Wie vertrauenswürdig sind Satellitenbilder im Netz?

von Leonie Dreschler-Fischer und Hartwig Spitzer

Öffentlich zugängliche Satellitenbilder haben die Welt transparenter gemacht. Wer einen Rechnerzugang hat, kann sich detaillierte Bilder von fast allen Teilen der Welt übers Internet anschauen, auch von sicherheitsrelevanten Gebieten. Solche Bilder können verfälscht oder gezielt verändert werden, z.B. durch Verschlechterung der Auflösung oder das Wegretuschieren von Bildinhalten. Aber das ist eher die Ausnahme.

Jedes photographische Bild liefert eine Teilansicht der Wirklichkeit. Der Sensor kann nur das aufzeichnen, wofür er empfindlich ist, z.B. sichtbares Licht oder Radarstrahlung. Die Bildbearbeitung bei der Herstellung des endgültigen Bildes (des Bildprodukts) öffnet ein weiteres Tor für die Veränderung oder Betonung von Bildmerkmalen, wie diejenigen erinnern, die noch im Fotolabor versucht haben, überbelichtete Stellen ihrer Schwarz-Weiß-Fotos nach zu dunkeln. Im Zeitalter der digitalen Photographie ist die gezielte Veränderung von Bildern gang und gäbe, z.B. das Glätten von Falten im Gesicht der Kanzlerin, das Herausretuschieren von störenden Personen oder die Fotomontage verschiedener Bilder.

Luft- und Satellitenbilder von vielen Teilen der Welt sind heute jedem zugänglich, der über einen Zugang zum Internet verfügt. Die Auflösung der dort gezeigten Satellitenbilder liegt zwischen 50 cm und einigen Metern, die der verwendeten Luftbilder zwischen ca. 10 cm und etwa einem Meter, also Werten, die durchaus sicherheitsrelevant sein können. Unter Auflösung wird hier die Größe eines Bildelements (Pixel) verstanden. Bei einer Auflösung von 50 cm lassen sich einzelne Personen bei niedrig stehender Sonne noch als Objekt erkennen. Größeres Militärgerät (gepanzerte Fahrzeuge, Flugzeuge) kann dem Typ nach identifiziert werden. Satellitenbilder von vielen sicherheitsrelevanten Gebieten können trotz einiger Einschränkungen auch von Nichtregierungsorganisation oder Friedensforschungsinstituten erworben und ausgewertet werden. Aus einem Originalbild lässt sich deutlich mehr Information gewinnen als aus den im Netz wieder gegebenen Bildern, z.B. durch Nutzung der größeren Datentiefe (bis zu 16 bit), Auswertung in mehreren Farbkanälen und gegebenenfalls auch Stereoauswertung.

Die Fälschung oder Verschlüsselung von militärisch relevanter Information hat eine lange Geschichte, z.B. das Wegretuschieren von militärischen Anlagen aus Landkarten (Brunner 2003; Bojanowski 2008). In diesem Beitrag wird nach der Zuverlässigkeit von Luft- und Satellitenbildern im Netz gefragt. Wann kann man von einer Fälschung sprechen? Wie häufig kommt so etwas vor? Wie sicher lassen sich Fälschungen erkennen? Die Autoren verstehen unter einer Fälschung die bewusste Veränderung eines Bildes zum »Vertuschen oder Vortäuschen« von Bildinhalten (siehe auch Trinkwalder 2008a).[1] Daneben wird von der technisch einfacheren »Informationsverringerung« Gebrauch gemacht, indem die Auflösung des Bildes gezielt verschlechtert wird.

Shutter Control

Die Vertreiber von Satellitenbildern haben in der Regel kommerzielles oder wissenschaftliches Interesse an der Zuverlässigkeit ihrer Bilder im Interesse ihrer Kunden. Sie unterliegen allerdings der staatlichen Gesetzgebung und Aufsicht. So behält sich die US Regierung in der Presidential Decision Directive 23 von 1994 vor, die kommerzielle Datennahme zu begrenzen, wenn die nationale Sicherheit, internationale Verpflichtungen oder Interessen der Außenpolitik beeinträchtigt werden. Diese »Shutter Control« soll aber auf das kleinstmögliche Gebiet und den kleinstmöglichen Zeitraum begrenzt werden (O´Connell 2001). Bei Beginn des Afghanistankrieges im Oktober 2001 hat die US Regierung z.B. alle Bilder des IKONOS-2 Satelliten über Afghanistan aufgekauft, um anderen Stellen den Zugang zu verwehren. Ebenso wurde in der heißen Phase des Irakkrieges von 2003 der freie Verkauf von aktuellen Bildern der amerikanischen kommerziellen Satelliten für einige Wochen unterbunden. US Regierung und Kongress haben außerdem verfügt, dass amerikanische Firmen Bilder von Israel nur mit einer Auflösung von 2m oder schlechter vertreiben dürfen. In der Praxis von Google Earth gilt das auch für die West Bank. In Deutschland wurde in einem Satellitendatensicherheitsgesetz vom 23. November 2007 geregelt, unter welchen Bedingungen hoch aufgelöste Bilder des TerraSAR-X Satelliten an Kunden verkauft werden dürfen.

Methoden zur Bildverfälschung

Digitalbilder sind mit Standardverfahren der Bildverarbeitung sehr leicht zu manipulieren – alle Verfahren, die wir hier vorstellen werden, lassen sich schon mit gängigen Programmen, z.B. Adobe Photoshop oder GIMP, am heimischen PC durchführen. Da wir an solchen möglicherweise manipulierten Bildern, die wir im Internet gefunden haben, nicht das Urheberrecht haben, können wir diese

hier nicht zeigen. Wir haben aber Verweise auf einige zugehörige Internetseiten, Google-maps und kmz-Files für die Ansteuerung bei Google Earth auf einer Internetseite zusammengestellt (http://web.me.com/dreschler/Leonie/Fake/Fake.html; Javascript-Aktivierung erforderlich).

Folgende Verfahren zur Bildmanipulation oder -verfälschung kommen infrage:

- Verpixelung: Die Manipulation, die bei Google Earth und Google Maps am häufigsten zu finden ist, ist die Reduktion der geometrischen Auflösung durch Verpixelung: Bildelemente werden zu Rechtecken oder zu unregelmäßigen Kacheln zusammengefasst, so dass weniger Details zu erkennen sind (vgl. Abb. 1). Die zufällige Kachelung hat den Vorteil, dass die Manipulation weniger auffällig ist als bei regelmäßigen Rechtecken. Ein Beispiel hierfür ist die Google Earth Darstellung der NATO-Airbase Geilenkirchen (Position 50°57‘38.37“N, 6° 2‘27.57“E), bei der die Startbahn und die umliegenden Gebäude deutlich schlechter aufgelöst sind als die Umgebung. Bei BING und NAVTEQ dagegen sind selbst einzelne Flugzeuge auf dem Vorfeld zu erkennen mit einer Auflösung von geschätzt 0,5-1 m. Auch der Marinehafen in Den Helder, Niederlande (52°57‘31.81“N, 4°47‘10.75“E) wurde bei Google Earth relativ stark mit unregelmäßiger Kachelung in der Auflösung reduziert. Gleichzeitig werden aber mehrere sehr scharfe Bodenaufnahmen von Kriegsschiffen eingeblendet.
- Verdeckung: Gelegentlich werden Bildbereiche mit einfarbigen oder texturierten (gemusterten) Formen überlagert und dadurch maskiert. Ein schönes Beispiel hierfür ist der Reaktorkomplex in Dimona, Israel (31° 3‘38.57“N, 34°59‘36.26“E). Die Gebäude erscheinen bei Google Earth durch eine große ovale Form maskiert, aber die Umzäunung und die Strassen sind noch zu erkennen.
- Ersetzen von Bildausschnitten: Die bisher genannten Verfahren führen zu offensichtlich erkennbaren Manipulationen. Anders verhält es sich, wenn Bildbestandteile durch andere Bildbestandteile ersetzt werden. So kann kritische Infrastruktur versteckt werden, ohne dass die genaue Position der Anlagen verraten wird, und die Manipulationen sind nicht immer leicht zu entdecken. Die eingefügten Masken können aus unterschiedlichen Quellen stammen: Sie können aus älteren Aufnahmen des Gebietes ausgeschnitten werden, bei denen das Gelände noch nicht bebaut war, oder aus anderen Aufnahmen stammen, die ein geeignetes, unbebautes Gebiet zeigen. Abbildung 2 zeigt ein Beispiel für dieses Verfahren, bei dem Teile desselben Bildes (ein Flugzeug) in der Helligkeit angepasst und im Bild verschoben wurden. Die Darstellung der Nellis AFB Bombing Range im Death Valley bei Google

Abb. 1: Ein Beispiel für Auflösungsverringerung durch Verpixelung und Weichzeichnung: Eine Luftaufnahme des Flughafens Nürnberg, Flughöhe 300m. Im linken Viertel des Bildes wurden je 8x8 Pixel zu einem Rechteck zusammengefasst, es folgt ein Streifen, der mit einem sog. Gaussfilter (Radius 3 Pixel) weich gezeichnet wurde, dann ein Streifen mit Originalauflösung von 90 cm; am rechten Rand wurde der Bildinhalt in unregelmäßigen Kacheln zusammengefasst, deren Form nach einem Zufallsverfahren variiert.

Quelle des Originalbildes: DLR und Universität Hamburg, CENSIS, Department Informatik

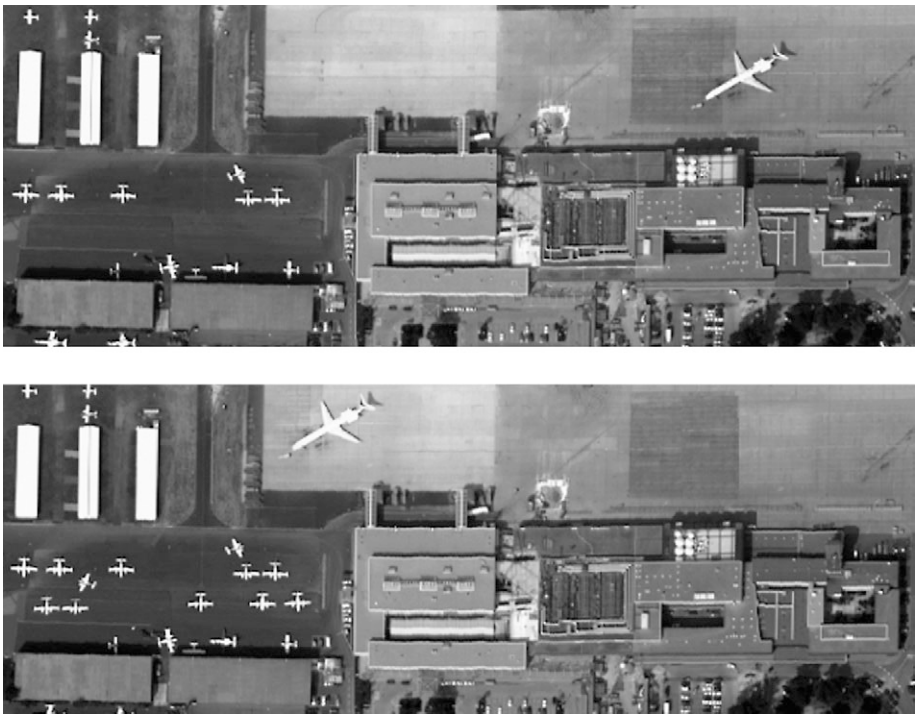

Abb. 2: Ein Beispiel für Modifikation durch Einsetzen von Bildausschnitten:

a) Das Originalbild des Flughafens Nürnberg, aufgenommen am 21. August 1991 mit einer Auflösung von 90 cm (Quelle: DLR und Universität Hamburg, CENSIS, Department Informatik)

b) Das modifizierte Bild. Das große Flugzeug wurde durch einen neutralen Hintergrund ersetzt und an einem Ort weiter links wieder eingefügt. Es wurden vier weitere Sportflugzeuge hinzugefügt.

Earth ist ein weiteres Beispiel für diese Technik. Ein kleiner länglicher Bereich an der Position (37°37‘51.82“N 116°52‘32.44“W) hebt sich in der Helligkeit und durch eine niedrigere Auflösung deutlich von der Umgebung ab, so dass eine Manipulation durch kopierte Bildbereiche oder Weichzeichner wahrscheinlich erscheint.

- Retusche: Ein Teil des Bildes wird mit virtuellen Pinseln so übermalt, dass der ursprüngliche Bildinhalt spurlos verschwindet und stattdessen ein neutraler Hintergrund oder verdeckender Vordergrund, z.B. Wolken, zu sehen sind. Ein schönes Beispiel hierfür ist die Retusche des Google Earth Bildes der »Area 51« in Nevada, die »allMIGHTY« (allMIGHTY, 2008) im abovetopsecret-Forum veröffentlicht hat. Hier ist zu sehen, wie das Groom Lake-Gebiet ohne die Elliot Air Force Base aussehen würde.

Über die Jahre hat sich die Darstellung ausgewählter Objekte bei Google Earth je nach politischer Lage geändert. Dieses kann über die Option »historisches Bildmaterial zeigen« nachvollzogen werden. Wenn Sie in Google Earth die Position 38°53‘51.44“N, 77°2‘11.56“W anfliegen, stehen Sie direkt über dem Weißen Haus in Washington und können durch Verschieben des Markers auf dem Zeitstrahl eine Zeitreise von 1999 bis jetzt machen und dabei unterschiedliche Grade der Maskierung von Gebäudeteilen und Verpixelung sehen.

Methoden zur Erkennung von Bildverfälschungen

In den letzten Jahren hat sich ein neues Teilgebiet der Bildverarbeitung etabliert, die »digital image forensics«, das man auf deutsch vielleicht mit Digitalbildforensik bezeichnen könnte, und das sich mit Methoden zur Entdeckung von Bildmanipulationen beschäftigt.

Zur Erkennung von Bildverfälschungen gibt es im Wesentlichen zwei Gruppen von Verfahren: Zum einen die statistischen Verfahren, die allgemein einsetzbar sind, und zum anderen die wissensbasierten Verfahren, die Vorwissen über die Szene erfordern und im Einzelfall anwendbar sein können. Eine Einführung in dieses Thema finden Sie bei Trinkwalder (2008b).

Statistische Verfahren

Statistische Verfahren arbeiten auf der Pixel- und Signalebene des Bildes und nutzen aus, dass das Rauschen des Bildsignals charakteristische Merkmale aufweist, die als Fingerabdruck der Kamera oder des Sensors betrachtet werden können. Betrachtet man die Gesamtheit der Pixel eines Bildes als Stichprobe, so lassen sich mit statistischen Modellen verschiedene Hypothesen testen: Wie wahrscheinlich ist beispielsweise, dass

- alle Pixel des Bildes von derselben Kamera aufgenommen wurden?
- alle Pixel mit einer bestimmten Kamera aufgenommen wurden?
- Teile des Bildes durch Kopieren verdoppelt wurden?

Der Vorteil dieser Verfahren ist, dass sie allgemein eingesetzt werden können und nichts über den Bildinhalt und die Aufnahmebedingungen bekannt sein muss. Daher können sie zum systematischen Durchsuchen großer Datenbestände eingesetzt werden (zum statistischen Fingerabdruck siehe beispielsweise Chen u.a. 2008).

Neben den Hypothesentests werden auch Korrelationsverfahren eingesetzt. Hiermit lassen sich kopierte, rotierte oder skalierte Bildausschnitte erkennen, aber auch Veränderungen durch eine Neuabtastung des Bildes, die beim Kopieren zwischen Bildern mit unterschiedlicher Auflösung notwendig ist (siehe beispielsweise Lu u.a. 2008).

Konsistenzprüfung/ Wissensbasierte Verfahren

Bei Fernerkundungsbildern (Satellitenbilder, Luftaufnahmen) sind in der Regel die Aufnahmebedingungen sehr genau bekannt. Aus der genauen Position der Aufnahmeplattform (Bahn des Satelliten, Flugbahn und Flughöhe des Flugzeugs) und dem Zeitpunkt der Aufnahme lässt sich mit photometrischen und geometrischen Modellen prüfen, ob die Form und der Ort von Bildkompo-

Quellen von Luft- und Satellitenbildern

Wegen des hohen technischen Aufwands und der hohen Kosten beim Bau, Start und Betrieb von hoch auflösenden Satelliten ist dieses Unterfangen großen Unternehmen und staatlichen Einrichtungen vorbehalten.

Folgende Unternehmen oder Einrichtungen betreiben kommerzielle oder öffentliche Satelliten mit hoher bis sehr hoher Auflösung (Auswahl):

- DigitalGlobe, USA (www.digitalglobe.com) mit den Satelliten »Quickbird-2« (Auflösung 0,6m), »Worldview-1« (0,5m)
- GeoEye, USA (www.geoeye.com) mit »IKONOS-2« (1m), »GeoEye-1« (0,4-0,5m)
- Spot Image, Frankreich (www.spotimage.fr) mit »SPOT-5« (2,5 m), vertreibt auch Bilder des koreanischen »KOMPSAT-2« Satelliten (1 m)
- Deutsches Zentrum für Luft- und Raumfahrt DLR (www.dlr.de) mit dem Radarsatellit »TerraSAR-X« (1m)

Die Bilder werden entweder direkt an die Endnutzer verkauft oder über Zwischenhändler, wie NAVTEQ (www.navteq.com), TerraServer (www.terraserver.com) und Infoterra (www.infoterra.de).

Ins Netz gestellte Luftbilder werden in Überfliegungskampagnen zahlreicher kommerzieller Luftbildfirmen gewonnen wie z.B.

- Terra Metrics (www.truearth.com)
- Geocontent (www.geocontent.de)
- AeroWest (www.aerowest.de)

Als Betreiber von Internetseiten mit Luft- und Satellitenbildern, die kostenlos aufgerufen werden können, sind vor allem folgende Firmen zu nennen:

- Google in Form von Google Earth und Google Maps (earth.google.com bzw. maps.google.com)
- Microsoft in Form von Bing Maps (www.bing.com/maps; Luftbilder)
- NAVTEQ (bieten auf ihrer Homepage www.navteq.com ebenfalls einen Service vergleichbar mit Google Maps an.)
- TerraServer USA (nur freie Bilder der USA) (www.terraserver-usa.com)
- diverse Regierungen vor allem im Zusammenhang mit der Wettervorhersage (z.B. Australien unter http://www.bom.gov.au/weather/satellite/).

nenten mit den gegebenen Aufnahmebedingungen konsistent sind. Mögliche Tests:

- Schatten: die Richtung der Schatten hängt von der Position der Sonne ab und sollte für alle Gebäude gleich sein.
- Globalstrahlung: Wenn wir den Sonnenstand und die Wetterbedingungen kennen, kann ein Atmosphärenmodell zur Berechnung der Globalstrahlung (des zur Beleuchtung des Geländes insgesamt verfügbaren Lichtes) verwendet werden. Bereiche, die zu hell oder dunkel erscheinen, wurden vermutlich zu einem anderen Zeitpunkt oder mit einem anderen Sensor aufgenommen.
- Radialer Versatz: Das Dach eines Gebäudes erscheint in Luftbildern bei schräger Aufsicht radial gegen die Gebäudebasis versetzt; die Richtung des Versatzes hängt von der Projektion, dem Ort im Bild und der Gebäudehöhe ab. Wenn der radiale Versatz eines Gebäudes nicht mit dem der Umgebung konsistent ist, lässt das auf eine Manipulation schließen.

Diese Prüfungen sind aber aufwändiger als die statistischen Verfahren und sind eher für eine Detailanalyse geeignet, wenn im Einzelfall ein Fälschungsverdacht besteht. Mit genügend krimineller Energie lassen sich die Bilder natürlich auch so fälschen, dass sie gegen diese Prüfkriterien bestehen können.

Stichproben

Wie zuverlässig sind Satellitenbilder im Netz? Eine systematische, umfassende Untersuchung würde den Rahmen dieses Artikels überschreiten. Es ist aber relativ leicht möglich, die Informationsverringerung durch Verschlechterung der Auflösung von Militärstandorten zu untersuchen. Wenn sich die Auflösung zwischen Umgebung und Standort oder innerhalb des Standorts ändert, kann das ein Indiz für gezielte Informationsverringerung sein.[2] Die Autoren haben Stichproben zur Auflösung von zehn Militärstandorten bei Google Earth gemacht. Es ergab sich kein einheitliches Bild, das auf eine systematische Informationsverschlechterung schließen lässt. Aber sie kommt vor.

Mehrere große Militärstandorte in den USA werden durchgängig mit einer erstaunlich guten Auflösung von geschätzt 30-70 cm gezeigt (Naval Station in Norfolk, Virginia, und San Diego, California, MacDill AFB, Coronado, Florida). Die Schätzung erfolgte anhand der Wiedergabeschärfe von bekannten Objekten wie PKW´s.

In zwei Fällen verschlechterte sich die Auflösung in Teilbereichen des Standorts, was auf eine Manipulation schließen lässt (Marine Corps Base Camp, Lejeune, North Carolina, Nellis AFB Bombing Range, Nevada (s.o.). Die in Deutschland liegenden Militärbasen bei Baumholder, Hammelburg und Ramstein und ihre zivile Umgebung werden mit einer Auflösung von geschätzt 1-2m gezeigt. Bei den Bildern von Baumholder und Ramstein (eingesehen am 15.8. 2009) fallen sehr helle Flächen auf, die von Verdeckung von Teilen des Flugplatzes und einiger Straßen im Gelände durch im Bild überlagerte Formen stammen können. Der zivile und der militärische Teil des Flughafens von Bagdad werden mit einer gleichbleibenden Auflösung von geschätzt 0,5 – 1m wiedergegeben, ebenso der Flughafen von Kabul ohne Anzeichen von Verdeckung.

Fazit

Die große Überzahl der Luft- und Satellitenbilder im Netz kann als vertrauenswürdig angesehen werden. Fälschungen oder Informationsverringerung auf Bildern können in der Regel erkannt werden. Es ist allerdings – wie bei Bildern der Kunstgeschichte – möglich, Bilder so geschickt zu fälschen, dass eine Entdeckung unwahrscheinlich wird. Die Chance, mit einer Fälschung unentdeckt zu bleiben, schwindet. Bilder verschiedener Anbieter und Bilder von verschiedenen Aufnahmezeiten liefern Möglichkeiten, Widersprüche aufzudecken. Ein Fälscher müsste alle Anbieter der Welt für alle Aufnahmen des relevanten Gebiets in die Pflicht nehmen. Viel wahrscheinlicher ist es, dass militärische und geheimdienstliche Stellen von zwei einfachen Möglichkeiten der begrenzten Kontrolle Gebrauch machen: verspätete Freigabe von Bildern sensitiver Orte und Informationsverringerung durch verschlechterte Auflösung.

Danksagung
Ein Teil der Recherche zu diesem Artikel wurde von Max Brauer und Timme Katz im Rahmen einer Projektarbeit im Department Informatik der Universität Hamburg durchgeführt.

Literatur

allMIGHTY (2008): http://www.abovetopsecret.com/forum/thread325113/pg1#pid3864265, zuletzt am 13.8.2009 besucht.

Bojanowski, Axel (2008): Es führt kein Weg nach nirgendwo, *Süddeutsche Zeitung* vom 10. Dezember 2008

Brunner, Kurt (2003): Geheimhaltung topographischer Karten und Manipulation ihres Inhalts, *Allgemeine Vermessungsnachrichten*, AVN, 5: 183-187

Chen, M. & Fridrich, J. & Goljan, M. & Lukas, J. (2008): Determining image origin and integrity using sensor noise. *IEEE Transactions on Information Forensics and Security* 3(1), S. 74-90.

Lu, W. & Sun, W. & Huang, J.-W. & Lu, H.-T. (2008). Digital image forensics using statistical features and neural network classifier. In: International Conference on Machine Learning and Cybernetics, Kunming, 5: 2831–2834.

O´Connell, Kevin & Hilgenberg, Greg (2001): U.S. Remote Sensing Programs and Policies, in: John C. Baker & Kevin O´Connell & Ray A. Williamson (Hrsg.): Commercial Observation Satellites, RAND, Santa Monica, ASPRS, Bethesda, 2001, S. 139-163

Popescu, A. C. & Farid, H. (2005). Exposing digital forgeries by detecting traces of re-sampling. *IEEE Trans. Signal Process* 53(2), S. 758-767.

Swaminathan, A. & Wu, M. & Liu, K. J. R. (2008). Digital image forensics via intrinsic fingerprints. IEEE Transactions on Information Forensics and Security, 3(1), S. 101-117.

Trinkwalder, Andrea (2008a): Können diese Pixel lügen? Der schmale Grat zwischen Bildoptimierung und -fälschung, *c't* 27(18):148-151.

Trinkwalder, Andrea (2008b): Pixelsezierer. Digitale Forensik: Algorithmus jagt Fälscher, *c't* 27(18):148-151.

Anmerkungen

1 Danach wäre auch ein erheblicher Teil der heutigen Werbefotos als Fälschung zu bezeichnen. Den Werbern geht es allerdings weniger ums Vertuschen als um die gezielte Beeinflussung von Meinungen und Präferenzen.

2 Es kann aber auch an der Verwendung eines anderen Originalbildes mit schlechterer Auflösung liegen. Die Form des veränderten Bereichs kann ein Schlüssel sein.

Leonie Dreschler-Fischer ist Professorin für Informatik (Bildverarbeitung/Kognitive Systeme) im Department Informatik der Universität Hamburg und Mitglied des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIFF). Hartwig Spitzer ist Professor i.R. im Department Physik und assoziiertes Mitglied des Carl Friedrich von Weizsäcker-Zentrums für Naturwissenschaft und Friedensforschung der Universität Hamburg.