**ECG BIOMETRIC AUTHENTICATION: A COMPARATIVE ANALYSIS**

**[1] Nesli Erdogmus and Sebastien Marcel. Spoofing face recognition with 3d masks. IEEE transactions on information forensics and security, 9(7):1084–1097, 2014.**

Spoofing is the act of masquerading as a valid user by falsifying data to gain an illegitimate access. Vulnerability of recognition systems to spoofing attacks (presentation attacks) is still an open security issue in biometrics domain and among all biometric traits, face is exposed to the most serious threat, since it is particularly easy to access and reproduce. In this paper, many different types of face spoofing attacks have been examined and various algorithms have been proposed to detect them. Mainly focusing on 2D attacks forged by displaying printed photos or replaying recorded videos on mobile devices, a significant portion of these studies ground their arguments on the flatness of the spoofing material in front of the sensor. However, with the advancements in 3D reconstruction and printing technologies, this assumption can no longer be maintained. In this paper, we aim to inspect the spoofing potential of subject-specific 3D facial masks for different recognition systems and address the detection problem of this more complex attack type. In order to assess the spoofing performance of 3D masks against 2D, 2.5D, and 3D face recognition and to analyze various texture-based countermeasures using both 2D and 2.5D data, a parallel study with comprehensive experiments is performed on two data sets: the Morph database which is not publicly available and the newly distributed 3D mask attack database.

**Summary:** Spoofing attacks continue to be a security threat for biometric recognition systems and face is among the most vulnerable traits due to its high accessibility. Majority of previous studies in face spoofing focus on preventing 2D attacks performed by displaying printed photos or replaying recorded videos on mobile devices. However, utilization of 3D masks for face spoofing attacks has become easier and cheaper with the advancements in 3D reconstruction and printing technologies.

**[2] A. Hadid, N. Evans, S. Marcel and J. Fierrez, "Biometrics Systems Under Spoofing Attack: An evaluation methodology and lessons learned," in IEEE Signal Processing Magazine, vol. 32, no. 5, pp. 20-30, Sept. 2015, doi: 10.1109/MSP.2015.2437652.**

Biometrics already form a significant component of current and emerging identification technologies. Biometrics systems aim to determine or verify the identity of an individual from their behavioral and/or biological characteristics. Despite significant progress, some biometric systems fail to meet the multitude of stringent security and robustness requirements to support their deployment in some practical scenarios. Among current concerns are vulnerabilities to spoofing? persons who masquerade as others to gain illegitimate accesses to protected data, services, or facilities. While the study of spoofing, or rather anti spoofing, has attracted growing interest in recent years, the problem is far from being solved and will require far greater attention in the coming years. This tutorial article presents an introduction to spoofing and anti-spoofing research. It describes the vulnerabilities, presents an evaluation methodology for the assessment of spoofing and countermeasures, and outlines research priorities for the future.

**Summary:** Unless they are equipped with suitable countermeasures, all biometric systems were shown to be vulnerable to spoofing. Even so, some modalities (e.g., gait) are more robust than others (e.g., fingerprint), however, this should not be interpreted as meaning they are more reliable; in the absence of spoofing, fingerprint recognition generally outperforms gait recognition. Multimodal biometric systems are also vulnerable and can be overcome by the spoofing of only a single modality.

**[3] N. Kose and J. Dugelay, "On the vulnerability of face recognition systems to spoofing mask attacks," 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, BC, 2013, pp. 2357-2361, doi: 10.1109/ICASSP.2013.6638076.**

There are several types of spoofing attacks to face recognition systems such as photograph, video or mask attacks. To the best of our knowledge, the impact of mask spoofing on face recognition has not been analyzed yet. The reason for this delay is mainly due to the unavailability of public mask attacks databases. In this study, we use a 2D+3D mask database which was prepared for a research project in which the authors are all involved. This paper provides new results by demonstrating the impact of mask attacks on 2D, 2.5D and 3D face recognition systems. The results show that face recognition systems are vulnerable to mask attacks, thus countermeasures have to be developed to reduce the impact of mask attacks on face recognition. The results also show that 2D texture analysis provides more information than 3D face shape analysis in order to develop a countermeasure against high-quality mask attacks.

**Summary:** In this study, a 2D+3D face mask attack database is used which was prepared for TABULA RASA research project. It is used to evaluate the performances of the state-of-the art face recognition techniques under spoofing attacks. The novelty of this study is, it is the first time that the impact of mask spoofing is analyzed on 2D, 2.5D and 3D face recognition. **[4]** **Majid Komeili, Narges Armanfard, and Dimitrios Hatzinakos. Liveness detection and automatic template updating using fusion of ecg and fingerprint. IEEE Transactions on Information Forensics and Security, 13(7):1810–1822, 2018.**

Fingerprints have been extensively used for biometric recognition around the world. However, fingerprints are not secrets, and an adversary can synthesis a fake finger to spoof the biometric system. The mainstream of the current fingerprint spoof detection methods are basically binary classifier trained on some real and fake samples. While they perform well on detecting fake samples created by using the same methods used for training, their performance degrades when encountering fake samples created by a novel spoofing method. In this paper, we approach the problem from a different perspective by incorporating electrocardiogram (ECG). Compared with the conventional biometrics, stealing someone's ECG is far more difficult if not impossible. Considering that ECG is a vital signal and motivated by its inherent liveness, we propose to combine it with a fingerprint liveness detection algorithm. The combination is natural as both ECG and fingerprints can be captured from fingertips. In the proposed framework, the ECG and fingerprint are combined not only for authentication purpose but also for liveness detection. We also examine automatic template updating using ECG and fingerprint. In addition, we propose a stopping criterion that reduces the average waiting time for signal acquisition.

**Summary:** ECG can be recorded from fingertips. Therefore, fingerprint is the natural choice to be fused with ECG. On the other side fingerprint is vulnerable to spoof attacks and ECG has inherent liveness detection. This paper presented a unified approach for fusion of fingerprint and ECG that fills the gap between these two sides. To get the most out of ECG, the proposed system fuses ECG with a conventional fingerprint liveness detection method for a better liveness detection performance, and also fuses it with a fingerprint recognition method for a better recognition rate.

**[5] P. P. K. Chan et al., "Face Liveness Detection Using a Flash Against 2D Spoofing Attack," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 2, pp. 521-534, Feb. 2018, doi: 10.1109/TIFS.2017.2758748.**

Face recognition technique has been widely applied to personal identification systems due to its satisfying performance. However, its security may be a crucial issue, since many studies have shown that face recognition systems may be vulnerable in an adversarial environment, in which an adversary can camouflage as a legitimate user in order to mislead the system. Although face liveness detection methods have been proposed to distinguish real and fake faces, they are either time-consuming, costly, or sensitive to noise and illumination. This paper proposes a face liveness detection method with flash against 2D spoofing attack. Flash not only can enhance the differentiation between legitimate and illegitimate users, but it also reduces the influence of environmental factors. Two images are taken from a subject, one with flash and another without flash. Four texture and 2D structure descriptors with low computational complexity are used to capture information of the two images in our model. Advantages of our method include low installation cost of flash and no user cooperation required. A data set of 50 subjects collected under different scenarios is used in the experiments to evaluate the proposed method. The experimental results indicate that the proposed model performs better than existing liveness detection methods in different environmental scenarios. This paper confirms that the use of flash successfully improves face liveness detection in terms of accuracy, robustness, and running time.

**Summary:** A dataset containing 50 subjects with 2D spoofing attacks, including paper photo, iPad photo, video, 2D mask and curved mask attack, are collected. In order to compare with the thermal image method, thermal images of 21 subjects with real and five types of attacks are also collected. Our method is also compared experimentally with five software-based and one hardware-based liveness detection methods. The experimental results show that the proposed method is better in terms of accuracy and running time.