004.
8. de Freitas Pereira, Tiago, André Anjos, José Mario De Martino, and Sébastien Marcel. "LBP–

TOP based countermeasure against face spoofing attacks." In Asian Conference on Computer Vision, pp. 121-132. Springer, Berlin, Heidelberg, 2012.

9. Wang, Tao, Jianwei Yang, Zhen Lei, Shengcai Liao, and Stan Z. Li. "Face liveness detection using 3D structure recovered from a single camera." In Biometrics (ICB), 2013 International Conference on, pp. 1-6. IEEE, 2013.
10. Ghorpade, Shruti, Dhanashri Gund, Swapnada Kadam, and Mr RA Jamadar. "Image Quality Assessment for Fake Biometric Detection: Application to Face and Fingerprint Recognition." International Journal of Emerging Technologies and Engineering (IJETE) Volume 2.
11. Galbally, Javier, Sébastien Marcel, and Julian Fierrez. "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition." IEEE transactions on image processing 23, no. 2 (2014): 710-724.
12. Wang, Tao, Jianwei Yang, Zhen Lei, Shengcai Liao, and Stan Z. Li. "Face liveness detection using 3D structure recovered from a single camera." In Biometrics (ICB), 2013 International Conference on, pp. 1-6. IEEE, 2013.
13. Kant C and Sharma N 2013 Fake face recognition using fusion of thermal image and skin elasticity International Journal for Computer Science and Information Security
14. Komulainen J, Hadid A and Pietikainen M 2013 Context based face anti-spoofing 6th International Conference on Biometrics: Theory, Applications and Systems (BTAS)
15. X. Tan, Y. Li, J. Liu, L. Jiang, Face liveness detection from a single image with sparse low rank bilinear discriminative model, in *Proceedings of the European Conference on Computer Vision (ECCV)*, LNCS, vol. 6316, Heraklion, Crete, Greece, (Springer, 2010), pp. 504–517
16. A. Anjos, M.M. Chakka and S. Marcel, *Motion-based counter-measures to photo attacks in face recognition* IET Biometrics, **3**(3), 147–158 (2014)
17. M.M. Chakka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia, M. Ristri, F. Roli, J. Yan, D. Yi, Z. Lei, Z. Zhang, S.Z. Li, W.R. Schwartz, A. Rocha, H. Pedrini, J. Lorenzo-Navarro, M. Castrillon-Santana, J. Maatta, A. Hadid, M. Pietikainen, Competition on countermeasures to 2-D facial spoofing attacks, in *International Joint Confer- ence on Biometrics (IJCB)*, Washington, DC., USA, 2011
18. Wu, H.Y., Rubinstein, M., Shih, E., Guttag, J., Durand, F., Freeman, W.T.: Eulerian video magnification for revealing subtle changes in the world. ACM Trans. Graph. (SIGGRAPH 2012) 31(4) (2012).
19. Chingovska,I.,Anjos,A.,Marcel,S.:Anti-spoofinginaction:jointoperationwithaverificati on system. In: Proceedings of IEEE Conference on Computer Vision and Pattern Recognition, Workshop on Biometrics (2013).