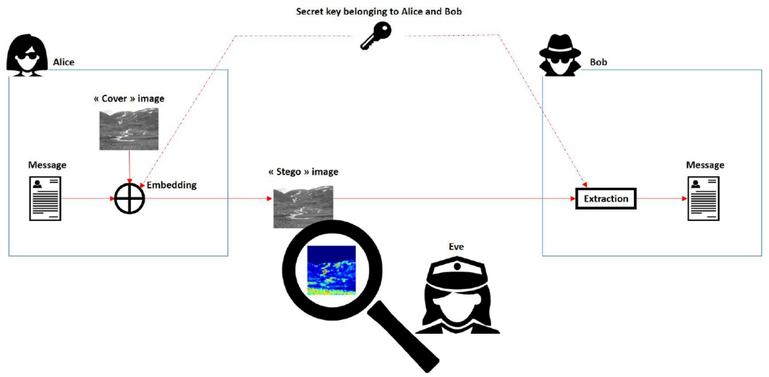
A Study on the Invariance in Security Whatever the Dimension of Images for the Steganalysis by Deep-Learning

Kévin PLANOLLES, Marc CHAUMONT, Frédéric COMBY, LIRMM, Univ Montpellier, Univ Nîmes, Montpellier, France



The scenario studied in this paper:

Eve does not know the images sizes

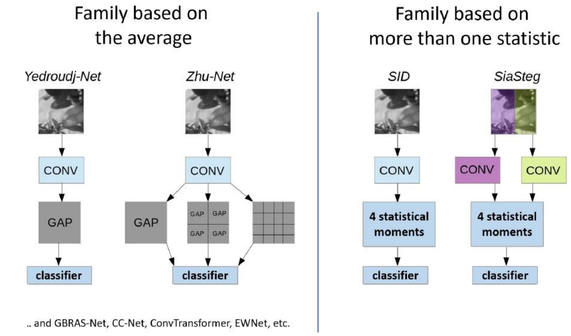
... She wants to keep "detection performances" constant whatever the dimension of the images

OBJECTIVE:

I. Define a fine evaluation protocol

II. Evaluate some architectures

Architectures able to "accept" images of various sizes



I. Define a protocol for ensuring an equal security whatever the dimension:

1) Build a set of Nested Images

→ ensure same "difficulty" & same statistics

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.

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

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

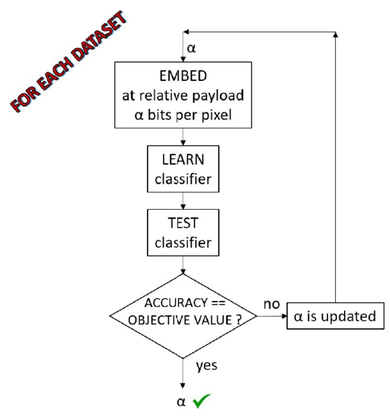
→ 4 datasets : NNID = UNI_2048, UNI_1024, UNI_512, UNI_256

2) Find the relative payload for each size

→ ensure same "security" whatever the dimension.

Relative payload for each dataset

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



3) Definition:

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

II. Evaluate the invariance with NNID:

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%

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.

III. Conclusions & Perspectives:

→ The NNID and its protocol allows fine evaluation

→ The 2 representatives DL are NOT invariant

→ Get a finer definition of invariance in security

→ Propose a new architecture

→ Evaluate on unseen dimensions

The authors would like to thank the French Defense Procurement Agency (DGA) for its support through the ANR Alaska project (ANR-18-ASTR-0009). We also thank Douglas Benhamou and Mohamed Benkhettou for their technical help.