

CLAIMS

1. A system for policy-gated authentication and cryptographic hashing, the system comprising :

an authentication policy engine, wherein the engine loads an authentication policy and evaluates an inbound media content against Boolean requirements;

plurality of pluggable authentication source adapters in communication with the authentication policy engine, wherein each of the adapter module evaluates the media content and returns a standardized result object;

a virtualization engine comprising a Sample Indexing Module, wherein the engine interrogates structural container data to map individual binary samples within a media data (MDAT) section by recording a byte offset and a temporal position;

a Sample Identity Manifest (SIM) Registry, wherein the registry stores a compound record comprising cryptographic hashes of a subset of the mapped binary samples and an Authentication Provenance Bundle in an immutable registry; and

an assembly-time verification module, wherein the module processes the virtual video containers by computing real-time cryptographic hashes from binary byte streams, fetches media samples from remote sources and performs a comparison against registered SIM hashes, confirming the authenticity of media content at the binary sample level.

2. The system of claim 1, further comprising a token validation module to validate a cryptographically validated control layer that governs conditions under which the virtual video container is permitted to resolve and assemble.
3. The system of claim 1, wherein the standardized result object comprises a source identifier, a confidence score and a verdict.
4. The system of claim 1, wherein the virtualization engine interrogates structural atoms of an MP4 file to extract sample tables and timing metadata.
5. The system of claim 1, wherein the immutable registry provides a traceable provenance chain report surfacing identities of contributing authentication source adapter modules and the signed authentication policy.
6. The system of claim 1, wherein the Sample Identity Manifest survives re-encoding of the media content by identifying a binary hash mismatch between the real-time hashes and the cryptographic hashes stored in the SIM registry.
7. The system of claim 1, wherein the Boolean requirements utilize composable operators that may include ALL OF, ANY OF, and N OF M to define graduated trust thresholds.
8. The system of claim 6, wherein the cryptographic hashes are computed once at a point of registration, and the confirmed authenticity is inherited by subsequent assemblies through hash comparisons.
9. The system of claim 1, wherein the assembly-time verification module performs real-time hash comparisons of the received binary samples against the registered SIM to confirm authenticity during playback.

10. A computer-implemented method for policy-gated sample-level content authentication, the method comprising the steps of ;
- a) receiving digital footage at an ingestion endpoint with a reference to a signed authentication policy and invoking plurality of authentication adapters via an authentication policy engine to generate evaluation results;
 - b) subjecting the results of step a to a Boolean policy evaluation using composable operators;
 - c) handling operational edge cases through pre-defined rules within the policy object, wherein the engine fails ingestion, skips checks, or routes the asset if an authentication source is unavailable or returns an inconclusive result;
 - d) virtualizing the footage through the Sample Indexing Module to extract structural metadata to map every discrete codec-encoded unit of media and executing a selection algorithm to choose a specific subset for hashing;
 - e) computing cryptographic hashes of the raw binary data for each selected sample within the MDAT section;
 - f) compiling the individual hashes and an Authentication Provenance Bundle into a compound Sample Identity Manifest (SIM) and registering said SIM in an immutable registry;
 - g) performing an assembly-time verification during a playback request by retrieving registered hashes from the SIM registry and fetching binary samples from a remote source;
 - h) hashing received binary sample as the virtual video engine processes the stream and comparing computed values against the registered SIM hashes; and

- i) executing a response based on a pre-selected verification mode and generating a provenance chain report.
11. The method of claim 10, wherein the composable operators may include ALL OF, ANY OF or N OF M.
 12. The method of claim 10, wherein the authentication adapters may include content provenance verifier (C2PA), a Photo Response Non-Uniformity (PRNU) camera sensor fingerprint analyzer, a codec forensics engine for compression artifact analysis, a generative artificial intelligence classifier, a studio production attestation validator, and a hardware capture device registry.
 13. The method of claim 10, wherein the policy is a signed data object authored by a rights holder to define specific trust thresholds for registration.
 14. The method of claim 10, wherein the verification mode may include a strict mode that blocks assembled video output upon a hash mismatch, an advisory mode that signals unverified samples to a user interface or an audit mode that logs verification results without interrupting playback .
 15. The method of claim 10, wherein the structural metadata may include a Sample Table (STBL), a Decoding Time to Sample table (STTS) and a Chunk Offset table (STCO).
 16. The method of claim 10, wherein the progressive assembly of digital video content is initiated by a cryptographic video token encoding user permissions and licensing terms, and wherein the assembly-time verification is a mandatory condition for validating the cryptographic video token.
 17. The method of claim 10, wherein the selection algorithm may be selected from deterministic, pseudorandom, or I-frame biased methods to choose a specific subset of the indexed individual binary samples for hashing.

18. The method of claim 10, wherein the Sample Identity Manifest (SIM) further comprises a signed Authentication Provenance Bundle to the immutable registry, bundle containing every standardized result object, evaluation timestamps, verifier signatures, and the specific version of the signed authentication policy applied.

19. The method of claim 18, wherein the immutable registry comprises a distributed ledger that provides a permanent, consensus-validated, and timestamped record of the SIM and the signed authentication provenance bundle.

20. The method of Claim 10, wherein the provenance chain report identifies which samples were verified, the token conditions under which the assembly occurred and the original trust signals provided by the authentication sources.