INTEGRATED
BIOMETRICS

Presentation Attack Prevention

Anti-spoofing technology
light years ahead of its time.

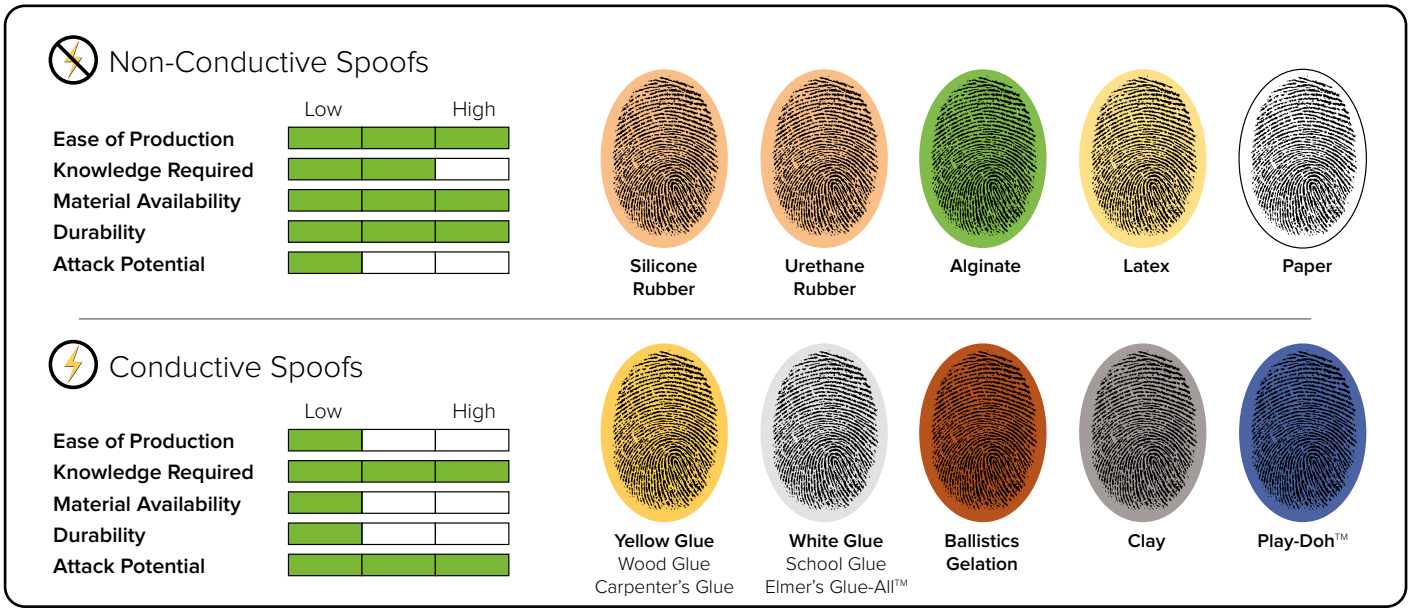
Presentation Attack Detection (PAD)

Everybody wants to beat the system. That's especially true for criminals faced with biometric fingerprint scanners. Methods commonly used to counter biometric fingerprint security include the production of counterfeit fingerprints and fingers, or the presentation of severed digits.

Presentation attack detection, or **PAD**, is the comprehensive approach to spoof-detection which includes both anti-spoofing and liveness detection technologies. Both are discrete methods to approaching biometric fraud, and each is optimized to resolve a distinct issue. **Anti-spoofing** refers to the detection of an artificial copy of a real or synthetic fingerprint. **Liveness detection** refers to the validation of human tissue as belonging to that of a genuine, living human being.

Unfortunately, the biometric industry often uses these terms interchangeably. Confusion of anti-spoofing and liveness detection often occurs when people mean to talk about PAD.

Non-Conductive vs. Conductive Spoofs



10 common spoof types we believe customers with biometric fingerprint systems may encounter in their environments.

In general, spoofs can be divided into 2 categories: non-conductive and conductive.

Non-conductive spoofs are common because they require a minimal amount of knowledge to produce and are made from materials which can be acquired from hardware, grocery, and costume stores. Materials such as silicone rubber, urethane rubber, alginate, latex, and paper printouts are often chemically stable which allows them to last over time. These materials regularly retain artifacts from their manufacture which makes them more susceptible to detection by PAD techniques.

Conductive spoofs possess electrical characteristics that better simulate genuine human fingerprints. These advanced spoofs are less common due to the additional knowledge and tools needed to produce them. Although common materials such as yellow glue, white glue, ballistics gelatin, clay, and Play-Doh™ may be used in creating these spoofs, the base formula usually requires additional materials to produce a viable conductive spoof. Conductive spoofs expire soon after production, often becoming dry, brittle, or non-conductive, but remain effective on scanners with non-conductive spoof vulnerabilities. These spoofs often retain the most tissue-realistic characteristics and present the highest degree of attack potential.

Beyond EER

Equal Error Rate (EER) is a good starting point for discussing PAD performance, and it is often used as a standard, but it is not the best metric. We include it here because it is expected from anyone operating in the PAD industry, however, EER has several shortcomings:

- What spoofs make up the performance? Easy ones, hard ones? What materials?
- EER alone can convey false impressions of performance.
- Customers do not present statistically valid sample sizes when evaluating spoof classifiers. They will present 1 – 3 spoofs and make a decision based on their subjective experience.
- Spoof recipes are guarded carefully, and many spoofs decay relatively quickly. How do you demo this capability?

When discussing fingerprint PAD EER, it is easy for companies to hide behind impressive looking data sets. This is a shortcoming of using EER, as one is not aware of how diluted the data set is. One solution would be to establish an international standard of benchmark spoofs and their recipes. While we at IB believe this is possible, it requires releasing recipes on the open market for anyone to use. Such a handbook on spoofing could serve as a how-to for bypassing government security measures around the globe. We opted to take a different approach.

The IB Approach

Integrated Biometrics' LES film technology already provided automatic spoof rejection, but the value of the information and systems protected were causing threat actors to step up their game, requiring us to raise the stakes in our Presentation Attack Detection.

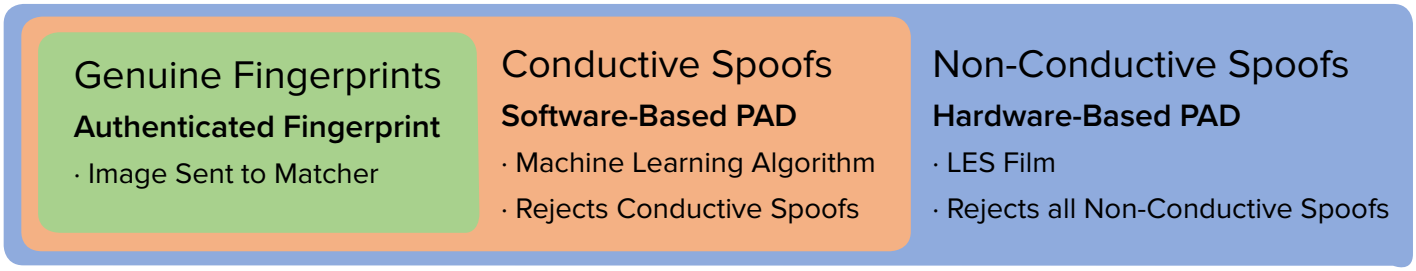
The trouble with many of the PAD systems currently available in the market is they are based on dated standards. The quality and types of materials used to create fake fingers have improved dramatically, and no one really knew how to test well. This provided us with an opportunity to innovate and push our already cutting-edge machine learning, allowing us to test closer to the actual user experience. The result is an advanced algorithm based on a robust data-driven framework supported by the ability of LES film to capture even more information.

Integrated Biometrics' approach to presentation attack detection is tiered verification. The first tier is hardware: LES film in IB scanners instantly rejects any non-conductive presentation attack, which nullifies the threat of the most common spoof constructions.

The second tier is software: a unique deep-learning AI algorithm trained to detect anomalies in fingerprints typical of spoof attacks discerns a liveness score with a high degree of accuracy. This PAD technique is completed in milliseconds with a latency that is imperceptible to the end user.

IB does not claim to detect 100% of presentation attacks. No one can. However, our research shows an aggregate EER (of all the tested materials) of about 3%. By anyone's measurement, this makes IB scanners a hard target even in a stand-alone scenario. When used in conjunction with industry standard IAFIS matchers, even the most skilled criminals will be dissuaded.

If a PAD system has a high level of attrition, then would-be attackers will find something else on which to spend their time. This is yet another reason to consider strong forms of encryption, such as IB's state of the art AES-256 encryption.

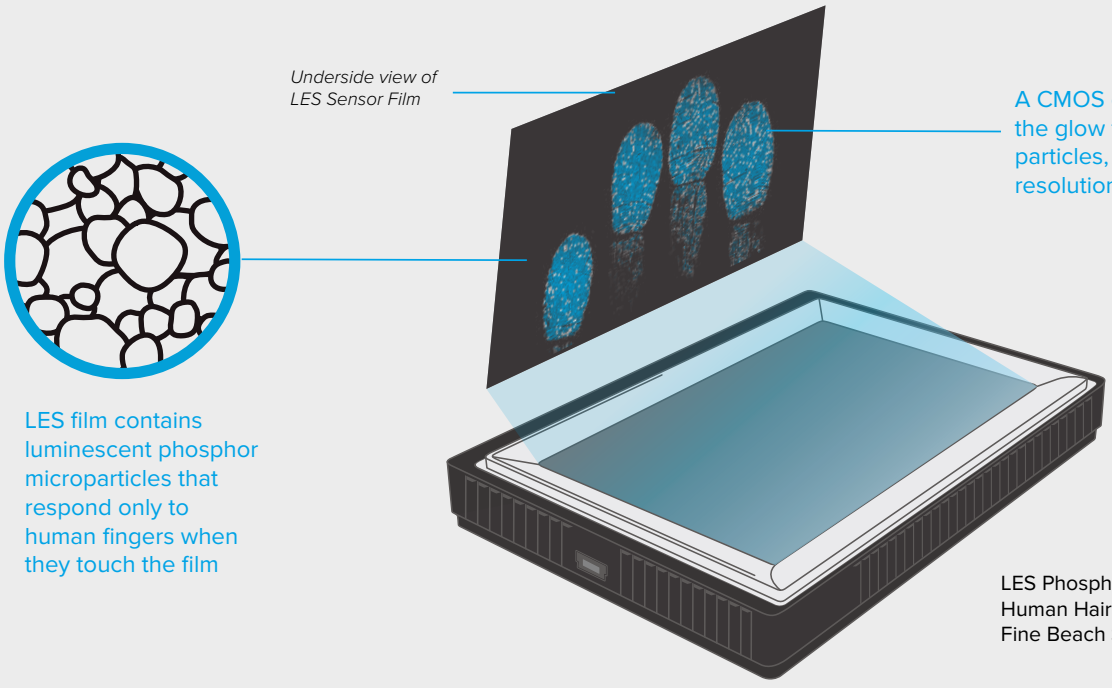


What's In Your Scanner?

	Optical Prism	Capacitive TFT	Multi-spectral Imaging	IB's PAD
PAD Capable	●	●	●	●
Software-based PAD	●	●	●	●
Hardware-based PAD		●	●	●
FBI Certified Images	●	●		●
Does not require proprietary IAFIS	●	●		●
Invulnerable to Non-conductive Spook Materials		●		●
Prevents False Trigger from Latent Prints		●		●
Proven Performance Discerning Cadaver Generated Images			●	●

LES Light Emitting Sensor Technology

Integrated Biometrics' scanners use our patented light-emitting sensor (LES) technology to deliver fixed and mobile FBI certified fingerprint imaging in an exceptionally durable, lightweight scanner.



+1 888 840-8034 | sales@integratedbiometrics.com | www.integratedbiometrics.com