International Journal of Pure and Applied Mathematics
Volume 117 No. 22 2017, 205-208
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

A Study on Spoofing Face Detection System

P. Kavitha [1], K.Vijaya [2]

[1]*Associate professor, Department of Computer Science and Engineering, R.M.K. Engineering College, Kavaraipettai*
[2]*Professor & Head, Department of Information & Technology, R.M.K Engineering College, KavaraipettaiIndia*
Email: pkavithaid@gmail.com

Abstract-As there are many biometric modalities deployed for the security in the recent years .the face recognition and the voice recognition has great attention among the researchers. Iris, signature passwords and normal fingerprints are used for the security in many applications .these biometric identifiers have its own advantages and disadvantages. Critical issue addressed in the face recognition system is that they are attacker by different attacks like photos and videos. This paper details the different techniques available for detecting the spoofing in face recognition system. This paper also describes the database which is used by different researcher. The parameters used for evaluating the method is discussed at the end of the paper .This paper gives an idea to provide a comprehensive overview on the work that has been carried over the last decades in the emerging field of anti -spoofing.

Keywords- Spoof attack, face recognition system, Biometric system, Attacks.

I. INTRODUCTION

There is a famous quote "Fingerprints cannot lie ,but liars can make fingerprints which has been proven right in many occasions .Not only the finger prints but also there are many biometric traits like face ,iris, voice which are unique in the recognition systems.[1] ace recognition. The research in the face recognition is being carried out from past 40 years and still there are many novel approaches are booming in the research day by day. There is no need for identity card or a password, you are your own key with face recognition system. There are many fields like pattern recognition, computer vision and image processing in which face recognition systems are partially used in different purposes. Though there is a very fast growth in the face recognition system, There is a vulnerabilities to face spoof attacks which creates a major impact in the systems. Recent study reported in [2] suggests that the success rate of face spoof attacks could be up to 70%, even when a state-of-the-art Commercial Off-The-Shelf (COTS) face recognition system is used. However the recognition of Face spoofing is still a challenging problem due to the difficulties in finding the discriminative and computationally inexpensive features. The methods that are already published have the limitation that the system needs to have the whole image or the video which consumes the memory and computational time. It is very important to develop a robust and an efficient method which can detect the spoofing in a well generalised manner with specific imaging conditions. Attacks are not restricted to some theoretical form but it is also may in the form of operational applications. The best example of this is the apple iPhone S5 fingerprint reader, just a day after it hit the shelves and using a regular and well known type of finger spoof is the only example of practical attack which is used in the real time with image processing. Currently the deployment of biometric systems keeps growing year after year in such different environments like airports, laptops and mobile phones and the number of users are becoming very familiar with day to day life so the security plays a very important role Hence this paper tries to evaluate the different methods available in the different stages of this identification technique and the various classification methods available. This path of technological evolution has permitted the use of biometrics in many diverse activities such as forensics, access control, surveillance and border security issues. The section 2 briefs the literate that deals with the different authors view in this spoofing and anti-spoofing techniques. Section 3details the face spoofing detection methods and next section is the biometric spoofing method followed by the metrics used for evaluation.

II. CLASSIFICATION OF SPOOFING

There are many researches going on in this field of spoofing detection system in the recent years .This sections briefs some of the methods used in this field. The spoofing biometric security has been promoted in the last 10 years significantly by number of research articles, conferences and the journals with innovative ideas[4,5].To our knowledge, one of the earliest studies on face spoof detection was reported in 2004 by Li et al. [3]. With the growing popularity of using face recognition for access control, this topic has attracted significant attention over the past five years among the researchers. Figure 1 represents the General classification of spoofing which can be broadly divided into two categories as 2D image spoofing[6] and 3D image spoofing[7].

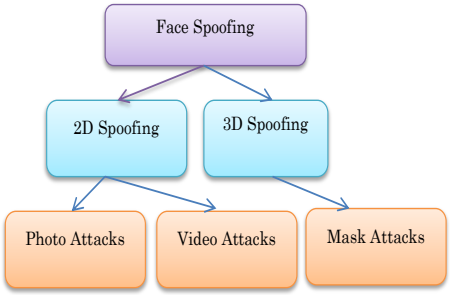

Figure1: general Classification of Spoofing

Photo Attacks: This type of fraudulent access attempts are basically of presenting a recognition system with a photograph of a genuine user. Attackers take the photos from the social media networks, or from the digital camera. The attacks may be on the printed images on the paper or the image displayed in the screen like mobile or tablet. Advanced type of attack in the photograph is the photographic masks.[8] These are the mask with high cut from the

photograph. Imposter is placed behind at the time of attacks, so that certain face expressions like eye blink can be reproduced.

Video Attacks: these attacks are referred as the replay attacks. These are the sophisticated version of this photo spoofs. Still images are not used in this attacks the video of the client from the digital device is used. Still images are not used in this attacks the video of the client from the digital device is used. Some of the videos from the mobile and the laptops are attacked which are more difficult to detect as not only because of its texture, but also because of its dynamics[9].

Mask Attacks: In this attack spoofing artefact is the face of the client or the 3D mask of the face.it is very difficult to have the counter measure against such mask attacks. 3D[10] structure of the face is masked and the face is imitated here. Depth cues can be used against photo and video attacks but mask attacks cues are in sufficient. Although the possibility to by pass a biometric system wearing a mask imitating the face of a different user is an idea that has been circulating for some time. Figure 2 shows the three types of the attacks.

Figure2: Samples for various spoofing

III. FACE SPOOF DETECTION METHODS

According to different types of cues used in face spoof detection, published methods can be categorized into four groups: (i) motion based methods, (iii)texture based methods, (iii) method based on image quality analysis, and (iv) methods based on other cues.

Motion based methods: These methods, designed primarily to counter printed photo attacks, capture a very important cue for vitality: the subconscious motion of organs and muscles in a live face, such as eye blink [4], mouth movement [5] and head rotation [8]. Given that motion is a relative feature across video frames, these methods are expected to have better generalization ability than the texture based methods that will be discussed below. However, the limitations of motion based methods are apparent. Additionally, motion based methods can be easily circumvented or confused by other motions, e.g. background motion, that are irrelevant to facial liveness or replayed motion in the video attacks.

(ii) **Texture based methods:** To counter both the printed photo and replayed video attacks, texture based methods were proposed to extract image artifacts in spoof face images. In[18], the authors argued that texture features (like LBP, DoG, or HOG) are capable of differentiating artifacts in spoof faces from the genuine faces. Texture based methods have achieved significant success on the Idiap and CASIA databases.

(iii) Methods based on image quality analysis: A recent work [9] proposed a biometric liveness detection method for iris, fingerprint and face images using 25 image quality measures, including 21 full-reference measures and 4 non reference measures. Compared to [9], other works are different in the following aspects: (1) While 25 features are required in [9] to get good results, no face-specific information has been considered in designing informative features for face spoof detection.

(iv)Methods based on other cues: Face spoof countermeasures using cues derived from sources other than 2D intensity image, such as 3D depth [10], IR image [6], spoofing context [11], and voice [12] have also been proposed. However, these methods impose extra requirements on the user or the face recognition system, and hence have a narrower application range. For example, an IR sensor was required in [6], a microphone and a speech analyzer were required in [12], and multiple face images taken from different viewpoints were required in [10]. Additionally, the spoofing context method proposed in [11] can be circumvented by concealing the spoofing medium. Some of the spoof detection methods are described in this section. Next section briefs some of the ant spoofing methods used in the literature.

IV. BIOMETRIC ANTI SPOOFING

In spite of some on-going efforts and proposals to reach a unified and standardized nomenclature for vulnerability related concepts, the biometric community has still not reached a general agreement on the best terminology to be used in each case [12], [13], [14]. Compared to algorithm-based evaluations, system-based ones provide a better estimation of the anti-spoofing capabilities of fully functional biometric systems, and not just of live ness detection algorithms. Such type of assessment also gives very valuable information regarding the real robustness against spoofing of commercial biometric applications which, in practice, are released as a complete finalized product and not as a group of independent modules. Furthermore, system based evaluations represent a closer approximation to spoofing attacks that could be carried out in a real-world scenario. Another important observation worth highlighting in the field of anti-spoofing assessment, is the distribution of fake samples across datasets. Up to date, in all algorithm-based competitions that have been organized (two in face, three in fingerprint and one in iris), the train and test sets distributed to the participants contained the same type of spoofs. This means that algorithms may be trained on the same type of data that will later be used for testing

V.SPOOFING DATABASE

Currently there are six large public face anti-spoofing databases that comprise most attacking scenarios described as the NUAA PI DB, the YALE-RECAPTURED DB, the PRINT-ATTACK DB, the CASIA FAS DB, the REPLAY-ATTACK DB and the 3D MASK-ATTACK DB. The first effort to generate a large public face anti-spoofng DB was reported in early days with the NUAA PI DB, which contains still-images of real access attempts and print-attacks of 15 users. The YALE RECAPTURED DB appeared soon after, and added the difficulty of varying illumination conditions as well as considering LCD spoofs. The PRINT-ATTACK DB represents yet another step in the evolution of face spoofing, both in terms of size (50 different users were captured) and of data acquired (it contains video sequences instead of still images). However, it still only considers the case of photo attacks. REPLAY-ATTACK DB was acquired with one single sensor using different attack devices of increasing quality under varying illumination and background conditions, while the CASIA FAS DB was captured with sensors of different quality under a uniform acquisition setting. From the six previous databases, the REPLAY-ATTACK DB is probably the most significant one, not only for its size, multiple and well defined protocols and attacks covered, but also because it was used in the last edition of the Competition on Countermeasures to 2D Facial Spoofing Attacks held in 2013 [15]. Figure 4 shows the different set of image from the database and the spoofed face with different attacks.

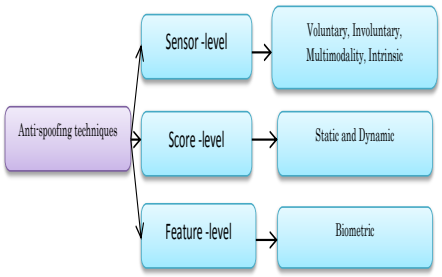

Figure 3: Various Anti-spoofing techniques

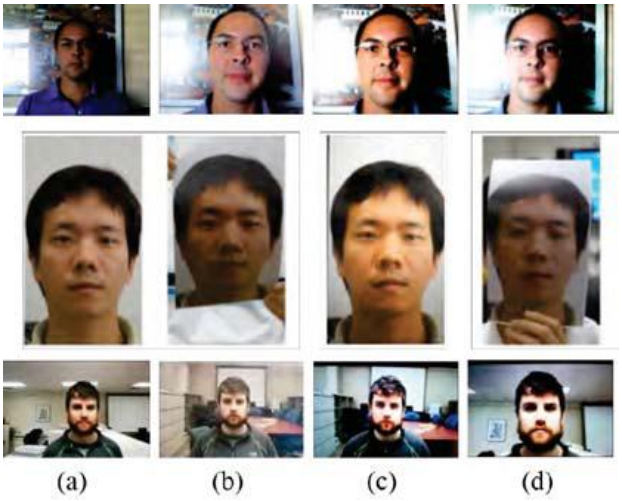

Figure 4; Sample face from data base(a) Genuine face images; (b) Spoof faces generated for printed photo attack; (c) Spoof faces generated by HD tablet screen; (d) Spoof faces generated by mobile phone screen (first and third row) or cut photo (second row).

VI.LIVENESS DETECTION –EVALUATION PARAMETERS

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

VII. CONCLUSION

The anti-spoofing community should also consider engaging in new fundamental research regarding the biological dimension of biometric traits, in order to break with the current popular trend embraced by many of the latest research where some well-known sets of features (e.g, LBP, LPQ,HOG or BSIF) are extracted from images in public databases and passed through a classifier. Classification plays again a vital role in recognition, in future some of the optimization techniques can be used for [13] enhancing the performance of the system.Hence this paper is restricted with the content of database and some of the spoofing methods .

IX. 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. Wen, Di, Hu Han, and Anil K. Jain. "Face spoof detection with image distortion analysis." IEEE Transactions on Information Forensics and Security 10, no. 4 (2015): 746-761.
3. 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.
4. Okereafor, Kenneth, and Clement Onime. "Enhancing Biometric Liveness Detection Using Trait Randomization Technique."
5. Galbally, Javier, Sébastien Marcel, and Julian Fierrez. "Biometric antispoofing methods: A survey in face recognition." *IEEE Access* 2 (2014): 1530-1552.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. Komulainen, Jukka, Abdenour Hadid, and Matti Pietikainen. "Context based face anti-spoofing." In *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on*, pp. 1-8. IEEE, 2013.
12. Chetty, Girija. "Biometric liveness checking using multimodal fuzzy fusion." In *Fuzzy Systems (FUZZ), 2010 IEEE International Conference on*, pp. 1-8. IEEE, 2010.
13. Sujatha, K., and D. Shalini Punithavathani. "Optimized ensemble decision-based multi-focus imagefusion using binary genetic Grey-Wolf optimizer in camera sensor networks." *Multimedia Tools and Applications* (2017): 1-25.
14. Johnson, Peter, Richard Lazarick, Emanuela Marasco, Elaine Newton, Arun Ross, and Stephanie Schuckers. "Biometric liveness detection: Framework and metrics." In *International biometric performance conference*, vol. 1. 2012.
15. Lazarick, R. "'Spoofs, subversion and suspicion: Terms and concepts." In *Proc. NIST Int. Biometric Perform. Conf.(IBPC)*. 2012.
16. Chingovska, Ivana, Jinwei Yang, Zhen Lei, Dong Yi, Stan Z. Li, Olga Kahm, Christian Glaser et al. "The 2nd competition on counter measures to 2D face spoofing attacks." In *Biometrics (ICB), 2013 International Conference on*, pp. 1-6. IEEE, 2013.