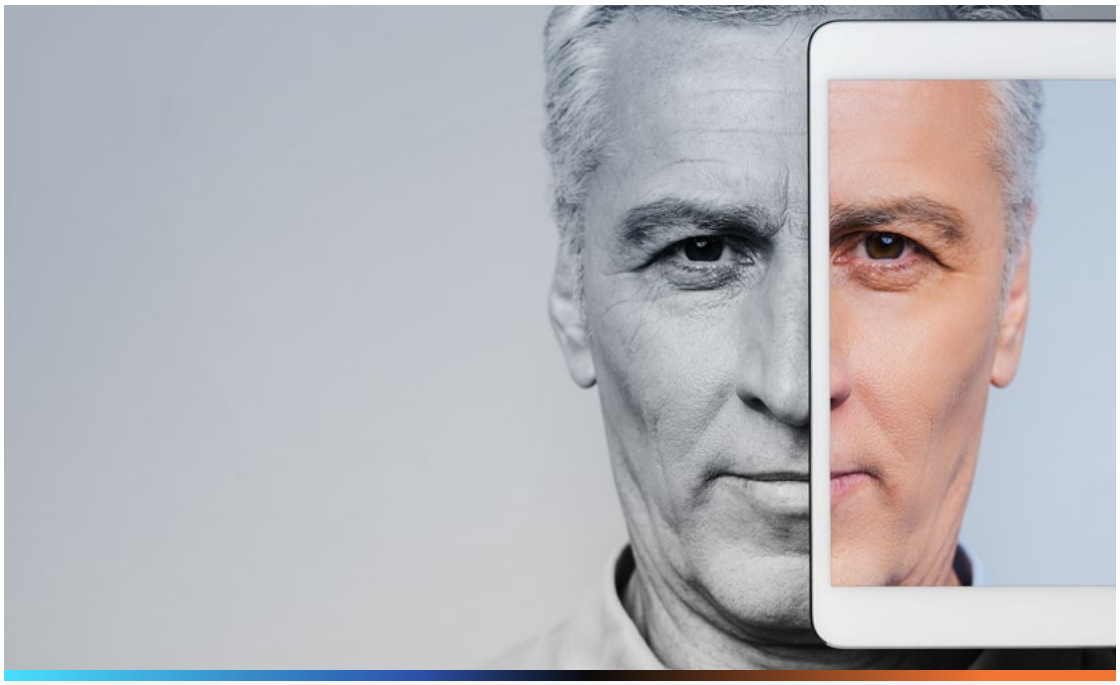
PARAVISION

AN INTRODUCTION **TO PRESENTATION ATTACK DETECTION**



→ paravision.ai

Trusted Vision AI

October 2020

Authenticity in Biometric Identity

Biometrics can deliver a unique combination of high security and ease of use in applications that require identity authentication, such as access control, payments, or travel. With recent advances in AI and computer vision, biometric systems have become dramatically more accurate, faster, and more resilient to environmental and user variables. However, even biometric systems can be attacked and bypassed without the right technology in place.

These direct attacks—commonly referred to as "spoofs" or presentation attacks (PAs)—can subvert a biometric system by using tools called presentation attack instruments (PAIs).

Examples of such instruments include photographs, masks, fake silicone fingerprints, or even video replays. Presentation attacks pose serious challenges across all major real-time biometric modalities (such as face, fingerprint, hand vein, and iris). For this paper, we will focus on face recognition-based presentation attacks, as face recognition has emerged as the dominant biometric in many applications due to its combination of low cost, accuracy, and usability.

What is **Presentation Attack Detection?**

The process of a biometric system detecting a biometric spoof is known as Presentation Attack Detection (PAD). PAD systems utilize a combination of hardware and software technologies to determine whether or not a presented biometric is genuine. A subset of this is liveness detection, which refers to a PAD system's specific ability to differentiate between human beings and non-living spoofs.

Some PAIs—such as 3D masks, synthetically generated irises, or photographs—can fool a less-secure biometric system. Furthermore, since these attacks occur in the physical world, detection systems often need to include a combination of illumination, sensing, and processing to determine the authenticity of the biometric sample.

Therefore, successful PAD often focuses on the interplay between hardware and software to maximize accuracy and usability.

PAD is crucial in applications where the combination of security and convenience is a priority. This is especially true in automated identification and authentication scenarios—such as physical access control, travel facilitation, payments, or online identity verification—where it may be inefficient, insufficient, or unworkable to have a qualified person manually ensure the authenticity of the presented biometric. time to market, and technology ecosystem support.

Categorizing Presentation Attacks

ISO 30107 defines PAIs as needing to fulfill three requirements: They must appear as genuine to any PAD mechanisms, as genuine to any biometric data quality checks, and must contain extractable features that match the targeted individual.

In practical applications, it is useful to establish a hierarchy in the sophistication and complexity of presentation attacks, which is beyond the scope of ISO 30107. Notably, iBeta and the FIDO Alliance have both established a three-level hierarchy of presentation attack sophistication.

iBeta's approach [§] is accepted as a de facto standard across varying applications, and is therefore presented here as the framework of choice for analysis:

Level 1

- **Expertise required:** none; anyone can perform these attacks.
- **Equipment required:** easily available.
- **Presentation attack instruments:** a paper printout of the face image, mobile phone display of face photos, hi-def challenge/response videos.

Level 2

- **Expertise required:** moderate skill and practice needed.
- **Equipment required:** available, but requires planning and practice.
- **Presentation attack instruments:** video display of face (with movement and blinking), paper masks, resin masks (targeted subject), latex masks (untargeted subject).

Level 3

- **Expertise required:** extensive skill and practice needed.
- **Equipment required:** specialized and not readily available.
- **Presentation attack instruments:** silicone masks, theatrical masks.

FIDO's three-level categorization can be found in section 6.2.4 of the FIDO Biometric Requirements. [2]

1. https://www.ibeta.com/iso-30107-3-presentation-attack-detection-confirmation-letters/

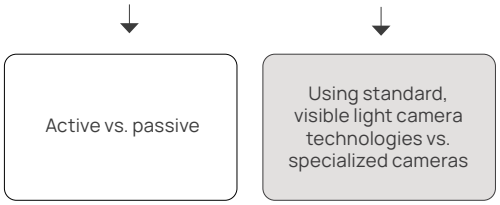
2. https://fidoalliance.org/specs/biometric/Biometrics-Requirements-v1.0-wd-20190606.html

How Presentation Attack Detection Works

PAD systems determine the authenticity of a presented biometric sample by measuring and analyzing some combination of physical characteristics and movement.

PAD methods are any technique that can determine whether a biometric being presented to a PAD sensor is genuine or a synthetically produced spoof. Different methods can be used in conjunction to ensure higher levels of accuracy.

Here, we separate PAD methods in two ways:



These top-level distinctions are interrelated. For instance, in order to achieve a high-accuracy passive system, it is often necessary to use specialized camera technologies that rely on characteristics beyond 2D visible light.

In addition to these two paradigms, there are a number of ways to process the collected data. Some approaches may rely on deep learning, which is a rapidly advancing approach to computer vision, whereas others may rely on traditional algorithmic techniques. Broadly speaking, approaches that rely on image processing, whether 2D or 3D, active or passive, will depend increasingly on deep learning due to substantial advantages regarding accuracy, time to market, and technology ecosystem support.

Active vs. Passive PAD

Active PAD

Active PAD verifies user identity and authenticity by having the user respond to a series of active challenges. This method relies on user participation.

Benefits	Disadvantages	Challenge Examples
Can deliver enhanced security with conventional camera technologies	Demands high levels of user cooperation Not suited for high throughput environments	Nodding/turning head sideways Blinking Following a dot on the screen Speaking a series of words or numbers Leaning into the camera

Passive PAD

Passive liveness detection requires no PAD-specific action by the user. Active challenges—such as nodding, blinking, or turning one's head—are not required.

Benefits	Disadvantages	Challenge Examples
Requires minimal user effort Useful for high throughput environments due to its speed and ease of use	May require specialized hardware	Analyzing a "selfie" Capturing a video

Standard (visible light) Camera vs Specialized Camera Technology

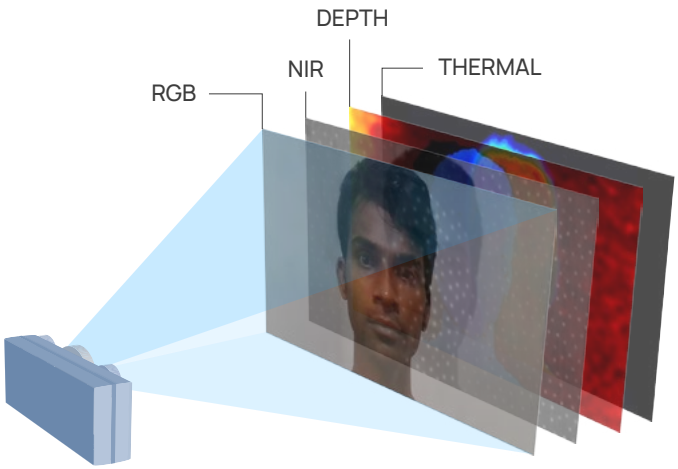
Standard cameras rely on visible light to perform PAD, while specialized cameras can use advanced sensors to measure depth, heat, reflectivity, or other parameters to deliver PAD.

Standard (visible light) cameras

Benefits	Disadvantages	Challenge Examples
Low cost	Often utilize an active approach to PAD, compromising user experience	Smartphone cameras
Ubiquitous presence	Not recommended in cases where high levels of speed, efficiency, and accuracy are required	Webcams
Same sensor can be used for face recognition and PAD		IP cameras

Standard, visible light cameras typically rely on an active PAD. While active PAD requires an undesirable level of interaction for high throughput environments such as point of sale or access control, the ability to deliver PAD on fully commoditized cameras is a tremendous value. For environments where speed is not critical, such as at-home onboarding or authentication, the value of using a commercially available mobile device or webcam outweighs the challenges of an active PAD user experience, making standard cameras a compelling proposition in many applications.

Specialized cameras



Benefits	Disadvantages	Challenge Examples
Can enable high-accuracy passive PAD Can deliver higher levels of security to protect against advanced PAs	More expensive Not typically integrated into consumer devices; therefore, not as easy to deploy, especially for remote onboarding	Depth sensing cameras Visible light / Near-infrared (NIR) cameras Thermal cameras

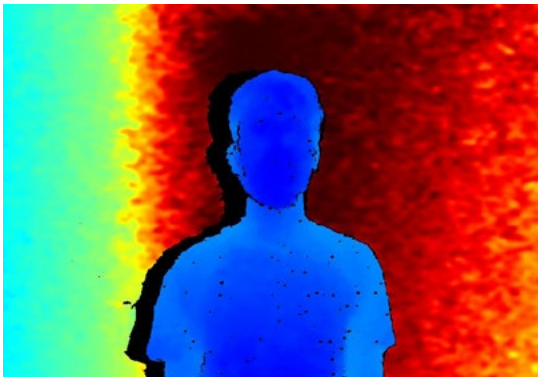
While specialized cameras come with an added layer of cost and complexity, they are the ideal tools for use cases that demand:

- **Improved accuracy:** Specialized cameras can aggregate multiple layers of information—ranging from depth perception, thermal detection, reflectivity measurement, and more.This allows the system to better gauge the object at hand, and by extension, more accurately distinguish between bona fide and counterfeit biometrics.
- **Increased robustness:** Specialized cameras come with different modules that can be used in conjunction with one another without sacrificing accuracy. As a result, they can perform precisely and efficiently in a wide variety of environments.
- **Enhanced user experience:** Due to their ability to deliver high levels of accuracy in passive settings, specialized cameras can provide an intuitive and frictionless user experience. When used with PAD systems, they eliminate the need for cumbersome activities like eye blinking, head rotating, or lip moving.

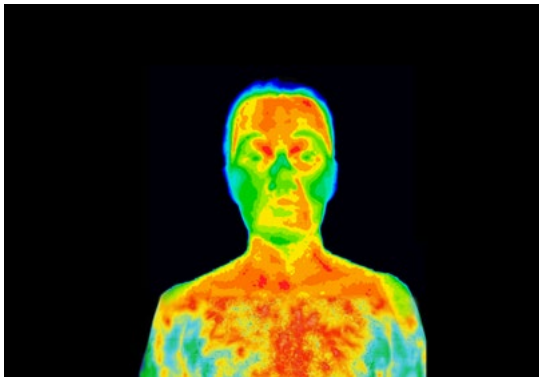
Specialized cameras can detect presentation attacks through one or a combination of these technologies:

Standard imaging: Standard cameras produce images using the visible light spectrum. This means that each pixel is some variation of red, green, or blue (RGB).

Multi-spectral imaging: Multi-spectral methods leverage the fact that human skin shows different reflective properties at different wavelengths of light. These measured reflective properties are then compared to values corresponding to other materials, such as human skin, latex, paper, etc.



3D imaging: By measuring depth, a PAD system can differentiate between the contours of a live face and a 2D spoof.



Thermal imaging: All objects emit heat, and as a result, exhibit an infrared signature. Since humans and synthetic materials emit significantly different amounts of heat, this approach can be used to determine wheter the object being presented is authentic.

Use Cases for PAD

Presentation Attack Detection is most critical in situations where it is not possible to have a person overseeing the validation of identity. This is most typically in remote identity validation—e.g., from home on a consumer smartphone—where it isn't possible to manually authenticate a presented identity or in an automated environment where the goal is to reduce manual overhead and improve throughput and user experience. Here are some of the most common use cases that are or should be relying on PAD for ensuring authenticity.

Access Control

The next generation of enterprise access control will be powered by computer vision. PAD will be critical to fast, secure electronic access.

Payments / Point of Sale

PAD systems are vital in cases where face recognition is replacing traditional payment methods. Even in attended point of sale application, automated PAD will be fundamental to establishing trust and minimizing risk.

Air Travel

Air Travel is increasingly reliant on touchless, frictionless passenger experiences driven by face recognition. High performance PAD will serve both mobile (at home) registration and rapid, seamless authentication at the airport .

Identity Validation (KYC)

PAD is essential to KYC applications such as mobile onboarding and authentication, where strong identity verification is needed to counter fraud, meet industry regulations, and establish customer trust.

In Conclusion

Dramatic advances in AI, camera technologies, and associated image processing hardware have enabled face recognition to rapidly evolve into the leading biometric for identification and authentication. While the usability, cost, and speed of face recognition are compelling, the face image is by its nature the easiest to replicate, making Presentation Attack Detection even more critical than with other biometrics.

There are multiple approaches to PAD, and there is no single correct or “best” approach. Rather, solution developers should consider the use case carefully as well as the associated throughput and security requirements. In any case, PAD should be foundational to any modern face recognition deployment for remote or automated registration, authentication, or identification.

PARAVISION

Trusted Vision AI

For more information or to schedule a demo, please contact us at:

info@paravision.ai