Rethinking Shape From Shading for Spoofing Detection

J. Matías Di Martino, *Member, IEEE*, Qiang Qiu, *Member, IEEE*, and Guillermo Sapiro, *Fellow, IEEE*

***Abstract*— Spoofing attacks are critical threats to modern face recognition systems, and most common countermeasures exploit 2D texture features as they are easy to extract and deploy. 3D shape-based methods can substantially improve spoofing prevention, but extracting the 3D shape of the face often requires complex hardware such as a 3D scanner and expensive computation. Motivated by the classical shape-from-shading model, we propose to obtain 3D facial features that can be used to recognize the presence of an actual 3D face, without explicit shape reconstruction. Such shading-based 3D features are extracted highly efficiently from a pair of images captured under different illumination, e.g., two images captured with and without flash. Thus the proposed method provides a rich 3D geometrical representation at negligible computational cost and minimal to none additional hardware. A theoretical analysis is provided to support why such simple 3D features can effectively describe the presence of an actual 3D shape while avoiding complicated calibration steps or hardware setup. Experimental validation shows that the proposed method can produce state-of-the-art spoofing prevention and enhance existing texture-based solutions.**

***Index Terms*— Liveness detection, spoofing attack, face recognition, active light, flash, 3D facial features.**

I. Introduction

FACE recognition became one of the most extended and popular biometric techniques. In particular, 2D face recognition algorithms have been ubiquitously deployed in the past years, e.g., at airports, ATMs, and personal devices. However, fake facial images can be deployed to spoof automatic face recognition systems.

Spoofing attacks proved to be a critical threats to modern face recognition systems. Various hacking methods have been developed to achieve illegal access to systems guarded with face recognition technology [1]. One of the most popular and simple hacking techniques consists of printing or replaying by some media a high quality picture of the target subject

Manuscript received August 28, 2019; revised March 9, 2020 and April 27, 2020; accepted June 1, 2020. Date of publication December 8, 2020; date of current version December 14, 2020. This work was supported in part by the Comision Sectorial de Investigacion Cientifica (CSIC), in part by the Google, in part by the Microsoft, in part by the Amazon, in part by the Cisco, in part by the NSF, in part by the National Geospatial Intelligence Agency (NGA), in part by the Office of Naval Research (ONR), and in part by the Army Research Office (ARO). The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Daniel L. Lau. *(Corresponding author: J. Matías Di Martino.)*

J. Matías Di Martino is with the Department of Electrical and Computer Engineering, Duke University, Durham, NC 27707 USA, and also with the Department of Physics and Electrical Engineering, Universidad de la República, Montevideo 11300, Uruguay (e-mail: matias.di.martino@duke.edu).

Qiang Qiu and Guillermo Sapiro are with the Department of Electrical and Computer Engineering, Duke University, Durham, NC 27707 USA (e-mail: qiang.qiu@duke.edu; guillermo.sapiro@duke.edu).

Digital Object Identifier 10.1109/TIP.2020.3042082

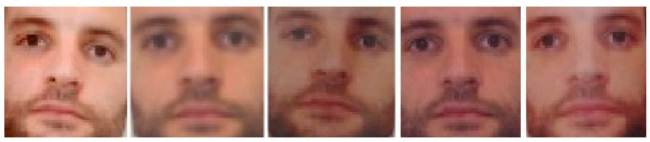

Fig. 1. Illustration of some of the challenges in identifying photos of real (live) subjects from a single image. From left to right, the second and fourth pictures correspond to a photo of the (live) subject. The first picture is a photo of a computer screen where the face of the test subject is displayed. The third and fifth pictures are taken by photographing a printed portrait of the test subject.

[2], [3]. A single image contains limited information to distinguish between a high quality replica of a subject and the subject itself, as is illustrated in Fig. 1. Systems that attempt to distinguish among 2D images as those in Fig. 1 are relatively easy to overcome, as we demonstrate in the following sections. Fortunately, spoofing detection can be substantially improved by extracting 3D information of the scene, but the main caveat is that pursuing a 3D reconstruction of the scene is a challenging task and typically requires complex hardware and expensive computation.

Shape-from-shading (SFS) is a classic computer vision theory that allows the extraction of the 3D shape of the scene from a few images of it. But the canonical SFS formulation is impractical for spoofing detection as it requires knowing the illumination conditions and involves solving non-trivial partial differential equations. By generalizing a Lambertian model and bypassing typical requirements of SFS, we arrive at extremely efficient shading-based 3D features with high discriminative power for the detection of spoofing attacks. We provide a theoretical analysis to show that such features capture actual depth information with invariant properties that make them calibration-free and suitable for real-world applications.

The main contributions of this article can be summarized as:

- We rethink shape-from-shading ideas and propose a simple and effective feature representation design for spoofing detection.
- We provide a theoretical analysis of the proposed features and show that they capture actual depth information while they present invariant properties that make them suitable for practical applications (with no need for calibration or a sensitive set up of the hardware).
- We show that texture-based spoofing strategies provide good results in specific circumstances, but they do not generalize well. Finally, we show that depth information can greatly improve generalization, e.g., making solutions less dependent on the resolution of the input images.