Tectra

Content Authenticity as a Service

Multi-Layer Provenance for the AI Content Era

Technical Solution Brief

Version 1.0 — March 2026

https://tectra.vision

Contents

Executive Summary

The proliferation of generative AI has created an unprecedented crisis in digital content trust. The volume of AI-generated images and video has grown exponentially, with major platforms reporting millions of synthetic media items created daily. Regulatory bodies worldwide—from the European Union's AI Act to emerging U.S. federal legislation—are increasingly mandating provenance tracking and disclosure for AI-generated media.

Tectra is a **Content Authenticity as a Service** platform that provides organizations with a turnkey, API-first solution for establishing and verifying the provenance of digital images and video. Rather than attempting to *detect* whether content was generated by AI—an arms race that generative models consistently win—Tectra takes a **provenance-first approach**: cryptographically signing content at the point of creation and embedding multiple independent layers of tamper-evident proof.

The platform combines **four independent verification layers**—cryptographic signatures, invisible watermarking, content fingerprinting, and blockchain anchoring—into a single API call. When any of these layers is verified, the content's origin, creator, and integrity can be confirmed with high confidence, even after compression, cropping, screenshotting, or re-encoding.

Layer 1: Cryptographic Signing Non-repudiable identity binding

Layer 2: Invisible Watermarking Survives compression & cropping

Layer 3: Content Fingerprinting Visual similarity detection

Layer 4: Blockchain Anchoring Immutable timestamped proof

Key Value Propositions

- **API-First Architecture:** Sign and verify content with a single REST API call or Python SDK invocation. Integration takes minutes, not months.
- **Multi-Layer Redundancy:** Four independent verification methods ensure authenticity survives any single point of failure or attack vector.
- **Origin Transparency:** Content is tagged with its source type—camera model, AI generator, creative tool—enabling downstream consumers to make informed trust decisions.
- **Regulatory Readiness:** Built-in support for EU AI Act provenance requirements and emerging digital content legislation.
- **Flexible Deployment:** Cloud API, Python SDK for local signing, and a Docker Agent for zero-code integration with camera systems and AI pipelines.

The Problem: A Crisis of Digital Trust

The AI Content Explosion

Generative AI has fundamentally altered the landscape of digital media production. Tools such as DALL-E, Midjourney, Stable Diffusion, and Sora can produce photorealistic images and video that are indistinguishable from authentic captures—at scale, at negligible cost, and by anyone with an internet connection. The barrier to creating convincing synthetic media has dropped to near zero: a single text prompt can generate a photorealistic image in seconds.

Trust Erosion Across Industries

The consequences extend far beyond social media misinformation:

- **Journalism & Media:** Newsrooms face growing difficulty verifying the authenticity of user-submitted photos and video, as AI-generated imagery becomes increasingly convincing.
- **Legal & Forensic Evidence:** Courts are beginning to question the admissibility of digital photographs as evidence, given the ease of undetectable manipulation.
- **Medical Imaging:** Manipulated radiology scans could lead to misdiagnosis. The integrity of diagnostic images is increasingly important.
- **Financial Services:** KYC document fraud using AI-generated identity documents is a growing concern across the industry.
- **Insurance:** AI-generated damage photos for fraudulent claims represent a growing loss vector.
- **National Security:** Deepfake campaigns targeting elections and public discourse have been documented across multiple countries.

The Regulatory Response

Governments worldwide are responding with legislation that increasingly requires provenance tracking:

- **EU AI Act (2024):** Mandates that AI-generated content be labeled and traceable. High-risk AI systems must maintain provenance records.
- **U.S. DEEPFAKES Accountability Act:** Requires digital watermarking of AI-generated content.
- **China's Deep Synthesis Regulations:** Mandates labeling and traceability for all synthetically generated media.

Why Detection Alone Fails

The conventional approach—training classifiers to distinguish AI-generated from authentic content—faces a fundamental limitation: **it is an arms race that defenders consistently lose.**

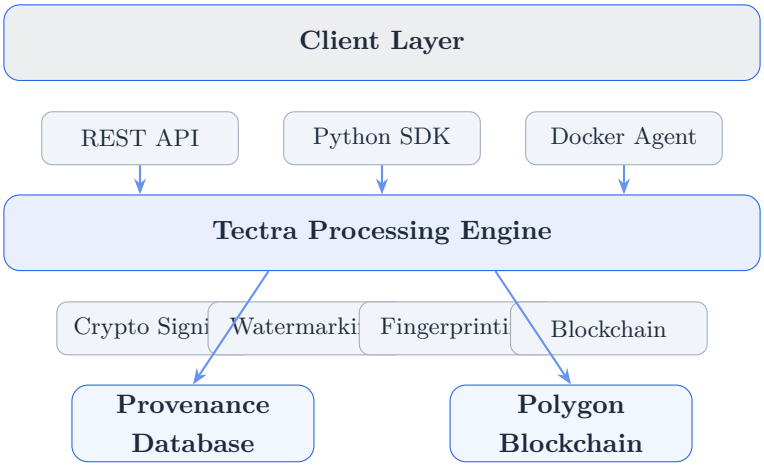
1. **Adversarial evolution:** Each new generation of AI models is specifically trained to evade detection artifacts.
2. **False positive risk:** Even a 1% false positive rate at scale means millions of authentic images incorrectly flagged.
3. **Post-hoc limitation:** Detection can only be performed after content is published and potentially viral.
4. **No attribution:** Even when detected, AI content detectors cannot identify *who* created the content or *when*.

The provenance-first approach inverts this model: instead of asking "is this content fake?" after the fact, it ensures that authentic content carries cryptographic proof of its origin from the moment of creation. The question becomes "can this content prove where it came from?"—a fundamentally more tractable problem.

The Tectra Platform

Tectra provides a unified content authenticity infrastructure that embeds multiple independent layers of provenance into digital media at the point of creation. Each layer is designed to survive different classes of content transformation, ensuring that at least one verification path remains intact regardless of how the content is subsequently processed, compressed, or distributed.

Architecture Overview



The Four Verification Layers

Layer 1: Cryptographic Signing

Every piece of content processed through Tectra is cryptographically signed using **Ed25519 digital signatures**—the same elliptic curve algorithm used by SSH, Signal, and major blockchain networks. Each user generates a unique signing keypair, and the private key is encrypted at rest using authenticated encryption.

The signature binds the content's cryptographic hash, visual fingerprint, timestamp, and signer identity into a single non-repudiable proof. Verification requires only the signer's public key, enabling offline and third-party verification without contacting Tectra's servers.

Layer 2: Invisible Watermarking

Tectra embeds an invisible watermark into the frequency domain of each image using advanced signal processing techniques. The watermark:

- Is **imperceptible** to the human eye (no visible artifacts or quality degradation)
- **Survives** JPEG compression, resolution scaling, moderate cropping, and format conversion
- Carries a **cryptographic payload** derived from the content's digital signature

- Can be **extracted and matched** against the provenance database with tolerance for signal degradation

This layer is particularly valuable for content that is screenshotted, re-uploaded to social media, or otherwise stripped of metadata—the watermark persists in the pixel data itself.

Layer 3: Content Fingerprinting

Tectra computes a **perceptual fingerprint** of each image and video—a compact numerical representation of visual content that remains stable across transformations. Unlike cryptographic hashes (which change if a single bit is modified), perceptual fingerprints enable:

- Detection of **near-duplicate** content (cropped, resized, recompressed)
- **Fuzzy matching** with configurable similarity thresholds
- **Video-level fingerprinting** that aggregates frame-level analysis into a single stable identifier

Content can be matched to its original registration even after substantial visual transformation, enabling provenance tracking across the content lifecycle.

Layer 4: Blockchain Anchoring

Content provenance records are anchored to the **Polygon blockchain**, providing an immutable, publicly auditable timestamp proof. Tectra uses an efficient batching architecture that groups multiple content registrations into a single on-chain transaction via cryptographic accumulation, achieving:

- **Sub-cent transaction costs** per content item (amortized across batches)
- **10-second anchoring intervals** for near-real-time blockchain confirmation
- **Independent verifiability** via any Polygon block explorer or RPC node
- **Mathematical proof** that specific content existed at a specific time

Each content item receives an individual cryptographic proof linking it to the on-chain record, enabling third-party verification without access to other items in the batch.

Origin Type Taxonomy

Every piece of signed content is tagged with an **Origin Type** that declares its source. Tectra maintains a comprehensive taxonomy across seven categories:

Category	Examples
Camera	DSLR, smartphone, security camera, dashcam, drone, body camera
AI Generator	DALL-E, Midjourney, Stable Diffusion, Sora, custom models
Creative Tools	Photoshop composite, Figma design, Blender render
Medical Imaging	Radiology scan, pathology slide, ultrasound
Document	Scanned document, digital certificate
IoT / Sensor	Satellite imagery, industrial inspection, scientific instrument
Other	User-generated, archival digitization

This taxonomy enables downstream consumers to make informed trust decisions. An AI-generated marketing image carries different trust implications than a camera capture from a credentialed photojournalist—and Tectra makes this distinction explicit and verifiable.

Verification & Confidence Scoring

When content is submitted for verification, Tectra independently evaluates each of the four provenance layers and produces a **composite confidence score**. The system reports:

- Which layers passed, failed, or were inconclusive
- The matched origin type and signer identity (if found)
- Blockchain transaction references for independent audit
- A human-readable authenticity determination

The multi-layer approach means that even heavily transformed content (compressed, cropped, re-encoded) can often be authenticated through the layers that survive transformation, while pristine content achieves maximum confidence through unanimous layer agreement.

Integration & Deployment Models

Tectra is designed for rapid integration into existing workflows. Organizations can choose the deployment model that best fits their architecture—from a single API call to a fully autonomous signing agent.

REST API

The Tectra REST API enables signing and verification with standard HTTP requests. Integration requires no specialized libraries or infrastructure.

Sign an image via the API

```
curl -X POST https://api.tectra.vision/api/v1/sign \
  -H "Authorization: Bearer $TECTRA_API_KEY" \
  -F "file=@photo.jpg" \
  -F "signing_key_id=$KEY_ID"
```

Verify an image (no authentication required)

```
curl -X POST https://api.tectra.vision/api/v1/verify \
  -F "file=@photo.jpg"
```

The API returns structured JSON including the authenticity determination, confidence score, individual layer results, origin type, signer identity, and blockchain references.

Python SDK

For applications requiring local signing (keeping content on-premise), the Tectra Python SDK performs watermarking and hashing locally, transmitting only metadata to the cloud for blockchain anchoring.

Local signing with the Python SDK

```python
from tectra_sdk import TectraClient

client = TectraClient(
    api_key="iai_your_key_here",
    signing_key_id="your-key-uuid"
)

# Sign locally, register metadata in the cloud
result = client.sign("photo.jpg")
print(f"Record ID: {result.record_id}")
print(f"Blockchain TX: {result.tx_hash}")
```

Docker Signing Agent

For zero-code deployments, the Tectra Docker Agent watches filesystem directories and automatically signs new images and videos as they appear. Ideal for:

- Security camera systems writing frames to a shared volume
- AI inference pipelines generating images to a designated output directory
- Photojournalism workflows with tethered camera capture
- Medical imaging systems exporting DICOM files

Deploy the signing agent

```
docker run -d \
  -v /camera-feed:/data/input \
  -v /signed-output:/data/signed \
  -v ./config.yaml:/app/config.yaml \
  tectravision/agent:latest
```

The agent requires only a YAML configuration file specifying the API credentials, watch directories, file patterns, and origin type metadata.

Web Dashboard

The Tectra web dashboard provides a visual interface for:

- Managing API keys and signing keys with origin type assignments
- Monitoring signing and verification activity with usage analytics
- Browsing provenance records with blockchain transaction links
- Performing ad-hoc signing and verification via drag-and-drop upload

Use Cases

AI Companies: Regulatory Compliance

As the EU AI Act and similar regulations mandate provenance labeling for AI-generated content, AI companies face a compliance burden. Tectra provides a drop-in solution:

- Integrate the Tectra API into the image/video generation pipeline
- Every output is automatically signed with the AI model's origin type (e.g., "DALL-E," "Stable Diffusion," "Custom Model")
- Blockchain anchoring provides an immutable audit trail for regulators
- Invisible watermarks persist even after content is reposted or compressed

Value: Demonstrate regulatory compliance with provenance-tracked AI outputs through a single API integration.

News & Media: Photojournalism Authentication

News organizations need to verify the authenticity of field-submitted photographs and video. With Tectra:

- Photojournalists sign images at the point of capture using the mobile SDK or Docker Agent on tethered laptops
- Editors verify submissions with a single API call or dashboard upload
- Published images carry embedded provenance that readers and fact-checkers can independently verify
- Blockchain timestamps prove that the image existed before the reported event timeline

Value: Restore audience trust and differentiate authentic reporting from AI-generated misinformation.

Legal & Forensic: Digital Evidence Chain of Custody

Digital photographs and video are increasingly challenged in court proceedings. Tectra establishes an unbroken chain of custody:

- Evidence is signed at the moment of capture with device-specific signing keys
- Blockchain anchoring provides tamper-proof timestamps admissible as evidence
- Multi-layer verification demonstrates that content has not been altered since capture
- Origin type metadata identifies the specific capture device

Value: Strengthen the admissibility and credibility of digital evidence in legal proceedings.

Medical Imaging: Diagnostic Integrity

Medical imaging integrity is critical for patient safety. Tectra protects DICOM and diagnostic images:

- Imaging systems sign outputs via the Docker Agent watching export directories
- Perceptual fingerprinting detects if images have been subtly altered
- Blockchain timestamps establish when a scan was performed
- Audit trails support HIPAA compliance and malpractice defense

Value: Protect patient safety and provide defensible proof of diagnostic image integrity.

Security & Surveillance: Camera Feed Authentication

Security camera footage is increasingly questioned as deepfake technology advances. Tectra ensures footage integrity:

- The Docker Agent integrates directly with camera NVR systems
- Every frame or clip is signed with the camera's unique identity and location metadata
- Invisible watermarks persist even if footage is screen-recorded or re-encoded
- Verification is available to law enforcement and insurance adjusters via the public API

Value: Ensure surveillance footage remains admissible and trustworthy as evidence.

Art & Creative: Creator Attribution

Digital artists and content creators need to prove original authorship:

- Sign artwork at the point of creation with a verified creator identity
- Blockchain anchoring provides irrefutable proof of creation date
- Perceptual fingerprinting detects unauthorized copies and derivatives

Value: Protect intellectual property and enable verifiable creator attribution across the internet.

Competitive Landscape

The content authenticity space includes several established players. Tectra differentiates through its combination of breadth, accessibility, and developer-first design.

Capability	Tectra	Truepic	Digimarc	Adobe CAI	Numbers
Cryptographic Signing	✓	✓	–	–	✓
Invisible Watermarking	✓	–	✓	–	–
Perceptual Fingerprinting	✓	–	✓	–	–
Blockchain Anchoring	✓	–	–	–	✓
Self-Serve API	✓	–	–	–	✓
Python SDK	✓	–	–	–	–
Docker Agent	✓	–	–	–	–
Video Support	✓	Limited	–	–	–
Origin Taxonomy	✓	Limited	–	–	–

Key Differentiators

1. **Four-layer redundancy:** No competitor combines all four verification methods. Most rely on one or two layers, creating single points of failure.

2. **Developer-first:** Self-serve API signup, comprehensive SDK, and Docker Agent. Competitors typically require enterprise sales engagement.

3. **Full media support:** Image and video signing with frame-level verification. Most competitors focus exclusively on still images.

4. **Open verification:** Anyone can verify content without an account. Signing requires authentication; verification is free and public.

5. **Origin transparency:** Comprehensive origin type taxonomy across seven categories, enabling nuanced trust decisions beyond binary "real or fake."

Security & Compliance

Cryptographic Standards

Tectra employs industry-standard, peer-reviewed cryptographic primitives throughout the platform:

Function	Algorithm	Standard
Digital Signatures	Ed25519	RFC 8032, NIST recommended
Content Hashing	SHA-256	FIPS 180-4
Key Encryption at Rest	Fernet (AES-128-CBC)	Built on NIST AES
Password Hashing	bcrypt	Industry standard, adaptive cost
Transport Security	TLS 1.3	IETF RFC 8446
Blockchain Signatures	ECDSA (secp256k1)	Polygon/Ethereum standard

Data Handling & Privacy

Tectra is designed with a **metadata-only** architecture by default:

- Content files are **not stored** on Tectra servers. Only cryptographic hashes, fingerprints, signatures, and metadata are retained.
- The SDK enables **fully local signing**—content never leaves the customer's infrastructure. Only metadata is transmitted for blockchain anchoring.
- All API communication occurs over TLS 1.3 encrypted connections.
- Private signing keys are encrypted at rest using authenticated encryption and are never transmitted in plaintext.

Compliance Readiness

- **EU AI Act:** Tectra's origin type taxonomy directly addresses the Act's requirements for AI content labeling and traceability.
- **GDPR:** Metadata-only architecture minimizes personal data processing. Content hashes are not considered personal data under GDPR guidance.
- **HIPAA:** The SDK's local-signing mode ensures protected health information never leaves the customer's environment.
- **SOC 2:** Architecture supports SOC 2 Type II compliance requirements for access control, encryption, and audit logging.

Product Roadmap

Current Capabilities (Shipped)

- Four-layer image authentication (sign, watermark, fingerprint, blockchain)
- Video authentication with frame-level signing and verification
- REST API with JWT and API key authentication
- Python SDK with local signing and directory watching
- Docker Signing Agent for zero-code deployments
- Web dashboard with key management and usage analytics
- Origin type taxonomy (7 categories, 25+ types)
- Polygon blockchain anchoring with batched Merkle proofs
- User management with email verification and password reset

Near-Term (Q2–Q3 2026)

- **Audio authentication:** Extend the signing and verification pipeline to audio files, addressing the growing threat of AI-generated voice content and audio deepfakes.
- **Mobile SDKs:** Native iOS and Android SDKs for signing content directly on mobile devices at the point of capture.
- **Real-time streaming:** WebSocket-based API for signing and verifying content in real-time video streams (RTSP, WebRTC).
- **Browser extension:** Chrome/Firefox extension enabling one-click verification of images encountered while browsing.
- **Webhook notifications:** Event-driven notifications for verification attempts, blockchain confirmations, and usage alerts.

Mid-Term (Q4 2026–Q1 2027)

- **Multi-chain anchoring:** Expand blockchain support beyond Polygon to Ethereum L1, Arbitrum, and Base for customer choice and redundancy.
- **AI detection integration:** Complement provenance-first verification with statistical AI detection as a supplementary signal (not primary).

- **Hardware secure element integration:** Partner with camera manufacturers to embed Tectra signing directly into camera firmware using hardware security modules.
- **Federation protocol:** Enable multiple Tectra instances to cross-verify provenance records, supporting decentralized deployment for government and enterprise customers.

Long-Term Vision

Tectra aims to become the **trust infrastructure layer** for all digital media—an invisible, ubiquitous system where every authentic image, video, and audio file carries verifiable provenance from creation to consumption. As AI-generated content becomes indistinguishable from reality, provenance becomes the only reliable mechanism for establishing digital trust.

Get Started with Tectra

Start Building with Tectra Today

Sign up for an account and begin authenticating content in minutes.

Web: https://tectra.vision

API Docs: https://tectra.vision/docs/api-reference

Contact: hello@tectra.vision

Step 1

Create an account & generate your API key

Step 2

Sign your first image with a single API call

Step 3

Verify content authenticity from anywhere

Version 1.0 — March 2026