Observing Bag Gain in JPEG Batch Steganography

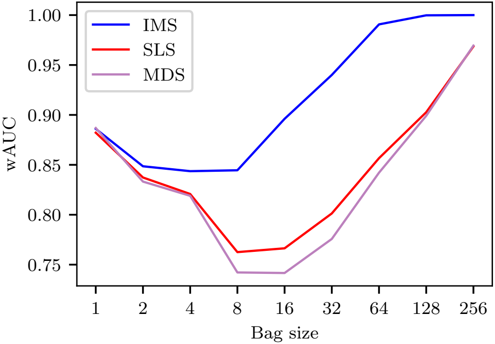
Edgar Kaziakhmedov, Eli Dworetzky, and Jessica Fridrich

IEEE WIFS 2023

BINGHAMTON UNIVERSITY
STATE UNIVERSITY OF NEW YORK

Bag Gain

- Alice spreads her payload across B images (a bag)
- Alice maintains a fixed positive rate (payload $\propto B$)
- Alice embeds more in "hard" images and less in "easy" images
- Warden steganalyzes the bag



Previous work on the bag gain

- First described in Y. Yousfi, E. Dworetzky, J. Fridrich, "Detector-Informed Batch Steganography and Pooled Steganalysis", IH&MMSec 2022
- Bag gain was observed for all studied spreading strategies
  - IMS: Image Merging Sender (ICASSP 2017)
  - SLS: Shift-limited Sender (IH&MMSec 2022)
  - MDS: Minimum Deflection Sender (IH&MMSec 2022)
- Explained in E. Dworetzky, J. Fridrich, "Explaining the Bag Gain in Batch Steganography", IEEE TIFS, vol. 18, pp. 3031-3043, 2023.

Focus of this paper

- Experimental study of the bag gain in the JPEG domain
  - Across different quality factors, rates, bag sizes
  - When Alice maintains fixed bpc or bpnzac
  - With different options for Warden's detector and pooler
- Explain some observed trends from a model

Batch steganography / pooled steganalysis[2]

Alice

- spreads payload across a bag of B images $\mathbf{X} = (X_1, \ldots, X_B)$

Warden

- has a single-image detector (SID) d and pools its soft outputs[1] $d(X_1), \ldots, d(X_B)$ to decide:

$$
\begin{aligned}
\mathcal{H}_0 : &\quad \mathbf{X} \text{ is cover bag} \\
\mathcal{H}_1 : &\quad \mathbf{X} \text{ is stego bag}
\end{aligned}
$$

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

[2] A. D. Ker "Batch steganography and pooled steganalysis" IH 2006

Who knows what

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

- detector d
- pooling method

Warden knows Alice's

- bag size B
- stego scheme
- cover source to train d

Alice's batch senders

IMS (Image Merging Sender)

- Alice considers the bag as one big image
- Content-adaptive scheme spreads the payload

MDS (Minimum Deflection Sender)

- Alice trains her own detector & adopts a model of its soft output
- Her detector "spreads the payload" by minimizing deflection of the optimal pooler

Warden's poolers[3]

Simple average (not aware of the spreading strategy)

$$\pi_{\mathrm{AVG}}(\mathbf{X}) = \frac{1}{B}\sum_{i=1}^{B} d(X_i)$$

Correlator (aware of the spreading strategy and rate r)

$$\pi_{\mathrm{COR}}(\mathbf{X}) = \sum_{i=1}^{B} d(X_i)\hat{\alpha}_i$$

[3] max pooler $\pi_{\mathrm{MAX}}(X_i) = \max_i d(X_i)$ performed poorly, poolers trained as Gaussian SVMs had the same performance as correlator

Setup of experiments

- ALASKA II dataset with 75,000 images split into three parts (Split 1, 2, and 3)
  - Each split divided into 22k / 1k / 2k images for TRN / VAL / TST
  - QF: 75, 85, 90, 95, 98
- **Alice**
  - J-UNIWARD on RD bound
  - two payload constraints (bpc and bpnzac)
  - two batch senders (IMS, MDS)
- **Warden**
  - two SIDs (binary, quantitative)
  - two poolers (AVG, CORR)

Alice's and Warden's detectors

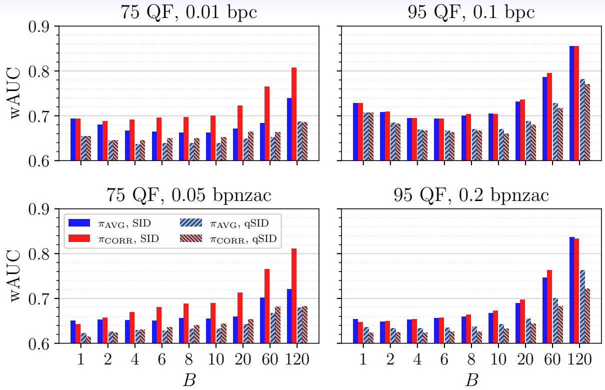
- **Alice**: MDS uses feedback from Alice's detector d_A trained as SRNet1 on Split 1 with payloads uniformly sampled from the set

$$\mathcal{P} = 0.05, 0.1, 0.2, \ldots, 0.9, 1 \text{ bpnzac}$$

- **Warden**: uses two types of detectors:
  - binary SID d as SRNet2 on Split 2 on $\mathcal{P}$
  - quantitative detector qSID, SRNet trained as payload regressor on

$$\mathcal{P}_\text{fine} = 0, 0.01, 0.02, ..., 0.09, 0.1, 0.2, \ldots, 0.9, 1 \text{ bpnzac}$$

wAUC as a function of bag size for IMS

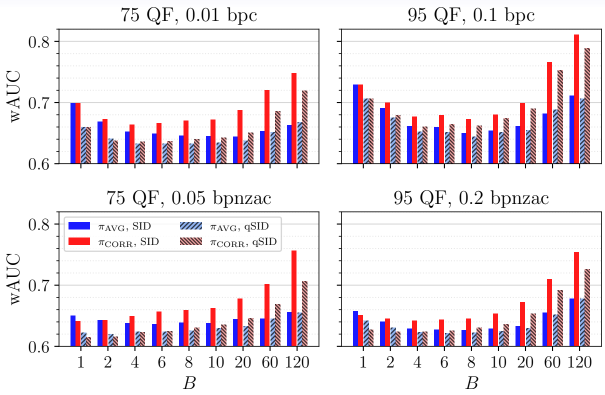


For Alice: Bag gain absent for payload in bpnzac

Bag gain present for bpc, more pronounced for QF 95 than 75

For Warden: binary SID generally better than quantitative qSID, correlator better than simple average

wAUC as a function of bag size for MDS

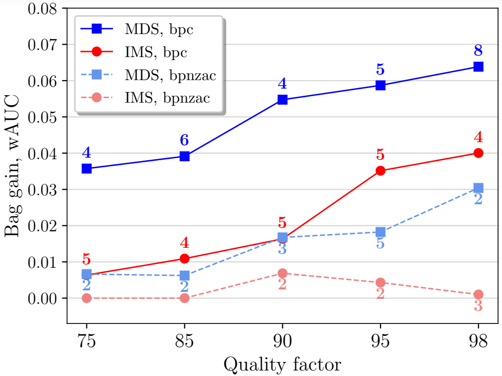


For Alice: Bag gain much more pronounced than for IMS (up to 0.065 wAUC)

Observed for both bpc and bnzac payload constraints

For Warden: Binary SID better than quantitative qSID, correlator better than simple average

Effect of quality factor (best pooler and SID)



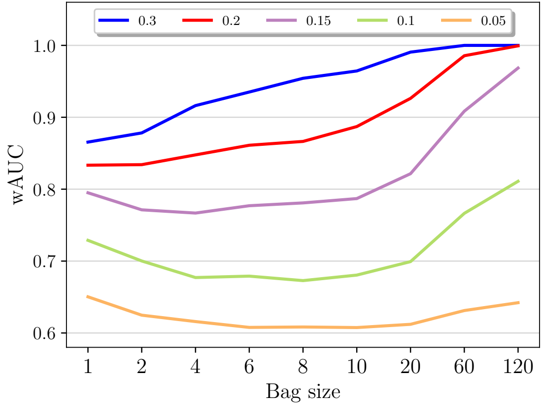
For Alice: MDS has a larger bag gain than IMS

Bag gain is larger for rates in bpc than in bpnzac

Bag gain generally increases with QF

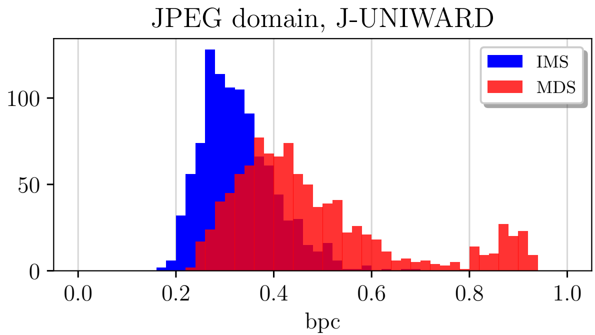
Optimal bag size is within a range relevant for practitioners

Effect of rate (in bpc), QF95



Bag gain is absent for rates $r \gtrsim 0.2$ bpc
Optimal bag size decreases with increased rate

Spreader's aggressiveness, QF95, B=15



Histogram of largest payload assigned in a bag

MDS is more aggressive than IMS; MDS exhibits larger bag gain

Conclusions

The bag gain relates to gain in security the sender can enjoy by selecting optimal bag size in batch steganography

Message for Alice

- Use optimal bag size for batch steganography for better security
- Optimal bag size depends on rate and QF
- Bag gain is larger for large JPEG qualities and when maintaining payload in bpc rather than bpnzac (see the paper for the analysis)
- Bag gain is absent for large enough rates

For the Warden

- Pooling soft outputs of a binary detector is better than with a quantitative detector
- Use the correlator pooler if you know the spreading strategy