Deanonymisierung von Profilen sozialer Netzwerke unter Nutzung von Metadaten aus Bildern

Ulrich Greveler[1] · Dennis Löhr[1]

[1]Fachhochschule Münster, Labor für IT-Sicherheit
{greveler | d.loehr}@fh-muenster.de

Abstract

Der Beitrag beschreibt, wie veröffentlichte Bilddateien genutzt werden können, Benutzer sozialer Netzwerke zu deanonymisieren oder Beziehungen zwischen Benutzern aufzudecken, die nicht über das soziale Netzwerk abgebildet sind. Dabei geht es nicht um Personen, die auf Bildern zu erkennen sind; vielmehr werden Metadaten oder Rauschmuster aus Bildern mit beliebigen Motiven ausgelesen und aggregiert, um Aussagen über den (Hobby-)Fotografen zu gewinnen bzw. Ähnlichkeiten zwischen Profilen zu identifizieren, die u. a. zur Bildveröffentlichung angelegt wurden. Wesentliche Metadatenfelder, die hierbei eine Rolle spielen, sind die via EXIF eincodierten Felder *Cell-ID* von Funkzellen, Seriennummer der Kamera und nutzerspezifische Einstellungen.

1 Einführung

Die breite und kostengünstige Verfügbarkeit digitaler Kameras und die niederschwelligen Möglichkeiten, Bilder zusammen mit erläuternden Texten und Profilinformationen im Netz zu präsentieren (soziale Netzwerke, private Homepages, Foto-Dienstleistungsportale wie *Flickr*[1]), führte in den letzten Jahren zu einem deutlichen Anstieg[2] von frei verfügbarem Bildmaterial im Internet.

Datenschützer und Web-2.0-Experten warnten in der jüngeren Vergangenheit davor, dass insbesondere jüngere (und unbedarfte) Nutzer sozialer Netzwerke, Bilder veröffentlichen, die die Reputation auf dem weiteren Lebensweg beschädigen können (Hauptkritikpunkt: freizügige Partybilder könnten von potentiellen Arbeitgebern gefunden werden[3]). Zwar könnte eine vollständige Spurenlosigkeit im Internet einen Bewerber ebenfalls *verdächtig* erscheinen lassen; es ist jedoch auf Datenschutzsicht zu begrüßen, wenn Nutzer sozialer Netzwerke ein Bewusstsein dafür entwickeln, welche personenbezogenen Informationen sie publizieren möchten (und welche besser nicht).

In diesem Beitrag untersuchen wir technische Möglichkeiten, anonym im Netz auftretende Personen über Metadaten, die in die Bilddateien eingebracht sind (insbesondere sog. EXIF-

[1] Dienst des Internetunternehmens *Yahoo* mit dem Webauftritt: http://www.flickr.com/

[2] Bei *Flickr* waren nach Unternehmensangaben (http://blog.flickr.net/en/2009/10/12/4000000000/) im Okt. 2009 bereits über 4 Milliarden Bilder gespeichert. Die Steigerungsrate nimmt kontinuierlich zu.

[3] Zitat von Constanze Kurz, Sprecherin des Chaos Computer Club (CCC): *Man sollte auf keinen Fall Bikini- oder Party-Bilder in einem solchen Netzwerk veröffentlichen.* Zitiert von *dpa* am 07.05.2008

Daten, aber auch Rauschmuster der Kamerasensoren), zu identifizieren und Beziehungen zwischen Personen aufzudecken, die nicht aus dem Web-2.0-Beziehungsgeflecht ablesbar sind. Diese Möglichkeiten untergraben die Entscheidungen der Nutzer (und Bildautoren), Bilder ohne Zuordnung zu einem Profil aus personenbezogenen Daten, zu veröffentlichen. Der beabsichtigte Schutz der eigenen Privatsphäre läuft ins Leere, wenn die Nutzer (vermutlich unbewusst) Metadaten mit ihren Fotografien publizieren, die eine Deanonymisierung des Bildautors zulassen oder Beziehungen zu anderen Personen aufdecken, die aufgrund einer bewussten Entscheidung nicht im sozialen Netzwerk abgebildet sind.

2 Technischer Hintergrund

Das *Exchangeable Image File Format* (meist EXIF abgekürzt), ist ein Standard [4] für die Codierung von Metadaten innerhalb einer Bilddatei. Digitale Kameras verwenden i. d. R. die Grafikformate *JPEG File Interchange Format* und *Tagged Image File Format* zum Speichern der Bilder. In diese Datenformate können EXIF-Metadaten ohne die Anlage zusätzlicher Dateien eingebracht werden. JPEG-Bilder können ohne weitere Bearbeitung bzw. Konvertierung im Internet publiziert und vom Webbrowser innerhalb einer Webseite oder ohne Kontext dargestellt werden. Neben EXIF spielt auch IPTC[4] als Metadatenformat[1], insbesondere zur Nennung des Autors und zur Einbettung von Schlagworten durch Bildbearbeitungsprogramme eine Rolle; in technischer Hinsicht sind die Formate gleichwertig (direkte Einbettung in die Bilddatei möglich).

Die Metadaten werden nicht dargestellt, können aber mit entsprechenden Werkzeugen (z. B. Exif Viewer[5] oder Bildbearbeitungssoftware) sichtbar gemacht und verändert werden.

Einige Metadaten sind nützliche Informationen, die von Bildbetrachtern ausgewertet werden (z. B. Orientierung der Kamera, um gedrehte Bilder zu vermeiden) oder Ortsinformationen, die für das sog. *Geotagging* (raumbezogene Referenzinformationen, z. B. GPS-Koordinaten) verwendet werden können. Zudem enthalten sie meist Belichtungszeiten, Empfindlichkeit (ISO), Brennweite, Farbraum, Datum und Uhrzeit (u. a.), die eine Sortierung der Bilder bzw. geeignete Weiterverarbeitung in Bildbearbeitungsprogrammen gemäß dieser Informationen ermöglichen. Datenfelder können frei definiert werden, so dass ein Kamera- bzw. Softwarehersteller auch neuartige Metainformationen und proprietäre Angaben einbetten kann.

EXIF-Felder können bereits unmittelbar personenbezogene Daten enthalten. Dies ist für den Nutzer nicht notwendigerweise transparent. Beispielsweise fragen einige von Handy-Herstellern bereitgestellte PC-Programme, die den Datenabgleich und Bildaustausch zwischen PC und Mobiltelefon bewerkstelligen, den Nutzer bei der Erstnutzung der Software nach Namen, Adresse und anderen persönlichen Angaben. Während dieser die Angaben arglos (z. B. bei der Registrierung zur Abwicklung von späteren Gewährleistungsfällen) vornimmt, kann die Handykamera im Zusammenspiel mit der Software so konfiguriert sein, dass diese personenbezogenen Daten später in die einzelnen Bilddateien via EXIF eincodiert werden. [2]

Lizenzinformationen über Bilder können ebenfalls in den Metadaten enthalten sein (z. B. Standardlizenzverträge nach *Creative Commons*). Dabei ist es möglich, Lizenzverstöße veröffentlichter Bilddateien automatisiert festzustellen. [5]

[4] IPTC: International Press Telecommunications Council

[5] Das Tool *Exif Viewer* 1.55 von Alan Raskin kann beispielsweise als Plug-In für den weitverbreiteten Webbrowser *Firefox* verwendet werden, um technische Resultate dieses Beitrags nachzuvollziehen.

Eine massenhafte Auswertung der Metadaten von Bilddatenbanken und sozialen Netzwerken ist nicht allein für den Betreiber möglich. Angesichts der großen Datenmengen (bei einzelnen Webportalen übersteigen die Bilddatenmengen bereits die Petabyte-Grenze) erscheint eine vollständige Auswertung über Netzzugriffe nahezu unmöglich; dies ist jedoch ein Trugschluss: Die EXIF-Daten sind zu Beginn der Bilddatei gespeichert; es ist daher für Außenstehende möglich, diese Daten durch gezielte, ressourcenschonende Zugriffe (TCP-Disconnect nach dem ersten Datenpaket) automatisiert abzufragen und in eine Datenbank zur weiteren Auswertung zu überführen. Die schlank kodierten EXIF-Daten einer großen Bilddatenbank können daher durchaus über eine private DSL-Leitung in ihrer Gesamtheit erhoben werden.

3 Nutzung der Metadaten zur Deanonymisierung

Das augenfälligste Merkmal, das von Kameras in die Bilddateien via EXIF eincodiert wird, ist eine (weltweit eindeutige) Seriennummer. Diese identifiziert die Kamera[6] ; unter der Annahme, dass die Kamera i. d. R. von genau einer Person bzw. im Beisein dieser Person genutzt wird, können wir veröffentlichte Bilder für diese Person zusammenfassen. Für die weiteren Überlegungen stützen wir uns auf diese Annahme, die nach Einschätzung der Autoren für die überwiegende Zahl der Digitalkameras und Fotohandys zutreffen dürfte. Nutzt diese Person mehrere soziale Netzwerke bzw. Webauftritte zur Veröffentlichung der Bilder – hierbei ist insbesondere die gleichzeitige Nutzung anonymer und nicht-anonymer Communities zu betrachten – können wir Profile mit personenbezogenen Daten anhand der Seriennummer der Kamera den anonym veröffentlichten Bildern zuordnen und die Person auf den anonym genutzten Plattformen deanonymisieren.

Neben der Seriennummer sind ortsbezogene Informationen von Bedeutung. Zwar könnten wir zunächst davon ausgehen, dass die Einbettung von GPS-Koordinaten zum Zweck des *Geotaggings* von den Nutzern bewusst herbeigeführt[7] wird (die Lokalisierung muss bei Kamerahandys meist aktiviert werden und erfordert einen zeitlichen Vorlauf), jedoch wird von einigen Handykameras auch die *GSM-Cell-ID* als EXIF-Datenfeld in die Bilder eingebracht. Diese stellt eine dem Mobiltelefon ständig bekannte, mittelbar ortsbezogene Information zur Funkzelle dar, womit eine Lokalisierung mit einer gewissen Genauigkeit (abhängig von den Ausmaßen der Funkzelle, die wenige hundert Meter, aber auch in ländlichen Gebieten einige Kilometer betragen kann) gegeben ist.

Ein weiteres Merkmal ergibt sich aus der Kombination von Datenfeldern, die durch Zusammenführung Eindeutigkeit erlangen. So verzeichnet die Kamera i. A. einen Hinweis auf Hersteller und Typ; dieser lässt sich auch aus der Information über die Existenz einiger Datenfelder weiter eingrenzen, da die Kameras sehr unterschiedlich von der Möglichkeit, gewisse Felder einzucodieren, Gebrauch machen. Nehmen wir dann längerfristige nutzerseitige Einstellungen hinzu (Empfindlichkeit, Daten aufgeschraubter Objektive, Timeslots wie regelmäßig bei der Bilderstellung auftretende Tageszeiten oder Wochentage, Auflösung, Blitzeinstellung, Rotation, Farbabgleicheigenschaften, Nummernraum der Dateinamen), lässt sich ein Fingerabdruck errechnen, der einer eindeutigen Seriennummer, zumindest für einen begrenzten Zeitraum (z. B. bis zum Objektivwechsel) gleichkommt.

Letztlich genügt im günstigsten Fall ein einziges Bild, das gemeinsamen mit personenbezoge-

[6] (Nicht alle Digitalkameras, die über eine Seriennummer verfügen, codieren das Feld ein.)

[7] Applikationen, wie sie für das weitverbreitete Mobiltelefon *iPhone* verfügbar sind, können die Ortskoordinaten unter Umständen auch ohne Kenntnis des Nutzers verarbeiten. [10]

Tab. 1: Meta-Informationen zur Identifizierung

Merkmal
GSM Cell ID + Datum/Zeit
Seriennummer
Lens ID + weitere Daten
Manuelle nutzerseitige Einstellungen + Kameratyp

nen Daten publiziert wurde (z. B. Mitarbeitergalerie eines Unternehmens oder Arbeitsproben eines (Hobby-)Fotografen), um die Person in allen Zusammenhängen zu deanonymisieren, in denen sie mit derselben Kamera (bzw. demselben Mobiltelefon) die Fotografien erzeugte. Dabei besteht insbesondere bei dienstlich genutzten Kameras oder Fotohandys die Gefahr, dass sich *Whistleblower* (Mitarbeiter, die auf Missstände beim Arbeitgeber aufmerksam machen) unbeabsichtigt selbst identifizieren.

Die inkriminierenden Metadaten können auf einfache Weise auch künstlich in ein Bild eingebracht werden; eine kryptographische Sicherung oder vergleichbare Maßnahmen werden gemäß o. g. Standards[1, 4] nicht angewandt. Es ist daher möglich, dass scheinbare Beziehungen zwischen Profilen sozialer Netzwerke mithilfe verfälschter Metadaten hergestellt und öffentlich gemacht werden – beispielsweise mit dem Ziel, einer Person zu schaden. Zudem kann es auch zu fehlerhaften Zuordnung kommen, wenn entgegen unserer Annahme Kameras oder Fotohandys zwischen Personen getauscht, bzw. an Personen außerhalb des Beziehungsgeflechtes weiterveräußert werden. Eine Interpretation von Metadaten, insbesondere eine forensische Auswertung, muss dieser Möglichkeit daher Rechnung tragen.

4 Nutzung der Metadaten zur Aufdeckung von Beziehungen

In sozialen Netzwerken können die Nutzer Ihr Beziehungsgeflecht offenlegen, z. B. *Freunde* (Facebook, StudiVZ), *Fans* (Facebook), *Kontakte* (XING) oder *Follower* (Twitter) für andere Nutzer oder allgemein für Suchmaschinen ausweisen. Dass auch die Offenlegung dieses Beziehungsgeflechtes bzw. die Information, mit einer ganz bestimmten Person bekannt (oder ein *Fan* von ihr) zu sein, Implikationen in Bezug auf die Privatsphäre hat, ist Gegenstand zahlreicher Hinweise von Datenschützern.

Wir können nun die Auswertung der Meta-Informationen in Bildern heranziehen, um weitere Beziehungen (die möglicherweise bewusst ungenannt bleiben) aufzudecken. Grundidee ist hier, veröffentlichte Bilder von zwei Personen zu finden, die Gemeinsamkeiten in den Meta-Daten aufweisen. Hierbei ist insbesondere die Kombination Cell-ID und Zeitpunkt entscheidend. Gelingt es, Bilder zu finden, die darüber Aufschluss geben, dass zwei (oder mehrere) Personen mehr als einmal zur selben Zeit (ungefähr) am gleichen Ort waren, liegt der Schluss nahe, dass diese gemeinsam gereist sind oder sich für dieselben Ereignisse interessieren und dort zusammengetroffen sind. Wir können mit einer personenbezogenen Suche damit alle Reisegefährten oder persönlich getroffene Personen ermitteln, die ihrerseits Bilder publiziert haben.

Die Autoren konnten anhand von Cell-IDs und Nutzung des Bilderangebots auf *Flickr* mehrere voneinander unabhängige Profile ermitteln, die Bilder enthielten, die in derselben Funkzelle aufgenommen wurden. Die automatisch ermittelte Übereinstimmung kann anschließend durch

Bildervergleich verifiziert werden (sofern Motivübereinstimmungen vorliegen).

Den derzeit marktführenden sozialen Netzwerken ist in Bezug auf das hier beschriebene Problem zugutezuhalten, dass diese hochgeladene Bilddateien bearbeiten (meist verlustbehaftet komprimieren) und dabei die eincodierten Metadaten entfernen, sodass die in diesem Abschnitt beschriebene Vorgehensweise nicht mehr möglich ist. Da jedoch die Möglichkeit, Bilddateien aus Bilddatenbanken bzw. Foto-Dienstleistungsportalen wie *Flickr* in die Profile der sozialen Netzwerke zu verlinken, besteht,[8] und die Bilder in diesen Bilddatenbanken unverändert abgelegt werden, wird diese (vermutlich ohnehin nicht beabsichtigte) Schutzfunktion ausgehebelt. Im folgenden Kapitel 5 werden wir zudem eine weitere Strategie vorstellen, die eine Zuordnung von Bildern auch bei entfernten Metadaten ermöglicht.

5 Ermittlung des spezifischen Rauschmusters

Eine weitere Methode der Zuordnung von Bildern zu einer Kamera und damit mittelbar zur Deanonymisierung von Profilen sozialer Netzwerke anhand von Bildern stellt die Ermittlung von Rauschmustern dar. Der Bildaufnahmeprozess bei digitalen Kameras wird durch Rauschen in den beteiligten Bauteilen gestört. Insbesondere das spatiale Rauschen, das in ähnlicher Form auf verschiedenen Bildern einer Kamera auftritt, sich jedoch von Kamera zu Kamera eindeutig unterscheidet, ist geeignet, ein charakteristisches *Rauschmuster*[9] einer Kamera zu erzeugen, das es ermöglicht, eine Kamera anhand der Bildinformation von anderen Kameras (auch baugleichen) zu unterscheiden. Als Ursache für dieses spezifische Rauschen, das eine wesentliche Rolle in der digitalen Bildforensik spielt und anstelle der Seriennummer einer Kamera zur Deanonymisierung verwendet werden kann, werden Varianzen bei der Fertigung und mikroskopische Materialfehler identifiziert; es sind derzeit keine Digitalkameramodelle bekannt, die kein charakteristisches Rauschmuster bei unbearbeiteten Aufnahmen aufweisen. [3, 9] Über das spatiale Rauschen hinaus bieten auch Kratzer und langfristig vorhandene Schmutzpartikel Merkmale, die eine spezifische Zuordnung zu einer Kamera ermöglichen; diese sind jedoch von geringerer Bedeutung als das spatiale Rauschen. [7]

Um das Rauschmuster einer Kamera zu gewinnen, werden mehrere Bilder, die von derselben Digitalkamera aufgenommen wurden, benötigt. Das errechnete Muster nimmt mit steigender Anzahl von Bildern an Genauigkeit zu und kann anschließend dazu verwendet werden, ein weiteres, einzelnes Bild einer Kamera zuzuordnen, wobei die Wahrscheinlichkeiten einer falschen Zuordnung zur Kamera (*false acceptance rate, FAR*) und einer gescheiterten Zuordnung eines tatsächlich mit der Kamera erzeugten Bildes (*false rejection rate, FRR*) jeweils minimiert werden sollen (und dabei gegenseitig einem Trade-Off unterliegen).

Die Anzahl benötigter Bilder hängt von einer Vielzahl von Umständen ab; besondere Aufmerksamkeit ist hierbei auf die Bildsättigung, die Texturen und die Signalabflachung (*signal flattening*) zu legen. Bei der Bildsättigung ist zu beachten, dass das Rauschmuster des Sensors sich gegenüber der Helligkeit multiplikativ verhält und deshalb in dunklen Regionen nur schwach nachweisbar ist, in überbelichteten Regionen tritt jedoch aus technischen Gründen kein Rauschen auf. In texturierten Bereichen wird durch den *wavelet denoise filter* das Rauschen stärker herausgefiltert, weshalb auch hier die Nützlichkeit des Rauschmusters vermindert wird.

[8] Den Usern von Facebook wird beispielsweise eine Applikation angeboten, ihre geposteten Flickr-Bilder automatisch in die persönliche Facebook-Pinnwand zu integrieren.

[9] Wir beziehen uns hier auf den Begriff des *photo-response non-uniformity noise (PRNU)*, der in der Bildforensik Verwendung findet.

Die Signalabflachung kann zu hohen falschen Korrelationen führen, wenn Bilder aus verschiedenen Kameraquellen mit dieser Eigenschaft untereinander verglichen werden.

Eine gezielte Auswertung der vorgenannten Faktoren ermöglicht eine algorithmische Vorhersage, die zur Korrektur der berechneten Korrelationswerte herangezogen werden kann und die zur Verbesserung der Zuordenbarkeit von Aufnahmen zu einer Kamera führt. Hierbei wird eine Matrixgleichung aus den Eigenschaften der Bildsättigung (*image intensity*), Texturen, Signalabflachung und dem Produkt aus Bildsättigung und Texturanteil erzeugt.[10]

Bei der diesem Beitrag zugrunde liegenden Arbeit [8] wurde bereits mit Rauschmustern aus 20–50 Bildern im Querformat, bei einer Auflösung von 600px Breite anwendbare (d. h. zur Deanomymisierung geeignete) Resultate erzeugt. Der Rauschabdruck wurde dabei über das von Fridrich et al. [3, 9] beschriebene Verfahren erzeugt. Dabei wird erst ein Rauschmuster einer Kamera erzeugt, wofür Bilder benötigt werden, die unzweifelhaft einer Kamera zugeordnet werden können. Diese werden zunächst mit einem *wavelet denoise filter* entrauscht und anschließend vom Original subtrahiert, um das Rauschen des Bildes zu ermitteln. Über eine Mittelwertbildung wird das grundlegende spatiale Rauschmuster des Kamerasensors errechnet, das unabhängig von den Rauscheigenschaften eines einzelnen Bildes existiert. Die Qualität des Rauschabdrucks wird gesteigert, wenn möglichst viele Bilder ausgewertet werden, die zwar hell aber nicht übersättigt sind und zudem wenige Texturen enthalten.

Bei der anschließenden Zuordnung eines Bildes aus unbekannter Quelle zu einem vorhandenem Rauschmuster sind wieder die Kriterien Bildsättigung, Texturen und Signalabflachung zu berücksichtigen. Die Abb. 1 zeigt beispielhaft links ein Bild, das gut geeignet ist, um einem Muster (d. h. einer Kamera) zugeordnet zu werden, rechts ist ein Bild, das aufgrund der genannten Kriterien mit (vergleichsweise) hoher Wahrscheinlichkeit einer falschen Kamera zugeordnet werden könnte.

Abb. 1: Bild mit guten (links) und schlechten (rechts) Zuordnungseigenschaften

Eine Erschwernis bei der Deanonymisierung von Profilen sozialer Netzwerke anhand von Bilddateien ist darin begründet, dass die Bilder vor der Veröffentlichung automatisch (vom System der Plattform) oder manuell (vom Bildautor mithilfe von Bildbearbeitungsprogrammen) in ihren Pixelausmaßen stark verkleinert werden; eine Verkleinerung auf 20% der Ausmaße pro Dimension, d. h. auf 4% der Pixelanzahl insgesamt, stellt angesichts der hohen Auflösungen moderner Digitalkameras keine Seltenheit dar.

[10] Dadurch ist es nach Fridrich et al. [6] auch möglich, falsche Einbettungen von Rauschmustern, d. h. Bildfälschungen, die mit der Absicht erzeugt werden, eine Kamera fälschlicherweise einem Bild zuzuordnen, zu erkennen.

Tab. 2: Verkleinerte Bilder: Kameraidentifizierung über Rauschen

Kamera	Schwellwert	FRR	Schwellwert	FRR	Schwellwert	FRR
	FAR = 1e-1		FAR = 2e-1		FAR = 3e-1	
K800i-1	0,0117	2,36E-01	0,0081	7,44E-02	0,0059	3,88E-02
K800i-2	0,0324	6,52E-01	0,0170	4,98E-01	0,0113	3,79E-01
EOS1000d	0,0221	9,14E-01	0,0154	7,21E-01	0,0110	5,00E-01
EOS450d	0,0255	7,20E-01	0,0113	4,51E-01	0,0065	3,21E-01
Trust770z	0,0394	9,06E-01	0,0207	6,71E-01	0,0134	4,82E-01

Eine Zuordnung eines verkleinerten Bildes zu einem anhand von Bildern in Originalgröße gewonnenem Rauschmuster ist jedoch – nach Anpassung der o. g. Verfahren – generell möglich. Wir geben empirisch gewonnene Ergebnisse in der Tabelle 2 wieder. Für diese Tabelle wurde der Anteil der falschen Zuordnungen (FAR) auf 0,1 (erste Spalte) begrenzt, um anschließend den zur Kamera gehörigen Schwellwert (gemessene Korrelation) und den FRR-Wert zu berechnen. Die weiteren Spalten zeigen alternative FAR-Werte. Die Bilder wurden mit dem Werkzeug *Imagekick-Convert*[11] auf die Größe 600x448 (bei den Canon-EOS-Modellen auf 600x400) reduziert. Die in der Tabelle 2 aufgeführten Daten geben zur Vermutung Anlass, dass durch die Kombination von mehreren Bildern aus unbekannter Quelle, von denen man jedoch annimmt, dass sie von derselben Kamera erzeugt werden, ein vorliegendes Rauschmuster identifizieren zu können. Dies wird anhand empirischer Daten bestätigt; einschränkend ist jedoch zu bemerken, dass hier nicht von einer statistischen Unabhängigkeit ausgegangen werden kann, vielmehr kommt es darauf an, möglichst viele Bilder mit positiven Eigenschaften bzgl. der Kriterien Bildsättigung, Texturen und Signalabflachung zu verwerten. Gelingt dies, ist auch eine Zuordnung zu Kameras mit enttäuschenden FRR-Werten (im Einzelfall wurden hier – wie in der Tabelle zu ersehen – Werte von über 90% ermittelt), möglich.

6 Fazit

Verräterische Datenspuren können die anonyme Nutzung von sozialen Netzwerken konterkarieren. Dafür gibt es zahlreiche Beispiele: Browser-Cookies, Javascriptangriffe auf die Browser-History, Timing Attacks (u. a.). Die Verwendung von Meta-Informationen in Bildern und die Auswertung von Rauschmustern bei Digitalkameras fügen dieser Problematik einen weiteren Baustein hinzu. Die anonyme Teilnahme an sozialen Netzwerken ist möglich, es sind jedoch umfangreiche Schutzmaßnahmen bzw. technische Kenntnisse erforderlich, um zuverlässig alle Datenspuren zu verwischen, bevor diese Teil publizierter Informationen werden.

References

[1] Core 1.1/Extension 1.1. *IPTC Standard Photo Metadata, July 2009*. International Press Telecommunications Council, 2009.

[2] ARD. *Verräterische Datenmengen*. Sendung Marktcheck, SWR Fernsehen vom 18.03.2010, 21.00 Uhr; Text unter http://www.swr.de/marktcheck/multimedia/handyfotos-exif-daten, 2010.

[11] http://www.imagemagick.org/script/index.php

[3] Mo Chen, Jessica Fridrich, and Miroslav Goljan. Digital imaging sensor identification (further study). *Proc. SPIE, Vol. 6505, 65050P (2007) San Jose, USA.*

[4] JEITA CP-3451. *Exchangeable image file format for digital still cameras: Exif Version 2.2*. Japan Electronics and Information Technology Industries Association, 2002.

[5] Oshani Seneviratne et al. Detecting Creative Commons License Violations on Images on the World Wide Web. *WWW2009, April 2024, 2009, Madrid, Spain.*

[6] Frdrich, Goljan, and Chen. Sensor Noise Camera Identification: Countering Counter-Forensics. *Proc. SPIE, Electronic Imaging, Media Forensics and Security XII, San Jose, CA, 2010.*

[7] Thomas Gloe. Digitale Bildforensik. *Arbeitstagung – Neue Erkenntnisse und Technologien in der digitalen Foto- und Videografie Hessische Polizeischule, Wiesbaden, 06.11.2007 (Vortragsfolien).*

[8] Dennis Löhr. *Deanonymisierung anhand von Bilddaten (Arbeitstitel, Masterarbeit)*. Fachhochschule Münster, Labor für IT-Sicherheit, 2010.

[9] Jan Lukas, Jessica Fridrich, and Miroslav Goljan. Digital Camera Identification from Sensor Pattern Noise. *Proceedings of the SPIE, 2006, San Jose, USA.*

[10] Nicolas Seriot. iPhone Privacy. *Black Hat DC 2010*, 2010.