From Blind to Quantitative Steganalysis

Tomáš Pevný[1], Jessica Fridrich[2], Andrew D. Ker[3]

[1]GIPSA-Lab, INPG, France
[2]Binghamton University, SUNY, USA
[3]University of Oxford, UK

19th January 2009

Outline

Outline

Steganalysis × Quantitative Steganalysis

Steganalysis

- *Steganalysis* detects presence of secret message.
- *Steganalyzer* is a binary detector (classifier).

Quantitative steganalysis

- *Quantitative steganalysis* estimates number of embedding changes (length of message).
- *Quantitative steganalyzer* is an estimator.

Time for Change

Advantages of Quantitative Steganalysis

- provide the steganalyst with further information (estimate of message length).
- useful for forensic analysis (message is encrypted).
- important in pooled steganalysis.[a]
- allow a finer control of false positive and false negative rate in targeted blind steganalysis.
- alleviate problems with dependence of the steganalyzer on message length in the training set.[b]

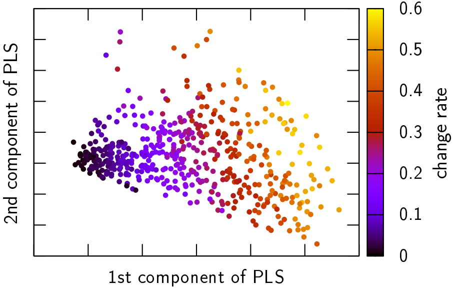
[a] A. D. Ker, *Batch Steganography and Pooled Steganalysis*, 2006.
[b] *Cancelli et al., A Comparative Study of* ± 1 *Steganalyzers, 2008.*

Outline

Methodology

Assumption

- *Steganographic features* used in blind steganalysis *react predictably* to the number of embedding changes.
- Identify relationship between *feature vector* and *change rate*



First two most significant components of merged features of nsF5 identified by Partial Least Square.

Quantitative Steganalysis by Regression

Problem

- We seek a function $\psi : \mathscr{X} \mapsto [0,1]$ revealing relationship between location of *feature vector* and *change rate* ($\mathscr{X}$ is the feature space).
- Function ψ is learned from a set of examples $\{(\mathbf{x}_1, y_1), \ldots, (\mathbf{x}_l, y_l)\}$, $\mathbf{x}_i \in \mathscr{X}$ features of stego image with change rate y_i.

- Construction of a quantitative steganalyzer is a regression problem, for which many tools are available.
- This work utilizes
  - linear ordinary least-square regression,
  - support vector regression.

Advantages over Prior Art

Prior art

Quantitative steganalyzers are built from heuristic principles and *always* rely on full knowledge of embedding algorithm.

Advantages of proposed method

- Cookie cutter approach:
  1. Find feature set detecting the stego algorithm.
  2. Create set of training examples $(\mathbf{x}_i, y_i)$.
  3. Use regression to learn dependence between features and change rate.
- The knowledge of embedding mechanism is not needed.

Outline

Experimental Settings

- Quantitative steganalyzers for 8 steganographic methods: JP Hide&Seek, Jsteg, MBS1, MMx, F5 with removed shrinkage (nsF5), OutGuess, Perturbed Quantization (PQ), and Steghide.
- Quantitative steganalyzers were constructed by
  - linear ordinary least-square regression (OLS)
  - support vector regression (SVR).
- Single-compressed JPEGs with quality factor 80, all created from 9163 raw images evenly divided into training/testing set.
- Random payload between zero and maximum for given image and algorithm was embedded into images.
- 274 "calibrated merged features" augmented by number of non-zero DCTs.

Outline

Detection Accuracy of MB1 and MMx

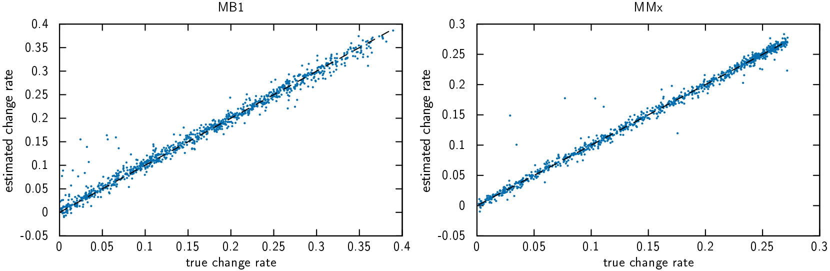


Figure: Estimated versus true relative change rate of SVR quantitative steganalyzers of MB1 and MMx.

Experimental Results

	OLS		SVR	
Algorithm	MAE	Bias	MAE	Bias
JP Hide&Seek	$7.91 \cdot 10^{-03}$	$-1.70 \cdot 10^{-04}$	$5.24 \cdot 10^{-03}$	$2.41 \cdot 10^{-04}$
Jsteg	$8.38 \cdot 10^{-03}$	$-5.29 \cdot 10^{-04}$	$1.9 \cdot 10^{-03}$	$2.5 \cdot 10^{-04}$
nsF5	$8.39 \cdot 10^{-03}$	$-5.29 \cdot 10^{-04}$	$4.82 \cdot 10^{-03}$	$-2.51 \cdot 10^{-04}$
MB1	$9.07 \cdot 10^{-03}$	$3.86 \cdot 10^{-05}$	$6.63 \cdot 10^{-03}$	$-1.63 \cdot 10^{-04}$
MMX	$3.25 \cdot 10^{-03}$	$1.58 \cdot 10^{-04}$	$2.70 \cdot 10^{-03}$	$1.08 \cdot 10^{-04}$
Steghide	$3.23 \cdot 10^{-03}$	$2.60 \cdot 10^{-04}$	$2.04 \cdot 10^{-03}$	$1.80 \cdot 10^{-04}$
PQ	$5.69 \cdot 10^{-02}$	$-2.89 \cdot 10^{-03}$	$4.83 \cdot 10^{-02}$	$-3.78 \cdot 10^{-02}$
OutGuess	$2.53 \cdot 10^{-03}$	$1.51 \cdot 10^{-04}$	$2.48 \cdot 10^{-03}$	$3.67 \cdot 10^{-04}$

Table: Median absolute error (MAE) and bias measured on testing images with random payload.

Outline

Compound Error

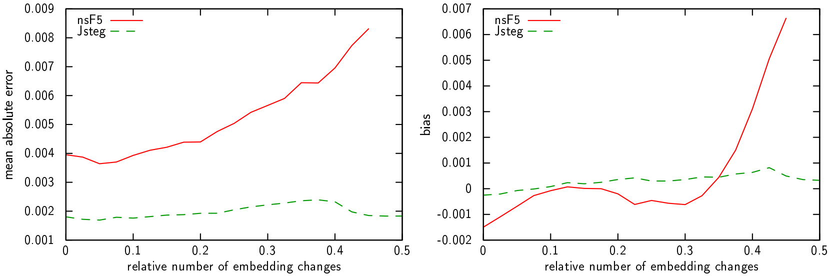


Figure: Median absolute error (MAE) and bias of SVR based estimators of nsF5 and Jsteg on 21 different fixed embedding change rates.

Outline

Comparison to Previous Art

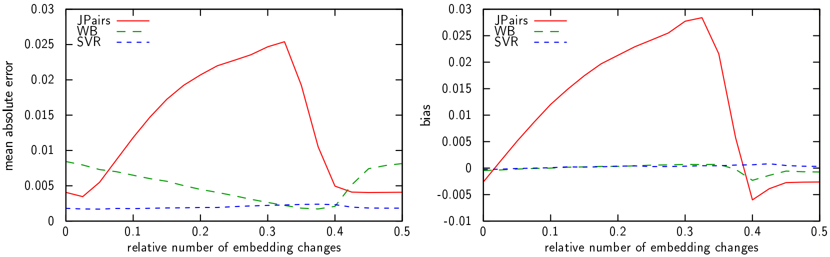


Figure: Comparison of accuracy of SVR, Jpairs, and Weighted non-steganographic Borders attack (WB) at 21 different fixed embedding change rates on 4563 images from testing set.

Outline

Conclusion

Conclusion

- A solid method to construct quantitative steganalyzer from features was presented.
- Regression is used to learn dependence between features for blind steganalysis and embedding change rate.
- Method was demonstrated on 8 JPEG stego-schemes.
- For Jsteg, accuracy is at least as good as best targeted attacks.
- Distributions of within image and between image error were estimated — same as of quantitative steganalyzers of LSB replacement.

Future Directions

Future directions

- Combine existing LSB quant. steganalyzers to improve accuracy.
- Improve control of false positive/false negative rate in targeted blind steganalysis.
- Quantitative steganalysis of ± 1, YASS?

Within and Between Image Error of Jsteg

	Jsteg			
β	Shapiro-Wilk $p > 0.1$	Between IQR $\Delta Q(Z_{cov})$	Within IQR $\Delta Q(Z_{pos})$	Flips IQR $\Delta Q(Z_{flip})$
0	–	3.63	0.00	0.00
0.025	90.2%	3.23	1.52	0.28
0.05	89.9%	3.02	1.91	0.39
0.125	90.2%	2.79	2.57	0.59
0.25	89.8%	2.87	3.25	0.78
0.375	90.3%	3.69	3.56	0.87

Within and Between Image Error of nsF5

	nsF5			
β	Shapiro-Wilk $p > 0.1$	Between IQR $\Delta Q(Z_{cov})$	Within IQR $\Delta Q(Z_{pos})$	Flips IQR $\Delta Q(Z_{flip})$
0	–	7.74	0.00	0.00
0.025	93.9%	6.99	2.81	0.29
0.05	93.9%	6.79	3.52	0.41
0.125	93.7%	6.93	4.78	0.62
0.25	94.2%	8.31	6.77	0.81
0.375	94.2%	10.63	8.47	0.91