



SUMMER 2026 E-NEWSLETTER

At Digital Mountain, we assist our clients with their electronic discovery, digital forensics, cybersecurity, and data analytics needs. For this E-Newsletter, we discuss how AI technology is pitting the forger and the authenticator in the battle over digital media in the legal arena.

AI-Powered Solutions for Digital Media Authentication: A Market Overview

An authenticator doesn't rely on a single method. They may choose pigment analysis for one painting, X-ray for another, and provenance research for a third. The tool pivots with the digital investigative demands. The same is true for digital media authentication in the age of Generative AI. As AI-generated images, audio, and video have become increasingly realistic and easier to produce, no single forensics tool answers every authenticity question. Additionally, real time authentication, verifying a person's identity live, in a video call



or biometric check, has become its own urgent front, as increasing numbers of fake remote workers are infiltrating organizations according to the Department of Justice ([press release](#)). In this article, we'll take a look at a small selection of authentication tools on the market.

Sensity AI ([sensity.ai](#)) is built to detect deepfakes directly, running a multilayer analysis across visual pixel structure, audio spectrum, and file-level forensic markers such as codecs and timestamps. That layered approach is what produces its court-ready output: confidence scores, audit trails, and reports built for admissibility in legal and investigative proceedings. It's the tool suited to the after-the-fact question: is this specific multimedia file real, and can that finding hold up under scrutiny?

GetReal Security ([getrealsecurity.com](#)) covers more ground than file review alone. Its platform runs both a forensic detection product for analyzing existing files and a real-time authentication product for live video and voice interactions, built around a zero-trust approach to verifying who's on the other end of a call, interview, or application. That multimodal structure makes it the one tool in this landscape that spans both categories: the forensic, after-the-fact review that Sensity specializes in, and the live, in-the-moment authentication that Pindrop and Truepic, featured below, focus on for their respective channels. Where Sensity's strength is answering questions

about content that already exists, GetReal is built to catch impersonation and synthetic identity as it's happening, across use cases from executive impersonation to fraudulent job candidates.

Pindrop Pulse (pindrop.com) is narrower by design, focused specifically on detecting synthetic voice. It analyzes live audio in contact centers and integrates with meeting platforms including Zoom and Webex, aiming to confirm within seconds whether a voice on a call is human and, when paired with Pindrop's authentication tools, whether it belongs to the person it claims to be. For organizations where the phone or a voice channel is the primary attack surface, that narrow focus is the point.

Truepic Vision (truepic.com) works upstream of most of these tools, verifying the capture of a photo or video at the moment it's submitted rather than analyzing it after the fact. It captures time, date, device, and location metadata alongside the image itself, and filters out AI-manipulated or synthetic submissions before they enter a workflow. Its use cases span far beyond any one industry: insurance claims, business and equipment lending, product recalls, home lending, and business credentialing all rely on the same underlying capability, trustworthy visual evidence collected at the source.

None of these four tools do the same job, and none of them do Digital Mountain's job. When digital evidence has to move through collection, review, and production and survive a challenge to its authenticity, that's a different level entirely, and it's the one we specialize in. We know which tools fit a given matter, follow the Daubert Principle to test before use, and when chain of custody and metadata preservation needs to be airtight. Our company documents the results, so they hold up under scrutiny in court. No single tool in this landscape solves every problem. It's the nature of authentication now, and it's why the choice of tool as much as the digital forensic expert.

Please direct questions and inquiries about electronic discovery, digital forensics, cybersecurity, and data analytics to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

ILTACON 2026

Nashville, TN: August 23-27, 2026

AI TECHWORLD 2026

Santa Clara, CA: September 1-3, 2026

NATIONAL EDISCOVERY LEADERSHIP INSTITUTE CONFERENCE 2026

Kansas City, MO: September 24-25, 2026

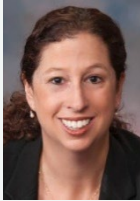
RELATIVITY FEST 2026

Chicago, IL: September 29, 2026 - October 1, 2026

THE AI CONFERENCE 2026

San Francisco, CA: September 29, 2026 - October 1, 2026

[Click here to see more upcoming events and links.](#)



Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.

4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

Contact us today!

www.digitalmountain.com

FOLLOW US AT:

