

Evelyn Runge

Eine kurze Geschichte der Authentizitätsinfrastrukturen, 1994 bis 2024 2025

<https://doi.org/10.25969/mediarep/24366>

Veröffentlichungsversion / published version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:

Runge, Evelyn: Eine kurze Geschichte der Authentizitätsinfrastrukturen, 1994 bis 2024. In: *MEDIENwissenschaft: Rezensionen | Reviews*, Jg. 42 (2025), Nr. 4, S. 535–553. DOI: <https://doi.org/10.25969/mediarep/24366>.

Nutzungsbedingungen:

Dieser Text wird unter einer Creative Commons - Namensnennung 3.0 Lizenz zur Verfügung gestellt. Nähere Auskünfte zu dieser Lizenz finden Sie hier:

<https://creativecommons.org/licenses/by/3.0>

Terms of use:

This document is made available under a creative commons - Attribution 3.0 License. For more information see:

<https://creativecommons.org/licenses/by/3.0>

Perspektiven

Evelyn Runge

Eine kurze Geschichte der Authentizitätsinfrastrukturen, 1994 bis 2024

Der vorliegende Beitrag perspektiviert Authentizitätsinfrastrukturen – ein Begriff, der im deutschen Sprachraum bislang nicht grundsätzlich verhandelt wurde (vgl. Ivens/Gregory 2019; Runge/Korte 2024). Authentizitätsinfrastrukturen sollen digitale Aufnahmen bereits in der Kamera mit über Metadaten hinausgehenden Signaturen versehen, um potenzielle Änderungen während der Publikationskette einzuschreiben und auch KI-generierte Bilder zu ‚authentifizieren‘. Authentizitätsinfrastrukturen sind genuin auf digitale Daten und ihre Verknüpfbarkeit bezogen, mit dem Ziel, „emerging and normative responses to misinformation“ (Gregory 2024, S.14) zu gestalten.

Dieser Beitrag skizziert punktuell und chronologisch entscheidende Phänomene der Jahre 1994 bis 2024 in Theorie und Praxis mit dem Ziel, die Genese und Komplexität von Authentisierungsstrategien in analogen Medien im Übergang zu Authentizitätsinfrastrukturen in digitalen Medien überblickshaft darzulegen. Bei digitalen Medien ist

zu beobachten, dass neben einer partizipativen Kultur der Open Source Information (OSINF) bekannte Technologieunternehmen wie Adobe versuchen, Produzent:innen auf ihre Software festzulegen durch sogenannte *walled-garden*-Ansätze („ummauerte Gärten“), die die frei gewählte Kombinationen von etwa Software oder Betriebssystemen erschweren.¹ Deutlich wird zudem, dass sowohl Authentisierungsstrategien und Authentizitätsinfrastrukturen als auch Open-Source- und *walled-garden*-Ansätze parallel fortbestehen, zum Teil von denselben Akteur:innen verwendet und zunehmend in Zusammenschau erforscht werden (vgl. Godarzeni-Bakhtiari 2025).

Fragen nach Authentizität gerade von Fotografien und Bewegtbildern begleiten diese seit ihrer Erfindung. Dies zeigt sich etwa in Manfred Hat-

1 Dieser Beitrag entsteht im Rahmen meines Forschungsprojekts „Glokalisierung des digitalen Bildes Ethik, Bildhandeln und Innovative Methoden“ (2023-2026, DFG-Schwerpunktprogramm Das digitale Bild). Gefördert durch die Deutsche Forschungsgemeinschaft (DFG) – Projektnummer 421462167.

tendorfs Versuch (1994), Authentizitätsstrategien des analogen Dokumentarfilms herauszupräparieren, und ebenso in Volker Wortmanns wegweisender Dissertation *Authentisches Bild und authentisierende Form* (2023 [2003]). Der breiteren Öffentlichkeit bekannt geworden sind die Möglichkeiten der Verknüpfung von Informationen, wie Metadaten in digitalen Fotografien, durch die Fotos im Gefängnis in Abu Ghraib 2004: Die Aufnahmen, die US-Soldat:innen und CIA im gleichnamigen Gefängnis im Irak während des sogenannten „War on Terror“ von Folterungen und Häftlingsleichen machten, stehen im Zentrum des Dokumentarfilms *Standard Operating Procedure* (2008) von Errol Morris (vgl. Gourevitch/Morris 2008a; 2008b; Letort 2013). Zwei Jahre nach Veröffentlichung des Films gründete Architekt Eyal Weizman am Goldsmiths College der University of London seine Forschungsgruppe Forensic Architecture, die kombinatorische digitale Verfahren entwickelt, um staatliche Gewalt und Menschenrechtsverletzungen zu belegen.

Digitale Bilder aus öffentlichen Quellen und Smartphone-Aufnahmen sind Teil visueller Beweisführung. 2014 gründete der Brite Elliot Higgins das Investigativbüro *bell:ngcat*, das sich auf Faktenchecks durch OSINF beziehungsweise Open Source Intelligence (OSINT) spezialisiert hat. Methoden und Techniken visueller Verifikation werden nunmehr auch in journalistischen Redaktionen eingesetzt – promi-

nent das Visual Investigations Team der *New York Times* sowie in Nicht-Regierungs-Organisationen (NRO) wie Human Rights Watch und Amnesty International. Die genannten Organisationen, ihre Methoden und Einsatzbereiche werden in diesem Beitrag knapp vorgestellt, um in aktuelles Basiswissen zu OSINF/OSINT einzuführen. Seit 2013 arbeitet die NRO WITNESS unter anderem mit dem Guardian Project an digitalen Signaturen, um digitale Bilder weitere Stufen der Verifikation beizufügen. Aus Fachartikeln des WITNESS-Direktors Sam Gregory (2022; 2024) lässt sich die Vorgeschichte zu Authentizitätsinfrastrukturen erschließen. Die NRO ist auch in der Beratung von Tech-Firmen zu Verifikationen digitaler Bilder involviert, nicht zuletzt in der Content Authenticity Initiative (CAI) und Coalition for Content Provenance and Authenticity (C2PA), in der sich unter anderem Adobe, Microsoft und Canon zusammengeschlossen haben, um die oben erwähnten Authentizitätsinfrastrukturen CAI/C2PA von der digitalen Kamera bis zu Produzent:innen als Standards entlang der Distributionsketten einzuführen. In der Absicht, sogenannte *content credentials* durchzusetzen, ist allerdings auch die altbekannte *walled-garden*-Mentalität marktbeherrschender Technologieunternehmen zu erkennen.

Der Beitrag schließt mit Anregungen zur Folgeforschung vor allem bezüglich KI-generierter Bilder sowie Verantwortlichkeiten von Tech-Unter-

nehmen, journalistischen Medien und individuellen Mediennutzer:innen und ferner mit Ideen, wie OSINF-Ausbildung in universitären Seminaren realisiert werden kann. Es geht längst nicht mehr – wie bei Hattendorf – um kritische Analyse dokumentarischer Formen, sondern um breitflächige Aufklärung und gesamtgesellschaftlichen Kampf gegen demokratiezersetzende Desinformation. Durch die Verquickung von Tech-Milliardären und ihren Unternehmen mit autoritären Kräften – gegenwärtig in den USA offen zu beobachten – stellen sich Fragen, die weit über Bildverifikation hinausgehen.

Authentisierungsstrategien und Dokumentarfilm

Hattendorf (1994) zufolge rufen filmische Strategien des Dokumentarfilms bei Rezipierenden den Eindruck von Glaubwürdigkeit hervor – und weniger das Verhältnis des Films zur dargestellten Realität (vgl. S.10 und S.67). Die formale Gestaltung sei für die filmische Glaubwürdigkeit konstituierend, also filminterne pragmatische Markierungen, die Hattendorf als dokumentarische Authentisierungsstrategien basierend auf einem Korpus von 19 Dokumentarfilmen typologisiert. Der beginnende Einfluss virtueller Welten ist Hattendorf zwar bewusst, für seine Analyse aber noch zu wenig verbreitet, um berücksichtigt zu werden: „Ein Problem, dass die Dokumentarfilmforschung in Zukunft sicherlich beschäftigen wird, ist das

der *Simulation* im Zusammenhang mit den Möglichkeiten computergesteuerter digitaler Generierung sogenannter virtueller Realitäten. Die technischen Entwicklungen in dieser Richtung sind zwar – zumal im Rahmen militärischer Forschung und Anwendung – schon weit fortgeschritten; die Popularisierung simulatorischer Cyberspace-Techniken im Unterhaltungssektor hat jedoch eben erst eingesetzt, so dass es verfrüht erscheint, Aussagen über die Auswirkungen referenzloser Simulationen im Wahrnehmungsbereich machen zu wollen“ (ebd., S.23).

Hattendorf setzt voraus, dass zwischen Film und Rezipierenden ein ‚Wahrnehmungsvertrag‘ geschlossen werde; auf die jeweiligen Authentizitätsversprechen dokumentarischer Filme reagierten Rezipierende mit Vertrauen oder dem Gefühl des enttäuschten Vertrauens. Als Haupttypen dokumentarischer Authentisierungsstrategien nennt Hattendorf: Dominanz des Wortes (Erklärdokumentarismus), Dominanz der Bilder (Verzicht auf Inszenierung und lenkende Kommentare), ausgewogenes Verhältnis visueller und verbaler Zeichen, rekonstruierende Inszenierung (Interpretation im Sinne ‚so könnte es gewesen sein‘), metadiegetische Inszenierung (selbstreflexive Verweise) (vgl. ebd., S.311ff.). Lassen sich diese Strategien auch nicht 1:1 an digitalen und multimedialen Formaten der Gegenwart spiegeln, so regt Hattendorfs Aufschlag zum Weiterdenken an, inwiefern gegenwärtige

Formate der Authentifizierung – der Verifikation – greifbar gemacht werden können. Dabei spielt vor allem der partizipative Charakter eine Rolle, der weit über Rezipient:innen-Status analoger Zeiten herausgeht.

Wortmann (2023) definiert Authentizität, Authentizitätseffekte, Authentizitätsversprechen als un abgeschlossenen, sich stets erneuernden Diskurs: „Authentizitätsdiskurse sind weder epochentypisch noch lassen sie sich historisch eingrenzen. Als Problemkonstellation scheinen sie epochenübergreifend wirksam – zumindest im Hinblick auf europäische und vom europäischen Bild- und Subjektverständnis beeinflusste Kulturen. [...] Authentizität als Effekt, Konstruktion und/oder als diskursive Strategie zu verstehen, ist ebenso vorausgesetzt wie unproblematisch. Wenn alles konstruiert ist, ist die Frage nach der Konstruktion obsolet“ (ebd., S.12). In den vielfältigen digitalen Bildkulturen sind gegenwärtig nicht unbedingt europäische Bild- und Subjektverständnisse ausschlaggebend; vielmehr ist im Antagonismus politischer Systeme liberaler Demokratien und Autokratien relevant, wie Bildverständnisse politisch unterlaufen und für hybride (Bild-)Kriegsführung benutzt werden. Verifikationen von Bewegt- und Standbildern sind im Bereich sogenannter Deepfakes relevant, aber auch von Bildmaterial aus Kriegs- und Konfliktzonen, die strafrechtlich bedeutsam sein können, etwa zur Prüfung von Zeit- und Ortsangaben.

Als Übergang zwischen analogen Authentisierungsstrategien im Anschluss an Hattendorf und zu OSINT-Recherchen, die eine größtmögliche Zahl digitaler Quellen zu relevanten Untersuchungsfeldern sammeln, ist der Folterskandal im US-amerikanischen Militärgefängnis Abu Ghraib im Irak bedeutsam. Wortmann schreibt: „Mit den Fotografien aus Abu Ghraib findet sich erstmals ein politischer, sozialer und bildkultureller Kumulationspunkt, an dem die digitale Fotografie als eigenständiges (und nicht nur defizitäres) Medium wahrgenommen wird, das entsprechend theoretisiert werden kann“ (ebd., S.258). Wortmann sieht in den Veröffentlichungen zu Abu Ghraib einen Wendepunkt in der Glaubwürdigkeit digitaler Fotografien, da „niemand die Authentizität der Fotografien in Frage stellte aufgrund der Tatsache, dass es sich um digitale handelte. Im Gegenteil: Es scheint, dass vor allem der Umstand, dass sie als digitale Bilder frei im Netz zirkulieren konnten und nicht über öffentliche Kanäle lanciert worden waren, sondern aus einer eigenen, bildsemantischen Dynamik heraus an die Öffentlichkeit drängten, ihre Authentizität zementieren half“ (ebd., S.255f).

Standard Operating Procedure: Forensic Report

Wichtiger Bezugspunkt in der Geschichte digitaler Bilder sind die Fotos, die von Folterungen irakischer Gefangener durch Angehörige des US-

amerikanischen Militärs im Gefängnis Abu Ghraib bei Bagdad gemacht wurden (vgl. Gunthert 2019, S.37ff.; Letort 2013; Mirzoeff 2006; Wortmann 2023, S.254ff.). Angehörige der 372. Military Police Company zwangen irakische Gefangene unter anderem zur Masturbation, sich zu Pyramiden auf dem Boden zu stapeln, angeleint auf dem Boden zu kriechen oder mit Exkrementen beschmiert mit ausgebreiteten Armen im Flur zu stehen, den eigenen Blick verdeckt unter Kapuzen und somit in noch größerer Unsicherheit gehalten. Bekannt wurden Porträts von Militärangehörigen, die mit gekühlten Leichen posierten, sowie das wissenschaftlich zentral diskutierte Foto des sogenannten ‚Kapuzenmannes‘ (*Bagman*): Ein in einer Kutte und mit Kapuze verhüllter Mann steht auf einer Kiste, an den Händen mit Kabeln verbunden – ihm wurde gesagt, er werde mit Stromschlägen getötet, sollte er sich bewegen (vgl. Tester 2005; Laustsen 2008; Kennedy 2012; Letort 2013; Singh 2024).

Das Fernseh-Nachrichtenprogramm *CBS 60 Minutes II* zeigte am 28. April 2004 erstmals Fotos aus Abu Ghraib; diese waren ein halbes Jahr zuvor aufgenommen worden, die Fotos datieren vom 17. Oktober bis 2. Dezember 2003 (vgl. Scherer/Benjamin 2006). In den Folgewochen und -jahren waren diese Aufnahmen immer wieder Gegenstand journalistischer und dokumentarischer Erzählungen – darunter das Onlinemagazin *Salon*, das am 14. März 2006 unter *The Abu Ghraib Files* der breite-

ren Öffentlichkeit 279 Bilder und 19 Videos bekannt machte, und Errol Morris' Dokumentarfilm *Standard Operating Procedure*. Für den vorliegenden Beitrag sind diese beiden Publikationen relevant, da sie sich explizit auf digitale Spuren der Fotografien beziehen, die es ermöglichten, beispielsweise Zeitleisten der Folterungen zu erstellen und darüber dann an den Folterungen Beteiligte zu identifizieren. Mittlerweile sind nicht alle Links bei *Salon* noch funktionsstüchtig, aber die zehn Kapitel der *Abu Ghraib Files* inklusive der Fotos und der Original-Bildunterschriften können im Internetarchiv *Archive.org* abgerufen werden, und die Fotos sind teilweise via *Wikimedia* aufzuspüren. Mark Benjamin von *Salon* hatte Dokumente des Criminal Investigation Command (CID) der US-Armee zugespielt bekommen, und *Salon* präsentierte „an annotated, chronological version of these crucial CID investigative documents – the most comprehensive public record to date of the military's attempt to analyze the photos from the prison. All 279 photos and 19 videos are reproduced here, along with the original captions created by Army investigators. [...] While many of the 279 photos have been previously released, until this point no one has been able to authenticate this number of images from the prison, or to provide the Army's own documentation of what they reveal. This is the Army's forensic report of what happened at the prison: dates, times, places, cameras and, in some though not all cases, identi-

ties of the detainees and soldiers involved in the abuse“ (Salon 2006). 173 der 279 Fotos wurden mit einer Sony FD Mavica aufgenommen, die Charles A. Graner gehörte, der später verurteilt wurde. Zudem gab es laut einem früheren CID-Report einen Laptop und acht CDs mit 1.325 Fotos and 93 Videos, die mutmaßliche Misshandlungen zeigen.

Salon stellte neben seinen zehn Kapiteln – von denen jedes mit den Worten beginnt: „Warning: Photos contain disturbing images of violence, abuse and humiliation“ – unter anderem einen Beitrag mit der Überschrift „Note on methodology“, in dem die Journalist:innen Auskunft über das Material geben, das sie erhalten und gesichtet haben, unter anderem mit Informationen über die Metadaten der digitalen Bilder: „Examination of the metadata revealed the photos were created by five separate digital cameras. The embedded metadata showed the make and model of the camera as well as the camera date and time when the picture was taken“ (Carstensen/Rockwell 2006). Auch die von *Salon* veröffentlichten Videos enthalten Bildunterschriften, die Uhrzeit und Datum, Bildinhalte und – sofern bekannt – Namen und Dienstgrad der abgebildeten Personen zeigen. Die Redaktion legt auch offen, welche Informationen von ihr stammen: „All caption information is taken directly from CID materials. Editor’s notes appear in brackets.“

Was die Mitarbeitenden von *Salon* aus dem *forensic report* der Armee nahmen und über ihre eigene Methode

der Untersuchung und Zusammenstellung von Metadaten veröffentlichten, beschäftigte von Oktober 2005 bis Februar 2008 Philip Gourevitch und Errol Morris: Der US-amerikanische Journalist Gourevitch schrieb ein Buch mit dem Titel *Standard Operating Procedure*, das er als kollaborative Arbeit mit dem Dokumentarfilmer Morris ausweist – letzterer hatte Hunderte von Interviews mit Beteiligten und Verantwortlichen in und für Abu Ghraib geführt und Dokumente ausgewertet. Gourevitch verzichtet im Buch bewusst auf Bilder: „The photographs have a place in the story, but they are not the story, and it would be untruthful here to submit once again to their frame“ (Gourevitch/Morris 2008b, S.283). Im Buch spielen die Fotos und Videos dennoch eine Rolle, in den Erzählungen der Angehörigen von Armee und Militärpolizei (vgl. ebd., S.154ff., S.191 und S.262) – und im Arbeitsauftrag, den Brent Pack erhielt: Der „lead forensic examiner of the computer crime unit of the U.S. Army Criminal Investigative Division“ sollte zwölf CDs mit „thousands of pictures“ untersuchen (ebd., S.265). „We want you to find the ones that depict possible prisoner abuse, or people that were in the area at the times abuse were occurring. And we want to know exactly when the pictures were taken. Put them on a time line so that a jury can see when each incident began and when it ended; how much time elapsed in between these photographs; how much effort went into what these people were doing to the priso-

ners; and who else was there when these things occurred“ (ebd.). Übrig blieben nach Packs Auswertung 280 Bilder, die er nach Vorfällen gruppierete, um beispielsweise fehlerhafte Einstellungen in den Zeit-Metadaten der Kameras aufzuspüren, die in US-Zeitzone statt der Zeitzone im Irak eingestellt waren und nicht mit den Arbeitsschichten der jeweiligen Kamerabesitzer:innen übereinstimmen konnten. Zwei Monate benötigte er, um Vorfälle, zeitliche Sequenzen und eindeutige Identifikation der Kameras, aus denen die Bilder stammten, zusammenzustellen.

Im Film *Standard Operating Procedure* berichtet Pack in fast denselben Zitaten wie im Buch über seinen Auftrag. Morris unterlegt Teile dieser Zitate mit Bildern, die den Zuschauenden verdeutlichen sollen, was Pack beschreibt: Thumbnails – in analogen Zeiten ‚Kontaktbögen‘ genannt – sind in unterschiedlichen Größen, Ausschnitten, Bewegungsrichtungen über den Bildschirm unterwegs, ein frühes *infinite scrolling*, zum Teil mit Listen von Dateinamen und Metadaten kombiniert. Als Sound unterlegt Morris das typische klickende Piepsen filmischer Tech-Dystopien und auch einzelne Aufnahme mit Vektorlinien, die sich im Orbit verlieren, zur Imagination der Digitalität – und der Möglichkeiten, die digitale Bilder Forensiker:innen eröffnen. Morris versucht filmisch darzustellen, wie Pack durch die Sortierung der Bilder überlappende Situationen über Sequenzierung via Zeitleiste belegen konnte. Hattendorfs Haupttypen doku-

mentarischer Authentisierungsstrategien sind in Morris' Film zu erkennen, zudem sei hervorgehoben, dass Morris vor der Schwierigkeit stand, Digitalität sichtbar zu machen – zu einem Zeitpunkt als zumindest in Europa digitale Kameras als Consumerprodukte erst langsam ihren Aufschwung nahmen und kamerafähige Smartphones noch als technische Utopien galten.

OSINT & OSINF: Akteure der Open Source Data Collection

Wenige Jahre nach Morris' Film nahmen die Forschungsgruppe Forensic Architecture um Eyal Weizman im Rahmen zweier ERC-Forschungsprojekte und Elliot Higgins' *bellngcat* – damals noch als Privatperson – ihre Arbeit auf. Ihre Arbeiten sind wegweisend für die wachsenden Open-Source-Information-Communities (vgl. Bois/Feher/Foster/Weizman 2016; Colquhoun 2016; Cooper/Mutsvaio 2021; Bär/Calderon/Lawlor/Licklederer/Totzauer/Feuerriegel 2023; Bellingcat Investigation 2023).

Waren die Ergebnisse der Recherchen von Forensic Architecture zunächst in Museen ausgestellt, erstveröffentlichte *bellngcat* seine Investigativbelege online auf Twitter und in den Kommentarspalten der Onlineausgabe von *The Guardian*. In den Folgejahren sind die Adressat:innenkreise gewachsen: Es geht nicht mehr nur darum, Kriegsverbrechen – von Staaten wie Syrien und Russland – zu dokumentieren, darüber aufzuklären

und gegebenenfalls Beweismaterial für (internationale) Strafgerichtsverfahren zur Verfügung zu stellen. Hybride Kriegsführung, die sich Deepfakes als Mittel der Falsch- und Desinformation bedient und weitverbreitet über soziale Netzwerke und Messengerdienste Menschen propagandistisch beeinflusst, hat das Ziel, Demokratien zu destabilisieren und Gesellschaften zu spalten. Infolgedessen sind Kenntnisse über Techniken der Verifikation relevant für journalistische Medien, Menschenrechtsorganisationen und individuelle Nutzer:innen von Social Media. Beispiele für journalistische Redaktionen und NROs, die längst in eigene Teams investieren, die sich auf visuelle Verifikationen spezialisieren, sind unter anderem die *New York Times* und ihr Visual Investigation Team sowie Human Rights Watch und Amnesty International. Zum Teil hatten diese bereits zuvor mit Forensic Architecture oder bellɔngcat kooperiert. Im deutschsprachigen Raum sind Kompetenzen eher in datenjournalistischen und Faktenchecking-Teams gebündelt, wie unter anderem bei Correctiv, dem österreichischen Verein Mimikama oder in Redaktionen wie dem Investigativteam der *Süddeutschen Zeitung*. Auch Menschenrechtsorganisationen bilden vermehrt eigene Teams mit OSINT-Fokus, so etwa Human Rights Watch mit dem Digital Investigations Lab (<https://www.hrw.org/topic/technology-and-rights/digital-investigations-lab>) und Amnesty International mit dem Evidence Lab ([\[citizenevidence.org/\]\(https://citizenevidence.org/\)\). Die US-amerikanische Menschenrechtsorganisation WITNESS, 1992 gegründet von Musiker Peter Gabriel, arbeitet seit 2009 unter dem Motto „Video for Change“ daran, Menschen für die Aufnahme von Videos als Beweis- und Verifikationsmaterial zu trainieren. Ihrem langjährigen Direktor Sam Gregory kann die Erstveröffentlichung des Begriffes ‚*authenticity infrastructure*‘ zugerechnet werden \(vgl. Ivens/Gregory 2019\). Eingedeutet als Authentizitätsinfrastrukturen ist der Begriff im deutschsprachigen Raum bisher noch nicht breitflächig in Gebrauch, dabei sind Technologien längst auf dem Markt.](https://</p>
</div>
<div data-bbox=)

Diese Recherchebüros haben eigene OSINT-Cycles entwickelt, also Verfahren der Sammlung, Kombination, Verifikation und Produktion öffentlich zugänglicher Informationen. Der Fokus in diesem Beitrag liegt auf investigativen und journalistischen Formaten der Sammlung digitaler, oft öffentlich zugänglicher Daten als Grundlage für Verknüpfung, Verifikation und Analyse etwa von Verbrechen und Kriegsverbrechen, und weniger auf Cyberkriminalität, Sicherheits- oder Geheimdiensten. Der Begriff ‚OSINT‘ wird generalisiert verwendet, wenn auch manche Autor:innen den Fokus auf ‚Intelligence‘ als englisches Wort für Nachrichtendienst legen und für zivilgesellschaftliche oder journalistische Verifikationsarbeit OSIN V – Open Source Investigation – oder OSINF – Open Source Information – bevorzugen.

In den hier vorgestellten OSINT-Beispielen werden so viele Daten wie möglich gesammelt, sowohl aus frei zugänglichen Quellen als auch von kommerziellen Anbietern etwa zeitnaher Satellitenaufnahmen. bellçngcats OSINT-Cycle etwa zeichnet sich dadurch aus, auch Informationen zu sammeln, die zunächst irrelevant scheinen, und sie in einem siebenstufigen Verfahren von Verifikation, Analyse, Review und Bestätigung auf sehr relevante Informationen einzugrenzen. In bellçngcats – zum Teil kostenfreien – Workshops werden spezifische Recherchewege erklärt und nachvollziehbar gemacht, beispielsweise Schattenanalyse oder das Tracking von Flugzeugen und Schiffen. Zudem werden digitale Tools, Programme, Vorgehensweisen, Verifikation und Analyse vermittelt: Bildungsangebote sind inhärenter Bestandteil des Engagements von bellçngcat und anderen Investigationsnetzwerken.

Die Methoden, Informationen und Daten zu sammeln, beziehen sich unter anderem auf die Nutzung von Suchmaschinen, sozialen Netzwerken, Emailadressen, User- und Echtnamen, Orten (z.B. über Geo- und GPS-Koordinatoren), IP-Adressen, Domainnamen. Diese werden technischen, inhaltlichen und investigativen Analysen unterzogen – etwa Metadaten, Source Codes, Geo- und Chronolokation, Bild- und Videovergleiche und -interpretationen, räumliche und raumzeitliche Analysen, Mapping der (Verbindungen der) involvierten Personen und Ereignisse. Für

soziale Netzwerke werden spezifizierte Analyseverfahren genutzt, die auch in medienwissenschaftlichen Forschungen verwendet werden (Sentiment Analysis, Natural Language Processing, Machine Learning, Social Network Analysis, Geotagging usw.). Im Rahmen von OSINF werden unterschiedliche Workflows angewendet, um diese Techniken in bestimmten Reihenfolgen, Kombinationen und Querverbindungen zur Verifikation vorliegender Informationen sowie Beweisführung für spezifische Fragen zu nutzen – je nach Verfügbarkeit gesammelter Daten.

Authentizitätsinfrastrukturen

Authenticity infrastructures nennen Gregory und Ivens (2019) jene digitalen Infrastrukturen, die entlang bildlicher Distributionsketten Herkünfte in Bilder einschreiben. Gregory und Ivens formulieren für ihre Arbeit für die Menschenrechtsorganisation WITNESS: „Within our Emerging Threats and Opportunities work, WITNESS is focused on proactive approaches to protecting and upholding marginalized voices, civic journalism, and human rights as emerging technologies such as AI intersect with disinformation, media manipulation, and rising authoritarianism“ (ebd. 2019, S.4). WITNESS ist seit 2013 involviert, unter anderem gemeinsam mit journalistischen Redaktionen, Technologie- und Kameraherstellern und NROs Bewegt- und Standbilder über Metadaten zu verifizieren

beziehungsweise über digitale Signaturen verifizierbar zu machen (u.a. das Guardian Project als Entwickler von Digitaltools und Apps wie ProofMode [<https://proofmode.org/>]). Die Grundidee ist, dass durch die Etablierung von Authentizitätsinfrastrukturen – eine Art Wasserzeichen, das Aufnahmezeitpunkt und -ort, Urheber:in sowie mögliche Manipulationen – auch KI-induzierte – nachvollziehbar macht (vgl. Sedlmeir/Rieger/Roth/Fridgen 2023; Jones 2023; Runge/Korte 2024). Das digitale Foto durchläuft verschiedene Schritte, bevor *content credentials* hinzugefügt werden, für Nutzer:innen sichtbar am cr-Logo in der rechten oberen Ecke. Schematisch betrachtet werden dem digitalen Bild *provenance information* und eine digitale Signatur zugefügt, die kryptografisch gesichert werden. Sollte das Foto bearbeitet und geändert werden, wird eine weitere digitale Signatur erstellt und wie eine weitere Schicht gesichert.

Als bislang bekanntestes, auch weil offensiv beworbenes Beispiel von Authentizitätsinfrastrukturen gelten die miteinander verwobenen Content Authenticity Initiative (CAI) und Coalition for Content Provenance and Authenticity (C2PA). Mitglieder der CAI sind Softwarefirmen, Medienunternehmen, Bildagenturen, Kamera-, Chip- und Prozessorenhersteller – unter anderem Adobe, Associated Press AP, Axel Springer Verlag, BBC, Canon, dpa, Getty Images, Leica, Microsoft, *New York Times*, Nikon, Nvidia, Reuters, Shutterstock, *Stern*,

Truepic. Laut Adobe-Blog wurde CAI auf der Adobe MAX 2019 gegründet; in den Texten von WITNESS wird hervorgehoben, dass die NRO mindestens ab 2013 digitale Signaturen über die Produktions- und Distributionslinie digitaler Bilder hinweg entwickelte. Parsons jubilierte im Oktober 2024 auf dem Adobe-Blog: „We’re seeing increased adoption and mainstream implementation of Content Credentials almost weekly now from both the public and private sectors, including this year alone — Google, TikTok, OpenAI, Meta, LinkedIn, Amazon, Sony and the U.S. Department of Defense (DoD) for its images hosted on DVIDS“ (Parsons 2024a). Adobe Firefly und Microsofts Bing Image Creator nutzen *creator credentials* für KI-generierte fotorealistische Fiktionalisierungen (vgl. Henrich 2024; Runge 2024). Klassisch-journalistische Medienunternehmen wie BBC und CBC haben angekündigt, ihr Archivmaterial mit *content credentials* zu versehen. Adobe verspricht, dass die kostenfreie Web-App ermögliche „to easily attach Content Credentials to their digital work – helping you protect your work, show attribution and better connect with your audiences online“ (Parsons 2024b). Der Werbespruch lautet: „Restoring trust and transparency in the age of AI“ (<https://contentauthenticity.org/>). Wie die Mediengeschichte zeigt, sind Schlagwörter eine Zeitlang aktuell und treiben Forschung voran (oder vor sich her), wie

etwa der Slogan ‚Sharing is caring‘, den heute allerdings keine Social-Network-Site mehr verwendet (ausführlich dazu siehe John 2012; 2017; 2024; Runge 2025). Ob Vertrauen und Transparenz bei User:innen – vor allem hinsichtlich KI-generierter fotorealistischer Fiktionalisierungen – durch Authentizitätsinfrastrukturen erhöht werden können, bleibt abzuwarten. Eliza Strickland (2024) betont: „While the major generative-AI platforms have protocols to prevent people from creating fake photos or videos of real people, such as politicians, plenty of hackers delight in ‚jailbreaking‘ these systems and finding ways around the safety checks. And less-reputable platforms have fewer safeguards“ (S.26). Allerdings haben Nutzer:innen bereits gezeigt, dass beispielsweise Gemini-Wasserzeichen einfach zu entfernen sind. Und noch ein Aspekt bleibt in den Berichten über CAI/C2PA unterbeleuchtet: Das cr-Icon, über das User:innen Informationen über die Herkunft des digitalen Bildes erhalten können (sollten), funktioniert nur in bestimmten Medien-Ökologien: „[V]iewers will see that information only if they’re using a social-media platform or application that can read and display content-credential data“ (ebd.).

Die Kameramodelle Leica M-11P und Nikon Z6III haben *content credentials* integriert; auf Smartphone-Ebene wird Qualcomm Snapdragon8 Gen3 durch C2PA-Partner Truepic digitale

Bilder kryptografisch authentifizieren. Die App ProofMode bezeichnet sich selbst als „Open-Source, Privacy-Focused Verifiable Camera App“ (2013 sagte Sam Gregory von WITNESS: „We believe in a future, where every camera will have a ‚Proof Mode‘ that can be enabled and every viewer an ability to verify-then-trust what they are seeing“). Eine weitere Idee der CAI/C2PA-Konsortien ist, dass mit *content credentials* versehene Bilder auf Social Media als vertrauenswürdig eingestuft und höher gerankt werden. Dennoch – und das gibt C2PA selbst zu – kann diese Vertrauenswürdigkeit nicht im Sinne von (In-)Authentizität des Bildinhalts verstanden werden: *content credentials* zeigen nicht an, ob ein Bild gefälscht ist oder nicht. Sie können lediglich positive Signale über Herkünfte eines Bildes liefern – nicht aber negative Signale über die Authentizität eines Bildes.

Kritik an Authentisierungsstrategien und Potenziale von OSINF

Den Abbilddebatten um dokumentarische Authentizität in Fotografie und Film sind, so Wortmann (2023), keine Grenzen „gesetzt im Hinblick auf das digitale Bild. Selbst die Tatsache, dass inzwischen künstliche Intelligenzen fotorealistische Bilder aus den Tiefen des Netzes emporrechnen und mit ihren *inauthentischen* Entwürfen Betrachter:innen hinters Licht führen, setzt dem Authentizitätsdiskurs kein Ende. Im Gegenteil: Die Verunsiche-

rungen, die entsprechende KI-generierte Bilder hervorrufen, halten ihn vielmehr virulent“ (S.27).

Kritische Perspektivierungen haben Eyal und Ines Weizman (2024) selbst formuliert: „Bei aller kreativen Nutzung der verfügbaren zeitgenössischen Bildanalysen dürfen wir nicht vergessen, dass die Technologien der forensischen Untersuchung dieser Gewalttaten mit jenen der Überwachung und Zerstörung identisch sind. Beide fußen auf der Lektüre von Vorher-Nachher-Bildern – wenn auch mit unterschiedlichen Blickwinkeln und Absichten. Der Schütze wird anhand von Vorher-Nachher-Bildern die Genauigkeit seines Angriffs bewerten, während Menschenrechtsaktivisten mittels desselben Bildpaars die zivilen Verluste dieses Anschlags untersuchen und anklagen“ (S.43). Auch Wortmann betont die Notwendigkeit reziproken Erwartungsmanagements: „Technische Neuerungen setzen Zäsuren nicht nur auf der Verfahrensebene, sie irritieren auch habitualisierte Gebrauchsweisen mit Bildern und evozieren Verlustdiskurse, die sich an der fraglich gewordenen Bildauthentizität abarbeiten. Diese [...] medialen Kontingenzerfahrungen evozieren wiederum neue Authentizitätsdiskurse, die notwendig sind, um die Authentizitätserwartungen an die neuen Verhältnisse anzupassen“ (Wortmann 2023, S.264; vgl. auch Schierbaum 2021).

Godarzeni-Bakhtiari (2025) konzeptualisiert die „dreifach verschachtelte Sinnkonstruktion“ (S.1) von

Investigationvideos über Videoartefaktanalyse als Meta-Artefakte. Durch die detaillierte Offenlegung, wie Informationen gesammelt wurden, wird laut Godarzeni-Bakhtiari eine Erzählung geschaffen, die oft zwischen dem, was tatsächlich geschah, und dem, was möglich gewesen wäre, oszilliert. Solche Berichte werden zunehmend als Machtinstrumente eingesetzt, um die öffentliche Wahrnehmung zu steuern. Dies deutet auf die Entstehung einer neuen Form von Medieninhalten hin, deren Hauptzweck nicht die Information, sondern die politische Einflussnahme ist (vgl. ebd., S.25).

Die CAI-Konsortien wollen C2PA als Standardverfahren der Authentizitätsinfrastrukturen etablieren und in den digitalen Alltag integrieren. Zum gegenwärtigen Zeitpunkt bleiben viele Fragen offen und damit ergiebige Forschungsdesiderate: Einerseits können Authentizitätsinfrastrukturen dazu beitragen, weitere Informationen und Verifikationen gerade im visuellen Bereich zu sammeln und zu nutzen. Andererseits sind gerade jene dadurch gefährdet, die vor Ort und unter bedrohlichen Umständen oder im Verborgenen Informationen sammeln, etwa Mitarbeitende und Zuträger:innen von Menschenrechtsorganisationen.

Durch die Integration – und gleichzeitiger *walled-garden*-Einkriegung – von CAI/C2PA werden Bedarfe geschaffen. Im Kamerabereich werden analog zu anderen Bereichen der Informationstechnologien Bedarfe

durch die Industrie selbst generiert. Ist es tatsächlich nötig, alle paar Monate neue Kameramodelle auf den Markt zu bringen, die sich beispielsweise in Pixelzahl und Sensorenqualität nicht relevant unterscheiden? Das gleiche gilt für Smartphones, Smartwatches, Tablets und andere Konsumgüter. Soll das Ziel erreicht werden, C2PA flächendeckend auf den Markt zu bringen, heißt dies, dass die Integration von C2PA/*content credentials* als Werbe- und Verkaufsargument genutzt wird. Kann eine am Rand des Klimakollapses stehende Welt es sich leisten, stets neue Smartphone- und Kameramodelle verkaufen zu wollen, bei ansteigendem Elektroschrott, seltenen Erden und massivem Energieverbrauch durch KI und Streaming? Durch die Erfahrungen mit der moralischen, politischen und rechtlichen Unzuverlässigkeit von Tech-Unternehmern wie Elon Musk (Twitter/X/x.AI), Peter Thiel (Palantir), Jeff Bezos (Amazon) oder Mark Zuckerberg (Alpha/Meta/Facebook/Instagram/WhatsApp) ist Vorsicht angebracht, inwiefern diese Personen nicht auch durch Initiativen wie CAI/C2PA gesammelte Daten zur globalen Überwachung missbrauchen – mit dem Ziel, Demokratien und Rechtsstaaten zu destabilisieren.

Gegenwärtig sind OSINF-Ausstellungen mit Kritik an Arbeiten von Kollektiven verknüpft, etwa an angeblich mangelnder historisch-politischer Einordnung vor allem in Bezug auf Israel und Palästina sowie bildlicher Übermacht, so Vorwürfe

gegen Forensic Architecture; zudem wird Initiativen wie CAI/C2PA unterstellt, sie würden von namentlich der *New York Times* zur monetären sowie deutungsmächtigen eigenen Monopolisierung genutzt (vgl. Meyer 2023; Schinke 2024; Naß 2024; Weizman 2024). Es mutet mehr als befremdlich an, dass die Kritiker:innen eher auf investigative Rechercheur:innen fokussieren als auf Plattformen und Tech-Unternehmer:innen, die zutiefst und spätestens seit dem Wahlkampf in den USA 2024 offensichtlich der Demontage demokratischer Institutionen bei gleichzeitig ausgestellter gegenseitiger Korruption frönen. Amy Schoenfeld Walker (2019) hebt hervor, dass weitverbreitete Unkenntnisse und Unverständnis über journalistische Arbeitsweise zum Misstrauen gegenüber journalistischer Produkte führen. In der Öffentlichkeit ein Verständnis für Produktionsbedingungen (inter-)medialer Erzeugnisse herzustellen, ist Teil von Medienpädagogik. In der derzeitigen Lage grundsätzlichen Misstrauens gegenüber journalistischen Medien und zunehmender Fehl- und Desinformation allerdings gerade Initiativen zu diskreditieren, deren Gründungszweck in der (visuellen) Verifikation und im Kampf gegen Falschinformationen liegt, spielt jenen ins Kalkül, die antidemokratisch agieren.

Es kommt auf die Kontextualisierung an; und im Rahmen journalistischer, menschenrechtlicher und wissenschaftlicher visueller Inve-

stigationen gehört verifikatorisches Handwerk zum Alltag, Kosten- und Spardruck zum Trotz.

Für die Medienwissenschaften lassen sich unterschiedliche Perspektiven aufzeigen. Die Publikationen zu OSINF ermöglichen es, Seminare darauf aufzubauen, sowohl in theoretischer als auch in praktischer Hinsicht – letzteres eröffnet Studierenden den Blick auf berufliche Möglichkeiten in Datenjournalismus und Menschenrechtsorganisationen. Schoenfeld Walker – eine frühere, in die Wissenschaft gewechselte Redakteurin der *New York Times* – fasste 2019 in einem Beitrag zusammen, welche OSINT-Kenntnisse vor allem in visueller Verifikation in der Ausbildung und im Alltag von Journalist:innen und Studierenden wichtig sind. Sie skizziert mögliche Aufgaben für Seminare, da Studien gezeigt haben, dass es selbst für Profis schwierig ist, (digitale) Bilder zu verifizieren. Durch noch immer zunehmenden Zeit- und Kostendruck in Redaktionen – eine der Folgen unregulierter und übermächtiger Tech- und Social-Media-Unternehmen, die sich nach wie vor weigern, mit journalistischen Medien gleichgestellt zu werden und entsprechenden Gesetzen (z.B. Presserecht und Jugendschutz) zu folgen – tendieren mitunter auch Journalist:innen und Redakteur:innen dazu, Social-Media-Bilder und -Videos nicht unbedingt erst einem Verifikationsprozess zu unterziehen, bevor sie sie weiterleiten oder als journalistischen Input

aufgreifen. Eine mögliche Erklärung ist, dass visueller Journalismus über viele Jahrzehnte als minderwertig gegenüber dem Wort(journalismus) betrachtet wurde. Eine andere Erklärung ist, dass Social-Media-Beiträge sehr günstig durch sogenannte kalte Recherche – also Recherche, für die sich Journalist:innen nicht von ihrem Schreibtisch wegbewegen und mitunter nicht mal mit Quellen und potenziellen Informant:innen telefonieren – Beiträge generieren (vgl. Runge 2021a; 2021b).

Schoenfeld Walker regt unter anderem an, mit Studierenden die Unterschiede von Mis-, Des- und Falschinformationen zu diskutieren, statt den Begriff ‚Fake News‘ zu nutzen. Vorgeschlagene Basis-Strategien zur Verifikation sind im Grunde OSINT-Techniken, wie erweiterte Nutzung von Suchmaschinen, Geolokation, Rückwärtssuche von Bildern oder Bot-Erkennungstools. Da gerade medien- und kommunikationswissenschaftliche Forschungsmethoden ähnlich vorgehen, sollte es sehr gut möglich sein, (visuelle) Verifikation in das universitäre Curriculum einzubauen. Ein Aspekt in der Lehre kann sein, eigene OSINT-Recherchen Schritt für Schritt zu dokumentieren und somit transparent und nachvollziehbar zu machen – auch hier sind erklärende Videos und Artikel zur eigenen Arbeitsweise (etwa von bell_ängcat) gutes Vorbild-Material. Beim Training von OSINT-Techniken geht es vor allem ums Bewusstmachen

des Vorhandenen und um die Erweiterung von Software-Kenntnissen sowie die Kombination und Einschätzung der Qualität von Rechercheergebnissen. Visuelle Investigationen „serve as a reminder for journalists [students, citizens etc.] to be rigorously critical of digital sources, to be transparent about their reporting methods, and to examine practical methods of instruction“ (Schoenfeld Walker 2019, S.228).

Nach wie vor geht es darum, Medien- und speziell Bildkompetenz zu stärken. Die Arbeitsgruppe „Visuelle Kompetenzen“ des Deutschen Fotorats hat praktische Hinweise gegeben (vgl. Paries/Gripp 2025); und für Redaktionen hat *Reporter ohne Grenzen* im November 2023 in Zusammenarbeit mit mehr als einem Dutzend Nachrichtenorganisationen die „Paris Charter on AI and Journalism“ herausgegeben. Diese widmet sich dezidiert digitalen Bildern und ruft Journalist:innen dazu auf, keine Impersonationen real existierender Personen und keine Fiktionalisierungen realer Ereignisse als KI-Bilder zu generieren. Da sich KI-Bildgeneratoren an Bildern orientieren, die in hoher Anzahl vorliegen und dementsprechend in Trainingsdaten verwendet werden, ähneln KI-Bilder allerdings durchaus existierenden Personen, und vor allem jenen, deren

Fotos bereits vielfach publiziert wurden (vgl. Runge 2024).

Gerade in den Medienwissenschaften, deren Absolvent:innen in Journalismus, Filmbildung und Filmförderung, Medienpädagogik und Erwachsenenbildung arbeiten, sind stetige Perspektivierungen wichtig. Übergreifende Technologie-Ethiken müssen sich auch mit Authentizitätsinfrastrukturen auseinandersetzen (vgl. Lester/Martin/Smith-Rodden 2022; Reporters Without Borders 2023a; 2023b; Sedlmeir/Rieger/Roth/Fridgen 2023). Aus den Bereichen (visuelle) Des- und Falschinformation sowie Umgang mit fotorealistischen Fiktionen KI-generierter Bilder ergeben sich weitere Aufgabenbereiche gesellschafts- und staatsbürgerlicher Verantwortung, die Verteidigung und Schutz der freiheitlich-demokratischen Grundordnung nicht nur beinhalten, sondern angesichts rechtsextremer und verfassungsfeindlicher Bestrebungen in den Vordergrund rücken müssen – gerade in den Medienwissenschaften. Zudem ergeben sich durch OSINF-Kenntnisse Berufsoptionen – im Datenjournalismus, bei investigativen Recherchenetzwerken und Menschenrechtsorganisationen. Die Bedarfe werden steigen, übrigens auch in den Bereichen Klima-, Umwelt- und Energie.

Literatur

Bär, Dominik/Calderon, Fausto/Lawlor, Michael/Lickleederer, Sophia/Totzauer, Manuel/Feuerriegel, Stefan: „Analyzing Social Media Activities at Bellingcat.“ In: *Proceedings of the 15th ACM Web Science Conference 2023*. Austin: ACM, 2023, S.163-173.

Bellingcat Investigation: „Russia’s Ghost Ships and the Evolution of a Grain Smuggling Operation“ (21.08.2023). <https://www.bellingcat.com/news/2023/08/21/russias-ghost-ships-and-the-evolution-of-a-grain-smuggling-operation/> (25.09.2025).

Bois, Yve-Alain/Feher, Michel/Foster, Hal/Weizman, Eyal: „On Forensic Architecture: A Conversation with Eyal Weizman.“ In: *October* 156, 2016, S.116-140.

Carstensen, Jeanne/Rockwell, Page: „Note on Methodology: How Salon produced The Abu Ghraib Files.“ In: *Salon* (06.07.2006). https://web.archive.org/web/20060706200659/http://www.salon.com/news/abu_ghraib/2006/03/14/methodology/ (25.09.2025).

Colquhoun, Cameron: „A Brief History of Open Source Intelligence.“ In: *Bellingcat* (14.07.2016). <https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/> (25.09.2025).

Cooper, Glenda/Mutsvaio, Bruce: „Citizen Journalism: Is Bellingcat Revolutionising Conflict Journalism?“ In: Skare Orgeret, Kristin (Hg.): *Insights on Peace and Conflict Reporting*. New York: Routledge, 2021, S.106-120.

Godarzeni-Bakhtiari, Mina: „Zur Analyse visueller Analysepraktiken: Evidenzkonstruktionen in Investigationsvideos von Forensic Architecture.“ In: *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research* 26 (2), 2025.

Gourevitch, Philip/Morris, Errol: „Exposure.“ In: *New Yorker* (17.03.2008a). <https://www.newyorker.com/magazine/2008/03/24/exposure-5>.

Gourevitch, Philip/Morris, Errol: *Standard Operating Procedure: A War Story*. London: Picador, 2008b.

Gregory, Sam: „Deepfakes, Misinformation and Disinformation and Authenticity Infrastructure Responses: Impacts on Frontline Witnessing, Distant Witnessing, and Civic Journalism.“ In: *Journalism* 23 (3), 2022, S.708-729.

Gregory, Sam: *From Social Media to Deepfakes: Participatory Human Rights Witnessing and Advocacy Using Audiovisual Media, Incorporating the Emerging Impacts of Deceptive AI and Technologies for Authenticity and Trust (2007-22)*. PhD thesis. London: University of Westminster, 2024. <https://doi.org/10.34737/W955W>

Gunthert, André (Hg.): *Das geteilte Bild: Essays zur digitalen Fotografie*. Konstanz: Konstanz UP, 2019.

- Hattendorf, Manfred: *Dokumentarfilm und Authentizität: Ästhetik und Pragmatik einer Gattung*. Konstanz: Ölschläger, 1994.
- Henrich, Nadine Isabelle (Hg.): *Viral Hallucinations: Agency in Media*. Hamburg: Deichtorhallen, 2024.
- John, Nicholas: „Sharing and Web 2.0: The Emergence of a Keyword.“ In: *New Media & Society* 15 (2), 2013, S.167-182.
- John, Nicholas: *The Age of Sharing*. Malden: Polity, 2017.
- John, Nicholas: „Sharing and Social Media: The Decline of a Keyword?“ In: *New Media & Society* 26 (4), 2024, S.1891-1908.
- Jones, Nicola: „How to Stop AI Deepfakes from Sinking Society — and Science.“ In: *Nature* 621 (7980), 2023, S.676-679.
- Kennedy, Liam: „Seeing and Believing: On Photography and the War on Terror.“ In: *Public Culture* 24 (2[67]), 2012, S.261-281.
- Laustsen, Carsten Bagge: „The Camera as a Weapon: On Abu Ghraib and Related Matters.“ In: *Journal for Cultural Research* 12 (2), 2008, S.123-142.
- Lester, Paul Martin/Martin, Stephanie A./Smith-Rodden, Martin (Hg.): *Visual Ethics: A Guide for Photographers, Journalists, and Media Makers*. New York: Routledge, 2022.
- Letort, Delphine: „Looking Back into Abu Ghraib: Standard Operating Procedure (Erroll Morris, 2008).“ In: *Media, War & Conflict* 6 (3), 2013, S.221-232.
- Meyer, Roland: „Everything that Happens to a Photo: Über analoge und digitale Protokolle der Bildlogistik.“ In: Plener, Peter/Werber, Niels/Wolf, Burkhardt (Hg.): *Das Protokoll*. Berlin/Heidelberg: Metzler, 2023, S.201-211.
- Mirzoeff, Nicholas: „Invisible Empire: Abu Ghraib and Embodied Spectacle.“ In: *Visual Arts Research* 32 (2), 2006, S.38-42.
- Naß, Mira Anneli: „Kritik an Forensic Architecture: Zweifelhafte Beweisbilder.“ In: *Die Tageszeitung: taz* (03.01.2024). <https://taz.de/Kritik-an-Forensic-Architecture/!5983353/> (25.09.2025).
- Paries, Sabina/Gripp, Anna: „Eine umfassende Bildkompetenz ist unabdingbar.“ In: Politik und Kultur (28.01.2025). <https://politikkultur.de/inland/eine-umfassende-bildkompetenz-ist-unabdingbar/> (25.09.2025).
- Parsons, Andy: „5-Year Anniversary of the Content Authenticity Initiative: What It Means and What’s Ahead?“ In: *Adobe Blog* (14.10.2024a). <https://blog.adobe.com/en/publish/2024/10/14/5-year-anniversary-content-authenticity-initiative-what-it-means-whats-ahead> (25.09.2025).
- Parsons, Andy: „Introducing Adobe Content Authenticity: A Free Web App to Help Creators Protect Their Work, Gain Attribution and Build Trust | Adobe Blog.“

In: *Adobe Blog* (10.08.2024b). <https://blog.adobe.com/en/publish/2024/10/08/introducing-adobe-content-authenticity-free-web-app-help-creators-protect-their-work-gain-attribution-build-trust> (25.09.2025).

Reporters Without Borders: „Paris Charter on AI and Journalism“ (10.11.2023a). <https://rsf.org/sites/default/files/medias/file/2023/11/Paris%20charter%20on%20AI%20in%20Journalism.pdf> (25.09.2025).

Reporters Without Borders: „RSF and 16 Partners Unveil Paris Charter on AI and Journalism | RSF“ (10.11.2023b). <https://rsf.org/en/rsf-and-16-partners-unveil-paris-charter-ai-and-journalism> (25.09.2025).

Runge, Evelyn: „Behind the Digital Image: Public Photographs on Community Platforms and Twitter as Repositories for Machine Learning and Journalistic Publications.“ In: *International Journal for Digital Art History DAHJ*, 2021a, S.105-118.

Runge, Evelyn: „SnAppShots: Fotojournalismus Auf Twitter – Zwischen Privater Fotografie Und Ware Für Fotoagenturen.“ In: Schühle, Judith/Hägele, Ulrich (Hg.): *SnAppShots: Smartphones als Kamera*. Münster: Waxmann, 2021b, S.91-108.

Runge, Evelyn: „Israel, Palästina und Bilder-Fragen: Eine erste Kartierung bildethischer Debatten und Herausforderungen nach dem 7. Oktober 2023.“ In: *Kommunikation@gesellschaft* 25 (1), 2024.

Runge, Evelyn: „Einzig beständig ist die Veränderung: Bildzirkulation, Foto-Sharing und Bildhandeln – ein Überblick.“ In: *Fotogeschichte: Beiträge zur Geschichte und Ästhetik der Fotografie* 3 (177), 2025, S.46-55.

Runge, Evelyn/Korte, Lydia: „Jenseits der Dichotomie: Ethische Kompetenzen im digitalen visuellen Journalismus.“ In: *Communicatio Socialis* 4, 2024, S.478-491.

Scherer, Michael/Benjamin, Mark: „Standard Operating Procedure. Chapter 1: Oct. 17-22, 2003.“ In: *Salon* (14.03.2006). https://www.salon.com/2006/03/14/chapter_1/ (25.09.2025).

Schierbaum, Vesna: *Diskurse und Ästhetiken kollektiver Intelligenz bei Forensic Architecture*. Master thesis. Köln: Universität zu Köln, 2021.

Schinke, Chris: „Ausstellung über Politkunst: Äußerst fragwürdiger Wahrheitsbegriff.“ In: *Die Tageszeitung: taz* (15.11.2024). <https://taz.de/Ausstellung-ueber-Politkunst/!6049071/> (25.09.2025).

Schoenfeld Walker, Amy: „Preparing Students for the Fight Against False Information with Visual Verification and Open Source Reporting.“ In: *Journalism & Mass Communication Educator* 74 (2), 2019, S.227-239.

Sedlmeir, Johannes/Rieger, Alexander/Roth, Tamara/Fridgen, Gilbert: „Battling Disinformation with Cryptography.“ In: *Nature Machine Intelligence* 5 (10), 2023, S.1056-1057.

- Singh, Trishla: *Torture, Terror, and Affect in Post 9/11 Literature and Culture*. PhD thesis. Durham: Durham University, 2024. <https://etheses.dur.ac.uk/15663/> (25.09.2025).
- Salon: „Introduction: The Abu Ghraib Files.“ In: *Salon* (14.03.2006). https://www.salon.com/2006/03/14/introduction_2/ (25.09.2025).
- Strickland, Eliza: „This Election Year, Look for Content Credentials: Media Organizations Combat Deepfakes and Disinformation with Digital Manifests.“ In: *IEEE Spectrum*, 2024. <https://ieeexplore.ieee.org/iel7/6/10380442/10380467.pdf> (25.09.2025).
- Tester, Keith: „Reflections on the Abu Ghraib Photographs.“ In: *Journal of Human Rights* 4 (1), 2005, S.137-143.
- Weizman, Eyal: „Reaktion auf Zeitungsartikel von Frau Mira Anneli Nass in Taz, 3.1.2024“ (05.01.2024). https://content.forensic-architecture.org/wp-content/uploads/2024/03/TAZ_Weizman.pdf (25.09.2025).
- Weizman, Eyal/Weizman, Ines: *Vorher & Nachher: Die Architektur der Katastrophe*. Zürich: Diaphanes, 2024.
- Wortmann, Volker: *Authentisches Bild und authentisierende Form*. Köln: Herbert von Halem, 2023.