A Fusion of Maximum Likelihood and Structural Steganalysis

Andrew Ker

adk@comlab.ox.ac.uk

Royal Society University Research Fellow

Oxford University Computing Laboratory

Information Hiding Workshop, St Malo

12 June 2007

A Fusion of Maximum Likelihood and Structural Steganalysis

Outline

- Maximum likelihood & structural steganalysis
- New structural analysis $\longrightarrow$ likelihood function
- Maximization
- Experimental results
- Conclusions & further work

Steganalysis of LSB Replacement

Replacement of low-order bits is particularly insecure steganography because of combinatorial structure.

Maximum Likelihood Steganalysis

1. *Analyse the effect of embedding on histogram/co-occurrence matrix/etc,*
2. *Likelihood function in terms of payload size,*
3. *Maximize likelihood.*

- Founded on sound statistical principles,
- Requires knowledge/estimation of cover source PMF/transition matrix/etc,
- Inaccurate estimator in practice.

Dabeer et al, *IEEE Trans. Signal Processing*, 2004.
Hogan et al. *SPIE/IS&T Electronic Imaging conference*, 2005.
Draper et al. *Information Hiding Workshop*, 2005.
Sullivan et al. *IEEE Trans. Information Forensics and Security*, 2006.

Steganalysis of LSB Replacement

Replacement of low-order bits is particularly insecure steganography because of combinatorial structure.

Structural Steganalysis

1. *Analyse the effect of embedding on pairs/triples/etc of samples,*
2. *Simple assumptions about cover objects,*
3. *Deduce payload size.*

- Dubious statistical rigour,
- Requires less knowledge about covers,
- Highly sensitive in practice.

Dumitrescu et al, *IEEE Trans. Signal Processing*, 2003.
Lu et al. *Information Hiding Workshop*, 2004.
Ker, *Information Hiding Workshop*, 2005.
Ker, *IEEE Trans. Information Forensics and Security*, 2007.

Steganalysis of LSB Replacement

Replacement of low-order bits is particularly insecure steganography because of combinatorial structure.

Structural Steganalysis

1. *Analyse the effect of embedding on pairs/triples/etc of samples,*
2. *Simple assumptions about cover objects,*
3. *Deduce payload size.*

- Dubious statistical rigour,
- Requires less knowledge about covers,
- Highly sensitive in practice.

Can we merge the statistical rigour of ML detection with the sensitive features found in structural steganalysis?

Trace Subsets

Every **pair** of adjacent samples is classified according to their values:

$\mathcal{E}_m$	$\mathcal{O}_m$
$(2k, 2k+m)$	$(2k+1, 2k+1+m)$

for example,

40	41	would be classified $\mathcal{E}_1$
43	40	would be classified $\mathcal{O}_{-3}$

It is also useful to write $\mathcal{D}_m = \mathcal{E}_m \cup \mathcal{O}_m$ i.e. pairs $(k, k+m)$

Trace Subsets

Every **pair** of adjacent samples is classified according to their values:

$$\begin{array}{cc} \mathcal{E}_m & \mathcal{O}_m \\ (2k, 2k+m) & (2k+1, 2k+1+m) \end{array}$$

Embedding Process

Supppose a cover of size N.

Uncorrelated payload of size Np embedded by replacing LSBs of a **pseudo-random** selection of values, so

LSB flips are independent with probability $\frac{p}{2}$

Cover object	Stego object

$$\underset{(2k,\,2k+2m)}{\mathcal{E}_{2m}} \xrightarrow{(1-\frac{p}{2})^2} \underset{(2k,\,2k+2m)}{\mathcal{E}_{2m}}$$

flip neither:
probability $(1-\frac{p}{2})^2$

LSB flips are independent with probability $\frac{p}{2}$

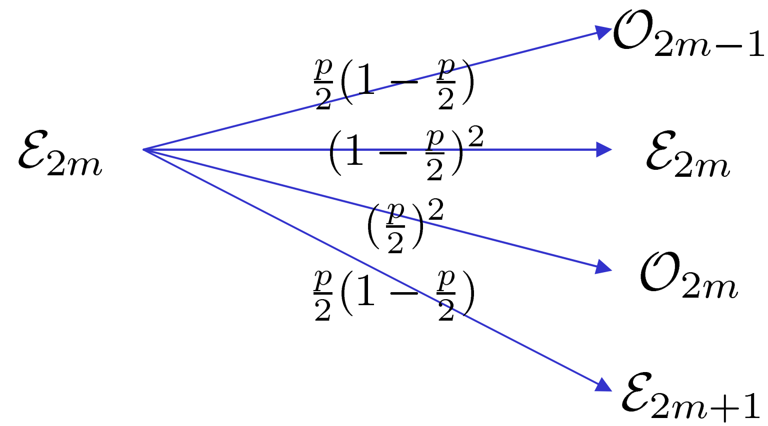
Cover object	Stego object

$$\begin{tikzcd} \mathcal{E}_{2m} \arrow[r, "(1-\frac{p}{2})^2"] \arrow[dr, "(\frac{p}{2})^2"'] & \mathcal{E}_{2m} \\ (2k, 2k+2m) & \mathcal{O}_{2m} \\ & (2k+1, 2k+2m+1) \end{tikzcd}$$

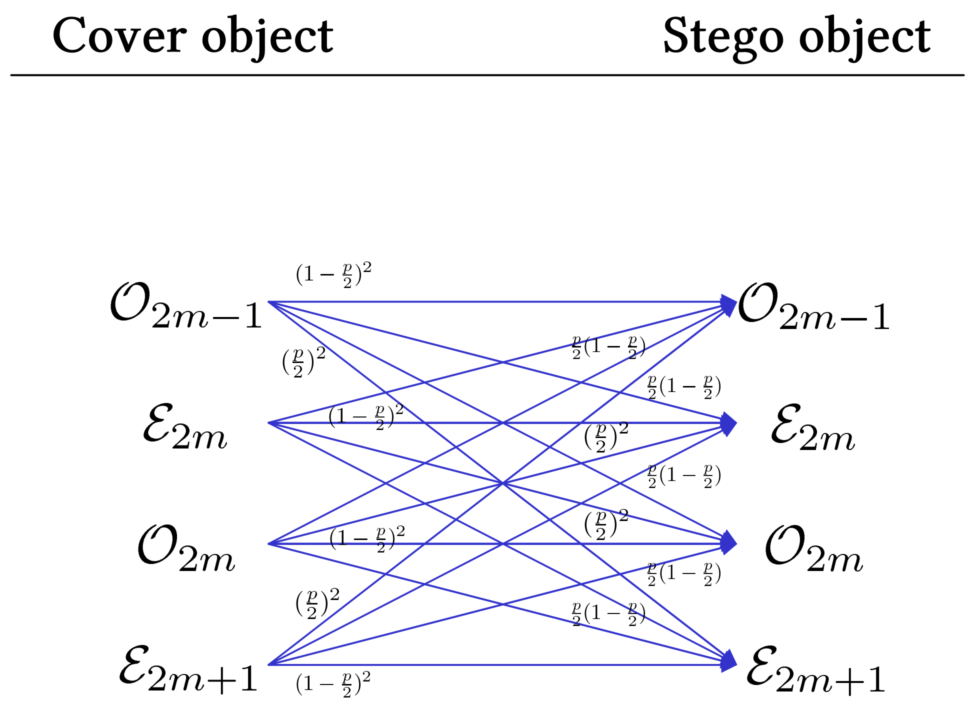
flip both:
probability $(\frac{p}{2})^2$

LSB flips are independent with probability $\frac{p}{2}$

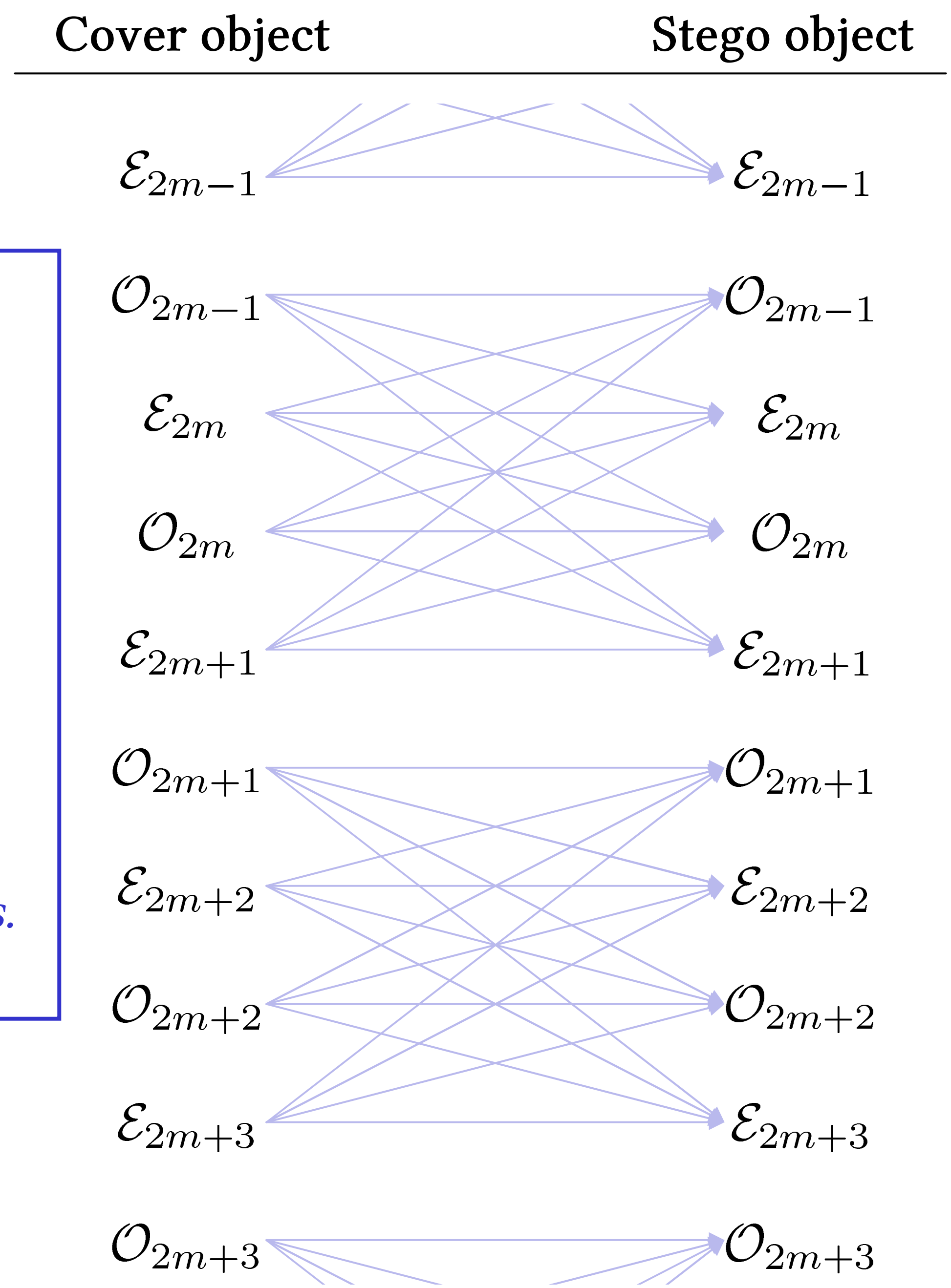
Cover object **Stego object**



LSB flips are independent with probability $\frac{p}{2}$



Cover object
Stego object
$\mathcal{O}_{2m-1}$
$\mathcal{E}_{2m}$
$\mathcal{O}_{2m}$
$\mathcal{E}_{2m+1}$
$(1-\frac{p}{2})^2$
$(\frac{p}{2})^2$
$\frac{p}{2}(1-\frac{p}{2})$
$\mathcal{O}_{2m-1}$
$\mathcal{E}_{2m}$
$\mathcal{O}_{2m}$
$\mathcal{E}_{2m+1}$



To estimate p:

1. Assume cover model:
$$|\mathcal{E}_m| = |\mathcal{O}_m|$$
in natural images;

2. Consider only odd m;

3. Assume
proportions = probabilities.

New Structural Analysis

Where does $|\mathcal{E}_m| = |\mathcal{O}_m|$ come from?

Recall that $\mathcal{D}_m = \mathcal{E}_m \cup \mathcal{O}_m$. Suppose the partition is random.

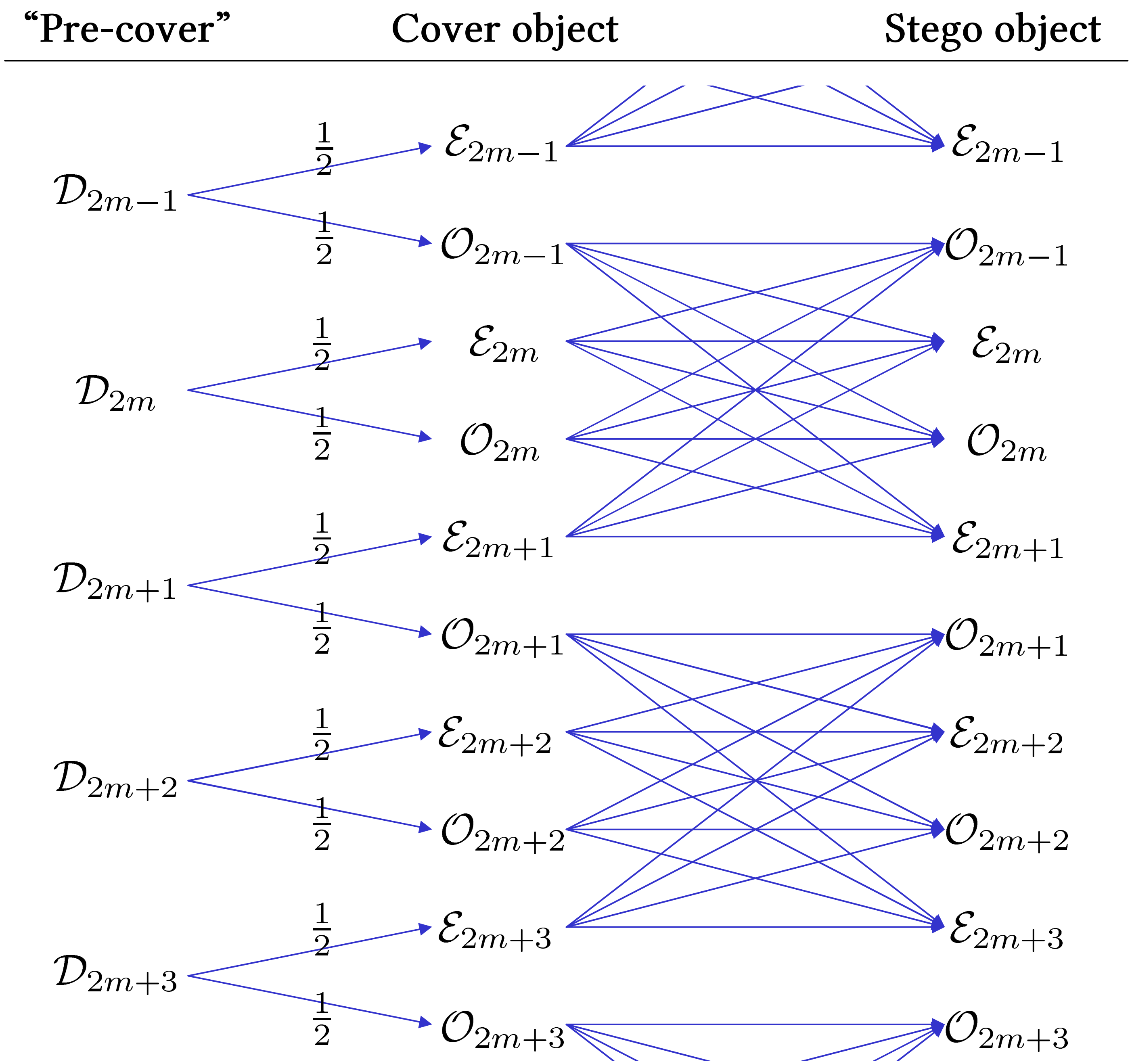
i.e., imagine that a cover object is derived from a "pre-cover", in which $|\mathcal{D}_m|$ are fixed, with pairs moving independently at random:

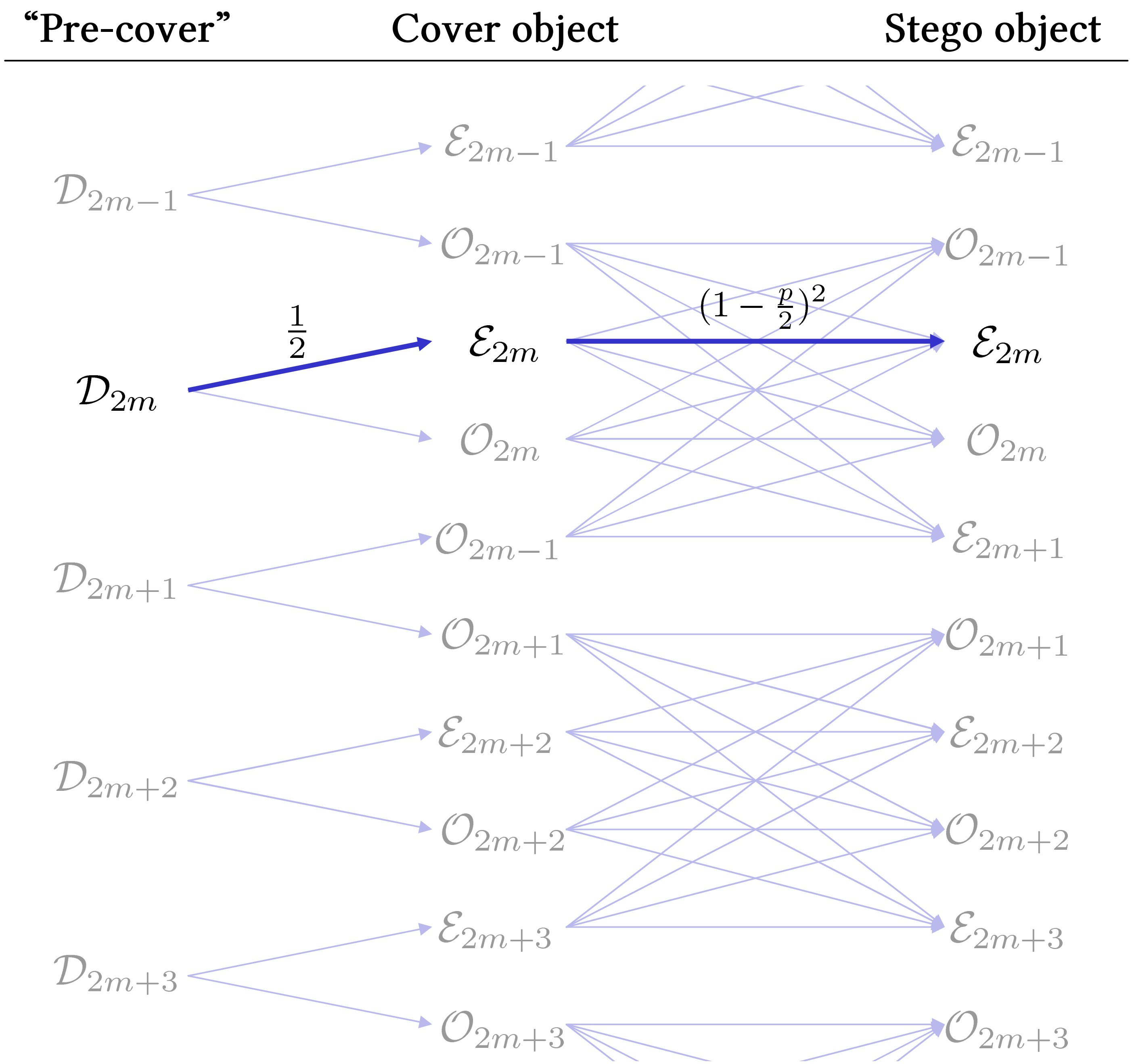
"Pre-cover"	**Cover object**

$$\begin{tikzcd} & \mathcal{E}_m \\ \mathcal{D}_m \arrow[ur, "\frac{1}{2}"] \arrow[dr, "\frac{1}{2}"'] & \\ & \mathcal{O}_m \end{tikzcd}$$

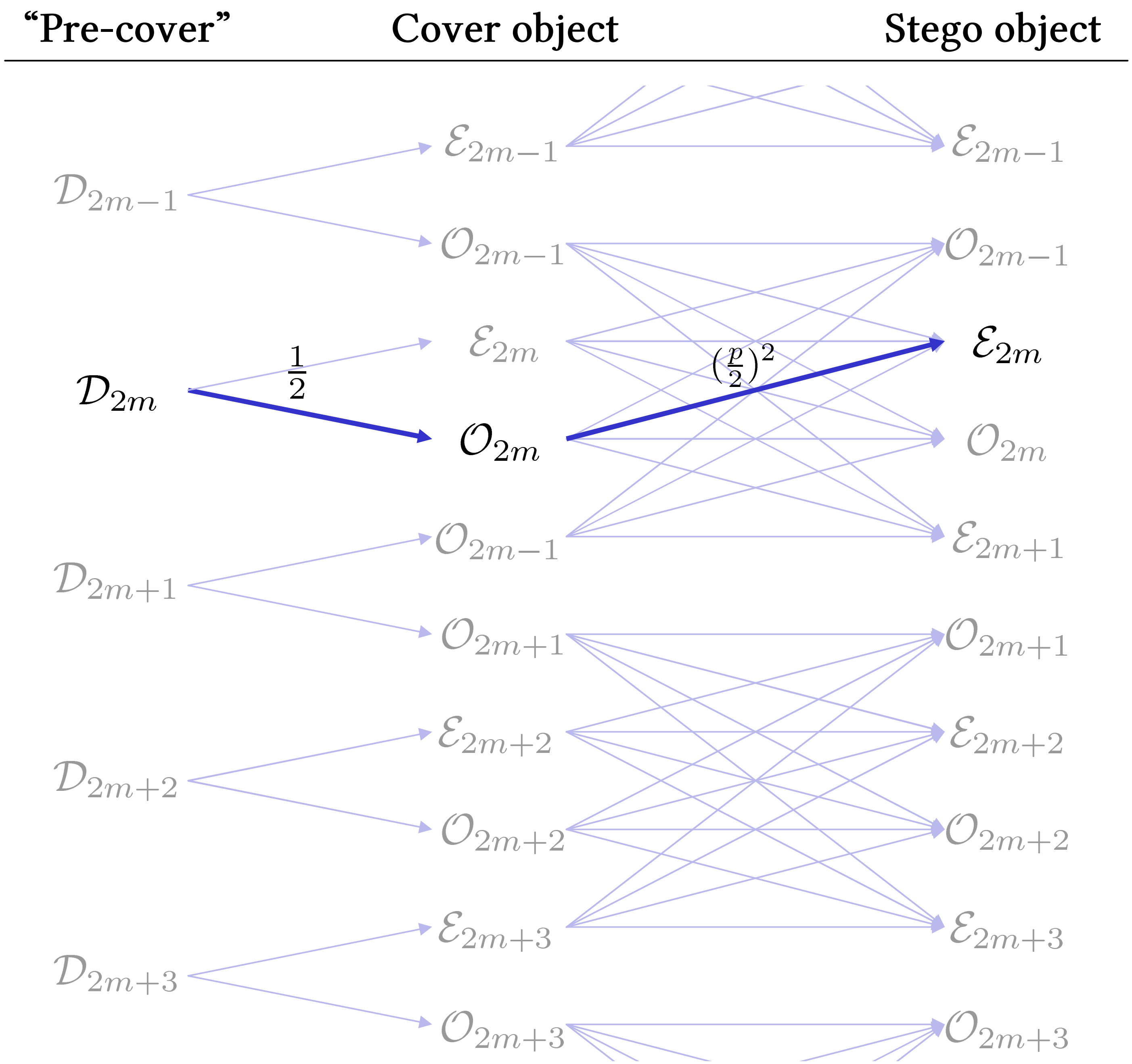
This model is validated in the literature, **except for** $m = -1, 0, 1$

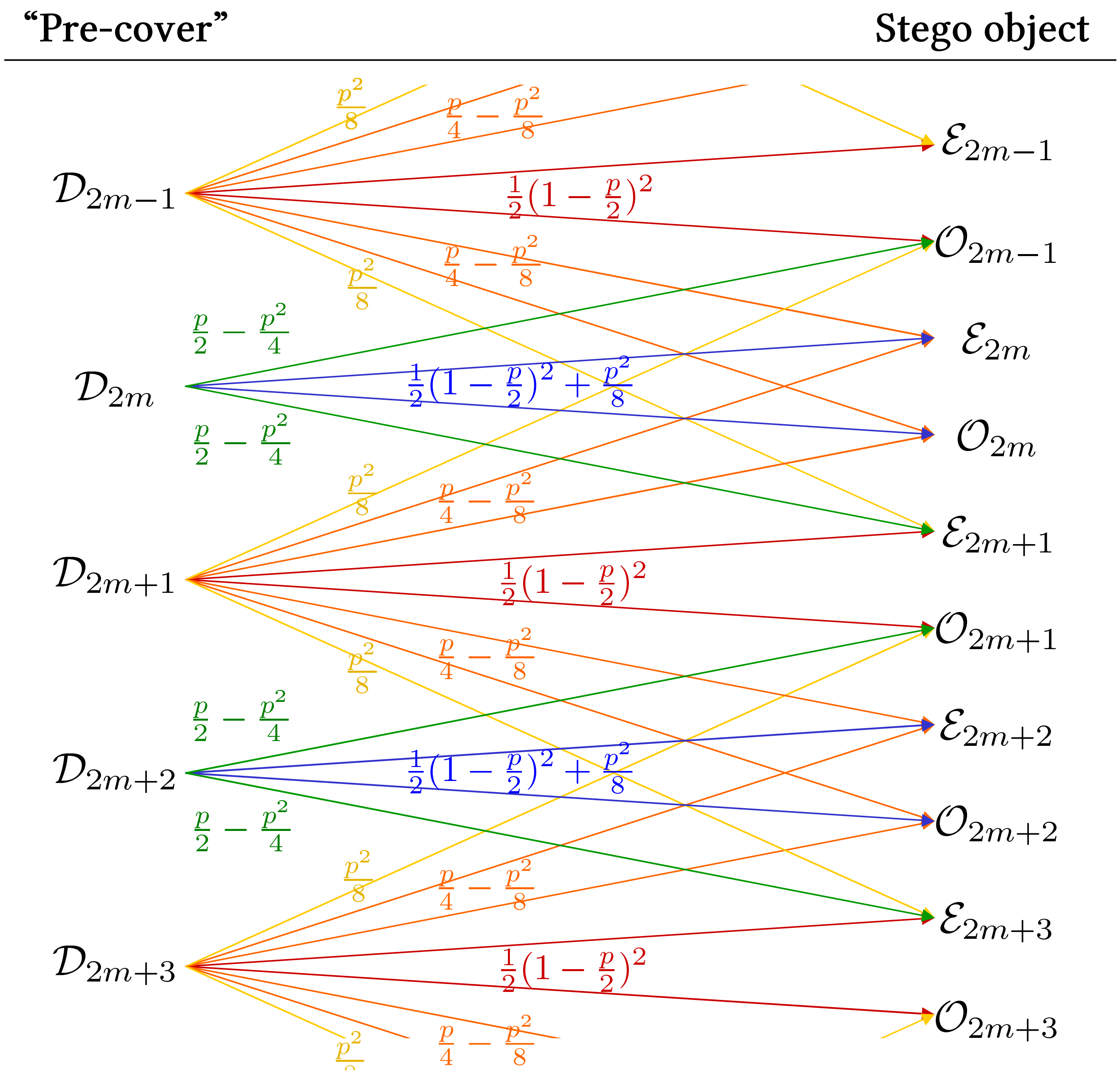
A. Ker, *Derivation of Error Distribution in Least-Squares Steganalysis,* IEEE Trans. Information Forensics and Security 2(2): 140-148, 2007.


"Pre-cover"
Cover object
Stego object
$\mathcal{D}_{2m-1}$
$\mathcal{D}_{2m}$
$\mathcal{D}_{2m+1}$
$\mathcal{D}_{2m+2}$
$\mathcal{D}_{2m+3}$
$\frac{1}{2}$
$\mathcal{E}_{2m-1}$
$\mathcal{O}_{2m-1}$
$\mathcal{E}_{2m}$
$\mathcal{O}_{2m}$
$\mathcal{E}_{2m+1}$
$\mathcal{O}_{2m+1}$
$\mathcal{E}_{2m+2}$
$\mathcal{O}_{2m+2}$
$\mathcal{E}_{2m+3}$
$\mathcal{O}_{2m+3}$

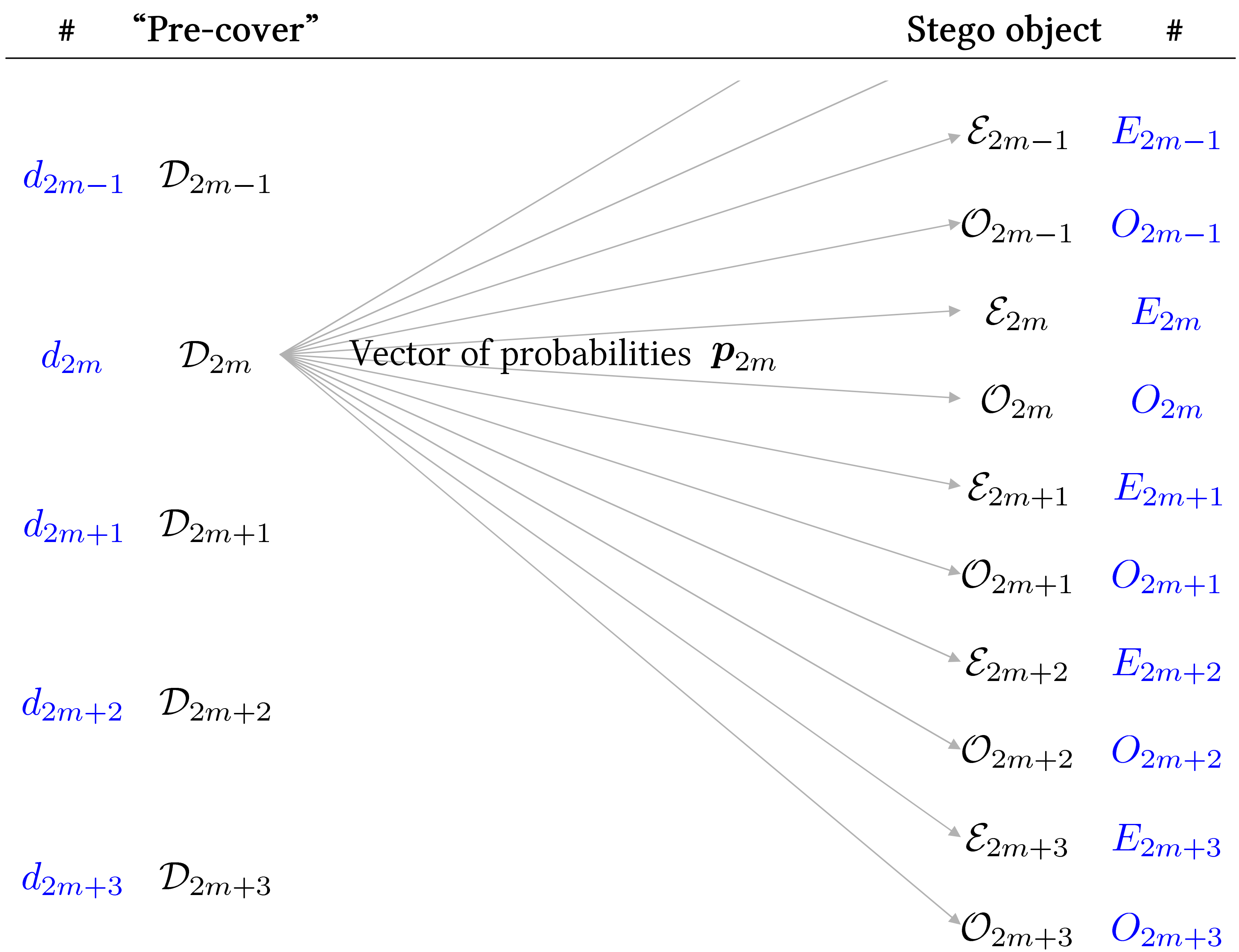


"Pre-cover"
Cover object
Stego object
$\mathcal{D}_{2m-1}$
$\mathcal{D}_{2m}$
$\mathcal{D}_{2m+1}$
$\mathcal{D}_{2m+2}$
$\mathcal{D}_{2m+3}$
$\frac{1}{2}$
$\mathcal{E}_{2m-1}$
$\mathcal{O}_{2m-1}$
$\mathcal{E}_{2m}$
$\mathcal{O}_{2m}$
$\mathcal{O}_{2m-1}$
$\mathcal{O}_{2m+1}$
$\mathcal{E}_{2m+2}$
$\mathcal{O}_{2m+2}$
$\mathcal{E}_{2m+3}$
$\mathcal{O}_{2m+3}$
$(1-\frac{p}{2})^2$
$\mathcal{E}_{2m-1}$
$\mathcal{O}_{2m-1}$
$\mathcal{E}_{2m}$
$\mathcal{O}_{2m}$
$\mathcal{E}_{2m+1}$
$\mathcal{O}_{2m+1}$
$\mathcal{E}_{2m+2}$
$\mathcal{O}_{2m+2}$
$\mathcal{E}_{2m+3}$
$\mathcal{O}_{2m+3}$

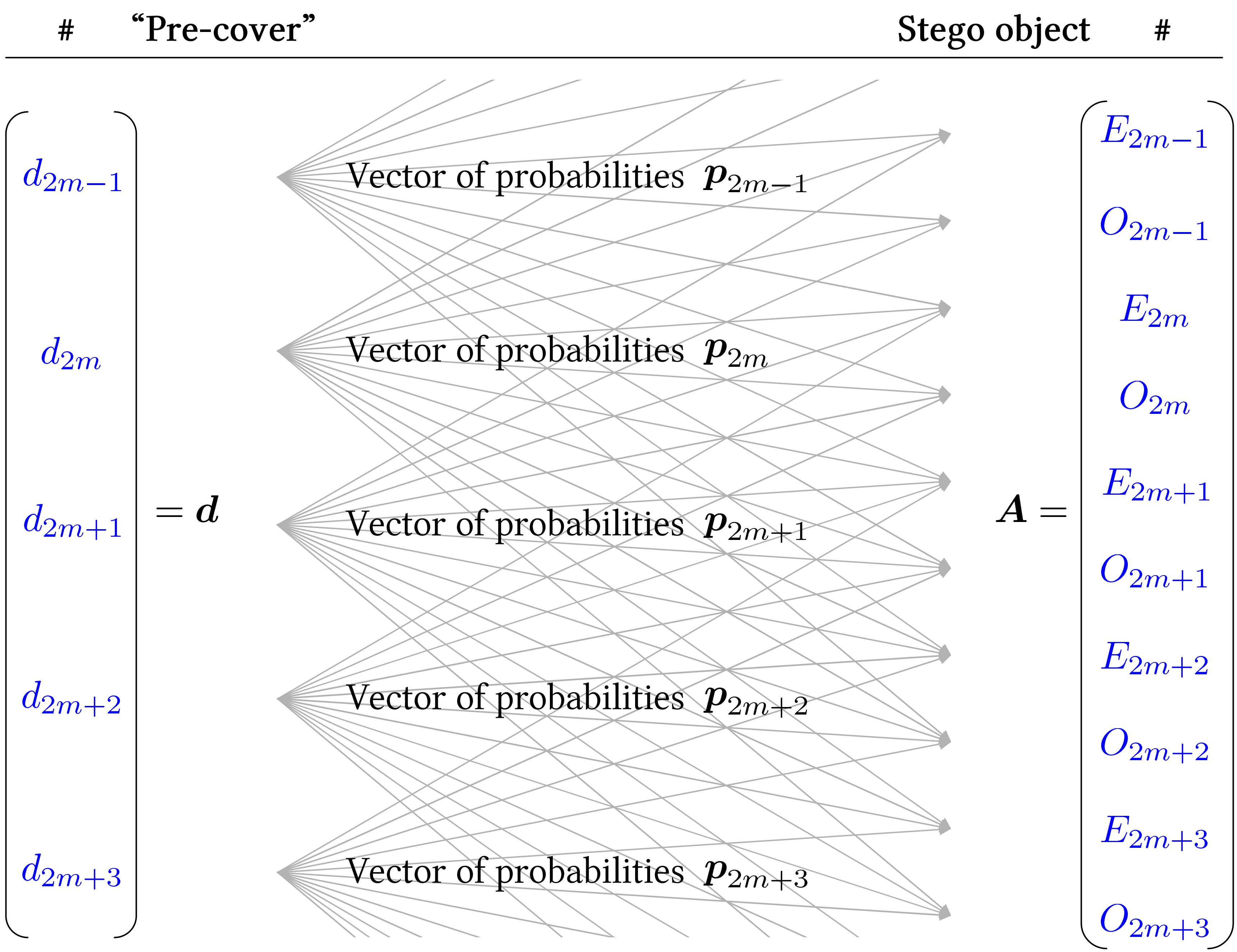

"Pre-cover"
Cover object
Stego object
$\mathcal{D}_{2m-1}$
$\mathcal{D}_{2m}$
$\mathcal{D}_{2m+1}$
$\mathcal{D}_{2m+2}$
$\mathcal{D}_{2m+3}$
$\mathcal{E}_{2m-1}$
$\mathcal{O}_{2m-1}$
$\mathcal{E}_{2m}$
$\mathcal{O}_{2m}$
$\mathcal{O}_{2m-1}$
$\mathcal{O}_{2m+1}$
$\mathcal{E}_{2m+2}$
$\mathcal{O}_{2m+2}$
$\mathcal{E}_{2m+3}$
$\mathcal{O}_{2m+3}$
$\frac{1}{2}$
$(\frac{p}{2})^2$
$\mathcal{E}_{2m-1}$
$\mathcal{O}_{2m-1}$
$\mathcal{E}_{2m}$
$\mathcal{O}_{2m}$
$\mathcal{E}_{2m+1}$
$\mathcal{O}_{2m+1}$
$\mathcal{E}_{2m+2}$
$\mathcal{O}_{2m+2}$
$\mathcal{E}_{2m+3}$
$\mathcal{O}_{2m+3}$



“Pre-cover”
Stego object
$\mathcal{D}_{2m-1}$
$\mathcal{D}_{2m}$
$\mathcal{D}_{2m+1}$
$\mathcal{D}_{2m+2}$
$\mathcal{D}_{2m+3}$
$\mathcal{E}_{2m-1}$
$\mathcal{O}_{2m-1}$
$\mathcal{E}_{2m}$
$\mathcal{O}_{2m}$
$\mathcal{E}_{2m+1}$
$\mathcal{O}_{2m+1}$
$\mathcal{E}_{2m+2}$
$\mathcal{O}_{2m+2}$
$\mathcal{E}_{2m+3}$
$\mathcal{O}_{2m+3}$
$\frac{p^2}{8}$
$\frac{p}{4} - \frac{p^2}{8}$
$\frac{1}{2}(1-\frac{p}{2})^2$
$\frac{p}{2} - \frac{p^2}{4}$
$\frac{1}{2}(1-\frac{p}{2})^2 + \frac{p^2}{8}$



#
“Pre-cover”
Stego object
#
d_{2m-1} $\mathcal{D}_{2m-1}$
d_{2m} $\mathcal{D}_{2m}$
d_{2m+1} $\mathcal{D}_{2m+1}$
d_{2m+2} $\mathcal{D}_{2m+2}$
d_{2m+3} $\mathcal{D}_{2m+3}$
Vector of probabilities $\boldsymbol{p}_{2m}$
$\mathcal{E}_{2m-1}$ E_{2m-1}
$\mathcal{O}_{2m-1}$ O_{2m-1}
$\mathcal{E}_{2m}$ E_{2m}
$\mathcal{O}_{2m}$ O_{2m}
$\mathcal{E}_{2m+1}$ E_{2m+1}
$\mathcal{O}_{2m+1}$ O_{2m+1}
$\mathcal{E}_{2m+2}$ E_{2m+2}
$\mathcal{O}_{2m+2}$ O_{2m+2}
$\mathcal{E}_{2m+3}$ E_{2m+3}
$\mathcal{O}_{2m+3}$ O_{2m+3}



“Pre-cover”
Stego object #
d_{2m-1}
d_{2m}
d_{2m+1}
d_{2m+2}
d_{2m+3}
$= \boldsymbol{d}$
Vector of probabilities $\boldsymbol{p}_{2m-1}$
Vector of probabilities $\boldsymbol{p}_{2m}$
Vector of probabilities $\boldsymbol{p}_{2m+1}$
Vector of probabilities $\boldsymbol{p}_{2m+2}$
Vector of probabilities $\boldsymbol{p}_{2m+3}$
$\boldsymbol{A} =$
E_{2m-1}
O_{2m-1}
E_{2m}
O_{2m}
E_{2m+1}
O_{2m+1}
E_{2m+2}
O_{2m+2}
E_{2m+3}
O_{2m+3}

Likelihood Function

Given the sizes of the trace subsets in the pre-cover $\boldsymbol{d}$, and p, the distribution of $\boldsymbol{A}$ is a sum of multinomials:

$$\boldsymbol{A} \sim \sum_m \mathcal{M}(d_m, \boldsymbol{p_m})$$

well-approximated by

$$\boldsymbol{A} \approx \mathrm{N}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$$

$$\begin{aligned} \boldsymbol{\mu} &= \textstyle\sum_m d_m \boldsymbol{p_m} \\ \boldsymbol{\Sigma} &= \textstyle\sum_m d_m (\boldsymbol{\Delta_{p_m}} - \boldsymbol{p_m}\boldsymbol{p_m}^T) \end{aligned}$$

The log-likelihood of an observation $\boldsymbol{a}$ of $\boldsymbol{A}$ is therefore

$$l(\boldsymbol{a}; p, \boldsymbol{d}) = -\frac{L}{2}\log(2\pi) - \frac{1}{2}\log|\boldsymbol{\Sigma}| - \frac{1}{2}(\boldsymbol{a}-\boldsymbol{\mu})^T\boldsymbol{\Sigma}^{-1}(\boldsymbol{a}-\boldsymbol{\mu})$$

where L is the length of the vector $\boldsymbol{A}$.

Σ

$$\pi_i = \tfrac{1}{2}(\tfrac{p}{2})^i(1-\tfrac{p}{2})^{2-i} \quad \sigma = \pi_0+\pi_2$$

	O_{2m-1}	E_{2m}	O_{2m}	E_{2m+1}
O_{2m-3}	$-\pi_0\pi_2 d_{2m-1}$	$-\pi_1\pi_2 d_{2m-1}$	$-\pi_1\pi_2 d_{2m-1}$	$-\pi_2^2 d_{2m-1}$
E_{2m-2}	$-\pi_0\pi_1 d_{2m-1}$	$-\pi_1^2 d_{2m-1}$	$-\pi_1^2 d_{2m-1}$	$-\pi_1\pi_2 d_{2m-1}$
O_{2m-2}	$-\pi_0\pi_1 d_{2m-1}$	$-\pi_1^2 d_{2m-1}$	$-\pi_1^2 d_{2m-1}$	$-\pi_1\pi_2 d_{2m-1}$
E_{2m-1}	$-\pi_0^2 d_{2m-1}$	$-\pi_0\pi_1 d_{2m-1}$	$-\pi_0\pi_1 d_{2m-1}$	$-\pi_0\pi_2 d_{2m-1}$
O_{2m-1}	$\pi_0(1-\pi_0)d_{2m-1}$ $+2\pi_1(1-2\pi_1)d_{2m}$ $+\pi_2(1-\pi_2)d_{2m+1}$	$-\pi_0\pi_1 d_{2m-1}$ $-2\pi_1\sigma d_{2m}$ $-\pi_1\pi_2 d_{2m+1}$	$-\pi_0\pi_1 d_{2m-1}$ $-2\pi_1\sigma d_{2m}$ $-\pi_1\pi_2 d_{2m+1}$	$-\pi_0\pi_2 d_{2m-1}$ $-4\pi_1^2 d_{2m}$ $-\pi_0\pi_2 d_{2m+1}$
E_{2m}	$-\pi_0\pi_1 d_{2m-1}$ $-2\pi_1\sigma d_{2m}$ $-\pi_1\pi_2 d_{2m+1}$	$\pi_1(1-\pi_1)d_{2m-1}$ $+\sigma(1-\sigma)d_{2m}$ $+\pi_1(1-\pi_1)d_{2m+1}$	$-\pi_1^2 d_{2m-1}$ $-\sigma^2 d_{2m}$ $-\pi_1^2 d_{2m+1}$	$-\pi_1\pi_2 d_{2m-1}$ $-2\pi_1\sigma d_{2m}$ $-\pi_0\pi_1 d_{2m+1}$
O_{2m}	$-\pi_0\pi_1 d_{2m-1}$ $-2\pi_1\sigma d_{2m}$ $-\pi_1\pi_2 d_{2m+1}$	$-\pi_1^2 d_{2m-1}$ $-\sigma^2 d_{2m}$ $-\pi_1^2 d_{2m+1}$	$\pi_1(1-\pi_1)d_{2m-1}$ $+\sigma(1-\sigma)d_{2m}$ $+\pi_1(1-\pi_1)d_{2m+1}$	$-\pi_1\pi_2 d_{2m-1}$ $-2\pi_1\sigma d_{2m}$ $-\pi_0\pi_1 d_{2m+1}$
E_{2m+1}	$-\pi_0\pi_2 d_{2m-1}$ $-4\pi_1^2 d_{2m}$ $-\pi_0\pi_2 d_{2m+1}$	$-\pi_1\pi_2 d_{2m-1}$ $-2\pi_1\sigma d_{2m}$ $-\pi_0\pi_1 d_{2m+1}$	$-\pi_1\pi_2 d_{2m-1}$ $-2\pi_1\sigma d_{2m}$ $-\pi_0\pi_1 d_{2m+1}$	$\pi_2(1-\pi_2)d_{2m-1}$ $+2\pi_1(1-2\pi_1)d_{2m}$ $+\pi_0(1-\pi_0)d_{2m+1}$
O_{2m+1}	$-\pi_0\pi_2 d_{2m+1}$	$-\pi_0\pi_1 d_{2m+1}$	$-\pi_0\pi_1 d_{2m+1}$	$-\pi_0^2 d_{2m+1}$
E_{2m+2}	$-\pi_1\pi_2 d_{2m+1}$	$-\pi_1^2 d_{2m+1}$	$-\pi_1^2 d_{2m+1}$	$-\pi_0\pi_1 d_{2m+1}$
O_{2m+2}	$-\pi_1\pi_2 d_{2m+1}$	$-\pi_1^2 d_{2m+1}$	$-\pi_1^2 d_{2m+1}$	$-\pi_0\pi_1 d_{2m+1}$
E_{2m+3}	$-\pi_2^2 d_{2m+1}$	$-\pi_1\pi_2 d_{2m+1}$	$-\pi_1\pi_2 d_{2m+1}$	$-\pi_0\pi_2 d_{2m+1}$

Maximum Likelihood

Estimator: find p (and $\boldsymbol{d}$) to maximize

$$l(\boldsymbol{a}; p, \boldsymbol{d}) = -\frac{L}{2}\log(2\pi) - \frac{1}{2}\log|\boldsymbol{\Sigma}| - \frac{1}{2}(\boldsymbol{a} - \boldsymbol{\mu})^T \boldsymbol{\Sigma}^{-1}(\boldsymbol{a} - \boldsymbol{\mu})$$

Maximum Likelihood

Estimator: find p (and $\boldsymbol{d}$) to maximize

$$l(\boldsymbol{a}; p, \boldsymbol{d}) = -\frac{L}{2}\log(2\pi) - \frac{1}{2}\log|\boldsymbol{\Sigma}| - \frac{1}{2}(\boldsymbol{a}-\boldsymbol{\mu})^T\boldsymbol{\Sigma}^{-1}(\boldsymbol{a}-\boldsymbol{\mu})$$

Difficulties:

- No analytical maximum (can't even differentiate!)

  Must use slow numerical methods.

- Dimensionality:

  24 ~~512~~ dimensional maximization problem

  each likelihood evaluation involves a quadratic form of length ~~1020~~ ~~44~~ 33

  Consider only $\mathcal{D}_{-11}$ to $\mathcal{D}_{+11}$.

- Overfitting

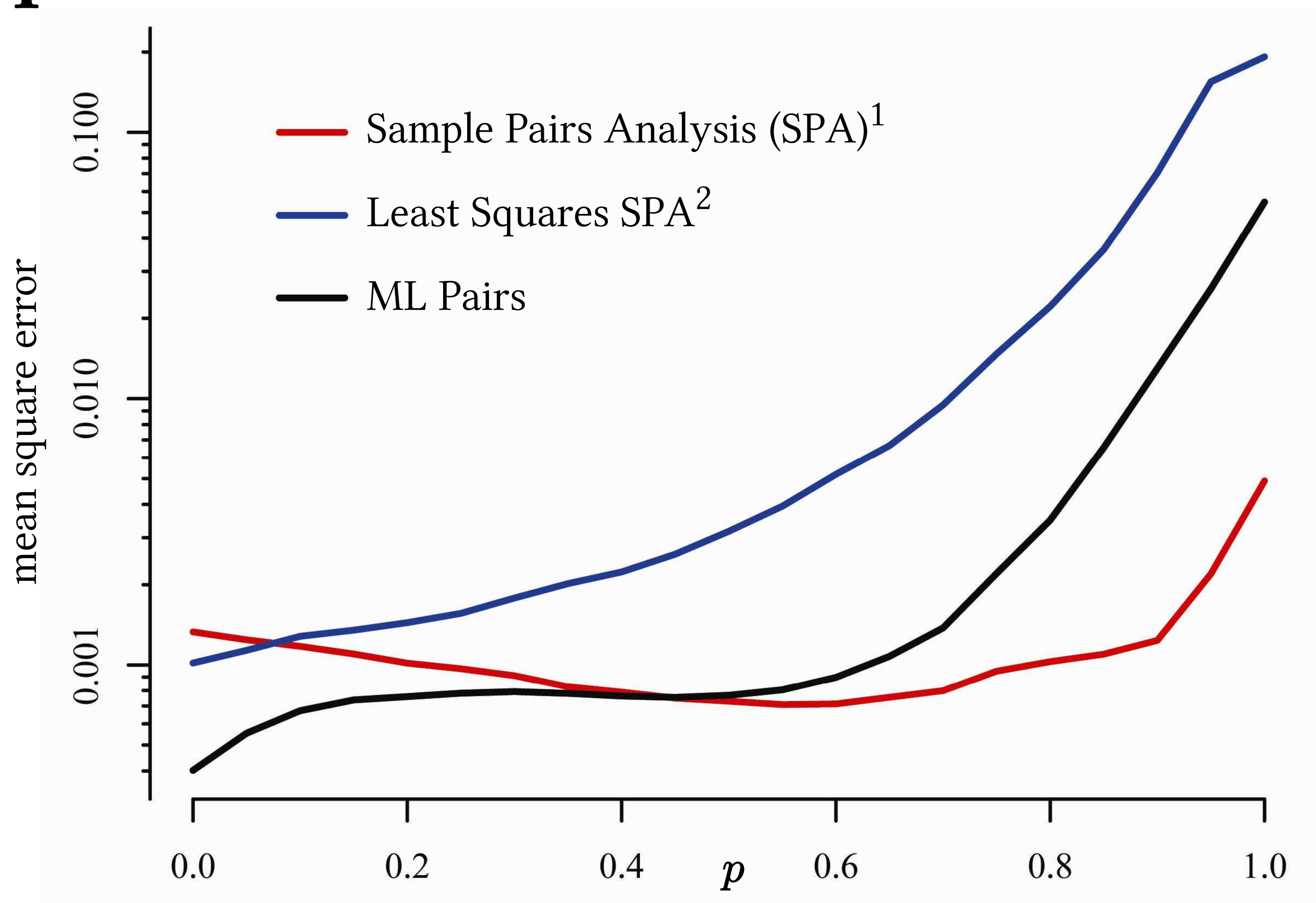
  Convert to MAP estimator with Gaussian prior for p.

Experimental Results

Experiments conducted on 3000 never-compressed grayscale bitmap images, size 0.3Mpixels.

Compared Structural/ML estimators with standard structural estimators by ***mean square estimator error*** (as estimates for p).

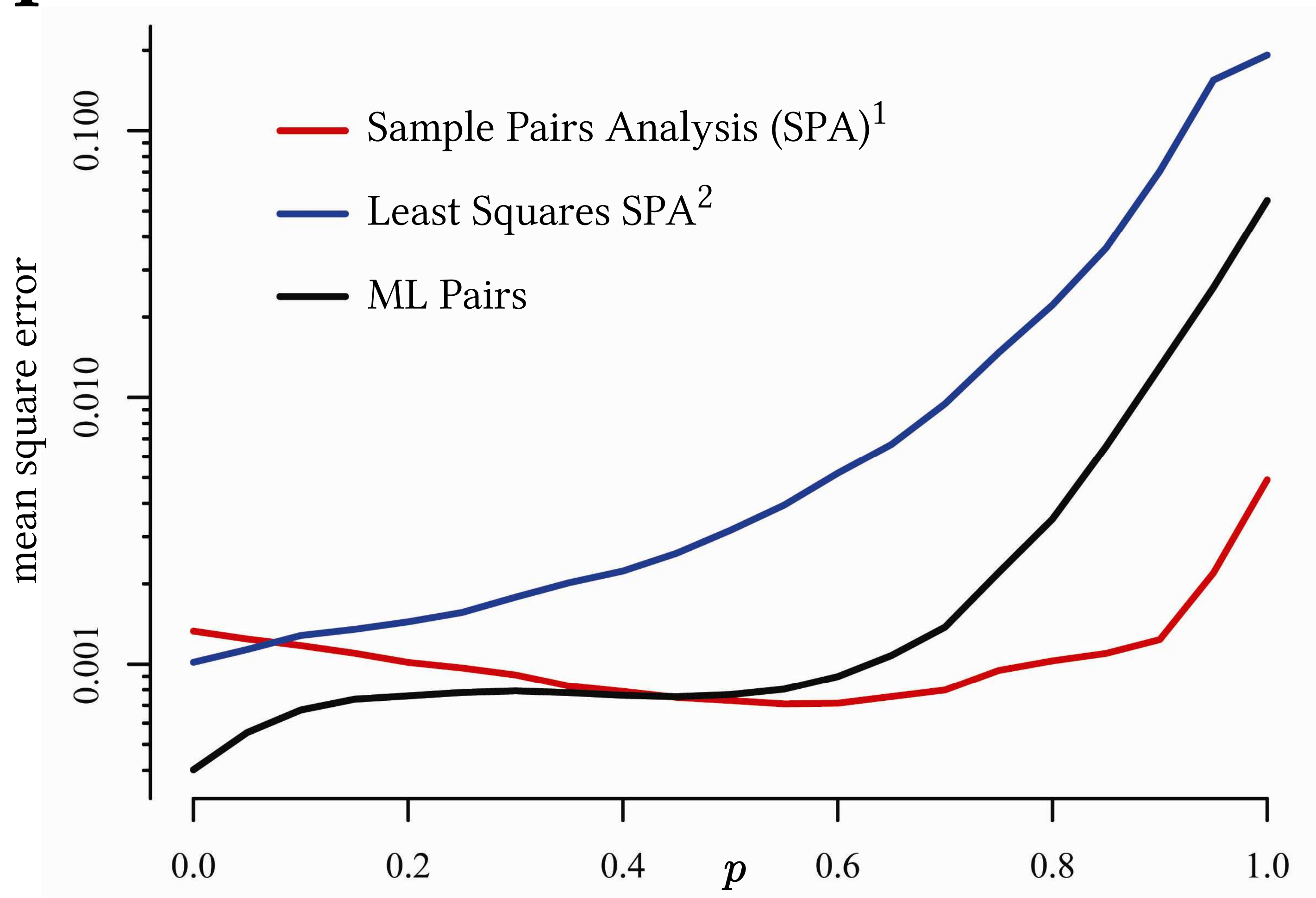
Experimental Results



[1] S. Dumitrescu *et al. Detection of LSB steganography via sample pair analysis.* IEEE Transactions on Signal Processing 51(7): 1995–2007. 2003.

[2] P. Lu *et al. An improved sample pairs method for detection of LSB embedding.* 6th Information Hiding Workshop, Springer LNCS 3200: 116–127. 2004

Experimental Results



For 1 Mpixel images, benchmarks:

- SPA and Least Squares SPA: 21 images/sec
- ML Pairs: 0.4 images/sec

Widening the Application

Other structural steganalyses, e.g.

- of LSB replacement in triplets of pixels[1]
- of replacement of two-least significant bits[2] ("2LSB")

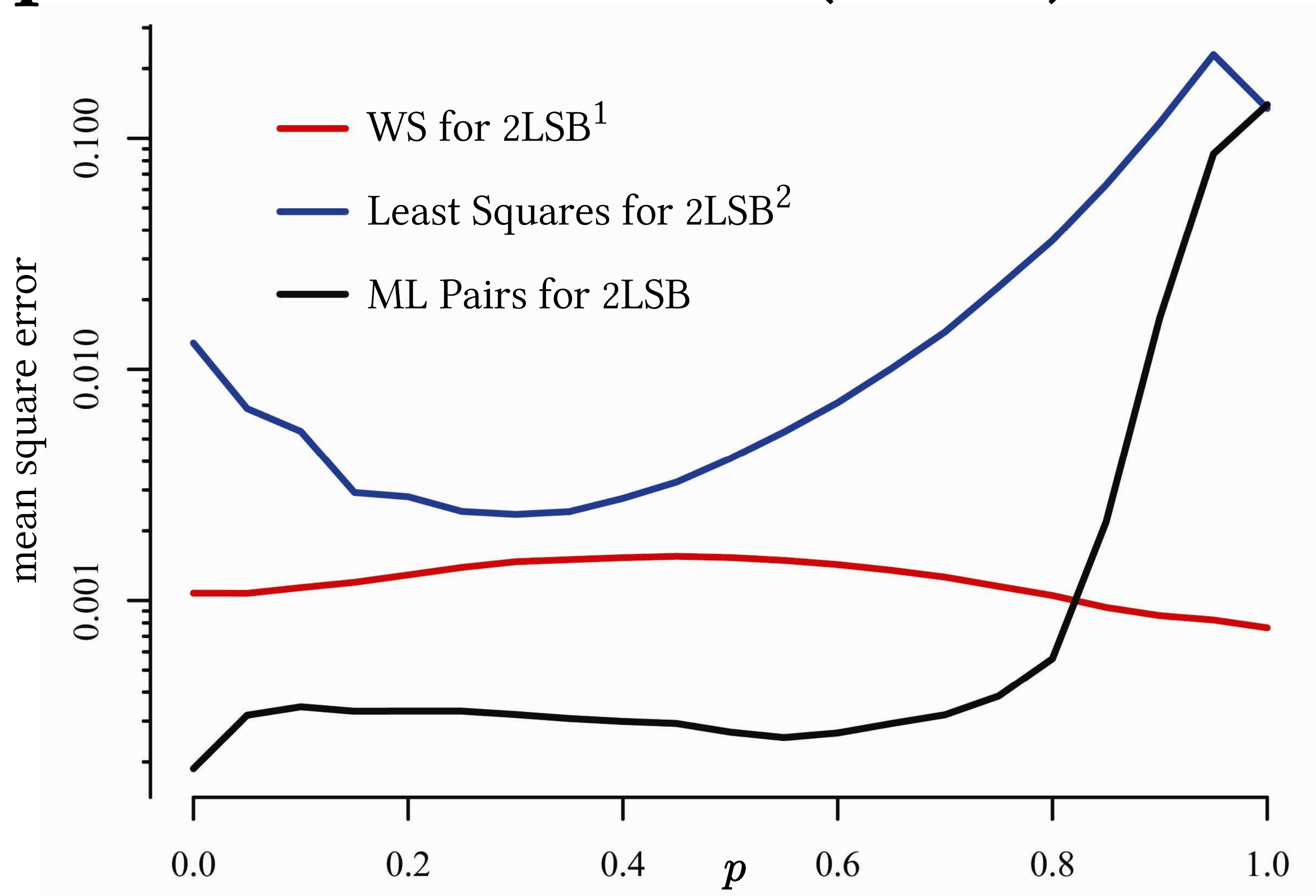
can receive the same treatment.

Sketch details in the paper; principles the same, algebra even more complex.

[1] A. Ker. *A general framework for the structural steganalysis of LSB replacement.* 7th Information Hiding Workshop, Springer LNCS 3727: 296–311. 2005.

[2] A. Ker. *Steganalysis of Embedding in Two Least Significant Bits.* IEEE Trans. Information Forensics and Security 2(1): 46–54. 2007.

Experimental Results (2LSB)



[1] X. Yu *et al. Extended optimization method of LSB steganalysis.* IEEE International Conference on Image Processing, vol. 2: 1102–1105. 2005

[2] A. Ker. *Steganalysis of Embedding in Two Least Significant Bits.* IEEE Trans. Information Forensics and Security 2(1): 46–54. 2007.

"Pre-cover"	**Cover object**

$$
\begin{tikzcd}[row sep=small]
 & \mathcal{E}_m \\
\mathcal{D}_m \arrow[ur, "\frac{1}{2}"] \arrow[dr, "\frac{1}{2}"'] & \\
 & \mathcal{O}_m
\end{tikzcd}
$$

This model is validated in the literature, **except for** $m = -1, 0, 1$

Conclusions

- It is possible to produce a statistically-rigorous likelihood analysis of the structure of bit replacement.

  The method presented here extends to other structural analyses.

- Estimation via the ML/structural combination is usually more accurate than ML or structural steganalysis alone…

  but the algebraic complexity and computational costs are inflated.

- Sometimes the maximization is computationally infeasible.

  This is a subject for further work:

  - *model pre-cover parametrically?*
  - *use derivative in optimization algorithm?*

- Need to refine the cover model to improve performance on large payloads.

  This is a subject for further work.

End

adk@comlab.ox.ac.uk