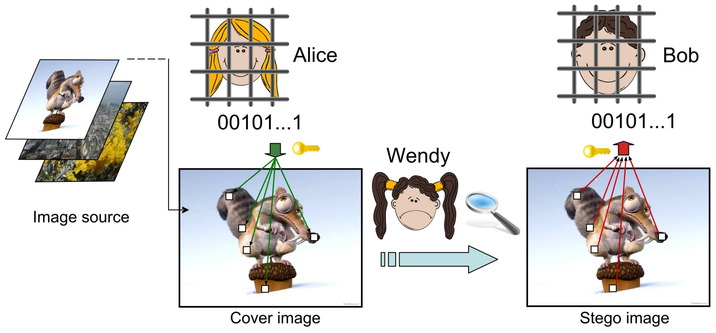
The Square Root Law of Steganographic Capacity

BINGHAMTON UNIVERSITY
State University of New York

Tomáš Filler, Jessica Fridrich
Department of Electrical and Computer Engineering, SUNY Binghamton, USA

Steganography

Steganography is a mode of covert communication.



Alice communicates with Bob by hiding her messages inside innocuous looking (cover) objects. Most practical steganographic methods embed messages by slightly modifying individual elements of the cover, obtaining thus the modified stego object that conveys the hidden message. Stego objects should be statistically indistinguishable from covers.

Perfectly secure stegosystem:

Cover distribution P and stego distribution Q satisfy $D_{KL}(P||Q) = 0$.

- exist only for artificial cover sources
- all known stegosystems for real digital media are **imperfect**, $D_{KL}(P||Q) = \varepsilon > 0$, and detectors exist.

Secure payload:

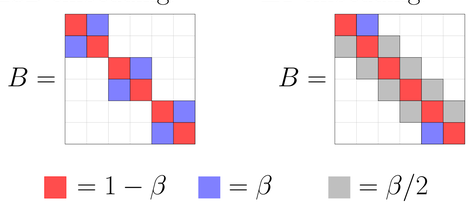
Number of bits Alice can send using a specific method in an n-element cover at fixed risk.

- known to be **linear** in n for perfectly secure stegosystems.
- unknown for imperfect stegosystems.

Mutually independent (MI) embedding model

We model the impact of embedding by a probabilistic mapping acting on each cover element (pixel, DCT, ...) independently.

LSB embedding: $B =$ ± 1 embedding: $B =$



B captures probabilistic impact of embedding

β denotes relative number of changes

Square Root Law of Imperfect Steganography

Secure payload of imperfect stegosystems scales as $r\sqrt{n}$.

Assumptions:

1. COVER SOURCE - Markov Chain
   Warden can always extract statistics in this form and use it for steganalysis.
2. EMBEDDING ALGORITHM - MI embedding
   Many practical schemes of our interest work by introducing indep. changes.
3. STEGOSYSTEM - imperfect stegosystem
   We believe that it is hard to preserve all statistics of complex cover source.

Theorem:

Embedding payload that grows

slower than $\sqrt{n}$	exactly as $\sqrt{n}$	faster than $\sqrt{n}$
$\Downarrow$	$\Downarrow$	$\Downarrow$
asymptot. perfectly secure stegosystem	$D_{KL}(P\|\|Q) < \varepsilon$	perfectly detectable stegosystem.

Quick & dirty proof for i.i.d sources: ($n\beta = \#$ of changes)

$$D_{KL}\left(P^{(n)}||Q_\beta^{(n)}\right) = \frac{1}{2}n\beta^2\mathtt{I} + O(\beta^3) = \varepsilon$$

$$\frac{1}{2}n\beta^2\mathtt{I} \approx \varepsilon \quad \Rightarrow \quad n\beta \approx \sqrt{\frac{1}{\mathtt{I}}}\sqrt{2\varepsilon n}$$

$\mathtt{I}$ ... Fisher information (rate) at $\beta = 0$.

Root rate: (more refined measure of capacity)

$$r \approx \frac{1}{\sqrt{\mathtt{I}}}$$

Describes how many bits can be embedded per $\sqrt{n}$ and per $\sqrt{D_{KL}}$.

Experimental verification - JPEG images [2]

Detectability is measured as probability of error

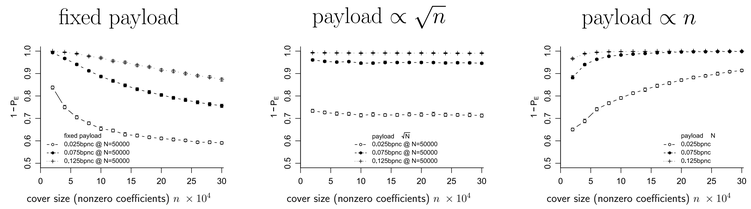
$$P_E = \frac{1}{2}\min(P_{FA} + P_{MD})$$

of an SVM classifier.

- $P_E = 0$ ... perfectly detectable steganography
- $P_E = 1$ ... perfectly **un**detectable steganography.

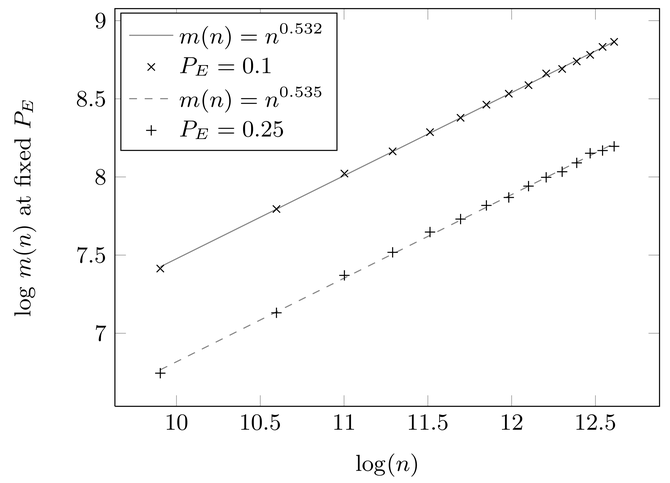
Comparison of different embedding strategies:

Detectability as a function of cover size for different embedding strategies.



Largest secure payload for fixed P_E:

Largest payload $m(n)$ embedded using nsF5 that produces a fixed steganalyzer error, P_E, for images with n non-zero DCT coefficients.



Conclusion

Secure payload of practical stegosystems that embed in digital media grows with the square root of the cover size. This phenomenon has been experimentally confirmed.

References

[1] T. Filler, J. Fridrich, and A. D. Ker. The square root law of steganographic capacity for Markov covers. In *Proceedings SPIE, Electronic Imaging, Security and Forensics of Multimedia XI*, San Jose, CA, 2009.

[2] A. D. Ker, T. Pevný, J. Kodovský, and J. Fridrich. The square root law of steganographic capacity. In *Proceedings of the 10th ACM Multimedia & Security Workshop*, Oxford, UK, 2008.