INF FAKULTÄT FÜR INFORMATIK

StegoDetect:
Steganographie und verdeckte Kommunikation - Attributierung

SMKITS
18.01.2023

Bernhard Birnbaum

Inhalt

1. Fortschritte
2. Identifizierte Attributierungsmerkmale
    a. Detektion
    b. Tool-Attributierung
    c. Daten-Attributierung
3. Implementierte Attributierung
4. Umgehen der Attributierung
5. Aussicht
6. Quellen & Fragen

1. Fortschritte

- Umsetzung abgeschlossen
- Detailanalyse und Auswertung beendet
- (abgeänderte) Aufgabenstellung vollständig bearbeitet
- Abschlussreport prinzipiell fertig

Organisation

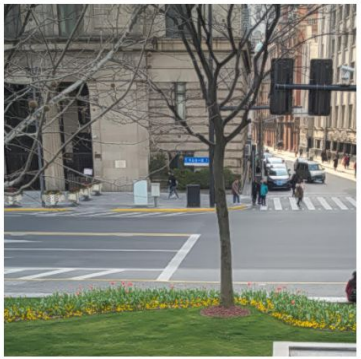
- wöchentliche Task-Coach-Meetings
- Code-Verwaltung und Dokumentation in GitHub-Repository

2. Merkmale zur Stego-Detektion

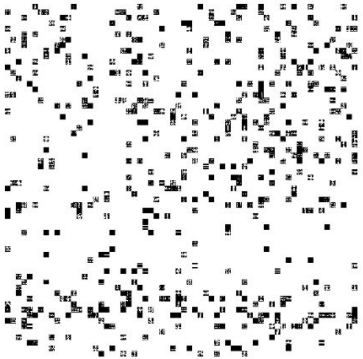
- **Entropie**: höhere Entropie weist auf Stego-Manipulation hin
- **Aufnahme-Kamera**: Metadaten wie Aufnahme-Kamera oder Geo-Daten werden durch Stego-Einbettungen verworfen
- **Encoding**: alle untersuchten Stego-Einbettungen wurden mit Baseline-DCT encodiert, auch wenn das Originalbild Progressive-DCT verwendet

2. Merkmale zur Tool-Attributierung

- **Dateityp**: bei *jsteg*-Manipulationen kann der Dateityp über *binwalk* nicht ausgelesen werden
- **JFIF-Version**: bei *jsteg*-Manipulationen kann die JFIF-Version über *binwalk* als auch *exiftool* nicht ausgelesen werden
- **Dateiheader**: *jsteg-*, *outguess/outguess-0.13-* sowie *f5*-Einbettungen haben jeweils immer den gleichen Dateiheader (durch für JPEG-Kompression verwendete Bibliotheken)
- **Detektionstools** *stegdetect/stegbreak*: Detektion von *jsteg-* (0-22%) und *outguess-0.13*-Einbettungen (0-20%)
- **Stego-Cover-Differenzbild**: *steghide* fällt durch Nähe zum Original-Bild auf
- alle Tools bis auf *steghide* führen bei der Speicherung des Stego-Bildes eine JPEG-Kompression durch, *steghide* komprimiert die Einbettungsdaten vor der Einbettung

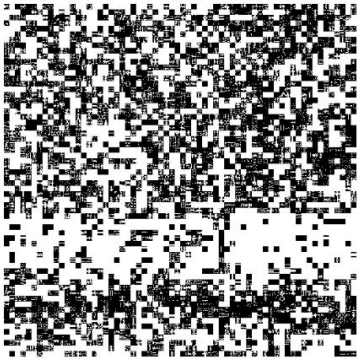


(a) Originalbild (Quality-Factor 75)

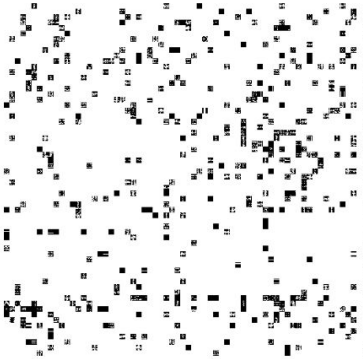


(b) ASCII-Daten (67 Bytes)

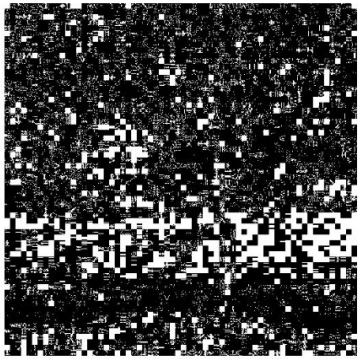
(c) ASCII-Daten (1.53 KB)



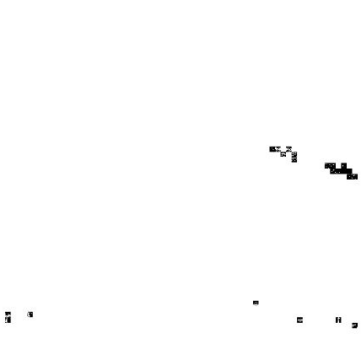
(d) ASCII-Daten (17.5 KB)



(e) ASCII-Daten (16 KB), minimale Entropie



(f) Binärdaten (16.8 KB)



(g) JPEG-Neukompression im Differenzbild (Quality-Factor 75)

(h) JPEG-Neukompression im Differenzbild (Quality-Factor 80)

2. Merkmale zur Einbettungsdaten-Attributierung

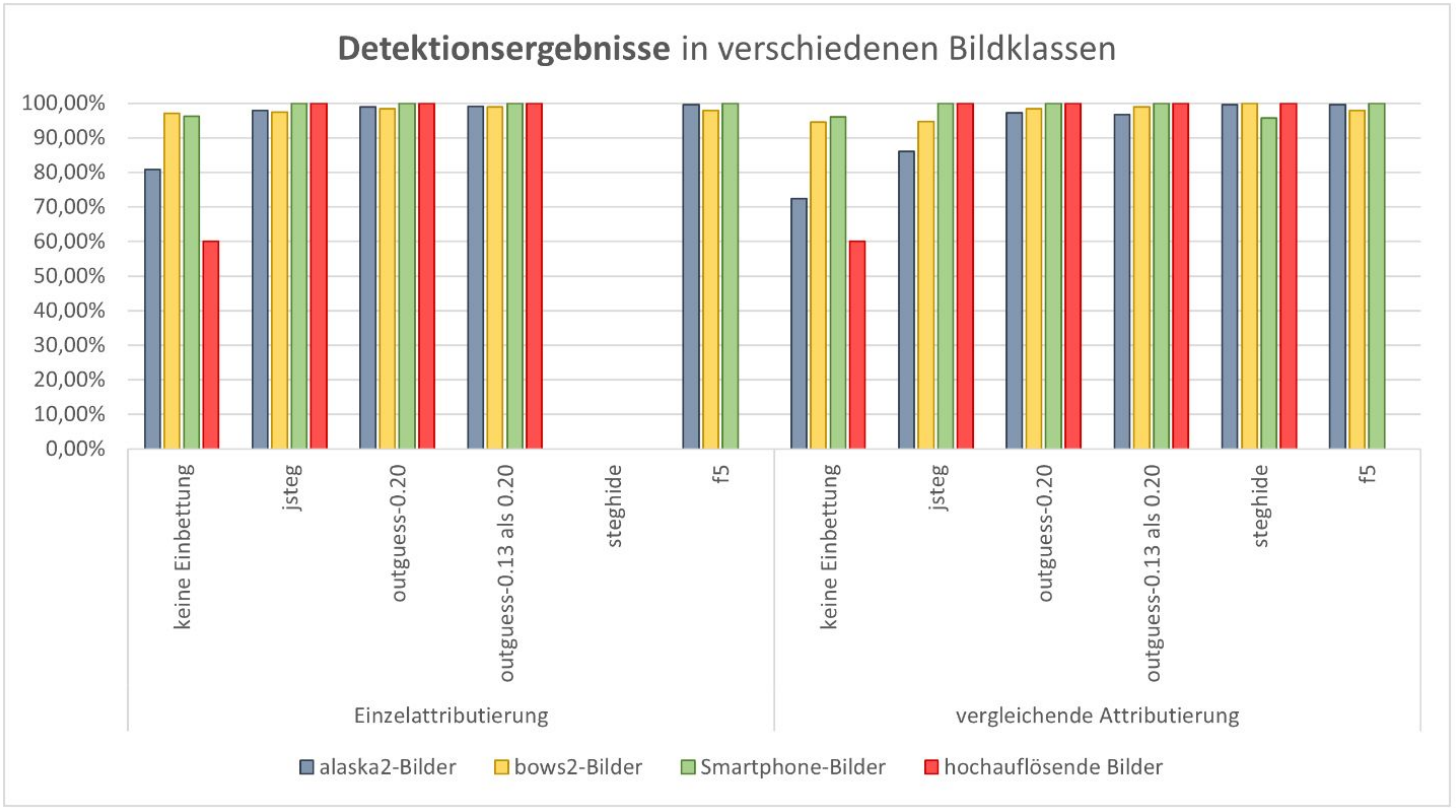
- Möglichkeit der Einbettungsdatenattributierung abhängig vom verwendeten Stego-Tool und Bildklasse
- vom Original **stärker abweichende Entropie** deutet auf mehr Einbettungsdaten hin
- zunehmende Einbettungsdatenlänge erzeugt **mehr Änderungen im Differenzbild**
- Beispiel Dateigröße**:**
    - *jsteg*: JPEG-Kompression, unabhängig von Einbettungsdaten
    - *outguess/outguess-0.13*: JPEG-Kompression, Stego-Bilder werden mit zunehmender Einbettungsdatenlänge größer
    - *steghide*: wie Original, unabhängig von Einbettungsdaten
    - *f5*: JPEG-Kompression, Stego-Bilder werden mit zunehmender Einbettungsdatenlänge kleiner
    - variiert zusätzlich in Details beim Intramedienvergleich

→ stark von Stego-Tool abhängig → Analyse/Implementierung von Attributierungsmerkmalen für Einbettungsdaten sehr aufwändig und z.T. sehr unscharf

3. Implementierte Attributierung

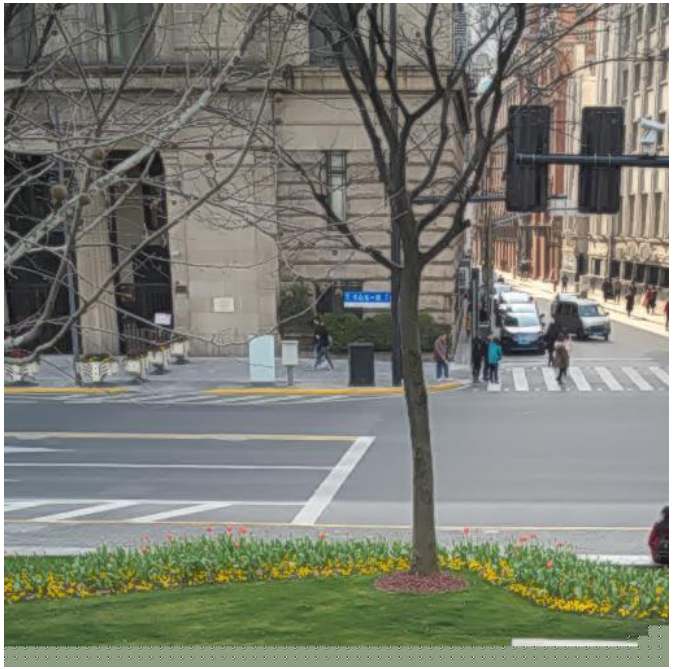
- bei der Implementierung liegt der Fokus auf der Tool-Attributierung
- direkte/vergleichende Attribute
- Test der Attributierung mit
  - kurzen Einbettungsdaten, da diese tendenziell am schwierigsten zu erkennen sind
  - ohne Schlüsselvariation, da Einfluss auf Merkmale minimal

Merkmal	Attributierungs-Tool	Stego-Tool
direkte Attribute		
JFIF-Version	*exiftool, binwalk*	*jsteg*
Dateiformat	*binwalk*	*jsteg*
Header	*strings*	*jsteg, outguess, outguess-0.13, f5*
Datei-Integrität	*foremost*	*jsteg*
Detektion	*stegdetect, stegbreak*	*jsteg, outguess-0.13*
vergleichende Attribute		
Dateigröße	*exiftool*	*steghide*
Differenzbild	*imagemagick*	*steghide*
Farbkanal-Differenzbild	*stegoveritas, imagemagick*	*steghide*


Detektionsergebnisse in verschiedenen Bildklassen
100,00%
90,00%
80,00%
70,00%
60,00%
50,00%
40,00%
30,00%
20,00%
10,00%
0,00%
keine Einbettung
jsteg
outguess-0.20
outguess-0.13 als 0.20
steghide
f5
keine Einbettung
jsteg
outguess-0.20
outguess-0.13 als 0.20
steghide
f5
Einzelattributierung
vergleichende Attributierung
alaska2-Bilder
bows2-Bilder
Smartphone-Bilder
hochauflösende Bilder

4. Umgehen der Attributierung

- volles Ausnutzen der Einbettungskapazität des Cover-Mediums macht Manipulationen einfacher zu erkennen
  → Daten sollten so kurz wie möglich sein
- Dateiheader und Metadaten sollten authentisch bleiben und nicht überschrieben werden
  → keine JPEG-Neukompression
- erzeugte Stego-Datei sollte nicht beschädigt sein
  → kein Einbetten von Daten direkt in den Header;
  → kein Überschreiten der Einbettungskapazität;
  sonst ist Erkennung trivial! (*jsteg*)



5. Aussicht

- Finalisieren des Reports m.H. der letzten Anmerkungen
- zahlreiche Ansatzpunkte für weiterführende Untersuchungen
    - erweiterte Detailanalyse (weitere Merkmale, Bildklassen, Analysetools, …)
    - Codeanalyse der Stego-Tools
    - Intermedienvergleich (Vergleich mit anderen Bild- oder Audioformaten, …)
    - parallele Implementierung (schnelleres Untersuchen größerer Coverdaten-Sets)
    - verbesserte inhaltsbasierte Untersuchung (Differenzbildzerlegung in Quadranten, AI-Methoden, …)
    - Stego-Analyse-Pipeline (Detektion → Tool-Attributierung → Datenattributierung)

6. Quellen

- siehe Draft-Literaturverzeichnis