WHITEPAPER

THE IMPORTANT ROLE OF LIVENESS DETECTION IN FACE BIOMETRIC AUTHENTICATION

AND HOW TO CHOOSE THE RIGHT ONE FOR YOUR USE CASE

IDR&D

In order for face biometrics to truly gain mainstream adoption as a better mode of authentication, it is essential to distinguish between a genuine live face and an attempt to spoof the system with an artificial representation of a face. Automated detection of presentation attacks, and specifically liveness detection, has become a necessary component of any authentication system that is based on face biometric technology where a trusted human is not supervising the authentication attempt.

This paper discusses the need for liveness, how it works, and approaches.

INTRODUCTION

Face biometrics is rapidly gaining acceptance with consumers and businesses alike as a convenient and secure method of identity verification. The technology closes security gaps that are frequently exploited in solutions that rely on something that can be lost or stolen, such as a password or the answer to a "secret" question, as well as new hacks such as SIM card fraud. Simply showing one's face for a selfie is also far less frustrating for users.

Face recognition technology has advanced dramatically in recent years with advancements in artificial intelligence, the widespread availability of high quality yet inexpensive cameras, and the subsequent creation of a huge amount of publicly available data for training face recognition algorithms. Continuous improvements in computational power, including graphical processing units (GPU) and their availability, have made it possible to apply sophisticated machine learning algorithms such as Convolutional Neural Networks and Deep Neural Networks to these systems and run them in everyday devices. In addition to being highly accurate, today's algorithms are fast enough to be implemented in large commercial authentication systems – even those with multiple millions of users.

Offering the ability to strengthen security and improve the user experience, face biometrics has found its way into use cases ranging from unlocking mobile devices, to securing financial transactions and health records, to improving digital onboarding processes.

ALTHOUGH THE POPULARITY OF BIOMETRIC AUTHENTICATION CONTINUES TO GROW, THE TECHNOLOGY IS NOT IMMUNE TO VULNERABILITIES THAT CAN BE TARGETED BY FRAUDSTERS IN THE DIGITAL ERA.

Real-life applications of facial biometrics for authentication raises the question of security. If a potential fraudster can easily access a representation of a person's face and present it as their own, can we rely on this method of authentication?

In order for face biometrics to truly gain mainstream adoption as a better mode of authentication, it is essential to distinguish between a genuine (bona fide) live face and an attempt to spoof the system with an artificial representation of a face. Thus, automated detection of presentation attacks, and specifically liveness detection, has become a necessary component of any authentication system that is based on face biometric technology where a trusted human is not supervising the authentication attempt.

Liveness also addresses the fear that our biometric data may be compromised – and unlike a password, our biometrics cannot be "reset." Encrypted biometric templates by nature are of little to no use if stolen, and the best practice is to store these templates separately from any Personally Identifiable Information (PII). But the reality is that our biometric data is already out there for the taking. Even if you don't have a profile on Facebook or post any pictures of yourself, your image can most likely still be found online. This is another reason why liveness detection is critical. By integrating liveness detection with facial recognition, we can render our biometrics useless to imposters.

IN THIS PAPER WE EXPLORE THE CRITICAL IMPORTANCE OF LIVENESS DETECTION WHEN DEPLOYING FACE BIOMETRICS FOR AUTHENTICATION, INCLUDING BEST PRACTICES AND SPECIFIC USE CASES.

HOW LIVENESS DETECTION ENABLES TRUST IN FACE BIOMETRIC AUTHENTICATION

When it comes to using face biometrics for authentication, accuracy and performance are no longer a concern. However, the threat of spoofing has evolved from theoretical articles and lab experiments to real-life attacks that impact businesses, customers, and their money. Detecting spoofs is essential for face biometric matching to be trusted.

Whereas facial recognition for authentication can accurately answer the question, “Is this the right person?”, it doesn’t answer the question, “Is this a live person?” This is the role of liveness detection.

COMPREHENSIVE BIOMETRIC AUTHENTICATION MUST ANSWER 2 QUESTIONS:

1. IS THIS THE RIGHT PERSON?
   (BIOMETRIC MATCHING)

2. IS THIS A LIVE PERSON?
   (LIVENESS DETECTION)

LIVENESS DETECTION EXPLAINED

Facial recognition works by comparing mapped features of an enrolled user — like the distance between their eyes or length of the jaw line – to a biometric template in order to verify identity. It examines the image it sees and makes measurements. What it does not do is recognize the physical presence of a user vs a quality print or digital representation. ***A photograph or image on a screen works just as well as the actual person!***

When using face biometrics for authentication, a bad actor can exploit this limitation to trick the system into thinking it sees the authorized user. We call this a presentation attack and these attacks have become easier for fraudsters due to ready online access to high-definition photos, screen images, masks and videos that can be used to spoof a facial recognition system.

Liveness detection works with a biometric system to measure and analyze physical characteristics and reactions in order to determine if a biometric sample is being captured from a living subject who is present at the point of capture. The technology doesn't perform any matching functionality, but instead detects presentation attacks. These include:

PHOTO OR VIDEO ATTACK

Fraudsters gain access to a photo or video of the authorized users. This can be as easy as performing a simple Google search or visiting an individual's social media account. The fraudster can use the printed image to create a 2D mask.

DEEPFAKE

Fraudsters take either a photo or video and, through editing with animation software, create a realistic version of the individual talking and nodding their head.

MODEL OR 3-D MASK

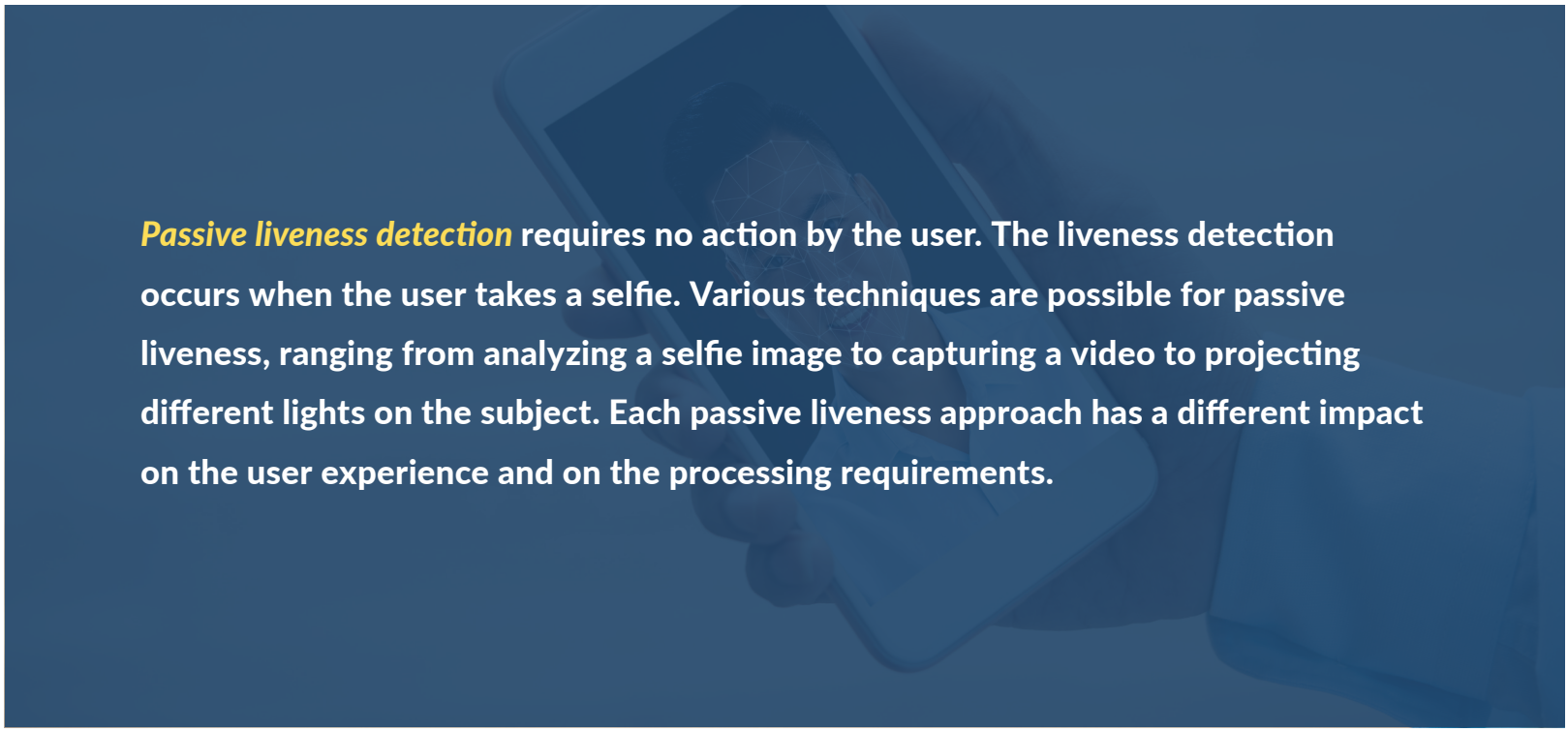
Fraudsters invest in three-dimensional masks or custom models that mimic an individual's physical likeness.

APPROACHES TO LIVENESS DETECTION - PASSIVE VS ACTIVE

A variety of approaches exist to detect liveness. At a high level, these can be classified as active or passive:

Active liveness detection **requires users to participate in the liveness check by responding to a challenge. Examples of systems deployed today include the following:**

- **Nodding or turning one's head from side to side**
- **Blinking**
- **Following a dot on a screen**
- **Smiling**
- **Speaking a series of words or numbers**
- **Moving the camera toward one's face or leaning into the camera**
- **Recording a short video**



Passive liveness detection **requires no action by the user. The liveness detection occurs when the user takes a selfie. Various techniques are possible for passive liveness, ranging from analyzing a selfie image to capturing a video to projecting different lights on the subject. Each passive liveness approach has a different impact on the user experience and on the processing requirements.**

PASSIVE OR ACTIVE: WHICH IS BETTER?

To understand the right type of liveness for you, the next section examines active liveness compared to passive liveness, followed by an explanation of the different types of passive liveness.

	PASSIVE LIVENESS	ACTIVE LIVENESS
USER EXPERIENCE	Requires no action by the user, resulting in lower abandonment and usually less time and effort.	Requires users to respond to "challenges" that add time and effort to the process, and are impractical for use cases with frequent face biometric matching, such as logging in. Companies report abandonment rates as high as 50% for active liveness.
SOFTWARE REQUIREMENTS	Some methods require installing a software component on a device first; others do not.	Usually requires installing software on the device, a problem for use cases such as remotely onboarding new customers in advance of downloading a native mobile application.
IMAGE ANALYSIS	This varies depending on the approach. May be based on a single image with processing in near real time.	Requires analysis of multiple frames of video to detect the requested movement.
BANDWIDTH REQUIREMENTS	Low based on the use of a single image or analysis. May use the same image taken for facial recognition, resulting in no incremental traffic to the server.	May require more data to be exchanged between the user's device and server-based solution, which is often a problem in areas with slow internet speeds.
SPEED	The speed of performing a passive liveness check varies depending on the method.	Active liveness always increases user effort, resulting in a longer liveness check.
ROBUSTNESS TO SPOOFING	Passive methods are generally more immune to spoofing, offering "security through obscurity" whereby the fraudster does not have clues as to how to defeat the liveness check.	Active systems provide fraudsters with information on how to attack and defeat the liveness check. Nearly all have known techniques to break them, such as using a simple 2D mask with cut out eyes and animation software to mimic head movements, smiling, and blinking.
PROVEN COMPLIANT WITH ISO 30107-3 STANDARD FOR ROBUSTNESS	Two solutions are certified compliant	Two solutions are certified compliant.

From nearly every vantage point, a passive solution with proven, measurable robustness is preferable to an active solution. Why provide clues to fraudsters, why suffer from abandonment, and why force a user to spend extra time and effort when a passive solution offers security and a user friendly experience?

PASSIVE VS. PASSIVE: WHAT'S DIFFERENT?

Not all passive solutions are the same. Four known variations follow:

- **Shine varying lights on the person to create different exposures and ensure a live face**
- **Capture short video to detect micro-movements**
- **Examine the same selfie image as the image used for face matching**
- **Use a hardware-assisted approach (e.g. depth measuring)**

PASSIVE APPROACH	PROS	CONS
SHINE VARYING LIGHTS	• Passive because the user does not need to move	• The user must hold the device steady • The process takes time • The approach fails in bright sunlight outdoors • Users may find the light flicker to be annoying
CAPTURE A SHORT VIDEO	• Passive because the user does not need to move	• The video takes time to capture • The video may require downloading software to the device beforehand or sending large amounts of data to a server • Passive observation relies on micro-mimics and small movements, which may be hard to capture
EXAMINE A SINGLE SELFIE IMAGE	• Requires absolutely no extra effort • Minimal data size because only one image is needed, not a video stream • Fastest speed of processing	• Requires a server-side component
HARDWARE-ASSISTED APPROACH (E.G. DEPTH MEASURING)	• Requires absolutely no extra effort • Acceptable data size because only a few images are required • Fast speed of processing	• Requires expensive and specific hardware on the client side (e.g. camera with IR and/or depth sensor) • Requires a server-side component • Uses more CPU power for processing

WHICH APPROACH IS BEST?

Passive liveness detection is clearly preferable to active. The approach closes security gaps in face biometrics without adding friction back into the authentication process and doesn't require users to be educated on the process.

Of the possible passive approaches, a single selfie image is preferable to the other options. However, in any case, choose a passive approach that is also ISO 30107-3 compliant.

USE CASES FOR LIVENESS DETECTION

Facial liveness detection combined with face biometrics provides powerful identity proofing and authentication whenever an application needs to verify a person's identity without a trusted human supervising the face matching process. Use cases include:

DIGITAL ONBOARDING FOR NEW CUSTOMERS AND ACCOUNTS

Enabling new customers to sign up for an account on a mobile device or computer instead of going to a physical location greatly increases the opportunity for businesses to acquire customers. An important step is "identity proofing" – the process of proving a person's identity before they set up an account. This typically requires the customer take a photo of a valid identification document, such as a passport, take a selfie image, and then submit the two items to a system that checks the validity of the document and matches the photo ID to the selfie. Liveness is critical to ensure that the person in the selfie is real and not a manufactured identity. Identity proofing is now regulated by government entities in most parts of the world as necessary for a "Know Your Customer" (KYC) process.

SECURING THE DIGITAL CUSTOMER

Any time that a digital channel, such as a mobile app, chatbot, or virtual assistant, uses face biometrics to authenticate a user, checking for liveness is critical. Passive liveness is especially critical to remove friction in the user experience so that authentication is fast, easy, and secure.

MULTI-FACTOR AND "STEP UP" AUTHENTICATION FOR PAYMENTS

As payments increasingly occur away from retail locations, the risk of fraud increases in turn. Face recognition with passive liveness provides the perfect second or third factor for higher risk payment transactions, shoring up vulnerabilities that might occur through SMS spoofing, SIM-card swaps, and other fraud attacks that compromise possession of the mobile device as a factor.

CARDLESS ACCESS

Self-service kiosks, terminals, ATMs, and entry systems often rely on cards or tokens, sometimes combined with PIN codes, as the means of accessing a system. These systems are easily compromised by theft of the card and knowledge of the PIN code. An additional factor is face recognition, but because no trusted human is there to supervise, liveness is critical. Passive liveness provides a superior solution as a fraudster has no idea that the liveness check is happening. And users no longer need to carry tokens or cards. A face, a liveness check, and optionally a PIN are all that are necessary for authentication.

WHICH LIVENESS DETECTION SOLUTION IS RIGHT FOR YOU?

FOLLOWING IS A SUMMARY OF CONSIDERATIONS WHEN EVALUATING TECHNOLOGIES:

SIMPLICITY

We've already touched on the differences between passive and active facial liveness and why the team at ID R&D believes that a passive solution is superior at balancing performance and the user experience. Find a solution that provides high security without causing frustration, which leads to abandonment and loss of customers.

ENVIRONMENTAL FACTORS

In general, liveness detection operates in the same conditions as a facial recognition system. Current liveness algorithms support varied lighting – from daylight and twilight to indoor and outdoor scenarios. Quality control functions should be in place to restrict liveness detection when there is no lighting, or an image is too blurry. For high-risk access, companies may consider step-up security using another biometric modality or authentication factor when face recognition/liveness conditions are poor.

CROSS CHANNEL COMPATIBILITY

Is the solution compatible with all mobile devices and desktop applications - whether on-device, in the cloud or server based?

When a solution will be used by customers with a variety of devices, it's important that the liveness check works universally across channels and is agnostic to the device make/model as long as it meets minimum criteria. The technology should support any device with an HD camera that is capable of taking a selfie at a resolution of at least 720px. As an example, the iPhone5, released in 2012 met this criteria and today's cameras are in the megapixel range.

EASE OF INTEGRATION AND DEPLOYMENT

Prevent lock in by choosing a liveness solution that can integrate with any third party face biometric solution. Also understand deployment options, which can range from cloud-based only to on-premise or private cloud. Ensure a vendor's options meet your business' requirements for data access and storage.

THIRD PARTY TESTING

iBeta Quality Assurance is the industry leader in biometrics testing and is the only biometrics testing lab accredited by the National Institute of Standards and Technology (NIST) under the National Voluntary Laboratory Accreditation Program (NVLAP). iBeta provides Presentation Attack Detection (PAD) testing conducted in accordance with ISO/IEC 30107-3.

During testing systems undergo thousands of presentation attacks. A Compliant solution (previously called "Certified") must detect 100% of the attacks.

iBeta offers Level 1 and 2 PAD testing. ID R&D is iBeta PAD Level 1 Compliant, having earned a perfect score and will soon undergo Level 2 testing.

Third party testing is an important consideration in validating a vendor's claims but should not take the place of internal testing and due diligence.

SUMMARY

Face biometric technology offers the ability to authenticate customers in a user-friendly way and at the same time strengthen security. But even the toughest solutions are susceptible to spoofing attacks using high-resolution images, video, masks, and deepfakes. Overcoming these challenges has introduced a level of friction for customers that is frustrating and a deterrent to successful biometric adoption.

Passive liveness detection closes security gaps in face biometrics without adding friction back into the authentication process. The technology works quickly in the background and doesn't require users to be educated on the process.

Lowering customer effort is a top priority for most businesses. When implementing liveness as part of a face biometric system, it's important to consider how the solution impacts the user experience. Will it slow users down, cause confusion or increase abandonment rates? In addition to user experience, there are other considerations such as software requirements, impact on speed, integration complexity, deployment options, solution robustness – and of course your specific use case.

WITH FACE BIOMETRICS BECOMING MORE COMMON FOR AUTHENTICATING ONLINE AND REMOTE USERS, LIVENESS DETECTION IS HAS EMERGED AS A CRITICAL PIECE OF A COMPREHENSIVE SOLUTION. LEARN MORE AND REQUEST A DEMO AT IDRND.AI

About IDLive™ Face by ID R&D

ID R&D provides IDLive Face, the world's first truly passive facial liveness detection product. IDLive Face works with any third-party facial recognition software and without any additional actions by the user for the liveness step. The technology uses a single shot analysis and doesn't require special capture-side software. It also works across mobile, web and standalone devices.

IDLive has passed Level 1 Presentation Attack Detection (PAD) conformance testing by iBeta with a perfect PAD score and is ISO/IEC 30107-3 compliant.

1441 Broadway, Suite 6019
New York, New York 10018 USA
info@idrnd.net