Yoti MyFace® Liveness

White Paper | Full version

March 2023

Introduction

The growing use of biometric and authentication solutions, online and offline, has raised the risk of 'spoofing' attacks, an attempt to spoof the system with an artificial representation. Therefore, having robust technology to mitigate against spoofing is essential as part of a mix of tools to verify someone. This is true whether that be for verifying age, identity or authenticating a returning customer.

The purpose of liveness is to make sure the person you are verifying is a real person. Liveness does not recognise who the person is (that's facial recognition), and it does not check a face against faces in a database. It is most commonly used in combination with other authentication factors to ensure that authentication or verification isn't being spoofed.

> **"The purpose of liveness is to make sure the person you are verifying is a real person"**

In addition, as is well documented, passwords or PINs can be discoverable, for example via a hack or leak. Biometrics provide stronger security for individuals and businesses, providing they are not spoofed. Spoofing is significantly more difficult to when liveness is incorporated as part of the process.

Liveness combats what is technically termed "presentation attacks". Without liveness, you are susceptible to a presentation attack - these could be:

- Paper image
- Mask
- Screen image
- Video imagery
- Deep fake video
- Injection attacks
- Bot attacks

Genuine customers do not object to efficient and effective security layers. In fact most customers appreciate companies taking the time, effort (and expense) to ensure their assets, accounts, or finances are being looked after and kept safe.

Where can it be used?

Identity Verification - used as part of the verification process to give a high confidence that the check is real.
Why important? - a stolen document plus an image could spoof an identity check.
Example use case - your customer wants to sign up to a new bank account and is required to prove their identity - liveness ensures the person signing up is a real person. Liveness is used in combination with data extraction, document authenticity and face match for a secure verification process.

Age Verification - ensuring the person is not only the right age but also not attempting to spoof the system with a presentation attack. This could be used online or offline (for example, at a supermarket self-checkout).
Why important? - to strengthen age verification and provide quick, privacy-preserving age checks.
Example use case - a shopper uses facial age estimation at a supermarket self-checkout. Liveness prevents someone from attempting to use a picture, mask or other spoofing attack to pass an age check. For online applications, it ensures industries, such as gaming and social media, know the person proving their age is a real person.

Digital ID - to create a reusable Digital ID we require a high level of confidence to determine: the document data extraction, document authentication, the document belongs to that person and finally that the person is real.
Why important? - pre-verified, reusable Digital ID can only be used with confidence with the highest level of security.
Example use case - A returning customer can easily access their account, and the business can be confident the customer is who they say they are.

Authentication - liveness can be an additional form of authentication for high risk / regulated environments, adding an extra layer which is makes it harder for spoofers to scam.
Why important? - multi-factor authentication is now required by many regulators and an efficient, low friction way to do this is actually desirable for customers.
Example use case - a genuine customer is accessing their account, or changing important information such as their bank details. A simple liveness check can add an authentication layer with low friction - key for sensitive account changes and to help prevent account takeovers.

Bot Detection - checking for liveness when capturing a face helps prevent bad actors from submitting hundreds or thousands of synthetic faces, or genuine, but unconsented faces.
Why important? - the financial and reputational cost to businesses from bot attacks can be significant.
Example use case: dating app Muzz uses liveness to confirm every account profile belongs to a real person.

Types of liveness - active and passive

Active liveness requires the user to present their face on camera and then follow one or more instructions during a check; for example, moving toward and away from the camera, or repeating random words. Then AI is used to complete the check.

This can create issues for some users, for example the words may not be in their native language, and adding movement to the check increases the margin for error. Additionally, not all individuals follow instructions carefully.

In general, the simpler the instruction and the less user time required, the better the user experience and completion rate. Passive liveness takes between on average 1 second, with active liveness taking between 15-20 seconds.

Passive liveness doesn't require any action from the user and works from a single selfie. Users no longer have to undertake head or hand movements to prove their 'liveness'. This reduces friction for users. It is simpler for people with accessibility needs and so more societally inclusive. This reduces drop off and speeds up the journey to verifying genuine customers.

	Passive	**Active**
User feedback	Instant feedback	User has to wait for video validation
Time to complete	1 second average	15-20 seconds
Complexity and accessibility	Take a selfie - this can be either at the click of a button, or using auto-capture.	User has to record a video and maintain the correct position for the duration. Language, audio input and noisy environments can be a problem for some users.
Permissions	Camera access	Camera & audio record
Network traffic	Upload a selfie	Upload a selfie & video

A comparison between passive and an example active video liveness

Yoti MyFace® proprietary liveness

Yoti MyFace® is a passive liveness software that uses a selfie image to detect presentation attacks. It doesn't require any action from the user and just works from a selfie, which is processed through a sequence of deep neural networks.

The network has been trained using a variety of models that analyse images in a different way. We have invested considerable time and effort to fine tune these models to optimise how they work together to create world class performance.

As an example, one of these models, for which we have requested a patent, uses 3D and 2D images as input to produce a model that can detect depth in a 2D image.

How it works

1. The user captures a selfie, either by;
    a. Auto-capture: we use face detection to ensure the image captured has the right amount of visibility - the user must generally just be attentive to the screen.
    b. User capture: a guided frame to capture the image at the touch of a button.

2. The image is cropped many times to produce the inputs for the relevant neural network models and is then processed using multiple models.

3. Results from each model are assessed together to produce a response and a confidence level that the image is of a real person.

4. A response is returned on average in 1 second, with the confidence level. Relying parties are able to configure their checks to pass only above a given confidence level, depending on their risk profile and regulatory requirements of the territories in which they operate.

MyFace® performance - true positive and true negative rates

We measure performance in terms of true-positives, and false-positives, success rates and completion times.

- When our model predicts that a real image is real, that is a true-positive (TPR).
- When our model predicts that an attack image is real, that is a false-positive (FPR).
- The aim is for a high true-positive rate, and a low false-positive rate.

Taking in combination the ease of access, time to complete, immediate feedback and ease of use, passive liveness significantly improves success rates.

On mobile phones, 90% of first attempts are successful, 97% after 3 attempts, at 1% FPR, 90.5% TPR

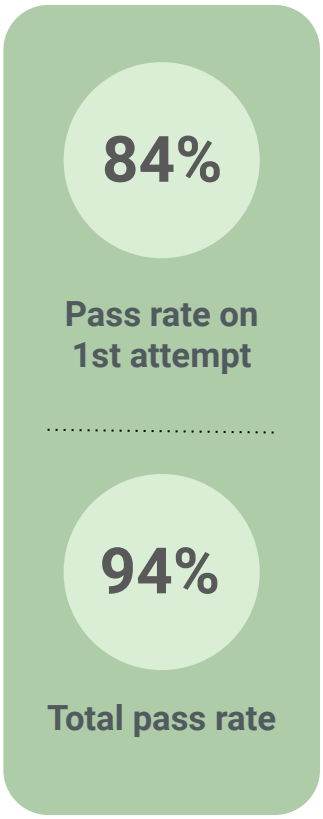
MyFace® performance in live environments

We have been using MyFace® in our facial age estimation solution, alongside other liveness providers.

We perform liveness across a variety of environments and applications. Performance is influenced by camera quality, image size, and environmental factors.

For example, during the Home Office trial in supermarkets in the UK, we were able to gain further intelligence on how the use of our technology on self-checkouts can be adversely affected by factors such as sun glare, overhead lighting and camera positioning in the self checkout.

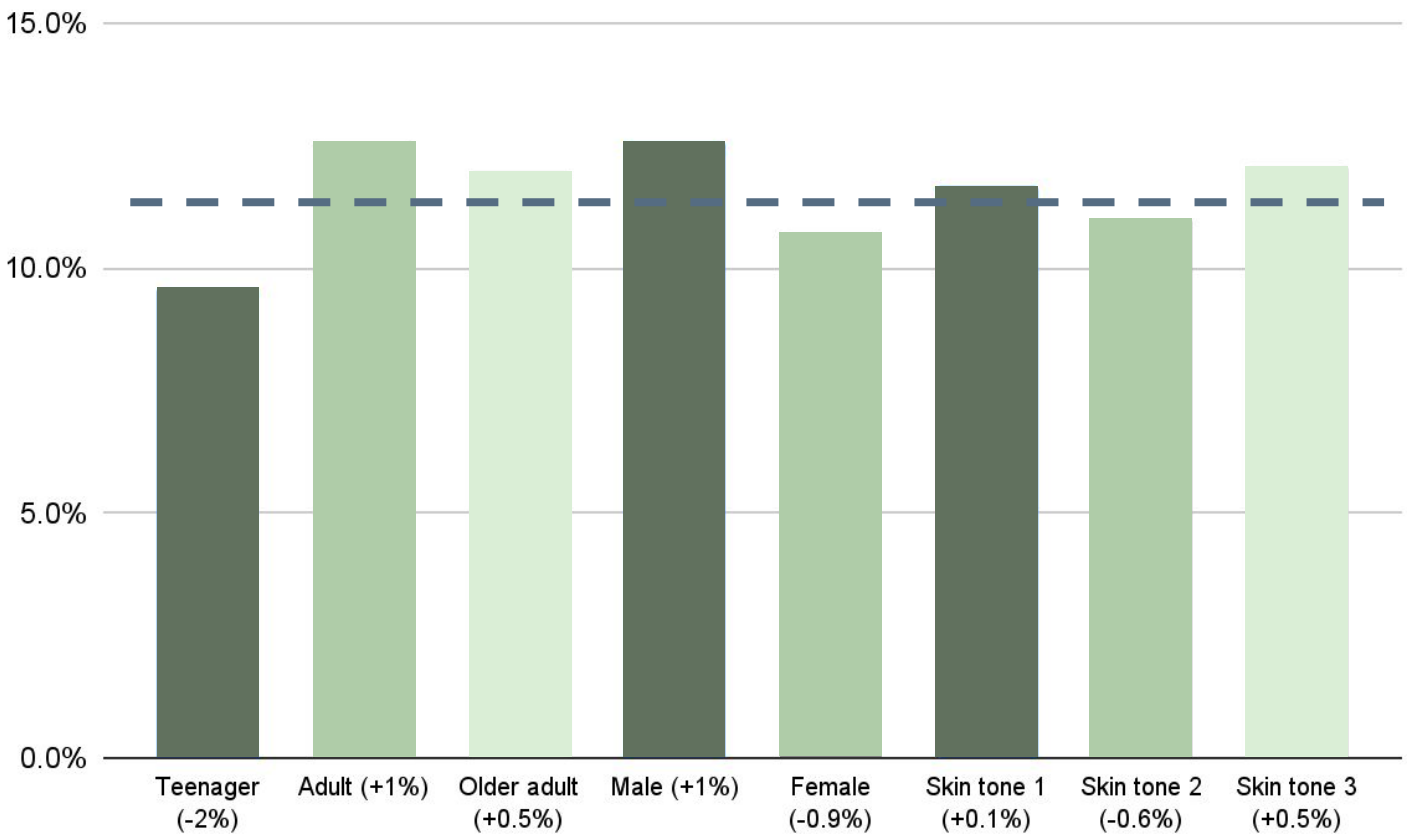
This also explains the discrepancy between the mobile only first attempt rates of 90%, and our live environment figures of 84%. Compared to laptop cameras and self-checkouts, mobile phones tend to have a high quality camera and users are used to taking ‘selfies’ on their phone.



Testing for bias

To test for bias we use Bona Fide Presentation Classification Error Rate (BPCER). BPCER is the percentage of real presentations assessed as a false positive, that is, incorrectly classified as a presentation attack.

Our mean BPCER across the dataset is 11.6%. Using this datapoint we can analyse the bias by age, gender and skin tone, with the dotted line representing our mean BPCER.



As this shows, our bias is relatively even across all measures, especially skin tone. The fact that teenagers have a lower rate against other ages may be due to our proprietary training data skew towards a younger audience.

Skin tones

For skin tone, our research team tagged the images using a scheme based on the widely used Fitzpatrick dermatological scale. Fitzpatrick uses six bands, from Type I (lightest) to Type VI (darkest). For the present, we present our data in three bands (based on Fitzpatrick Types I & II, Types III & IV, and Types V & VI).

Skin tone scale

Third party testing: NIST levels 1 and 2

NIST is the National Institute of Standards and Technology (NIST), a non-regulatory agency of the United States Department of Commerce. NIST provides a framework for testing performance levels of liveness.

NIST Level 1 involves testing against materials that could be found in a normal home or office. Materials used for testing should not cost more than $30. Masks are excluded.

To pass NIST Level 1, the Liveness service must detect every attack and limit false negatives to less than 15%. We were tested with over 900 attacks and our tested MyFace® model was not allowed to have one false positive.

In February 2022, MyFace® achieved NIST level 1 certification with 100% attack detection rate. We worked with iBeta, a NIST NVLAP accredited biometrics testing lab, for our level 1 compliance.

NIST Level 2 involves testing against more expensive, specialist attacks, such as 3D printers, and resin or latex face masks. Materials used for testing should not cost more than $300.

To pass NIST Level 2, the service must detect 99% of attacks and limit false negatives to less than 15%.

In February 2023, MyFace® achieved NIST Level 2 compliance, again working with iBeta, with 100% attack detection rate.

Yoti memberships, associations, accreditations & awards

To learn more about Yoti MyFace® liveness solution please **get in touch**.