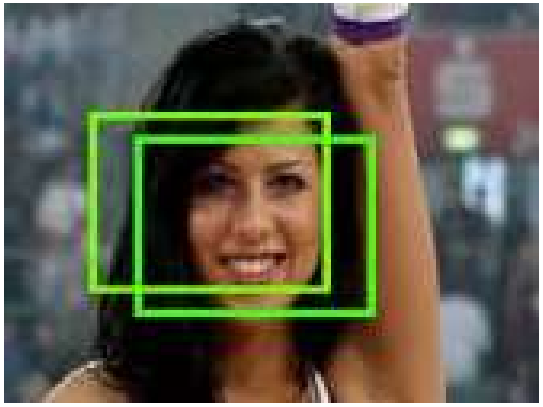
FaceHash

– Robustheit gegen Beschneiden durch hashen von Gesichtern

http://www.cheerleader-frankfurt.de/galacticdancers

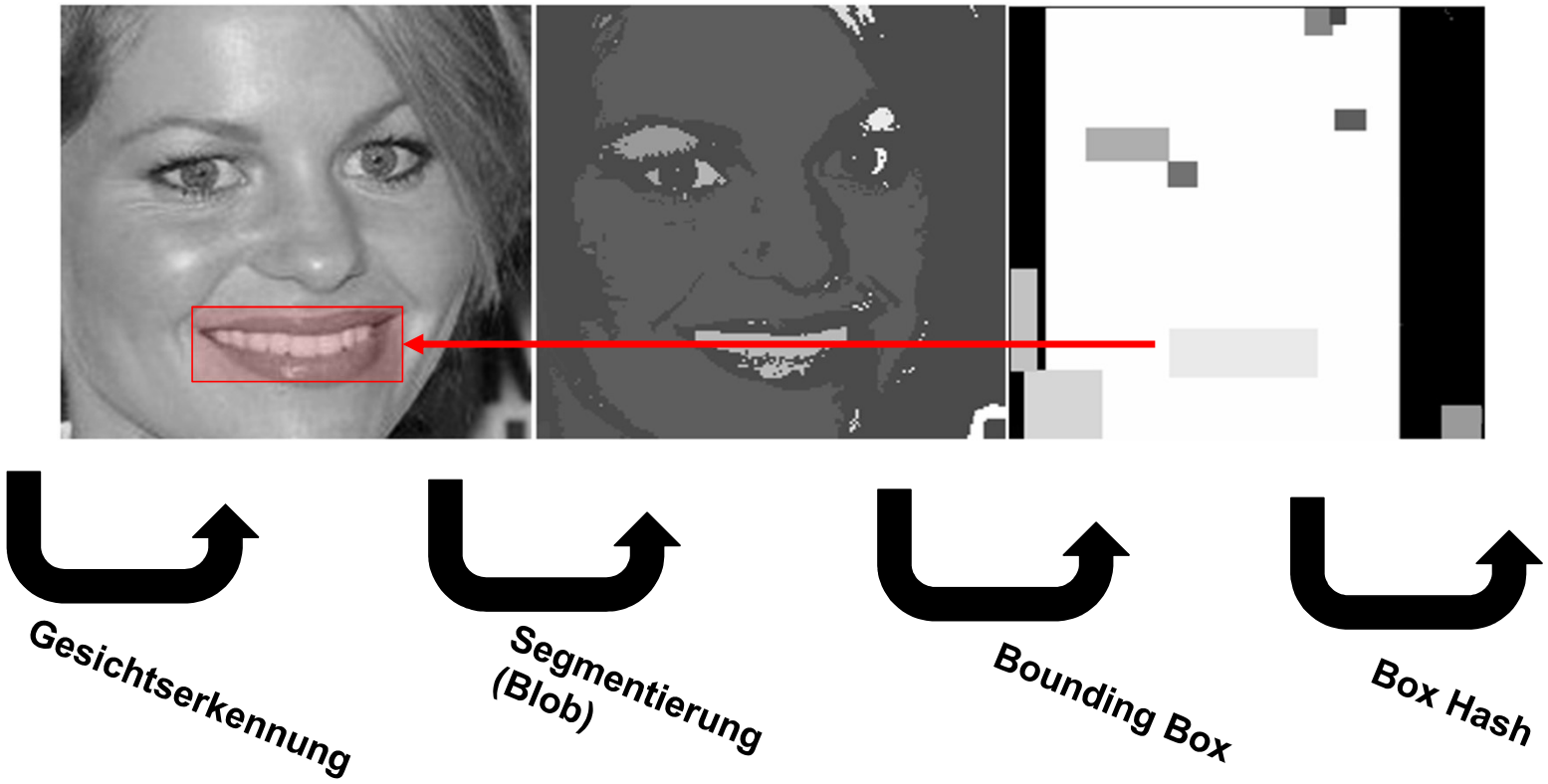
FaceHash

– Problem: Gesichtsbereich wird nicht immer an der gleichen Stelle erkannt



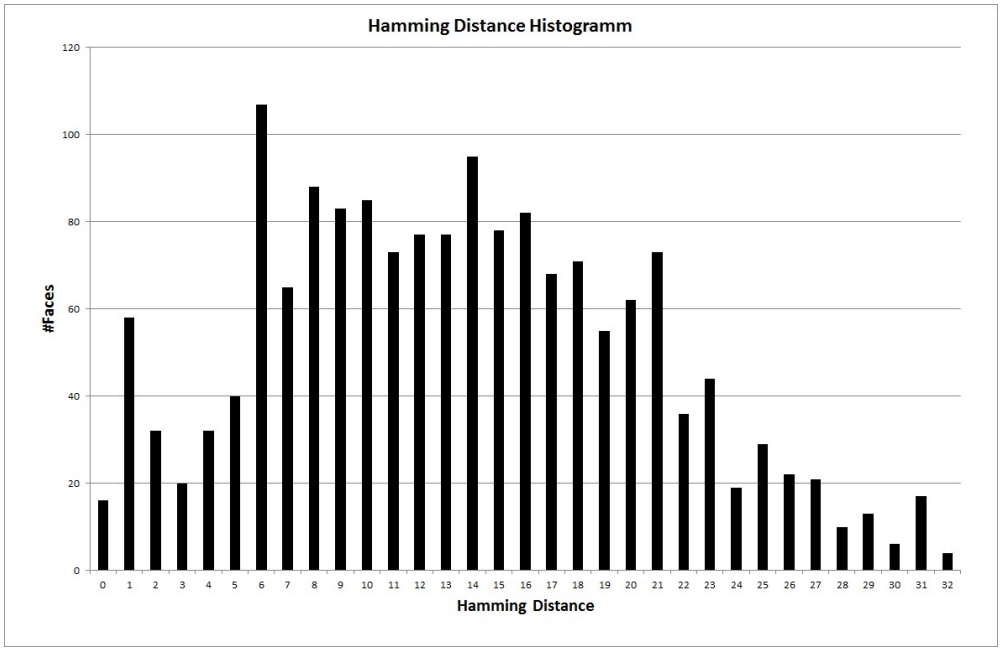
http://www.cheerleader-frankfurt.de/galacticdancers

– Lösung: Komination mit Blob-Berechnung



Ergebniss: Hohe Robustheit gegen Cropping

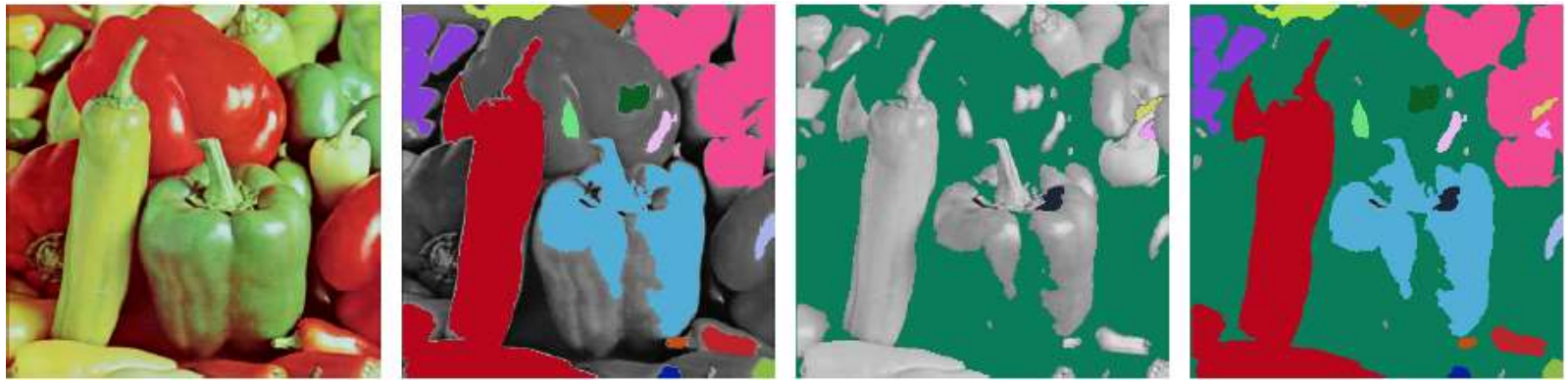
(http://models.com/newfaces/dailyduo/3624)



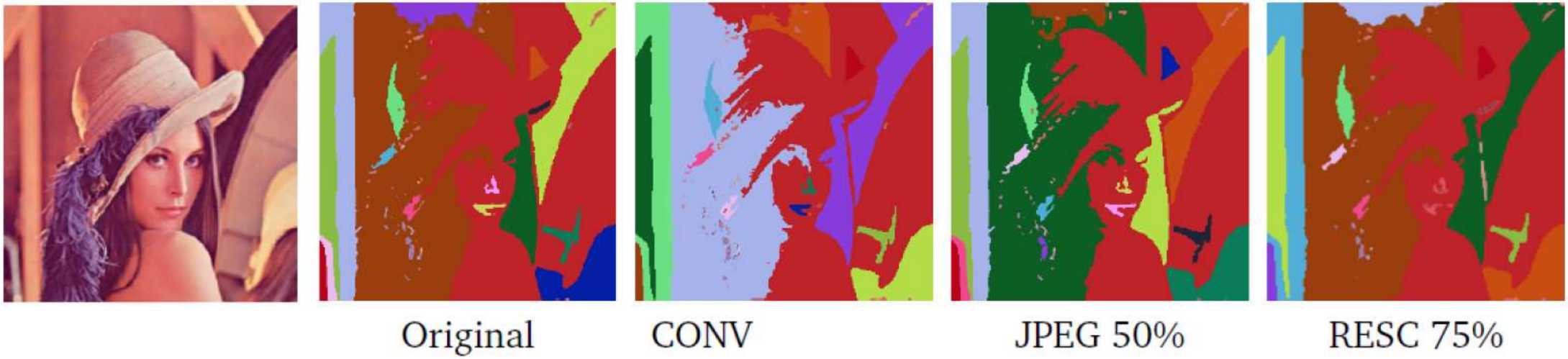
Steinebach, Martin, Huajian Liu, and York Yannikos. "FaceHash: face detection and robust hashing." *International Conference on Digital Forensics and Cyber Crime*. Springer, Cham, 2013.

SegmentHash

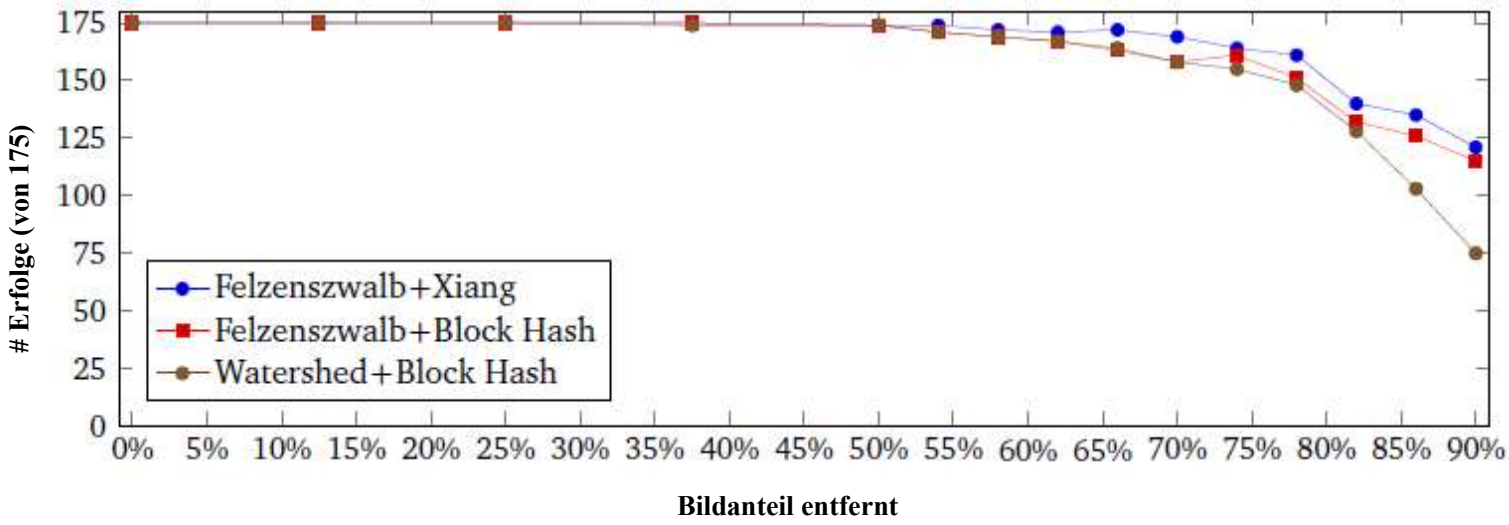
- Robustheit gegen Ausschneiden von Bildteilen durch Hashen von Bildsegmenten
  - Watershed Segmentierung
    - Original, “Berge”, “Täler”, Kombination



– Beispiel Segmentierung Lena



– Hohe Robustheit auch gegen starke Angriffe



Steinebach, Martin, Huajian Liu, and York Yannikos. "Efficient cropping-resistant robust image hashing." *2014 Ninth International Conference on Availability, Reliability and Security*. IEEE, 2014.

Motivation

- **Problem: Fake News**
- **Montagen lassen Fake News überzeugender wirken**
- **Zweck: Diffamierung, Propaganda**
- **Wie können Montagen schnell, robust und korrekt erkannt werden?**

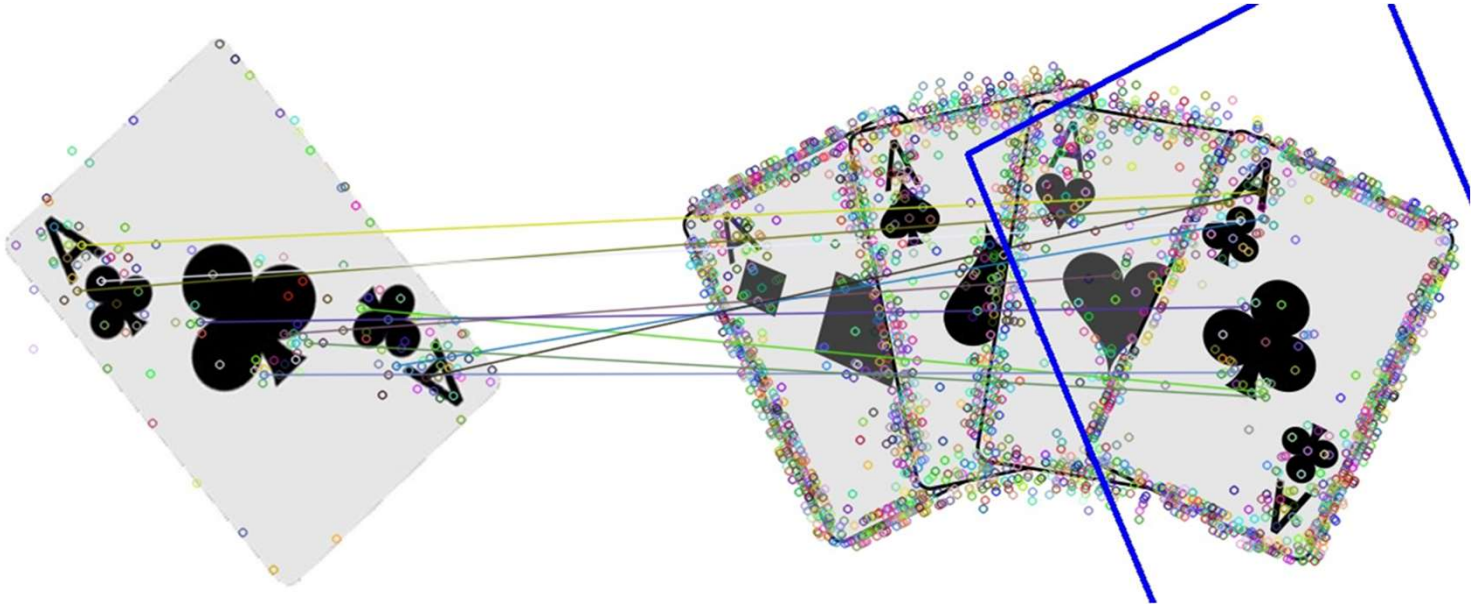
- **Beispiel mit bekannten Quellen**

(a) Montage: newpoliticstoday.com

(b) Source 1: picture-alliance / AP Photo

(c) Source 2: Boston Globe / Getty Images

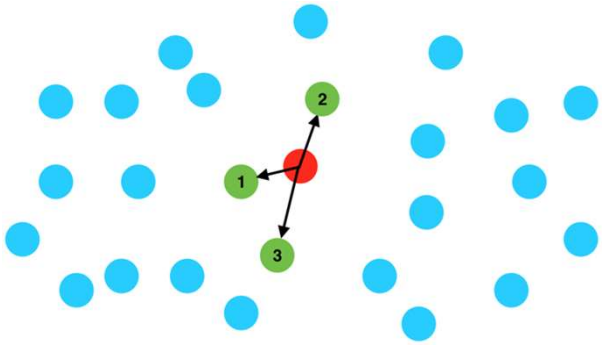
Stand der Technik – Feature Detektion



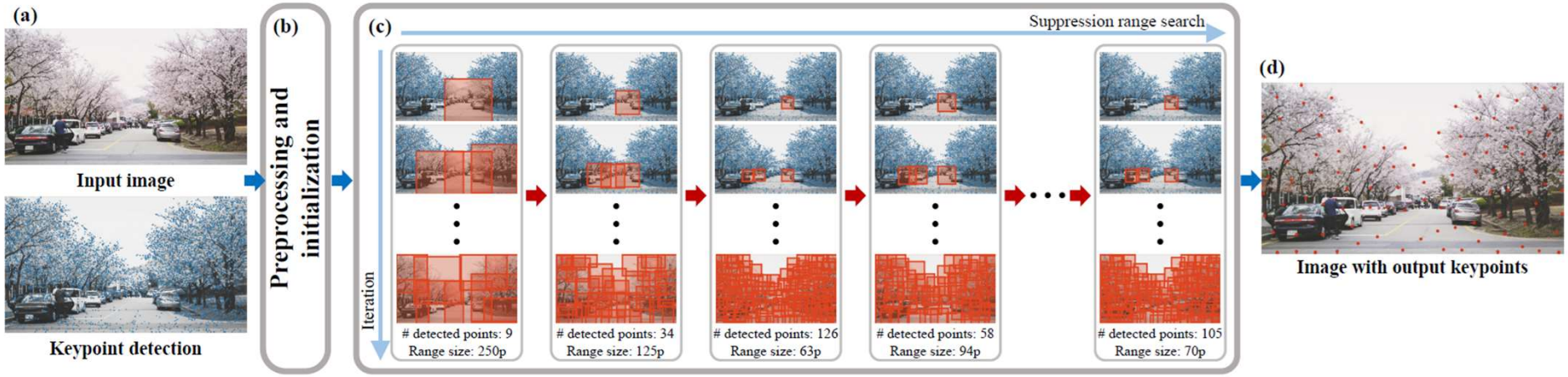
- Finden von interessanten Bildteilen (Keypoints)
- Extrahieren der lokalen Umgebung von Keypoints (Deskriptoren)
- Vergleichen der Deskriptoren von verschiedenen Bildern (Matching)
- Feature Detektoren: Sift, Surf, Orb, Akaze und etc.

Stand der Technik – Nächste Nachbar Suche

- Ermöglicht schnelle Suche nach ähnlichen Punkten
- Punkte werden einmalig indexiert z.B. als Baumstruktur
- Suche mit unbekannten Punkt gibt die K nächsten Nachbarn zurück
- Algorithmen: Flann, Annoy, KD-Tree und etc.



- Feature Detektoren finden zu viele Features in Bildern
- Können mit mit TopN gefiltert werden
  Problem: Es entstehen Regionen ohne Features
- ANMS behält starke Features, aber garantiert eine homogene Verteilung

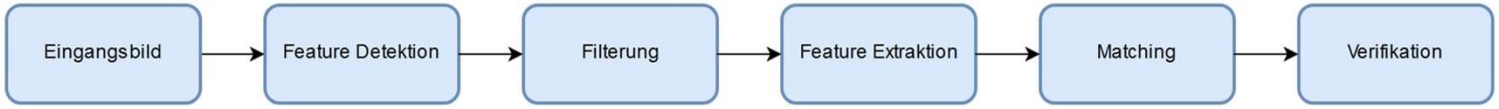


Konzept

- Feature Detektion: Keypoints eines Bildes werden bestimmt
- Filterung: Keypoints werden gefiltert
- Feature Extraktion: Deskriptoren der Keypoints werden bestimmt
- Indexierung: Deskriptoren werden Indexiert
- Matching: Deskriptoren von mehreren Bildern werden verglichen
- Verifikation: Struktur der Matches wird verglichen

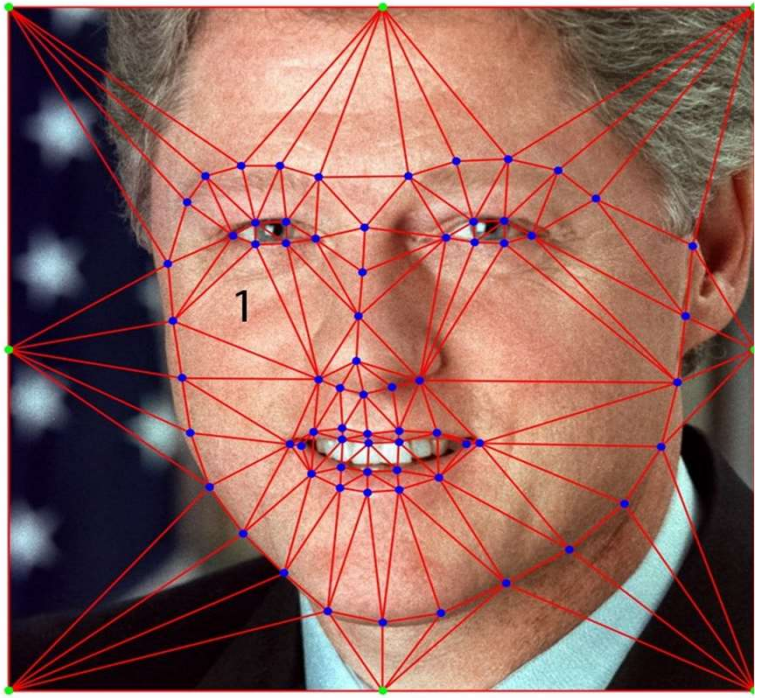
→Initialisierung:

→Abfrage:



Konzept – Mesh Verifier

- Gegeben sind die Matches von zwei Bildern als zwei Listen
- Es werden aus den ersten drei Matches beider Listen zwei Dreiecke gebildet
- Vorgang wird für alle Matches wiederholt
- Zwei Dreiecke sind ähnlich, wenn ihre Innenwinkel ähnlich sind
- Zwei Netze sind ähnlich, wenn genügend Dreiecke ähnlich sind

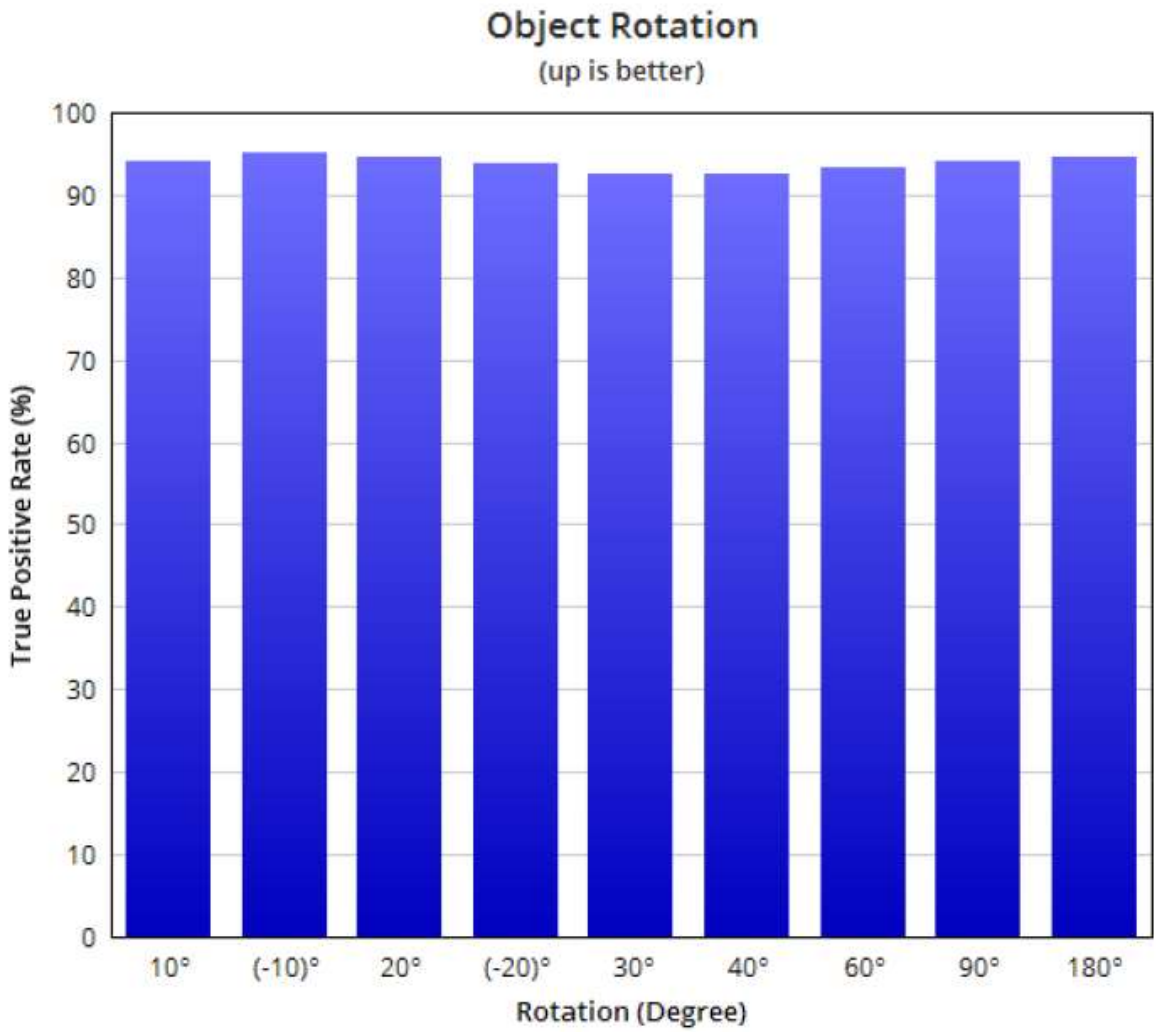


(Symbolbild)

Robustheit gegen Rotation ist sehr hoch

Steinebach, Martin, Karol Gotkowski, and Hujian Liu. "Fake News Detection by Image Montage Recognition." *Proceedings of the 14th International Conference on Availability, Reliability and Security*. 2019.

Open Access:
https://journals.riverpublishers.com/index.php/JCSANDM/article/view/1131



Medienforensik

- Manipulationserkennung
- Ballistik
- File Carving

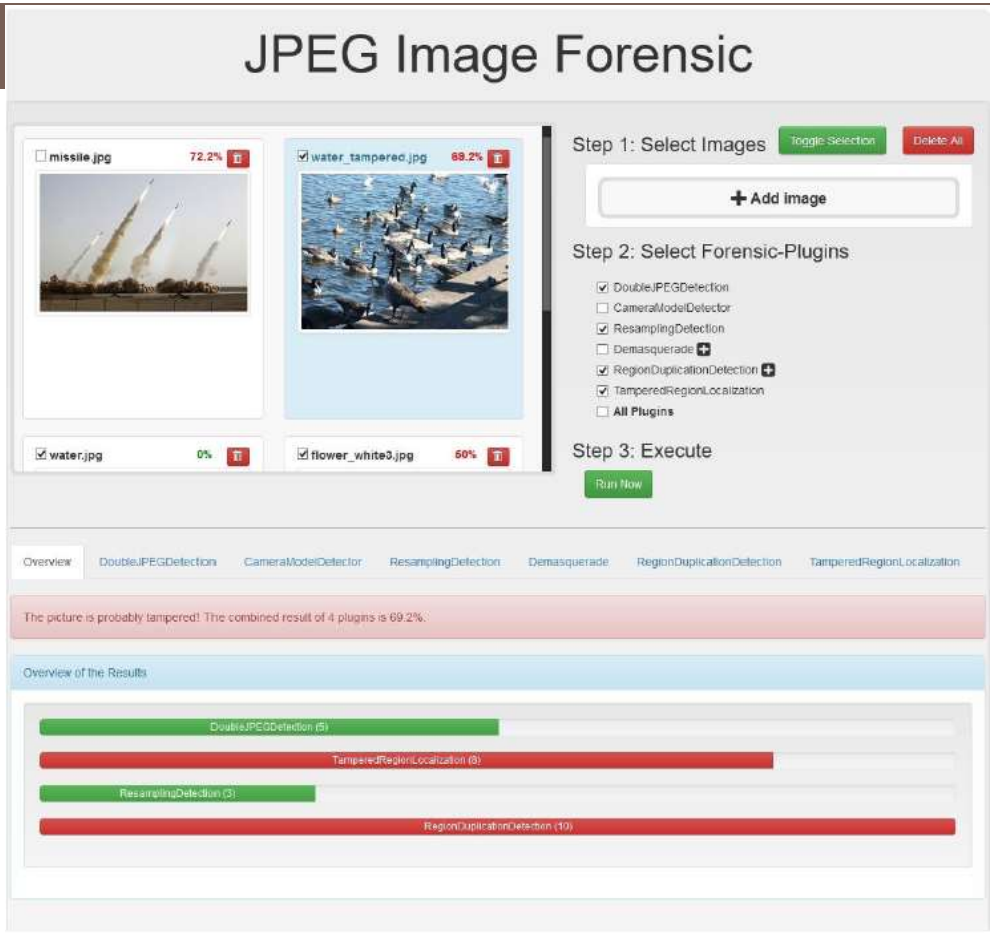
- Forensische Anwendungen im Bildbereich sind mehrfach belegt
  - Optimierung von Bildern, die z.B. mit Überwachungskameras aufgenommen wurden
    - Rauschen entfernen

  - Erkennen von Manipulationen in Bildern
    - „Passive-blind image forensics“
  - Zurückverfolgen von Quellen
    - Geräte
    - Unterscheidung zwischen Foto und fotorealistisch gerenderte Bildern

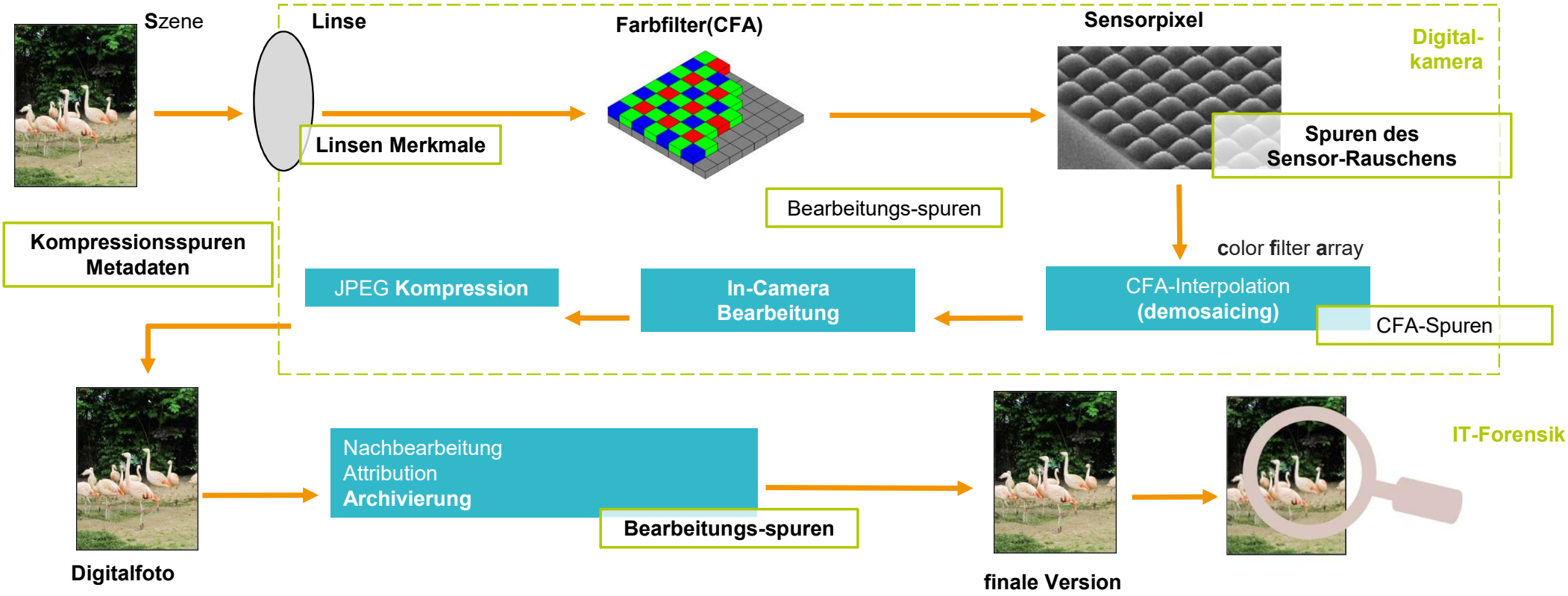
http://www.csse.uwa.edu.au/~pk/Forensic/index.html

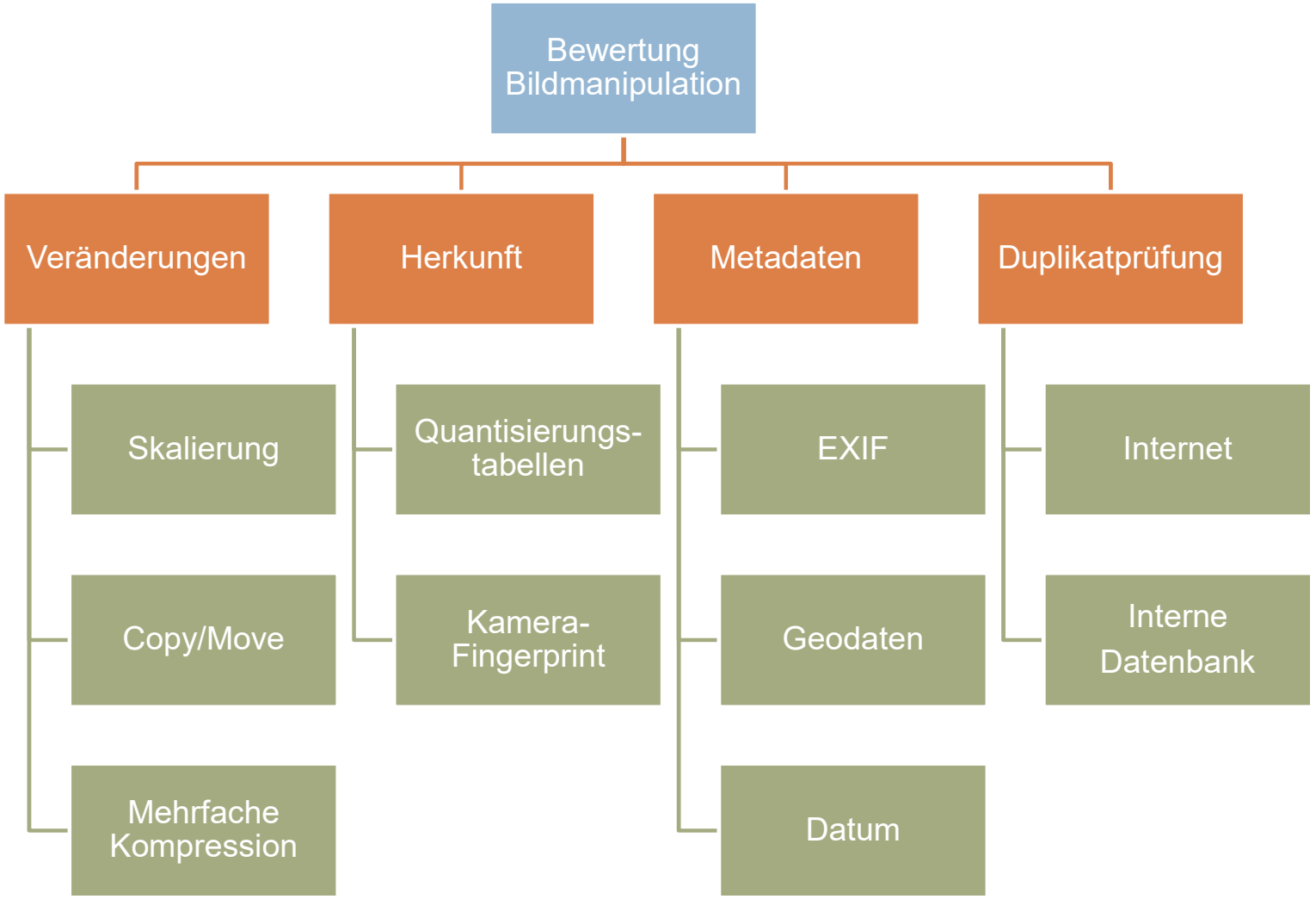
Image Forensics: Erkennen von Manipulationen

- Methoden zum Erkennen von Manipulationen von Bildern
  - Kein Original liegt vor
  - Kein Hash des Originals ist bekannt
  - Keine Methode zum Schutz der Integrität im Voraus eingesetzt
- Vorgehensweise
  - Modell eines nicht verändertes Bildes finden
  - Abweichungen vom Modell errechnen
- Beispiele für Methoden
  - Erkennen von identischen Stellen im Bild
  - Erkennen von statistischen Abweichungen
- Erfolg der Methoden sind abhängig vom Angriffstyp



Lebenszyklus eines digitalen Bilds




Bewertung Bildmanipulation
Veränderungen
Herkunft
Metadaten
Duplikatprüfung
Skalierung
Copy/Move
Mehrfache Kompression
Quantisierungs-tabellen
Kamera-Fingerprint
EXIF
Geodaten
Datum
Internet
Interne Datenbank

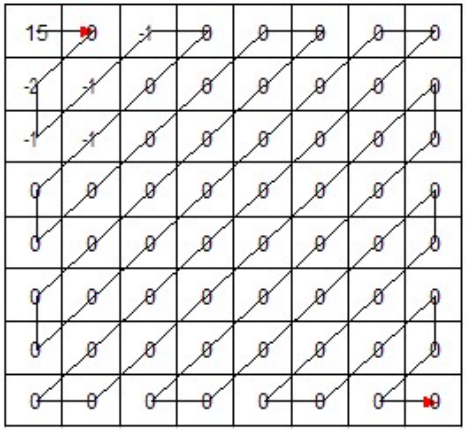
JPEG Tables

- Für JPEG können verschiedene Quantisierungstabellen verwendet werden
  - Optimiert z.B. vom Hersteller von Kameras
- Forensische Fragestellung:
  - Passt Kompression bzw. Tabelle zum Gerät?

- JPEG Quantisierungstabelle
  - Oft individuelle Tabelle von unterschiedlichen Aufnahmegeräten und Bildbearbeitungssoftware
  - Erlaubt
    - Aufnahmegerättyp zu identifizieren
    - Bearbeitungssoftware zu identifizieren, z.B. Photoshop

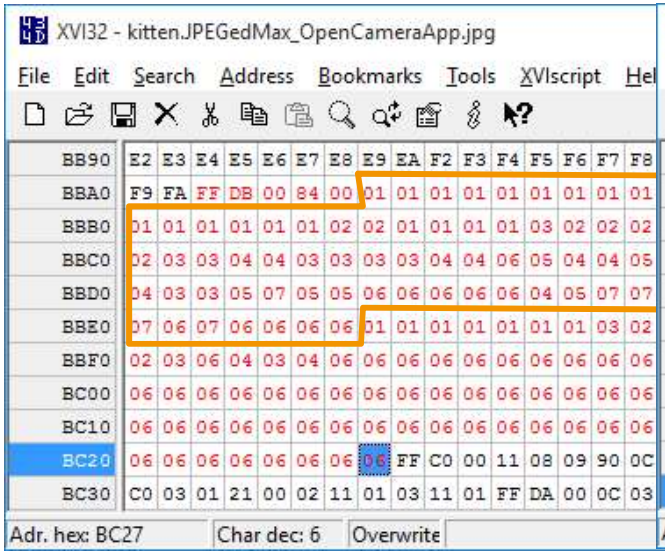
- Limit
  - Begrenzte Verlässlichkeit
  - Einfach mit bekannten Tabelle zu verfälschen

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

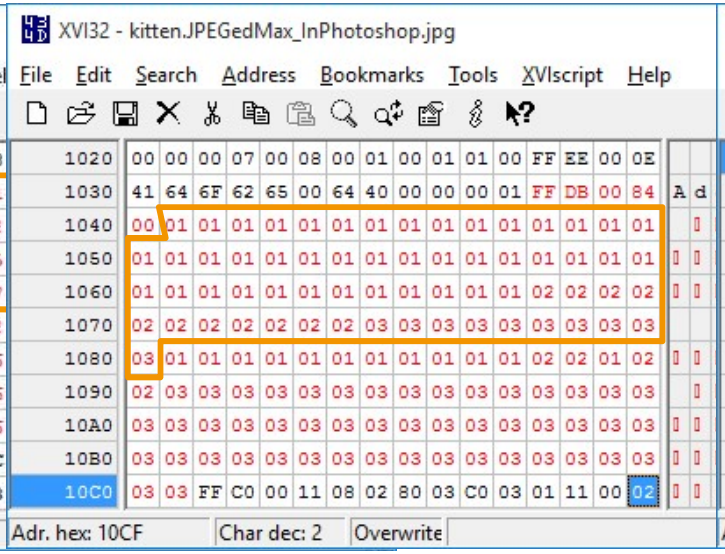


- JPG-Metadaten: Quantisierungstabellen abhängig von der Firmware / Software
- Beispiel: „maximale Bildqualität“

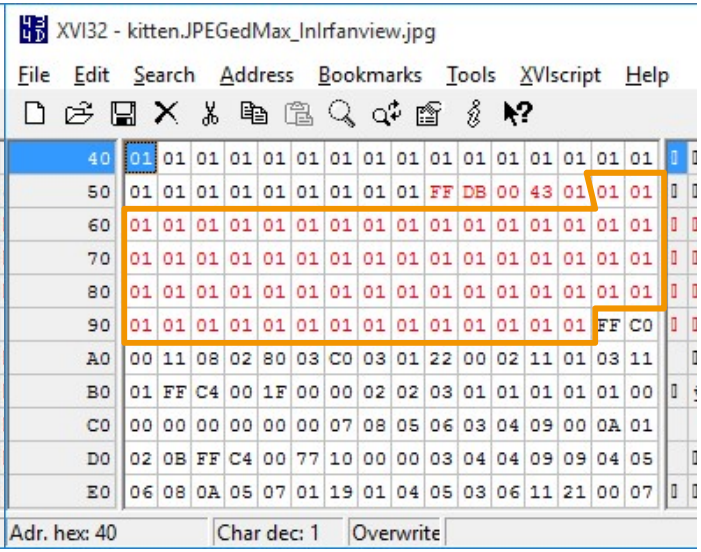
OPEN CAMERA („100%“)



PHOTOSHOP 6.0 (Quality „12“)



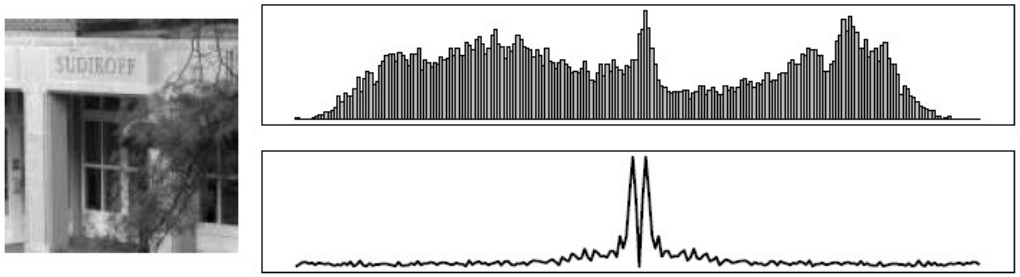
IRFAN VIEW („100%“)



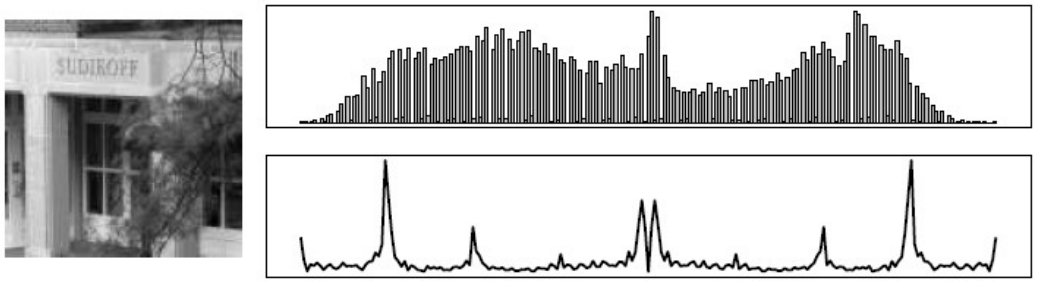
Double Compression

- Erkennen von Mehrfachkompression
  - Rekompression ist ein unvermeidliche Schritt nach Bildmanipulation.
- Forensik Technik
  - Statistische Spuren von Codierung

Histogramm der DCT Koeffizienten nach einmal JPEG 85%



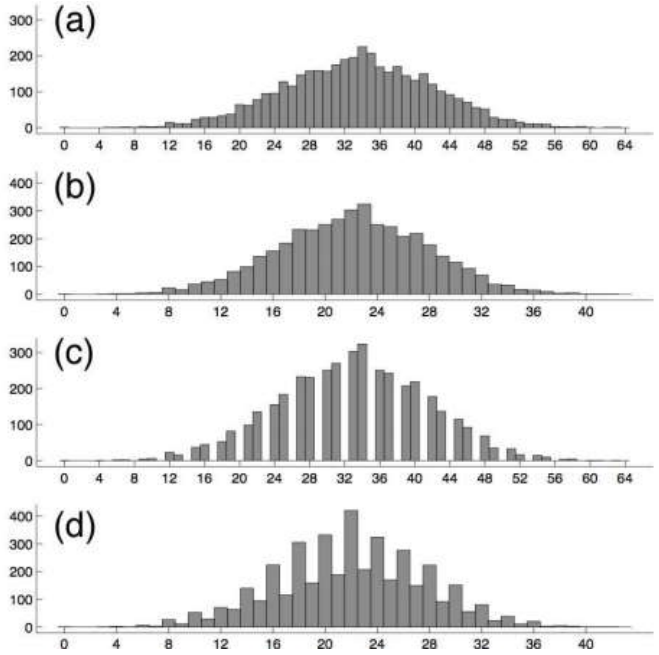
Histogramm der DCT Koeffizienten nach **zwei**mal JPEG, 75% und 85%



Double Compression

- Spuren von mehreren Kompressionen können gefunden werden
  - Histogramm der Koeffizienten
  - Zeigt Anzahl von diskreten Zuständen

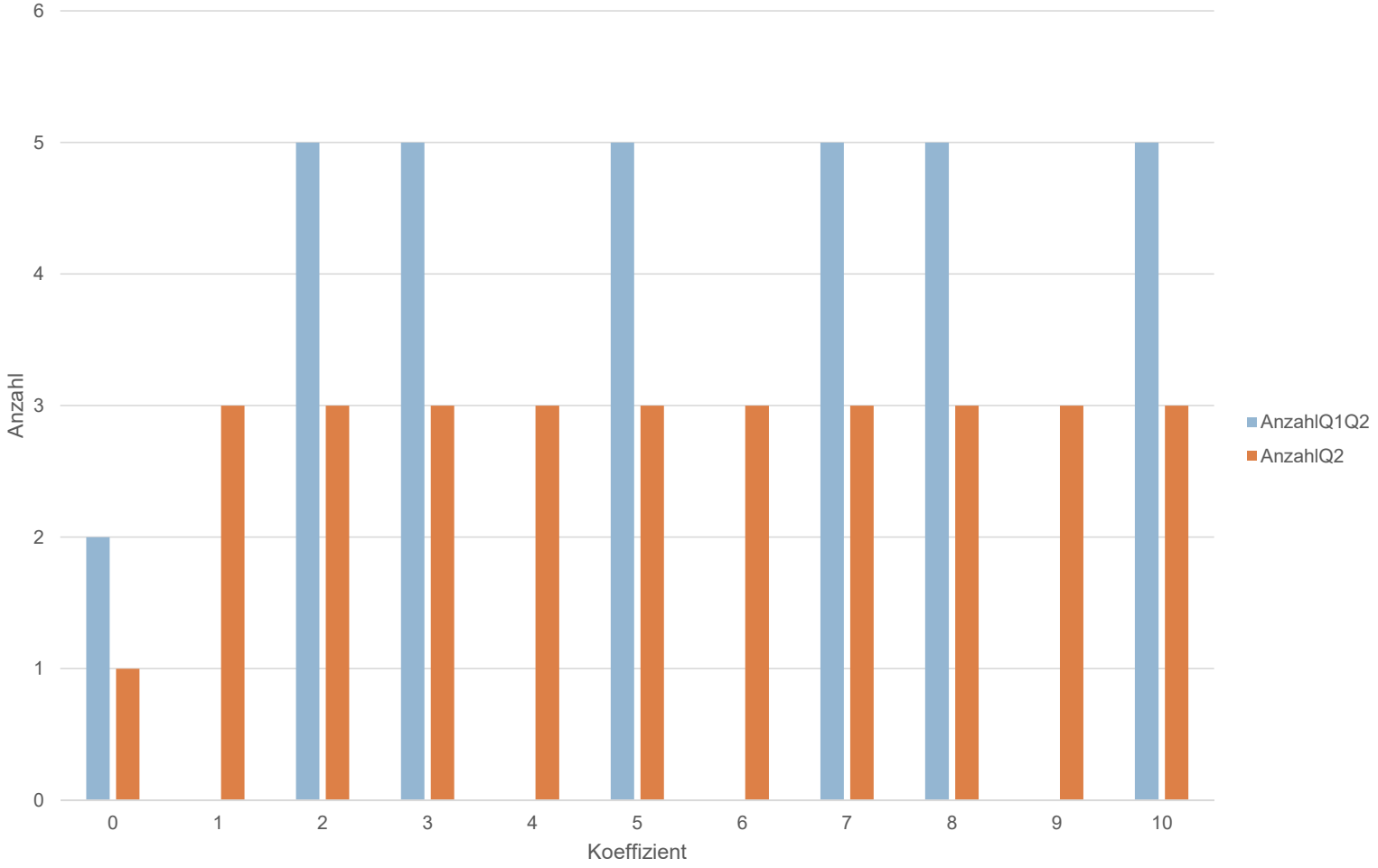
  - A: Feine Kompression (2)
  - B: Grobe Kompression (3)
  - C: Erst grob, dann fein (3,2)
  - D: Erst fein, dann grob (2,3)



http://www.cs.dartmouth.edu/farid/downloads/tutorials/digitalimageforensics.pdf

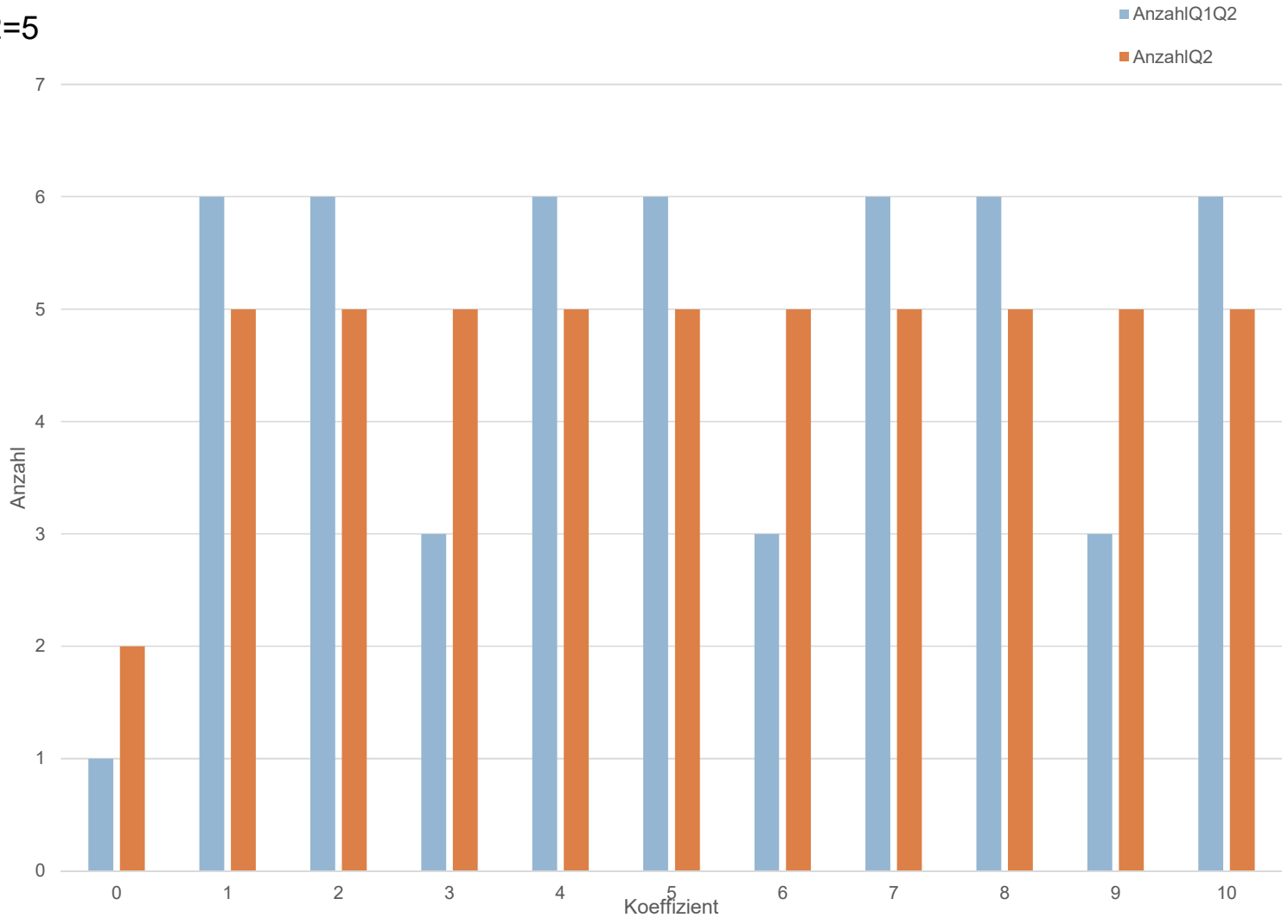
Double Compression

- Quantisierung 1=5, Quantisierung 2=3
- Q1Q2=Double Compression
- Q2=Nur 2. Quantisierung



Double Compression

- Quantisierung 1=3, Quantisierung 2=5
- Q1Q2=Double Compression
- Q2=Nur 2. Quantisierung



Double Compression

- Problem
  - 20 megapixel Kamera
  - 3 megapixel Email Anhang
  - Spuren
    - Gehen verloren
    - Sind irreführend

Erkennen von Duplikaten

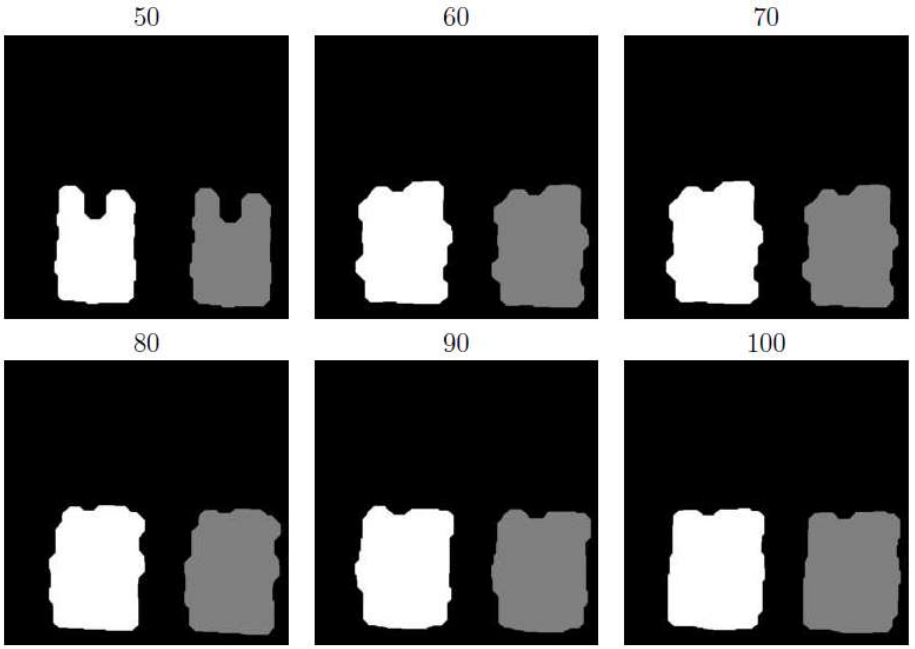
- Hintergrund:
  - Kopieren einiger Bildbereiche an eine andere Stelle ist eine übliche Form der Bildretusche.
    - Entfernen von Objekt
    - Verdecken von Objekt
  - Unauffällig bei geschickter Anwendung
  - Erkennbar durch forensische Analyse
- Erkennen duplizierter Bildbereiche.
  - Copy-Move innerhalb eines Bilds
  - Geometrische Anpassung
  - Beleuchtung Anpassung

Erkennen von Duplikat

- Copy-Move
  - ohne/mit Skalierung
  - ohne/mit Rotation
  - ohne/mit Spiegelung
- Block Matching
  - DCT Koeffizienten
  - Block Merkmale
  - PCA (Principal Component Analysis)
  - FMT (Fourier-Mellin Transform)
  - LPFT (Log-Polar Fourier Transform)

Erkennen von Duplikat

- Block Matching mit PCA
- Nach verschiedenen Stufen der JPEG-Kompression



http://www.cs.dartmouth.edu/farid/downloads/tutorials/digitalimageforensics.pdf

Erkennen von Duplikat

- Image Feature Matching
  - Local features
    - SIFT (Scale Invariant Feature Transform)
    - SURF (Speeded Up Robust Features)
  - Geometrische Invarianz
  - Matching mit Spiegelung

Erkennen von Duplikate

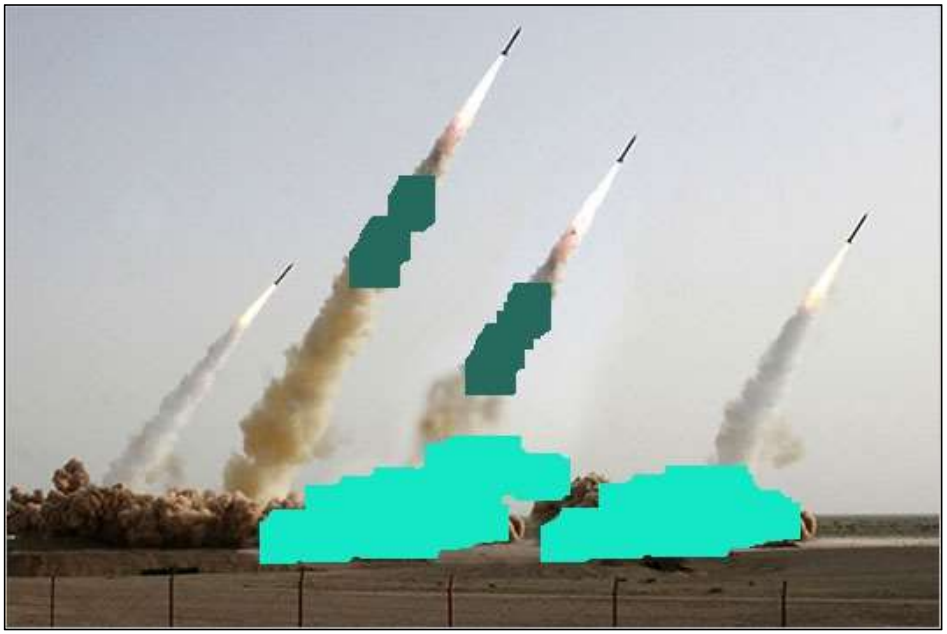


Image Forensics: Änderungserkennung

- Automatisches Erkennen von Veränderungen
  - Vergrößern
  - Verkleinern
  - Rotieren

- Forensik
  - Beispiel: Erkennung von Vergrößerungen
  - Werden Bilder vergrößert, so geschieht dies durch eine Interpolation von Originalpixeln

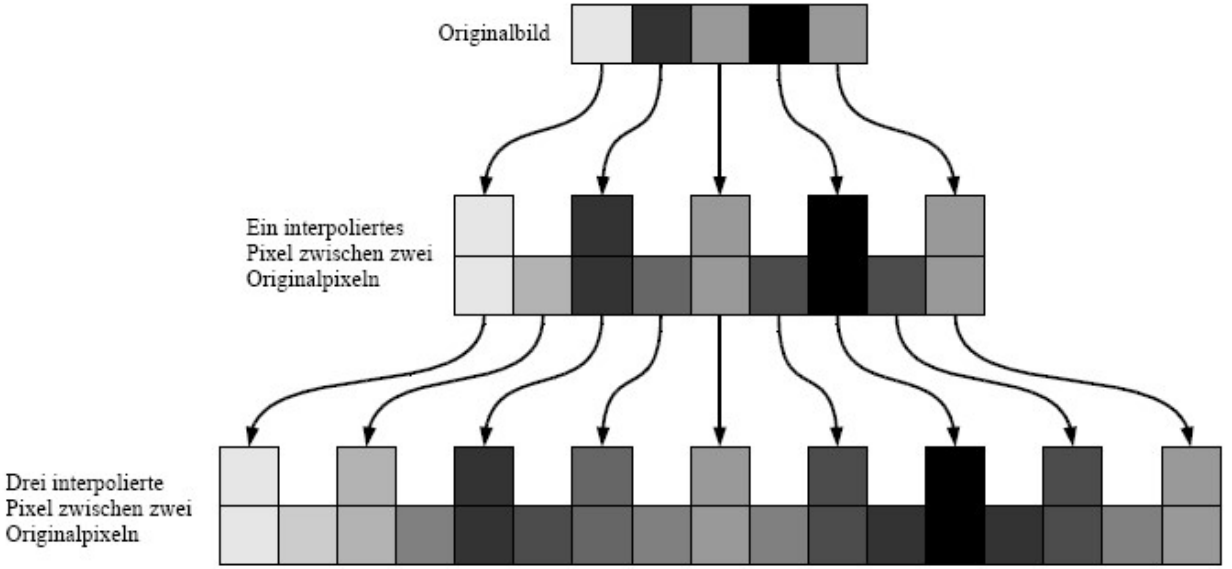
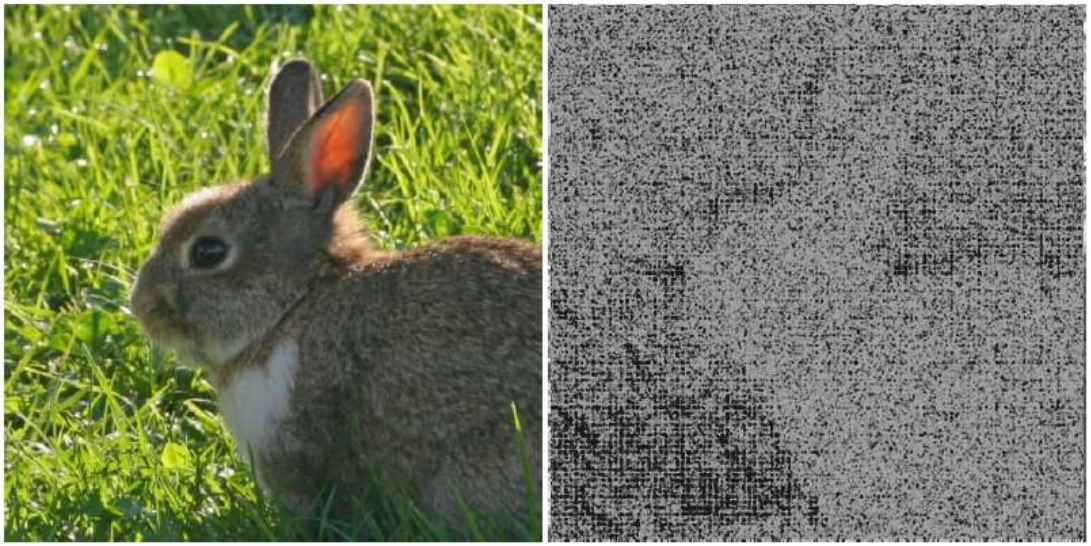
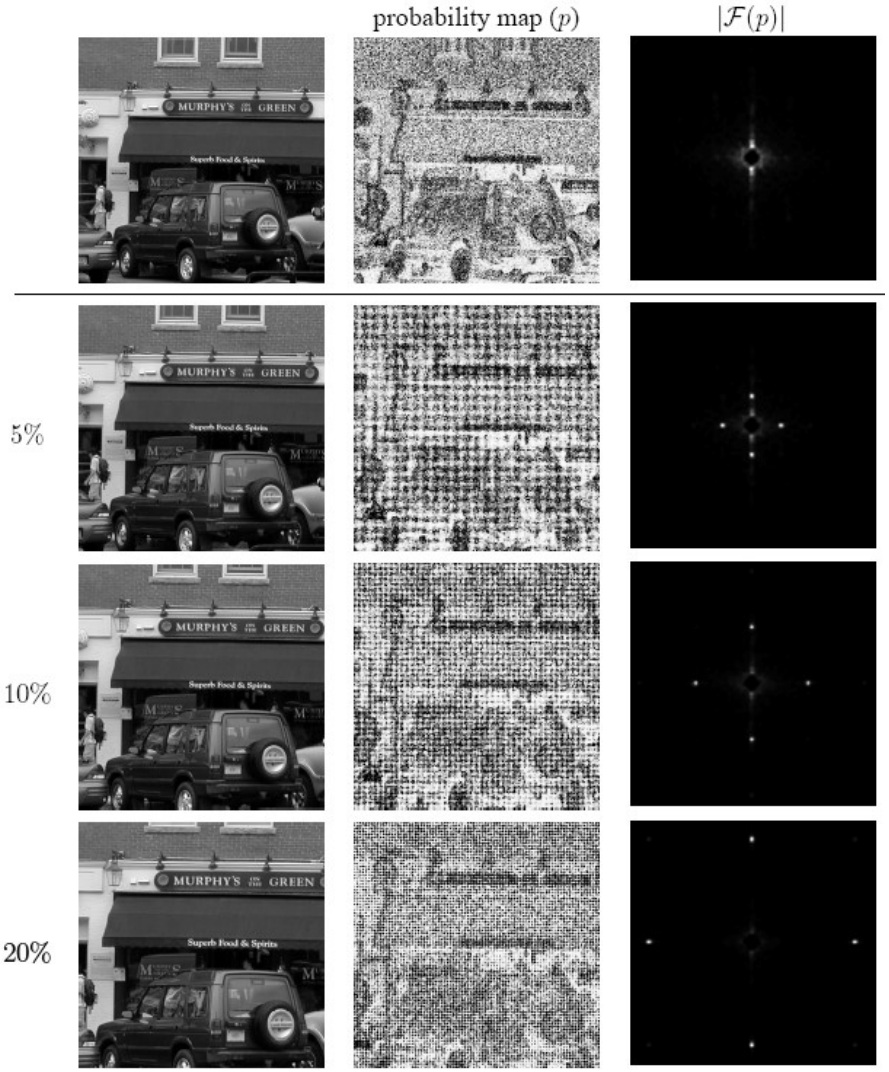


Image Forensics: Änderungserkennung

- Forensik
  - Der Expectation-Maximization (EM) Algorithmus berechnet für jeden Pixel die Wahrscheinlichkeit, dass er durch eine Interpolation von benachbarten Pixeln entstanden ist oder ob er von den Pixel unabhängig ist
  - Ergebnis: Probability Map (PM)
    - Zyklische Strukturen lassen auf Skalierung schließen



- Artefakte bei Vergrößerung
  - Spektrum der veränderten Bilder zeigt Schwerpunkte

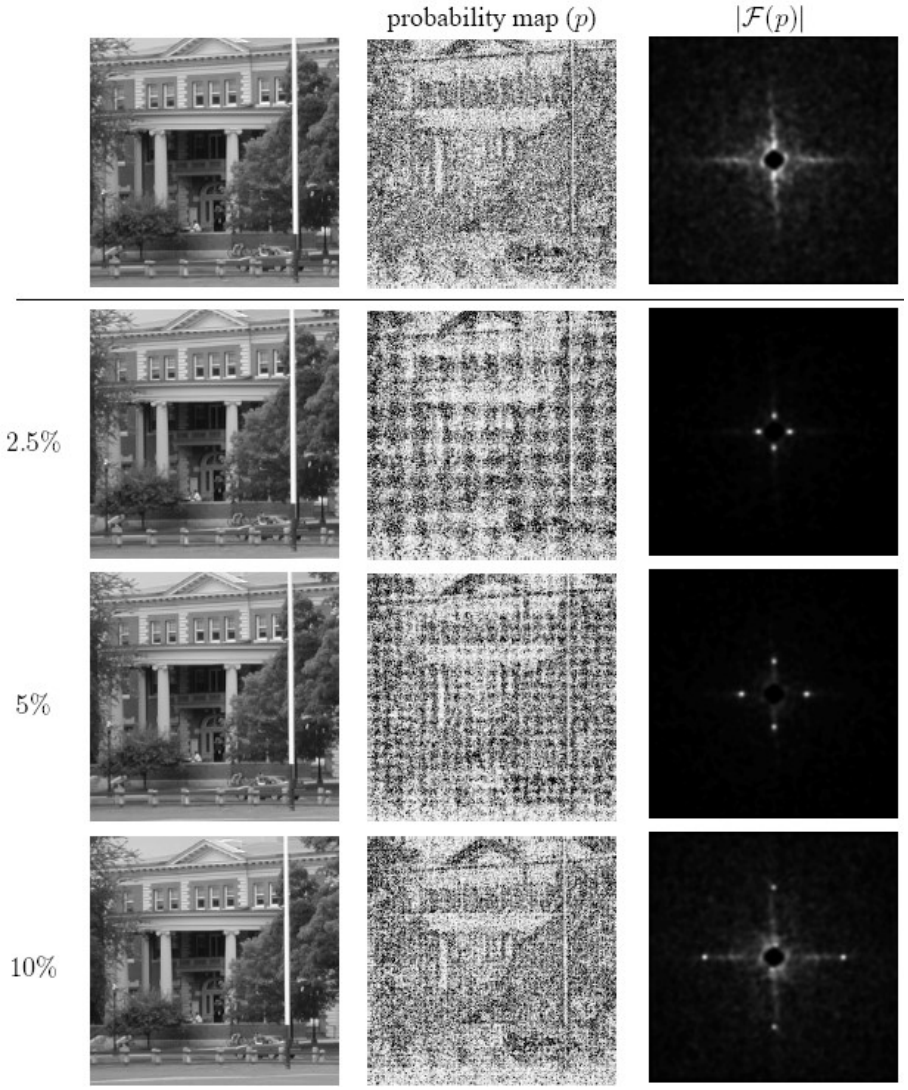


Statistical Tools for Digital Image Forensics

A.C. Popescu *(advisor: H. Farid)*

Ph.D. Dissertation, Department of Computer Science, Dartmouth College, 2005

- Artefakte bei Verkleinerung
  - Spektrum bei 10% „verwischt“ wieder

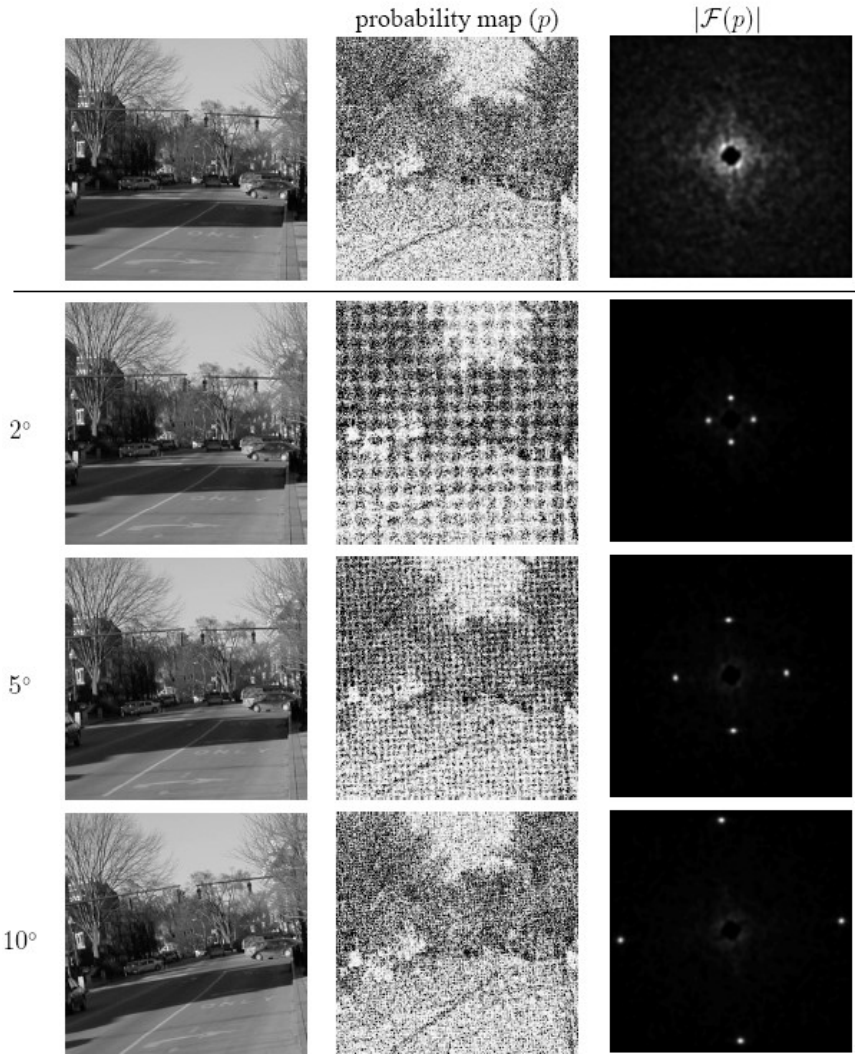


Statistical Tools for Digital Image Forensics

A.C. Popescu *(advisor: H. Farid)*

Ph.D. Dissertation, Department of Computer Science, Dartmouth College, 2005

- Artefakte bei Rotation
  - Spektrum zeigt deutliche Schwerpunkte



Statistical Tools for Digital Image Forensics

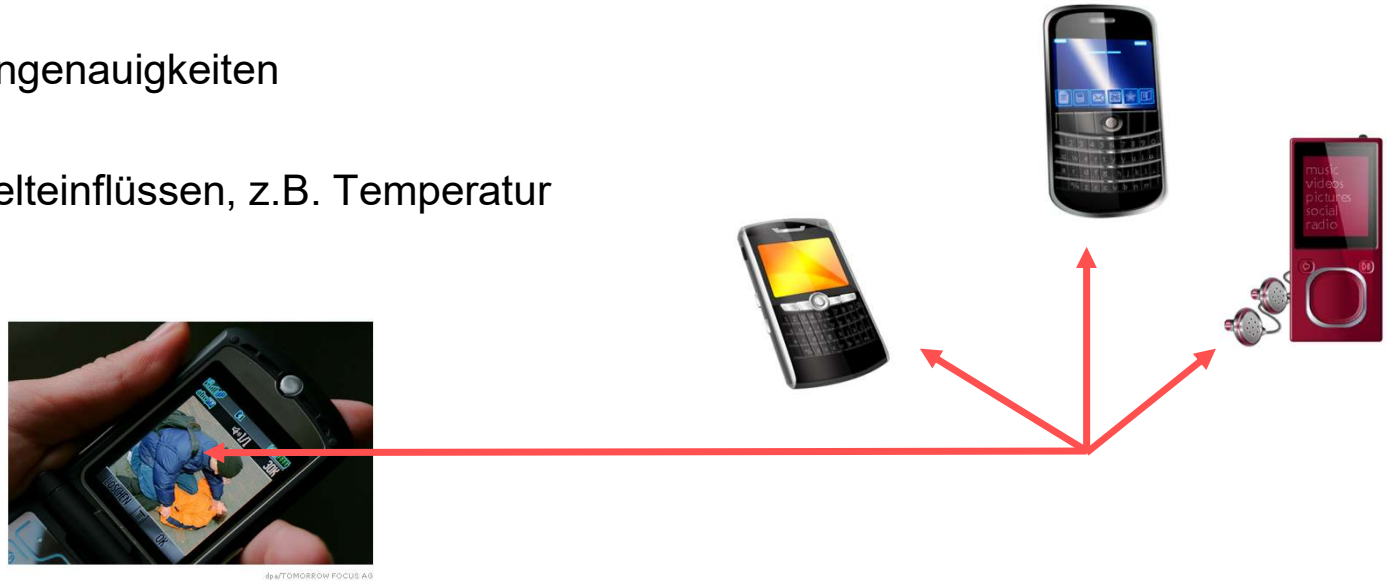
A.C. Popescu *(advisor: H. Farid)*

Ph.D. Dissertation, Department of Computer Science, Dartmouth College, 2005

Image Forensics: Erkennen von Geräten

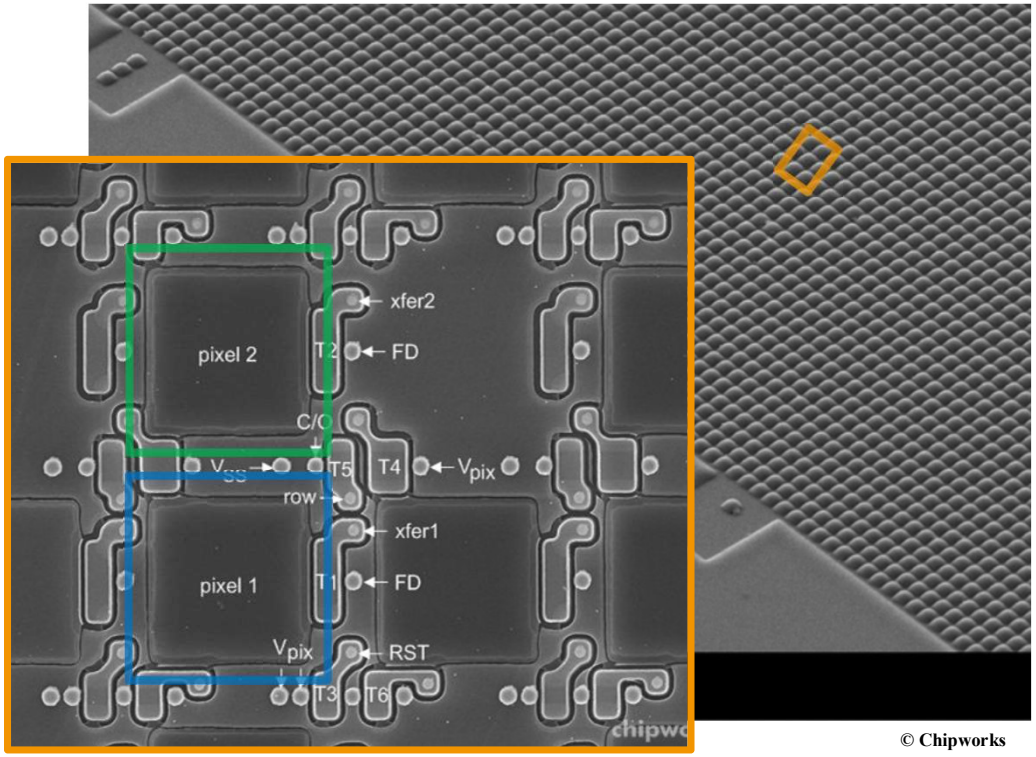
- Rückverfolgen von digitalen Medien auf Ursprung
  - Ohne vorheriges Einbetten von Wasserzeichen
  - Ohne Metainformationen
- Prinzip:
  - Jedes Gerät hat eine Charakteristik, die sich in erzeugten Medien widerspiegelt
    - Analog zu der Erkennung von Schreibmaschinen durch Druckbild…
  - Genauigkeit schwankt von Gerätelinie bis hin zum einzelnen Modell
  - Charakteristik wird beispielsweise bestimmt durch
    - Fehler in Aufzeichnungsmechanismen
      - Chip in Kamera
    - Fehler in Wiedergabemechanismen
      - Druckbild
    - Rauschen der AD Wandlung

- Rauschen von Bildsensoren
  - CCD-Arrays
    - CCD: - Charge-Coupled Device
  - Jedes Pixel benötigt ein CCD Halbleiterbauelement
    - Licht wird in elektronische Signale gewandelt (AD-Wandlung)
    - Dabei entsteht Rauschen
  - Rauschen kann unterteilt werden
    - Statisches Rauschen
      - Abhängig von Bauungenauigkeiten
    - Dynamisches Rauschen
      - Abhängig von Umwelteinflüssen, z.B. Temperatur



Sensor-Fingerprinting

- Im Kamera-Sensor: Analog-Digital-Wandlung
  - Pixelfehler → „tote“ Pixel
  - Thermisches Rauschen im Sensor → DSNU
  - Lichtempfindlichkeit der Sensorpixel unterschiedlich → PRNU
- dies hinterlässt „Sensor-Fingerprint“
  - ist charakteristisch für den einzelnen Sensor
  - ist zeitlich konstant

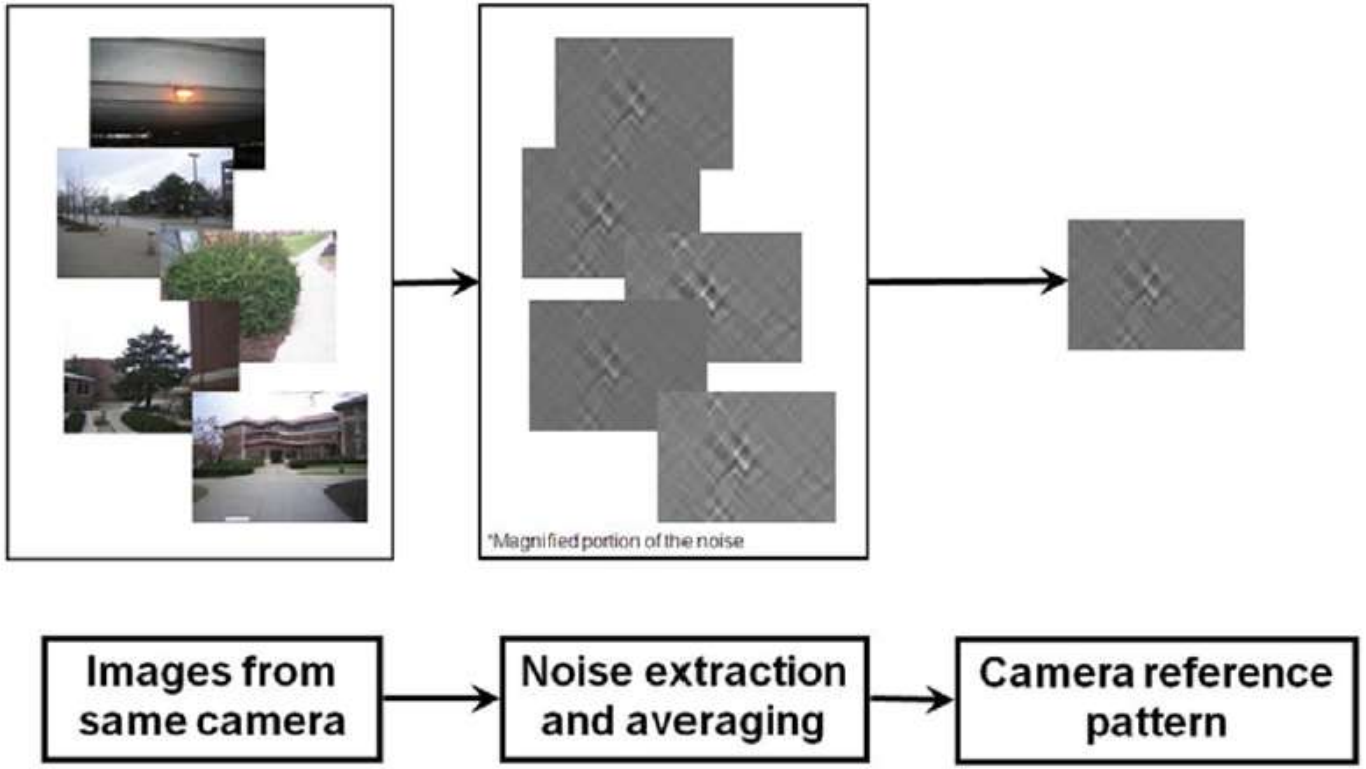


© Chipworks

- Beispiel für Characteristik:
  - Vorgehensweise
    - Dark Current
      - Aufnahme bei verdecktem Objektiv
      - Ermöglicht Normalisierung der Pixel
    - Dark Signal Non-Uniformity (DSNU)
      - Basis: 100 x Bilder mit unterschiedlichen Belichtungszeiten nehmen
      - Berechnung der durchnittlichen Pixelwerte an eine Position über die Bilder hinweg
      - Normalisieren der Pixelwerte
      - Berechnen der Abweichung der normalisierten Pixelwerte über die Positionen hinweg
    - Photo Response Non-Uniformity (PRNU)
      - Basis: 100 Bilder homogener Natur (z.B. Himmel)
      - Durchschnitt der Bilder berechnen
      - DSNU abziehen
      - Varianz der resultierende Pixelwerte berechnen
      - Berechnung Stärke der Abweichung für jedes Pixel (Varianz / Pixelwert)

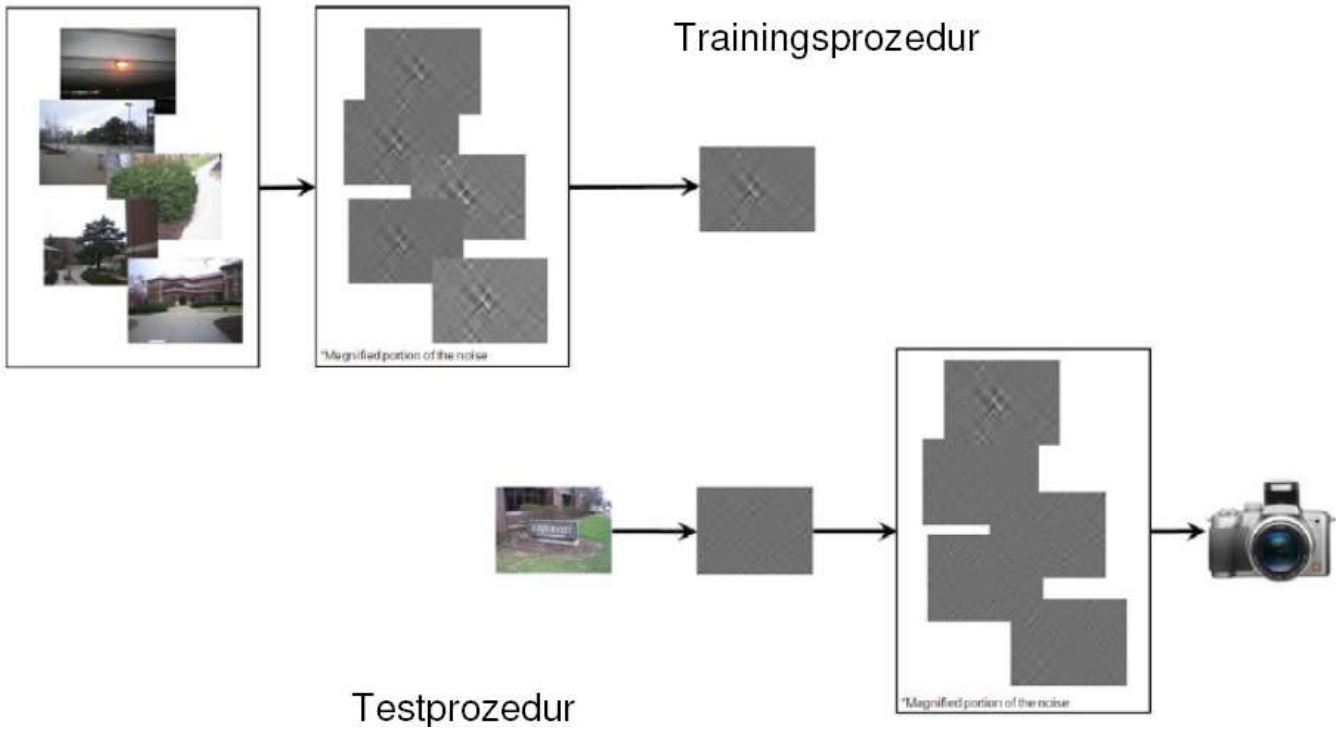
http://scien.stanford.edu/class/psych221/projects/05/joanmoh/

- Grundprinzip



Nitin Khanna, Aravind K. Mikkilineni, Edward J. Delp, Forensic Camera Classification: Verification of Sensor Pattern Noise Approach, Forensic Science Communications (FSC), vol. 11, no.1, (2009).

- Erkennen von Kameras über Rauschen

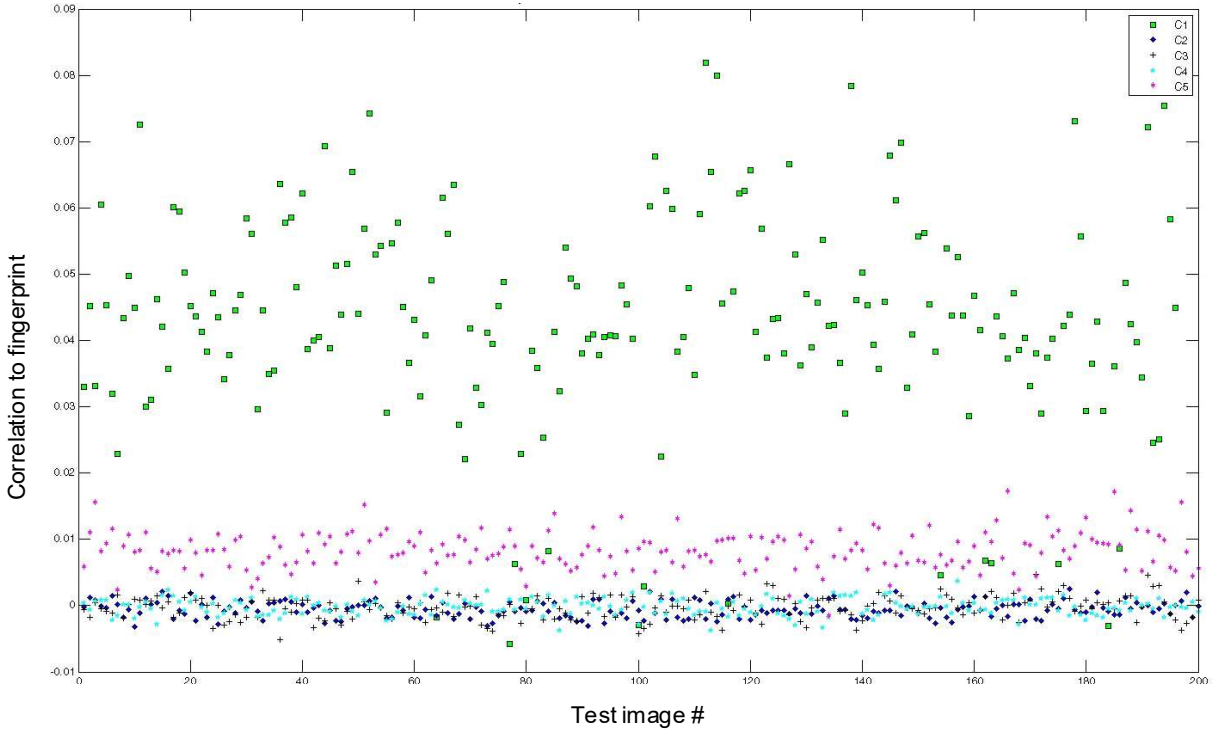


Nitin Khanna, Aravind K. Mikkilineni, Edward J. Delp, Forensic Camera Classification: Verification of Sensor Pattern Noise Approach, Forensic Science Communications (FSC), vol. 11, no.1, (2009).

Sensor-Fingerprinting für Quellenkennung

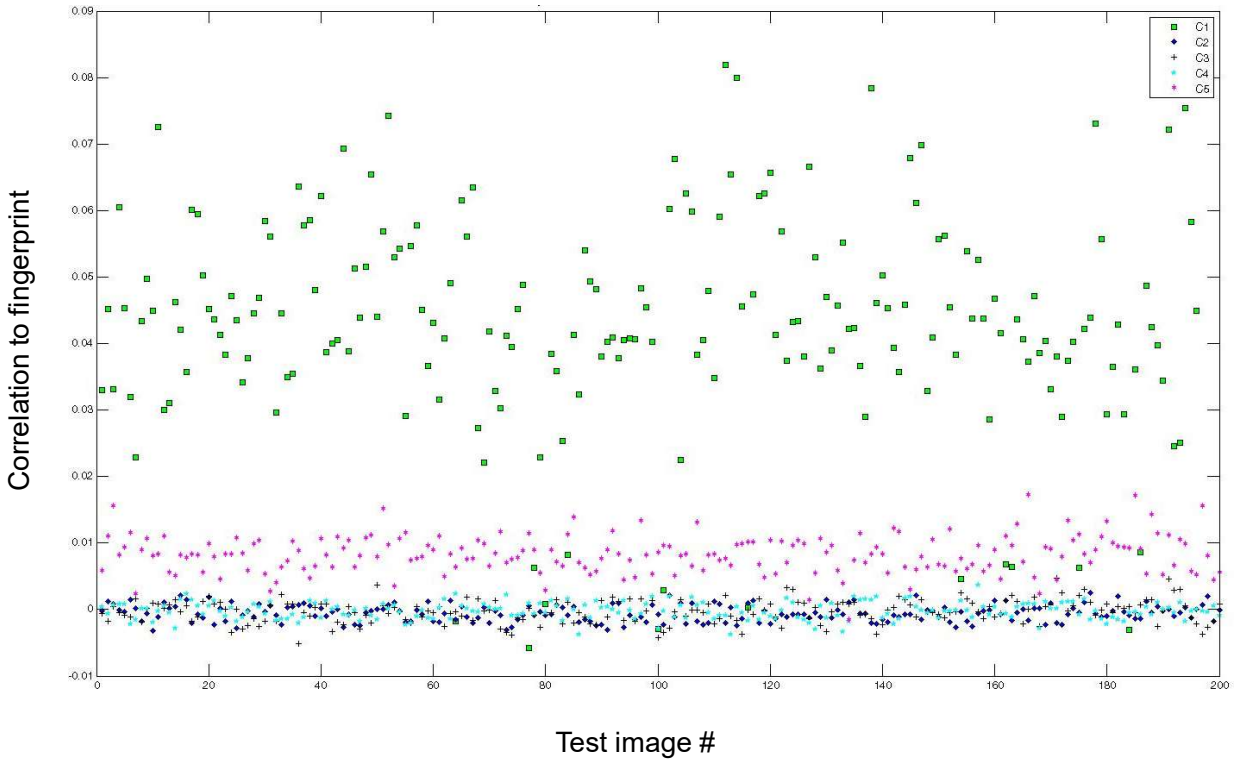
- Chancen der Quellenerkennung mittels Sensor-Fingerprinting
  - In den vielen Fällen: signifikante Unterscheidung ist möglich
  - funktioniert auch aus Papierausdrucken
  - Alterungseffekte im Sensor → Pixelfehler → Zeitpunkt der Aufnahme
- Limitierung des Verfahrens:
  - Sensor-Fingerprint bei Bildern stark texturierten Inhalten schwierig zu berechnen
  - Sensor-Fingerprint kann in Einzelbild gelöscht und ersetzt werden

- Erkennungsraten
  - Charakteristisches Muster von 5 Kameras aus 100 Bildern gewonnen
  - Korrelation von 200 Bildern, aufgenommen von C1 mit den Mustern von C1 bis C5
  - Unterscheidbarkeit ist in den meisten Fällen gegeben



	Handy	Resolution	Flash	Autofocus
C1	Nokia N95	2592x1944	Yes	Yes
C2	SonyEric. K550i	1632x1224	No	Yes
C3	Palm Treo 500v	1600x1200	No	No
C4	SonyEric. K550i	1632x1224	No	Yes
C5	Sony Eric K610i	1600x1200	No	No

300 Bilder für jedes Handy:
- **100 Training**
- **200 Test**



- **Erkennungsrate eines Fingerprints über fünf Handymodelle**

Webcam Forensics

- Experiment von 2009
  - Van Houten, Wiger; Geradts, Zeno J.;Using Sensor Noise to Identify Low Resolution Compressed Videos from YouTube; International Workshop on Computational Forensics, 2009
- Webcam mit Auflösung 640x480 Pixel
  - 8 identische Exemplare
- Training über „flatfield“ Aufnahmen, also ohne Inhalt
- Upload zu youtube
- Download und Erkennung
  - Erkennung bedeutet hier: Korrelation mit korrektem Muster stärker als mit jedem anderen Muster
- Erkenntnisse:
  - Aufnahmen in niedrigerer Auflösung reduzieren Erkennungsraten
  - Selbst starke Kompression wie bei youtube kann gut überstanden werden

Kamera: 640x 480, youtube: 480x360

	cam1	cam2	cam3	cam4	cam5	cam6	cam7	cam8
ρ_m	**0.1334**	**0.2301**	**0.1279**	**0.1818**	**0.1596**	**0.1622**	**0.1515**	**0.2099**
ρ_{mm}	0.0374	0.0512	-0.0009	0.0342	0.0355	0.0290	0.0118	0.0421

Kamera: 320x 240, youtube: 320x240

	cam1	cam2	cam3	cam4	cam5	cam6	cam7	cam8
ρ_m	**0.1044**	**0.0936**	**0.1090**	0.0153	**0.0304**	**0.1044**	**0.0984**	0.0334
ρ_{mm}	0.0280	0.0616	0.0803	**0.0407**	0.0245	0.0526	0.0652	**0.0648**

- Wie sicher ist die Quellenerkennung?

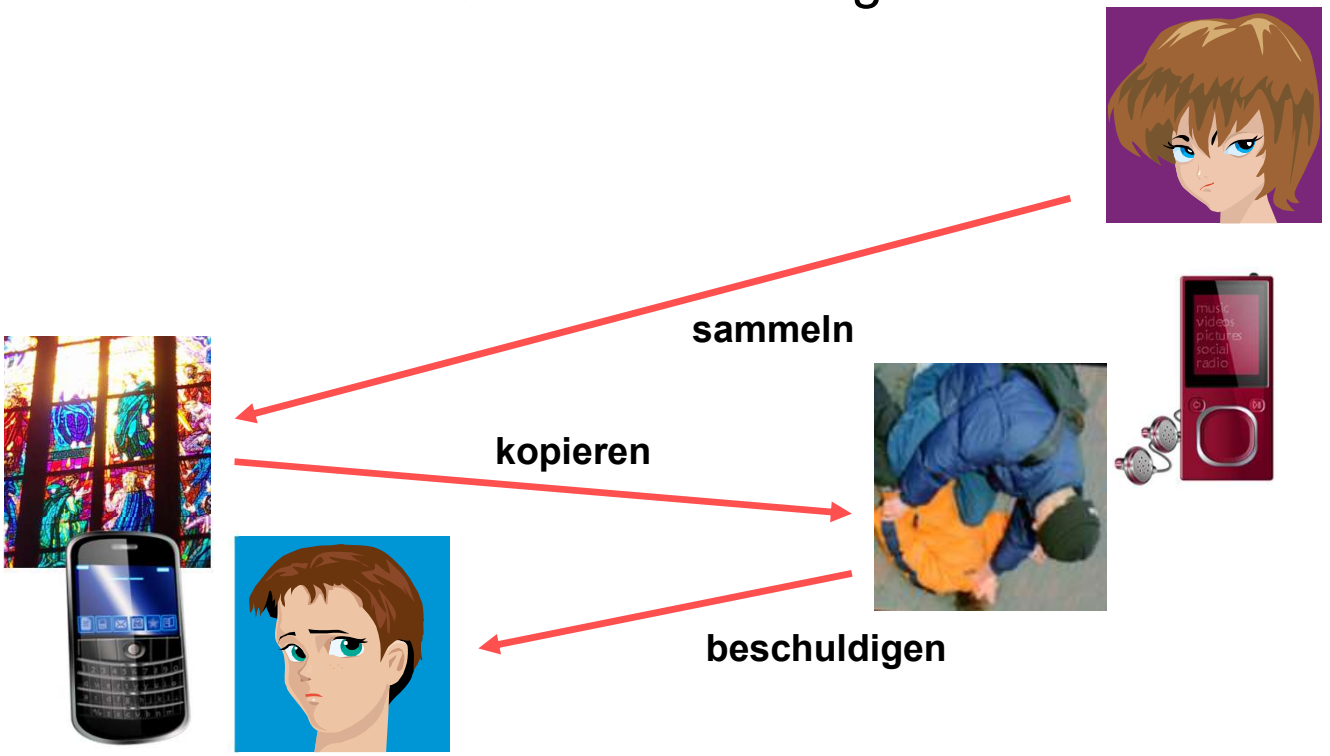
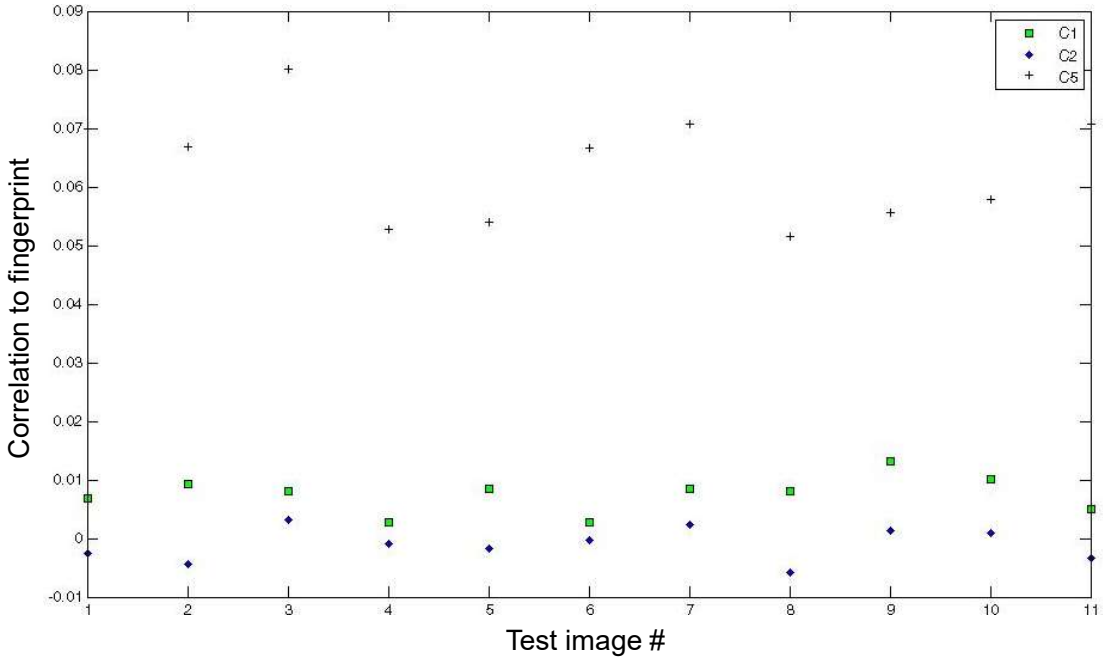
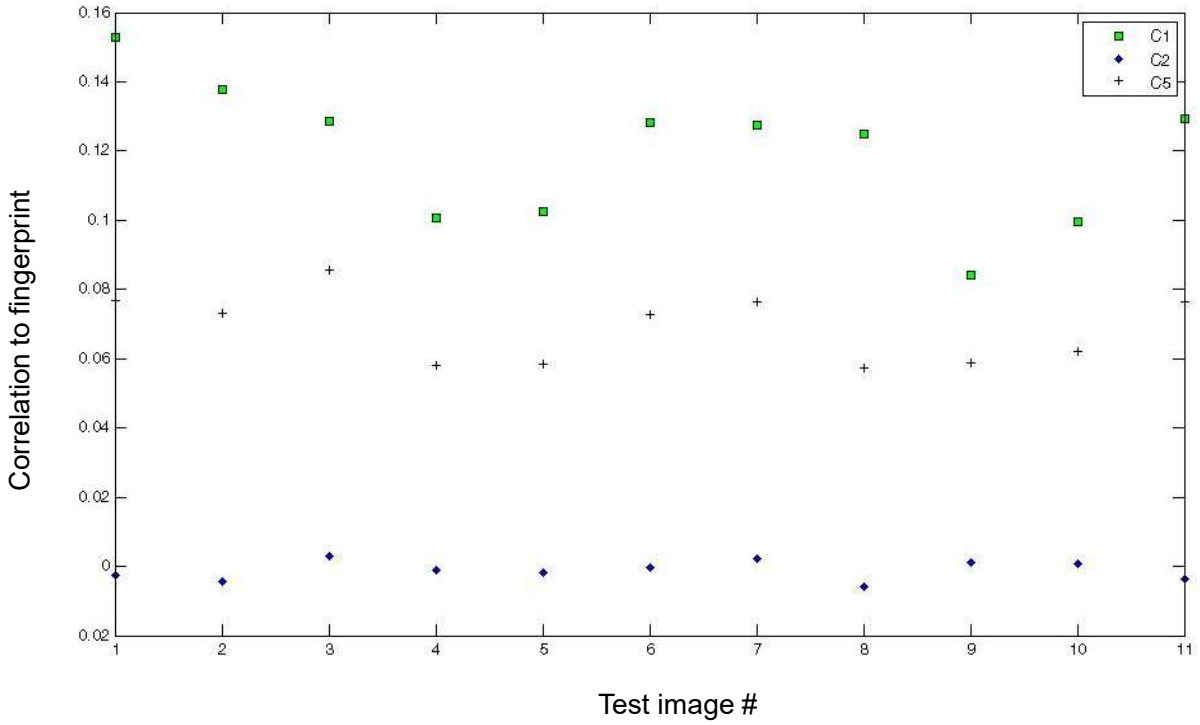


Image Forensics: Kameraerkennung

- Einfacher Angriff
  - Fingerabdruck Kamera A errechnen
  - Bild mit Kamera B erstellen
  - Fingerabdruck von Kamera A auf Bild kopieren
- Problem:
  - Bild enthält Fingerabdruck beider Kameras



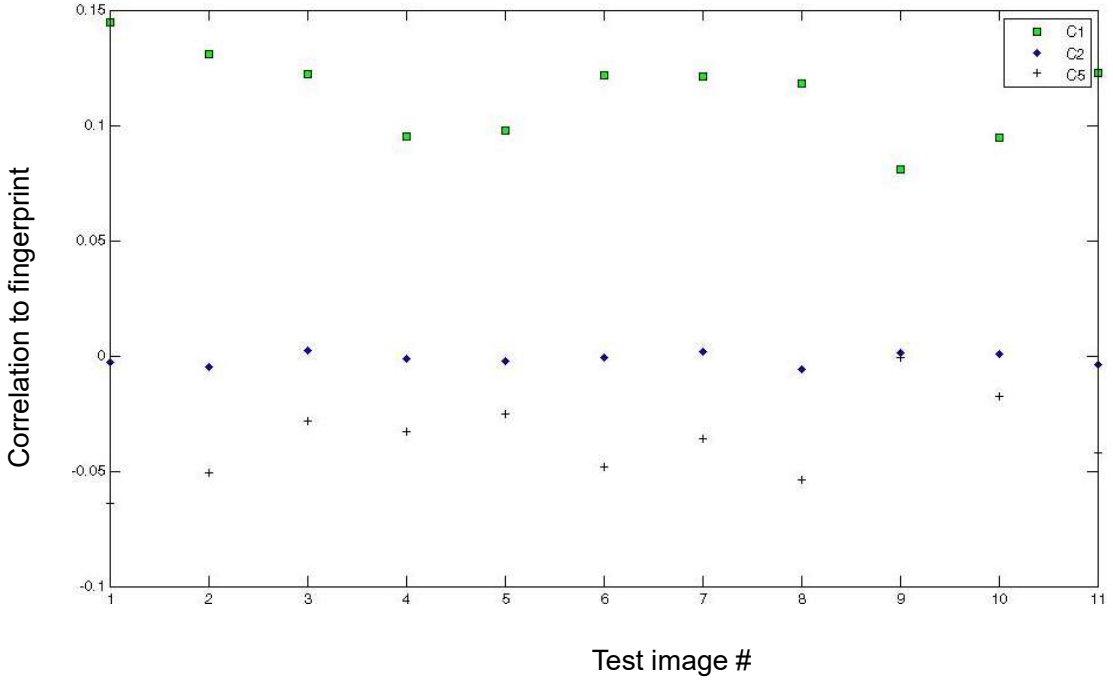
- **Ohne Anriff: Bilder wurden mit C5 erstellt, hohe Korrelation mit korrekten Fingerabdrücken**



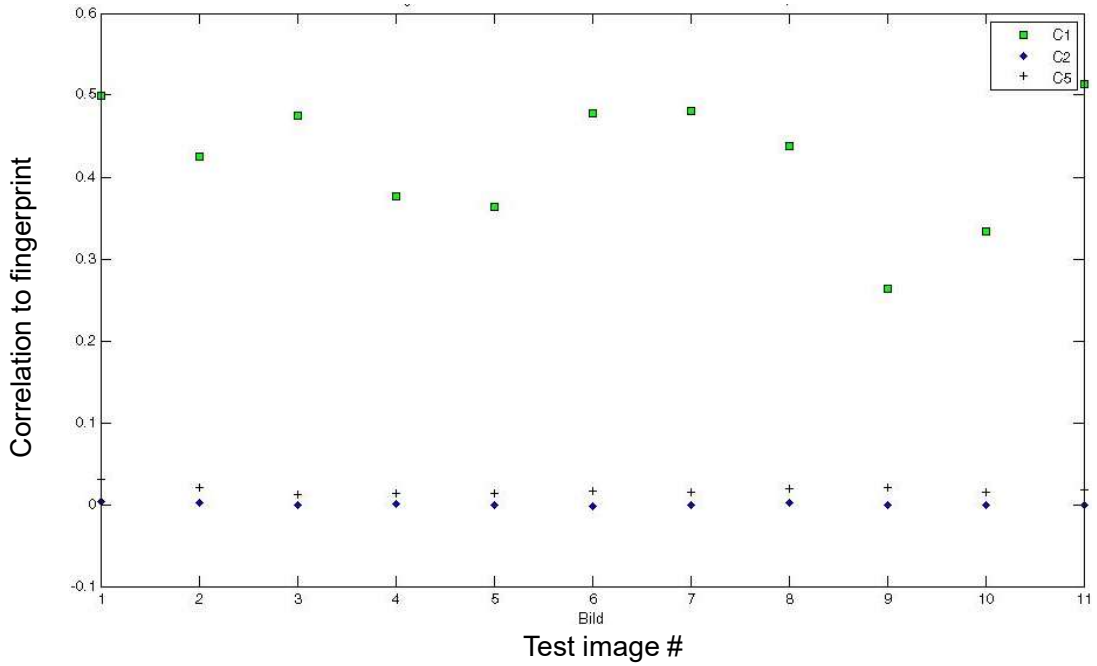
- **Nach Kopierangriff: Fingerabdruck von Kamera C1 wurde auf Bilder von C5 kopiert, hohe Korrelation mit C1, aber auch C5 ist erkennbar**

Image Forensics: Kameraerkennung

- Komplexer Angriff
  - Fingerabdruck von Kamera A berechnen
  - Bild mit Kamera B erstellen
  - Fingerabdruck von B löschen
  - Fingerabdruck von A kopieren



• Vor dem Kopieren von Fingerabdruck C1 wird Fingerabdruck von C5 gelöscht, die Folge ist eine verdächtige negative Korrelation



- **Optimierter Angriff mit vorgeschalteter Rauschunterdrückung**

Literaturtip

- http://www.cs.dartmouth.edu/farid/downloads/tutorials/digitalimageforensics.pdf
  - Tutorial von Farid zu Bild- und Videoforensik

- http://dud.inf.tu-dresden.de/~kirchner/Documents/image_forensics_and_counter_forensics.pdf
  - Text von Matthias Kirchner

Sexting und Nacktheit Erkennung