

Woher weiß ich, ob ein Bild echt ist?

➤ 3 Ansätze:

Content Credentials · SynthID · Fingerprinting

Das Vertrauen in digitale Medien erodiert

KI-generierte Bilder sind kaum noch von echten zu unterscheiden. Deepfakes verbreiten sich in Sekunden. Ohne Herkunftsnachweis können wir einem Bild nicht mehr einfach vertrauen.

Die gute Nachricht: Die Industrie arbeitet an Lösungen.
Drei Technologien stehen im Mittelpunkt.

Content Credentials

SynthID

Fingerprinting

Content Credentials

C2PA (Coalition for Content Provenance and Authenticity) ist ein offener Standard, getragen von Adobe, BBC, Google, Microsoft, OpenAI und Sony.

Es ist ein digitales Protokoll, das an eine Bilddatei angehängt wird:

**Welche Kamera,
Software oder KI?**

**Wann wurde es
erstellt?**

**Welche Bearbei-
tungsschritte?**

Jeder Eintrag ist kryptografisch signiert – Änderungen sind nachweisbar.

Googles unsichtbares Wasserzeichen

SynthID von Google DeepMind schreibt ein unsichtbares Signal direkt in die Pixeldaten eines Bildes ein – nicht als Anhang, sondern im Bild selbst.

Kann es

Überlebt Zuschchnitt, Skalierung & Komprimierung

Bilder aus Gemini, Imagen & Veo erkennen

Kann es nicht

Bilder anderer KI-Anbieter erkennen

Detaillierte Bearbeitungshistorie liefern

Content Fingerprinting

Das Bild als sein eigener Ausweis

Ein Algorithmus berechnet aus Farben, Strukturen und Mustern eines Bildes einen eindeutigen digitalen Fingerabdruck ohne etwas einzubetten.

Du kennst das Prinzip bereits:

▶ YouTube Content ID

Erkennt geschützte Videos – auch
gespiegelt & geschnitten

♪ Shazam

Erkennt Songs in Sekunden, selbst bei
Hintergrundlärm

Google Bildersuche

Findet ähnliche Bilder unabhängig von
Größe & Format

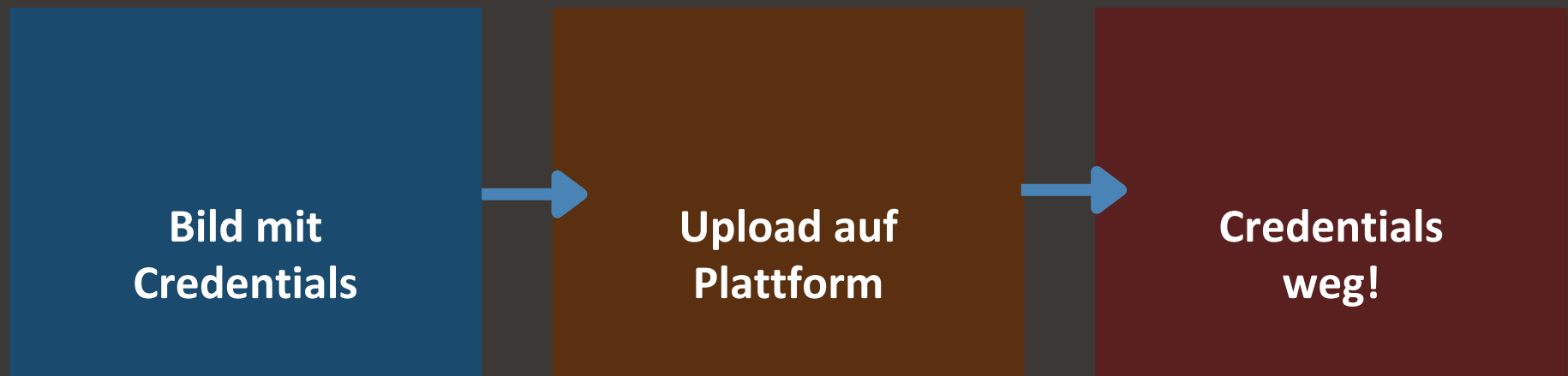
PhotoDNA

Erkennt illegale Inhalte ohne das Bild
sichtbar zu machen

Warum es drei Ansätze braucht

Wenn Bilder auf Social Media hochgeladen werden, entfernen Plattformen automatisch die meisten Metadaten, aus Speicher und Geschwindigkeitsgründen.

Für Content Credentials ist das fatal: Das Protokoll verschwindet.



Lösung: Wasserzeichen & Fingerprinting stecken im Bildinhalt selbst – sie überleben das Entfernen von Metadaten.

So prüfst du ein Bild selbst

Beide Tools sind kostenlos nutzbar.

Content Credentials prüfen

verify.contentauthenticity.org

Bild hochladen → Protokoll prüfen: verwendete Software, KI-Beteiligung, Erstellungsdatum.

SynthID prüfen

gemini.google.com

Bild hochladen → Fragen: „Ist dieses Bild KI-generiert?“ oder @synthid eingeben.
Limit: ca. 10 Prüfungen/Tag.



Mehr dazu?

Den vollständigen Artikel lesen

Content Credentials, SynthID, Fingerprinting – alle drei Ansätze, die technischen Hintergründe, Grenzen des Systems und eine Schritt-für-Schritt-Anleitung.

→ Jetzt auf Substack lesen
afterthepromptjournal.substack.com