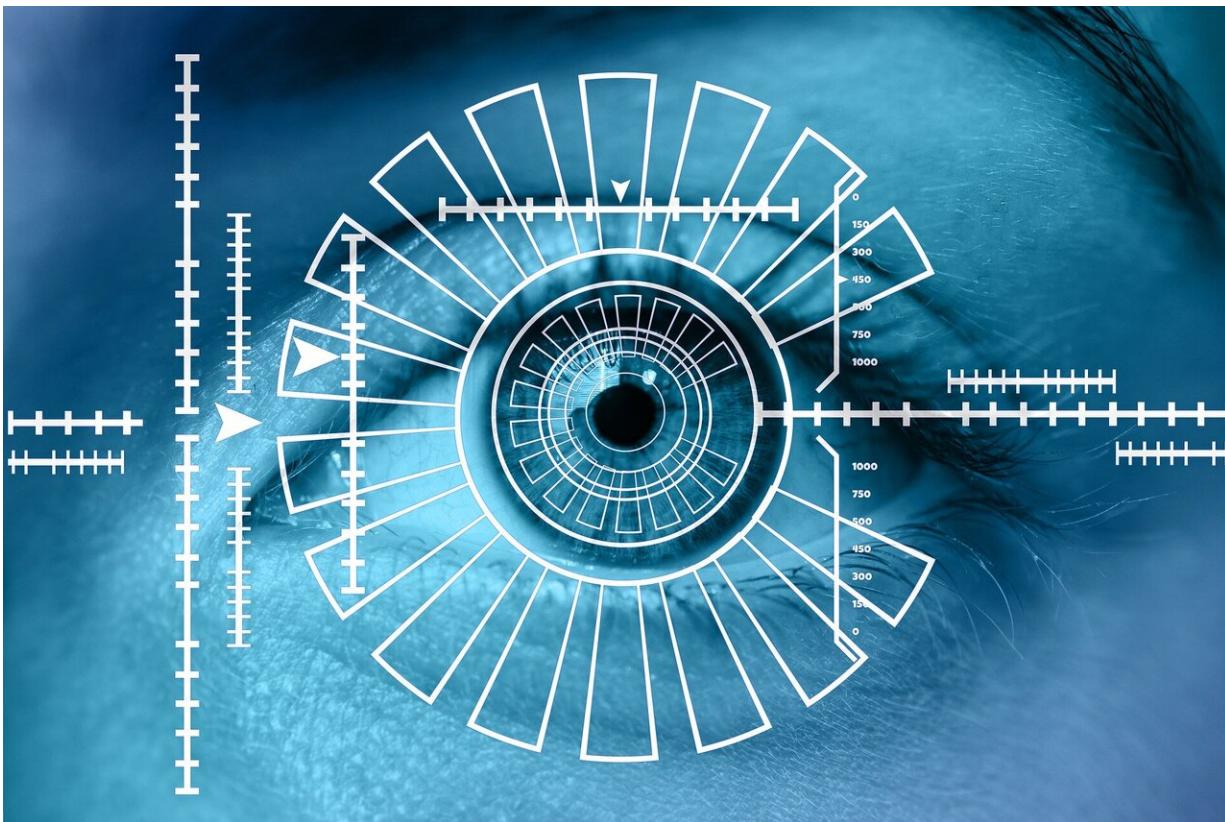


Blurred lines in face recognition

May 6 2021, by David Bradley



Credit: CC0 Public Domain

Face recognition has come on apace from a clichéd trope of science fiction to a reality of the modern world with widespread use in photography databases, social media, and the security world. However, as with any tool, there are those who would abuse it for nefarious ends. New research published in the *International Journal of Biometrics*

investigates one such aspect of face recognition where a third party might "spooft" the face of a legitimate user to gain access to systems and services to which they are not entitled and offers a suggestion as to how such spoofing might be detected.

Sandeep Kumar, Sukhwinder Singh, and Jagdish Kumar of the Punjab Engineering College in Chandigarh, India, explain how biometrics, including face [recognition](#), has come to the forefront of [security](#) in all sorts of realms from the simple accessing of a person's smartphone to securing sensitive premises. The key to precluding [face recognition](#) spoofing lies in the determination of whether the face being presented to the security [camera](#) or device is "live" or a static photograph or video rather than the actual person.

The team has turned to an improved SegNet-based architecture that can measure "blur" on the basis of local minimum and maximum left and right edges and calculate blur of horizontal and vertical edges. A flat image such as a photograph or video display presented to a [security camera](#) or device would be wholly in focus whereas "depth-of-field" comes into play. With a three-dimensional object, such as a real face, presented to the camera, the eyes would be sharply in focus assuming the camera focused on that part of the face, but the curved sides of the head would be slightly out of focus because they are not in the same plane relative to the camera lens as the eyes. Regardless, it is technically impossible for the whole of a three-dimensional object presented to a camera to be in focus, detecting the blur of parts of the object in front of or behind the [focal plane](#) is key to discerning whether a real face is in front of the camera or a flat image.

The team's proof of principle offers up to 97 percent accuracy, which is an improvement on earlier algorithms when tested against standard benchmarks. Moreover, it can determine the "liveness" of a presented face within about one second. The researchers are now working on

improving their system's speculation abilities by looking at shading, another characteristic of a real face that is obvious to a person looking at a face but difficult for a computer to detect via a camera.

More information: Sandeep Kumar et al. Face spoofing detection using improved SegNet architecture with a blur estimation technique, *International Journal of Biometrics* (2021). [DOI: 10.1504/IJBM.2021.114639](https://doi.org/10.1504/IJBM.2021.114639)

Provided by Inderscience

Citation: Blurred lines in face recognition (2021, May 6) retrieved 16 April 2024 from <https://techxplore.com/news/2021-05-blurred-lines-recognition.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.