Steganographic Strategies for a Square Distortion Function

Andrew Ker
adk@comlab.ox.ac.uk

Royal Society University Research Fellow
Oxford University Computing Laboratory

SPIE/IS&T Electronic Imaging, San Jose, CA
28 January 2008
Steganographic Strategies for a Square Distortion Function

Outline

• The “Batch Steganography” problem
• Square distortion
• Optimal batch embedding strategies

• The “Sequential Steganography” problem
• Sequential embedding strategies
• Example
Batch Steganography

- *Spreading a payload amongst multiple covers*
Alice

payload size $M$

embedding

N covers

embed $m_1$ bits making $p_1$ changes

embed $m_2$ bits making $p_2$ changes

embed $m_3$ bits making $p_3$ changes

... 

embed $m_N$ bits making $p_N$ changes

Warden

$X_1^{p_1}$ $X_2^{p_2}$ $X_3^{p_3}$ ... $X_N^{p_N}$

Square Distortion

**Notation**

**Observation of cover $i$, with $p_i$ embedding changes:**

Random vector of $N$ cover objects:

Random vector of $N$ stego (or cover) objects:

For the purposes of this paper we assume:

- That “evidence” is modelled by KL divergence.
- That KL divergence is additive across objects.
- That KL divergence in a single object is proportional to the square of the number of changes induced by embedding.

\[
D_{KL}(X^0, X^p) = \sum_{i=1}^{n} D_{KL}(X^0_i, X^p_i) = \sum_{i=1}^{n} Q_i p_i^2
\]
Optimization Problems

Want to maximize total payload transmitted $M$, subject to limit on allowable KL divergence:

$$D_{KL}(X^0, X^p) = \sum_{i=1}^{N} Q_i p_i^2 \leq D$$

There are a number of variations:

1. Uniform covers, simple embedding (no adaptive source coding)
2. Nonuniform covers, simple embedding (no adaptive source coding)
3. Uniform covers, adaptive source code at embedder
Theorem

Distortion bound:
\[ D_{KL}(X^0, X^p) = \sum_{i=1}^{N} Q_i p_i^2 \leq D \]

Uniform covers:
\[ Q_i = Q \]
(identical Q-factor)

No adaptive source coding:
\[ p_i = m_i/e \]
(each embedding change transmits e payload bits)

The optimization problem is

Maximize \[ M = \sum m_i \] s.t. \[ \frac{Q}{e^2} \sum m_i^2 \leq D \]

and the solution is
\[ m_i = \sqrt{\frac{De^2}{NQ}}, \quad M = \sqrt{\frac{De^2N}{Q}} = O(\sqrt{N}). \]
Theorem

**Distortion bound:**

\[ D_{KL}(X^0, X^p) = \sum_{i=1}^{N} Q_i p_i^2 \leq D \]

**Uniform covers:**

\[ Q_i = Q \]

*(identical Q-factor)*

**Adaptive source coding:**

\[ p_i = n H^{-1} \left( \frac{m_i}{n} \right) \]

*(asymptotically achievable bound [1])* 

The optimization problem is

Maximize \[ M = \sum m_i \]

s.t. \[ \frac{Q}{n} \sum m_i^2 \leq D \]

and the solution is

\[ m_i = \sqrt{\frac{D e^2}{N Q}}, \]

\[ n H \left( \sqrt{\frac{D}{N Q n^2}} \right), \]

\[ M = \sqrt{\frac{D e^2 N}{Q}} n H \left( \sqrt{\frac{D}{N Q n^2}} \right) = O(\sqrt{N}). \]

\[ O(\sqrt{N} \log N). \]

Sequential Steganography

- *Embedding a hidden payload stream in an infinite stream of covers*
Alice

payload stream

infinite stream of covers

embedding

\[ \text{embed } m_1 \text{ bits making } p_1 \text{ changes} \]

\[ \text{embed } m_2 \text{ bits making } p_2 \text{ changes} \]

\[ \text{embed } m_3 \text{ bits making } p_3 \text{ changes} \]

\[ \vdots \]

\[ \text{embed } m_N \text{ bits making } p_N \text{ changes} \]

\[ \text{embed } m_{N+1} \text{ bits making } p_{N+1} \text{ changes} \]

\[ \vdots \]

Warden

any?

\[ X_1^{p_1}, X_2^{p_2}, X_3^{p_3}, \ldots, X_N^{p_N} \]
Distortion Bound

Want to maximize payload transmitted $M$, as a function of $N$, subject to limit on allowable KL divergence:

$$\sum_{i=1}^{N} Q_i p_i^2 \leq D \quad \text{for all } N.$$
Distortion Bound

Want to maximize payload transmitted $M$, as a function of $N$, subject to limit on allowable KL divergence:

$$\sum_{i=1}^{\infty} Q_i p_i^2 \leq D$$
Sequential Strategies

*Distortion bound:* $\sum_{i=1}^{\infty} Q_i d_i^2 \leq D$

*Uniform covers:* $Q_i = Q$

*No adaptive source coding:* $p_i = m_i / e$

The “optimization” problem is

Find a sequence $(m_i)$ whose partial sums $M(N) = \sum_{i=1}^{N} m_i$ grow as fast as possible, given that $\sum m_i^2$ converges.

Theorem $\sum m_i^2$ convergent forces $M(N)/\sqrt{N} \rightarrow 0$.

Zeta Embedding Set $m_i = i^{-\frac{1}{2} - \epsilon} \sqrt{D e^2 / Q \zeta(1 + 2\epsilon)}$

Then $(*)$ is equality and

$$M(N) \sim N^{1/2 - \epsilon} \frac{e}{\sqrt{\frac{D}{Q \zeta(1 + 2\epsilon)}}}$$
Sequential Strategies

**Distortion bound:** \( \sum_{i=1}^{\infty} Q_i p_i^2 \leq D \)

**Uniform covers:** \( Q_i = Q \)

**Adaptive source coding:** \( p_i = \frac{m_i/e}{nH^{-1}(\frac{m_i}{n})} \)

The “optimization” problem is

Find a sequence \((m_i)\) whose partial sums \( M(N) = \sum_{i=1}^{N} m_i \) grow as fast as possible, given that \( \sum m_i^2 \) converges.

**Theorem** \( \sum m_i^2 \) convergent forces \( M(N)/\sqrt{N} \to 0. \)

**Zeta Embedding** Set \( m_i = i - \frac{1}{2} - \epsilon \sqrt{De^2/Q\zeta(1+2\epsilon)} \)

Then \((*)\) is equality and

\[
M(N) \sim (\log_2 N)N^{\frac{1}{2} - \epsilon} \frac{1}{1 - \epsilon} \sqrt{\frac{D}{Q\zeta(1+2\epsilon)}}
\]
Illustration

We compute some theoretical capacities with parameters corresponding to realistic steganography/steganalysis.

- The cover size corresponds to a 1 megapixel grayscale image. $n = 10^6$
- Embedding by LSB matching, no source coding. $e = 2$
- The KL divergence bound forces detector’s ROC into unshaded region: $D = 1$

No source coding

With matrix embedding
**Conclusions**

- In the batch steganography case, capacity grows with the square-root of the number of covers $N$.

  *With adaptive source coding this improves to $O(\sqrt{N} \log N)$.*

- The sequential steganography gives different results: capacity can be infinite, but only order $N^{\frac{1}{2} - \epsilon}$ is achievable.

  *Adaptive source coding gives an extra factor of $\log N$.*

- The whole paper is predicated on the assumption of square distortion.

  *Some theoretical and experimental justification exists, but it is not necessarily universally true.*

- Some other unrealistic assumptions (fractional bit payload, etc.) do not seem critical.