Guide

Fingerprint recognition & anti-spoof for National ID Systems

An introduction to the core technologies for secure and trusted identity systems.

YOU are the key

Introduction

Biometric authentication has become a cornerstone of modern security — from unlocking mobile phones and accessing workplaces to verifying identities in national ID programs. Unlike passwords or PINs, biometrics offer something far more convenient — security that is part of who you are.

With this growing adoption, attackers have also become more creative in attempting to trick biometric systems. This practice, known as spoofing or presentation attacks, involves presenting a fake or manipulated biometric sample to bypass security.

Fingerprint recognition stand out as one of the most trusted and widely deployed modalities. It combines accuracy, ease of use, and broad public acceptance. But like all biometrics, it must be protected against spoofing attempts to ensure trust and compliance.

Glossary

Spoofing (or presentation attack)
Attempt to fool a biometric system using fake traits.

Liveness detection
Technology that ensures the biometric sample is from a living person.

Ultrasonic sensor
Sensor using sound waves to capture detailed 3D biometric data.

Multispectral imaging
Captures images across multiple wavelengths to detect live skin.

AI/Deep learning
Machine learning techniques used to identify patterns and anomalies.

False accept rate (FAR)
Probability that an imposter is wrongly accepted.

False reject rate (FRR)
Probability that a genuine user is wrongly rejected.

Relevant stakeholders

AI-powered anti-spoofing creates value at every level of a National ID program, from technology providers to citizens — everyone benefits from trusted solutions minimizing risk.

Who benefits from anti-spoofing technology:

- Sensor & scanner manufacturers
- System integrators
- Governments
- Project & program managers
- Banks & financial institutions
- Individuals in society

Understanding spoofing in biometrics

At its core, spoofing means trying to impersonate someone by fooling a biometric system. Instead of stealing a password, the attacker fabricates a biometric trait — a fake fingerprint, a printed palm, or even a prosthetic hand.

There are two main categories of attacks:

Presentation attacks: Direct attempts to fool the sensor or scanner by presenting a fake biometric (e.g., a gummy fingerprint).

Digital attacks: Attempts to manipulate the biometric data in transit or storage (e.g., replaying a captured fingerprint template).

This guide focuses on presentation attacks, since they are the most common and directly tied to real-world spoofing scenarios.

Why does it matter?

- A successful spoof can lead to unauthorized access, identity theft, or financial fraud.
- For governments and enterprises, it undermines trust in critical systems.
- For vendors and integrators, it can mean reputational damage and regulatory non-compliance.

Common spoofing attacks

Spoofing attacks come in many forms, but they all share one goal: to trick a biometric system into accepting a fake sample as genuine. Attackers often take advantage of the fact that biometric traits leave traces everywhere — a fingerprint on a glass or even a scan shared online.

The most common techniques include:

Artificial replicas
Fake biometrics are created using materials like silicone, gelatin, latex, or glue. These replicas mimic the ridges, lines, and overall patterns of real fingers.

Printed images and patterns
High-resolution photos or 2D/3D-printed patterns can be presented to a scanner. With advanced printing technology, attackers can replicate fine details that fool less sophisticated sensors.

Latent print lifting
Fingerprints traces left on everyday surfaces can be captured and reconstructed into a spoof. This forensic-style attack is surprisingly effective if no liveness detection is in place.

Prosthetics and overlays
Entire artificial hands, gloves, or overlays are produced with embedded ridge or vein structures, making them appear highly realistic to sensors.

Digital display attacks
Images or videos displayed on high-resolution screens can sometimes trick biometric systems, especially when combined with clever lighting and angles.

The risk
Whether made with low-tech household materials or advanced 3D printing, these spoofing attempts can grant unauthorized access, enable fraud, or undermine entire identity systems if not properly defended.

- Access secured devices, systems, or physical areas.
- Commit financial fraud or unauthorized transactions.
- Impersonate citizens in large-scale programs, leading to systemic trust issues.

In short: even the most advanced biometric recognition systems need an equally advanced anti-spoofing layer.

How anti-spoofing works

The principles of liveness detection

Anti-spoofing is about distinguishing a live biometric sample from a fake one. Liveness detection looks for biological signals that cannot easily be replicated — such as skin texture, sweat pores, or micro-movements.

There are two broad approaches

- **Hardware-based**: Using specialized sensors to detect additional signals (infrared light, multispectral imaging, or ultrasonic sound waves), which often is more cumbersome.
- **Software-based**: Using AI and advanced algorithms to analyze patterns, textures, and behaviors that reveal whether the input is genuine. This is often a more flexible and agile way, with a shorter time to market.

Hardware-based techniques

- **Ultrasonic sensors:** Capture 3D fingerprint details, including sweat pores and subsurface structures, making it harder to spoof.
- **Infrared/multispectral imaging:** Capture skin characteristics at different wavelengths to detect live tissue versus fake materials.

Software-based techniques

- **AI & deep learning models:** Trained on millions of samples, they can detect anomalies and patterns invisible to the human eye.
- **Texture and ridge analysis:** Distinguish natural skin from materials like silicone or paper.
- **Micro-movement detection:** Identify natural variations when a real hand or finger interacts with the sensor.

Passive vs. Active detection

- **Passive detection:** Runs in the background without requiring user interaction.
- **Active detection:** Asks the user to perform an action (e.g., move a finger) to confirm liveness.

PRECiSE BIOMETRICS

Key considerations when choosing anti-spoofing

When evaluating anti-spoofing solutions for fingerprint recognition, consider:

- **Security vs. usability:** Strong protection should not slow down or frustrate users.
- **Compliance requirements:** Many sectors (payments, national IDs) mandate certified anti-spoofing.
- **Integration flexibility:** Open, modular solutions work best across devices, platforms, and vendors.
- **Performance:** Detection must happen in real time, with minimal latency, even at scale. Top performance also helps balance usability and security.
- **Scalability:** Can it handle millions of authentications per day?
- **Future-proofing:** AI-driven solutions can evolve with new spoofing techniques.

The Precise BioLive solution

PRECiSE BIOMETRICS

BioLive is Precise Biometrics' AI-powered anti-spoofing and liveness solution designed specifically for fingerprint recognition.

Key strengths:

- **Real-time protection:** Detects spoofs instantly during authentication.
- **AI-driven accuracy:** Built on advanced deep learning models trained on diverse spoofing attempts.
- **Seamless UX:** Runs in the background without requiring user actions.
- **Proven deployments:** Trusted in national ID programs, mobile devices, and enterprise systems.
- **Easy integration:** Flexible and easy to integrate into an existing ecosystem without any retrofits or cumbersome integration work. Also available for both mobile phones and for integrated systems with limited processor capabilities.
- **Compliance ready:** Meets requirements from ISO/IEC 30107, FIDO, Aadhaar, and other frameworks.

With BioLive, organizations can achieve both robust security and frictionless usability — two factors often seen as a trade-off.

Learn more about Biolive →

PRECiSE
BIOMETRICS

Visit our website →

☎ Contact us