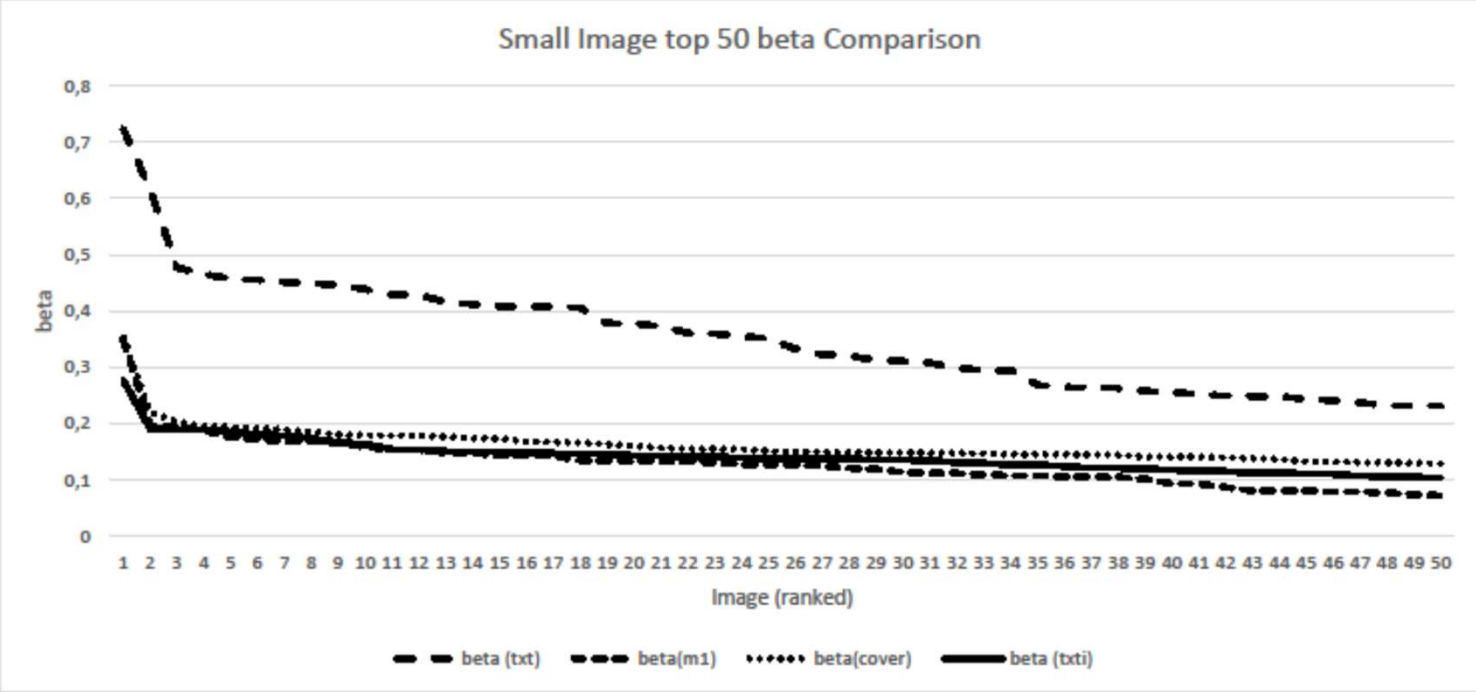
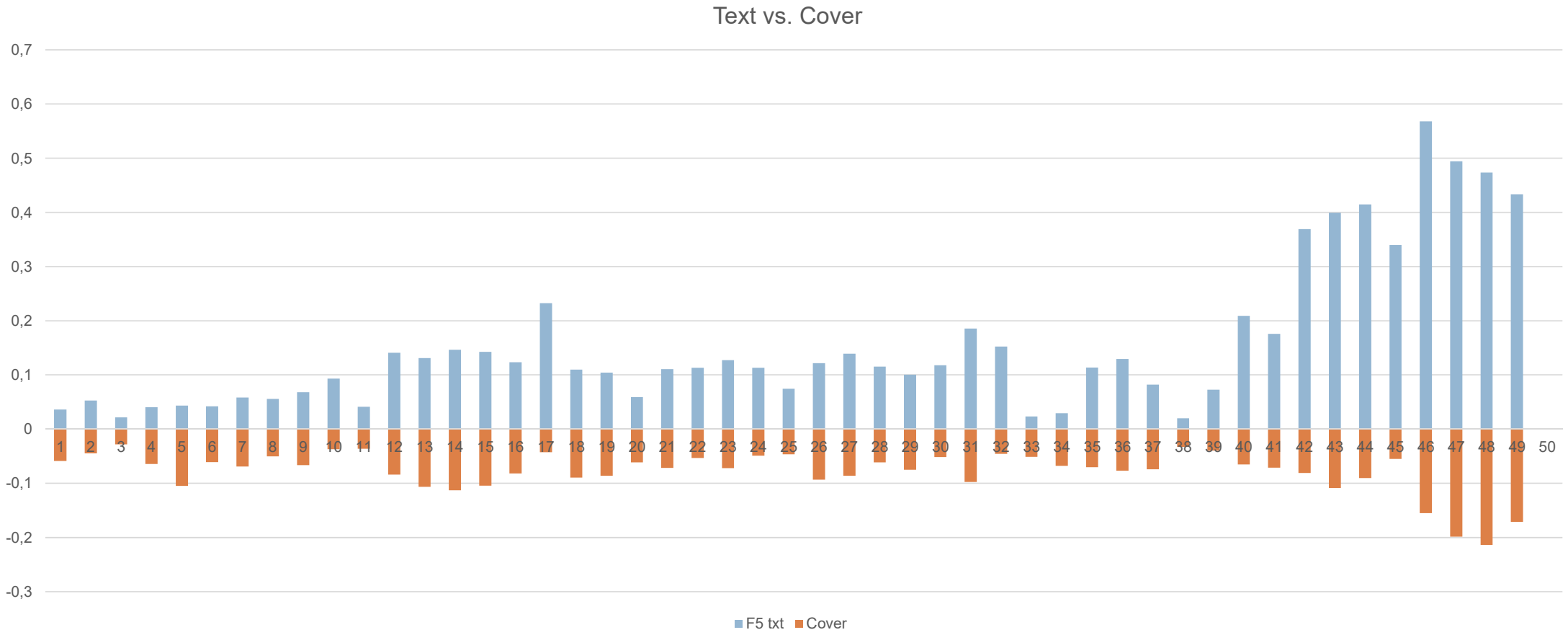
- Nachrichten, die die Kapazität ausnutzen, können verhältnismäßig gut erkannt werden
- Cover mit kurze Nachrichten (wenige Worte) sind nicht von einem Cover zu unterscheiden
- Eine Erweiterung des F5 Algorithmus erschwert/verhindert die Detektion deutlich
  - Einfach die Richtungen der Änderungen variieren, um Häufungen zur Null hin zu verhindern

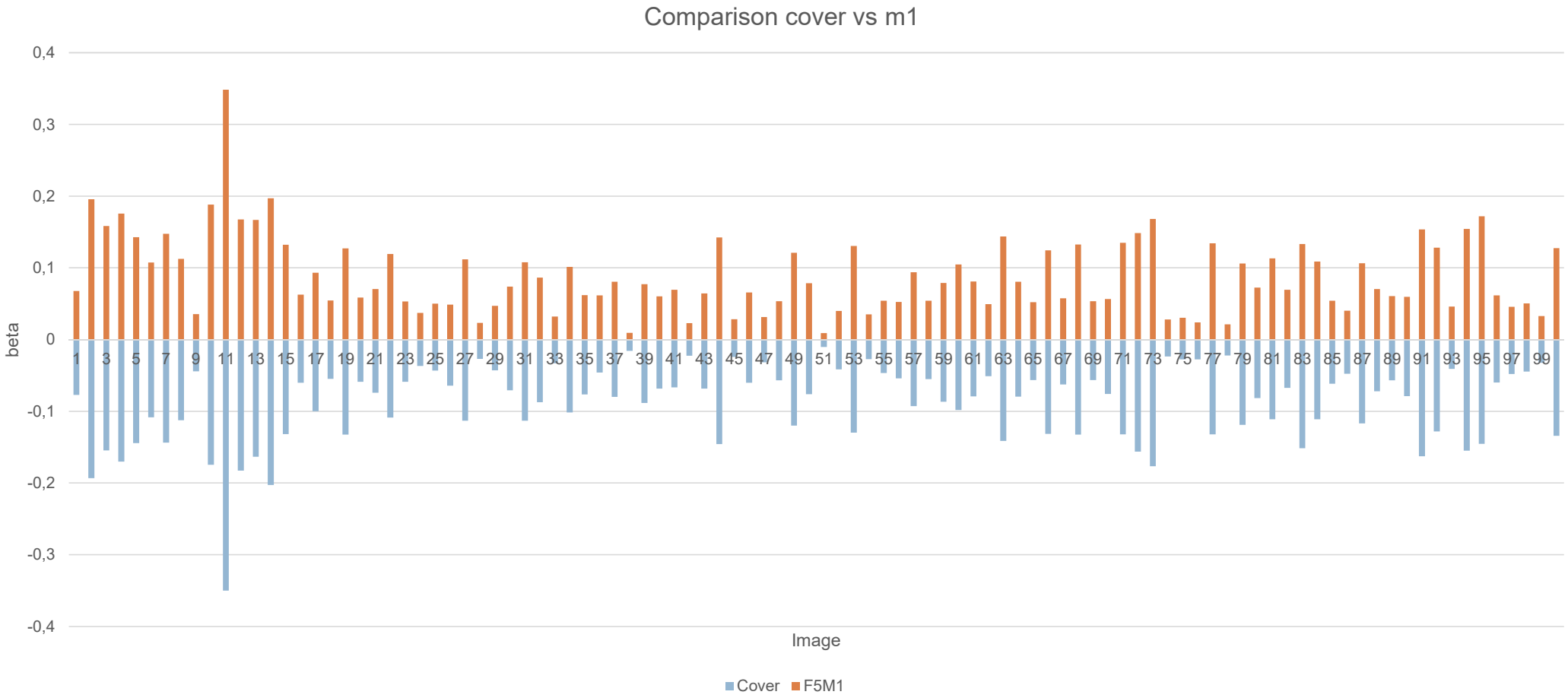


Steganographie/ F5

- Einbetten von Nachrichten führt zu einem signifikanten Ansteigen der beta-Werte



- Vergleich beta-Werte der Analyse bei kurzen Nachrichten



Erkennung von Steganographie in Kanälen

- Social Media provides many channels with lots of images
  - 1 to 1 (communication)
  - 1 to n (groups)
  - 1 to x (web)
- Steganography has been verified to be used for criminal purposes
- Steganalysis aims to recognize stego usage
- Error rates are still high
  - 2018: Tsang and Fridrich, 13% combined error rate
  - 2018: Lin et al., 24% combined error rate
  - Own experiments also 25% with „standard“ steganalysis on F5

Zahlen

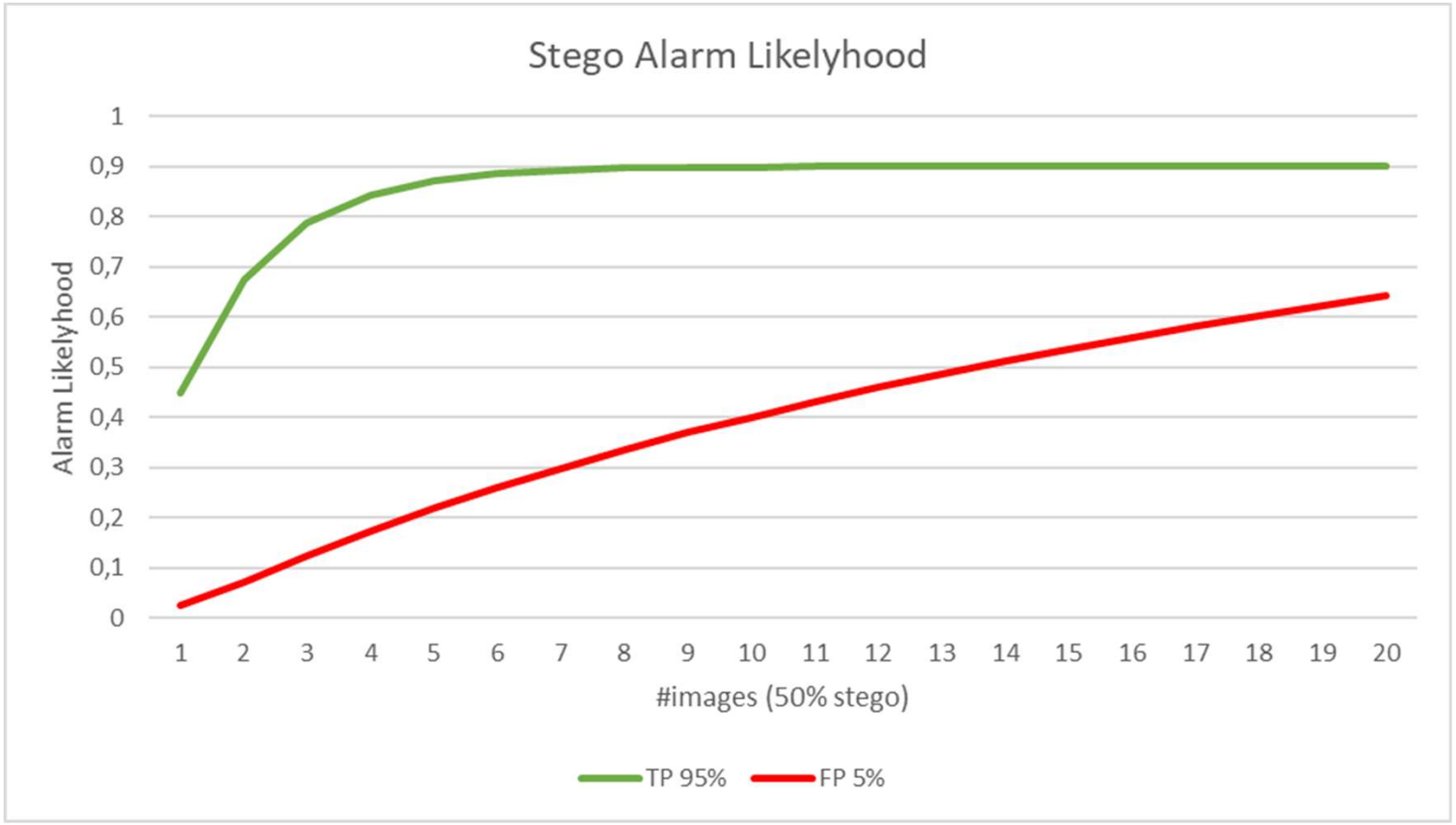
- 2018 (*)
  - Instagram: 95 Million photos uploaded on an average day
    - Estimated daily false alarms: 12,4 Million
  - Instagram: > 40 billion photos already shared
  - Snapchat: > 20,000 photos shared every second (1.728.000.000 per day)
    - Estimated daily false alarms: 225 Million
- Facebook: 300 Million photos per day (Gizmodo)
    - Estimated daily false alarms: 39 Million

(*)https://www.socialpilot.co/blog/social-media-statistics

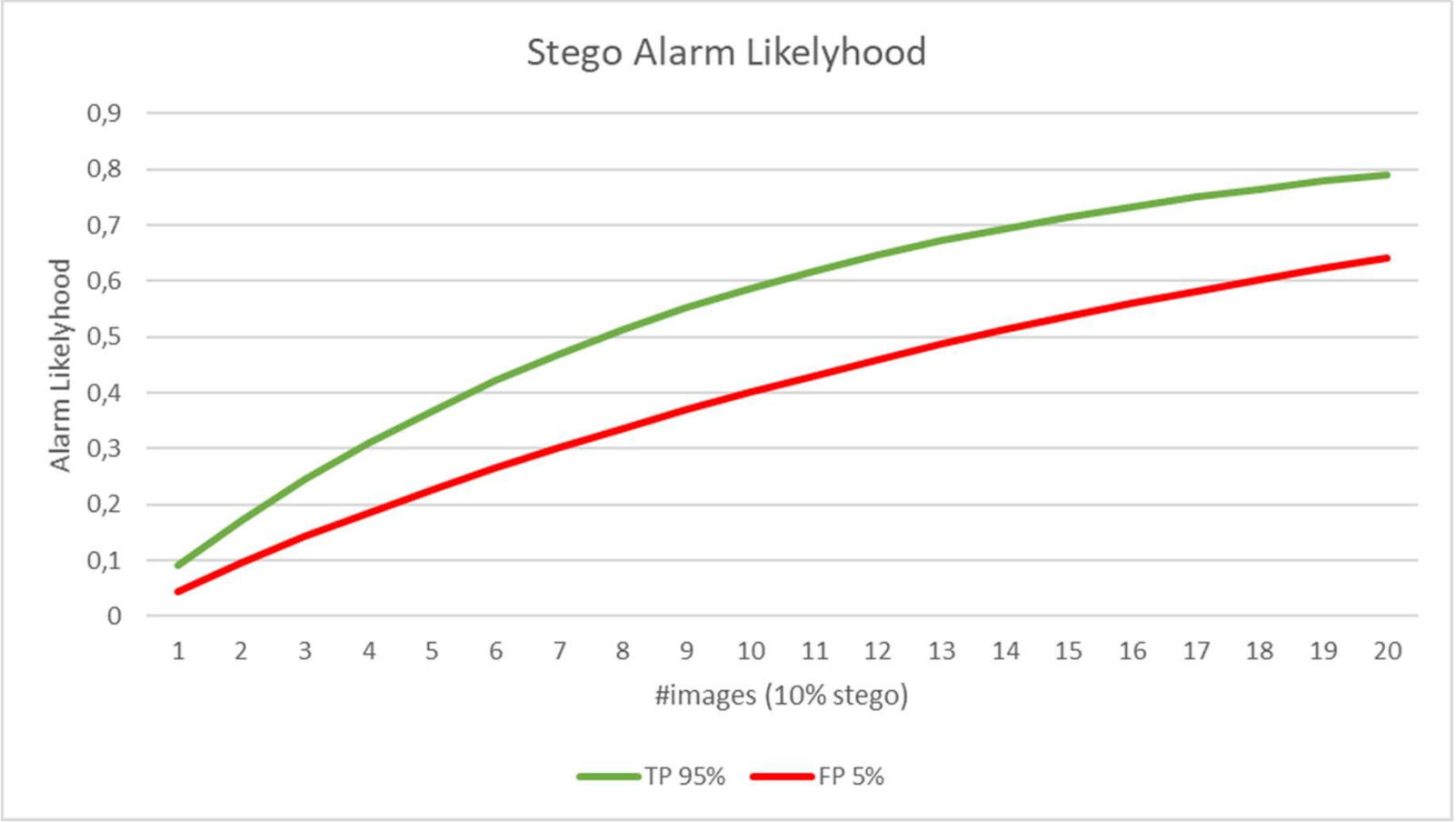
Basis Steganalyse

- Stego example and attack:
  - F5 by Westfeld
    - JPEG-based embedding
    - Modification of low frequency coefficient parity
  - Attack by Fridrichs
    - Detection of coefficient histogram changes
- Results depend on capacity used
  - FPR< 10% for big payload (long text)
    - FNR>60%
  - FPR> 30% for small payload (short message/ tweet)
    - FNR>75%

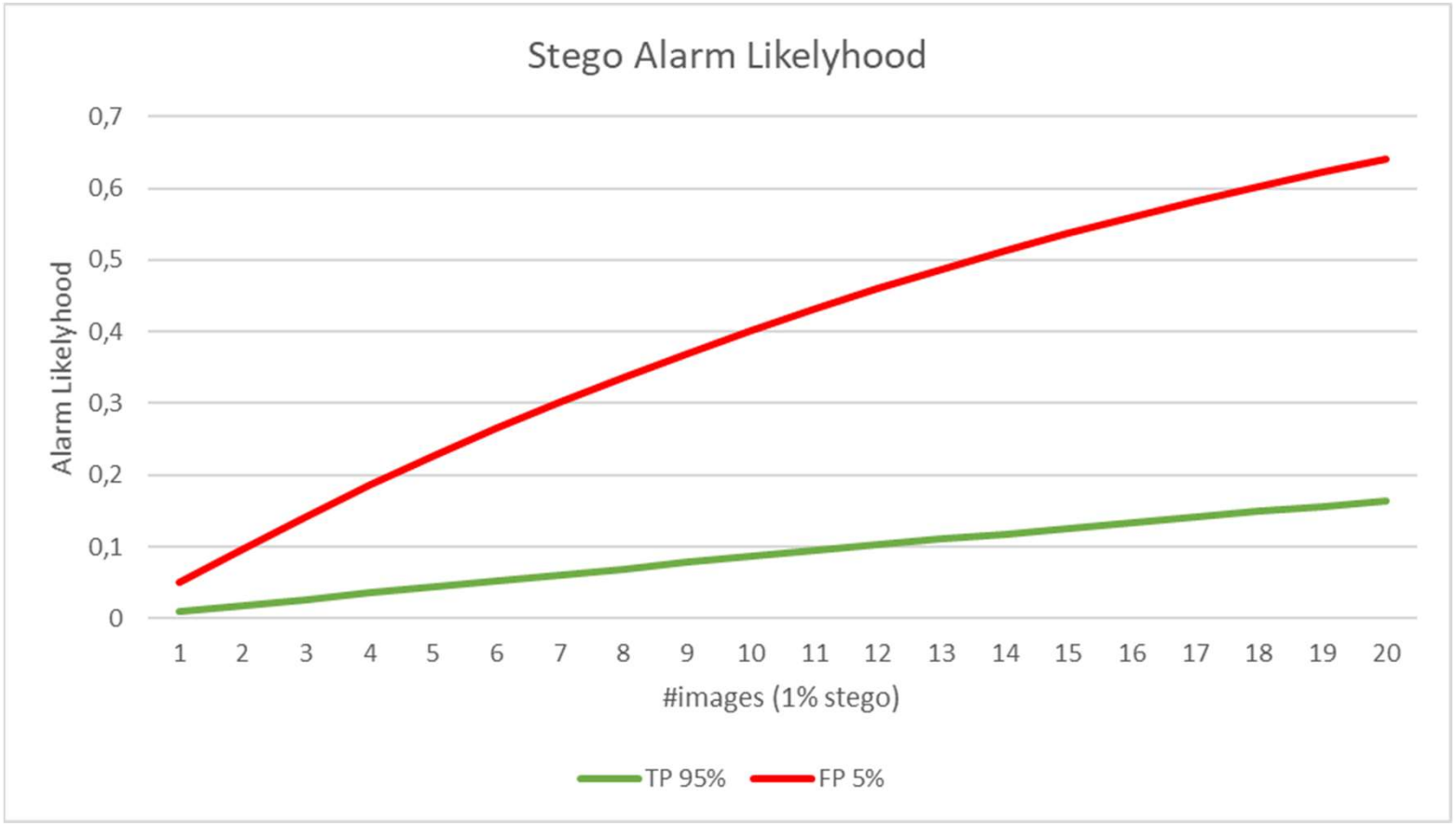
TPR vs FPR vs Stego Occurences (50%)



TPR vs FPR vs Stego Occurences (10%)



TPR vs FPR vs Stego Occurences (1%)



Stego attack: Double Embedding

- F5 increases number of coefficients 0 in JPEG file
  - Embedding at full capacity changes 50% of all potential bit / coefficients
  - Embedding twice increases number of changed bits
- Performance
  - FPR: 1,3%
  - FNR: 38%

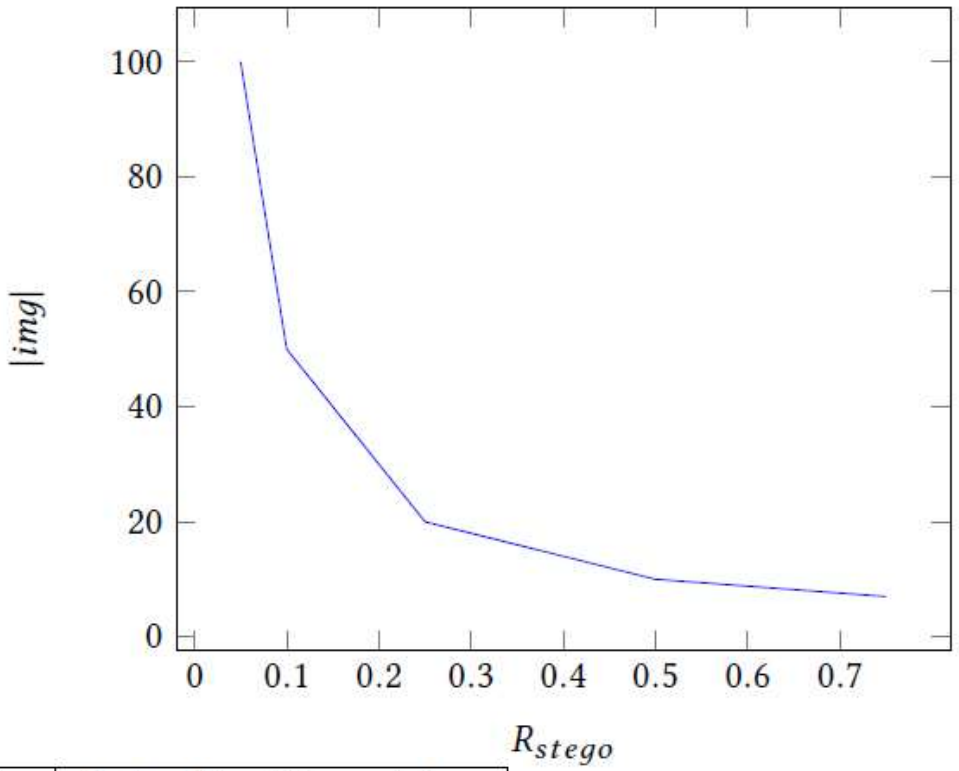
The Need for Steganalysis in Image Distribution Channels
Martin Steinebach, Huajian Liu and Andre Ester

https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/8/3/4

Stego attack: Capacity Estimation

- Estimation of capacity based on image size
- Testing by embedding and comparison of actual capacity
- Performance
  - FPR: 30%
  - FNR: <1%

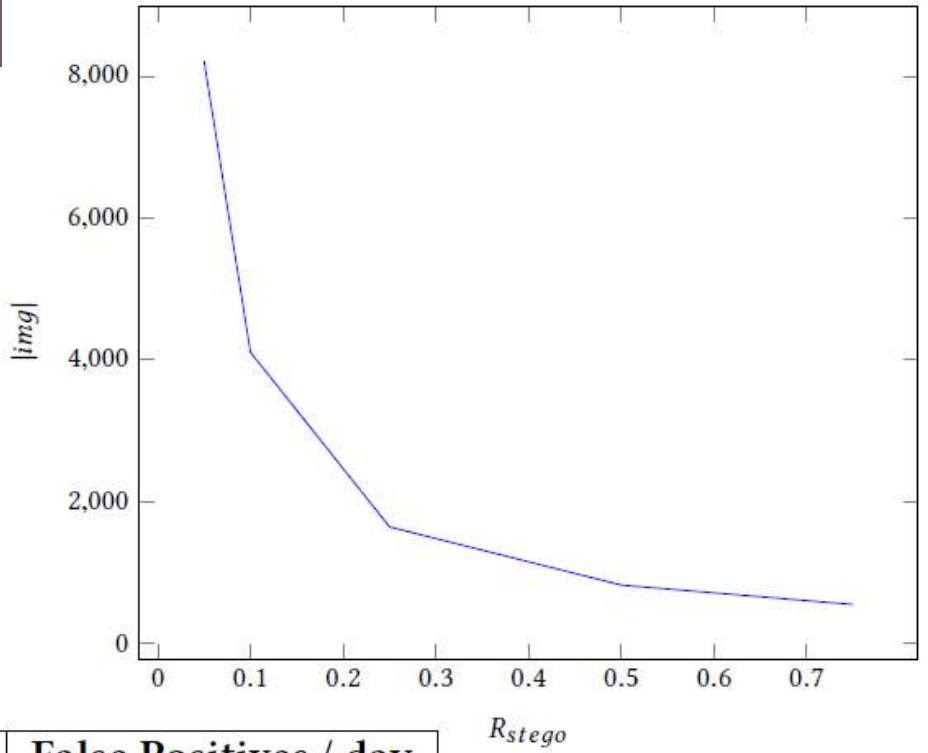
- False Positive Rate using Double Embedding Attack with Cap_{used}: 0.93
  - „best case“
  - TPR 93%



Threshold	False Positive Rate	False Positives / day
1 Positive	0.0039011703511	370611.1834
2 Positives	0.0000152191301	1445.82
3 Positives	0.0000000593724	5.64
4 Positives	0.0000000002316	0.022
5 Positives	0.0000000000009	0.00008584

FP/d 1

- False Positive Rate using Double Embedding Attack with Cap_{used}: 0.3
  - „worst case“
  - TPR 2,4%



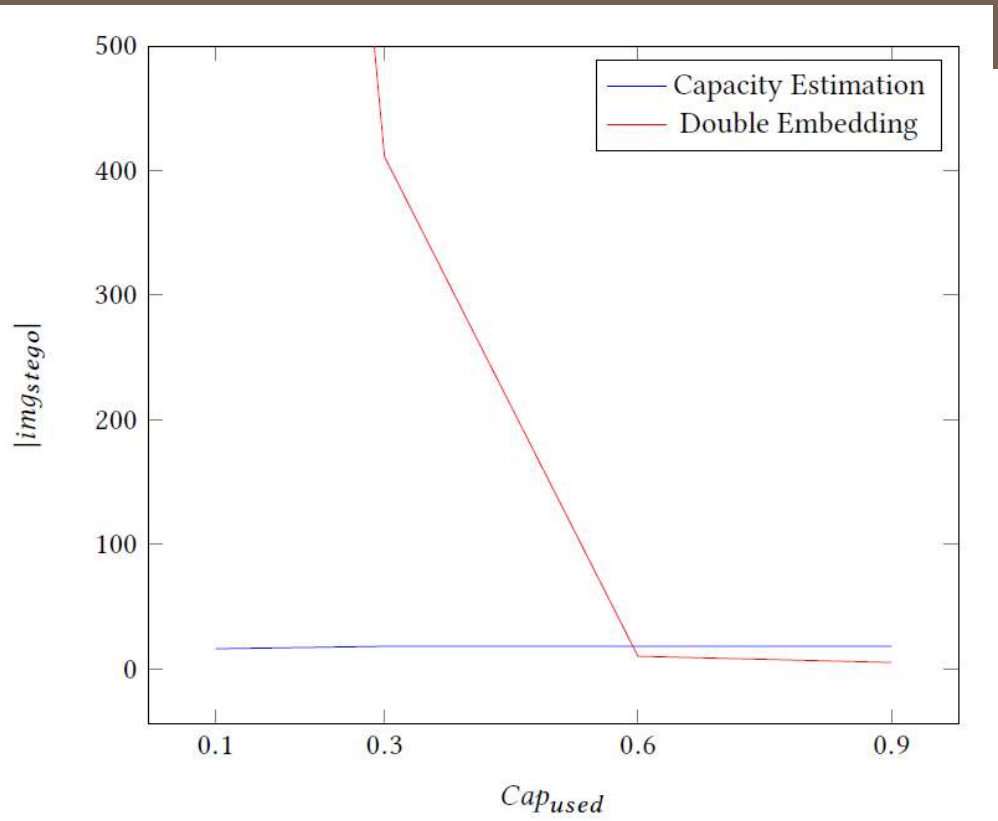
Threshold	False Positive Rate	False Positives / day
1 Positive	0.1304347826	12391304.3478
2 Positives	0.0170132325	1616257.0888
⋮	⋮	⋮
9 Positives	0.0000000109	1.0382
10 Positives	0.0000000014	0.1354

FP/d 1

- Network Wide Monitoring

  - False Positive Rate using Capacity Estimation Attack with Cap_{used}: 0.3
    - „worst case“

Threshold	False Positive Rate	False Positives / day
1 Positive	0.306846999	29150464.9197
2 Positives	0.094155081	8944732.6846
⋮	⋮	⋮
15 Positives	0.000000020	1.9123
16 Positives	0.000000006	0.5868



- R_{stego} 0.1
- Capacity Estimation attack outperforms Double Embedding at low capacity usage
- Double Embedding is only slightly better at high capacity usage

- Capacity Estimation Attack with Cap_{used}: 0.3
  - Best case
  - 100 images, R_{stego} 0,1
- 6 of 10 images need to be classified as stego
- Missing 5 stego images is extremly unlikely
- Less than 1 false alarm per 100 channels

Threshold	False Positive Rate	False Positives / 100 images
1 Positive	0.306846999	30.6847
⋮	⋮	⋮
4 Positives	0.008865179	0.8865
5 Positives	0.002720254	0.2720
6 Positives	0.000834702	0.0835

False Negatives	False Negative Rate	Occurrence / 100 images
1	0.00162074554295	0.162074554295
2	0.00000262681611	0.000262681611
3	0.00000000425740	0.000000425740
4	0.00000000000690	0.000000000690
5	0.00000000000001	0.000000000001

- Capacity Estimation Attack with Cap_{used}: 0.1

Threshold	False Positive Rate	False Positives / 100 images
1 Positive	0.306587838	30,6588
⋮	⋮	⋮
4 Positives	0.008835267	0.8835
5 Positives	0.002708785	0.2709
6 Positives	0.000830481	0.0830

Steganographie/ Wie sicher ist Steganographie?

- Was meinen wir jetzt mit „sicher“ ?
  - Vertraulich: Ja, wenn man „Geheimnis“ des Auslesens nicht kennt
  - Authentizität: Symmetrisch – „Geheimnis“ gleicht einem Schlüssel
  - Integrität?
  - ....

Steganographie/ Wie sicher ist Steganographie?

- Steganographie ermöglicht eine vertrauliche und unverdächtige Kommunikation.
- Steganographie kann durch automatisches leichtes Stören von C oft unterbinden
- Steganographie hat das gleiche Problem wie die Symmetrische Verschlüsslung
- Der *naive* Schlüsselraum ist sehr begrenzt

Steganographie/ Wie sicher ist Steganographie?

- Der *naive* Schlüsselraum ist sehr begrenzt
  - Wenn es nur um das Geheimnis, wie Informationen eingebettet wird, geht
- Erweiterung: Verknüpfung mit Kryptogaphie
  - M wird verschlüsselt
  - Nicht jeder möglicher Punkt wird genutzt, sondern nur die pseudozufällig gezogenen
  - ...

Steganographie/ Wie sicher ist Steganographie?

- Was kann gegen die einfache Störung / das einfache Entfernen unternommen werden?
  - Redundanz
  - Fehlerkorrigierende Codes
  - Stärkere Änderung des Originals
    - Höhere Bitwerte (Im LSB-Beispiel)

  - Dadurch erzeugen wir **ROBUSTHEIT**

Steganographie/ Überleitung Wasserzeichen

- Herausforderung Mediensicherheit:
  - Urheberschutz
- Macht hier Steganographie Sinn?
  - Ja, wenn man zum Beweis der Urheberschaft einen Schlüssel „zückt“ und mit ihm eine Information aus dem Medium extrahiert
  - Aber:
    - K muss sicher sein
    - M muss schwer aus C entfernbar sein