Modern Steganalysis: The ALASKA II Challenge

Yassine Yousfi, yyousfi1@binghamton.edu

BINGHAMTON
UNIVERSITY
STATE UNIVERSITY OF NEW YORK

ALASKA Breakers II

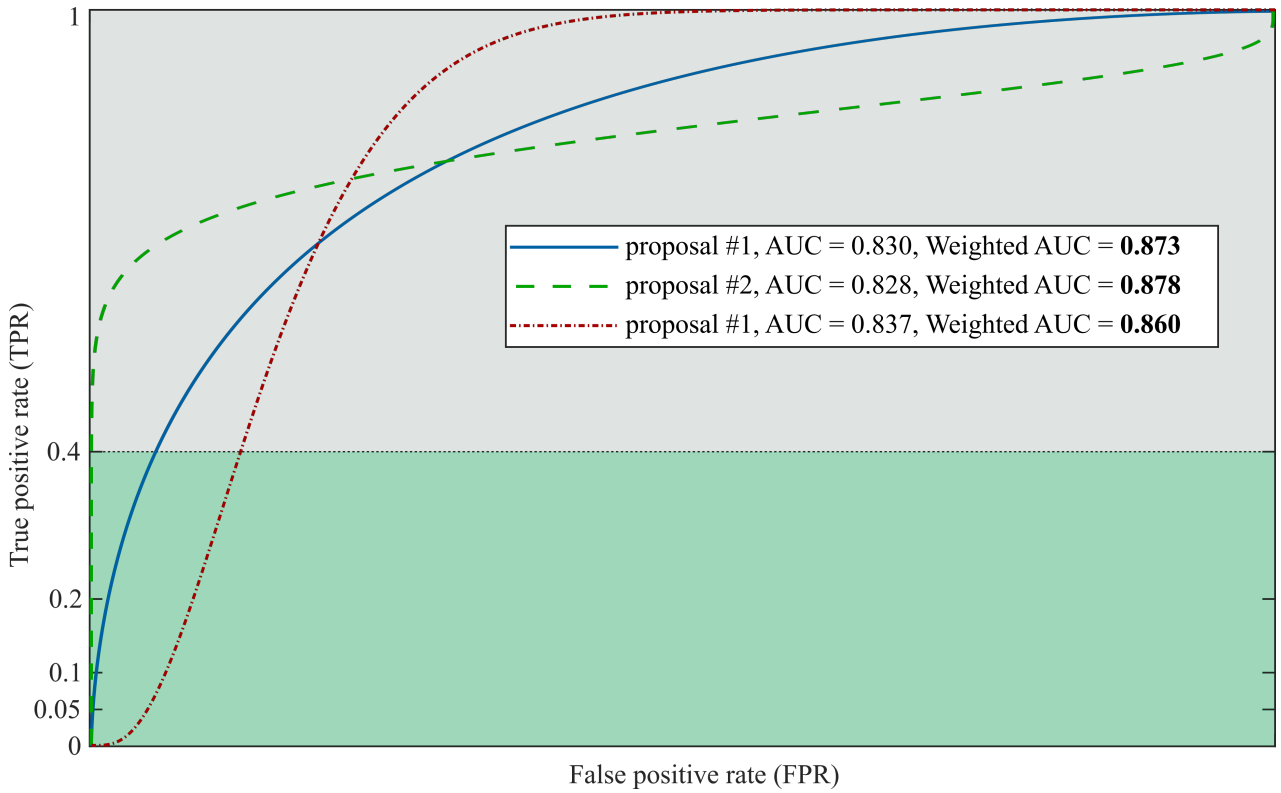
- Jessica Fridrich, *Binghamton*
- Jan Butora, *Binghamton*
- Eugene Khvedchenya, *Odessa, Ukraine*
- Yassine Yousfi, *Binghamton*

The ALASKA II Challenge

- Color JPEGs, payload embedding in Y, U and V (Y, Cr and Cb)
- Multiple stego schemes: J-UNIWARD, J-MiPOD (new), UERD
- Same image size 512×512
- Variable payload (DeLS scaled using rich models)
- 3 JPEG QFs 75, 90, 95
- Randomized cover image processing operations (resizing, sharpening, denoising, ...)
- Ordering images instead of hard decisions
- Submissions in the kaggle platform

Performance score

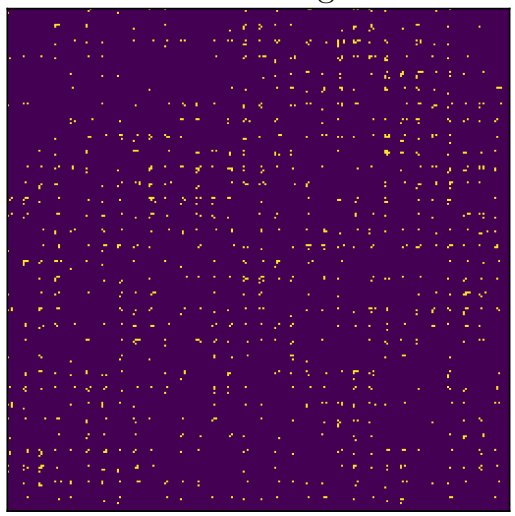
- Public + Private test set = 5,000 images
- Ordering (scoring) images allowed drawing the **ROC curve** in the back-end
- **wAUC**: weighted AUC



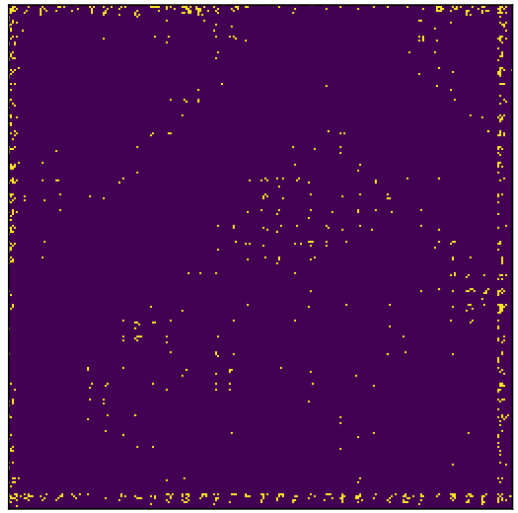
Faulty UERD

03460.jpg

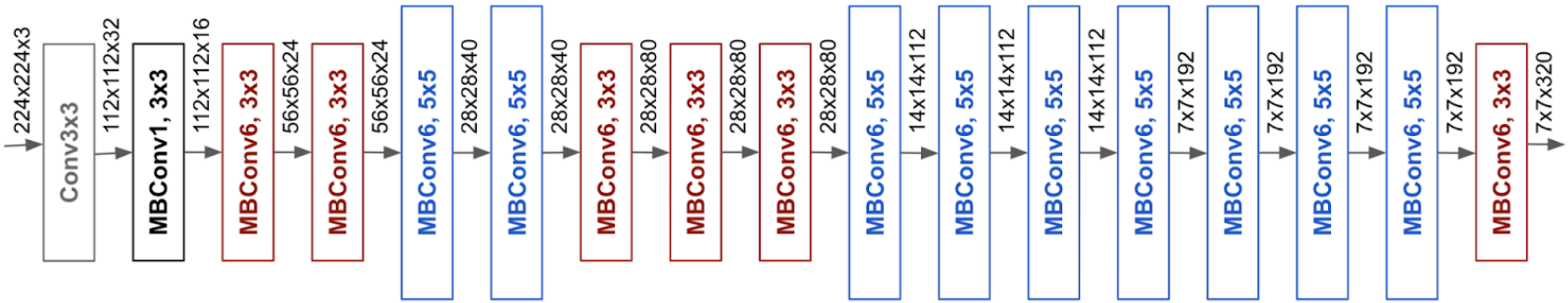
JUNI changes



UERD changes



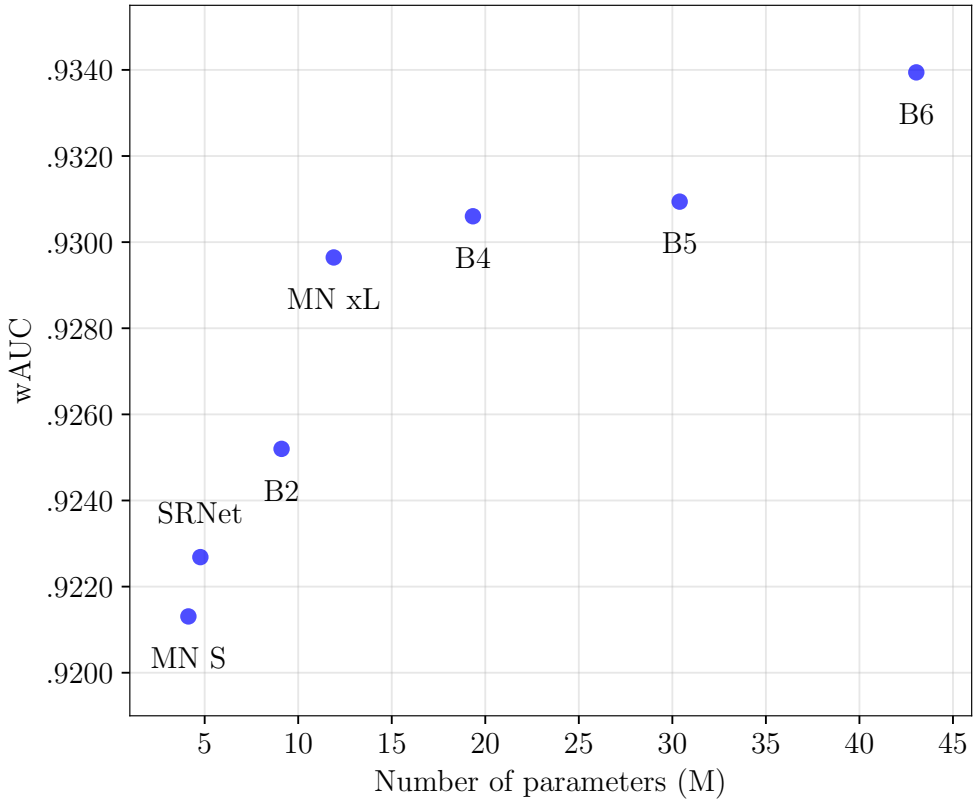
Out of the box EfficientNet



Out of the box EfficientNet

- Pretrained on ImageNet (1.3M images - 1k classes)
- Converges without any steganalysis trick (faulty UERD helped the nets converge)
- No Pair Constraint training
- Trains fast

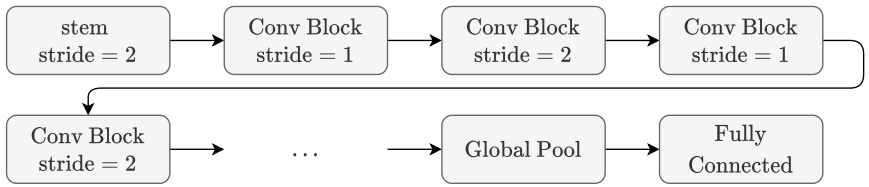
Out of the box EfficientNet



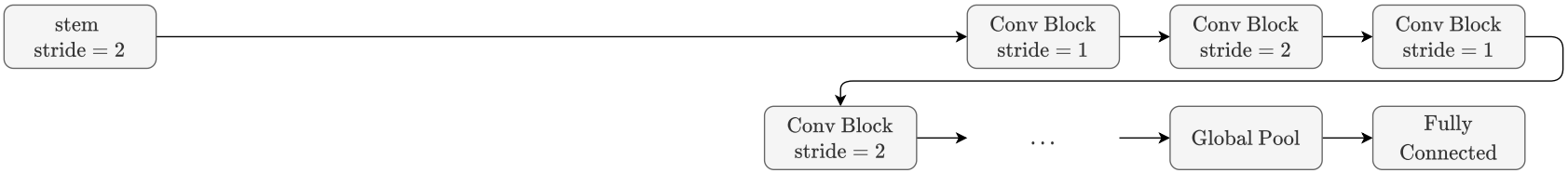
Surgeries

- Add steganalysis architecture pattern to EfficientNet
- Unpooled layers!
- Remove the stride and pooling in the first conv layer (memory intensive)
- Insert even more unpooled layers in the stem (good computational trade-off)

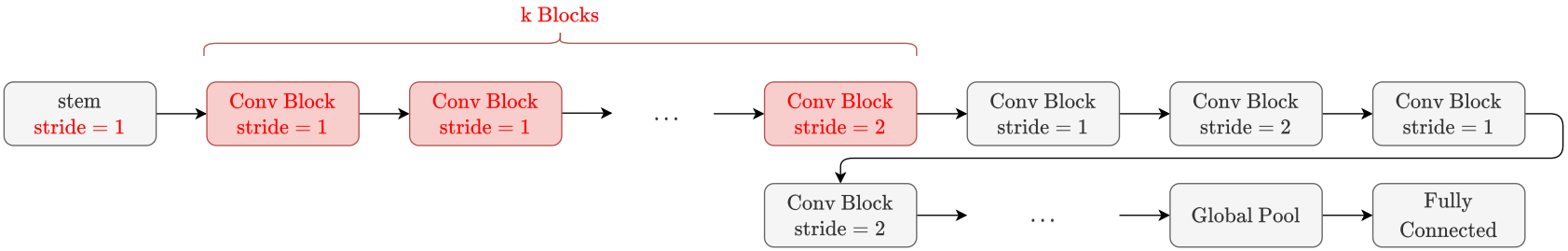
Surgeries


stem
stride = 2
Conv Block
stride = 1
Conv Block
stride = 2
Conv Block
stride = 1
Conv Block
stride = 2
...
Global Pool
Fully
Connected

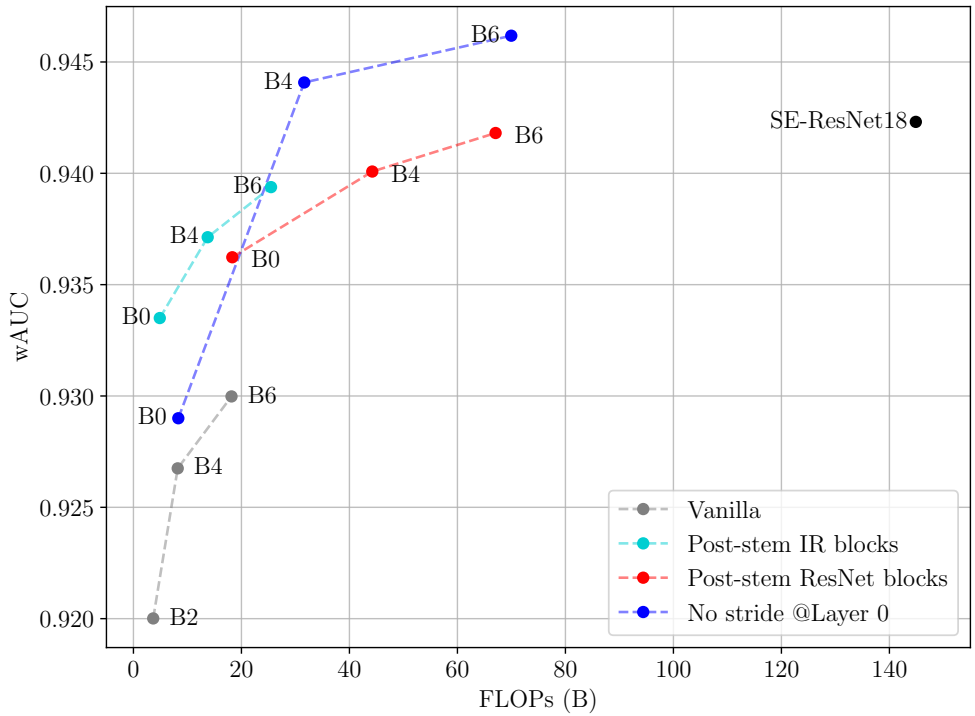
Surgeries


stem
stride = 2
Conv Block
stride = 1
Conv Block
stride = 2
Conv Block
stride = 1
Conv Block
stride = 2
...
Global Pool
Fully
Connected

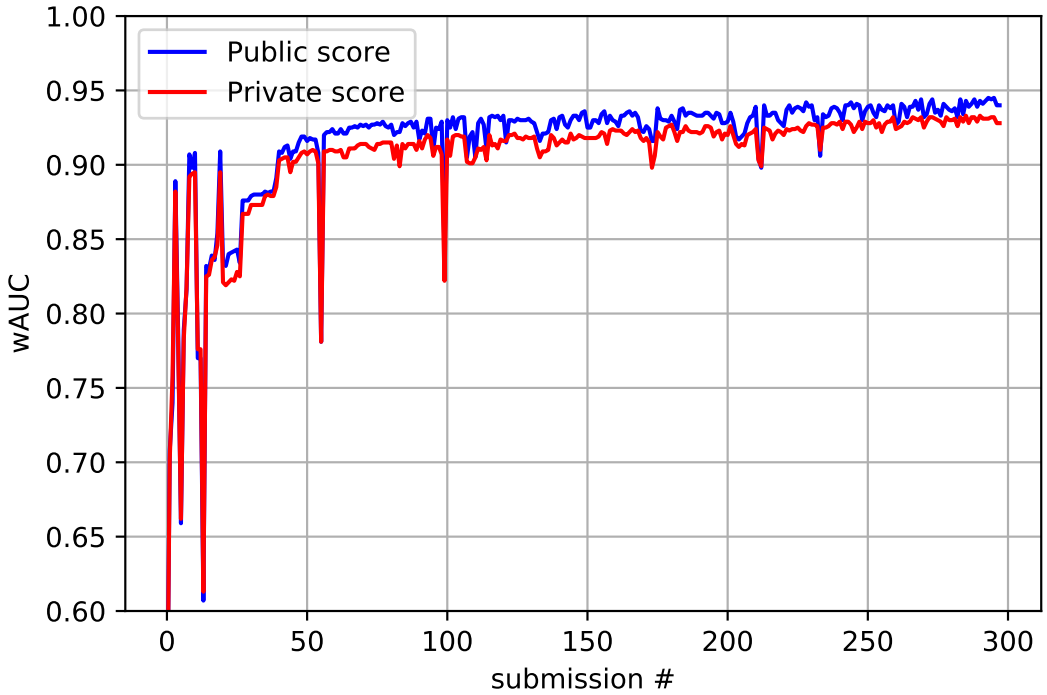
Surgeries


k Blocks
stem
stride = 1
Conv Block
stride = 1
Conv Block
stride = 1
...
Conv Block
stride = 2
Conv Block
stride = 1
Conv Block
stride = 2
Conv Block
stride = 1
Conv Block
stride = 2
...
Global Pool
Fully
Connected

Surgically Modified Nets



ABBA timeline



Lessons learned

- Pretraining helps speed and accuracy
- When do EfficientNet outperform SRNet
- How to make EfficientNet even better with reasonable compute (surgeries)
- Still learning ...
  - Understanding how CNNs arrive at their decision and extracting human readable knowledge
  - Using SOTA CNNs to algorithmically improve steganography (adversarial attacks)