Data Augmentation for JPEG Steganalysis

Tomer Itzhaki, Yassine Yousfi, and Jessica Fridrich

WIFS 2021

BINGHAMTON UNIVERSITY
STATE UNIVERSITY OF NEW YORK

Introduction

- CNNs $>>$ Rich models.
- But more data hungry $\Longrightarrow$ Need to augment training datasets.
- For steganalysis $=$ important to augment without destroying the stego signal.
- The typical augmentations used are rotations and flips (D4).
- Can we do better with other augmentations?
- Note that RMs also used "augmentation-like" trick - feature symmetrization.

Experimental setting

- Alaska II 256×256 QFs 75, 90, and 95 [Cogranne et al. WIFS2020].
- EfficientNet B3 (trained as in Alaska II) [Yousfi et al. WIFS2020].
- Color J-UNIWARD using CCM.
- Grayscale J-MiPOD and nsF5.

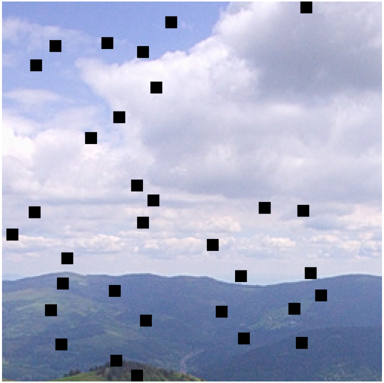
Our findings

- Can significantly increase performance with little to no cost using data augmentation beyond D4.
- Up to 3% in accuracy and 5% in MD5.
- Smaller datasets are likely to benefit more from the studied augmentation.

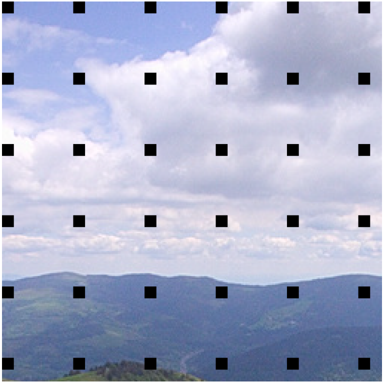
"Dropout" augmentations

- Randomly set a set of pixels to zero.
- Usually rectangles/squares.
- Simulates occlusions.

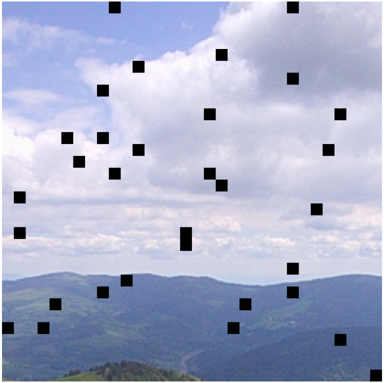
Coarse dropout



Grid dropout



Random grid dropout



“Channel” augmentations

- For color steganography.
- Augmenting using channels (RGB).
- Simulates images with different color compositions.

Channel shuffle

To gray

“Mixing” augmentations

- Mixing two images from different classes.
- Changing the label accordingly to a soft-label.

BitMix

BitMix

$$
\begin{aligned}
X &= M \odot C + (1 - M) \odot S \\
\lambda &= \frac{\|M \odot C - M \odot S\|_1}{\|C - S\|_1} \\
y_X &= (\lambda, 1 - \lambda)
\end{aligned}
$$

M binary mask, C, S cover, stego image, y_X soft label

ConvexMix

$$
\begin{aligned}
X &= \lambda C + (1-\lambda)S \\
y_X &= (\lambda, 1-\lambda)
\end{aligned}
$$

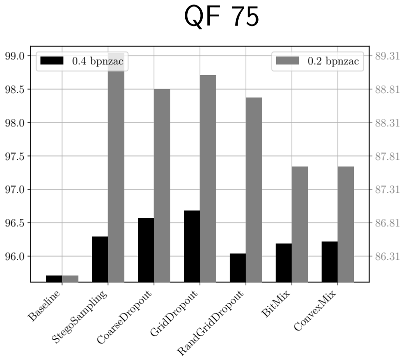
C, S cover, stego image, y_X soft label

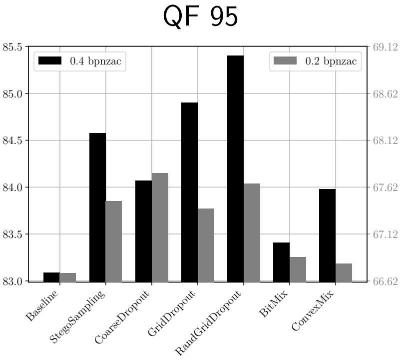
Stego Sampling

- Sample different stego images from the embedding simulator.
- Inflates the stego class.
- Requires sampling stego images on the fly - pre-computing change rate maps.

Results

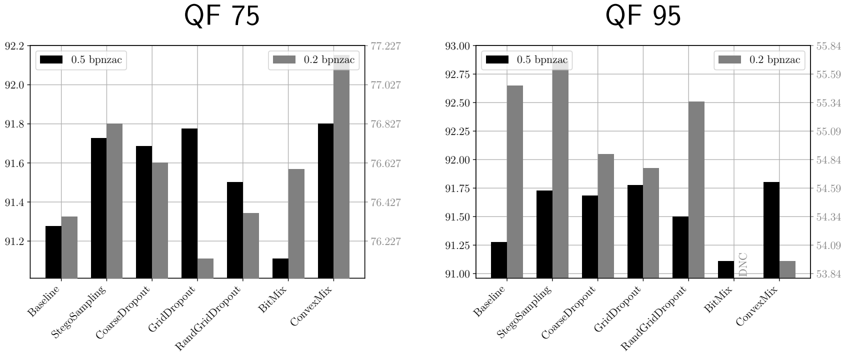
J-UNIWARD



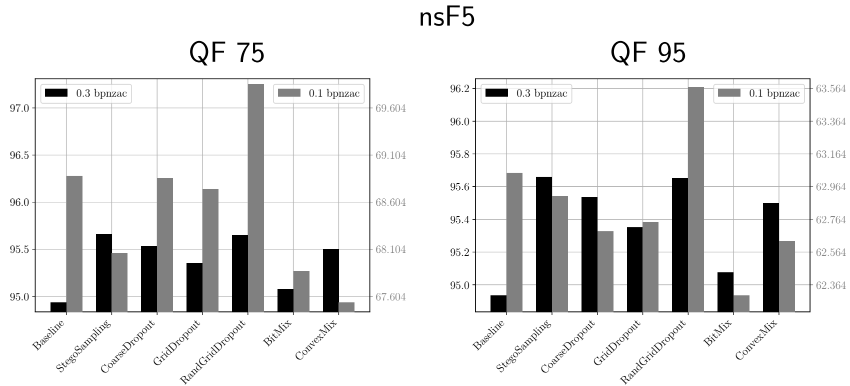


Results

JMiPOD



Results


nsF5
QF 75
QF 95
0.3 bpnzac
0.1 bpnzac
97.0
96.5
96.0
95.5
95.0
69.604
69.104
68.604
68.104
67.604
96.2
96.0
95.8
95.6
95.4
95.2
95.0
63.564
63.364
63.164
62.964
62.764
62.564
62.364
Baseline
StegoSampling
CoarseDropout
GridDropout
RandGridDropout
BitMix
ConvexMix

Low data regime

Data Augmentation	Accuracy	MD5	FP80	wAUC
$66,000$ training images				
Baseline, YCrCb	95.3841	0.0232	0.0016	0.9966
CoarseDropout	96.5672	0.0158	0.0013	0.9975
$10,000$ training images				
Baseline, YCrCb	0.8881	0.1701	0.0335	0.9797
CoarseDropout	0.9029	0.1488	0.0293	0.9812

Conclusions and future directions

Summary

- Beyond D4, other augmentations can give a significant boost (up to 3% in accuracy and 5% in MD5)
- More beneficial in low data regimes.
- Using all augmentations increases performance but not significantly when compared to the best single augmentation.

Future

- More augmentations, e.g. adapt Pixels-off [Yedrouj et al. IH2020] to the JPEG domain or to an on-the-fly augmentation.
- Augmentations to be studied together with data scalability laws [Ruiz, Chaumont et al. ICPR2021].