Pixels-off: Data-augmentation Complementary Solution for Deep-learning Steganalysis

IH&MMSec2020

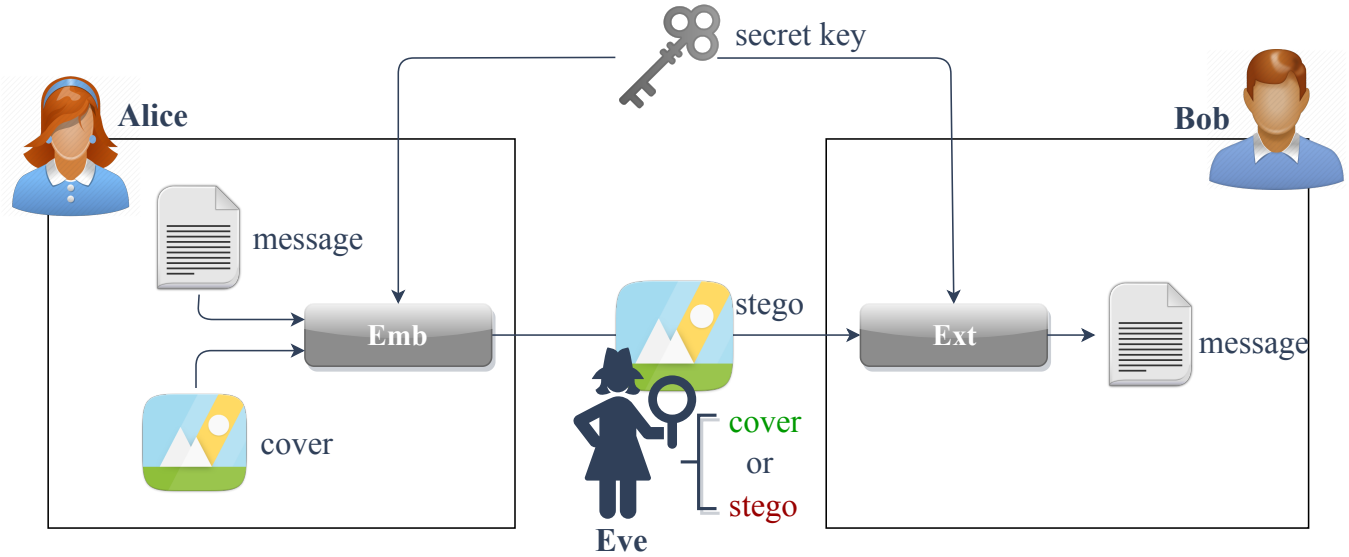
15 June 2020

Presented by
Dr. Mehdi YEDROUDJ

Authors
Dr. Mehdi YEDROUDJ
A. Pr. Marc CHAUMONT
A. Pr. Frédéric COMBY
M. Ahmed OULAD AMARA
Pr. Patrick BAS

Outline

Steganography & Steganalysis

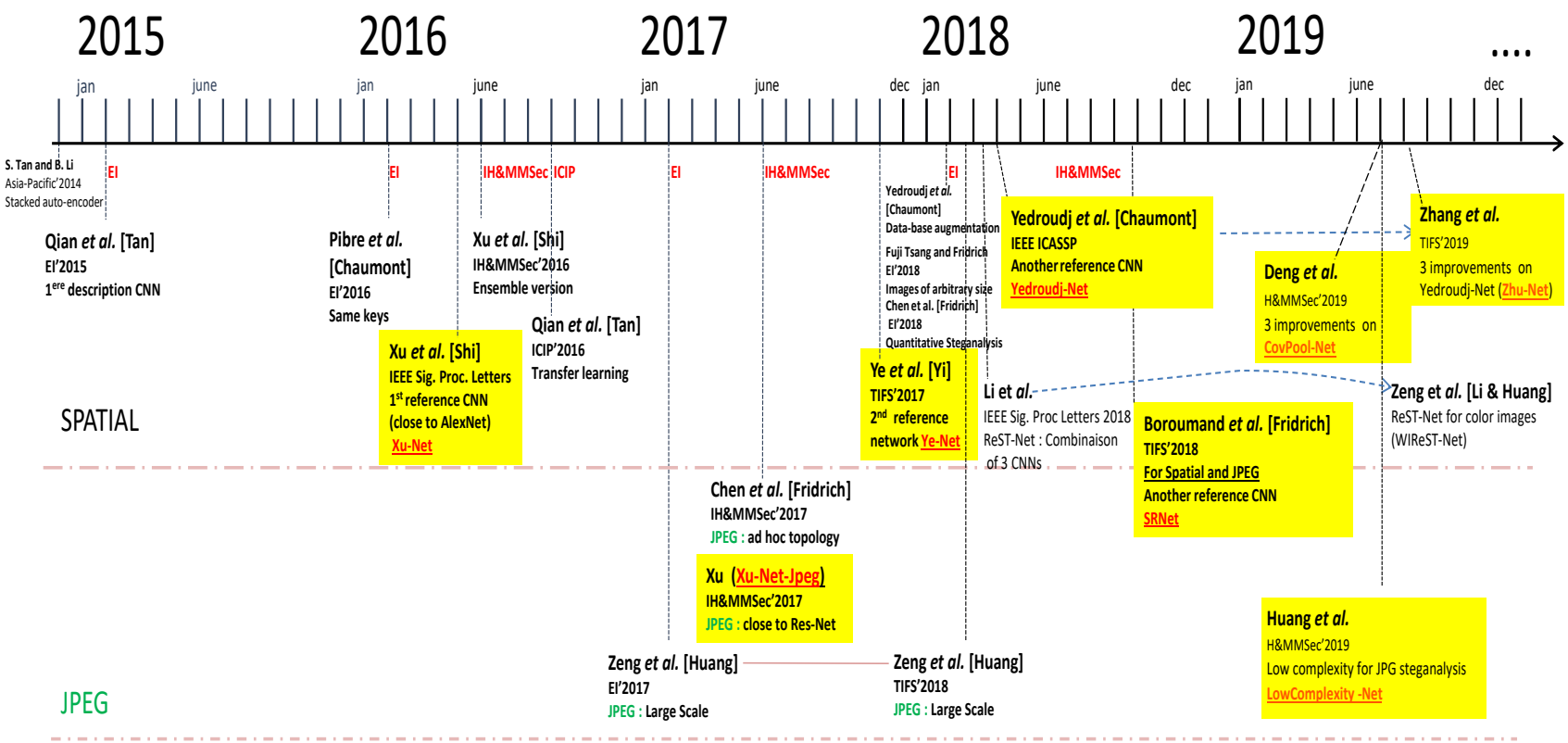


Steganography vs. Steganalysis

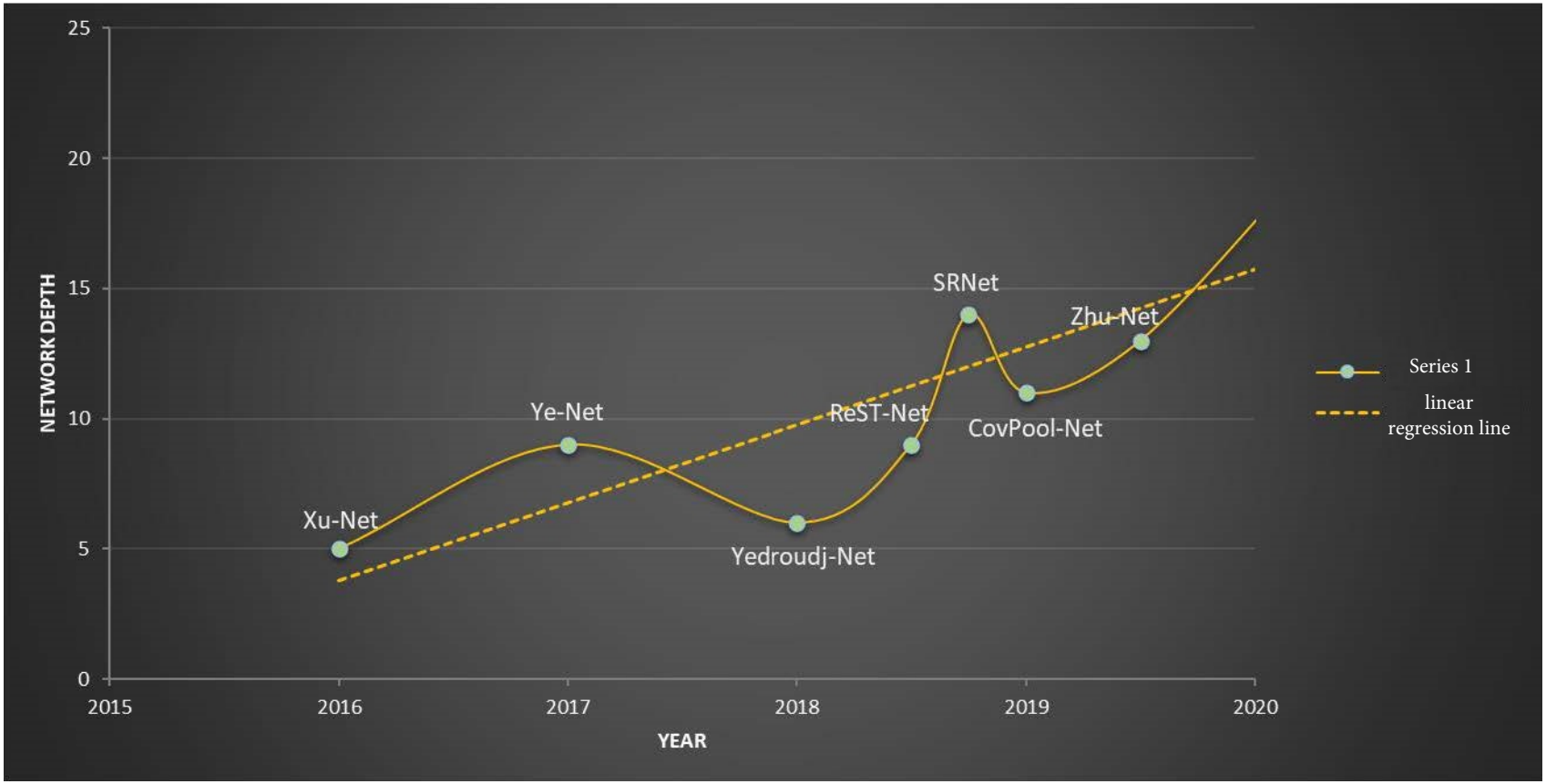
Steganography: the practice of concealing a secret message within a digital support.

Steganalysis: the analysis of a cover material to identify the presence of hidden information.

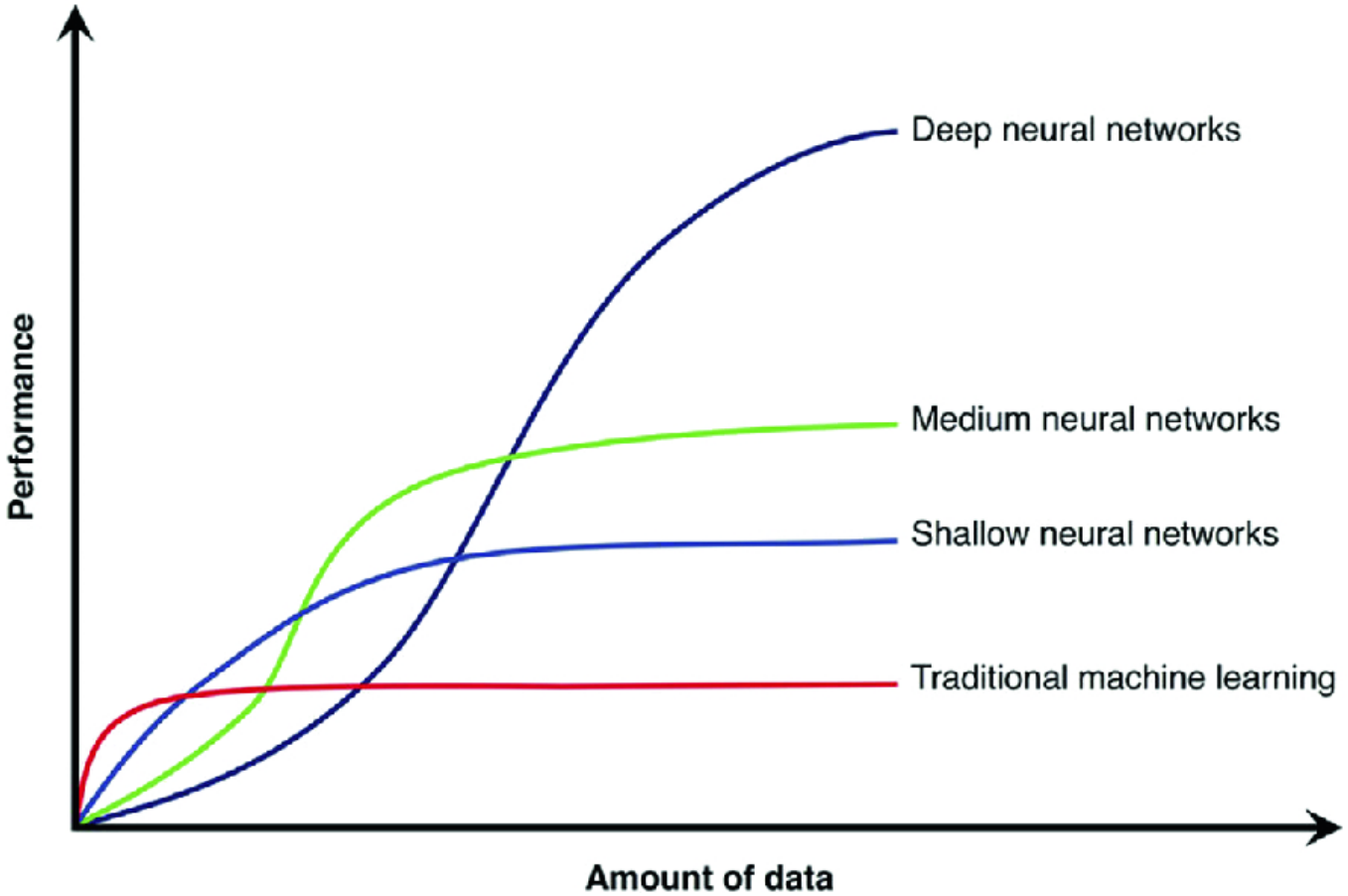
The chronology of steganalysis DL models evolution



The evolution of steganalysis models depth over the last 5 years



NN's performance in terms of depth and amount of data



Inspired from [1]

[1] Deep neural networks are able to learn from massive amounts of data — adapted from 'AI is the New Electricity' (Andrew Ng)

Steganalysis models performance in terms of depth and amount of data

Test protocol

- Stéganographie: WOW
- Payload: 0.2bpp

	BOSS (4000)	BOSS+BOWS2 (14000)	BOSS+BOWS2+VA (112000)
Xu-Net	32.4 %	30.3 %	30.5 %
Yedroudj-Net	**27.8** %	**23.7** %	20.8 %
Ye-Net	33.1 %	26.1 %	22.2 %
SRNet	32.5 %	24.1 %	**19.0** %

[2] M. Yedroudj, M. Chaumont, F. Comby *YEDROUDJ-NET:An efficient CNN for spatial steganalysis.* (ICASSP), 2018

Xu-Net:5_{conv} Ye-Net:8_{conv} Yedroudj-Net:5_{conv} SRNet:14_{conv}

Existing solutions for data enrichment

Given a target database:

For the learning of the NN:

- Apply straightforward virtual data augmentation in either online or offline manner (flip & rotation $\rightarrow \times 8$),
- Use other database similar to the target database (e.g. BOSS+BOWS2),
- Use similar cameras to capture new images, and reproduce the same development than the target database,
- Apply similar developments to those in the target database on the original RAW images.

[3] M. Yedroudj, M. Chaumont, F. Comby *How to augment a small learning set for improving the performances of a CNN-based steganalyz.* (EI), 2018

Problematic: Real life case scenario

Limitation of existing data augmentation solutions

- Due to storage limitations, RAW images are not usually available, besides not easy to reproduce the same development:
  - ~~Apply similar developments to those in the target database on the original RAW images.~~

Problematic: Real life case scenario

Limitation of existing data augmentation solutions

- Due to storage limitations, RAW images are not usually available, besides not easy to reproduce the same development:
  - ~~Apply similar developments to those in the target database on the original RAW images.~~
- Definition of database 'resemblance' is not yet well established (no objective measurement):
  - ~~Use other database similar to the target database (i.g. BOSS+BOWS2) ,~~

Problematic: Real life case scenario

Limitation of existing data augmentation solutions

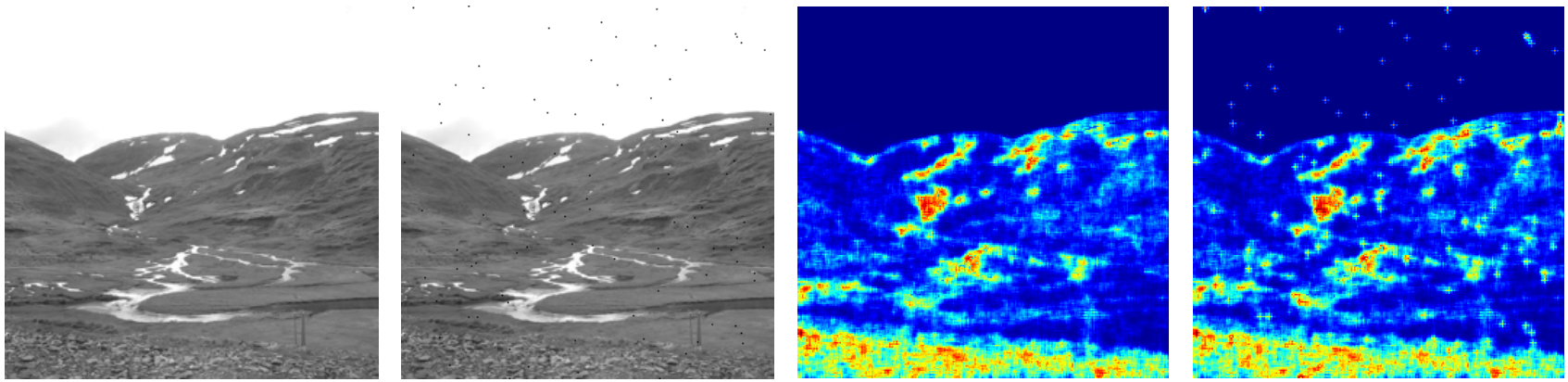
- Due to storage limitations, RAW images are not usually available, besides not easy to reproduce the same development:
  - ~~Apply similar developments to those in the target database on the original RAW images.~~
- Definition of database 'resemblance' is not yet well established (no objective measurement):
  - ~~Use other database similar to the target database (i.g. BOSS+BOWS2) ,~~
- The enormous variety of existing digital cameras:
  - ~~Use similar cameras to capture new images, and reproduce the same development than the target database,~~

Problematic: Real life case scenario

Limitation of existing data augmentation solutions

- Due to storage limitations, RAW images are not usually available, besides not easy to reproduce the same development:
  - ~~Apply similar developments to those in the target database on the original RAW images.~~
- Definition of database 'resemblance' is not yet well established (no objective measurement):
  - ~~Use other database similar to the target database (i.g. BOSS+BOWS2) ,~~
- The enormous variety of existing digital cameras:
  - ~~Use similar cameras to capture new images, and reproduce the same development than the target database,~~
- Very small amount of data to start with (10,100 images):
  - Apply straightforward virtual data augmentation in either online or offline manner (flip & rotation $\rightarrow \times 8$)

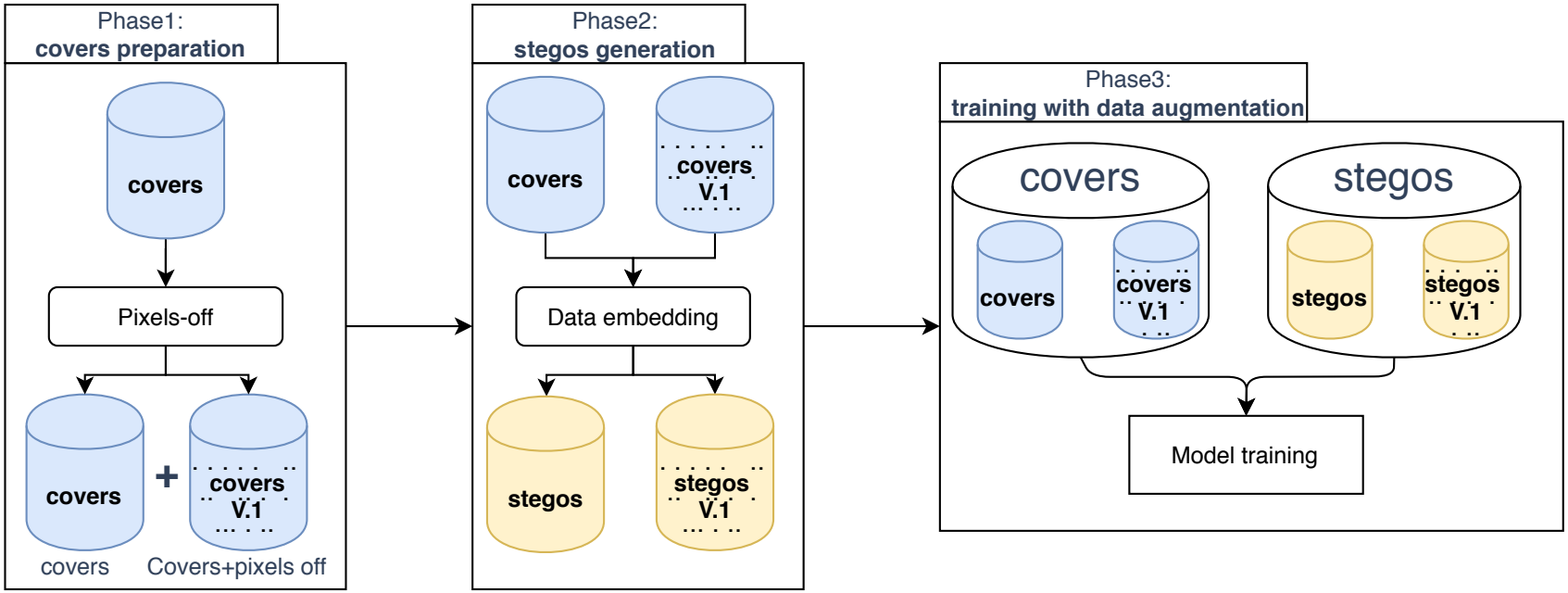
Proposed approach



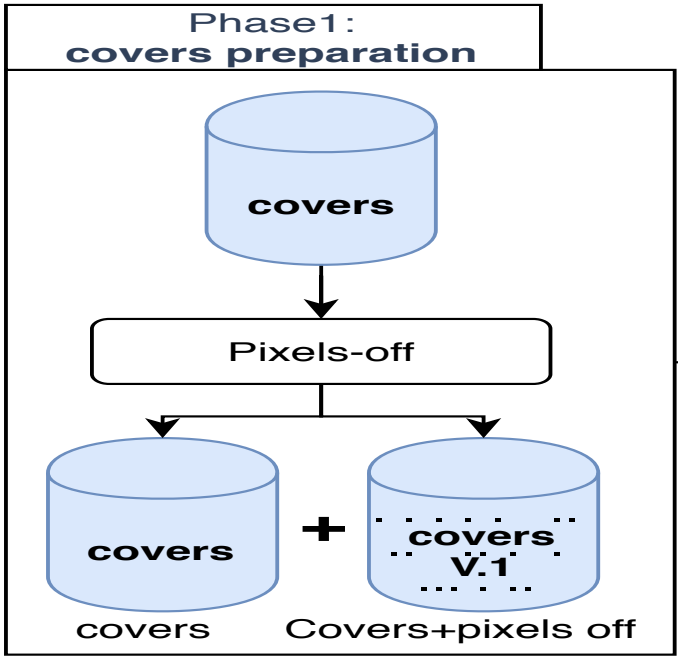
Pixels-off technique

- A new way to enrich a database in order to improve the CNN-based steganalysis performance,
- An efficient, generic approach which is usable in conjunction with other data-enrichment approaches,
- It can be used to build a "Side-Channel-Aware database" (SCA-database).

Global flowchart of the pixel-off technique



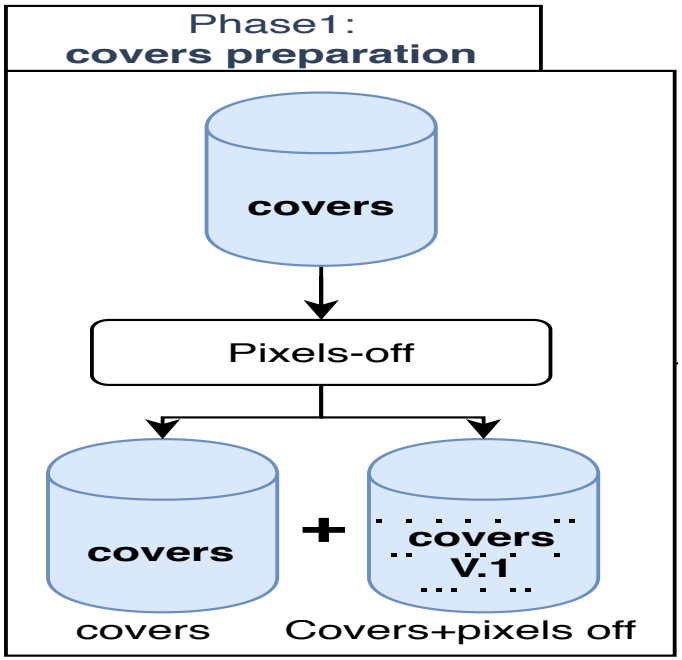
Phase1 : covers preparation

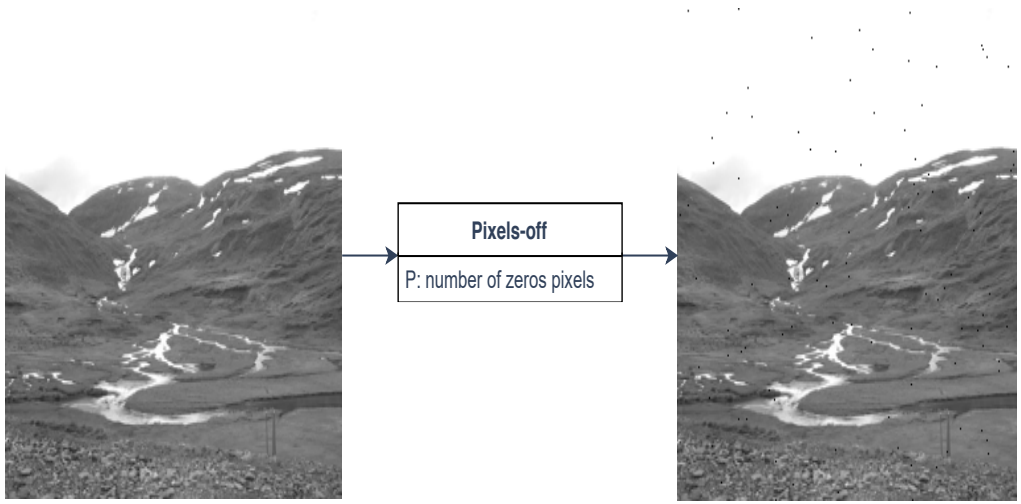


Protocol

- Set the value of "P", the number of pixels to switch off,
- Generate a pixels-off version of cover images,
- A new set of covers is produced.

Phase1 : covers preparation

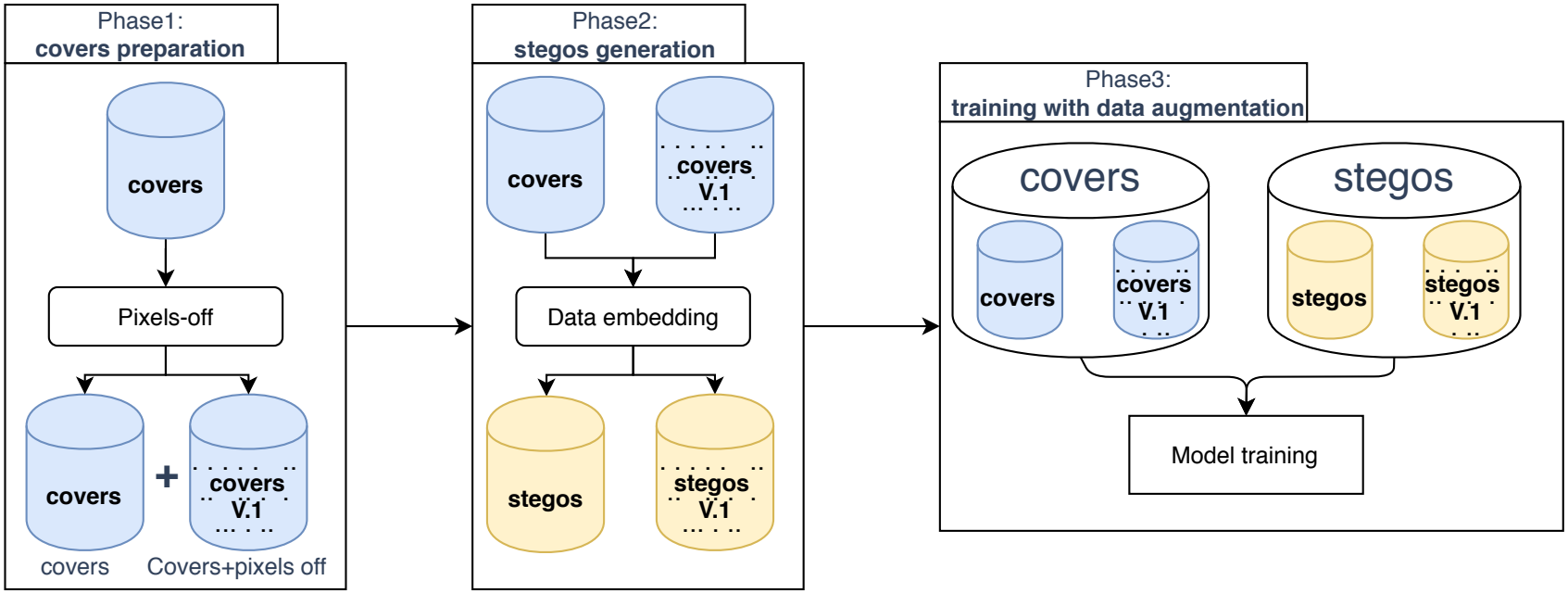




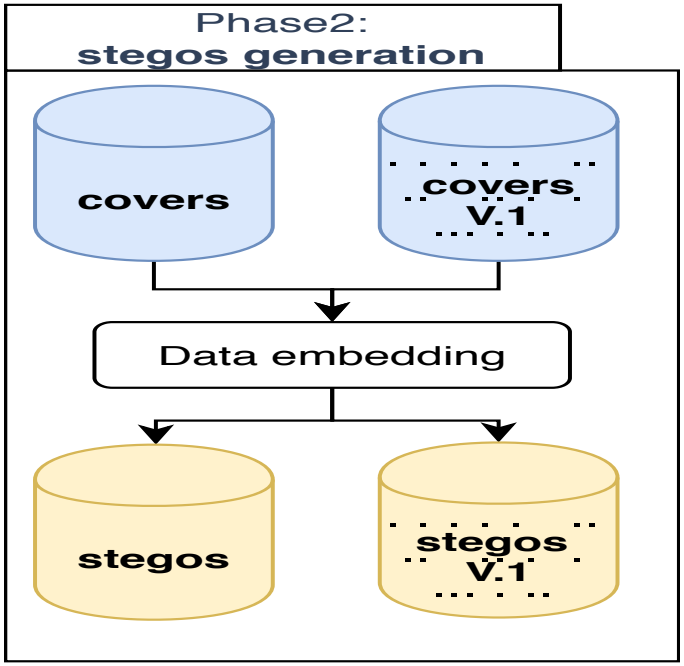
Protocol

- Set the value of "P", the number of pixels to switch off,
- Generate a pixels-off version of cover images,
- A new set of covers is produced.

Global flowchart of the pixel-off technique



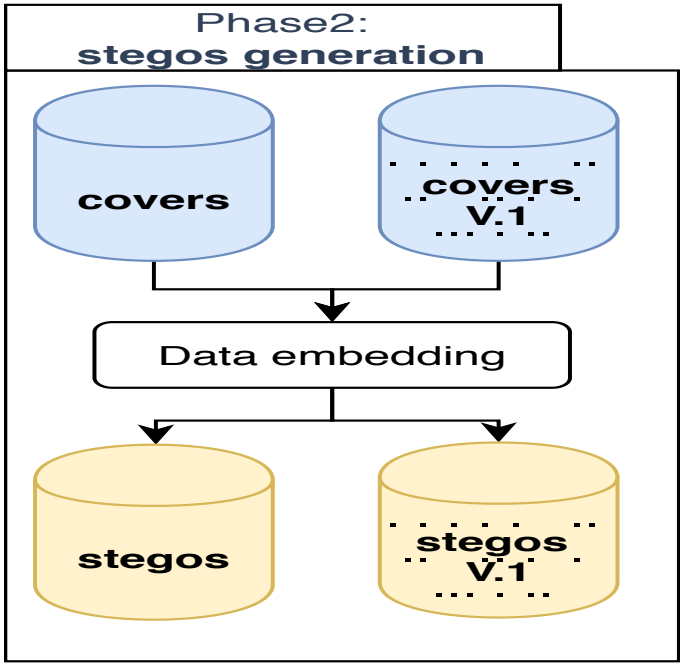
Phase2 : stegos generation



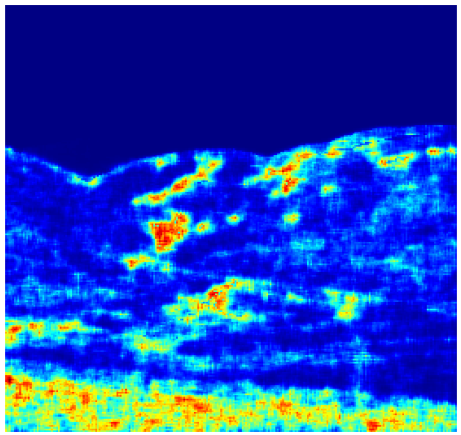
Protocol

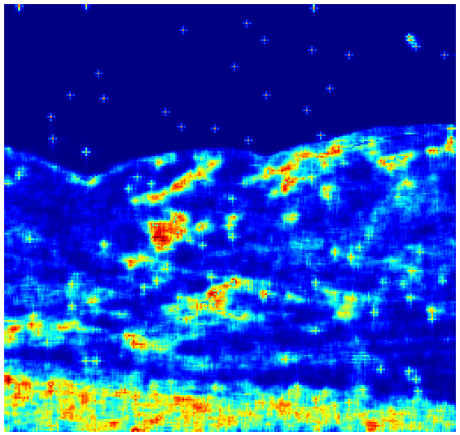
- Chose an embedding algorithm,
- Set a payload size,
- Two sets of stegos are generated.

Phase2 : stegos generation



The embedding modification probabilities map for the cover (resp."pixels-off" version) used by S-UNIWARD model with a payload of 0.4 bpp

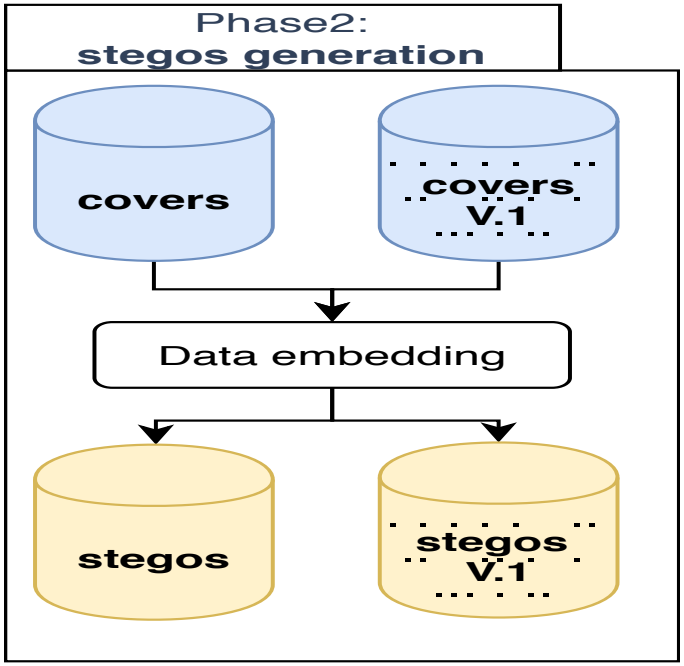




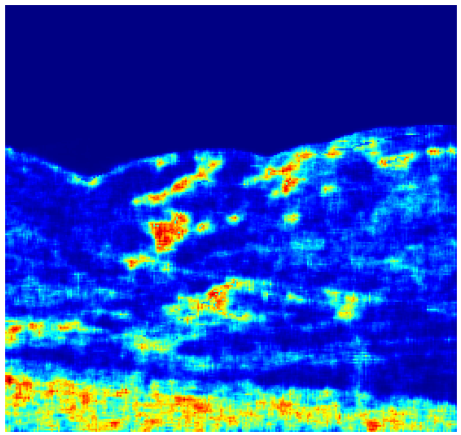
Protocol

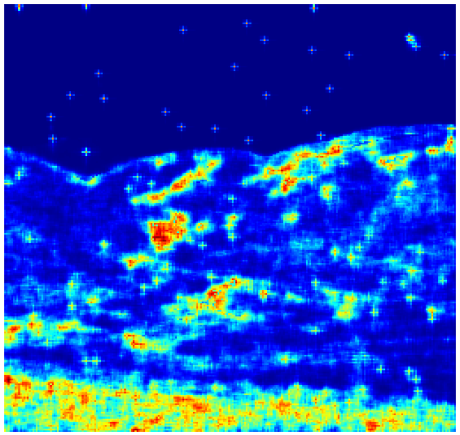
- Chose an embedding algorithm,
- Set a payload size,
- Two sets of stegos are generated.

Phase2 : stegos generation



The embedding modification probabilities map for the cover (resp."pixels-off" version) used by S-UNIWARD model with a payload of 0.4 bpp

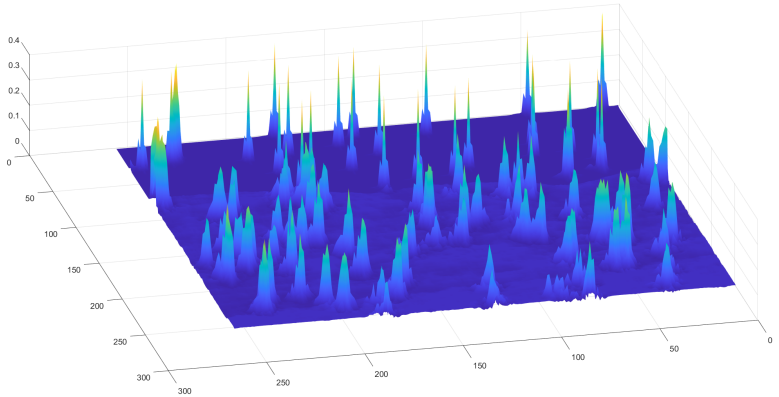




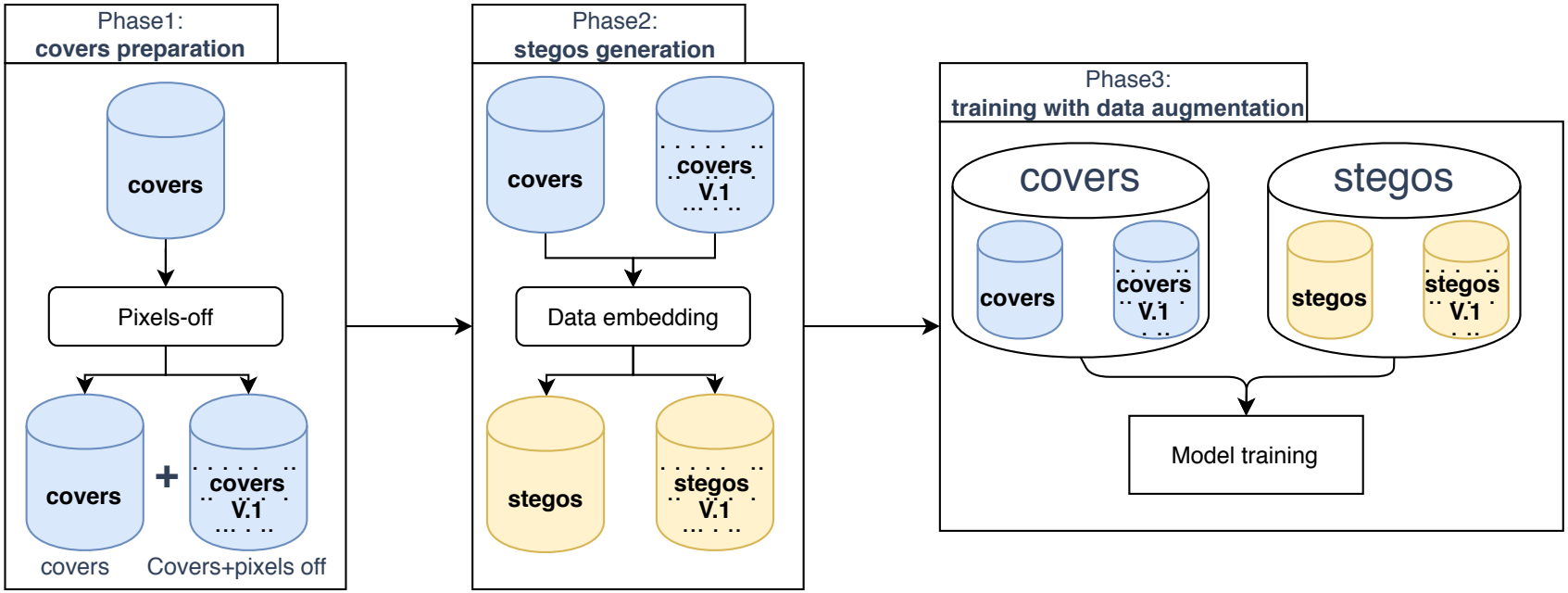
Protocol

- Chose an embedding algorithm,
- Set a payload size,
- Two sets of stegos are generated.

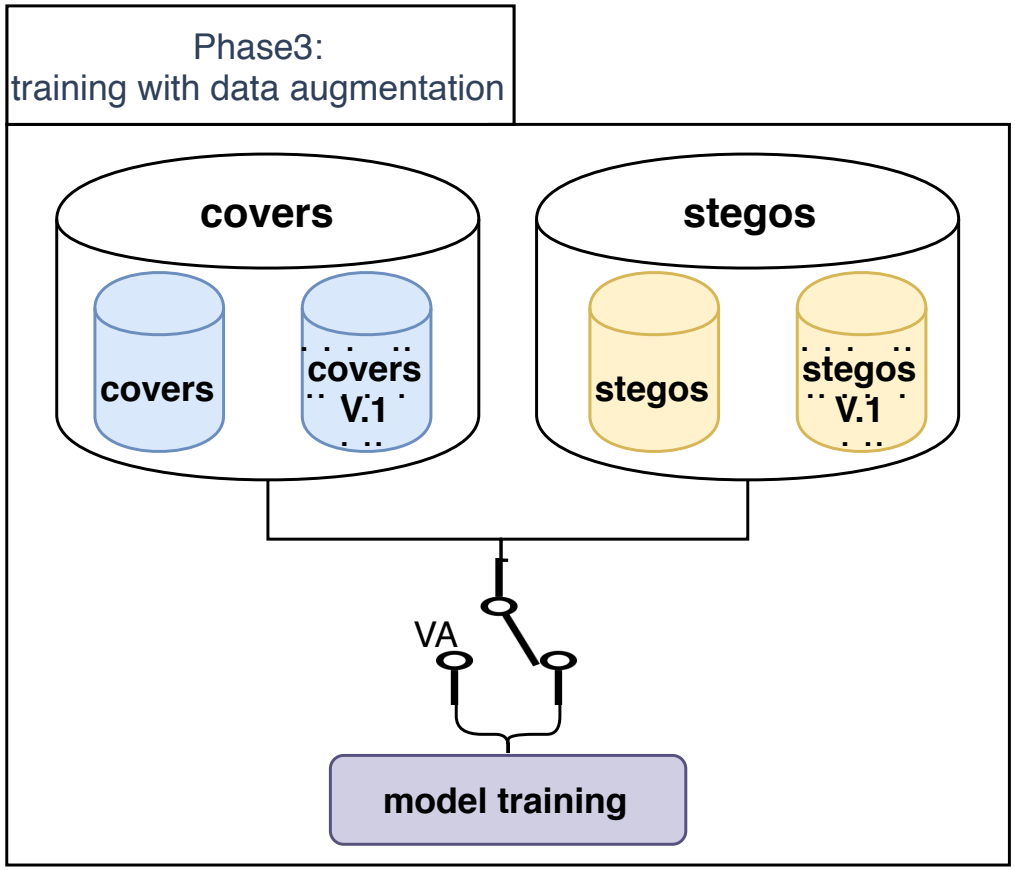
Visualization by elevation for the PMs differences



Global flowchart of the pixel-off technique



Phase3 : training with pixels-off enrichment



Protocol

- Prepare the training set (initial cover/stego database + the pixels-off cover/stego images),
- Choose whether to use other given data augmentation techniques e.g. VA,
- Initiate the model training.

Experimental results

Setup 1:

The enrichment method: pixels-off,
The steganalysis: Yedroudj-Net,
The database: BOSSbase.

	WOW		SUNIWARD		examples (pairs)	conv time
	0.2bpp	0.4bpp	0.2bpp	0.4bpp		
$\mathbf{B}$ = BOSS	27.71	15.27	35.42	22.70	4,000	4-5h
$\mathbf{B}_1 = \mathbf{B}$+100-off	25.31	14.3	33.1	19.4	8,000	9-10h
$\mathbf{B}_2 = \mathbf{B}_1$+256-off	23.95	13.41	29.8	17.8	12,000	13-14h
$\mathbf{B}_3 = \mathbf{B}_2$+400-off	23.5	13.44	29.3	16.95	16,000	17-18
$\mathbf{B}_4 = \mathbf{B}_3$+1024-off	23.8	13.65	29.2	16.98	20,000	21-22

Conclusion:

- The optimal parameter is roughly around $P = 400$ pixels-off,
- Combining various enrichments with P between 100 and 1024 improves the steganalysis efficiency.

Experimental results

Setup 2:

The enrichment method: pixels-off,
The steganalysis: CovPool-Net,
The database: BOSSbase.

	WOW		SUNIWARD		examples (pairs)	conv time
	0.2bpp	0.4bpp	0.2bpp	0.4bpp		
$\mathbf{B}$ = BOSS	26.08	15.60	31.89	18.32	4,000	5-6h
$\mathbf{B}_1 = \mathbf{B}$+100-off	25.33	14.63	28.54	16.25	8,000	10-11h
$\mathbf{B}_2 = \mathbf{B}_1$+256-off	24.88	13.11	26.61	15.00	12,000	14-15h
$\mathbf{B}_3 = \mathbf{B}_2$+400-off	23.34	13.02	26.64	15.44	16,000	19-20h
$\mathbf{B}_4 = \mathbf{B}_1$_VA	17.5	9.23	21.58	10.54	64,000	10-11h

Conclusion:

- The proposed method can improve performance of different steganalyzer,
- Accumulating VA + pixels-off can improves further the performance.

Does other weak noise signal work?

Setup 3:

The enrichment method: pixels-off, Gaussian, salt&pepper noise,
The steganalysis: Yedroudj-Net,
The database: BOSSbase.

	WOW0.4	SUNIWARD0.4
BOSS	15.27	22.70
BOSS+100-off	14.3	19.4
BOSS+Gaussian	16.08	23.25
BOSS+salt&pepper (d = 0.05)	15.16	22.25
BOSS+salt&pepper (d = 0.0016)	14.76	19.92

Conclusion:

- Low-power noise (less than 1.5% modified pixels) can be useful,
- Other noises such as +/-1 noise achieve good results.

SCA-database:

Setup 4:

The enrichment method: selective pixels-off,
The steganalysis: Yedroudj-Net,
The database: BOSSbase.

	WOW0.4	SUNIWARD0.4
BOSS	15.27	22.70
BOSS+100_off	14.3	19.4
BOSS+100_off-lowP	15.17	20.85
BOSS+100_off-highP	13.65	18.15

Conclusion:

- More beneficial to limit the pixels-off to pixels with a high modification probability,
- Another way of doing SCA steganalysis, by generating SCA training sets (to be investigated).

Outline

Conclusion

The pixel-off technique is:

- A novel technique for data-base enrichment for CNN-based steganalysis.
- Close in principle to noise addition, but made so that the pixel distribution of the resulting image remains close to that of the original image.
- Efficient, simple to implement, and come with low complexity.
- Suitable to be a complementary option to other enrichment techniques.
- May be used for building informed database "Side-Channel-Aware database".

Pixels-off: Data-augmentation Complementary Solution for Deep-learning Steganalysis

Thank you for your attention

IH&MMSec2020

15 June 2020