SWEAR™

SWEAR Authenticity Platform

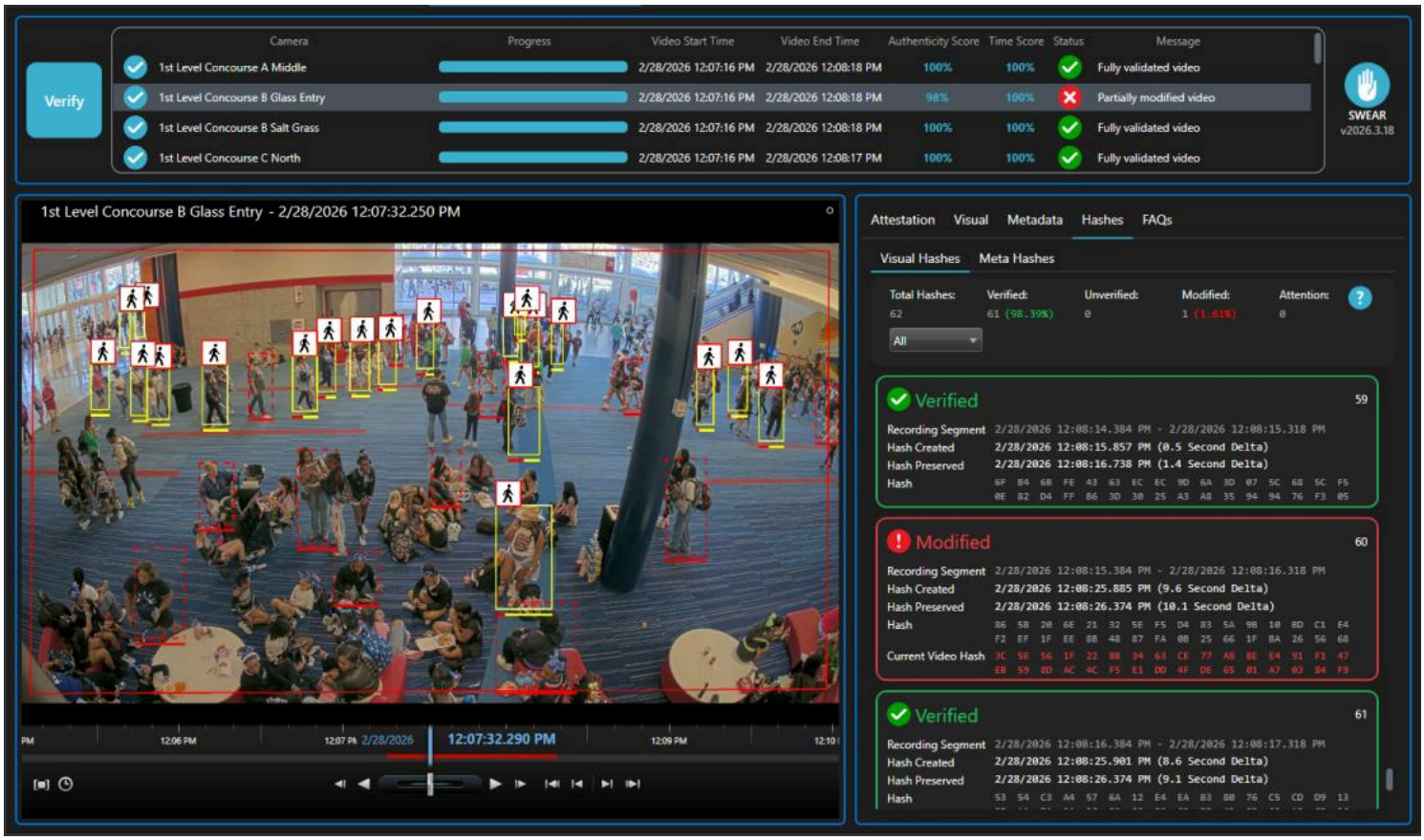
WHITE PAPER

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

Abstract

Artificial intelligence is changing the evidentiary value of digital media. As AI-manipulated video becomes faster, cheaper, and harder to detect, organizations can no longer assume that recordings will be trusted simply because it exists. Traditional safeguards such as watermarking, encryption, and forensic analysis were not designed for an era in which evidence can be altered with extraordinary speed and precision. A new standard is required: one that protects authenticity at the moment of capture by preserving the proof independently from the media itself.

In the age of AI, the burden is shifting from proving media is fake to proving it is real.



Problem Statement: A Global Crisis of Trust

Seeing is no longer believing. AI-generated deepfakes and synthetic media are eroding confidence in digital video, audio, and images across journalism, law enforcement, courts, corporate security, and public discourse.

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 weaponized. Legacy technologies such as forensic analysis, watermarking, and file-based security were not designed to prove authenticity at the moment of creation.

SWEAR answers that challenge by creating independent proof during recording, before manipulation, compression, redistribution, or dispute can occur. The result is AI-resistant video evidence that can be independently verified later with cryptographic confidence.

Creating AI-Resistant Video Evidence

SWEAR changes the authenticity model from after-the-fact detection to proof at the point of creation. Rather than trying to determine whether content has been manipulated, SWEAR creates an independent chain of custody that protects the authenticity of content from the edge all the way to it being viewed as evidence.

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

SWEAR protected recordings can not be modified without detection - even with AI-based manipulation tools.

Certification - Real Time Digital DNA Mapping

As digital content is captured — whether video, audio, or metadata — the SWEAR Authenticity Platform generates cryptographic fingerprints (hashes) for every frame, pixel, audio sample, and data channel. This process occurs entirely within the customer's environment, ensuring that no private content, device identifiers, or user data ever leave the system. Privacy is maintained. Only the Digital DNA is preserved with cryptographic fingerprints — mathematically derived hashes that cannot be reverse-engineered.

Patents: #10,560,261; #10,853,456; #11,669,598; #11,683,180; #11,755,693; #11,886,544

Protection - Immutable and Independent Chain-of-Custody

SWEAR anchors the Digital DNA fingerprints with a blockchain-protected ledger, creating an immutable chain of custody that records each content fingerprint with timestamps and cryptographic hashes. No personal/private information, device IDs, or client data ever leave the customer's environment. The ledger stores only what is essential for proof: cryptographic fingerprints and temporal anchors.

A distributed blockchain network creates the final audit layer to protect the authenticity of the Digital DNA.

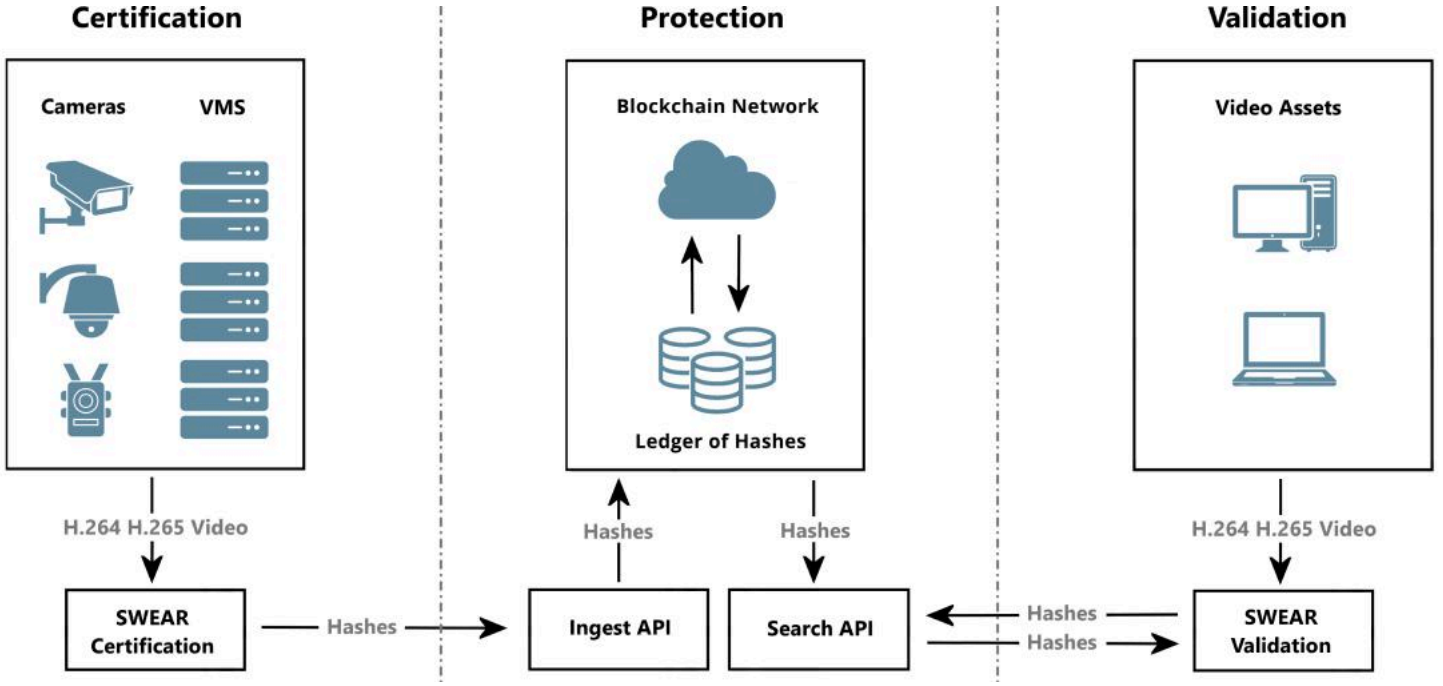
Patents: #10,355,865; #11,941, 090

Validation - Pixel Level Precision On-Demand Proof

At any point — moments later or years in the future — the authenticity of SWEAR-certified content can be instantly verified. The SWEAR Validation System recalculates the Digital DNA of a current recording and compares it to the original fingerprints protected by blockchain. If even a single pixel in a single frame has been altered, SWEAR' s precision will flag the counterfeit second. Investigators, journalists, regulators, courts, and enterprise security teams can determine whether content remains authentic or whether it has been altered.

Patents: #10,348,505; #11,055,384; #11,163,855; #12,278,856

Architecture



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

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 Authenticity Platform enables verification through a dedicated validator engine — available as standalone software or embedded into VMS playback systems. During playback or review, SWEAR re-computes the live content's fingerprints and compares them against the originals protected on the ledger. The authenticity of content can be proven by providing forensic-grade validation to investigators, courts, or corporate security teams.

Technical Features of the SWEAR Authenticity Platform

- **Point-of-Creation Integrity**: SWEAR maps authenticity directly at capture and in real-time.
- **Independent Blockchain-Backed Ledger**: Tamper-evident, distributed, and independently verifiable.
- **Pixel-Level Cryptographic Fingerprinting**: Every frame, channel, and critical data element can be verified.
- **No Original Media Stored**: Only hashes and timestamps are stored remotely in ledgers — protecting privacy.
- **Real-Time Operation:** Certification and anchoring occur during recording without interrupting workflows.
- **Seamless Integration:** Compatible with body cameras, smartphones, surveillance networks, and VMS.
- **Scalable:** Designed to support enterprise surveillance systems and large-scale video environments.

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

Primary Application Domains

Security & Surveillance

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

Law Enforcement & Judiciary

Preserve defensible digital evidence with an independent chain of authenticity that supports investigators, prosecutors, courts, 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 media to be trusted. Organizations can no longer rely on the existence of a recording alone. They need 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 manage digital media. It helps them prove what is real.

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