Estimating the Information Theoretic Optimal Stego Noise

Andrew Ker

adk@comlab.ox.ac.uk

Royal Society University Research Fellow

Oxford University Computing Laboratory

8th International Workshop on Digital Watermarking

University of Surrey, 25 August 2009

Estimating the Information Theoretic Optimal Stego Noise

Outline

- *Optimality*
  - *the square root law of capacity*
  - *Steganographic Fisher Information*
- *Embedding*
  - *(mod k)-matching*
  - *convex combinations*
- *Experimental results: optimal embedding*

Capacity

The capacity problem is: given fixed

- cover source,
- embedding method,
- limit on "risk" (maximum probability of detection),

what is the largest payload which can safely be embedded?

The square root law says:

the capacity is asymptotically proportional to the square root of the size of the cover.

- Proved for multiple independent covers (Ker, 2007; Ker, 2008).
- Proved for individual Markov chain covers (Filler, Ker, & Fridrich, 2009).
- Verified empirically (Ker, Pevný, Kodovský, & Fridrich, 2008).

Optimality

If the cover size is n, the max payload size m follows

$$m \sim r\sqrt{n},$$

where r is the "root rate".

Optimal embedding method: gives the highest the root rate.

If $P(\lambda)$ is distribution of images from a particular source, embedded with payload rate λ using a particular embedding method, for small λ

$$D_{\mathrm{KL}}(P(0) \,\|\, P(\lambda)) \sim \tfrac{1}{2} I \lambda^2.$$

I is the **Steganographic Fisher Information (SFI)** for this embedding w.r.t. this source. It measures the **evidence** of embedding.

A. Ker. *The Ultimate Steganalysis Benchmark?* Proc. ACM Workshop on Multimedia & Security, 2007.

Optimality

If the cover size is n, the max payload size m follows

$$m \sim r\sqrt{n},$$

where r is the "root rate".

Optimal embedding method: gives the highest the root rate.

If $P(\lambda)$ is distribution of images from a particular source, embedded with payload rate λ using a particular embedding method, for small λ

$$D_{\mathrm{KL}}(P(0) \,\|\, P(\lambda)) \sim \tfrac{1}{2} I \lambda^2.$$

I is the **Steganographic Fisher Information (SFI)** for this embedding w.r.t. this source. It measures the **evidence** of embedding.

- *I determines r: $I \propto 1/r^2$, so lowest I is optimal.*
- *I can be estimated empirically from a large corpus of covers [assuming that covers are made of independent pixel groups].*

(mod k)-matching

- Spatial domain embedding in images.
- Embed one k-ary symbol per location by altering the remainder (mod k) to nearest correct value.

(mod 3)-matching is ***ternary embedding***. The embedding effect matrix is

$$
\begin{array}{c c}
 & \begin{array}{cccccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & & \dots & & & & & & \end{array} \\
B = \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \\ \\ \\ \\ \\ \\ \\ \\ \end{array} & \begin{pmatrix}
\frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & & \cdots & & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & & \cdots & & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & & \cdots & & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & & \cdots & & 0 & 0 & 0 & 0 & 0 & 0 \\
 & & & & & & \ddots & & & & & & & & \\
 & & & & & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & & & & & \\
 & & & & & & & & \ddots & & & & & & \\
0 & 0 & 0 & 0 & 0 & 0 & & \cdots & & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & & \cdots & & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & & \cdots & & 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\
0 & 0 & 0 & 0 & 0 & 0 & & \cdots & & 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3}
\end{pmatrix}
\end{array}
$$

The embedding efficiency is $e = \log_2 3$ bits per location.

(mod *k*)-matching

- Spatial domain embedding in images.
- Embed one *k*-ary symbol per location by altering the remainder (mod *k*) to nearest correct value.

(mod 3)-matching is ***ternary embedding***. Embedding efficiency $e = \log_2 3$.

(mod 5)-matching is ***quinary embedding***. Embedding efficiency $e = \log_2 5$.

(mod 7)-matching is ***septenary embedding***. Embedding efficiency $e = \log_2 7$.

...

Convex combinations

We can make a continuous interpolation of embedding functions $(F_1, \ldots, F_k)$ by the following procedure.

- Sender and recipient agree on a secret key which determines a PRNG.
- At each cover location, choose embedding function F_i with probability π_i.

If each F_i has embedding matrix B_i, the combined embedding effect will be $\sum \pi_i B_i$.

If each F_i has embedding efficiency e_i, the combined embedding efficiency will be $\sum \pi_i e_i$.

We seek the optimal mixture of ternary, quinary, and septenary embedding.

SFI estimation

The SFI for pixel groups $\boldsymbol{X} = (X_1, \ldots, X_n) \in \mathcal{X}^n$ can be estimated by

$$\hat{I} = \frac{\displaystyle\sum_{\boldsymbol{y}\in\mathcal{X}^n} \frac{A(\boldsymbol{y})^2}{P(\boldsymbol{X}{=}\boldsymbol{y})} - n^2}{ne^2} \qquad A(\boldsymbol{y}) = \sum_{j=1}^{n} \sum_{u\in\mathcal{X}} P(\boldsymbol{X}{=}\boldsymbol{y}[u/y_j])B(u, y_j)$$

embedding efficiency

embedding effect probability

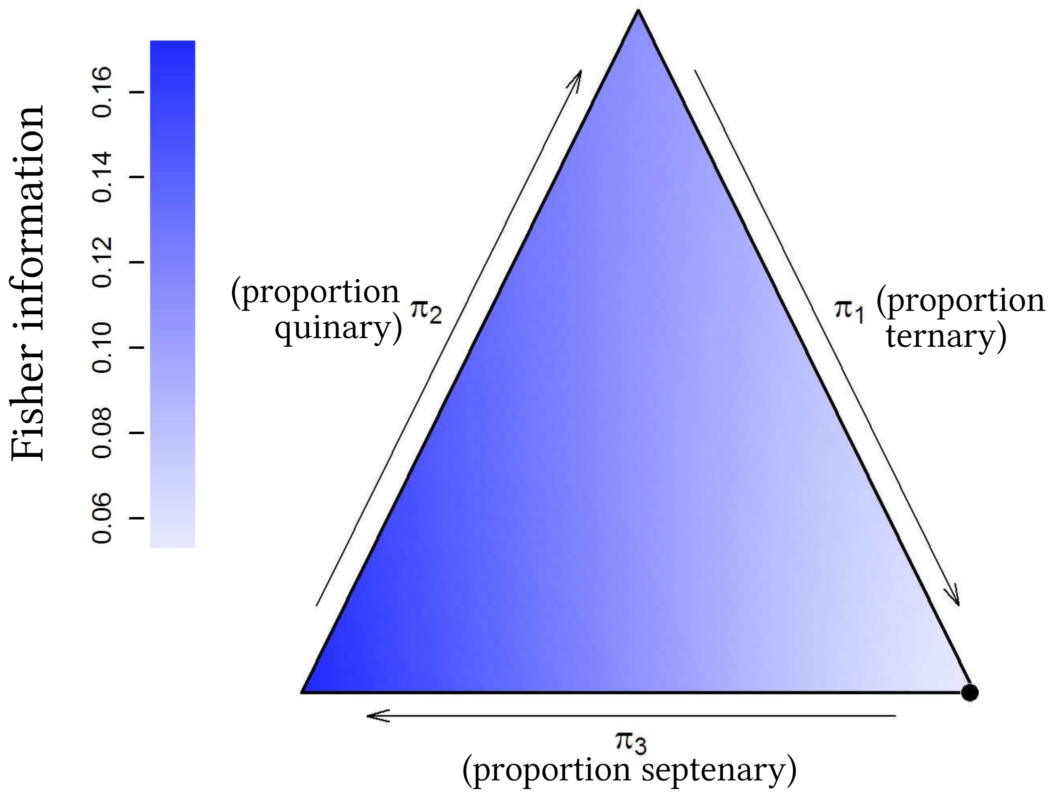
where the probabilities $P(\boldsymbol{X}{=}\boldsymbol{y})$ are taken from empirical joint n-gram histograms.

[And the SFI for a convex mixture π of embedding functions is always convex in π.]

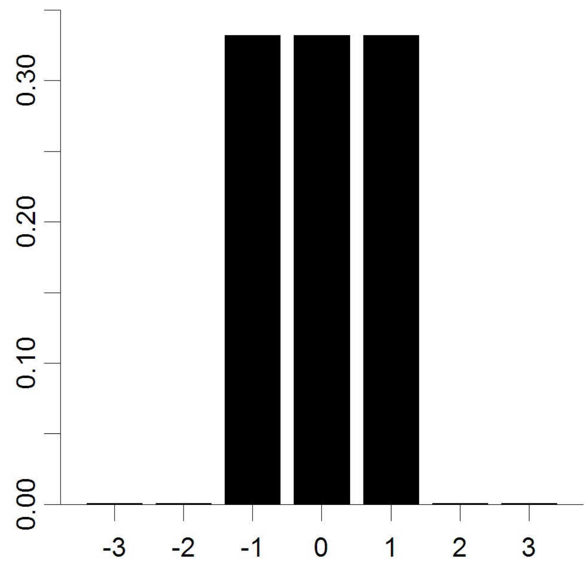
Results

RAW camera images (heavily denoised, saturated images excluded)

2121 images, 4.7Mpixels each, total evidence base 40B pixel groups



Optimal mixture: pure ternary

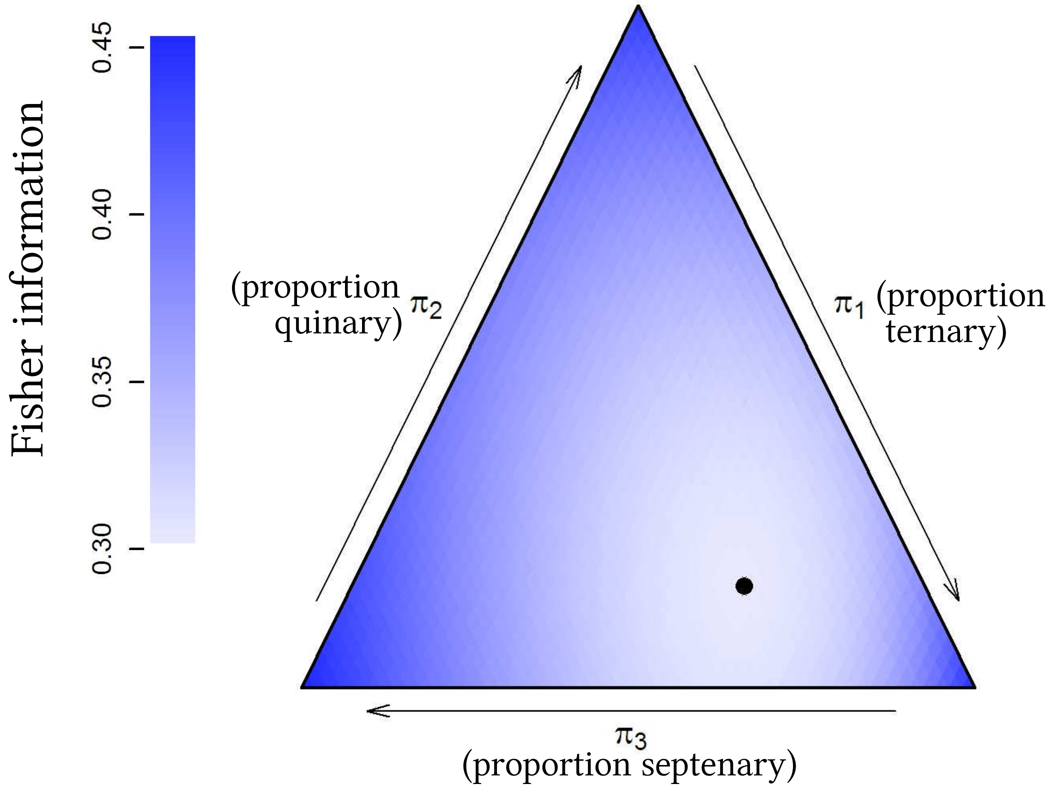


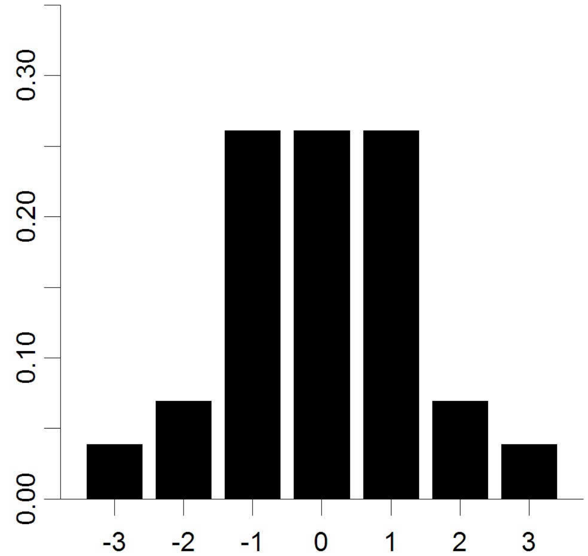
Optimal combination stego noise density

Results

RAW camera images from mixture of cameras (default denoising)

1040 images, 1.5Mpixels each, total evidence base 6B pixel groups





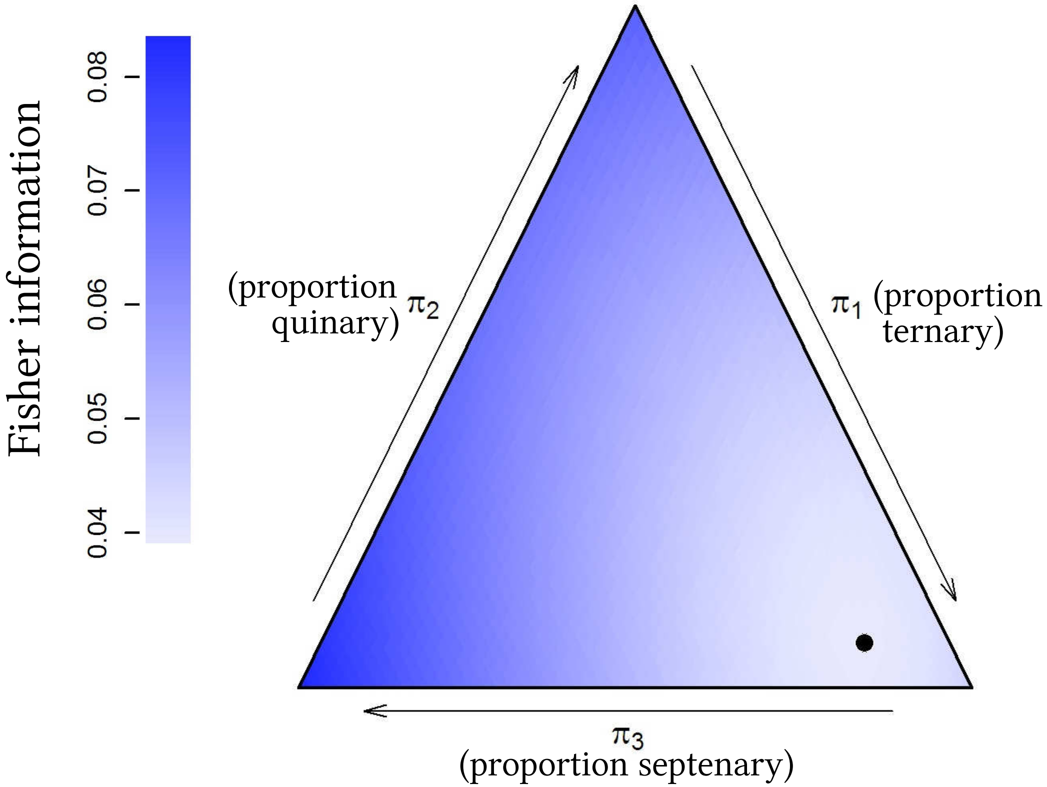
Optimal combination stego noise density

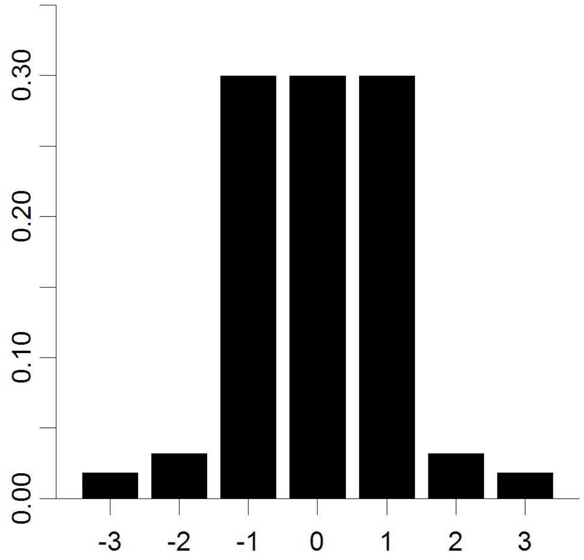
Optimal mixture: 58% ternary 15% quinary 27% septenary
Root rate 21% higher than pure ternary

Results

RAW camera images (all denoising disabled, saturation allowed)

3200 images, 4.7Mpixels each, total evidence base 15B pixel groups





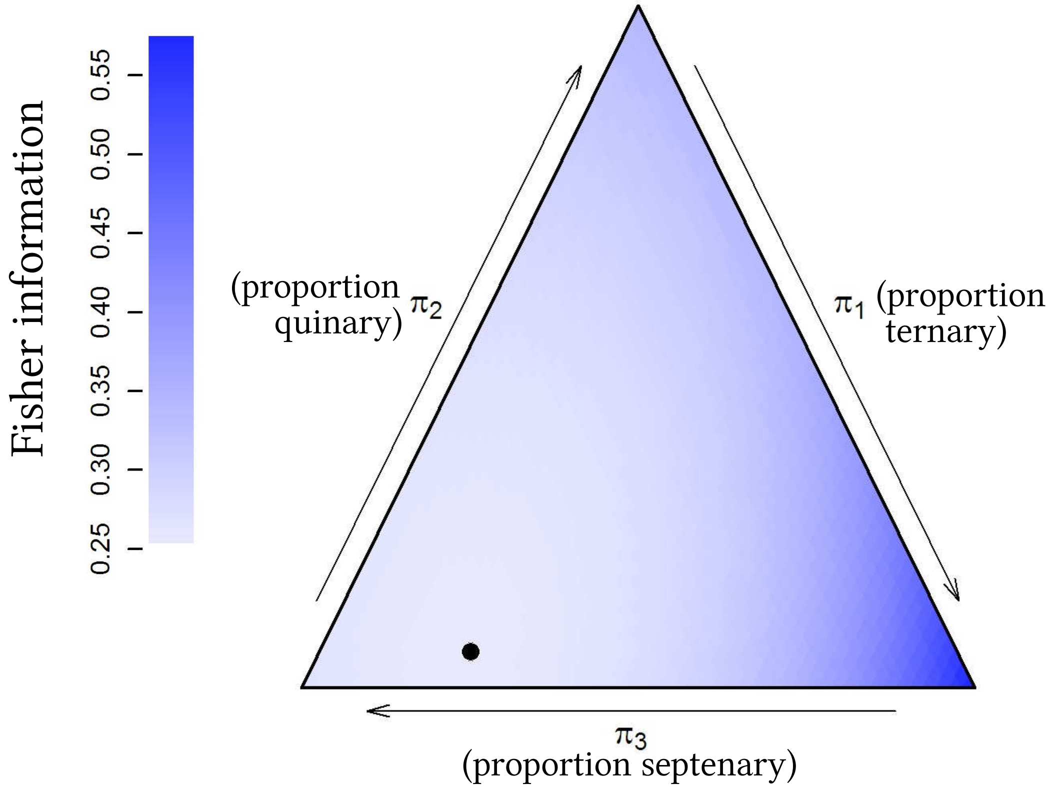
Optimal combination
stego noise density

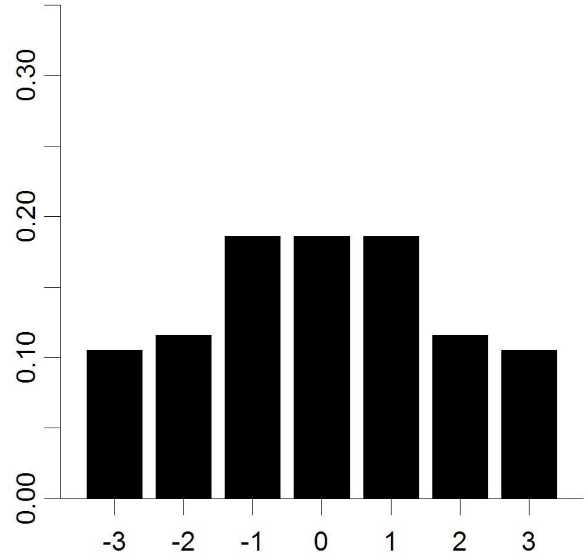
Optimal mixture: 80% ternary 7% quinary 13% septenary
Root rate 6% higher than pure ternary

Results

Decompressed JPEGs

10000 images, 0.54Mpixels each, total evidence base 20B pixel groups





Optimal combination stego noise density

Optimal mixture: 21% ternary 5% quinary 74% septenary

Root rate 50% higher than pure ternary

Conclusions

- This paper aims to illustrate the computation of optimal embedding mixtures:
  - *Steganographic Fisher Information is the proper metric,*
  - *estimating it has high computational demands.*

- We restricted attention to (mod 3)-, (mod 5)-, (mod 7)-matching:
  - *further work is to extend to wider embedding methods,*
  - *extend to adaptive source coding (results will probably be different).*

- The results depend on the cover source:
  - *not surprising that more noise can be embedded in noisy covers,*
  - *saturation is a significant factor, and needs further study.*

Conclusions

- This paper aims to illustrate the computation of optimal embedding mixtures:
  - *Steganographic Fisher Information is the proper metric,*
  - *estimating it has high computational demands.*

- We restricted attention to (mod 3)-, (mod 5)-, (mod 7)-matching:
  - *further work is to extend to wider embedding methods,*
  - *extend to adaptive source coding (results will probably be different).*

- The results depend on the cover source:
  - *not surprising that more noise can be embedded in noisy covers,*
  - *saturation is a significant factor, and needs further study.*

End