

ABSTRACT

A system and computer-implemented method for policy-gated sample-level authentication and cryptographic verification of digital media content are disclosed. The system includes an authentication policy engine configured to evaluate media content against Boolean trust requirements using multiple pluggable authentication source adapters. A virtualization engine indexes binary media samples within a media data section by extracting structural metadata and mapping byte offsets and temporal positions. Selected samples are hashed and compiled into a Sample Identity Manifest (SIM) together with an Authentication Provenance Bundle, which is stored in an immutable registry. During playback or assembly, an assembly-time verification module retrieves registered hashes, computes real-time hashes from streamed binary samples, and compares the computed hashes with the registered SIM hashes to verify authenticity at a sample level. The system further supports configurable verification modes, cryptographic token validation, provenance reporting, and traceable authentication workflows for secure media virtualization, licensing, and content integrity management.