Available online at www.worldscientificnews.com

World Scientific News

An International Scientific Journal

WSN 41 (2016) 92-98 EISSN 2392-2192

Anti-Spoofing Method: A Survey on Biometric Face Recognition

M. Saranya*, P. Amudha

Department of Computer Science and Engineering, Avinashilingam Institute for Home Science and Higher Education for Women Faculty of Engineering, Coimbatore, India

*E-mail address: saran.mvk93@gmail.com

ABSTRACT

In recent decades, the evolution of biometric technology from the first revolutionary works in faces and voice recognition to the current state of development such as fingerprint, face, or iris, signature or hand. This path of technological growth has naturally led to a dangerous issue that has started emerging in recent years. The conflict of this rapidly emerging technology to external attacks and, in specific, to spoofing. Spoofing, referred by the term attack in modern standards. It refers that it has ability to fool a biometric system by means of giving forged version of original biometric system into the sensor where illegitimate user acts as an genuine user. The entire biometric community, including researchers and developers has put themselves into the challenging task of proposing and developing efficient protection methods. The main objective of this paper is to provide a broad overview on anti-spoofing, with special attention to face modality.

Keywords: Biometric, face spoofing, security, anti-spoofing

1. INTRODUCTION

An anti-spoofing method is automatically distinguish between real biometric trait in sensor and the falsely produced artifacts in biometric system. It is also worth noticing that certain anti-spoofing techniques may also be extremely effective to detect many other types of

(Received 01 February 2016; Accepted 10 February 2016; Date of Publication 11 February 2016)

presentation attacks. The work covers methodologies, state-of-the-art techniques, and also aims at providing an outlook of research development. The rest of the paper is structured as follows. In Sect. II some general anti-spoofing concepts are summarized. In Sect. III the person who reads can find a comprehensive survey of the different research works in face anti-spoofing. To conclude, the summary and discussion are given in Sect. IV.

2. METHODOLOGIES

In general perspective the anti-spoofing is classified into three methods. That depends upon the biometric system module. They are sensor level, feature level, score level.

- **Sensor Level methodology**: In general, sensor level methodology is hardware-based approach. It measures one of three characteristics, namely: (i) intrinsic properties of a living body, including physical properties, electrical properties, spectral properties or visual properties (e.g., colour and opacity); (ii) involuntary signals of a human body which can be recognized to the nervous system (e.g., pulse, blood pressure) (iii) response to external stimuli, also identified as challenge-response methods, which require the user support as they are based on detecting voluntary or involuntary responses to an external signal.
- **Featured Level methodology:** In general, featured level methodology is software-based approach. In this the standard sensor will sense the sample and detect the fake trait. As such, the biometric system will distinguish between the original and fake system (e.g., images, speech, face etc.,) not directly from the human body, in the case of sensor-level techniques. It is classified into two methods namely; static and dynamic anti-spoofing. It depends on whether they work with only one instance or with a sequence of samples in biometric trait. In common, static features are preferred more over dynamic method. This sub-division method is predominantly used in face recognition system, where the system works on single image (e.g., passport picture) or video sequence (e.g., surveillance camera).

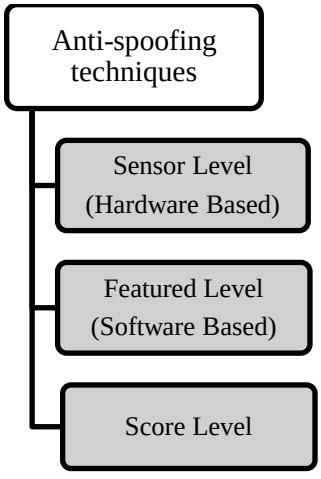

Figure 1. General classification of Anti-Spoofing techniques

- **Score Level methodology:** In general, score level method is a combination of both software and hardware. It has been started analyzing in the field of finger anti-spoofing. This protection method, much less common than the previous two categories. Due to their partial performance, they are designed as complementary measures to the sensor-level and feature-level techniques presented above, and are usually integrated in the matcher(as shown in Fig. 1)

3. STATE-OF-THE-ART TECHNIQUES

A concise summary of the most general face spoofing techniques is presented. This initial short overview on spoofing can be helpful to understand spoofing techniques.

A. FACE SPOOFING

This generation, probably the most current version of this tradition to change one self's physical appearance, is the using plastic surgery, which is becoming more popular ,gratitude to the availability of advanced technology, with affordable cost and high speed. In recent times, it has been a challenge for automatic face authentication trait to recognize a person after some face surgery. Even without turning to permanent treatments, some works have also exposed that face-based biometric systems may be circumvented just by wearing regular make-up .The general classification of face spoofing are categorized into three types namely; photo attack, mask attack, video attack.

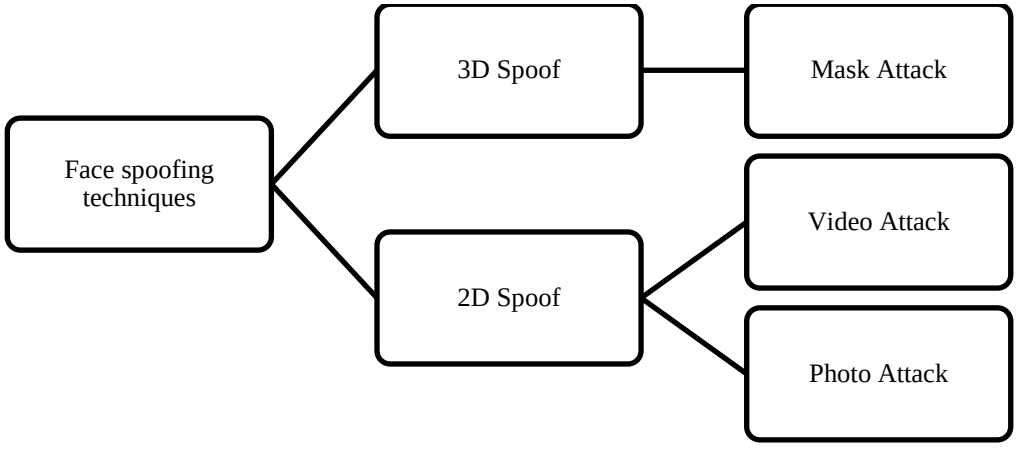

Figure 2. General classification of Face Spoofing techniques

B. FACE ANTI-SPOOFING

Though the initial face anti-spoofing works date back more than a decade it has not been until the last few years. Many countries have focused on this spoofing attack to biometric trait where Europe created revolution in doing projects. Among the entire important factor for the development of new protection methods against many attacks. The acquisition and distribution of several public face spoofing databases that have made possible for researchers to focus on

the design of efficient countermeasures and not on data acquisition issues considered to be the most efficient method. The both factors have fostered the recent publication of multiple techniques in 2D face anti-spoofing and to initiate a promising research line in new protection algorithms for 3D face recognition systems against mask attacks.

C. FACE RECOGNITION

Face recognition is one of the types of biometric software application. That can recognize a specific person in a digital image by analyzing and comparing the patterns it with the database. This recognition system is mainly used for security purposes in many fields. Here it summarizes the survey on face recognition system.

Sooyeon Kim *et al.,* [1] proposed a new method to secure face identification systems from fake 2D photos. The key factor that is utilized are, camera functioning, variable focusing. In shape-from-focus, by using focus measures, it is possible to construct 3D images. In order to calculate the existence of depth information, used the characteristic of defocusing method, even though need not recover the 3D depth images. The parts of image that are not in focus become blurry, by adjusting the focusing parameters. With this function, can estimate differences in the degree of focus between original faces and fake faces. Then use this information to detect face liveness. To evaluate this method, controlled two databases using a handheld digital camera and a webcam which results in optimized detection of liveliness of faces with presence of various noises.

Javier Galbally and Riccardo Satta [2] provide a comprehensive study on the likelihood to spoof 2.5D and 3D face recognition systems with minimum-cost self-manufactured models. Models have been produced by taking advantage of the newly available and inexpensive off-the-shelf 3D sensing, processing technology and printing technology. It reports a systematic and rigorous evaluation of the real risk posed by a newly acquired spoofing database. The usual low-complexity and low-cost characteristics of attacks make them accessible to the general public. The current study addresses the spoofing issue analyzing the feasibility to perform minimum-cost attacks with self-manufactured three-dimensional (3D) printed models to 3D and 2.5D face recognition systems. A new database with 2D, 2.5D and 3D real and fake data from approximately 26 subjects was acquired for the experiments.

Sonal Girdhar *et al.,* [3] proposed a method using soft biometrics. Although soft biometric system such as eye color, age, gender, ethnicity, etc., requires the ability to uniquely identify an individual, yet they provide some additional information about the user and improve the efficiency of the system. Here projected a technique to integrate liveness detection with soft biometrics to enhance the performance of the authentication system. It provides a good high end solution for liveness detection which is difficult to breech.

Andr´e Anjos *et al.,* [4] proposed new technique of countermeasure solely based on foreground/background motion correlation using Optical Flow. Firstly begin a publicly available photo-attack database with associated protocols to measure the value of counter-measures. Based on the available data, conduct a study on current state-of-the-art spoofing detection algorithms based on motion analysis, showing they fail under the light of these new dataset. Outperforms all additional algorithms achieving nearly perfect scoring with an equal-error rate of 1.52% on the available test data.

R. Raghavendra and Christoph Busch [5] proposed a novel PAD algorithm based on statistical features extracted using BSIF (Binarized Statistical Image Features) and the Cepstral features extracted using 2D-Cepstrum. The proposed PAD algorithm forms a standard solution

for both face and iris biometric modality. Given a biometric sample, the proposed PAD algorithm will extract both BSIF and 2D Cepstrum features separately, which were fused to form a single feature vector before obtaining a decision using the linear SVM. Extensive experiments are carried out on the face and iris publicly available database like CASIA and ATVS. For face used CASIA face spoof database and for the iris used ATVS. The proposed Presentation Attack Detection algorithm will extract the statistical features that can capture the micro-texture variation using BSIF and Cepstral features .That can reflect the micro changes in frequency using 2D Cepstrum analysis.

Tiago de Freitas Pereira *et al.,* [6] proposed a novel and appealing approach to detect face spoofing using the dynamic texture (spatiotemporal) extensions of the highly popular local binary pattern operator(LBP). The key idea of the approach is to find out and detect the structure and the dynamics of the facial micro-textures that characterize real faces but not fake ones. Evaluated the approach with two publicly available databases (Replay-Attack Database and CASIA Face Anti-Spoofing Database). The results show that our approach performs better than state-of-the-art techniques following the provided evaluation protocols of each database.

Sooyeon Kim *et al.,* [7] proposed a new feature descriptors extracted from the raw light field photograph. In addition, an anti-spoofing face method is proposed by applying new feature descriptors. To evaluate our method and to measure error rates in experimentation section, created databases using the light field camera. A light field camera is a sensor that can record the directions as well as the colors of incident rays. This suggests a novel approach for defending face spoofing attacks, like printed 2D facial photos and HD tablet images, using the light field camera. By viewing the raw light field photograph from a different standpoint, extract two special features which cannot be obtained from the conventional camera. To verify the performance, had experiments on compose light field photograph databases. This method achieves at least 94.78% accuracy or up to 99.36% accuracy under different types of spoofing attacks.

Jukka Komulainen *et al*., [8] proposed, under several types of scenic face attacks, addressess this issue by studying fusion of motion and texture based countermeasures. It provide an intuitive way to explore the fusion potential of different visual cues and show that the performance of the individual methods can be vastly improved by performing fusion at score level. The simplified anti-spoofing framework actually works significantly better when spoofing decision is made within 100 frames.

Ivana Chingovska *et al.,* [9] proposed techniques for decision level and score-level fusion to integrate a recognition and anti-spoofing systems, using an open-source framework that handles the ternary classification problem (clients, impostors and attacks) clearly. By doing so, able to report the impact of different spoofing counter-measures, fusion techniques and thresholding on the overall performance of the final recognition system. It may be intuitive to imagine that a multimodal biometric system will be more robust to spoofing, because one needs to bring copies of more than one biometric trait to mislead the system.

Allan da Silva Pinto *et al.,* [10] proposed video-based face spoofing detection through visual rhythm analysis. It takes advantage of noise signatures generated by the recaptured video to distinguish between fake and valid access. To capture the noise and to obtain a compact representation, we use the Fourier spectrum followed by the computation of the visual rhythm and extraction of the gray level co-occurrence matrices, used as feature descriptors.

Roberto Tronci *et al.,* [11] proposed a method in which both video and static analysis in order to employ complementary information about motion, texture and liveness and

consequently to obtain a more robust classification. Its technology is intrinsically flat to spoof attack. The reported performances are strictly linked to the specific kind of attack which they refer to.

4. CONCLUSION

To conclude this paper, various methods were learned which involved in face recognition system. It may be stated that, although a large amount of work has been done in the field of spoofing detection and many advances have been reached, attacking methodologies have also evolved becoming more and more sophisticated. As a importance, there are still big challenges to be faced in the protection against direct attacks, that will optimistically lead in the coming years to a new generation of more secure biometric systems.

References

[1] Sooyeon Kim, Yuseok Ban and Sangyoun Lee, Face Liveness Detection Using Defocus. *Sensors* 15 (2015) 1537-1563; doi: 10.3390/s150101537

[2] Javier Galbally, Riccardo Satta, "Three-dimensional and two-and-a-half dimensional face recognition spoofing using three-dimensional printed models. *IET Biometrics* Volume 5, Issue 2, June 2016, p. 83-91DOI: 10.1049/iet-bmt.2014.0075

[3] Sonal Girdhar, Arun Kumar Yadav, Dr. Chander Kant, Improving Performance of a Face Liveness Detection System Using Soft Biometrics. *International Journal of Computer Science and Communication*, Volume 6, Issue 2, 2015, 9-12

[4] Andre Anjos, Murali Mohan Chakka and Sebastien Marcel, Motion-Based Counter-Measures to Photo Attacks in Face Recognition. *IET Biometrics*, 2014. Volume 3, Issue 3, September 2014, Pages 147-158. https://doi.org/10.1049/iet-bmt.2012.0071

[5] R. Raghavendra, Christoph Busch, Presentation Attack Detection Algorithm for Face and Iris Biometrics. Signal Processing Conference (EUSIPCO), 2014 Proceedings of the 22nd European 1-5 Sept. 2014.

[6] Freitas Pereira, T.d., Komulainen, J., Anjos, A. *et al.* Face liveness detection using dynamic texture. *J Image Video Proc* 2014, 2 (2014). https://doi.org/10.1186/1687-5281-2014-2

[7] Sooyeon Kim, Yuseok Ban and Sangyoun Lee, Face Liveness Detection Using a Light Field Camera. *Sensors* 2014, 14, 22471-22499; doi:10.3390/s141222471.

[8] J. Komulainen, A. Hadid, M. Pietikäinen, A. Anjos and S. Marcel, Complementary countermeasures for detecting scenic face spoofing attacks. *2013 International Conference on Biometrics (ICB)*, 2013, pp. 1-7, doi: 10.1109/ICB.2013.6612968

[9] I. Chingovska, A. Anjos and S. Marcel, Anti-spoofing in Action: Joint Operation with a Verification System. *2013 IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 2013, pp. 98-104, doi: 10.1109/CVPRW.2013.22

[10] Allan da Silva Pinto, Helio Pedrini, William Robson Schwartz, Anderson Rocha, Video-Based Face Spoofing Detection through Visual Rhythm Analysis. Graphics, Patterns and Images (SIBGRAPI), 2012 25th SIBGRAPI Conference on 2012.

[11] R. Tronci *et al*. Fusion of multiple clues for photo-attack detection in face recognition systems. *2011 International Joint Conference on Biometrics* (IJCB), 2011, pp. 1-6, doi: 10.1109/IJCB.2011.6117522