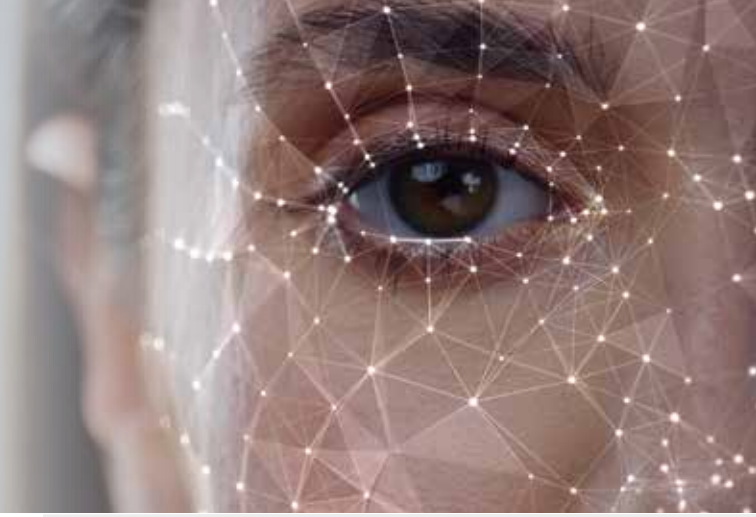
IDR&D

Protect Against Deepfakes: Facial Liveness with Injection Attack Detection

1350 Broadway, Ste 605 | New York, NY 10018 USA | www.idrnd.ai

Protect biometric security from deepfakes and other types of fraudulent digital imagery by detecting injection attacks



Facial recognition systems rely on presentation attack detection (PAD) to ensure that a live human face is the subject of the selfie taken during biometric capture.

Injection attacks pose a different vulnerability, where hardware and software hacks are used to bypass a proper capture process that uses the camera. Without countermeasures, fraudsters can emulate camera capture with non-live digital facial imagery in a way that can defeat certain liveness detection measures.

As with presentation attacks, injection attacks pose a fraud risk to biometric identity verification and authentication. Deepfakes can be used to create synthetic identities that fraudsters use to either open fraudulent accounts or access and take over their victims' accounts.

Stop Fraud from Deepfakes by Detecting Injection Attacks

IDLive® Face Plus combines award-winning presentation attack detection with a unique approach to injection attack detection to prevent deepfakes and other fraudulent digital content. Instead of focusing on the content of digital fakes,it helps shut down the channels used to deliver it, such as virtual cameras in desktop browsers and sophisticated hardware attacks.

Desktop and mobile browsers as well as mobile apps are protected in a way that is completely transparent to the user.

Detect key injection points

- Address external and virtual cameras
- Prevent JavaScript code modifications in browser

Prevent a variety of fraudulent, non-live facial imagery

- Images, recorded video, and live streaming
- Deepfakes and digital renderings
- Face swaps and morphs

Apply deepfake countermeasures without adding user friction

- Imperceptible to users and fraudsters
- Implementation and mobile footprint options

Gain protection on mobile devices and desktops

Mac and Windows browsers

iOS and Android browsers and apps

Requires adopting a client SDK for the image capture process

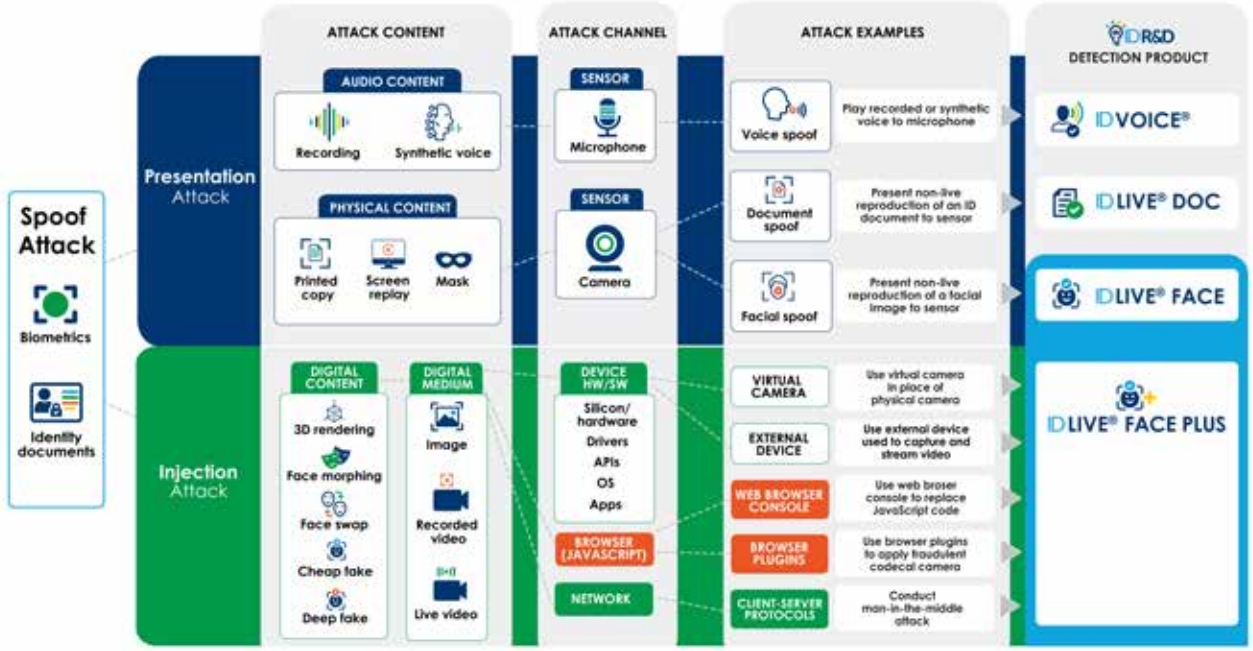
- Customizable so you control the user interface

Ready to learn more? Visit **www.idrnd.ai** for details, demos or to contact us.

IDR&D

A comprehensive, frictionless liveness detection solution

IDLive® Face Plus applies AI to detect critical injection attack paths fraudsters use to target biometric systems. These paths are used to inject fraudulent non-live facial imagery ranging from simple image-based attacks to advanced deep fakes. Injection attacks using external cameras, virtual cameras, and browser code manipulations are addressed.



IDLive® Face Plus is built on many decades of collective research and development focused on advanced machine learning algorithms, proper data collection and categorization, and training. The product uses computer vision techniques and extensive internal innovation to deliver unique injection attack detection capabilities.

- Complement presentation attack detection with injection attack detection
- Prevent deepfakes, face morphs, face swaps, and rendered video
- Detect imagery injected using external and virtual cameras
- Prevent JavaScript code modifications in browser console and plug-ins
- Protect mobile devices and desktops
- Avoid adding user friction

About Us

ID R&D is on a mission to replace fraud-prone onboarding and frustrating authentication practices with a frictionless user experience that is significantly more secure.

Founded in 2016, ID R&D is growing rapidly, with headquarters in New York City and staff based around the world. Our biometrics research and engineering teams are domain experts and industry veterans, with PhDs in speech, image processing, and machine learning.

Ready to learn more?
Visit **www.idrnd.ai** for details, demos or to contact us.

ID R&D