

Einführung in die Multimedia-Forensik

Meta-Daten

- Meta-Daten enthalten oft wertvolle Zusatzinformationen, z. B. Kamera-Modell, GPS-Daten und Aufnahmezeitpunkt
- Fotos müssen nicht zwingend Meta-Daten enthalten
- Meta-Daten lassen sich sehr leicht fälschen; trotzdem können Sie als Indiz bzw. Hinweise für Tatsachen genutzt werden

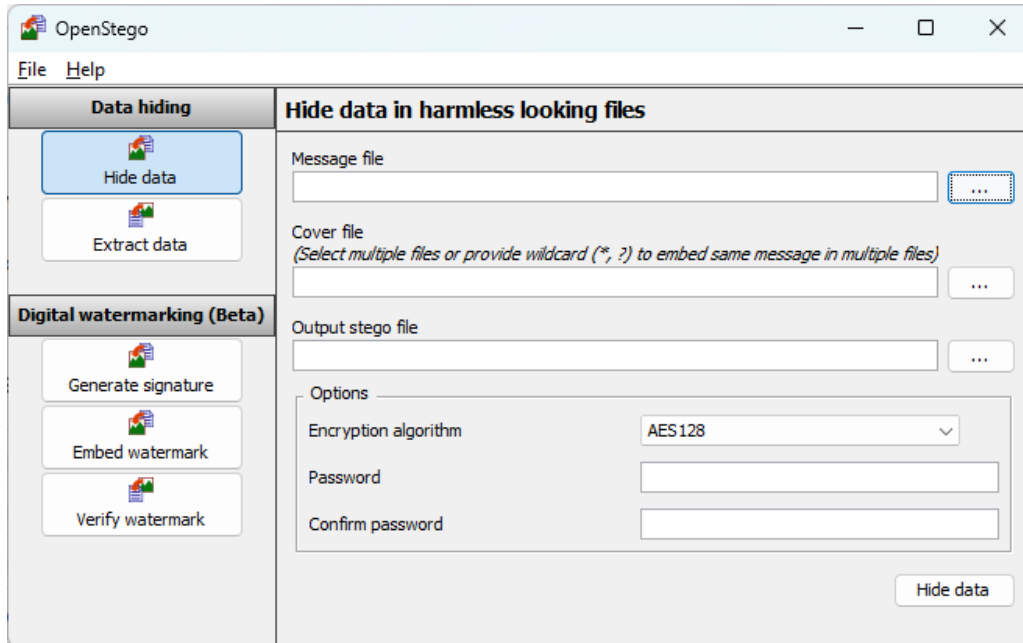
Finden von bekannten Fotos

- Abgleich mit (polizeilichen) Hash-Datenbanken
- Nutzung von Rückwärts-Suchmaschinen
 - Google Fotos
 - <https://www.reverseimagesearch.com/de> (kostenpflichtig)

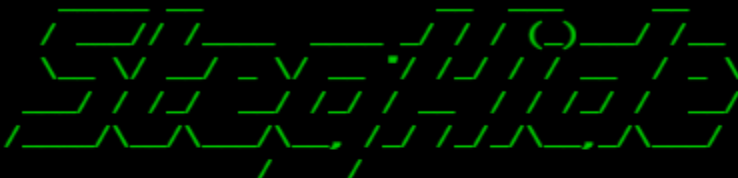
Steganografie

- Informationen unbemerkt in Multimedia-Daten verstecken
- Vorteil: Im Idealfall bekommt niemand unberechtigtes mit, dass überhaupt Informationen übertragen werden
- Nahezu in allen Multimedia-Formaten möglich

Beispiele Steganographie-Programme




```
$ bash steghide.sh
```



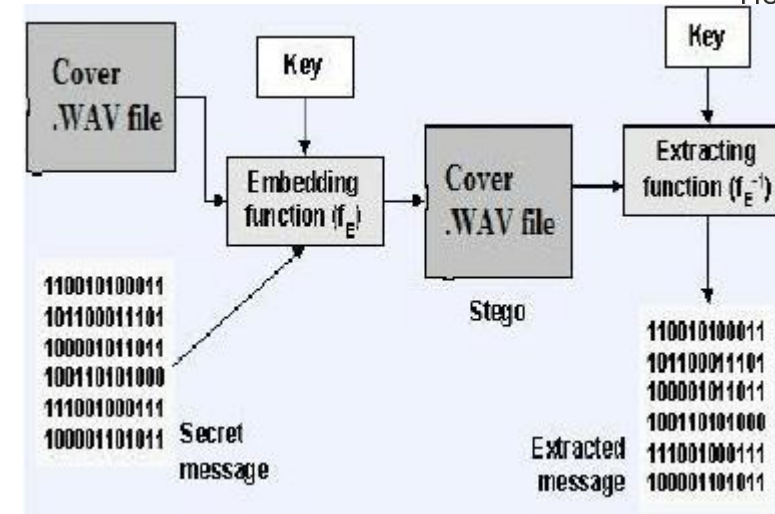
```
"If you are too lazy to type a single command,  
Allow my program to do it for you."  
-(https://github.com/ZechBron)
```

```
[Z] Please Choose:  
1. Embed a file in an image (jpeg, au, bmp and wav)  
2. Extract an image  
3. View Info of an image
```



Beispiel Audio Steganographie

- Theoretisch verschiedene Möglichkeiten
 - Änderung der Geschwindigkeiten → insbesondere bei Techno
 - Überlagerung mit kaum hörbaren Geräuschen
 - ...
- Bei Überlagerung ist die Differenz zum Original die Nachricht
- Identifizierung durch Vergleich mit Original, wenn dies bekannt
- Bei allen Verfahren gilt → Änderung darf durch menschliches Gehör (kaum) wahrnehmbar sein



Möglichkeiten zur Bildfälschung

- Copy-Paste-Fälschung
- Nachträgliches Einfügen von Inhalten
- Entfernen von Inhalten
- Drehen, Strecken, Verkleinern von Teilbereichen
- ...

Beispiel iranische Raketen



Das Originalfoto zeigt, dass eine der Raketen nicht funktionierte. Quelle: Spiegel vom 10. Juli 2008

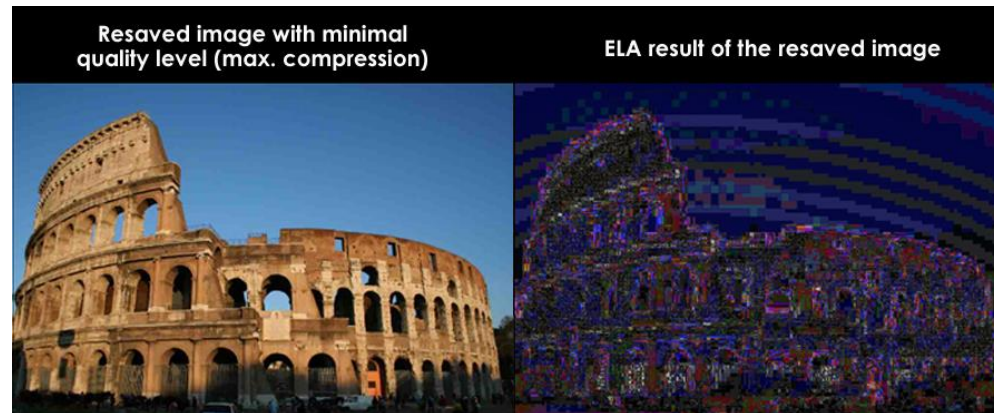
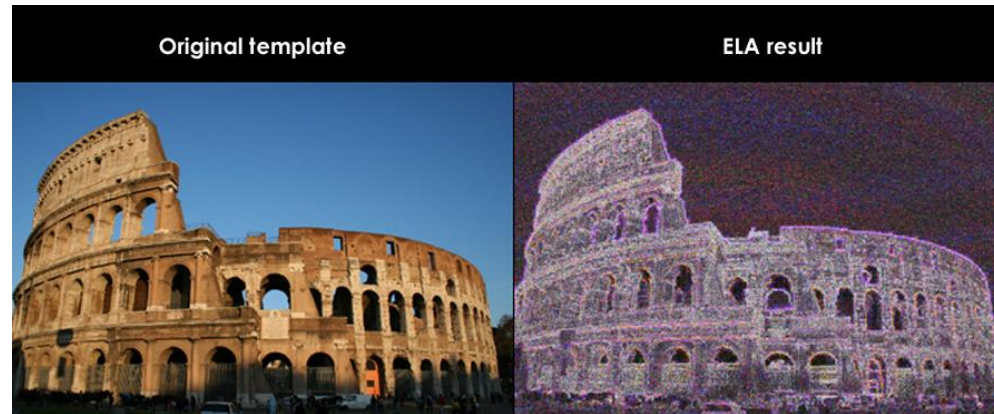
Möglichkeiten zur Erkennung von Bildmanipulation

- Erkennung stark Abhängig von Qualität der Fälschung
- Bei schlechten Fälschungen genügt ein Aufmerksames betrachten des Bildes (z. B. unlogische Schatten, Reste von Armen oder Beinen ...)
- Vergleich der Pixeldichte
- Doppelt vorkommende Bereiche
- ...

Error-Level-Analyse (ELA)

- Das Grundprinzip von JPG-Dateien ist, dass Bilddaten komprimiert werden → Verlust an Qualität
- Durch jede Speicherung und Kopie eines Bildes bzw. eines Ausschnitts wird dessen Qualität schlechter
- Unterschiedliche Qualitätsstufen eines Bildes können ein Hinweis auf eine Manipulation sein

Beispiel ELA



Bildquelle:

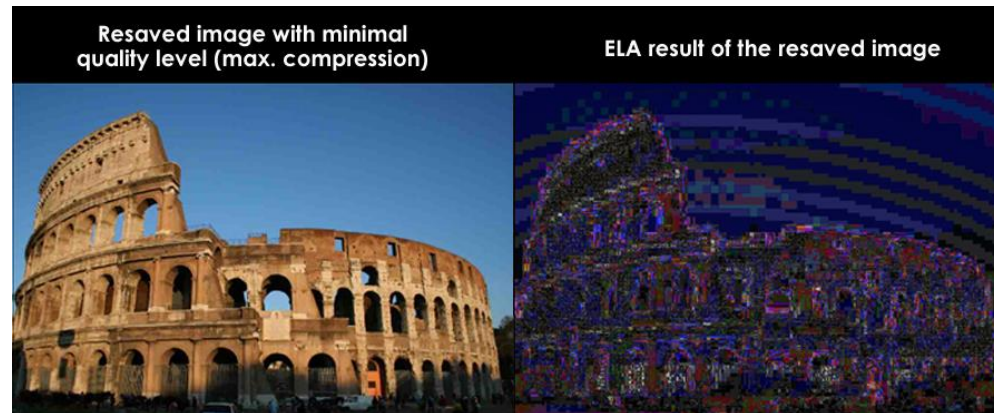
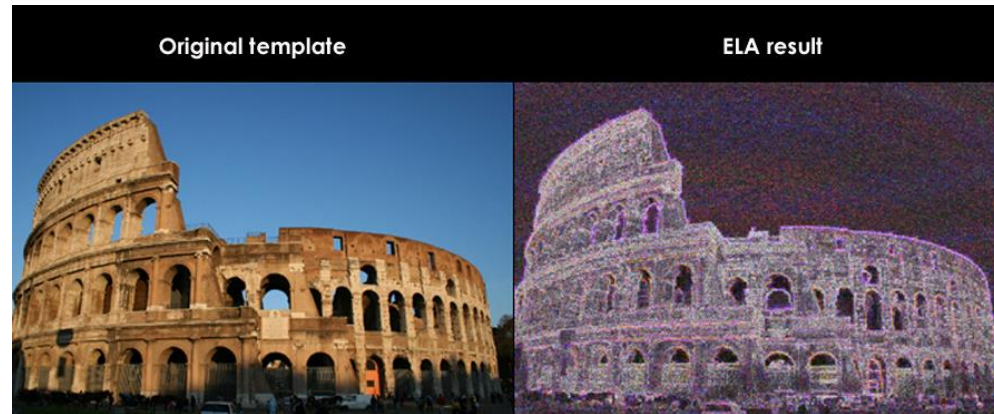
https://forensics.map-base.info/report_2/index.shtml

05.05.2023

Martin Morgenstern

11

Beispiel ELA



Bildquelle:

https://forensics.map-base.info/report_2/index.shtml

05.05.2023

Martin Morgenstern

12

Online-Dienste zur Identifizierung von kopierten bzw. gefälschten Bildern

- <https://fotoforensics.com/>
- <https://www.fakeimagedetector.com/>

Was ist die Nutzung solcher Dienste sinnvoll? Wann nicht?

Deep-Fakes

- Künstliche Videos die interagieren
- Tools (z. B. FaceLab), aber auch Online-Services
- Durch ständige Verbesserung mittlerweile eine reale Gefahr
- Erkennungsmöglichkeiten:
 - Noch wird meistens nur die Front gut simuliert, nicht aber die Seiten (bitten Sie die Person sich zu drehen)
 - Fragen stellen die nur die richtige Person beantworten kann