EPFL-TTO

EPFL Innovation Park J
CH-1015 Lausanne
Switzerland
+41 21 693 70 23
http://tto.epfl.ch/

Research Contact

Martin Vetterli
+41 21 693 13 38
martin.vetterli@epfl.ch

TTO Contact

Mauro Lattuada
+41 21 693 35 63
mauro.lattuada@epfl.ch

Licensing Opportunity

TTO – Technology Transfer Office

Authenticating Captured Visual Content By Analog Fingerprinting

Ref. Nr

6.2644

Keywords

Image Authentication, Analog Fingerprinting, Anti-Deepfake, Media Forensics, Watermarking, Imaging Systems

Intellectual Property

PCT/IB2025/055632

Publication

N/A

Date

19/12/2025

Description

Current image authentication relies on digital metadata or digital watermarking, which can be easily manipulated or removed through compression and editing. Optical encryption techniques exist but require coherent illumination (laser) and precise alignment, making them impractical for everyday use. These limitations leave images vulnerable to deepfake attacks and unauthorized alterations.

The technology introduces a novel analog fingerprinting method for authenticating real-world visual content. Instead of embedding watermarks digitally, the system applies an optical distortion during image capture, creating a unique analog fingerprint before the image reaches the digital sensor.

The technology works under normal lighting conditions (incoherent illumination), unlike previous optical encryption methods. It can be integrated into consumer devices (e.g., smartphones) or professional imaging systems. The analog fingerprint is unique per camera or user and can change dynamically, offering robust protection against deepfakes and tampering.

Advantages

- Resistant to Metadata Manipulation: No reliance on digital metadata.
- Deepfake Mitigation: Verifies real-world origin of images.
- Broad Protection: Distortion applied to the entire image, not just localized regions.
- Works Under Normal Lighting: No need for lasers or complex setups.
- Dynamic Fingerprints: Programmable masks allow time-based changes for enhanced security.
- High Security: Analog fingerprints encode far more complexity than standard encryption keys.

Applications

- Media Forensics: Detect tampering and verify authenticity.
- Copyright Protection: Embed analog certificates in captured content.
- Source Identification: Confirm the origin of images or videos.
- Anti-Deepfake Solutions: Validate real-world scenes in social media and journalism.
- Secure Imaging in IoT and Surveillance: Ensure integrity of visual data streams.
- Authentication of Optically Encoded Data: Extendable to audio-visual content.