Explaining the Bag Gain in Batch Steganography

Eli Dworetzky, Jessica Fridrich

IH&MMSEC 2023

BINGHAMTON UNIVERSITY
STATE UNIVERSITY OF NEW YORK

Batch / Pooled Stego

Alice

- spreads payload across a bag of images
- maintains fixed communication rate $r > 0$

Warden

- inspects a bag of B images $\mathbf{X} = (X_1, \ldots, X_B)$
- has a single-image detector d
- pools the soft outputs[1] $d(X_1), \ldots, d(X_B)$ to decide:

$$\begin{aligned} \mathcal{H}_0 : \quad & \mathbf{X} \text{ is cover} \quad (r = 0) \\ \mathcal{H}_1 : \quad & \mathbf{X} \text{ is stego} \quad (r > 0) \end{aligned}$$

[1] E.g. logits of neural network, outputs of quantitative steganalyzer, projection of linear classifier in a rich model, etc.

Who knows what

Alice does **not** need to know Warden's

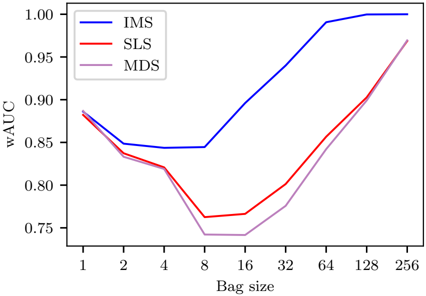
- detector d
- pooling method

Warden knows Alice's

- communication rate $r > 0$
- bag size B
- stego scheme
- spreading strategy
- cover source to train d

Performance vs. Bag Size

- Best pooler[2] for 3 spreading strategies
  - IMS: Image Merging Sender
  - SLS: Shift-limited Sender
  - MDS: Minimum Deflection Sender
- Fixed rate $r = 0.3$ bpp (HILL, ALASKA II)



[2] Y. Yousfi, E. Dworetzky, J. Fridrich, "Detector-Informed Batch Steganography and Pooled Steganalysis", IH&MMSEC 2022.

Warden's Pooler

- Suppose detector outputs $d(X_1), \ldots, d(X_B)$ are Gaussian r.v.s
- Embedding payload α_i in image X_i shifts the mean by $b_i \alpha_i$
- The parameter b_i reflects the difficulty of steganalyzing image X_i

$$
\begin{aligned}
\mathcal{H}_0 : \quad & d(X_i) \sim \mathcal{N}(0, 1) \quad \text{for all } i \\
\mathcal{H}_1 : \quad & d(X_i) \sim \mathcal{N}(b_i \alpha_i, 1) \quad \text{for all } i
\end{aligned}
$$

- Mean-shifted Gauss-Gauss problem $\Longrightarrow$ Warden's most powerful pooler is a correlator
- Deflection coefficient describes detectability in bag $\mathbf{X}$

$$
\Delta^2(\mathbf{X}) = \sum_{i=1}^{B} b_i^2 \alpha_i^2
$$

Alice's Cover Source

Alice's cover source has two types of images: easy and hard.

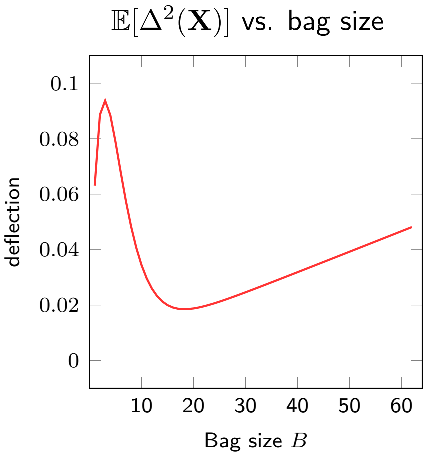
Hard to steganalyze (complex content / strong noise)

- $b_i = \varepsilon > 0$ (small)
- selected with probability $p \in (0, 1)$

Easy to steganalyze (smooth content / weak noise)

- $b_i = 1$
- selected with probability $1 - p$

Bag loss and bag gain ($\varepsilon = 0.05$, $p = 0.3$)



Bag loss and bag gain in ALASKA II