FaceTec PAD Testing Methodology

A Detailed Look At Human Liveness & 3D Depth Detection

Updated April 11th, 2020

www.FaceTec.com
1707 Village Center Circle, Ste 200
Summerlin, NV 89134, USA

©2020 FaceTec, Inc. All Rights Reserved.

Overview

FaceTec tests liveness and 3D depth detection AI in a state-of-the-art spoof lab and R&D center in downtown San Diego, CA. In addition to the many decades of biometric experience among the development team and advisory board, FaceTec has five years of experience testing its own technology against many other Face Matching systems. These rigorous tests have led to a unique understanding of the challenges of detecting 3D depth, human liveness and have proven FaceTec to be unmatched in the market.

This document provides 3rd-party testers, customers, strategic partners and users insight into the methodologies, test cases and tools used to create FaceTec's AI and to test it against all types of real-world attacks. It also explains FaceTec's philosophy around Presentation Attack Detection (PAD), Artificial Intelligence (AI) and the critical features of face authentication systems in general.

Third-party testing is the most important validation any biometric authenticator can have. FaceTec was tested in August 2018 and is the *first and only* biometric to achieve a **Level 1 & 2** rating in the NIST/NVLAP-certified iBeta Presentation Attack Detection (PAD) ISO 30107-3 Certification Test. Over **3,300 spoof sessions** utilizing hundreds of high resolution photos, videos, 3D Mask and Dolls were attempted over the twelve days of iBeta testing. **No spoof attempts were able to fool the system and FaceTec achieved a perfect 100% anti-spoofing score in both tests.**

iBeta PAD Certification Executive Summary:
https://www.facetec.com/wp-content/uploads/2018/08/FaceTec_iBeta_PAD-Level-1-Letter.pdf
https://www.facetec.com/wp-content/uploads/2019/02/190204_FaceTec_PAD_Level_2_Certification_Letter.pdf

Bad Actors & Cooperative Users

The ISO 30107-3 Standard stipulates that a PAD system must thwart a "fully cooperative user" and be tested with spoof artifacts escalating in sophistication.

A cooperative user is defined as one who is willing to provide *any and all* biometric data that he/she possibly can to facilitate an attack.

Cooperative users may perpetrate fraud themselves, they may be working complicity with other bad actors, or they may have had their biometric data phished by them. Most legacy 2D biometric systems cannot defend against cooperative user attacks at all, because anyone with a copy of a fingerprint, voice recording or a photo slideshow simulating blinking eyes can spoof their systems.

FaceTec was designed to prevent external bad actors, complicit users, and even cooperative testers from presenting the necessary concurrent biometric data that could spoof the system. It is our belief that if liveness detection is capable of reliably preventing a fully cooperative user/tester

©2020 FaceTec, Inc. All Rights Reserved.

from spoofing the system, even with unlimited access to their own biometric data, that such a system becomes truly secure. FaceTec has achieved the security level required to replace passwords, while also not risking a Biometric Honeypot, a goal all other biometric vendors have failed to accomplish.

Spoof Modalities / Presentation Attack Types

When testing liveness and depth detection, it is important to consider the various categories of presentation attack types that can be presented to the system. For the purposes of testing, each general category of attack should be considered a different spoof modality. Each modality has many sub-modalities derived from the dimensions present within that specific type.

Consider a “simple” modality like a printed photo. Following are some examples of dimensions within testing liveness detection of a printed paper photo presentation to the system:

- Low resolution through high resolution images.
- Matte, glossy, or other types of paper (or even non-paper, like plastic and more).
- A full sheet of paper or a cutout separated from the background of the original image.
- Eyes, nose or mouth cut out and held in front of a real person’s face or 3D bust.
- Bent, crumpled or curved photo presented to the system.
- A single face created from multiple, different people’s photos.
- Source faces could have been created in different lighting conditions, and with glasses, facial hair and various expressions.
- Different devices running the target technology (i.e. FaceTec), exhibiting different:
    - Camera intrinsics
    - Performance/speed characteristics
- Different testers attacking, exhibiting differences in usage and behavior, & much more...

Most of the above dimensions can be combined with one or more additional dimensions. The possibilities that are created by combining each dimension of the “printed photo spoofing problem” presents an essentially unlimited set of test cases for even this single spoof type!

Computer Vision, AI and Combinatorial Explosions

Testing a broad set of the spoof combinations is critically important. AI algorithms can be “black boxes” to some extent. Even simple, well-known, well-researched algorithm pipelines trained to do tasks like classifying “photo vs. a real human subject” using texture information has many caveats.

©2020 FaceTec, Inc. All Rights Reserved.

For instance, what is a “photo”? As we saw with the various spoof sub-modalities, it can be printed on many different types of paper with different textures, glossiness and reflectivity. A change like eye holes cut outs can present a completely different class of spoof from the perspective of the algorithm. Taking it another step deeper, if a live subject is added behind the paper and is blinking his/her eyes, another new sub-modality is born.

In Computer Vision (CV), every real-world capture is different. Even if you attempt the same spoof twice, there are changes in the lighting and scene, and at the pixel level changes in positioning occur. Thus, the process of testing all viable dimensions and submodalities must be done over as many people and the broadest possible set of real-world data to be able to generalize well. It can take months just to gather the data necessary from several hundred or thousand people to train the algorithm on just one subset of one spoof modality.

The key takeaway is that changing one small variable can make the difference between easily detecting a spoof and fooling the system. **With so many combinations to test, it is of utmost importance to test the breadth in addition to depth.**

Computer Vision+AI pipelines fail to catch spoofs due to four main causes, each explained below by example, and as they relate to face authentication technology:

1. Underfitting

Example: the anti-spoof algorithm is trained against a diverse combination set. Though broad, it only has a few hundred or thousand of each type of sample to learn on. While the algorithm generally performs well in training and testing, it will randomly fail simply because it has not learned enough about the general problem space.

2. Overfitting

Example: the anti-spoof algorithm is trained against a very rich set of every combination of the above sub-modality bullet points. The dataset is rich and large. However, through some data science/analysis oversight, it only includes one skin tone in the subjects in both the spoof and real records. The algorithm is highly likely to have undefined (and poor) behavior for differently skin-toned subjects, both spoof and real. The algorithm fit really well to the data present and is highly accurate, but doesn’t generalize to the **actual** problem space in the real world.

3. Inherent inability to classify due to limitations of the chosen learned feature

Let’s say the liveness algorithm bases its classification specifically on changes in the eye or mouth region. Let’s say it looks for a blink or for movement in the eye. This algorithm can be highly accurate at performing this measurement. Thus, while it is great at analyzing the designed “feature space” it focuses on, it is not capable of seeing the difference between a real human vs. a video of someone talking and blinking, and thus will create a huge security problem in the real world.

©2020 FaceTec, Inc. All Rights Reserved.

4. Inherent inability to classify due to lack of data in the modality
An extreme example: In an algorithm that uses a photo resized to a 2x2 pixel image, real human faces are going to be practically impossible to distinguish from spoofs. You only have 2 * 2 * (number of colors in color space) values with which to learn how to separate. A 640x480 image or even higher is quite a bit more data. Algorithms can definitely be created using a single 2D image that are better than a coinflip for a significant amount of spoofs. Adding processing and averaging over more frames from a video can make it better. FaceTec operates on an average of 100 or more high resolution frames per session, and measures the user's face's 3D signature as the camera is at different distances from the face. This incredibly rich signal offers orders of magnitude more data with which to learn off of over 2D images or even streams of 2D images at a specific distance.

In the above, we have illustrated why it is critical to test on vast, diverse sets of data, and to combine various concepts within each sub-modality to attempt to find ways to bypass the system.

FaceTec has collected massive amounts of 3D face data from users of all ages, genders and ethnicities in the wild with varying light conditions and backgrounds from 160-plus countries. FaceTec has developed AI to address these three problems and has designed an extensive Computer Vision+AI pipeline to address all of the above challenges.

Attacks Against Non-3D Tech

The vast majority of FaceTec competitors cannot derive a 3D signal. They will use "active" techniques like face movements, blink eyes etc., to try to make spoof determinations. This does *not* address the cooperative bad actor described in ISO 30107-3 and leaves vulnerable several attacks, including but not limited to:

- General high resolution images on paper and screens
- High resolution paper images particularly on matte paper
- High resolution paper images on matte paper with eye cutouts and blinking, or other simulated face movement.
- Glossy paper can create artifacts that can interfere with texture detection algorithms
- Videos where a subject moves their face, talks, etc.
- Animated 3D avatar from photo software like Crazy Talk 8
    - https://youtu.be/pAoTmlqMqjg
- Tech that relies on eye gaze detection is generally inaccurate and thus will have a high FAR and can also be spoofed by software that allows manipulation of eye gaze in real time.
- Many more, depending on the liveness detection method

©2020 FaceTec, Inc. All Rights Reserved.

Certain FaceTec competitors will require the subject blink or smile to “prove” liveness. These can be spoofed via trivial means like:

- Creating an image of the subject blinking using Photoshop and fading between images with a slideshow to make it appear as if their eyes open and close (FaceTec has demonstrated this spoof against USAA Bank (tech from Daon - IdentityX))
- Many more, depending on the liveness detection method

Biometric Data Compromise

System Integrators, Identity and Access Management Platform players, and App developers using face matching technology *without* Certified Liveness detection should be extremely concerned about real-world availability of user biometric data.

With today’s technology and social media environment, it is becoming increasingly easy to:

- Find a photo of a target person’s face
- Find a photo of a target person’s face smiling
- Find a photo or video of a target person’s face blinking
- Find a video of a target person
- Find a video of a target person looking directly into the camera making facial movements, blinking, and smiling (i.e. Instagram/Snapchat/etc)
- Create 3D controllable avatars that can be created from a simple photo

The biometric data required for a successful FaceTec authentication is called a “3D Facemap” -- this biometric modality is proprietary to FaceTec. **The FaceTec 3D Facemap cannot be derived from 2D face photos, videos or even a 3D head scans.** FaceTec’s Facemaps are not available in any public or private database from any source and **are not reusable.** The User’s “Liveness Data” is a large percentage of the data in the ~300kb 3D FaceMap, and once the FaceTec Server SDK verifies the User’s Liveness, the “Liveness Data” is deleted from the FaceMap. That FaceMap can only be used for server -side matching in the future, it in now incomplete and can’t have liveness verified again. The User must pass liveness again with a new 3D FaceMap for that to happen. By deleting the “Liveness Data” immediately after verification the FaceTec Server SDK prevents any biometric Honeypot risk, as even if Encrypted 3D FaceMaps were somehow stolen they would not work to impersonate the users.

FaceTec’s algorithms detect Liveness by detecting concurrent unique human traits and identifying generation loss; simply put, they know if they are seeing a real human or a re-created copy. Even if they wanted to, users themselves cannot record the biometric data needed to re-create a 3D Facemap with today’s media technology, because FaceTec has a built-in mechanism to prevent 2nd generation replay attacks.

©2020 FaceTec, Inc. All Rights Reserved.

All of these factors provide a massive security increase for any system that FaceTec is integrated into because users can no longer share credentials (like they can with passwords) and cannot be tricked into providing useful biometric data with phishing schemes or social engineering.

An Important Note About Biometric Data Privacy – When addressing biometric data privacy concerns it is critical to understand the importance of *Liveness Detection*. FaceTec automatically deletes all Liveness Date after each session so it must be recaptured everytime. For a successful login, the correct user *must* be physically present at the time of authentication, they MUST pass liveness detection EVERY time a matching attempt is performed making spoof attempts futile and stolen user media useless.

Liveness & Depth Detection Modes

- Liveness and Depth Detection **During Enrollment**
  - Robust Liveness detection during Enrollment should be mandatory, as proving the reference enrollment is from a real human creates trust at the root of identity.
- Liveness and Depth Detection **During Authentication**
  - Robust Liveness detection during Authentication should be mandatory, as proving the user accessing the account is not just a real human, but also is the ***correct*** real human is essential to establishing trust.
- Liveness and Depth Detection **Without Enrollment or Authentication**
  - Only the users Liveness and Depth are verified, not the identity.
  - This mode can be used to protect against against bots.
  - Deters bad actors as they do not want to use their real face to gain access.
  - A previous enrollment to match the face against is not required in this mode.

General Recommendations for Liveness Testing

- Use as many different faces & photos as possible, not the same ones over and over.
- Attempt as many combinations of sub-modality dimension combinations, variety is critical, do not test the same combinations over and over.
- Run the Face Authentication application on many different spec phones and tablets, not the same one or two different devices over and over.
- Use many different target mediums, devices and materials to present the spoofs, like different monitors, projectors, phones, laptops, types of paper, etc.
- Try to enroll with masks, dolls, mannequins, etc.not only 2D photos and videos.
- Attempt to capture from different angles of the spoof medium.
- Attempt to disrupt the timing of the capture technology.

- Test as many distinct combinations from every modality and its submodality as possible.
- Enrollment and Authentication sessions should not be allowed when the user's eyes are closed for longer than a blink to prevent attacks on sleeping/passed-out users.

Liveness-related Systems and Capabilities

Below is a list of dimensions/features/capabilities that are not directly involved with Liveness Detection, but relate to the system security as a whole.

- **Lockout mechanism**
  - If the technology does not have a lockout mechanism against attackers built in, they will be able to find vulnerabilities quicker because of the opportunity of unlimited attempts and an instant feedback loop (ex., Face ID has no lockout).
  - FaceTec detects repeated spoof attempts and locks out attackers attempting to gain special knowledge about the system, breaking the feedback loop.
- **Speed of enroll/auth/verification**
  - Accessible, intuitive, convenient and secure should be the goal. The technology should not take more than a few seconds after the user successfully frames their face in order to complete processing (and across a broad set of devices).
  - On most devices, FaceTec completes processing within one or two seconds of the user framing their face in the large oval.
- **Enrollment vs. Authentication vs. Liveness/Depth-only Modes**
  - Liveness should not be able to be turned off or its sensitivity turned down.
  - Enrollment must detect liveness and depth for the root identity to be trusted.
  - Liveness/Depth-only Mode is critically important for KYC and onboarding flows. And FaceTec's Liveness check should be performed *before* the ID or passport of the user is scanned. This deters bad actors from showing their faces to the camera and prevents access to the less secure ID scanning portion of the onboarding process.
  - FaceTec performs liveness/depth on every single session, but can be set to liveness/depth-only mode. The app will never receive a "live" signal unless the subject presented is a 3D human present and alive during the session.
- **Performance in Enrollment/Liveness/Depth-only versus Authentication modes**
  - Liveness during enrollment and liveness/depth-only modes should not exhibit significant performance differences from Authentication mode.
  - Enrollment, liveness/depth-only, and authentication modes all perform extremely strong, virtually spoof-proof liveness detection.
  - Note that liveness seen during Authentication is slightly stronger than liveness during enrollment or liveness-only modes. Because a spoof must not only fool the liveness algorithms but *also* perfectly match the user's identity. Authentication

©2020 FaceTec, Inc. All Rights Reserved.

mode should be tested heavily as a part of any testing of the liveness/depth engine which requires enrolling with a live human.

- **Liveness Confidence Score**
    - Liveness Confidence Scores should not provide enough data to enable hill climbing attacks.
- **Ease of integration/integration details**
    - Integration should be straightforward and the developer should not need to become a expert in handling biometric data, android camera compatibility, performance across thousands of devices, etc.
    - While not directly related to liveness, the more the app developer/integrator needs to implement, the more they must become "biometrics experts". We strongly believe this is a difficult, if not impossible, task to achieve at scale.
    - FaceTec handles the user interface, camera compatibility, performance, encryption/decryption of biometric data and tested on over 4000 device models.
- **Open Systems**
    - https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle
    - FaceTec is not open source, but the **technology is wide open** for public testing. FaceTec isn't kept hidden until after you talk to a salesman, we allow anyone anywhere in the world to access and test production level versions.
    - We know that any attacker in the real-world can potentially access our binary using a rooted device and one of our customer's apps, and can try to reverse engineer it. Thus, our system has been designed to remain secure even if an attacker fully reverse engineers our system.
    - More developers are using the FaceTec SDK every day, contributing to the battle-tested nature of our library. By requesting features, reporting bugs and donating data, they are constantly contributing to the self-enhancing ecosystem that increases the security and usability of FaceTec.
    - Very few other biometric technology providers allow instant technology access and evaluation to anyone, especially not competitors, reviewers, reporters and even hackers. FaceTec does.
- **Spoof Bounty Programs**
    - Spoof attacks can come from anyone, and with a little creativity and ingenuity they can beat many of today's best attempts at security. 80% of Fingerprint Scanners were spoofed within 20 tries by a Cisco Security Team.
    - Lab testing is a great prerequisite, but it's expensive and always limited in scope.
    - Public Spoof Bounty Programs offer the best security assurances possible in biometrics. So if a vendor has a persistent and well promoted Spoof Bounty in place for many months they should be trusted far beyond any that do not.
    - FaceTec is the only company with an ongoing Spoof Bounty Program - currently **$75,000** with information available at www.SpoofBounty.com.

©2020 FaceTec, Inc. All Rights Reserved.

Other Important Considerations

Here, we define several other dimensions to face authentication systems that do not directly relate to liveness and presentation attack detection.

- **Package Size**
  - The final size of an app incorporating this technology should not be too large.
  - On iOS & Android, FaceTec adds ~6.7MB to app size, the Web SDK is ~3MB.
- **Device/camera/compatibility**
  - The technology should work on the vast majority of devices that the application's users possess and should also perform well on lower-tier devices.
  - FaceTec is compatible with all modern web browsers on computers with webcams, on smart devices it requires Android 4.3+, iOS 8.3+, and a front-facing camera. There are *no other requirements*. Explicit care is taken to ensure FaceTec is performant and looks consistent across older and lower-tier devices.

Notes on FaceTec Testing Methodologies

- Please see our San Diego "Spoof Lab" video for a visual overview of the spoof modalities, tools, and materials we use on a daily basis to test FaceTec.
  - Spoof Lab Tour
  - Watch FaceTec stop 120 Spoofs in 90 seconds
- **Seen in the Spoof Lab video:**
  - High-res masks
  - 3D busts
  - Hyper-realistic ($1000+) masks
  - Fake facial hair, real hair, hats/beanies
  - Drawing instruments
  - Many different styles of eyeglasses
  - High-resolution photos
  - Low-resolution photos
  - Cutouts of faces in paper, cardboard, etc.
  - Large-print images
  - Spoofs of projector images of faces
  - 3D printed masks
  - Paper faces with holes cut out in all sorts of different locations
  - FaceTec SDK running spoof automation from a variety of Android/iOS devices
  - Photos printed of 1000s of different identities
  - Various face segments printed for wearing over real faces or applying to 3D busts

©2020 FaceTec, Inc. All Rights Reserved.

- ○ 3D Avatar/CrazyTalk 8 sample videos are available for simple 3D animations that can be used to spoof FaceTec's competitors, please contact FaceTec for access.

FaceTec's Training Set Diversity

FaceTec has been trained on millions of face images from tens-of-thousands of unique users with more than 4000 different device models in over 170 countries.

Copyright 2018 FaceTec, Inc.