SWEAR™

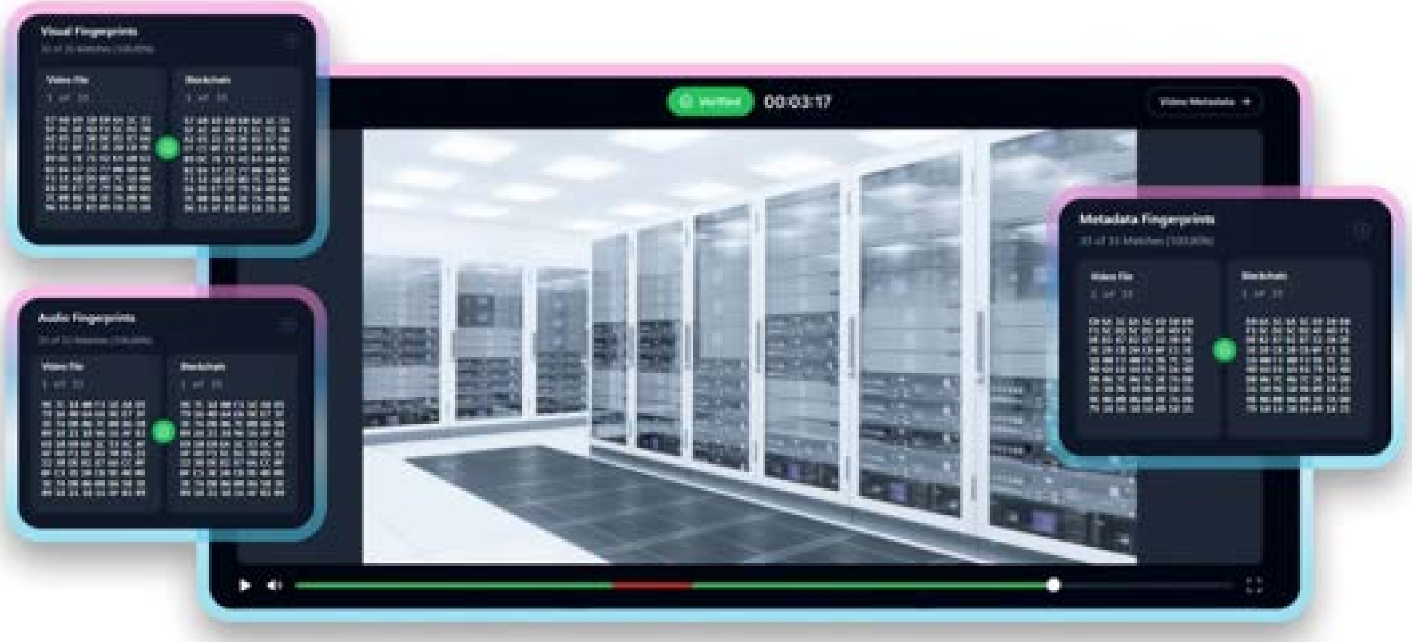
Technical White Paper: SWEAR Authenticity Platform

AI-Resistant Digital Recordings

● TECHNICAL WHITE PAPER

Abstract

The SWEAR Authenticity Platform delivers uncompromising, real-time digital content authenticity at the point of creation. In an era where AI-powered deepfakes and synthetic media threaten the credibility of digital evidence, SWEAR empowers organizations to protect truth at the source. By embedding cryptographic fingerprints directly into digital content the moment it's captured, and securing those fingerprints on blockchain, SWEAR transforms digital media into tamper-evident, verifiable records that can be trusted forever.



Problem Statement: A Global Crisis of Trust

Seeing is no longer believing. AI-generated deepfakes and synthetic content are eroding confidence in digital media, undermining the credibility of journalism, courts, law enforcement, corporate security, and public discourse. When anyone can forge convincing fake videos or audio, every piece of digital evidence becomes suspect. Without provable authenticity, even genuine content can be weaponized or dismissed. The world needs more than forensic detection after-the-fact — it needs proof of truth at the moment of creation.

SWEAR exists to answer that call.

The SWEAR Approach: Locking In Authenticity at Capture

The SWEAR Authenticity Platform flips the deepfake problem on its head. Rather than trying to identify which content is fake after it's already circulating, SWEAR ensures that digital content is born authentic — with an unbreakable chain of trust that follows it wherever it goes. We capture, anchor and verify digital content in real time.

Certification: Digital DNA Mapping

As digital content is captured — whether video, audio, or metadata — the SWEAR Authenticity Platform generates cryptographic fingerprints 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. Only the cryptographic Digital DNA — mathematically derived hashes that cannot be reverse-engineered — are generated and secured. This separation of channels (visual, audio, metadata) enables granular integrity tracking across every layer of digital content.

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

Blockchain Anchoring: Immutable Chain-of-Custody

SWEAR anchors the Digital DNA fingerprints to a distributed, permissioned blockchain ledger — creating an immutable chain-of-custody that permanently records each content fingerprint with timestamps and opaque, non-identifiable metadata. No personal information, device IDs, or client data ever enter the blockchain. The ledger stores only what is essential for proof: cryptographic fingerprints and temporal anchors.

The blockchain network is designed for ultimate flexibility — customers can choose to deploy SWEAR's ledger infrastructure as SWEAR-hosted, self-hosted, fully on-premises, or across any major cloud provider.

Patents: #10,355,865

Verification: Instant Proof of Authenticity

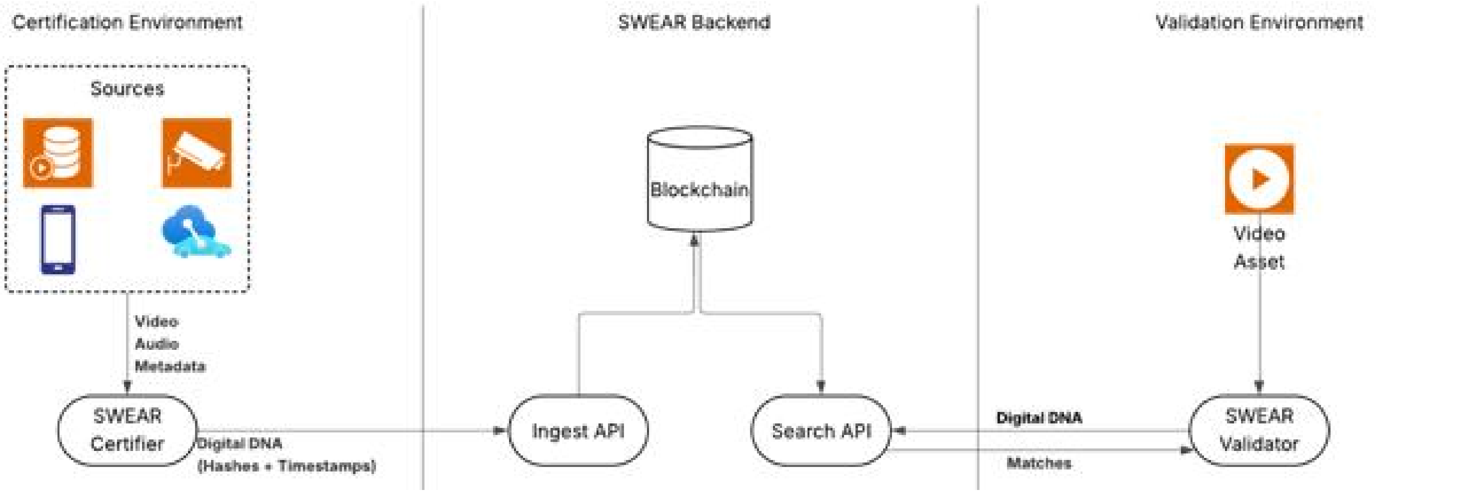
At any point — moments later or years in the future — the authenticity of SWEAR-certified content can be instantly verified. Our verification engine recalculates the current Digital DNA and compares it to the original fingerprint on the blockchain. Even a single altered pixel, frame, or audio sample triggers instant tamper-evidence. This isn't guesswork or probability — it's cryptographically absolute. Investigators, journalists, regulators, or courts can obtain definitive proof: either the content remains authentic or it has been altered, and exactly where.

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

Technical Features of the SWEAR Authenticity Platform

- **Point-of-Creation Integrity**: SWEAR maps authenticity directly at capture and in real-time.
- **Immutable Blockchain Ledger**: Tamper-proof, distributed, and permanent.
- **Pixel-Level Cryptographic Fingerprinting**: Every frame, every channel, and every detail is secured.
- **Zero Identifiable Data Exposure**: Only hashes and timestamps are stored in blockchain — protecting privacy.
- **Deployment Flexibility:** SWEAR-hosted, self-hosted, on-premises, or cloud — full customer control.
- **Real-Time Operation:** Certification and anchoring happen during recording, without interrupting workflows**.**
- **Seamless Integration:** Compatible with body cameras, smartphones, surveillance networks, and VMS.
- **Scalable:** From individuals to enterprise surveillance systems, SWEAR operates efficiently at any scale.
- **Lightweight:** Minimal impact on infrastructure — less than 1Mb of Digital DNA protects one hour of video.

Technical Specifications



Certification (Capture)

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.

Protecting (Anchoring to Blockchain)

Following certification, SWEAR anchors the generated Digital DNA into Hyperledger Fabric — a permissioned enterprise-grade blockchain optimized for privacy, resilience, and transaction finality. 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. SWEAR's architecture eliminates the risk of forks, retroactive manipulation, or unauthorized ledger tampering.

Validation (Verification On Demand)

The SWEAR Authenticity Platform enables validation 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 immutable originals stored on the blockchain. Even after years of storage or countless copies, the authenticity of content can be proven or challenged within seconds, providing forensic-grade verification to investigators, media outlets, courts, or corporate security teams.

Primary Application Domains

Security & Surveillance

SWEAR ensures surveillance and operational video assets remain authentic and forensically verifiable.

Law Enforcement & Judiciary

SWEAR creates a secure chain-of-custody for digital evidence that withstands legal challenges.

Media Integrity & Journalism

SWEAR protects the credibility of reporting and enables outlets to distinguish real footage from forgeries.

Setting the Standard for Authentic Content

SWEAR defines a new global standard for digital truth. We don't chase fakes after the damage is done — we prevent tampering at its root by embedding authenticity at creation. With cryptographic fingerprints, blockchain anchoring, and real-time verification, SWEAR makes content authenticity provable, permanent, and indisputable.

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