DOT

INNOVATRICS
building a world of instant trust

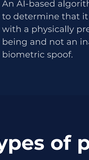
Facial Liveness Detection In a Nutshell

Crucial part of remote identity verification to prevent identity fraud

Institutions such as banks, telecom operators, insurance agencies and basically anyone who needs to reliably onboard customers, needs to make sure that the data used for customer identification is genuine, and they are required to take measures to verify it. Liveness detection is part of the remote identity verification process performed typically during the digital customer onboarding.

Identity fraud is real

YoY stats on fraud



Identity fraud rates have doubled compared to 2020

Customers perception

Most important aspects of online experience

Security

Preferred security method

Physical biometrics

Essential terminology

Presentation Attack Detection (PAD)

An AI-based algorithm's ability to determine that it is interfacing with a physically present human being and not an inanimate biometric spoof.

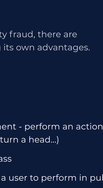
Facial Liveness Detection

The specific detection of whether a face present at the time of capture is taken from a live individual – as opposed to a recording, picture or another non-living spoof.

Types of presentation attacks

A: Hi-res paper & digital photos, hi-def challenge/response videos and paper masks.

B: Commercially available lifelike dolls, and human-worn resin, latex & silicone 3D masks under $300 in price.

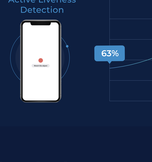


C: Custom-made ultra-realistic 3D masks, wax heads, etc., up to $3,000 in creation cost.

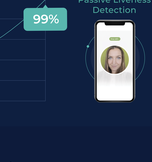
Human v algorithms identifying fraud

Why do you need technology?

Human



Algorithm



Active v passive liveness detection

Targeting to detect presentation attacks to prevent identity fraud, there are two main types of liveness detection, each of them having its own advantages.

Active

- Requires user's involvement - perform an action (follow a moving object, turn a head...)
- Takes time to perform/pass
- May be inconvenient for a user to perform in public
- Involvement of a user may lead to higher abandonment rates

Passive

- No user interaction required
- Is basically immediate as it runs in the background of the face verification process
- Only need one frame to tell if the person is real and alive
- Lack of friction for a user leads to higher completion rates

Combination of both - Smile liveness

- Combines unrivaled security of active liveness with little or no user-experience trade-off of passive liveness
- Users may feel higher security when asked for interactive checks

Completion rates

Check the accreditation

The most commonly used NIST NVLAP certified testing lab for PAD evaluations is iBeta. iBeta Level 2 accreditation is the highest level of PAD evaluation in widespread use today.

iBeta LEVEL 1 ISO 30107-3 COMPLIANT

iBeta LEVEL 2 ISO 30107-3 COMPLIANT