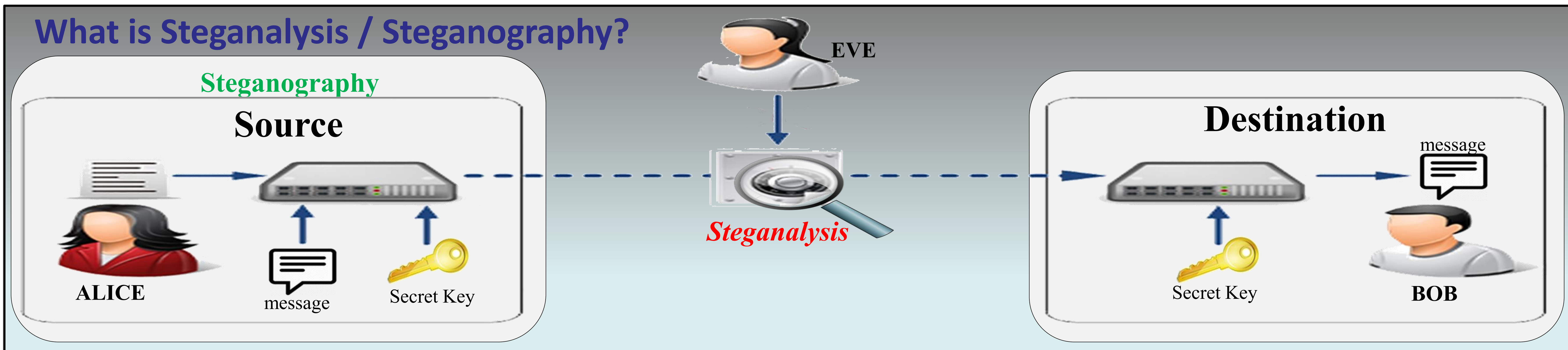
# Yedrouj-Net: An efficient CNN for spatial steganalysis

Mehdi Yedroudj, Marc Chaumont, Frédéric Comby

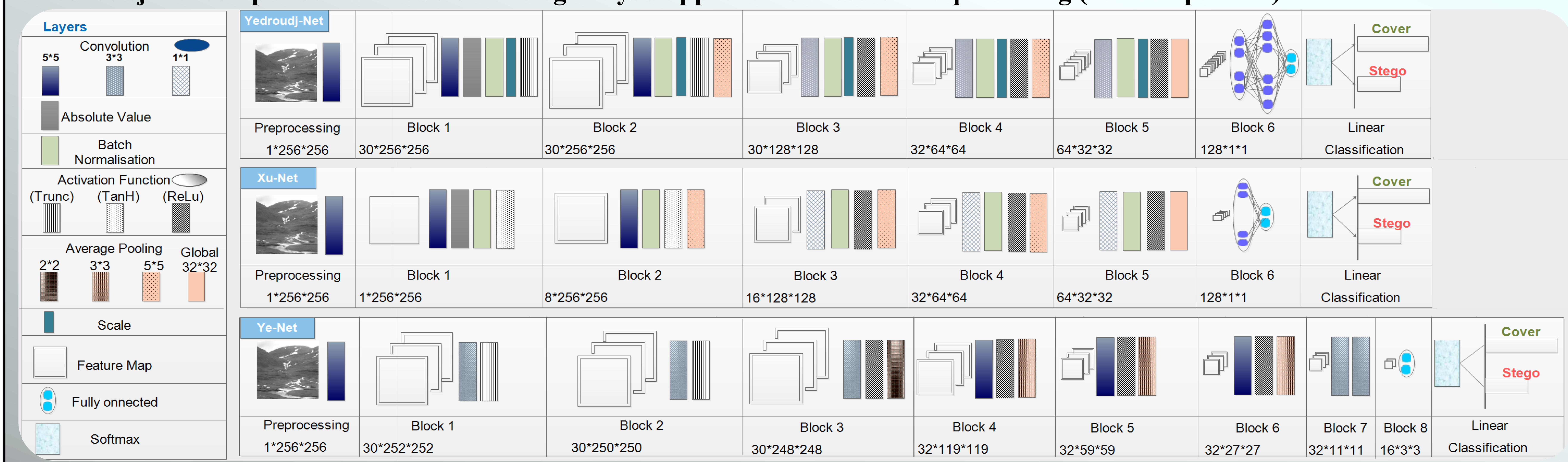
ICASSP 2018

## What is Steganalysis / Steganography?




## Proposed architecture

**Yedroudj-Net comparison with two other steganalysis approaches based on deep learning (fair comparison).**




Yedroudj-Net:

1. It has the advantage of using 30 SRM kernels which increases the diversity.
2. A shallow network compared to the Ye-Net equipped with a "value clipper" (hard tanh) activation function.
3. Thanks to batch normalization, Yedroudj-Net converges faster and is more robust with respect to hyperparameters.

## Results

### 1. *Clairvoyant protocol:*

- Resize the 10000 images of BOSSBase to 256*256.
- Use the two algorithms WOW and S-UNIWARD to generate the stegos.
- Select 1000 pairs from the training set for validation.
- Use the 5000 images of the test set to evaluate the obtained model.

**Comparison of Yedroudj-Net and three state-of-the-art steganalysis methods in terms of steganalysis probability of error.**

| | *BOSS 256×256* | | | |
|---|---|---|---|---|
| | **WOW** [6] | | **S-UNIWARD** [5] | |
| | 0.2 bpp | 0.4 bpp | 0.2 bpp | 0.4 bpp |
| SRM+EC [1], [2] | 36.5 % | 25.5 % | **36.6 %** | 24.7 % |
| Yedroudj-Net | **27.8 %** | **14.1 %** | **36.7 %** | **22.8 %** |
| Xu-Net [3] | 32.4 % | 20.7 % | 39.1 % | 27.2 % |
| Ye-Net [4] | 33.1 % | 23.2 % | 40.0 % | 31.2 % |

### 2. *Base augmentation protocol:*

- *Add 10 000 pairs of cover/stego of BOWS2Base to the training set (Clairvoyant protocol).*
- *Rotate and flip the 14000 images of the training set.*
- Use the 5000 images of the test set to evaluate the obtained model.

**Comparison of Yedroudj-Net's and two state-of-the-art steganalysis's probability of error against a steganographic algorithm WOW at a payload of 0.2 bit per pixel (bpp).**

| | *WOW 0.2 bpp* | | |
|---|---|---|---|
| | BOSS | BOSS+BOWS2 | BOSS+BOWS2+VA |
| Yedroudj-Net | **27.8** % | **23.7** % | **20.8** % |
| Ye-Net | 33.1 % | 26.1 % | 22.2 % |
| Xu-Net | 32.4 % | 30.3 % | 30.5 % |

## Conclusions

- An efficient approach based on deep learning (CNN) for steganalysis.
- Our method outperforms the state-of-the-art and others CNN-based models with and without taking extra measures (train set augmentation).
- Future work:
  1. Increase the size of the training set.
  2. Try other tricks such as transfer learning.
  3. Try an ensemble of Yedroudj-Nets.

## Related Work[7]

For an efficient database augmentation 2 options:

- Produce new images using the same cameras and development than the original base.
- Eve has an access to the original RAW images to use them for producing new images with similar developments.

## References


1. J. Fridrich and J. Kodovsky, "Rich Models for Steganalysis of Digital Images," IEEE Transactions on Information Forensics and Security, TIFS, vol. 7, no. 3, June 2012.
2. J. Kodovsky, J. Fridrich, and V. Holub, "Ensemble Classifiers for Steganalysis of Digital Media," IEEE Transactions on Information Forensics and Security, TIFS, vol. 7, no. 2, pp. 432–444, 2012.
3. G. Xu, H. Z. Wu, and Y. Q. Shi, "Structural Design of Convolutional Neural Networks for Steganalysis," IEEE Signal Processing Letters, vol. 23, no. 5, May 2016.
4. J. Ye, J. Ni and Y. Yi, "Deep Learning Hierarchical Representations for Image Steganalysis," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 11, pp. 2545-2557, Nov. 2017.
5. V. Holub, J. Fridrich, and T. Denemark, "Universal Distortion Function for Steganography in an Arbitrary Domain," EURASIP Journal on Information Security, JIS, vol. 2014, no. 1, 2014.
6. V. Holub and J. Fridrich, "Designing Steganographic Distortion Using Directional Filters," in Proceedings of the IEEE International Workshop on Information Forensics and Security, WIFS'2012, Spain, Dec.2012, pp. 234–239.
7. M.Yedroudj, M.Chaumont, F.Comby, "How to augment a small learning set for improving the performances of a CNN based steganalyzer?," MWSF'2018, Electronic Imaging2018, Burlingame, California, USA, 28 Jan - 2 Feb 2018.