EchoMark

Getting Started Sample PDF

What is Forensic Watermarking?

Forensic watermarking is a digital security technique used to embed imperceptible, yet identifiable, information into digital content such as videos, images, audio, or documents. Unlike visible watermarks, forensic watermarks are designed to be covert and resilient, remaining intact even after compression, resizing, or format changes. This embedded data typically contains unique identifiers that can trace the origin or distribution path of the content. The process is particularly valuable in environments where intellectual property and confidential data are at risk of unauthorized use or disclosure.

Many traditional forensic watermarks are vulnerable to the “analog hole”. Digital content must ultimately be rendered as visual or audio output—on screens, speakers, or printed pages—for users to consume it. At this point, the data becomes vulnerable to capture, as protections no longer apply to the analog form. This allows individuals to bypass digital safeguards by photographing screens, recording audio through speakers, or manually copying displayed information. For example, a DRM system with watermarking system may successfully block a user from transferring a confidential document to a USB device or sending it via email, but it cannot prevent that same user from taking a photo of the screen with a smartphone. The analog hole thus represents a fundamental challenge to information security because no digital control can fully prevent the unauthorized capture of data once it is displayed or played.

What is EchoMark?

EchoMark specializes in visual content protection that embeds invisible marks into the content itself that often survives the analog-hole providing content creators additional tools to investigate such information leak vectors. EchoMark offers an email workflow solution that automatically watermarks all emails and attachments.