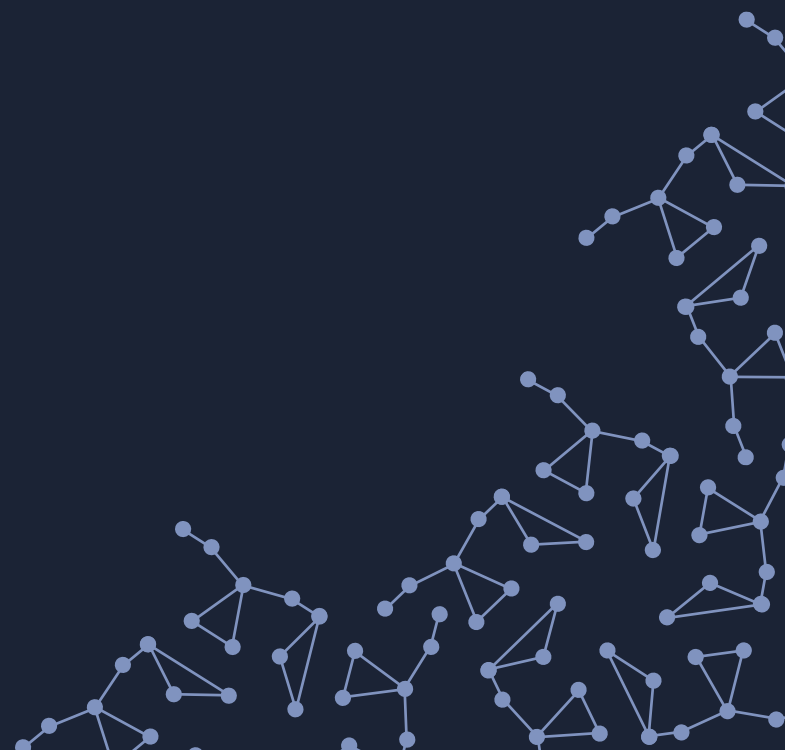
BioID
be recognized

Anti-Spoofing

powered by biometrics



Whitepaper

Face Presentation Attack Detection & Liveness Detection

What is Biometric Anti-Spoofing?

Biometric Anti-Spoofing aims at preventing the fraudulent usage of human traits by impostors. In order to design comprehensive anti-spoofing, it is important to distinguish and secure the different targets of an attack. Presenting replays or masks of a person to a sensor, e.g. a camera, is considered an attack at the sensor level. Opposed to this are attacks at the application level, e.g. the injection of a (manipulated) video into an operation. While application-level attacks require countermeasures like secure image capturing and out-of-band authentication, sensor-level attacks can be addressed by presentation attack detection.

What is Presentation Attack Detection?

Presentation attack detection (PAD) is a mechanism for noticing spoofing attempts with fake or stolen biometrics at the sensor-level, e.g. by presenting replays of a person to a camera. The term liveness detection is commonly used as an equivalent to PAD.

What types of face presentation attacks need to be considered?
Face spoofing attacks can be conducted with various materials, in 2D and 3D, static or moving/animated. Some examples can be found below:

- 2D photos made with high-definition face pictures on flat paper.
- Image swapping with multiple 2D photos in a sequence.
- 2D Cut-outs and paper masks, e.g. with holes.
- 3D paper masks.
- Video replays.
- 3D prints, wax heads, or sculptures.
- 3D masks in resin, latex, or silicone with holes for eyes, mouth or other areas.
- 3D deepfakes, digital doubles or avatars.

Please note:

While deepfake attacks at the sensor-level can be rejected by PAD systems, deepfake attacks at the application level need to be addressed differently: one effective mitigation against such an intrusion is by means of out-of-band authentication using a mobile device. As application-level deep-fake spoofing requires the use of a virtual camera in order to intercept and manipulate the video stream, liveness detection using a mobile app minimizes an impostor's possibilities and mitigates this risk.

What techniques is PAD based on?

Some of the state-of-the art technologies for presentation attack detection are the following:

Artificial Intelligence: Artificial Intelligence (AI) is leveraged through powerful DCNNs (deep convolutional neural networks). DCNNs are trained with dedicated data to detect presentation attacks like 3D paper and silicon masks, videos on displays, video-projections on various material, etc.

Motion-based analysis, e.g. using optical-flow analysis to calculate 3D mov- ment from two subsequent 2D images. Eye blinking or smiling are less reliable techniques for motion-based liveness detection. This analysis prevents any 2D spoofing attacks, such as printed or displayed photos, cutouts, etc.

Texture analysis: Image forensics can be utilized to examine the source of the biometric traits. A recaptured or manufactured version of a face differs drastically from a real face concerning certain features. This difference can be exploited to determine genuine biometrics.

Challenge-response: The user can be guided to turn their head in a certain, randomized way. The directional analysis and interaction with the user prevent any prerecorded videos, 3D avatars or deep fakes from passing liveness detection.

What applicable standards are in play?

The international PAD standard ISO/IEC 30107 defines different levels of presentation attacks as well as the criteria for a liveness detection system to be conforming with the ISO standard.

Depending on the purpose of the certification, there are two types of compliance indicators to consider for an objective liveness detection performance assessment:

> **Liveness Detection evaluation performed by a FIDO Accredited Biometric Laboratory against criteria based on FIDO Biometric Certification Requirements v1.1 and ISO/IEC 30107.**
>
> **FIDO biometric component certification which tests a facial recognition system including its PAD mechanism according to the standards ISO 19795 and ISO/IEC 30107.**

About BioID

BioID is the cloud biometrics company

We make strong, convenient, privacy-assured face recognition available to everyone, on any device, anytime, anywhere so people can be protected in the cyber world and forget about passwords!

Guided by the vision that anonymous biometric recognition empowers internet users to secure their online identities with privacy, BioID offers a reliable link between a real person and digital identities by verifying the user's presence in a convenient and natural way - just the way they look and/or the way they sound. The company's technology has been proven through many years of use in enterprises, banks and government organizations.

Privately held with R&D based in Germany, BioID has offices in Switzerland and the US.

Contact us for further information and test our biometrics at

playground.bioid.com.

Our demo App is available for Android and iOS.

BioID® GmbH
Bartholomaeusstr. 26D
90489 Nuremberg
Germany

+49 911 999 9898-0
e-mail: info@bioid.com