The Square Root Law of Steganographic Capacity for Markov Covers

Tomáš Filler(1), Andrew D. Ker(2) and Jessica Fridrich(1)

(1) Dept. of Electrical and Computer Engineering, SUNY Binghamton
(2) Oxford University Computing Laboratory, Oxford, United Kingdom

IS&T/SPIE 2009, San Jose, CA

Steganographic Capacity

Capacity of the steganographic channel:
number of bits that can be transmitted in n-element cover without possible detection by the passive warden.

Perfectly secure stegosystem:
cover and stego distributions are identical — no statistical test can detect the presence of the message.

Assuming full knowledge of the cover source, it is known that the capacity of perfectly secure stegosystems is linear in n.

Communication rate of perfectly secure stegosystems is non-vanishing.

[Wang, Moulin - 2004]

Imperfect Stegosystems

Imperfect stegosystem:
cover and stego distributions are different — statistical detectors exist.

- perfectly secure stegosystems exist for artificial cover sources
- all known stegosystems for digital media are imperfect
- digital media cover sources will hardly ever be perfectly understood

What is the capacity of ε-secure imperfect stegosystems?

Many hints suggest that the capacity is sublinear.

Capacity of Imperfect Stegosystems

Capacity of imperfect stegosystems is sublinear.

- Anderson (1996) 1st International Hiding Workshop

"Thanks to the Central Limit Theorem, the more covertext we give the Warden, the better he will be able to estimate its statistics, and so the smaller the rate at which [the Steganographer] will be able to tweak bits safely. The rate might even tend to zero..."

- Ker (2007 & 2008)
  analysis of batch steganography and pooled steganalysis

Capacity of Imperfect Stegosystems

Capacity of imperfect stegosystems is sublinear.

- Anderson (1996) 1st International Hiding Workshop
- Ker (2007 & 2008)
  analysis of batch steganography and pooled steganalysis

Steganographic capacity of imperfect stegosystems only grows as the square root of the number of communicated covers

Problem investigated in this paper:

Square Root Law of imperfect steganography
for covers that allow dependencies (Markov chains)

Square Root Law of Markov Covers

Stegosystem is imperfect due to the lack of the full knowledge of the cover source.

Kerckhoffs' principle:

Warden knows the embedding algorithm and cover source

Basic assumptions:

1. cover source = first order Markov chain
2. embedding operation = indep. substitutions of states
3. stegosystem is NOT perfectly secure

Markov cover source:

- use suitable representation of the cover
- first-order stat., higher order stat. (Markov chain)

Mutually Independent Embedding Operation

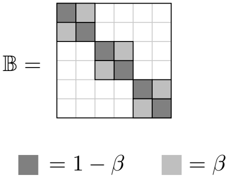
Embedding operation can be modeled as independent substitution of one state for another - MI embedding.

$$Pr(Y_k = j | X_k = i) = b_{ij}(\beta)$$

X_k ... k-th cover element
Y_k ... k-th stego element
β ... change rate (rel. payload)

- can be found in majority of practical methods
- examples: ± 1, LSB, F5, nsF5
- analytically tractable - stego objects form Hidden Markov Chain

LSB embedding:



Square Root Law of Markov Covers

Under the assumptions of Markov covers, MI embedding, and imperfect stegosystem, we prove the following theorem.

Theorem (SRL for Markov Covers):

1. embedding payload that grows slower than $\sqrt{n}$ leads to eventual ε-security for arbitrarily small $\varepsilon > 0$
2. embedding payload that grows exactly as $A\sqrt{n}$ leads to ε-secure stegosystem with fixed $\varepsilon > 0$
3. embedding payload that grows faster than $\sqrt{n}$ leads to eventual detection with arbitrary P_{FA} and P_{MD}

This implies that the steganographic capacity of imperfect stegosystems with Markov covers and MI embedding scales as $A\sqrt{n}$.

SRL Proof 1&2/3 - Undetectability & ε-security

embedding payload that grows slower than $\sqrt{n}$ leads to eventual ε-security for arbitrarily small $\varepsilon > 0$

β ... change per pixel $\Rightarrow$ βn ... total number of changes

Assume cover is i.i.d. P $\Rightarrow$ stego is i.i.d. Q_β $\quad (Q_0 = P)$

KL divergence between n-pixel cover and stego:

$$D_{KL}\left(P^{(n)}||Q_\beta^{(n)}\right) = nD_{KL}\left(P||Q_\beta\right) = \frac{1}{2}n\beta^2 I(0) + O(\beta^3)$$

$I(0)$ ... Fisher Information at $\beta = 0$ $\quad (0 < I(0) < C)$

if $\lim_{n\to\infty} \frac{\beta n}{\sqrt{n}} = 0$ then $D_{KL}\left(P^{(n)}||Q_\beta^{(n)}\right) \to 0$

SRL Proof 3/3 - Existence of The Detector

Cover is i.i.d. $P \Rightarrow$ stego is i.i.d. Q_β and $Q_\beta[i] = P[i] + \beta c_i$

embedding payload that grows faster than $\sqrt{n}$ leads to detection with arbitrarily small errors

Problem: decide H_0 : cover ($\beta = 0$) or H_1 : stego ($\beta > 0$).

$$T_\beta(Y) = \sqrt{n}\left(\frac{1}{n}\mathbb{I}_{\{Y=i\}} - P[i]\right)$$

β ... change rate
Y ... data vector of length n
$\mathbb{I}_{\{Y=i\}}$ ... # of k, where $Y_k = i$

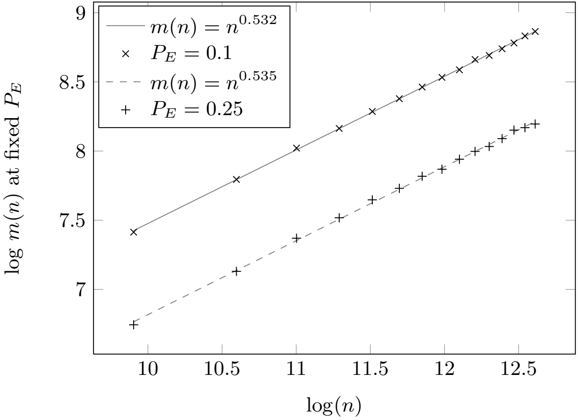
difference of means under both hypotheses

$$E\left[T_\beta - T_0\right] = \sqrt{n}\left(Q_\beta[i] - P[i]\right) = \sqrt{n}\beta c_i$$

if $\lim_{n\to\infty} \frac{\beta n}{\sqrt{n}} = \infty$ then $E\left[T_\beta - T_0\right] \to \infty$

SRL - Experimental Verification - F5

Largest payload $m(n)$ embedded using F5 that produces a fixed steganalyzer error, P_E, for images with n non-zero DCT coefficients.



[Ker et al., The Square Root Law of Steganographic Capacity, ACM, 2008]

Conclusion

There is a wide range of situations in which secure capacity grows as square root of the cover size.

Square Root Law:

- secure capacity $\approx A\sqrt{n}$ — rate is vanishing
- holds for imperfect stegosystems
- first formal proof alowing dependency between pixels
- applies to number of changes
- Matrix Embedding $\Rightarrow$ secure capacity $\approx A\sqrt{n}\log n$

Consequences and Future Directions

Consequences:

- same relative payload is easier to detect in larger covers
- distribution of image sizes in database in steganalysis

Cover model mismatch $\Rightarrow$ sub-linear capacity.

Future directions:

- if secure capacity scales as $A\sqrt{n}$ then
  how to use constant A to compare stegosystems

Consequences and Future Directions

Consequences:

- same relative payload is easier to detect in larger covers
- distribution of image sizes in database in steganalysis

Cover model mismatch $\Rightarrow$ sub-linear capacity.

Future directions:

- if secure capacity scales as $A\sqrt{n}$ then
  how to use constant A to compare stegosystems

Thank you!

tomas.filler@binghamton.edu