FOTOHITS
FOTOGRAFIEREN UND FILMEN
Nr. 6/2023

FOTOHITS

THINKTANK PHOTO
40% RABATT AUF SIGNATURE-TASCHEN
+ E-Book „GIMP 2.10“

PORTRÄTS
Schmeichelhaft, aber glaubwürdig retuschieren

FOTOBÜCHER
So schneiden Standard- und Premium-Varianten in Schwarz-Weiß ab

TESTS

FLACHMANN
Nikkor Z 26mm f/2.8

WEGWEISEND
Sony FE 50mm F1.4 GM

SONNEN-KÖNIG

So entstehen die „Fine Art Nudes“ von Starfotograf Manfred Baumann

Deutschland: € 7,90
Österreich: € 8,80, Schweiz: Sfr 13,40
Benelux: € 9,50, Italien: € 10,40, Spanien: € 10,40,
Dänemark DKK 90.95, Tschechien CZK 315

06
4 197023 507909

Autor: EliotHiggins/Midjourney

FAKT ODER **FAKE?**

Angesichts von Fake-Bildern wählt ein Laie zwischen zwei Übeln: Keiner Aufnahme mehr zu vertrauen oder blind zu hoffen, kein Betrugsopfer zu werden. Dazwischen ist freilich noch etwas Raum für Abwägungen. FOTOHITS stellt Indizien und Werkzeuge vor, mit denen jeder Fälschungen aufspüren kann. Zudem gibt ein Experte seine Einschätzung, was die Zukunft bringt.

Auf gefälschte Fotos hereinzufallen, kann teuer werden. Beispielsweise platzieren Schurken falsche Profilbilder auf Dating-Portalen oder bevölkern eine betrügerische Anwaltskanzlei. Porträts etwa von http://this-person-does-not-exist.com wirken so vertrauenswürdig, dass sie eine Irreführung zumindest erleichtern.

Andere Manipulationen zielen nicht auf den Geldbeutel, sondern den gesellschaftlichen Zusammenhalt. So wie Gerüchte und Verschwörungsmythen verbreiten sie ein Gift, gegen das man nur schwer ankommt. Unmöglich ist es glücklicherweise nicht.

Um vorwegzugreifen: Mit Gewissheit kann zwar höchstens ein Experte feststellen, ob eine Fälschung vorliegt. Aber es existieren einige Anhaltspunkte, die in summa die Wahrscheinlichkeit senken, auf einen Scharlatan hereinzufallen. Mit ihnen in der Rückhand kann ein Sachkenner zumindest argumentieren, wo andere nur mutmaßen.

INDIZIEN

Leser, die sich ohnehin mit Fotografie beschäftigen, bringen eine gewisse Medienkompetenz mit. Die ersten Anhaltspunkte werden daher manchem vertraut sein.

1. Zu den äußeren Merkmalen, die per Augenschein überprüfbar sind, gehören:

- Schatten: Hier tun sich KIs noch schwer. Doch anders als vermutet sind auf www.midjourney.com/showcase/ kaum unlogisch fallende Lichter und Schatten zu finden. Häufiger sind die Gebilde allzu makellos. Die meisten von ihnen wirken, als hätten zahllose Studioleuchten samt Diffusor die gesamte Szenerie illuminiert. Oder kurz: Die KI meint es zu gut.
- Wechselnde Qualität: Eine KI schwankt aus falsch verstandener Gründlichkeit zwischen perfekten und verschmierten Oberflächen und Kanten. Einerseits versteht sie in ihrer derzeitigen Lernstufe Gesichter als frei etwa von Altersflecken. Andererseits will sie regelmäßige Strukturen variieren, was zu unregelmäßigen, schlierigen Füllflächen führt.
- Text: Beschriftungen auf Schildern werden häufig per Zufallsgenerator gefüllt, was Unsinn ergibt.
- Körperform: Momentan verzerren KIs Gesichter und Hände vornehmlich von Nebenpersonen etwa in der Menge.
- Klone: Bei einer Scientology-Feier vermehrte sich das Publikum, indem Personen geklont wurden (Quicklink sciklon. Quicklinks ersparen es, lange Web-Adressen abzutippen. Leser geben sie auf www.fotohits.de in das Feld rechts oben ein. Ein Mausklick auf das Lupen-Symbol leitet sie weiter.). Wiederkehrende Gesichter oder Objekte sind also untrügliche Zeichen für eine eigenhändig vorgenommene Manipulation.
- Kulturelles Wissen: Es ist die wohl stärkste Waffe gegen Betrug. Der Papst trägt niemals Rap-Style, Präsident Putin fällt nicht vor seinem chinesischen Kollegen auf die Knie (Quicklink: putinxi).

1. Der Text ist unsinnig. 2. Das Gesicht ist völlig makellos. 3. Die Regallinien verlaufen krumm. 4. Der Schatten passt nicht zur Deckenbeleuchtung.
Lizenz: Quicklink ccommons

2. Der Kontext, in dem ein Video oder Foto steht, widerspricht seiner Glaubwürdigkeit oder unterstützt sie:

- Ein aufgeklärter Bürger akzeptiert, dass es mehr oder weniger seriöse Quellen gibt. Beispielsweise hält die FOTO HITS-Redaktion das Recherchezentrum Correctiv aufgrund seiner sorgfältigen Nachprüfungen für vertrauenswürdig.
- Ersetzen Verallgemeinerungen die Fakten, gibt es Grund zum Misstrauen. Rassisten etwa verunglimpften Eritreer, die angeblich an ein Gotteshaus uriniert hätten. Correctiv und andere erfuhren auf Nachfrage von der Münchner Kirchengemeinde St. Gertrud, dass sie aufgrund eigener Traditionen draußen an den Mauern beteten (Quicklink gertrud).
- Rückwärtssuche: Gern werden Aufnahmen wie die gerade genannte aus dem Zusammenhang gerissen und sollen etwas gänzlich anderes darstellen. Als weiteres Beispiel entpuppte sich Angela Merkels Verstoß gegen Corona-Regeln als ein Treffen, das vor der Pandemie stattgefunden hatte (Quicklink merco). Manchmal lässt sich die eigentliche

Laut Correctiv tauchte das KI-generierte Bild erstmals am 20. März 2023 im Telegram-Kanal namens News.GRP auf. Verdächtig sind die unregelmäßige Tapete am Stuhl, die unförmige Hand und das Gesicht sowie die extrem glatte Oberflächentextur. Noch wichtiger ist: Telegram ist keine seriöse Quelle und Präsident Putin fällt vor keinem Amtskollegen auf die Knie.

Das angebliche Porträt von Wolodymyr Selenskyj generierte Stable Diffusion (Autor: Roman Kubanskiy, Lizenz Copyleft). Letztlich bräuchte es aber keine KI. Ein Betrüger könnte ein echtes Porträt nachbearbeiten oder den trauernden Präsidenten mit der Falschmeldung „Ukraine hat kapituliert“ versehen.

Quelle herausfinden, indem man ein Digitalfoto kopiert und www.tineye.com oder Googles Bildersuche damit füttert.

3. Einige Computerdaten sind von Laien kontrollierbar:

- Computer-generierte Fotos enthalten keine EXIF-Daten, die Kameras hineinschreiben. Diese liest fast jeder Bildbetrachter aus. Allerdings ist zu bedenken, dass man sie leicht hineinkopieren kann.
- Falls Meta-Daten vorhanden sind, kann man untersuchen, ob sie plausibel sind: Passt der Zeitstempel für Januar zu blühenden Wiesen, ist ein Bildautor für Nachfragen erreichbar?
- Tiefer gehende Dateiinformationen enthüllen nur spezielle Forensik-Programme, einige stellen wir nachfolgend vor.
- Als Antwort auf die Fälschungen bieten einige Firmen Echtheitszertifikate. Welche es gibt und wie sie einsetzbar sind, listet ebenfalls der nächste Abschnitt auf.

FAZIT

Keine der genannten Verfahren ist alleine zuverlässig. Oder andersherum: Jeder Verdachtsmoment kann manipuliert werden. Man muss sie alle zusammen überprüfen und dann die Wahrscheinlichkeit abschätzen, ob sie sich als halbwegs hieb- und stichfest erweisen.

Vernünftige Skepsis sollte aber niemanden veranlassen, manisch alles zu hinterfragen. Denn wenn angeblich jede Tatsache eine Lüge ist, verführt es dazu, ein noch unwahrscheinlicheres Glaubenssystem zu basteln. Innerhalb dieses erscheint es unerträglich, dass es mehr oder weniger plausible Fakten gibt, die zu einer möglichst widerspruchsfreien Schlussfolgerung führen. Völlig unmöglich ist es für Verschwörungsgläubige, selbst einen positiven, anerkannten Beweis zu erbringen. Folgerichtig bleibt die Wahrheit unumstößlich, dass die Erde eine Scheibe sei.

Fake-Bilder selbst verändern weder die Realität noch rationales Denkvermögen. Aber sie wirken sich auf unsere Fotokultur aus. Ihre Grundfesten wurden schon ab 1869 erschüttert, als William H. Mumler wegen seiner Geisterfotos vor Gericht stand. Obwohl damit der Glaube an eine unbestechliche Technik schwand, gelang es Fotografinnen und Fotografen, sich auf gemeinsame Standards zu verständigen. Ansätze wie „Truepic Lens“ (siehe Überschrift „Zertifikate“) sind auch jetzt bereits am Start.

PRÜFGERÄTE

Verfahren, wie sie Gutachter benutzen, bleiben Normalbürgern meist verwehrt. Zudem lassen sich professionelle Forensiker ungern in die Karten schauen.

Man darf aber sogar von Profiprogrammen nicht erwarten, dass sie nach der Analyse schlicht ein grünes Häkchen setzen. Sie geben vorrangig Hinweise, die ein Fachkundiger zu interpretieren weiß. Die unten genannten Helfer entdecken beispielsweise nur, ob ein JPG-Format mehrfach unterschiedlich komprimiert wurde, wie es bei der digitalen Nachbearbeitung geschehen kann.

Wie wahrheitsgemäß die vorgestellten Softwares urteilen, wagt die FOTO HITS-Redaktion also nicht zu beurteilen. Sie listet ausschließlich die eingesetzten Verfahren auf und gibt eine Einschätzung.

Fotoforensics

Die Analyse-Website steht allen Interessenten offen. Die Betreiber weisen darauf hin, dass gleichnamige Apps nur ihren Namen für eigene Zwecke ausnutzen. Für eine juristische oder kommerzielle Nutzung verweisen sie auf den geschlossenen Service http://lab.fotoforensics.com.

Welche Bilddaten man hochladen kann, unterliegt Einschränkungen: Als Formate sind JPEG, PNG, WebP, HEIC und AVIF erlaubt. Die Dateigröße muss innerhalb von zehn Megabyte bleiben und die längste Seite kürzer als 10.000 Pixel sein.

Offizielle Dokumente wie Ausweise werden automatisch erkannt und nicht ausgewertet. Denn schließlich soll niemand sich bestätigen lassen, dass sein gefälschter Reisepass überzeugend ausfällt. Desgleichen sind pornografische Inhalte verboten, was zudem zur Sperrung des Benutzers führt.

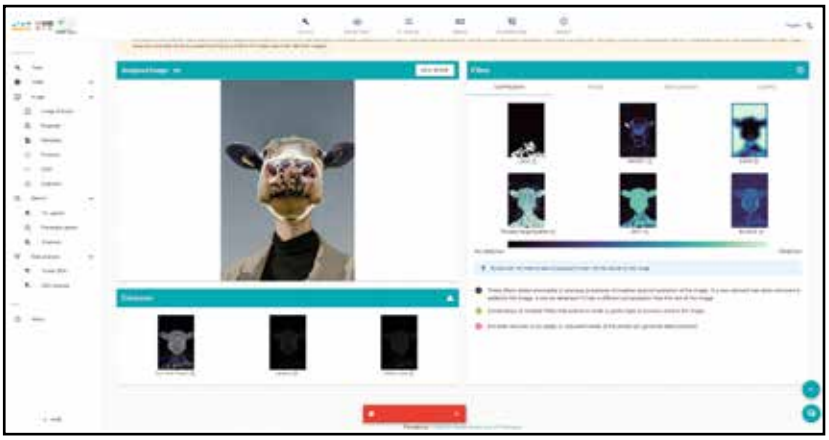
Die Rechte jeder Einreichung verbleiben beim Urheberrechtsinhaber. Laut eigener Aussage zieht das System keine Rückschlüsse auf Personen oder entsprechende Daten.

- Error Level Analysis (ELA): Der Algorithmus entdeckt veränderte Kompressionsraten innerhalb des Bilds. Diese werden als helle verrauschte Flächen hervorgehoben. Eindeutig ist das Resultat aber nicht: Der Kuhkopf in unserer Montage wurde zwar erkannt. Ebenso aber die wegen einer Nachschärfung erfolgte Komprimierung, die ein Smartphone zur Bildverbesserung durchführte. In dem Fall bedeutete die Hervorhebung nicht, dass eine Fälschung vorlag.
- Games: Es handelt sich wirklich nur um ein Puzzle-Spiel, das die Beobachtung schulen soll (oder dem Programmierer der Website einfach Spaß machte).
- File Digest: Er fasst verschiedene Eigenschaften einer Datei zusammen. Der Sucher lädt zuerst ein Digitalfoto hoch, zusätzlich benötigt er das Original, was sich oft als unmöglich erweist. Ein minimal verändertes Test-JPG unterschied sich im Vergleich zur Vorlage durch den Zeitstempel (Filetime), die Anzahl der Einzelfarben (Unique Colors), die Dateigröße (File Size) sowie die Check-Summen MD5, SHA1 und SHA256.

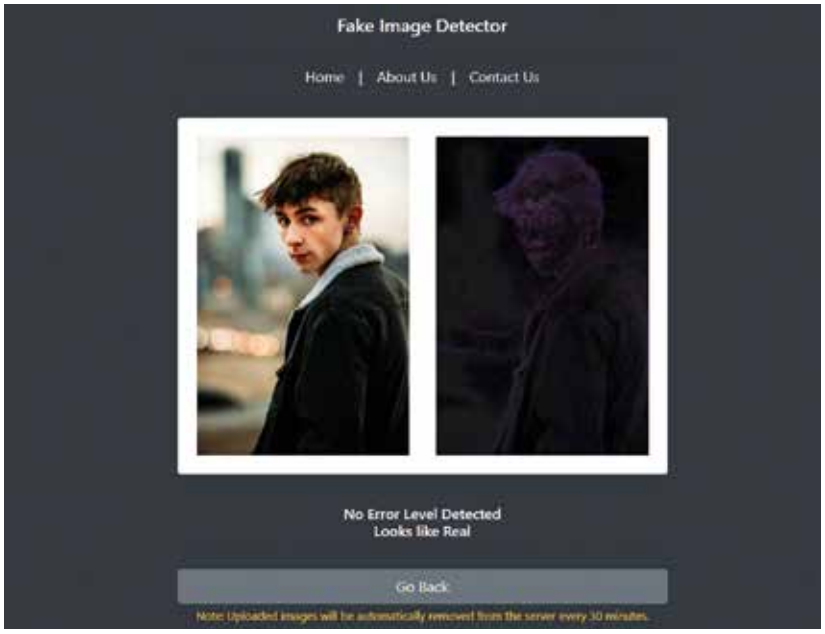
Das gefälschte Papst-Foto sorgte in den vergangenen Wochen für Furore, da es bis auf die kurzen Finger der rechten Hand sehr überzeugend ausfiel.
Quelle: Reddit/r/midjourney

Wer glauben will, der hält auch ein Selfie mit Alien für plausibel. Doch kritische Menschen fordern, dass eine Behauptung nachprüfbar, wiederholbar, folgerichtig und innerhalb anderer Denksysteme widerspruchsfrei ist sowie äußerer Kritik standhält.
Autor: Icygyrosi, Lizenz: Quicklink ccommons

Unsere ohnehin plumpe Montage entlarvte Fotoforensics und hob den aufgepflanzten Kuhkopf hervor. Bei geringen Änderungen bleiben solche Stellen allerdings so unscheinbar, dass sie kaum erkennbar sind.



Der Fake News Debunker stellt vielfältige Funktionen bereit. Viele dienen eher der Recherche als der eindeutigen Identifizierung. Angesichts der Fülle empfiehlt es sich, das Tutorial durchzulesen.



Der Fake Image Detector erwies sich als wenig hilfreich.

- Hidden Pixel: Wer ein Objekt in eine Aufnahme montiert, stellt es zuerst frei und fügt es dann mit transparentem Hintergrund ein. Auch wenn Kopie und Original miteinander verschmelzen, kann Fotoforensics die ursprünglichen transparenten Pixel sichtbar machen. Sie erscheinen im halbdurchsichtigen Schachbrettmuster als gesonderte Bereiche.
- ICC+: Das übliche Farbprofil aus der Kamera und im Internet ist sRGB. Für den Druck oder andere Zwecke bettet ein Medienschaffender ein spezielles Farbprofil ein, bei FOTO HITS ist es „ISO Coated v2 300% (ECI)“. Dieses listet Fotoforensics auf. Die Aussagekraft, dass jemand eine Datei für den Druck vorbereitete, ist freilich gering.
- JPG %: Es zeigt die letzte Kompressionsstufe des JPG-Formats an. Normalerweise beträgt sie 95 bis 99 Prozent, wenn ein Werk frisch aus der Kamera kommt. Bei unter 90 Prozent dürfte sie ein Bildbearbeitungsprogramm vorgenommen haben.
- Metadata: Solche Informationen sind wie eingangs erwähnt in jedem Foto eingebettet. Man kann etwa Kameramodell, Aufnahmedatum oder Verschlusszeit auf Plausibilität prüfen. Falls etwa ein nächtliches Drohnenfoto von einer DSLR stammt, mittags aufgenommen wurde und im Flug mit einer Verschlusszeit von 1/4 Sekunde knipste, kann etwas nicht stimmen. Schwindler sind aber selten so dämlich, solche Fehler zu begehen.
- Strings: Es stellt die Daten als HEX-Werte da, also als für einen Laien sinnlose Zeichen. Spezialisten können eventuell unbekannte Metadaten oder Steganographien herauslesen.
- Source: nach dem Hochladen durchläuft die Datei einige Untersuchungen. „Source“ zeigt nochmals das Quellbild an, das im Allgemeinen unverändert aussieht. Die Funktion ist daher gewöhnlich uninteressant.

http://fotoforensics.com

Fake News Debunker

Das Plug-in für den Internet-Browser „Google Chrome“ lässt sich mühelos über die Schaltfläche „Hinzufügen“ auf der Website installieren. Es enthält einige Werkzeuge, um die Echtheit von Fotos und Filmen zu überprüfen. Sie stehen nach einem Rechtsklick auf eine Bilddatei unter „Fake News Debunker“ bereit.

„Open with assistant“ öffnet eine strukturierte Oberfläche, ansonsten kann man einige Helfer direkt für das angeklickte Bild nutzen: Ausschnittvergrößerung oder eine Rückwärtssuche mithilfe eines Suchdienstes oder gleich von allen verfügbaren. Die „Advanced Tools“ stehen erst offen, wenn man als Journalist registriert ist. Übersetzt sind sie in Englisch, Französisch, Spanisch und Griechisch. Die wichtigsten Helfer sind:

- Magnifier: Mit der Lupe lassen sich einzelne Bildregionen inspizieren. Unter „Video – Keyframes“ geht dies auch mit Einzelbildern eines Films. Jedoch leistet dies fast jeder Bildbetrachter.
- Metadata: Die EXIF- und IPTC-Daten werden angezeigt.
- Forensic: Neben der bereits bekannten ELA nehmen sich weitere Filter ein Bild vor. Was sie machen, erklärt ein Tutorial. Grob gesagt: Wenn unter „Filters“ die Markierungen grüner werden, ist die Wahrscheinlichkeit einer Bildmanipulation größer.
- Image Analysis: Die Untersuchung von Instagram- und Facebook-Bildern ist stark eingeschränkt, da Facebook laut Meldung die Analyse von Usern und Gruppen nicht erlaube. Damit stellt sich die Frage nach dem Sinn dieser Option.
- Factcheck.org: Das The Annenberg Public Policy Center ist ein Forschungszentrum für öffentliche Politik in Pennsylvania. Die ins Plug-in eingebaute Direktsuche erlaubt, nach Stichworten zu suchen. Allerdings ist man hierzulande etwa mit Correctiv ebenso gut bedient.
- XNetwork: Um diese erweiterte Suchmaschine sinnvoll zu nutzen, muss der Fragende exakt formulieren, wonach er sucht. Eventuell findet er mehr, aber nicht unbedingt erhellendere Aussagen.

Quicklink fndeb

Fake Image Detector

Die Seite bietet zwei Analysen an. Die ELA leistet aber nicht mehr als die von Fotoforensics, die andere war blind für Hinweise.

- Error Level Analysis: Die ELA arbeitet mit einem Local Binary Patterns Histogram (LBPH) zusammen, einem Algorithmus zur Gesichtserkennung. Die Anzeige nach der Analyse gleicht freilich der von Fotoforensics. Sie markierte den Kuhkopf, untertitelt mit der Nachricht: „Error Level Detected. Looks like FAKE or Computer Generated“ (Fehler-Niveau entdeckt. Sieht aus wie Fälschung oder mit dem Computer erzeugt). Doch rutschte ein Porträt, das ein Beauty-Filter stark aufgehübscht hatte, klaglos durch.
- Metadata Analyze: Sie sollte aufzeigen, ob und welches Bildbearbeitungsprogramm ein Werk speicherte. Gewöhnlich ist dies unsichtbar vermerkt. Leider behauptete der „Fake Image Detector“ auch bei eindeutigen Photoshop-Produkten: „No Software Signature Found“.

www.fakeimagedetector.com

Der AI Image Detector ist nützlich, um falsche Profilbilder zu entlarven.

AI Image Detector

Die Website ist darauf spezialisiert, per KI erstellte Kreationen zu erkennen. Stichproben der Redaktion erkannte sie mit Wahrscheinlichkeiten von 70 bis über 90 Prozent relativ zuverlässig.

Quicklink aidet

ZERTIFIKATE

Truepic Lens

„Truepic Lens“ fügt Bildern und Videos bei der Aufnahme unter anderem Auflösung, Aufnahmeort und -uhrzeit hinzu. Im Unterschied zu EXIF-Daten sind sie verschlüsselt, sind also nicht manipulierbar. Alle späteren Änderungen werden den eingebetteten Informationen hinzugefügt, was jeder Interessent einsehen kann.

Der Service steht nicht jedem Nutzer offen. Vielmehr können Portale oder Anwendungen wie Adobe Photoshop ihn lizenzieren lassen. Airbnb etwa versichert mit einem so verifizierten Foto, dass ein Gästezimmer wirklich wie abgebildet aussieht.

http://truepic.com

Content Authenticity Initiative

Mit Truepic vergleichbar ist die „Content Authenticity Initiative“ (CAI). Auch sie kann beispielsweise ein Kamerahersteller lizenzieren. Seine Geräte sichern danach alle Aufnahmen mit fälschungssicheren Zertifikaten. Unter anderem die New York Times strebt mit ihrer Mitgliedschaft in der CAI an, es fest in den journalistischen Arbeitsprozess zu integrieren.

http://contentauthenticity.org

FAZIT

Keines der genannten Prüf-Programme bestätigt eindeutig die Echtheit eines Fotos, noch weniger geschieht dies per Mausklick. Ein Fahnder muss selbst fähig sein, die Resultate zu interpretieren.

Am übersichtlichsten ist „Fotoforensics“ gestaltet. Mit der Error Level Analysis (ELA) und Hidden Pixel lässt sich visuell mutmaßen, ob eine Bilddatei geändert wurde. Auch der Vergleich von Prüfsummen mit „File Digest“ gibt klare Hinweise. Voraussetzung hierfür ist, dass zwei Dateien vorliegen, deren Identität behauptet wird.

Allerdings muss ein Original nur geschärft worden sein, um die Werkzeuge irrezuführen, sie melden dann ein „False Positive“, also eine scheinbare Fälschung. Noch problematischer sind echte Pressebilder, die jemand in einen erlogenen Kontext stellt.

Im Bereich des Fotojournalismus könnten Echtheitszertifikate ein guter Ansatz sein. Erste Zeitungen sind bereits dabei, die Glaubwürdigkeit ihrer Pressebilder damit zu untermauern.

Die vorgestellten Strategien erscheinen erfolgversprechend. Doch wie beurteilt sie ein Experte? **FOTO**HITS fragte den Forensiker Dr. Stefan K. Braun nach dem Stand der Technik und wie er mit ihr Manipulationen aufdeckt.

FOTOHITS: **Bildforensik kennen die meisten nur vom Hörensagen. Es wäre daher erhellend, sie in Bezug auf Künstliche Intelligenz einzuordnen.**

Dr. Braun: Grundsätzlich gilt, dass seit den Anfängen der Fotografie auch gefälscht wird. Berühmt ist etwa das Porträt von Abraham Lincoln von zirka 1860, bei dem sein Kopf auf den Körper des Südstaaten-Politikers John Calhoun montiert wurde. Zur zeitlichen Einordnung: Das erste Lichtbild entstand 1826 und die Lincoln-Fälschung ist 160 Jahre alt.
Im FOTO HITS-Artikel kommen drei Bereiche zusammen: KI, Bild- und Fotoforensik. Die Bildforensik befasst sich überwiegend mit Bildern, die aus Digitalkameras kommen. Selten bekomme ich allerdings Originale, sondern häufiger etwa YouTube-Links oder gar Screenshots. Schlimmstenfalls wurden die Bilder ausgedruckt, abfotografiert und dann in ein PDF-Dokument eingebettet. Aus ihnen lässt sich nichts mehr herauslesen.

FOTOHITS: **Mancher Laie sähe solche Änderungen sofort als Beweis, dass ein Original verfälscht wurde. Dagegen bewertet ein Wissenschaftler das PDF als kontaminiertes und damit unbrauchbares Ausgangsmaterial, richtig?**

Dr. Braun: Richtig. Das war auch der Fall bei Ihrem montierten Kuhkopf. Hier entpuppten sich nicht einmal die beiden Ausgangsbilder als original: Sowohl die Kuh als auch die Frau wurden von ihren Fotografen massiv nachbearbeitet, dann erstellte die Redaktion ein Mischbild aus beiden. Damit war bereits das Grundmaterial für einen Test ungeeignet. Wie also soll man noch „echt“ von „falsch“ abgrenzen?
Nochmals zur Einordnung: Die Bildforensik ist eine Teildisziplin der Multimedia-Forensik. Sie ist darauf ausgelegt, die Authentizität digitaler Bilder festzustellen und gilt als blindes Verfahren. Das heißt, dass ich gewöhnlich keine Originale vorliegen habe, sondern nur die Manipulation. Es fehlt der direkte Vorher-Nachher-Vergleich. Der Fälscher ist schließlich nie so dumm, das Original mitzuliefern. Rein am Computer erstellte Grafiken würde ich hier ebenfalls ausklammern, sie deckt die Bildforensik nicht ab.
Wichtig ist zudem, die Bild- von der Fotoforensik abzugrenzen. Letztere beschäftigt sich mit vorrangig damit, Metadaten auszulesen. Dazu gehören etwa die Dateisysteme von Kameras, Bildformate, Daten im Sinne der Informationstechnik sowie Personen-Identifizierung oder „Face Recognition“ im Unterschied zur bloßen „Face Detection“, die ein Fotograf als kleines Rechteck auf seinem Kameramonitor sieht. Wir sprechen über Bildforensik!

FOTOHITS: **Welche Art von Fälschungen begegnen Ihnen in Ihrem Berufsalltag am häufigsten?**

Dr. Braun: Im kriminalistischen Umfeld geht es um Straftaten wie Einbrüche, Überfälle und Sexualdelikte. Gerade zu letzterem Thema wird es Ihnen nicht möglich sein, öffentliche Online-Tools wie fotoforensic.com zu benutzen, da Nacktdarstellungen zur Sperrung führen. Das gilt umso mehr, wenn Sie mit wirklich schlimmen Fällen wie etwa Missbrauch kommen.
In anderen Strafverfahren werden Menschen denunziert oder retuschierte Fotos auf Porno-Plattformen hochgeladen. Des Weiteren täuschen Kontrahenten Körperverletzungen vor, indem sie Hämatome aufmalen. Sie werden dann an den Sachverständigen in der Hoffnung geschickt, dass er den Fake nicht aufdeckt und er ihn auf diese Weise sogar reinwäscht. Manchmal geht es auch um Baumängel, die angeblich nicht vorhanden sind. Solche Sachen sind oft dilettantisch ausgeführt.
Falls jetzt ein Leser auf die Idee kommt, mir ein Bild zuzuschicken, damit es der Experte rasch überprüft: Die Analyseverfahren, die wir gleich besprechen, sind sehr aufwendig. Je besser der Fake, um so komplizierter ist es, eine sichere Aussage zu treffen. Bei manchem erkenne ich mit bloßem Auge die schlechte Retusche, dann genügen ein bis zwei Methoden, um den Verdacht nachzuprüfen und die Fälschung zu beweisen. Wenn ich damit ein bis zwei Tage zubringe, kostet das selbstverständlich Geld.

FOTOHITS: **Angesichts Ihrer Praxis bleibt festzuhalten, dass ein Papst in Rapper-Klamotten das geringste Problem zu sein scheint.**

Dr. Braun: Solche Bilder sind ebenso wie die der Trump-Verhaftung lächerlich. Hier genügt es, den gesunden Menschenverstand einzuschalten, dass sie nicht stimmen können.
Grundsätzlich ist die Künstliche Intelligenz nicht neu, 1956 förderte etwa die Rockefeller-Stiftung ein Forschungsprojekt, das Vorgänge des menschlichen Denkens automatisieren sollte. Den Gedanken griffen auch Science-Fiction-Autoren wie Stanislaw Lem oder Isaac Asimov auf, der das friedliche Zusammenleben von KI und Mensch beschrieb. Sie gibt es also seit 70 Jahren, bekam aber in den letzten Jahren eine neue Dynamik.
Das maschinelle Lernen ist momentan erst in einer Trainingsphase. Sie können davon ausgehen, dass es sich in den kommenden Jahren in großen Sprüngen verbessern wird. Dazu kommen Entwicklungen wie die Quanten-Technologie, die schnellere und komplexere Rechenvorgänge ermöglicht. Die Kombination mit KI wird revolutionär sein.

FOTOHITS: **Wir reden an dieser Stelle darüber, Manipulationen an einem echten Foto aufzudecken. Trotz aller Einschränkungen scheint mir die Error-Level-Analyse (ELA) die griffigsten Resultate zu bringen.**

Dr. Braun: Sie gehört zu den unzuverlässigeren Methoden, da gibt es Besseres. Aber ich würde sie nicht als minderwertiges Tool bezeichnen. Die ELA schafft einen Interpretationsspielraum, der je nach Vorlage größer oder kleiner ist. Es benötigt einige Erfahrung, die mehr oder weniger deutlichen Ergebnisse zu erkennen.
Es existieren ein bis zwei Dutzend Methoden, um Bildinhalte zu analysieren. Nicht jede von ihnen funktioniert immer. Man sollte sich also nicht auf ein Verfahren kaprizieren, die Wahl hängt von der Entstehung einer Aufnahme, der Tages- oder Nachtzeit sowie der Art der Manipulation ab.

FOTOHITS: **Einige Ihrer Analysen haben wir online gestellt, sie sind auf der Seite www.fotohits.de unter „Themen – Report“ neben dem ausführlichen Interview nachzulesen. Unsereins erkennt nach der Filterung unter „Color Palette“ nur psychedelische Muster und türkise Flächen, noch kryptischer sind die Zahlenreihen.**

Dr. Braun: Sie und die anderen Verfahren unterstützen nur die Erkenntnis, dass das Foto bearbeitet wurde. Daher wäre es in einem gerichtlichen Zusammenhang nicht mehr verwertbar. Es gehört eher zum sportlichen Ehrgeiz, nachzuweisen, wo überall eingegriffen wurde.

FOTOHITS: **Ihre Antwort verdeutlicht nochmals, dass mehrere Methoden zusammenarbeiten müssen, deren Erkenntnisse sich bestenfalls verdichten. Das ist mit fotoforensics.com eingeschränkt möglich, doch sind die Resultate ebenso wie ihre Interpretation problematisch. Haben Sie im Hase-und-Igel-Rennen von Forensik und Fälschern mit Ihren Techniken momentan noch einen Vorsprung?**

Dr. Braun: Der forensische Analyse-Prozess ist komplex und enthält zahlreiche Herangehensweisen. Erst in der Kombination ihrer Erkenntnisse zeichnen sich schließlich Antworten ab. Anders gesagt beruht die Lösung immer auf Wahrscheinlichkeiten, es geht also von „unwahrscheinlich“ bis zu „an Sicherheit grenzender Wahrscheinlichkeit“.
Hase und Igel würde ich gern durch Forensik und Anti-Forensik ersetzen. Dieses Wettrennen existiert tatsächlich, und dabei ist einmal die eine und dann die andere Seite vorn. Wenn gewissermaßen die Bösen überholen, beflügelt das die Guten, einen neuen Ansatz zu finden, um sie auszubremsen.
Die erschreckende Professionalisierung der Deep-Fake-Videos etwa bereitete mir anfangs Sorgen. Suchen Sie beispielsweise einmal bei TikTok nach „Fake“ und „Tom Cruise“. Das Ergebnis ist vom originalen Schauspieler nicht zu unterscheiden. Doch führte ich bei einer Sicherheitsmesse ein Gespräch mit jemandem vom Austrian Institute of Technology. Die Forschungseinrichtung ist dabei, dem etwas mit einer Deep Fake Detection entgegenzusetzen.

FOTOHITS: **Als Zwischenbilanz bleibt einem Laien nur übrig, sein kulturelles Wissen zu nutzen, dass eine Emma Watson, die zuletzt in „Little Women“ brillierte, nie in einem Porno mitspielen würde. Darüber hinaus ist er von Ihrem Fachwissen abhängig.**

Dr. Braun: In der theoretischen Annahme, dass die Videos hundertprozentig perfekt wären und der Forensik weitere Mittel fehlten, der Anti-Forensik die Stirn zu bieten, bliebe in letzter Konsequenz, Fotos und Filme nicht mehr als Beweismittel zuzulassen.

FOTOHITS: **Genau das meinte ein Mitarbeiter von Lucasfilm Arts schon 1982. Mit ihrer Tricktechnik sei „das Ende der Fotografie als Beweis für egal was besiegelt“.**

Dr. Braun: Da hat er nicht völlig unrecht. Doch sagt uns der technische Fortschritt, dass das Spiel von Forensik und Anti-Forensik immer weitergehen wird. Es wird nur immer anspruchsvoller und schwieriger. Wenn ich bereits nur vier ELA-Methoden anwende, dann bekomme ich vier unterschiedliche Erkenntnisse, die es zu interpretieren gilt.
Daher kann ein Normalbürger eigentlich keine sinnvolle Analyse mehr vornehmen. Sie erfordert vertieftes IT-Wissen, technisches und gestalterisches Verständnis sowie die richtigen Werkzeuge. Darüber hinaus muss er deren Resultate richtig interpretieren. Ein Fachmann beschäftigt sich jahrelang damit, sammelt Erfahrungen und ist immer auf dem neuesten Stand, was neue Entwicklungen angeht.

FOTOHITS: **Abschließend würde mich interessieren, was Sie von Echtheitszertifikaten wie TruePic halten.**

Dr. Braun: Das gehört weniger zu meinen Themengebieten. Ich denke, sie sind unter bestimmten Bedingungen ganz nützlich, aber kein Allheilmittel. Denn sie bieten weitere Angriffsflächen. Die Musik- und Buchindustrie versuchte es zum Beispiel mit Kopierschutz-Varianten, die den Benutzer jedoch auf bestimmte Geräte und Installationen einer Firma einengte. Das halte ich nicht für zielführend. Wer kreiert so ein fotografisches Wasserzeichen? Wer schafft einen internationalen Standard, wer verwaltet ihn, wer verfügt über die Datenbank? Hier fehlt mir die Fantasie, wie ein einheitlicher internationaler Standard geschaffen werden soll.
Schon seit Jahrzehnten kann man Wasserzeichen einbinden. Trotzdem hat sich kein Weltstandard durchgesetzt. Ohne ihn entstehen erstens viele Einzelverfahren. Zweitens ist es ohne Überblick schwer nachprüfbar, ob überhaupt ein echtes Zertifikat vorliegt. Dazu kommen ähnliche Probleme wie bei SSL, dass Sicherheitszertifikate kompromittiert werden können und sich damit die Authentizität der verwendeten Zertifikate nicht mehr gewährleisten lässt.

FOTOHITS: **Welche Lösung erscheint Ihnen dann sinnvoll?**

Dr. Braun: Neben einer technischen Implementierung unveränderlicher Metadaten würde ich auch auf die ethische Verpflichtung setzen. Schon wenn ein Fotograf ein Bild aus seiner Kamera nicht nachbearbeitet, kann man es als nachprüfbares Dokument betrachten. Falls notwendige Modifizierungen etwa mittels Druckprofil nötig sind, gibt er der Kopie das unbearbeitete Original mit. So ist für jeden erkennbar, was bearbeitet wurde.

Dr. Stefan K. Braun ist Buch- und Wissenschaftsautor und arbeitet als Forensiker mit den Schwerpunkten Bild-, Audio-, Video- und Medienforensik. In dieser Eigenschaft wurde er in Kriminalfällen hinzugezogen. 2018 wurde er zum Handelsrichter am Landgericht Frankfurt am Main berufen. Dr. Braun hält Gastvorträge an Universitäten zu aktuellen Medienthemen und tritt als wissenschaftlicher Berater in TV-Produktionen in Erscheinung. Bei der IHK Frankfurt am Main ist er Mitglied in den Prüfungsausschüssen für Mediengestalter, Gestaltung und Technik Digital, Konzeption und Visualisierung, Beratung und Planung sowie Gründungsmitglied des Prüfungsausschusses Musikfachwirt/-in (IHK).
www.instagram.com/medienforensiker
https://medien.expert