SWEAR™

SWEAR Authenticity Platform

WHITE PAPER

Creating AI-Resistant Evidence with Digital DNA Mapping and Blockchain Verification

Abstract

Artificial intelligence is changing the value of digital evidence. As AI-powered video manipulation tools become faster, cheaper, and harder to detect, organizations can no longer assume that digital evidence will be trusted simply because it exists. Traditional safeguards such as watermarking, encryption, and forensic analysis were not designed for the AI era in which evidence can be altered with extraordinary speed and precision. A new evidentiary standard is needed to combat these AI-based threats: one that creates an independent chain of custody to protect digital assets from the edge until evidence.

Your video may be real, but in the age of AI, real is not enough unless you can prove it.

Problem: A Global Crisis of Trust

Seeing is no longer believing. AI-generated deepfakes and synthetic media are eroding confidence in the authenticity of digital recordings across social media platforms, journalism, law enforcement, courts, corporate security, auditors, compliance, and the general public. For organizations that rely on digital evidence, this creates a serious risk. A recording may be real, but once its authenticity is questioned, its evidentiary value can be weakened, delayed, dismissed, or even weaponized.

The challenge facing industries that depend upon the authenticity of digital evidence is their reliance on decades old technologies to protect their digital assets. Advances in AI are circumventing legacy authenticity methods (including watermarking, encryption, localized hashing, and provenance) to create exposure and call into question the viability of digital authenticity.

Organizations need a new evidentiary standard: one that protects digital evidence at the point of creation and preserves independent proof that it has not been manipulated.

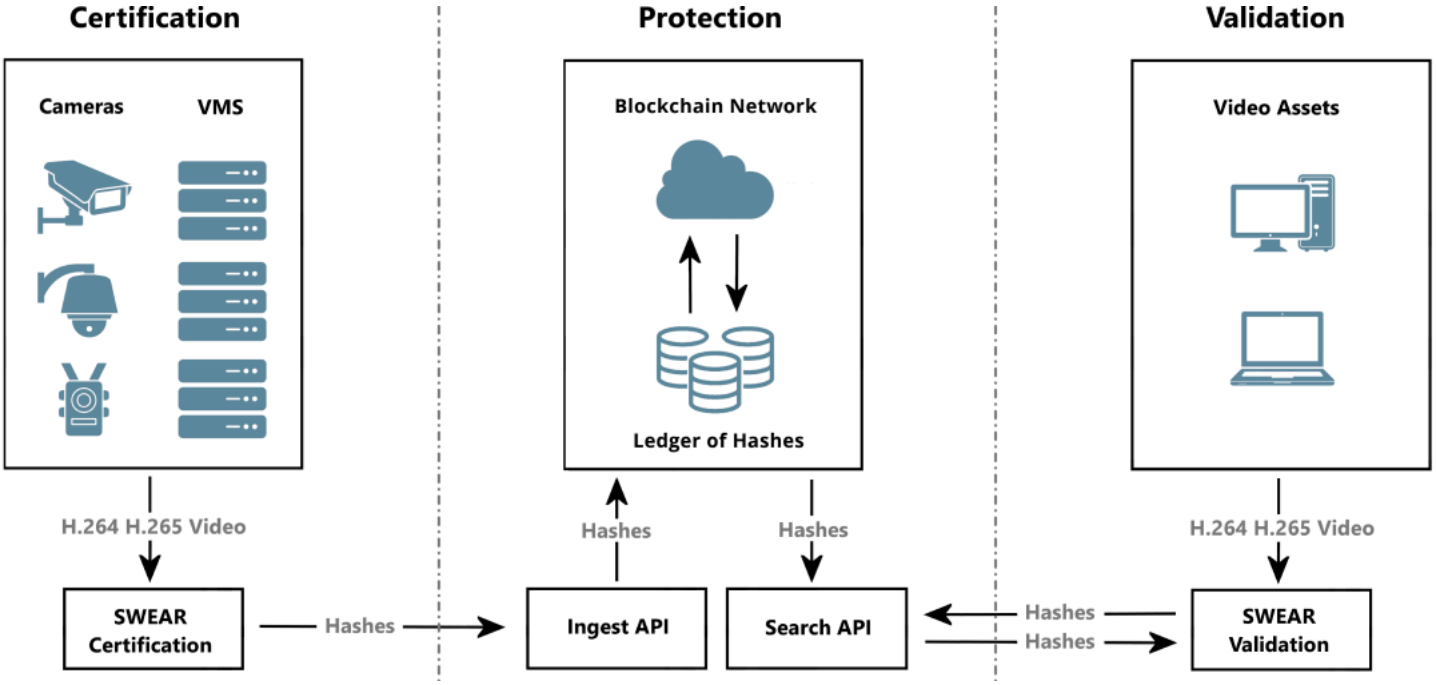
Solution: Creating AI-Resistant Video Evidence

SWEAR changes the authenticity model from after-the-fact analysis to proof at the point of creation. Rather than requiring investigators, courts, auditors, or security teams to determine if a recording has been manipulated, SWEAR creates an independent chain of custody while the video is being captured.

The result is a verification model that does not depend on trusting the storage system, the file owner, or the asset itself. The media remains under the organization's control, while the proof of authenticity is preserved independently and can be used later to verify the integrity of the evidence.

SWEAR separates the video asset from the proof of authenticity, allowing organizations to retain control of their media while preserving an independent record for verification.

SWEAR Architecture



Certification — Mapping With Cryptographic Hashes

The SWEAR Authenticity Platform directly integrates with content capture sources — including security cameras, body cameras, car cameras, smartphones, or any VMS stream. Cryptographic fingerprints are generated via secure hashing algorithms across multiple synchronized channels (visual frames, audio streams, and associated metadata). This multi-channel certification ensures any subsequent manipulation — whether splicing, audio dubbing, or metadata tampering — becomes instantly detectable. SWEAR supports all major media formats, including H.264, H.265, MJPEG, raw video streams, and compressed or uncompressed audio codecs.

Protection — Anchoring With Blockchain

Following certification, SWEAR anchors the generated Digital DNA into an independent ledger and then maps the DNA with a blockchain network. All anchored records contain only cryptographic fingerprints, timestamps, and opaque transaction identifiers. Identity management utilizes X.509 certificates while advanced access controls ensure strict permissioned participation.

Validation — Comparing Cryptographic Hashes

The SWEAR platform enables verification through a dedicated validation engine - available as standalone software or embedded into VMS playback systems. During playback or review, SWEAR recomputes the cryptographic fingerprints and compares them against the original fingerprints preserved on the ledger. The authenticity of content is compared frame-by-frame and second-by-second to create a forensic-grade validation to investigators, courts, auditors, compliance departments, or corporate security teams.

SWEAR Technical Features

- **Point-of-Creation Integrity**: SWEAR maps authenticity directly at capture and in real-time.
- **Blockchain-Backed Ledger**: Tamper-evident, distributed, and independently verifiable.
- **Pixel-Level Cryptographic Fingerprinting**: Every frame and pixel are protected.
- **Privacy Maintained:** Only hashes and timestamps are stored remotely in ledgers.
- **Real-Time Operation:** Certification and anchoring occur during recording - not after.
- **Seamless Integration:** Compatible with body cameras, smartphones, and VMS.
- **Scalable:** Designed to support enterprise surveillance systems and large-scale environments.

SWEAR turns video into evidence that organizations can prove, defend, and trust.

Primary Application Domains

Security & Surveillance

Protect operational video evidence from authenticity challenges after incidents, investigations, insurance claims, or public scrutiny.

Law Enforcement & Judiciary

Preserve digital evidence with an independent chain of authenticity that supports investigators, auditors, and legal review.

Media Integrity & Authenticity

Verify original recordings and distinguish authentic content from AI-generated, synthetic, or manipulated media.

Setting the Standard for Authentic Content

AI has changed what it takes for digital evidence to be trusted. Organizations can no longer rely on the existence of a recording alone. They need an independent chain of custody for proof that the recording is authentic, unchanged, and defensible from the moment it is created.

SWEAR does not simply help organizations protect digital evidence — it helps them prove it's real.

For demonstrations, technical integration details, or partnership inquiries, please visit www.swear.com.