FaceTec embraces new ISO-based anti-spoof testing for face biometrics

Nov 13, 2018, 2:12 pm EST | Sponsored Post

CATEGORIES Brand Focus | Features and Interviews

The rapid global adoption of biometrics for identification and access management by organizations of all sizes clearly indicates they are here to stay. Yet, until 3D face authentication technology became available in late 2017, 2D face recognition, matching two face images, was all that was available. 2D Face Recognition vendors promised security, but without any proper third-party testing available, it was left to each organization to perform their own due diligence. Without the sophistication of new 3D FaceMap technology the 2D face recognition solutions rarely saw any large-scale deployments, and even those were plagued by fraud FaceTec VP of Sales, Steve Cook told Biometric Update in a recent interview.

3D FaceMaps contain as much as 100 times more data than a 2D photo, Cook says, and are required to accurately recognize the correct user's face while concurrently verifying their human "liveness." This liveness check is especially critical in unsupervised authentication scenarios such as confidential account access management and high-value mobile transactions. It must be proven in real-time that the person requesting access is actually the correct user, not just a representation, like a photo, video or mask.

"Buyers should demand vendors have the viability of their anti-spoofing performance tested by 3rd parties before they use them to secure their applications," Cook points out. "Biometrics development has begun to hit stride, particularly for

FACETEC EXHIBIT 2036
JUMIO v. FACETEC
IPR2025-00107

AI-driven applications like ZoOm. And significant gains in usability and security performance have not only raised the bar, but have begun to expose critical weaknesses in many of the legacy solutions in use today."

FaceTec launched its ZoOm 3D Face Login authentication platform just over a year ago, and the market has responded with consistent user growth from new deployments and a dozen new channel partners, according to Cook, while the company has been in the news showcasing innovation, and being honored by CIO Review.

In what was an industry-first move, ZoOm also recently passed tests by iBeta for Level 1 anti-spoofing capabilities in a rigorous ISO 30107-3 Presentation Attack Detection (PAD) certification process. ZoOm is currently the only face authenticator to achieve a perfect anti-spoofing score.

"Sanctioned, third-party certification is vitally important," Cook says. "The biometrics industry has been facing a credibility challenge, largely of its own making, and needs to be much more transparent."

An industry challenge

In many instances, Cook says, in an effort to grab market share the technology vendor sold an incomplete or inappropriate solution. Customers are often unable to distinguish a modified recognition product from a true authentication solution, despite fundamental differences between the two. Some vendors are all too willing to overlook the differences to make a sale, he says, leaving customers and users with a false sense of security and unknown levels of risk.

Customers seeking biometric authentication technologies are rarely subject-matter experts, and without recognized standards and independent third-party verification they have little to go on when attempting to assess what biometric solutions will provide high-performance, long-term security for their particular use cases.

The terms "recognition" and "authentication" are often used interchangeably by those not familiar with the differences, Cook explains. Authentication identifies a correct user through image-matching, but also concurrently verifies them as a real, live human. This "Turing Test in reverse" has only recently been made possible by significant, AI-driven abilities that can observe numerous living human traits and characteristics in real-time and concurrently.

"Different use cases require significantly different applications. It may seem like they are interchangeable to some extent, but you can't take a recognition algorithm that's optimized for airport surveillance and use it for 1-to-1 authentication for a ten-thousand-dollar transaction," says Kevin Alan Tussy, FaceTec CEO. "With face identification, you want to put a name to a face from a database of millions of faces. In authentication, you know exactly what face it's supposed to be, and if it's present, you have to verify that it is alive, and not a spoof, like a photo or video. These two types of face recognition technologies look similar at first glance but are actually very, very different. Liveness isn't important for face identification, but it is a mission-critical requirement for face authentication."

Customers tell Cook they have too often been disappointed with biometrics results. Further, controversies like the disagreements between rights groups and Amazon over the marketing to law enforcement of their facial recognition product, Rekognition, become muddled with face authentication, further confusing the different face technologies.

The importance of true liveness detection for authentication can become lost in the noise. Acuity Market Intelligence Principle Researcher Maxine Most has noted that, "One of the main challenges ahead is educating markets about what constitutes the integrity of a biometric system, including how to apply best practices for liveness detection."

In the past, face recognition systems are known to have failed to detect spoofs with photographs, videos, and masks. Worse, the knowledge of how to defeat a high-value system can not only be acted upon immediately by those who discover it, but also disseminated over the internet via dark web forums, creating a fraud nightmare for any company that implemented sub-par liveness technology. The stakes are high.

Businesses live the cat-and-mouse security game and pay for it every day, but most are still not sure how to effectively use biometric technology because biometrics are still largely a “black-box” technology, poorly understood even by those who claim to be experts, Cook says. Until the NIST-certified, ISO-guided iBeta test, there was no recognized standard for performance claims and no transparency.

“The first thing new customers say is, ‘We hear similar liveness detection claims from everybody in the industry, so what makes you different?’”, says FaceTec CTO Josh Rose in an email. “We can now say ZoOm is the only 3rd-party certified Liveness Detection solution on the market. The other so-called face authentication vendors use schemes that are all-too easily bypassed, and most of the companies peddling these half-baked solutions have either tried and failed testing or know they can’t pass and won’t even bother. Only we can provide customers a copy of our iBeta liveness certification report, a sanctioned, objective performance evaluation supporting our claims in black and white.”

Why it works (and spoofs don’t)

FaceTec’s lab makes use of an extensive collection of what ISO and NIST call “artefacts” to test ZoOm’s spoof detection capabilities against hundreds of presentation attack vectors. Well-known attack methods range from simple, easily available photographs and video footage on social media to sophisticated methods involving masks, makeup, projectors, wax figures and more. Testing artefacts repeatedly and in different conditions is the only way to ensure AI systems can recognize the truly definitive characteristics of human liveness in real-world situations, according to Cook.

“A nod, blink or smile are all easily reproduced human liveness indicators,” Rose says, “Whereas true liveness detection requires wholistic observation of the characteristics of the face and surrounding environment.”

What happens behind the scenes of ZoOm’s deceptively simple selfie interface is highly complex. The familiar, patented “zoom” motion processes up to 30 frames of hi-res video, and as the device gets closer to the user the camera observes perspective distortion, or what is commonly called the fisheye effect, Cook explains. Advanced AI determines if concurrent human liveness traits are present and decides in milliseconds whether the user is a living person. This liveness detection method is applied during both enrollment and authentication and includes texture, reflectivity, movement, 3D depth and much more. ZoOm does not require expensive 3D cameras or infrared sensors, making it compatible with the literally billions of smartphones, tablets, desktops, laptops and embedded systems with standard 2D cameras currently in use.

There are three levels of iBeta's PAD certification testing, each with successively more complex, expensive artefacts. ZoOm is in continuous development, and FaceTec is confident it will pass, among other tests, all three levels in the near future.

"The biometrics industry has suffered in credibility and transparency as many of the biometric vendors have conducted internal testing and presented results that do not, in all cases, communicate their test methodology," says iBeta Director of Biometrics Kevin Wilson. "With the release of the ISO 30107-3 Presentation Attack Detection standard, the industry can now elect to test with this test methodology and provide uniform liveness detection results that will not only provide the benefit of a wider understanding of their system capabilities but also allow their customers to compare their results to those of other system offerings."

According to Cook, FaceTec is also currently working with other internationally recognized testing organizations, and its ZoOm technology is undergoing rigorous tests "in the wild" by major government agencies, all of which will provide additional valuable security validation. "We want as many of the testing organizations, hackers and even our competitors to take ZoOm to task," Cook says. "It helps make our solution stronger, and whenever we uncover a weakness from a new hacking approach, we can now address it very quickly."

The company recently signed an agreement with Digital Identity giant Jumio, which has performed more than 150 million identity verifications and counting. Looking ahead, Cook says 2019 will see ZoOm added to an even wider range of applications in additional verticals all around the world. As worldwide mobile user growth continues, FaceTec will offer ZoOm's robust authentication and liveness detection capabilities to meet the need for highly secure, easy-to-use, cross-platform and cross-device biometric authentication.