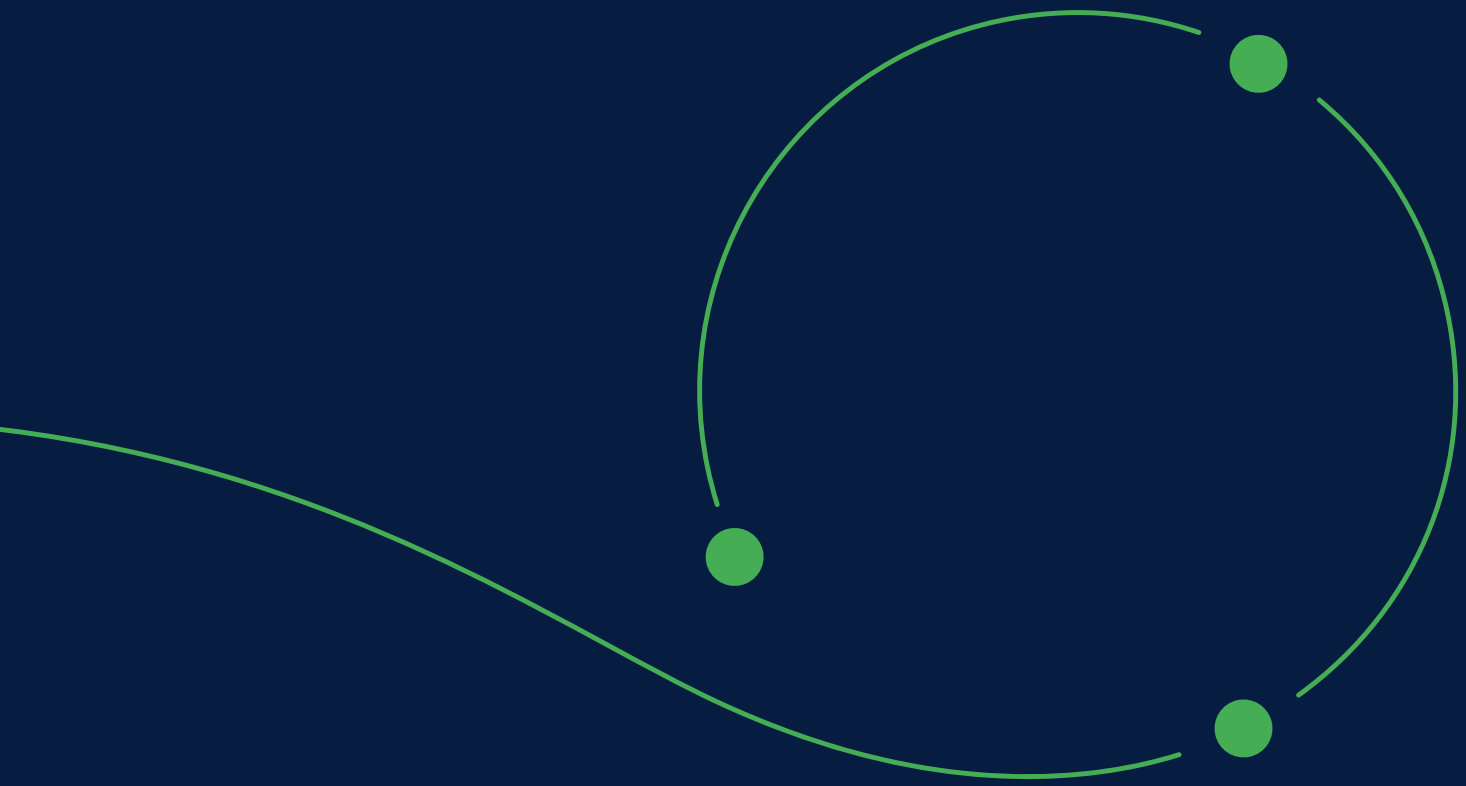
INNOVATRICS

Innovatrics liveness detection cross-verifies the identity of an enrollee during the onboarding process to make sure that the person is real.

White Paper

Facial Liveness Checks: Active, Passive, or Both?



Why We Do It the Way We Do

To ascertain that a user is alive, two distinct methods are used for liveness checks in remote onboarding solutions. Depending on what is required of the user, they are classified as either active or passive.

Active liveness checks

- Usually give random directions to the user (turn head, smile, blink) and check whether the user complies
- Very difficult to spoof with pre-recorded video due to the random nature of the directions
- The level of involvement of the user may be off-putting to some, leading to higher abandonment rate of onboardings
- Inconvenient for users to fulfill tasks in public such as making faces during onboarding
- Some implementations make directions hard to follow (e.g. reading instructions with head turned away from the screen)
- Impractical for users to perform in every transaction due to the involvement factor

Passive liveness checks

- Use image recognition deep learning techniques to tell a real face from an image (e.g. perspective distortion, involuntary eye movement or facial muscle twitching)
- Run in the background of the face capture process; only need one frame to tell if the person is real and alive
- Very difficult to spoof even with 3D masks
- Require minimum user interaction as are done just by looking at the phone
- Are usually faster, because they don't need the user to perform a randomized set of actions

Why is Liveness Check Important

The short answer is that European AML Regulation pretty much demands it, especially in financial and telecommunication industries. Any individual with access to the financial and mobile infrastructures must be thoroughly identified. Failure to comply can lead to severe fines or even suspending license.

The long answer: When providing remote unsupervised services through digital onboarding, this means not only checking whether the credentials fit, but also whether person is actually alive and physically present (in a brick & mortar branch, this check is pretty straightforward: if a person walks in, they are quite obviously alive). If such a check is not possible or reliable enough, the company may face the demand from regulator to amend its process or stop using remote enrollment altogether.

Hybrid solution

Innovatrics is unique in the bio-metric market with its decision to provide the customers with both active and passive liveness checks to suit their requirements for any given use case.

Innovatrics active liveness check is already more of a hybrid solu-tion – instead of requiring large head movements, it just instructs user to follow a randomly moving dot onscreen. The background process checks whether the eyes are looking in the right direction and whether the face performing the check is the same as the one on the selfie and ID document. This is to double-check that the onboarding is done by the one and the same person throughout the whole process.

Stranger to loan in 8 minutes

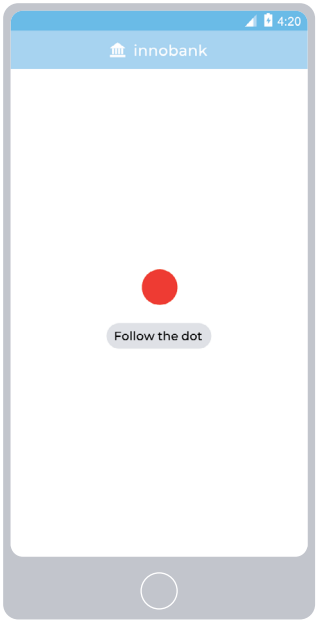
Superior to video calls, this type of liveness check is easier to scale than a call center. Since it's much faster, the abandonment rate is quite low. This supports studies citing that time spent onboard-ing is directly proportional to the abandonment rate during registration.

One of our clients in the banking sector has gained more busi-ness after adopting our digital onboarding solution. Not only can its clients remotely open a new bank account, they can also instantly access pre-approved loans. Due to their agile banking system, they were able to deposit a new loan onto a newly created account in 8 minutes, available to be used for payment or withdrawal.

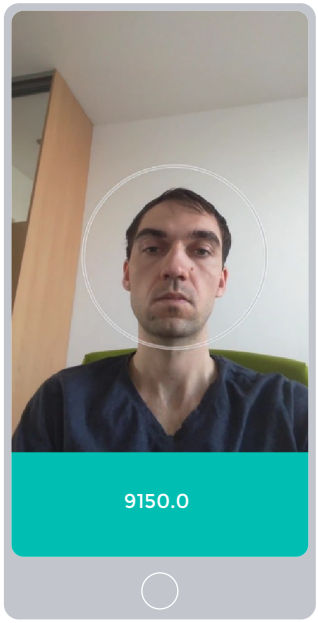
More than a selfie

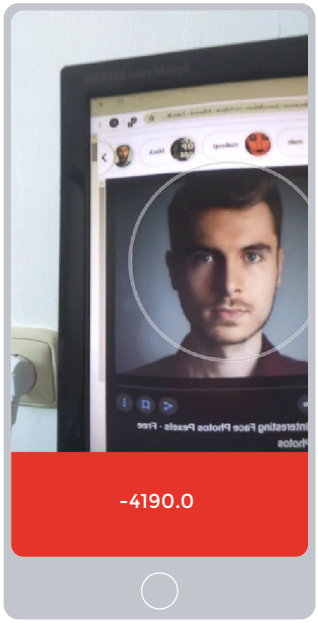
With passive liveness check, the onboarding can be shortened even further. Its speed comes in handy e.g. when repeated identity verification is necessary, such as making transactions over certain threshold.

It should be noted that no special technology is necessary for pas-sive liveness check, all it needs is a smartphone camera. Although some smartphones contain 3D, stereoscopic or IR cameras that would be useful for reliable live-ness check, they are far from in-dustry standard. In retail sectors such as banking, telecoms and others, the market penetration of a given technology is directly proportional to the adoption of onboarding solutions. Until these technologies become household, they can be used for niche, spe-cialized uses only.



Active: Follow a random-moving dot while camera checks for eye movement.





Passive: Passive Liveness Check can distinguish a real face from an image even without user interaction.

We combine both

The combination of both types of liveness checks in a single solution gives the client unique advantages.

- The client can choose which one of the checks to use: active liveness check is more conspicuous, which is useful in some cases, as it gives user reassurance of the safety of a given app (e.g. in finance).
- Passive liveness check can be run more often during events requiring extra security, while active liveness can be used only during onboarding (e.g. confirming larger transactions or verifying user identity in remote signing process).
- If one of the checks proves repeatedly inconclusive, the other one can be deployed (useful e.g. for clients with eye movement disorders).
- Combining both approaches gives extra security to onboarding process.
- The clients have full discretion over how the checks are deployed according to their risk management profiles and their desired user interaction.

The integration with internal risk management systems goes even deeper with DOT Trust Server component. This module transparently communicates all the scores gathered during the onboarding.

This level of granularity instead of just simple yes/no answer allows each client to set up accept/reject thresholds according to their own risk appetite. If the application is at any point less certain of identity of a user, it can trigger a passive liveness check or verification procedure. On failure, it can reject a transaction and send an image or notification to the central system of a client.

So far, no other provider in biometric industry provides both types of liveness checks in a single package. This gives clients with requirements of extra security and thorough ID verification an ability to implement both and deploy them as necessary according to differing risk scenarios, both increasing security of the user and improving the risk profile of the client.

Is video call the ideal solution?

To properly check liveness and verify identity, many institutions still use video calls. While reliable and extremely difficult to spoof against the most common attacks, they have several drawbacks.

First, AI-powered face recognition is already more accurate than a human even under a variety of conditions that a live call from different smartphone models provide.

Second, it requires a human operator, which is expensive. If a company wants to be truly digital and operational 24/7, the video call center has to be equipped for such service. In effect, the enrollment can be costly.

Third, the video call model is difficult to scale. Once the company outgrows its initial stages, it will need to increase its video call capacity, and fast, which is again costly. Outsourcing is one way to handle the capacity bottleneck, but at the cost of giving up full control over the process.

The Technology Behind Liveness Checks

Both the passive and active liveness checks have been developed internally by Innovatrics R&D team, which specializes in image recognition technologies.
They use deep learning and convolutional neural networks to analyze large image datasets for patterns that can tell that a given image is alive or not. Thanks to the internal character of both approaches, they are under full control of the company and are being further improved all the time.
We use neural networks in many other areas, such as optical character recognition (OCR), where they help read ID documents extremely quickly and accurately. **Both our liveness checks can run completely on-device** with the same accuracy and speed as our server-based solution. Utilizing the power of neural networks compressed into a lightweight mobile component, our clients can benefit from the top-performing facial recognition algorithm in the same way as having our server-based solution in place.

How it works

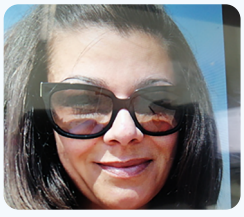
1. Active liveness

- The training data set contain eyes looking at different directions, so the neural network learns where the eyes are looking at
- During the active liveness check we display a dot at different positions of the screen and take pictures of the users' eyes
- The neural network then evaluates whether the eye movement corresponds to the dot movement

2. Passive liveness

- The training set contains many different spoof vectors: printed photographs, printed masks, screenshots from mobile or PC screen
- The training set also contain many genuine photos of a person
- The neural network is trained to distinguish whether a provided picture is e.g. a photo-captured screen (moire effect, reflections), printed paper (reflections) or a real photo

Printed paper (reflections)



Captured screen (moire effect, reflections)

Real photo

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. For over 15 years 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

Taiwan (R.O.C.)
+886 2 7741 4036

Slovakia (HQ)
+421 2 2071 4056

Singapore
+65 3158 7379

USA
+1 404 984-2024

© 2020. Innovatrics. All Rights Reserved.