A Study on the Invariance in Security Whatever the Dimension of Images for the Steganalysis by Deep-Learning

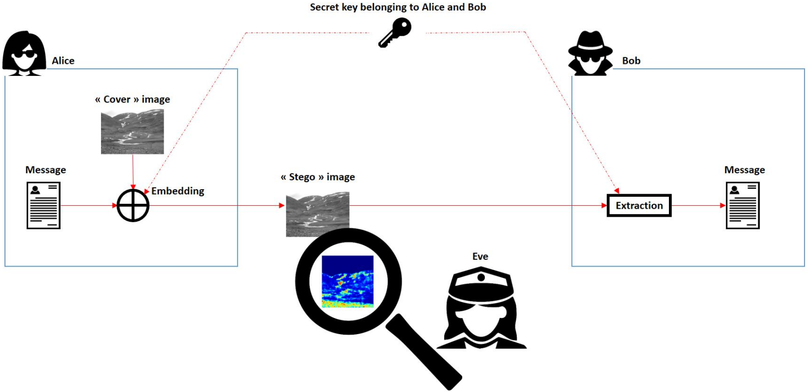
Kévin PLANOLLES[1,2], Marc CHAUMONT[1,3], Frédéric COMBY[1,2]
LIRMM[1], Univ Montpellier[2], Univ Nîmes[3], Montpellier, France

April 13, 2023

IEEE ICASSP'2023, International Conference on Acoustics, Speech, and Signal Processing, June 04 to June 10, 2023, Greek Island of Rhodes.

Outline

Steganography / Steganalysis



Scenario

The usual laboratory steganalysis scenario:

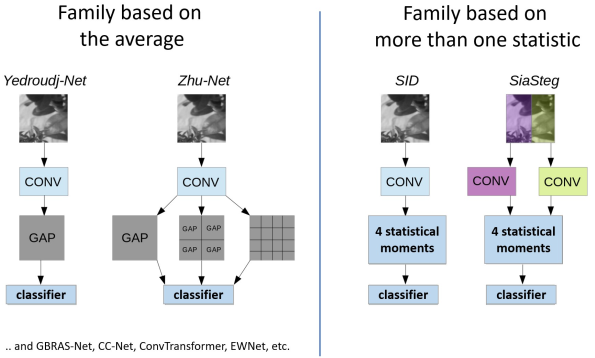
- A few state-of-the art **CNN** networks,
- A **database** with cover/stego images (splitted in learn, validation, test),
- **Eve knows** images size, payload size, embedding algorithm, image development, and statistics of images.

The scenario studied in this paper:

- **Eve does not know the images <u>sizes</u>**
  ... She wants to keep "detection performances" constant whatever the dimension of the images.

In this paper, we propose a **protocol to check this properly**.

Architectures able to "accept" images of various sizes



→ How to check finely if detection performances are constant whatever the dimension?

We need to embed to get a "same security level" whatever the dimension.

Equal security whatever the dimension? (1)

The Square Root Law (relative payload for an image of size $w \times h$):

$$\alpha = \frac{k}{wh} \times \sqrt{wh} \times \log(wh) \quad (bpp)$$

with k a positive.

$\rightarrow$ In practice, it does not ensure equal security whatever the dimension (i.e. CNNs accuracy is not constant when learn/test at different dimension).

Equal security whatever the dimension? (2)

Our proposition for building a proper dataset:

- Build a set of Nested Images
  $\rightarrow$ ensure same "difficulty" & same statistics,
- Find the relative payload for each size
  $\rightarrow$ ensure same "security" whatever the dimension.

$\rightarrow$ NNID (Nearly-Nested Image Datasets).

Outline

Introduction

NNID building

Experiments & Results

Conclusions and perspectives

SmartCrop 2

In this paper, we only work on cropping (not resizing).

Smart crop 2 :

Take the area of the mother image that keeps the same distribution of **costs** between the mother image and the cropped one.

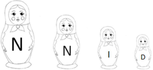
$$\mathcal{D}_{\mathrm{KL}}(P, Q) := \sum_i P(i) \log \frac{P(i)}{Q(i)} + \sum_i Q(i) \log \frac{Q(i)}{P(i)}, \qquad (1)$$

→ **cost** obtained with the SUNIWARD algorithm,

→ use the integral histogram approach,

→ same "difficulty" for each dataset.

SmartCrop 2: Illustration (Nearly-Nested Image Datasets)



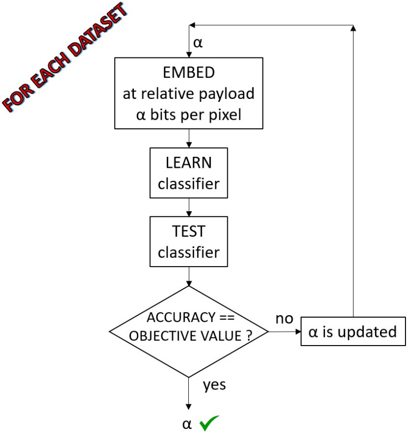
`https://www.lirmm.fr/~chaumont/NNID.html`

2048x2048 1024x1024 512x512 256x256

→ 4 datasets : NNID = UNI_2048, UNI_1024, UNI_512, UNI_256

Relative payload for each dataset

Input: NNID + Algo; **Output:** Same "security" for each dataset



Invariance in security

Definition:

A deep learning network **invariant in security** with respect to the dimension when its obtained **average accuracy is the same whatever the dimensions**.

→Let us test the networks!

Outline

Experimental protocol

- For each dataset (of NNID):
  12 000 pairs for train, 2400 for validation, 3000 for test,
- S-UNIWARD for embedding,
- Payload ensuring "same security" (using Yedroudj-Net):

Dimension	Relative payload	Accuracy (Yedroudj-Net)
256	0.4	76.97%
512	0.3204	76.38%
1024	0.28895	76.78%

Two tests of the invariance in security:

1. learn on 1 size,
2. learn on several sizes.

Test 1: Learn on 1 size & Test on another size

Accuracies for SID and Dilated-Yedroudj-Net (noted `DY`)

Dim	`SID-256`	`SID-512`	`SID-1024`
256×256	**69.48%**	67.05% (↓)	60,9% (↓)
512×512	69.30%	**70.7%**	66.93% (↓)
1024×1024	66.73% (↓)	66.93% (↓)	**69.62%**

Dim	`DY-256`	`DY-512`	`DY-1024`
256×256	**77.7%**	76.25% (↓)	71.92% (↓)
512×512	75.21% (↓)	**77.3%**	76.2% (↓)
1024×1024	72.03% (↓)	76.88%	**77.53%**

- Diagonal values are close
  → relative payload in NNID (→ difficulty/security) is correct,
- Performance decrease compared to the diagonal,
- Behavior differs in fonction of images dimension.

→ no invariance in security.

Test 2: Learn on several sizes

Still 12 000 pairs for train, 2400 for validation, 3000 for test, with same proportion randomly picked in each dataset.

Dim	SID-MULTI	Y-MULTI	DY-MULTI
256×256	66.93% (↓2.53)	73.93% (↓1.07)	75.63% (↓2.83)
512×512	69.46%	75.5%	78.1%
1024×1024	70.6%	75%	78.06%

- variations in accuracies are less important,
- invariance still not reached.

Outline

Conclusions

We propose a way to check if DL keep "detection performances" constant whatever the dimension of the images.

Proposition:

- Smart crop 2 (use of integral histogram)
  $\rightarrow$ same difficulty,
- Dichotomous method (to obtain a relative payload)
  $\rightarrow$ same security,
- Definition of invariance in security.

Conclusion:

- The NNID and its protocol allows fine evaluation,
- 2 representatives DL are NOT invariant.

Perspectives

Future work:

- Get a finer definition of invariance in security
  (work at the image level and no more at the data-set level),
- Propose a new architecture given the definition of invariance,
- Evaluate on unseen dimensions.