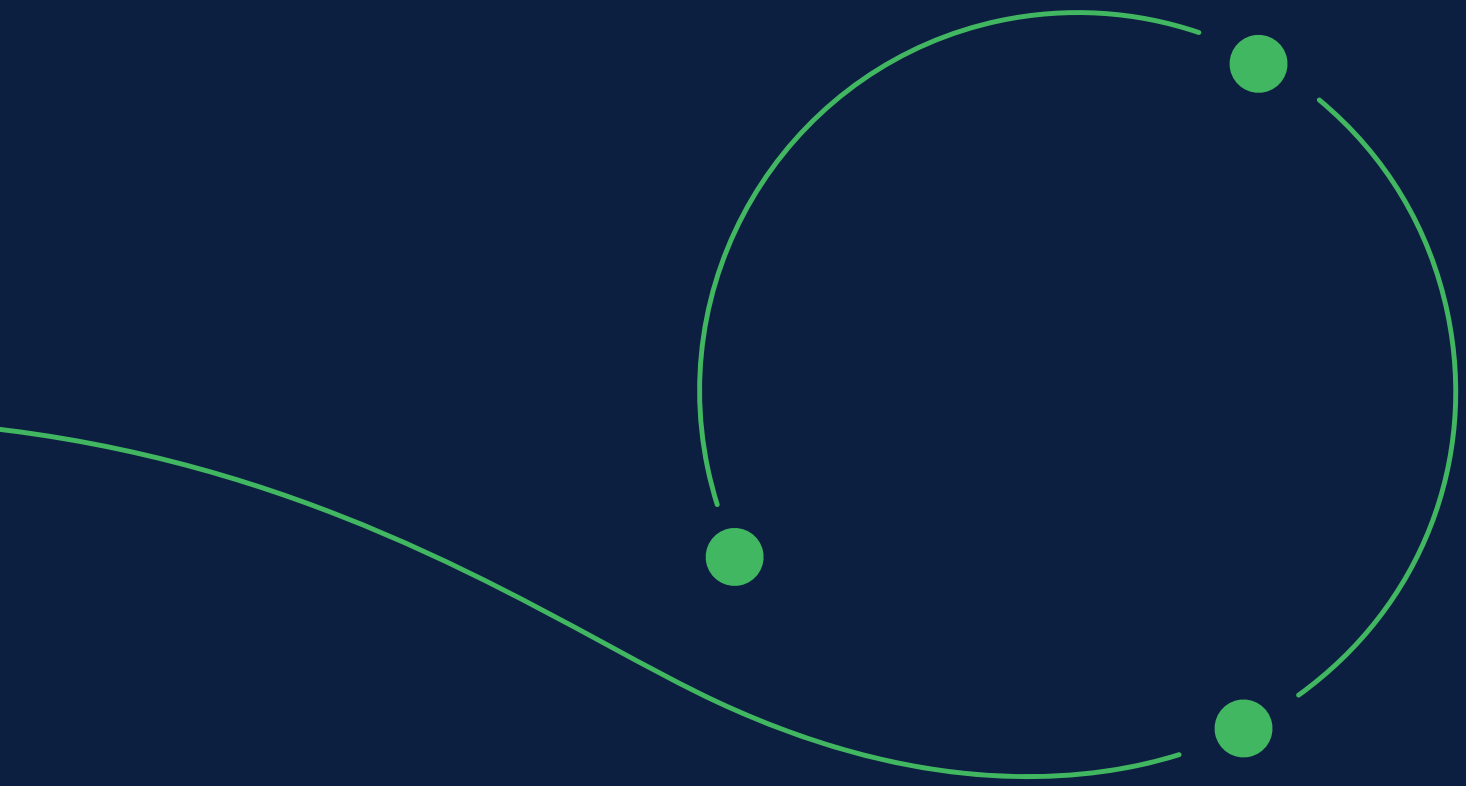
INNOVATRICS

DOT

What do you need to know when choosing your facial liveness vendor?

White Paper

Liveness Detection



innovatrics.com

Why Having the Best Liveness Detection Technology Partner Matters

Identity fraud poses a global threat, hitting the financial sector hardest. Organizations now face the transition from traditional paper-based security to combatting sophisticated threats like deepfakes. A recent study[1] by ID Analytics reveals that synthetic identity fraud constitutes a staggering 80–85% of all identity fraud cases, recording a sharp 132% surge in incidents in 2022, with expectations of continued growth. Ensuring trust in technology is paramount, assuring users that their identity will not be compromised even if someone possesses their photo.

As the prevalence of identity fraud grows, selecting a reliable facial liveness vendor becomes crucial. In this paper, we delve into the key considerations one must address when choosing a technology partner for facial liveness.

To Use Liveness Detection or Presentation Attack Detection

PAD, or Presentation Attack Detection, is mainly about automatically determining if someone is trying to deceive the system. In simpler terms, it's a method that checks if a biometric sample, like a fingerprint or face scan, is from a real, living person at the time of capture, as defined by sources such as NIST SP 800-63-3[2] and ISO/IEC 30107-1:2023[3].

In our white paper, we will use liveness detection vand PAD interchangeably since they essentially mean the same thing.

The Role of Liveness Detection

The capabilities of algorithms in identifying people surpass human capacities. These algorithms operate seamlessly at any time and scale. Unlike the past reliance on branch visits or video calls, algorithms now offer a more efficient and accurate means to confirm the liveness of individuals.

The rise of sophisticated attackers has prompted the development of Presentation Attack Detection (PAD) as a critical component in identity verification. PAD has thus become instrumental in distinguishing genuine customers from potential threats.

[1] bit.ly/3Rpqn1Y
[2] bit.ly/3tgZ0zf
[3] bit.ly/48d6fqL

What Are Typical Presentation Attacks?

To catch a fraudster, you will have to think like one. If you successfully trick a company into believing you are someone else, you might get a loan and never have to pay it back.

Here is a high-level overview of how to deceive a system:

Type of attack	What you need as an attacker
Print attacks	Stolen ID and printed image (including a 2D paper mask) of the person from an ID
Screen replay attack	Stolen or forged ID and a digital picture or video of the person from ID
3D mask attack	3D mask of someone else

Based on the type of presentation attack used, we can discuss certain types of identity fraud. The table shows the different technological ways to detect fraudulent attempts:

It is hard enough to deal with one person staging an attack once in a while. Imagine having hundreds of attackers generating thousands of such attempts every single day.

Type of fraud	What you need as an attacker	How to stop it
Identity theft (Stolen identity)	A good face photo of the victim, possibly a fake or stolen ID of the victim; Could be used with knowledge about victim's accounts	• Liveness detection • Video injection detection
Synthetic identity (Manipulated)	A fall guy willing to cooperate and multiple fake IDs with their face	• Face deduplication • Document authenticity check
Synthetic identity (Manufactured)	A software to generate synthetic faces or to create deepfake videos, and to create fake IDs	• Liveness detection • Video injection detection

Liveness Detection: What Are My Options?

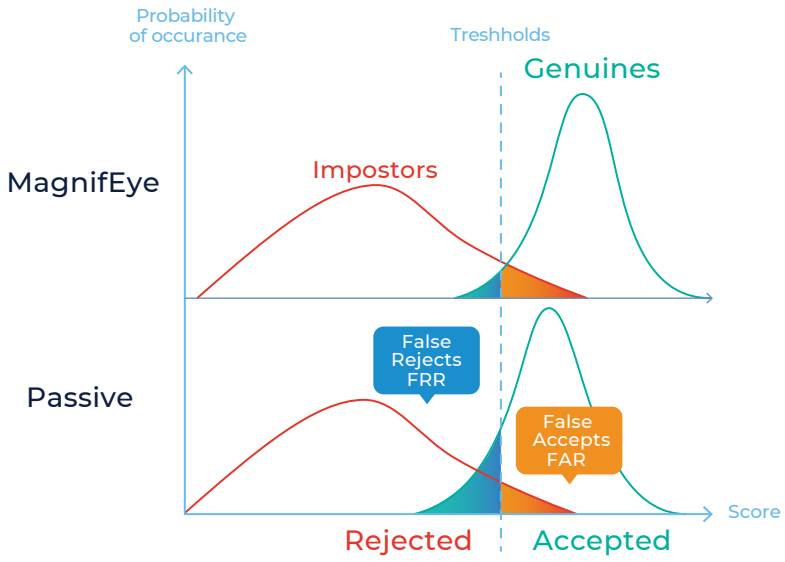
Liveness detection employs different biometric measurements to confirm that the face in question is genuinely alive and not a replica. At present, where deepfakes and synthetic identity fraud pose significant threats, it is crucial to incorporate a video injection attack detection system. This ensures that users are physically present and actively undergoing authentication, adding an extra layer of security.

Implementing such security measures comes in various forms. These diverse methods contribute to a comprehensive strategy for countering the evolving challenges of identity verification in a digital environment.

One Type Does Not Fit All

The effective use of liveness detection technology in real-life situations lies in the balance between security and user experience. It is shaped by the algorithm's accuracy and its impact on user engagement, which directly influences drop-off rates. Achieving optimal security involves considering two crucial parameters: the False Accept Rate (FAR) and the False Reject Rate (FRR).

When evaluating different liveness detection algorithms, it is essential to consider their score distribution, decision threshold, and the resulting balance of false accepts and false rejects. Moreover, factors like completion rate (affected by false rejects) and the time needed for data capture significantly



contribute to the overall usability of the algorithm. Therefore, a thorough assessment of accuracy and usability factors becomes imperative when choosing a liveness detection algorithm. The accompanying chart on page 3 provides a visual comparison example.

Having a technology partner who can tailor liveness detection technology to align with your specific use case is a substantial advantage. This guarantees that the technology not only meets your security requirements but is also finely tuned to enhance user experience.

Performing Passive Liveness the Right Way

For specific use cases where prioritizing user experience is important, passive liveness is the top priority. The interaction, although simple, influences completion rates. Furthermore, it enhances security by making it challenging for attackers to spoof the system. The attacker remains unaware of when or if the liveness verification has occurred, adding an extra layer of defense.

Innovatrics' algorithm stands out by offering liveness verification with just one image. This approach not only ensures simplicity but also highlights the flexibility and effectiveness of passive liveness in diverse use cases.

When a Selfie Is Not Enough – Active Liveness

In some cases, active liveness can add an extra check for more security or user involvement. Though it might be a hassle when users need to do something like smiling or gazing at a moving object, it also makes the system seem more credible in protecting against fraud. The intentional involvement of users not only adds a practical security measure but also contributes to establishing trust in the system.

Don't Underestimate Synthetic Data

Synthetic face generation opens the door to creating entirely new faces, evading recognition by biometric deduplication systems due to their uniqueness. Its scalability enables fraudsters to flood remote identity verification systems with deepfake videos, potentially registering millions of new identities through standard verification processes before detection.

Recent fraudulent attempts are quite different from conventional print attacks, focusing on deceiving identity verification through video injection. Various methods, including emulation, virtual cameras, phone camera replacement, hacking apps, and man-in-the-middle attacks, inject fake videos into the remote verification process. In such cases, traditional liveness detection falls short in identifying video injection attacks.

Modern identity verification systems must incorporate video injection detection as a vital component of liveness detection. This ensures that users are not only physically present but also actively authenticating during the remote onboarding process.

Innovatrics Liveness Detection in a Nutshell

At Innovatrics, we have established thorough liveness testing carried out at our own R&D center. Here are some of the highlights.

Building High-Quality Datasets

Our liveness detection algorithm is tested for presentation attacks using digital screens showing photos and videos, other 2D (printouts, paper masks), and 3D attacks (wigs, silicon, and plastic masks). Crowdsourcing has helped us immensely.

It was imperative to build our own datasets. If not for the hundreds of thousands of images of real faces and real attacks, our liveness technology would not be robust enough.

In addition to this, we have deployed various sophisticated techniques to generate additional training data.

Leveraging Machine Learning

Apart from datasets, we also work with cutting-edge and well-established machine-learning techniques. Our solution is built

using PyTorch and PyTorch Lightning frameworks, which are commonly used in the research community.

Our deep learning models use a well-tuned combination of multiple loss functions. For performance on mobile devices, we have selected the well-known Mobilenet architecture because of its accuracy & speed trade-off.

Sharing these details is a non-issue for us since our technology is not only about the tools but the entire R&D process. And of course, keeping everything up to date.

Following the Market's Needs

We have fine-tuned our liveness detection offering to fit any use case while having the best possible FAR/FRR ratio. With different types in our portfolio, you can choose the best option possible for the specific requirements of your clients as shown in the table below:

Type	Use Cases	Benefits
Passive Liveness	Requiring the highest completion rates	• Optimized user experience • Instant results • No capture component needed
Smile Liveness	Requiring moderate user involvement	• Little or no user experience trade-off • Fast and easy to complete • Positive emotion
MagnifEye Liveness	Requiring the highest levels of security	• Best FAR/FRR ratio • Active user involvement • Multiple frames evaluated

How to Pick a Liveness Detection Vendor You Can Trust

Doing passive liveness detection correctly requires performing complex processes. Although these only involve elementary matrix algebra, applying the math is a completely different ball game.

This is the simple reason why your biometric vendor needs to have its own R&D department. If you choose a vendor without it, you risk getting left behind since the product might seem impressive now but could end up being obsolete shortly after.

Trust but Verify

Maintaining a bit of skepticism is also important. Some vendors will try to convince you that they can perform a 3D scan using a standard mobile camera. While it is true that using advanced machine learning techniques can recreate a 3D model of a face from a 2D image, it is still only a vague estimation.

Talking about 3D scans without actually using a 3D camera is therefore misleading. Ultimately, it isn't even clear how this is supposed to help when it comes to liveness, as a lot of the attacks are 3D in nature.

Since neural networks are complicated tools, what you need is independent verification and not just bold claims.

Standards that Matter

Although there is no standardized framework to evaluate active liveness to this date, there are a few options for getting an independent review of passive liveness technology.

iBeta

The iBeta laboratory conducts Level 2 tests, assessing liveness systems on both Android and iOS devices. These evaluations recreate various attacks, each valued at under 300 USD, aligning with ISO/IEC standards. The tests include challenges like 2D transparent printouts, 3D paper, latex, silicone, and resin masks. iBeta rigorously attempts to breach the liveness system numerous times during testing, adopting a strict criterion where even a single failure results in an overall test failure.

iBeta's testing methodology involves attempting several types of attacks on the liveness system, each designed to simulate real-world threats.

Notably, Innovatrics' submission for the iBeta Level 2 Liveness test demonstrated a strong performance. Scoring between 0 to 0.4 percent false rejects (depending on the device), the system maintained a 0 percent false acceptance rate. This reliability affirms Innovatrics' capability to withstand various attacks, as validated by the iBeta[4] Level 2 testing process.

NIST PAD

NIST, in its Face Analysis Technology Evaluation (FATE)[5] report from September 2023[6], reviews passive liveness systems, specifically face presentation attack detection (PAD) algorithms using only one face image. The evaluation encompasses diverse attack types, excluding live image acquisition or interaction with real users to ensure comparability across vendors. It is crucial to note that these results might not universally apply, as the absence of live image components could impact overall system performance. Enhancements in capture components can contribute positively to liveness effectiveness.

Recent results from NIST, the sole publication to date, indicate that Innovatrics' performance aligns comparably with its competitors. The assessment, focusing on passive liveness algorithms, provides insights into system capabilities without live image involvement.

Tried and Tested, with a Dose of Transparency

Technology endorsed by any official independent framework carries a certain level of validity, representing a baseline standard that is better than having no evaluation at all. It is important to remember that no laboratory can test every aspect comprehensively. Since identity verification (IDV) systems are complex, relying on single benchmarks with specific datasets only addresses a fraction of the system's overall performance.

IDV systems consist of various components, including auto-capture, video injection detection, and server protection. For instance, the method of data collection, where auto-capture components play a substantial role, significantly influences the outcomes of remote identity verification. It is essential to understand that each benchmark focuses on individual aspects, underscoring the necessity of evaluating the entire system's performance.

In conclusion, selecting a vendor with extensive experience in real-life projects is paramount. Vendors who actively develop technology can collaboratively enhance performance based on practical feedback from their customers. This adaptability allows adjustments to meet specific needs or use cases, reinforcing the importance of choosing a vendor with both expertise and direct involvement in technology development.

[4] bit.ly/4akokVx
[5] pages.nist.gov/frvt/html/frvt_pad.html
[6] https://bit.ly/3tjOQxW

Innovatrics iBeta Level 2 PAD testing results

Test Species		Android			iOS		
		PAs*	APCE**	APCER***	PAs*	APCE**	APCER***
1.	3D Curved Paper Mask	150	0 of 150	0%	150	0 of 150	0%
2.	Latex Mask	150	0 of 150	0%	150	0 of 150	0%
3.	Inexpensive Silicone Mask	150	0 of 150	0%	150	0 of 150	0%
4.	Resin Mask	150	0 of 150	0%	150	0 of 150	0%
5.	Layered 2D Transparent Photo	150	0 of 150	0%	150	0 of 150	0%
Total per species			0 of 150	0%		0 of 150	0%
Total for all species			0 of 750	0%		0 of 750	0%

* Presentation Attack | ** Attack Presentation Classification Error
*** Attack Presentation Classification Error Rate

(find more at: https://bit.ly/3ccJysa)

Questions to Ask a Face Liveness Check Provider

What to consider	What to look for	
Technology ownership	Does the provider own all underlying technologies? How often is the algorithm upgraded?	Are the upgrades free?
User experience	Does it require an action from a customer? How fast is the processing? Does it work for people with disabilities?	Does it provide user guidance on taking photos? Can the system select the best photo by itself?
Requirements	What devices does it support? What are the camera requirements?	What are the minimal environmental (e.g., light) conditions?
Integration	How hard is it to integrate? Do I need to use some specific technology stacks? Do I get samples?	Is the API standardised and well-documented? Does the provider offer integration support?
Testing and transparency	Does the vendor test the technology internally? Is the technology tested independently? Are the tests ISO-compliant?	What types of attacks were tested? Are you able to test the technology on your data?
Market penetration	Is the technology being used on the market?	Is it being used in different countries and industries?
Liveness approach	Does the vendor provide active, semi-passive, or passive liveness? Can they provide various combinations of liveness approaches?	Does the system prevent video injection or replacement of the camera input?
Video injection prevention	Does the vendor offer detection of video injection?	Is it offered for both mobile and web environments?
Network requirements	How much data do you need to transfer? Is the transport secure from man-in-the-middle attacks?	Can you process the data on your servers, or do you need to send them to the vendor?
Storage requirements	Do you need to store some data? Does the data need to stay on the user's device?	Where do you need to store it? Does the data need to leave your infrastructure?
Speed	How fast can the liveness be evaluated? Does network transfer impact the processing speed?	How does CPU speed impact the processing speed? Do you need specialised hardware (e.g., GPU)?
Accuracy	What is the False Accept/False Reject trade-off? Can the trade-off be configured with a threshold?	Can the accuracy be improved by combining different approaches?

About us

We are an independent EU-based provider of multimodal biometric solutions. Our algorithms consistently rank among the fastest and most accurate in fingerprint and face recognition. Since 2004, we have partnered with all types of organizations to build trusted and flexible biometric identification solutions. Our products are being used in more than 80 countries, benefiting more than a billion people worldwide.

Contact

sales@innovatrics.com
www.innovatrics.com

Brazil

+55 11 4210-5185

USA

+1 404 984-2024

Slovakia (HQ)

+421 2 2071 4056

Singapore

+65 3158 7379