Finde den Fehler

Wie man digitale Inhalte auf ihre Echtheit prüft

Florian Sturm
Medienradar, 09/2022

In Zeiten digitaler Medien ist nicht jede Nachricht das, wonach sie aussieht. Online kursieren unzählige manipulierte Fotos und Nachrichten. Sie zu erkennen, ist in erster Linie Aufgabe von Journalist:innen. Doch Medienkompetenz betrifft uns alle. Inzwischen gibt es zahlreiche einfache und effektive Methoden, digitale Inhalte auf ihre Echtheit zu prüfen.

Die Präsidentschaft von Donald Trump hat es gezeigt wie keine Zeit zuvor: Fehlinformation und gezielt platzierte Falschnachrichten sind längst Teil des medialen und gesellschaftlichen Mainstreams. Die rasante technologische Entwicklung der letzten Jahre macht es dabei immer leichter, digitale Inhalte zu verfälschen. Während vor etlichen Jahren noch mäßige Bildmanipulationen das Maß aller Dinge waren, ermöglichen künstliche Intelligenz und maschinelles Lernen inzwischen gefälschte, aber täuschend echt wirkende Fotos sowie Audio- und Videonachrichten. Etwa von der Flutkatastrophe in Deutschland im vergangenen Jahr[1] oder dem Ukraine-Krieg[2]. Manche dieser sogenannten Deepfakes sind technisch derart fortgeschritten, dass selbst speziell ausgebildete Forensiker:innen Mühe haben, die Fälschungen als solche zu entlarven. Das klappt nicht immer[3] – aber fast immer.

Oftmals genügen jedoch ein kritischer Blick und einige kostenfreie Tools, um die Echtheit digitaler Inhalte zu verifizieren. Das ist zwar in erster Linie Aufgabe von Journalist:innen. Doch um der Flut an Fake News Herr zu werden, müssen alle Teile der Gesellschaft medienkompetent genug sein. Das gilt insbesondere für Schulen.

In den USA widmet sich die Initiative First Draft News[4] seit vielen Jahren dem Kampf gegen Fehl- und Falschinformation. Für das Vorgehen bei der Verifizierung digitaler Inhalte hat sie diese fünf Eckpfeiler identifiziert:

1. Herkunft: Schaue ich mir gerade die Originaldatei an?
2. Quelle: Wer hat das Video/Foto erstellt?
3. Datum: Wann wurde die Aufnahme gemacht?
4. Ort: Wo wurde die Aufnahme gemacht?
5. Motivation: Warum wurde die Aufnahme gemacht?

Fragwürdige Inhalte entdecken und deren Herkunft prüfen

Der erste Schritt bei der Verifizierung ist stets, die Herkunft des Materials zu prüfen. Gerüchte oder offensichtliche Falschnachrichten verbreiten sich – nachdem sie eine kritische Masse erreicht haben – rasend schnell über soziale Medien. Kanäle also, die vor allem bei der jüngeren Generation eine zentrale Rolle spielen: Facebook, Reddit, Twitter und 4chan sind die wichtigsten Plattformen; Snapchat, YouTube, TikTok und Instagram gehören aber auch dazu.

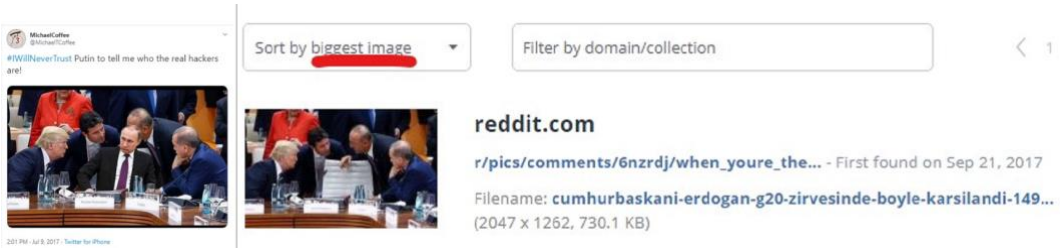
Den lückenlosen Überblick über diese Kanäle zu behalten, ist für einen Menschen unmöglich. Algorithmen können zwar in der Breite mehr Content beobachten, sind jedoch nur so gut und präzise, wie die Menschen, die sie programmieren. Zwei Tools, mit denen sich diverse Social-Media-Plattformen beobachten lassen, sind CrowdTangle und TweetDeck.

Um herauszufinden, wer den Content erstellt oder zumindest ursprünglich hochgeladen hat, helfen vor allem diese Methoden:

1. Rückwärtige Bildersuche

Die „Reverse Image Search“ sollte für jede Überprüfung visueller Inhalte der erste Schritt sein. „Sie ist mit Abstand das wichtigste Tool“[5], sagt Aimee Rinehart von First Draft News. Zudem ist die rückwärtige Bildersuche unkompliziert und liefert schnell gute Anhaltspunkte. Wenn beispielsweise ein Foto oder Video eines Events bereits vor dem Tag des Ereignisses online war, kann die zu prüfende Datei nicht echt sein. Google hat den größten Suchkatalog.[6] Über einen individuellen Suchzeitraum lässt sich rasch erkennen, ob das Material schon vor dem eigentlichen Event online kursierte. Auch Bing[7] ermöglicht die rückwärtige Bildersuche, ist allerdings weniger präzise.

TinEye[8] hat sich auf die rückwärtige Bildersuche spezialisiert und erkennt auch veränderte Kopien. Der Katalog umfasst rund 38,5 Milliarden Fotos – Tendenz steigend. Die Software gibt es auch als Browser-Add-on für Chrome, Firefox und Opera, was die Suche noch einfacher macht. Mit dem Add-on RevEye Reverse Image Search lassen sich direkt Google, Bing, Yandex (Russlands größte Suchmaschine) und TinEye durchforsten. Generell gilt: Je mehr Suchmaschinen man einsetzt, desto besser.



[Quellen: (li) *MichaelCoffee* (*@MichaelTCoffee*), Twitter; (re) Reddit]
Neugieriger Trump mit und ohne Putin. Die linke Variante (mit Putin) kursierte tausendfach online. Die rückwärtige Bildersuche deutet an, dass die rechte Variante das Original zu sein scheint. Je größer die Bilddatei, desto weniger wahrscheinlich ist ein Fake, denn mit jedem sogenannten Scrape gehen Bilddaten verloren.

Für Videodateien funktioniert die rückwärtige Suche derzeit noch nicht. Allerdings kann man markante Standbilder aus dem Video extrahieren – entweder mit einem simplen Screenshot, über die Frame-by-Frame-Funktion des VLC Players oder mit der von der Presseagentur AFP entwickelten Software Invid. Und es gibt:

2. Unique Identifiers

Der US-Ableger von Amnesty International hat eine Suchmaschine entwickelt[9], die das genaue Upload-Datum von YouTube-Videos ermittelt – und so wichtige Hinweise bei der zeitlichen Einordnung von digitalem Content liefert. Sie zeigt außerdem die originale Video-ID an und Links zur rückwärtigen Google-Bildersuche. Diese sogenannten Unique Identifiers gibt es auf fast allen Plattformen (außer Facebook): Bei YouTube ist es die Zahlen-Buchstaben-Kombination hinter dem =; bei Instagram jene hinter instagram.com/p/ und bei Twitter die Zahlenfolge hinter /status/ in der Browser-Zeile. Wer nach diesem einzigartigen Code bei Google sucht, sieht, wo dieser Content noch hochgeladen wurde. Dabei gilt es stets zu beachten: Das Upload-Datum muss nicht mit dem Erstelldatum übereinstimmen!

3. Exif-Daten

Der Blick auf die Exif- oder Metadaten lohnt sich, um die Autorenschaft von digitalen Inhalten zu prüfen. Sie geben Auskunft über Ort, Zeitpunkt, Urheber:in der Aufnahme und technische Details der Kameraeinstellungen. Allerdings funktioniert das nur bei der Originaldatei (und nicht für Videos). Tools wie der Exif Data Viewer[10] sind gute Anlaufpunkte für die Überprüfung. Allerdings lassen sich Metadaten sehr einfach löschen (Social-Media-Plattformen tun das beim Upload meist automatisch) oder verändern: Datei runterladen, per Rechtsklick in die Exif-Daten gehen, drauflosmanipulieren, Foto wieder hochladen – fertig ist die gefälschte Datei, Scrape genannt.

In der Regel sind Scrapes aber deutlich kleiner als Originaldateien und auch die Qualität ist schlechter. So lassen sie sich leichter erkennen.

4. Die Quelle finden

Ist der Originalpost ausfindig gemacht, gilt es, anhand der Quelle die Echtheit des Materials zu prüfen. Jede:r Nutzer:in hinterlässt online einen digitalen Fußabdruck – meist auf der eigenen Website und auf mehreren Plattformen. War der:die Internetnutzer:in zur Zeit der Videoaufnahme überhaupt am Ort des Geschehens? Oder zeigen seine Instagram- oder Facebook-Posts, dass er:sie zum relevanten Zeitpunkt ganz woanders war? „Bei der Überprüfung eines digitalen Fußabdrucks sollte ich auch auf Konsistenz in den Themen achten. Die meisten Leute reden auf sozialen Medien über zwei oder drei Themen: Politik, Sport, die eigenen Kinder oder Kochrezepte. Wenn jemand plötzlich über zwölf Themen spricht, ist das auffällig“[11], sagt Digitalexpertin Rinehart.

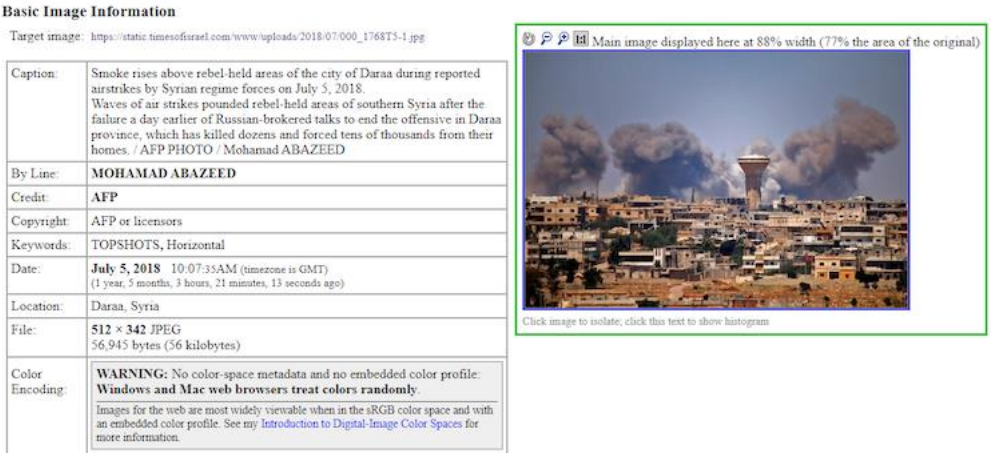
5. Ort und Zeit bestätigen

User-Generated Content (UGC) wird, je nach aktivierter Einstellung, automatisch mit Zeitstempeln und Geo-Tags versehen, um den genauen Aufnahmeort zu markieren. Doch selbst wenn diese Daten vorliegen, ist Vorsicht geboten: Manche Tags beschreiben nicht den Aufnahme-, sondern Upload-Ort, außerdem lassen sich diese Infos leicht manipulieren. Laut First-Draft-Mitgründerin Claire Wardle werden lediglich ein bis zwei Prozent aller Social-Media-Einträge überhaupt mit Geo-Tags versehen.[12] Eine eigenhändige Prüfung bleibt somit unerlässlich.

Um die Angaben von Zeit und Ort zu verifizieren, hilft die auf künstlicher Intelligenz basierte Website Wolfram Alpha[13]. Mit ihr lässt sich beispielsweise feststellen, wie das Wetter zur Zeit des zu prüfenden Events vor Ort war: tatsächlich warm mit wolkenlosem Himmel (wie das Foto/Video zeigt) oder in Wahrheit doch bedeckt und regnerisch? Dann nämlich stimmt mit dem Material etwas nicht. Um das herauszufinden, muss man einfach einen Befehl wie „Tell me the weather in Berlin on November 4th 2019“ in die Suchmaske eingeben und schon spuckt die Website etliche Daten aus. Um sicherzugehen, sollte man diese mit lokalen Wetterstationen oder anderen zeitgleichen Social-Media-Fotos vergleichen.

Eine weitere Methode ist die Geo-Location: Satellitenaufnahmen via Plattformen wie Google Maps, Google Earth oder Wikimapia geben einen ersten Überblick, ob Elemente aus dem zu prüfenden Material – Straßen, Häuser oder markante Punkte in der Landschaft – vor Ort tatsächlich zu finden sind. Im Idealfall führt Google Street View sogar direkt durch die Umgebung, sonst lassen sich Fotos dieses Ortes suchen und mit dem fragwürdigen Material vergleichen. Die konkreten

Koordinaten eines Standortes können ebenso hilfreich für die Authentifizierung sein wie die Maps-Funktion, mit der sich Entfernungen messen lassen.



Basic Image Information

Target image: https://static.timesofisrael.com/www/uploads/2018/07/000_1768T5-1.jpg

Caption:	Smoke rises above rebel-held areas of the city of Daraa during reported airstrikes by Syrian regime forces on July 5, 2018. Waves of air strikes pounded rebel-held areas of southern Syria after the failure a day earlier of Russian-brokered talks to end the offensive in Daraa province, which has killed dozens and forced tens of thousands from their homes. / AFP PHOTO / Mohamad ABAZEED
By Line:	**MOHAMAD ABAZEED**
Credit:	**AFP**
Copyright:	AFP or licensors
Keywords:	TOPSHOTS, Horizontal
Date:	**July 5, 2018** 10:07:35AM (timezone is GMT) (1 year, 5 months, 3 hours, 21 minutes, 13 seconds ago)
Location:	Daraa, Syria
File:	**512 × 342** JPEG 56,945 bytes (56 kilobytes)
Color Encoding:	**WARNING:** No color-space metadata and no embedded color profile: **Windows and Mac web browsers treat colors randomly.** Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.

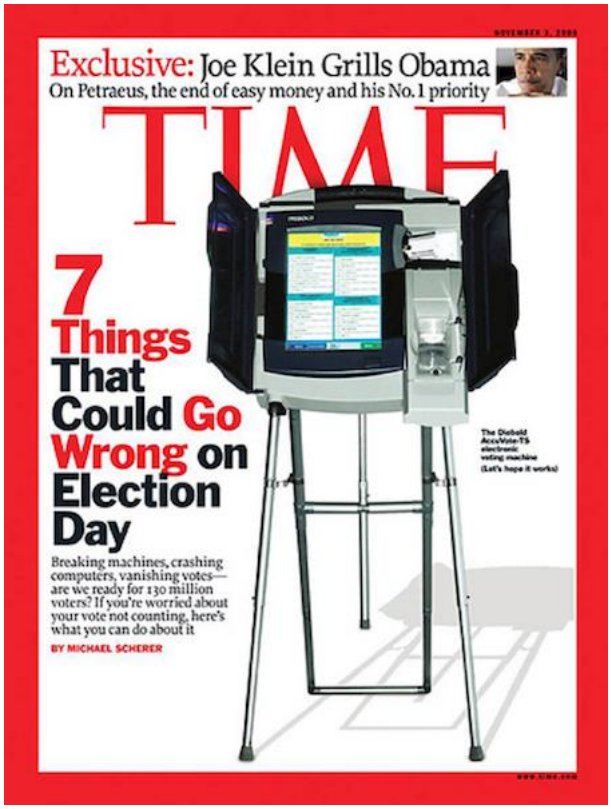
Main image displayed here at 88% width (77% the area of the original)

Click image to isolate; click this text to show histogram

[Quelle: Screenshots aus der Präsentation von First Draft News]
Je mehr Exif-Daten eine Bilddatei aufweist, desto eher lassen sich Rückschlüsse über die Urheberschaft ziehen. Doch Vorsicht: Exif-Daten lassen sich problemlos manipulieren.

6. Bildmanipulationen entdecken

Um herauszufinden, ob ein Foto manipuliert wurde, reichen oft drei, vier kritische Blicke auf Übergänge zwischen Personen oder Objekten beziehungsweise auf die Schatten im Bild. Denn Schatten sind unglaublich schwer makellos zu fälschen und daher ein gutes Indiz bei der Verifikation: Ist jeder Schatten an der richtigen Stelle oder fehlt er irgendwo? Fallen die Schatten in die falsche Richtung oder haben, für die jeweilige Tages- und Jahreszeit, eine merkwürdige Form oder Länge?



[Quelle: Time Magazine]
Auch renommierte Medien sind vor fehlerhaften Schattendarstellungen nicht gefeit – so wie dieses Time-Cover vom 3. November 2008.

Fazit

Die meisten Techniken zur Verifikation digitaler Inhalte sind effektiv, einfach zu bedienen und nur ein paar Mausklicks entfernt. Im Grunde gleicht die Spurensuche bei der Verifikation einer digitalen Detektivarbeit, bei der man sich Schritt für Schritt nach vorn arbeitet. Eines sollte man dabei allerdings nie vergessen: Man sollte keinem Tool blind vertrauen, sondern sie lediglich als Hilfestellung bei der eigenen, kritischen Beurteilung zu Rate ziehen.

Glücklicherweise steigt jedoch nicht nur die technische Qualität von digital gefälschten Inhalten, sondern auch das Bewusstsein, über die Problematik solcher Fälschungen zu sprechen. So wie in diesem Deepfake mit Ex-US-Präsident Barack Obama.

[Quelle: *BuzzFeedVideo*, YouTube]
Im Videoclip *You Won't Believe What Obama Says In This Video!* wird auf die Gefahr der Manipulation mittels Deepfakes aufmerksam gemacht.

Nur durch diesen Diskurs können wir bei Schüler:innen die Fähigkeit erweitern, auch in der digitalen Welt Wahrheit und Fälschung voneinander zu trennen – und menschliche sowie digitale Quellen gleichermaßen kritisch zu betrachten.

Linktipps

- Artikel der Deutschen Welle über die Notwendigkeit von Faktenchecks in den Nachrichten: *Faktencheck: Wie Kinderbilder für Propaganda missbraucht werden*
- Fact-Checking-Werkzeugkasten vom Lehrstuhl Wissenschaftsjournalismus der TU Dortmund: *Ein Werkzeugkasten für Verifikation und Fact-Checking*
- Dorian-Projekt des Fraunhofer Leistungszentrums „Sicherheit und Datenschutz in der digitalen Welt": *Desinformation aufdecken und bekämpfen*

Quellennachweise

1. **Deutsche Welle**: *Fact check: The fake images of the German floods*, vom 23.07.2021, https://www.dw.com/en/fact-check-the-fake-images-of-the-german-floods/av-58613841 (zuletzt abgerufen am 26.08.2022).

2. **Gensing, P.**: *Desinformationen zum Ukraine-Krieg: Veraltete Bilder und fiktive Journalisten*, in: Tagesschau.de vom 01.03.2022, https://www.tagesschau.de/faktenfinder/krieg-ukraine-bilder-videos-101.html (zuletzt abgerufen am 26.08.2022).

3. **Sterz, C.**: *Falschmeldungen im Netz – Den Fakes auf der Spur*, in: Deutschlandfunk vom 29.10.2016, https://www.deutschlandfunk.de/falschmeldungen-im-netz-den-fakes-auf-der-spur-100.html (zuletzt abgerufen am 26.08.2022).

4. Im Juni 2015 schlossen sich neun Organisationen – darunter die Google News Initiative, Bellingcat, Verification Junkie, Storyful und der Eyewitness Media Hub zu einem weltweiten gemeinnützigen Netzwerk zusammen. Das gemeinsame Ziel: den Kampf gegen gezielte Fehl- und Falschinformation im Internet aufnehmen. Inzwischen gehören renommierte Redaktionen wie ABC, ARD, BBC, Al Jazeera, CNN, die New York Times, Reuters und Zeit Online zum Kreis der 84 weltweiten Kooperationspartner. Seit kurzem gibt es auf der First-Draft-Website deutsche Untertitel zu zahlreichen Tutorials, welche die hier vorgestellten Techniken im Detail und an konkreten Beispielen erläutern. Vgl. First Draft, https://firstdraftnews.org/ (zuletzt abgerufen am 26.08.2022).

5. **Rinehart, A.**, im Interview mit Florian Sturm, vgl. https://firstdraftnews.org/articles/author/twinstates/ (zuletzt abgerufen am 26.08.2022).

6. Vgl. Google Bilder, https://images.google.com.

7. Vgl. Microsoft Bing, www.bing.com/images/search.

8. Vgl. TinEye Reverse Image Search, www.tineye.com.

9. Vgl. Youtube Data Viewer, Amnesty International, citizenevidence.amnestyusa.org/.

10. Vgl. exifdata, www.exifdata.com.

11. **Rinehart, A.**, im Interview mit Florian Sturm, vgl. https://firstdraftnews.org/articles/author/twinstates/ (zuletzt abgerufen am 26.08.2022).

12. **Wardle, C.**, Fact Checking Workshop, Knight Science Journalism, MIT, 2021.

13. Vgl. WolframAlpha, www.wolframalpha.com.

Link zum Artikel

https://www.medienradar.de/hintergrundwissen/artikel/finde-den-fehler