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

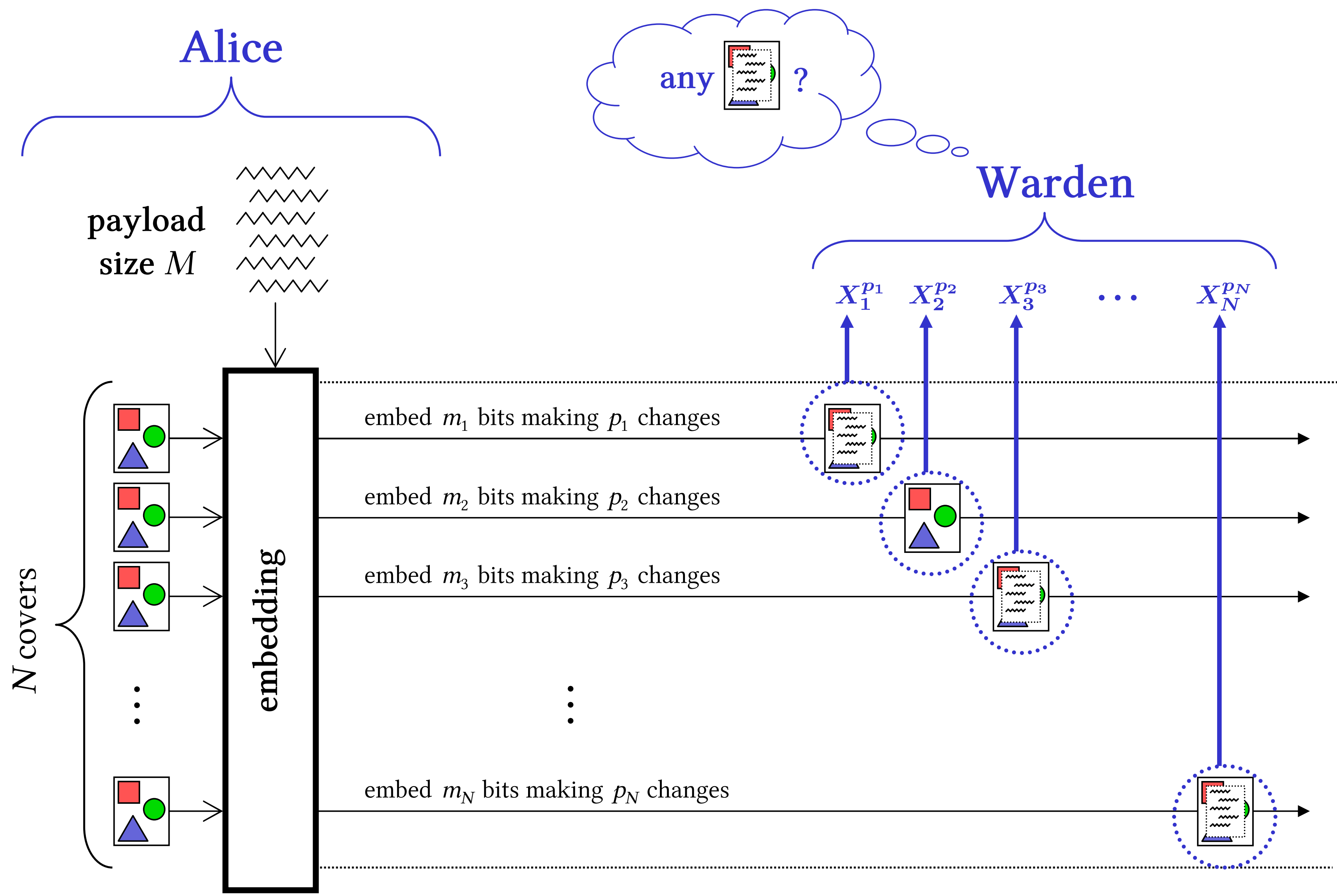
Outline

- *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*



A. Ker, *Batch Steganography & Pooled Steganalysis,* Proc. 8th Information Hiding Workshop, Springer LNCS, 2006.

Square Distortion

Notation

Observation of cover i, with p_i embedding changes: $X_i^{p_i}$

Random vector of N cover objects: $\boldsymbol{X^0} = (X_1^0, \ldots, X_N^0)$

Random vector of N stego (or cover) objects: $\boldsymbol{X^p} = (X_1^{p_1}, \ldots, X_N^{p_N})$

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.

$$D_{\mathrm{KL}}(\boldsymbol{X^0}, \boldsymbol{X^p}) = \sum_{i=1}^{n} D_{\mathrm{KL}}(X_i^0, X_i^{p_i}) = \sum_{i=1}^{n} Q_i p_i^2$$

Optimization Problems

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

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

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

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

$$\textbf{Maximize} \qquad M = \sum m_i \qquad \textbf{s.t.} \qquad \tfrac{Q}{e^2} \sum m_i^2 \leq D$$

and the solution is

$$m_i = \sqrt{\tfrac{De^2}{NQ}}, \qquad M = \sqrt{\tfrac{De^2 N}{Q}} = O(\sqrt{N}).$$

Theorem

Distortion bound: $D_{\mathrm{KL}}(\boldsymbol{X^0}, \boldsymbol{X^p}) = \sum_{i=1}^{N} Q_i p_i^2 \le D$

Uniform covers: $Q_i = Q$

(identical Q-factor)

Adaptive source coding: $p_i = nH^{-1}\left(\frac{m_i}{n}\right)$

(asymptotically achievable bound [1])

The optimization problem is

$$Qn^2 \sum \left(H^{-1}\left(\frac{m_i}{n}\right)\right)^2$$

$$\textbf{Maximize} \qquad M = \sum m_i \qquad \textbf{s.t.} \qquad \cancel{\frac{Q}{e^2}\sum m_i^2} \le D$$

and the solution is

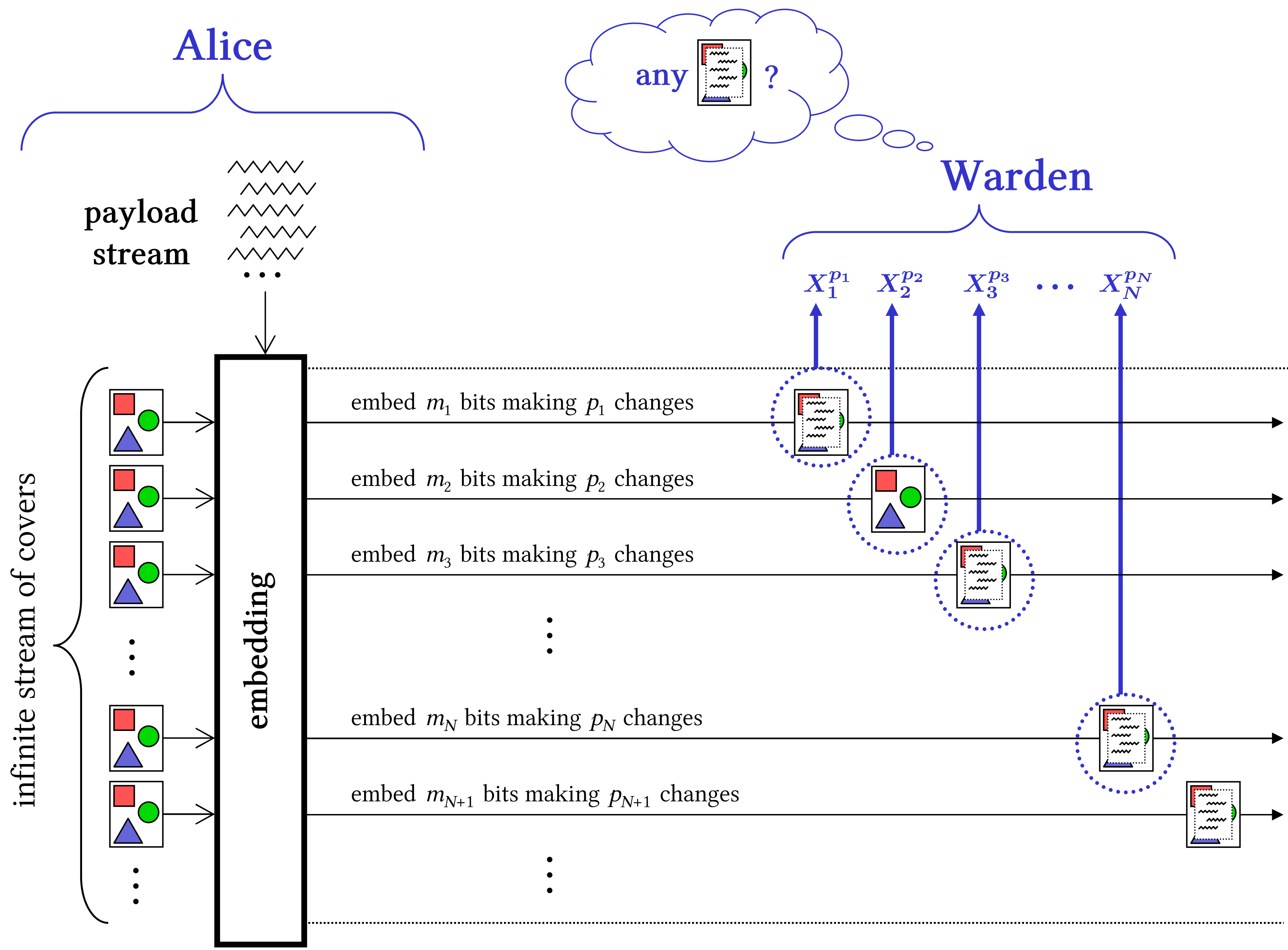
$$m_i = \cancel{\sqrt{\frac{De^2}{NQ}}}, \quad nH\left(\sqrt{\frac{D}{NQn^2}}\right) \qquad M = \cancel{\sqrt{\frac{De^2N}{Q}}} \; nNH\left(\sqrt{\frac{D}{NQn^2}}\right)$$

$$= \cancel{O(\sqrt{N})}. \quad O(\sqrt{N}\log N).$$

[1] J. Fridrich & D. Soukal, *Matrix embedding for large payloads*, IEEE Trans Info. Forensics & Security, 2006.

Sequential Steganography

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


Alice
payload stream
any ?
Warden
$X_1^{p_1}$ $X_2^{p_2}$ $X_3^{p_3}$ … $X_N^{p_N}$
infinite stream of covers
embedding
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
embed m_{N+1} bits making p_{N+1} changes

Distortion Bound

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

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

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

$$\left.\begin{array}{rl} \textit{Distortion bound:} & \sum_{i=1}^{\infty} Q_i p_i^2 \le D \\ \textit{Uniform covers:} & Q_i = Q \\ \textit{No adaptive source coding:} & p_i = m_i/e \end{array}\right\} \qquad \sum_{i=1}^{\infty} m_i^2 \le \frac{De^2}{Q} \quad (*)$$

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.**

<u>Theorem</u> $\sum m_i^2$ convergent forces $M(N)/\sqrt{N} \to 0$.

<u>Zeta Embedding</u> Set $m_i = \boldsymbol{i^{-\frac{1}{2}-\epsilon}} \sqrt{De^2/Q\zeta(1+2\epsilon)}$

Then $(*)$ is equality and

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

Sequential Strategies

Distortion bound: $\sum_{i=1}^{\infty} Q_i p_i^2 \le D$

Uniform covers: $Q_i = Q$

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

$$\cancel{\sum_{i=1}^{\infty} m_i^2 \le \frac{De^2}{Q}} \quad (*)$$

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** $\sum \cancel{m_i^2}$ **converges.**

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

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

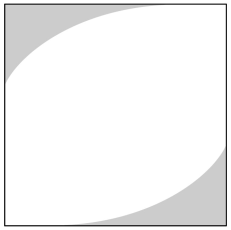
Then $(*)$ is equality and

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

Illustration

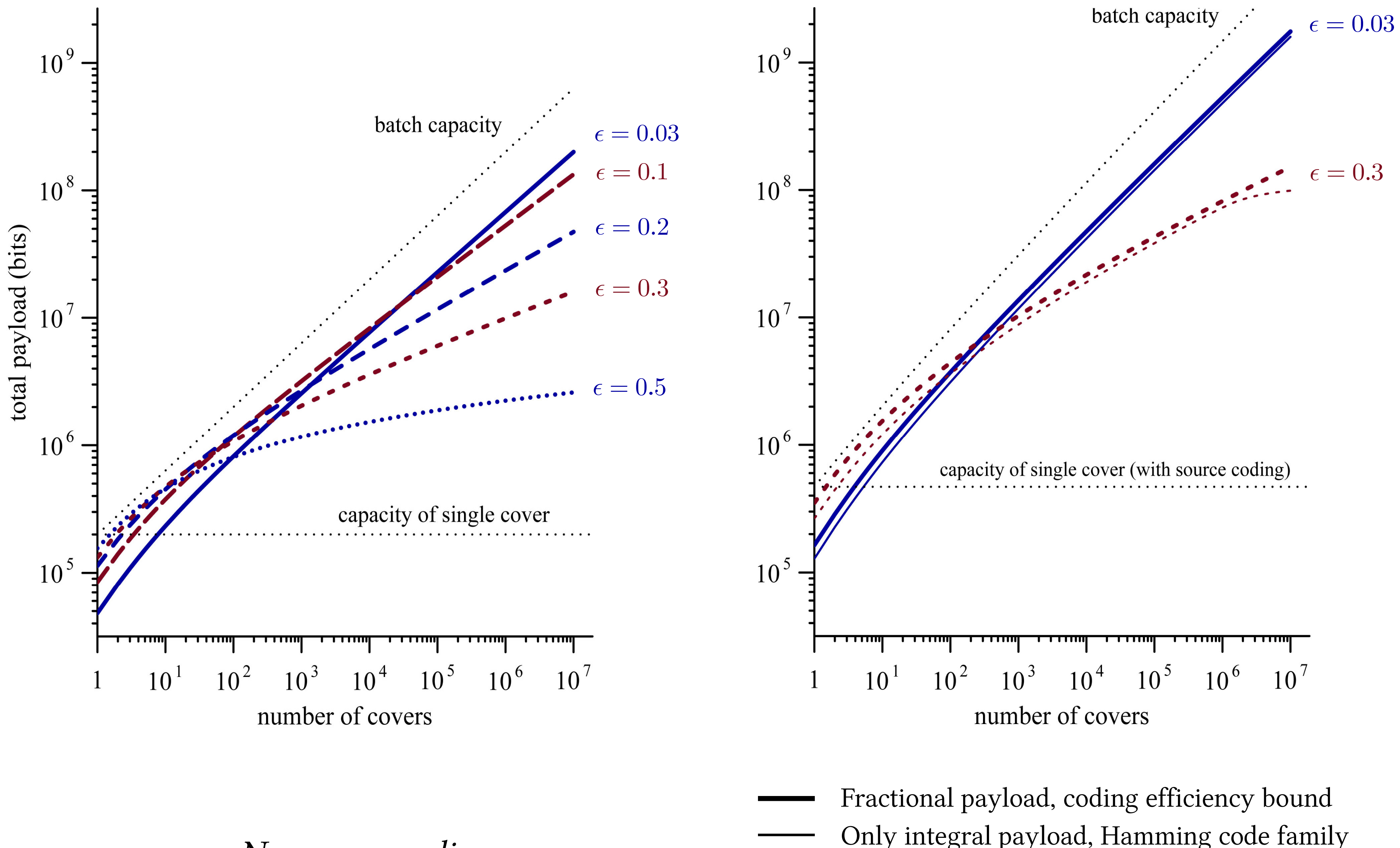
We compute some theoretical capacities with parameters corresponding to realistic steganography/steganalysis.

- The cover size corresponds to a 1 megapixel grayscale image. $n = 10^6$
- Embedding by LSB matching, no source coding. $e = 2$
- Calibrated HCF COM steganalysis [1] at detector.
  A realistic Q-factor [2] is... $Q = 10^{-10}$
- The KL divergence bound forces detector's ROC into unshaded region: $D = 1$



[1] A. Ker, *Steganalysis of LSB Matching in Grayscale Images*, IEEE Signal Processing Letters, 2005.

[2] A. Ker, *The Ultimate Steganalysis Benchmark?*, *Proc. ACM Workshop on Multimedia and Security*, 2007.



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.

End

adk@comlab.ox.ac.uk