

FORENSICS

AI-Powered Deepfake Analyzer for Media Authentication and Synthetic Identity Detection

AI-powered media authentication platform that detects deepfake video, AI-generated imagery, cloned voices, and synthetic identities using multi-model ensemble analysis. Delivers probability scores, visual heatmaps, and court-ready forensic reports.



[Deepfake Analyzer](#)

[Official Brochure](#)

SOLUTION SNAPSHOT

<p>DETECTION TYPES</p> <p>Video / image / audio / document</p>	<p>ANALYSIS MODELS</p> <p>Ensemble of 12+ specialised detectors</p>	<p>OUTPUT</p> <p>Probability score + heatmap + report</p>
<p>PROCESSING SPEED</p> <p>< 60 s for 5-min video clip</p>	<p>API</p> <p>REST API for automated pipeline</p>	

Built for Real Operations

Analyses submitted media through a battery of complementary detection models — including spatial inconsistency analysis, frequency-domain artefact detection, and biometric liveness scoring — to produce a consensus authenticity score with confidence interval. The visual explanation layer highlights specific regions of manipulation, giving investigators and legal teams the evidence they need to challenge suspect media in court or regulatory proceedings.

APPLICATIONS

Where This Product Fits

Law Enforcement & Judicial Authentication

Verifies the authenticity of video and audio evidence submitted in criminal proceedings where deepfake manipulation is suspected.

Media & Journalism Verification

Allows newsrooms and fact-checking organisations to authenticate footage and images before publication to prevent misinformation spread.

KYC & Identity Fraud Prevention

Detects AI-generated identity documents and face-swap attempts during remote onboarding and video KYC verification processes.

SPECIFICATION

Technical Details

Detection Types	Video / image / audio / document
Analysis Models	Ensemble of 12+ specialised detectors
Output	Probability score + heatmap + report
Processing Speed	< 60 s for 5-min video clip
API	REST API for automated pipeline
Supported Formats	MP4 / MOV / AVI / JPG / PNG / WAV / MP3
Report Format	PDF forensic report + JSON data
Deployment	Cloud SaaS / on-premise air-gapped
Accuracy	> 95% on benchmark datasets
Warranty	Annual licence with SLA

"The heatmap output was decisive in our case. The jury could see exactly which frames had been manipulated — no expert testimony required to understand the evidence."

Senior Prosecutor

Digital Crimes Division, High Court

RESOURCES

Media & Questions

Q. What is the false-positive rate?

A. On standard benchmark datasets, the false-positive rate is below 4%. The ensemble approach is specifically designed to minimise false accusations of manipulation on genuine media.

Q. Is an on-premise deployment available for classified use?

A. Yes. An air-gapped on-premise appliance is available for intelligence agencies and judicial bodies handling classified or sensitive media.

Q. Can it detect audio deepfakes (voice cloning)?

A. Yes. The audio analysis module detects voice synthesis and cloning artefacts, including GAN-generated speech and TTS-based voice substitution.

Ready to deploy Deepfake Analyzer?

Talk to Nirikhon for product consultation, installation planning, integration support, and enterprise deployment.

Hotline: 01712345678 | Website: www.nirikhon.com