The world's most accurate deepfake detection system

Deepsight protects organizations from deepfakes, AI-driven impersonation, synthetic document fraud, camera injections, and device tampering with unmatched accuracy, because when identity can be faked, everything breaks.

An existential threat

Deepfake attacks are increasing faster than legacy defenses can keep up

Generative AI now makes deepfakes easy to create, cheap to scale, and nearly impossible for humans or traditional systems to detect, creating an existential threat to digital trust.

<1 minute

Time it takes to generate a convincing deepfake with free AI tools.

Source: MIT Tech Review, 2023

50–59%

Human accuracy in spotting deepfakes, barely better than chance.

Source: Cooke et al., 2024

$47B

Lost to identity fraud by U.S. banking customers in 2024.

Source: AARP/Javelin, 2024

700%

Increase in fintech deepfake incidents in 2023.

Source: Deloitte, 2024

The defense

Defend verification journeys against deepfakes from start to finish

Incode Deepsight is a multi-layered fraud detection system that blocks attacks across every critical verification touchpoint. By analyzing behavioral signals, device and camera integrity, the perception layer, and document authenticity in real time, it ensures only real people with real documents are verified, stopping AI-driven identity fraud in its tracks.

- **Behavioral layer**

  Flags anomalies in device motion and user behavior that signal bots or scripted fraud.

- **Integrity layer · device**

  Detects tampered, emulated, or rooted devices that allow spoofing or injection.

- **Integrity layer · camera**

  Blocks virtual cameras and prevents video injection using camera source validation.

- **Perception layer**

  Detects deepfakes by using a large multi-modal AI (video, motion, and depth) and Vision Language Model that identifies document inconsistencies typical of Gen AI tools.

Why Incode Deepsight

Unmatched accuracy

Detect deepfakes, injections, and tampered devices with the world's best deepfake detection system, with accuracy independently validated by Purdue University.

Stop threats before they cost you

Even a single attack can cause major financial and reputational damage. Using a multi-modal AI to stop sophisticated AI-fraud without impacting performance, Deepsight blocks costly threats before they succeed.

Enterprise-grade, frictionless

Enable enterprise-grade protection without slowing down your team. Deepsight integrates seamlessly with your IDV process and provides automatic updates through the Incode Trust Platform.

Get ahead of accelerating AI-assisted fraud

Fraud evolves quickly and strikes from multiple angles. Deepsight responds in real time.

Threats to your business	Deepsight's solution
Deepfakes and physical spoofs that bypass liveness checks	✓ Detects deepfakes and spoofs with multi-modal analysis across video, motion, and depth
Virtual camera and manipulated video feeds	✓ Identifies virtual camera feeds with camera source validation
Devices running in emulators or tampered environments	✓ Detects tampered devices and emulators with device integrity checks
Bots and automation that mimic real users	✓ Flags automated behavior and high-frequency bot activity in real time
Adding new fraud detection layers can increase friction and overheads	✓ Provides frictionless protection, invisible to the end user and not affecting verification speed

Independently validated

"We evaluated nine of the most widely used commercial deepfake detection systems and found that Incode's detector achieved the highest accuracy in identifying fake samples, yielding the lowest false acceptance rate."

Shu Hu · Assistant Professor & Director, Purdue Machine Learning Lab

68x
better false-positive rate in identity verification than the next-best commercial technology

2.5x
lower false-acceptance rate across all deepfake samples

10x
surpassing human labelers across every test

1,350+
deepfakes in the representative in-house testing sample

Deepsight for Documents

AI-generated documents are the next frontier of identity fraud

Generative AI doesn't just create convincing fake faces, it creates convincing synthetic documents. Deepsight for Documents protects the document layer, catching forged IDs, passports, and supporting documents that traditional verification tools miss. Its AI forgery detection identifies documents created or altered by generative AI tools by detecting visual artifacts, font inconsistencies, and layout anomalies invisible to the human eye.

10x

increase in AI-generated document fraud over 2 years

8.8x

more fraud caught by Deepsight for Documents than document-based checks alone

25%

of all identity fraud attempts are now AI-assisted, estimated to grow to 50% by end of year

Where deepfakes break digital trust

- **Onboarding & KYC**
  Fraudsters use deepfake selfies and videos to bypass biometric verification.
- **Helpdesk & support**
  Attackers fool helpdesk agents with fake identities or manipulated videos.
- **Account recovery**
  Imposters use stolen IDs, deepfakes, or prerecorded videos to access accounts.
- **Bot attacks at scale**
  Bots overwhelm IDV systems by flooding them with activity and simulating real users.

Frequently asked questions

What is Incode Deepsight?

Deepsight is Incode's proprietary deepfake and liveness detection engine. It uses a multi-layer AI model to identify AI-generated faces, video injection attacks, and presentation attacks in real time, validated by Purdue University as the most accurate system in its class.

How accurate is Deepsight compared to other tools?

Deepsight achieves a 68x better false-positive rate in identity verification compared to the next-best commercial technology, independently validated by Purdue University's Machine Learning Lab. It operates in milliseconds, making it suitable for real-time identity verification flows.

What is a video injection attack?

A video injection attack occurs when a fraudster routes a synthetic or pre-recorded video feed into an identity verification system through a virtual camera driver, bypassing liveness checks that only analyze camera input. Deepsight detects injection attacks at the signal level, not just the visual level.

What is liveness detection and why does it matter?

Liveness detection confirms that the person in front of the camera is physically present, not a photo, video, or deepfake. Without liveness detection, any biometric system can be spoofed with a printed photo or a deepfake video.

Does Deepsight work across devices and lighting?

Yes. Deepsight is designed for real-world conditions, operating accurately across mobile cameras, webcams, variable lighting, and different skin tones, maintaining consistent performance at scale.

Get in touch

Eliminate fraud and drive growth in a single platform

Orchestrate identity verification, compliance, and fraud prevention in one platform designed to grow with your business.

Request a demo → incode.com/contact