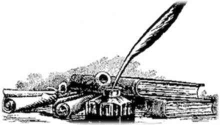
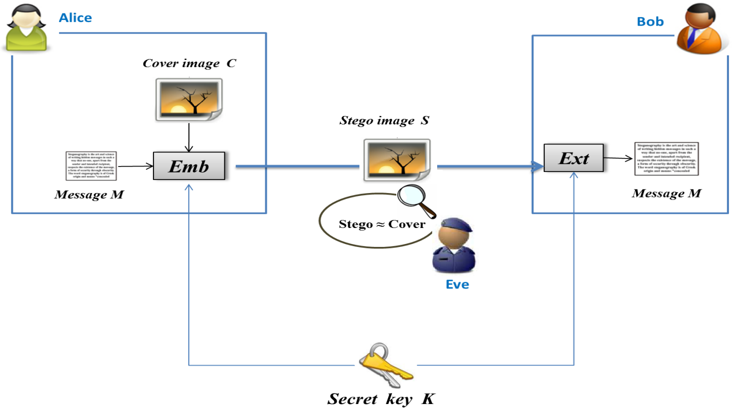
Technical Points about Adaptive Steganography by Oracle (ASO)

Sarra Kouider, Marc Chaumont, William Puech



E-mail: firstname.surname@lirmm.fr
http://www.lirmm.fr/~kouider

Steganography vs Steganalysis



Adaptive steganography

Goal

Transmit $\boldsymbol{m}$ bits in a cover object $\mathbf{X}$ of $\boldsymbol{n}$ elements by making small perturbations.

Solution

- Defining the embedding impact:
  $D(\mathbf{X}, \mathbf{Y}) = \parallel \mathbf{X} - \mathbf{Y} \parallel_{\rho} = \sum_{i=1}^{n} \rho_i \mid x_i - y_i \mid$.
- Find the stego object $\mathbf{Y}$ that minimizes the distortion function D under the constraint of the fixed payload: $\mathbf{Y} = Emb(\mathbf{X}, m) = \arg\min D(\mathbf{X}, \mathbf{Y})$.

$\Longrightarrow$ HUGO [Pevný et al., IH 2010]. $\Longrightarrow$ MOD [Filler et al., SPIE 2011].

Adaptive steganography

Goal

Transmit $\boldsymbol{m}$ bits in a cover object $\mathbf{X}$ of $\boldsymbol{n}$ elements by making small perturbations.

Solution

- Defining the embedding impact:
  $D(\mathbf{X}, \mathbf{Y}) = \| \mathbf{X} - \mathbf{Y} \|_\rho = \sum_{i=1}^{n} \rho_i \mid x_i - y_i \mid$.
- Find the stego object $\mathbf{Y}$ that minimizes the distortion function D under the constraint of the fixed payload: $\mathbf{Y} = Emb(\mathbf{X}, m) = \arg\min D(\mathbf{X}, \mathbf{Y})$.

$\Rightarrow$ HUGO [Pevný et al., IH 2010]. $\Rightarrow$ MOD [Filler et al., SPIE 2011].

Outline

1. Introduction

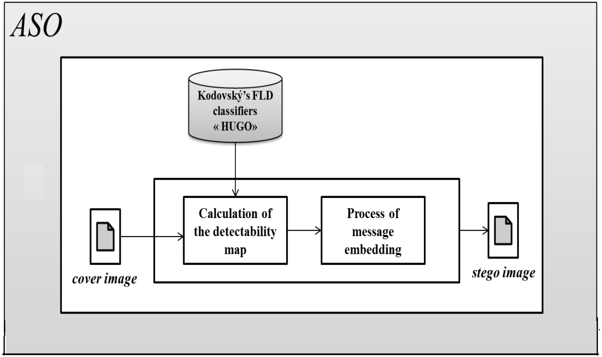
2. The proposed ASO scheme
   - The detectability map computation
   - Embedding process
   - ASO's design

3. Steganography by database

4. Experimental results

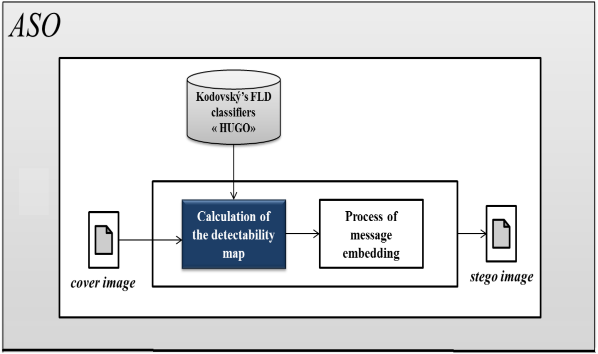
5. Conclusion

The proposed ASO scheme

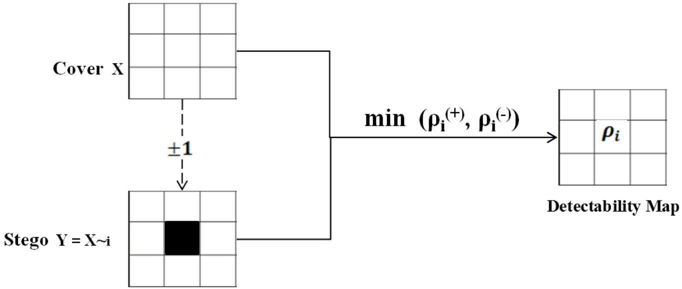


The Adaptive Steganography by Oracle (ASO).

The detectability map computation



The detectability map computation

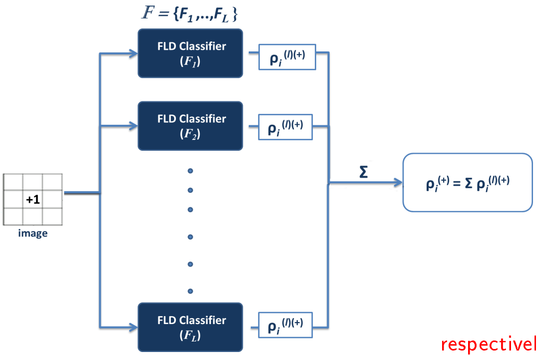


For each pixel $(x_i) \Longrightarrow \rho_i = min(\rho_i^{(+)}, \rho_i^{(-)})$.

T. Pevný, T.Filler, and P. Bas
Using High-Dimensional Image Models to perform Highly Undetectable Steganography. *In IH'12th International Workshop*. LNCS. Calgary, Canada. June 28-30, 2010.

The detectability map computation

Our proposed approach :



respectively for $\rho_i^{(-)}$

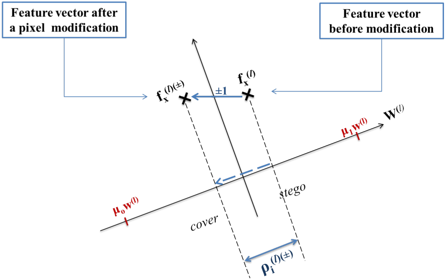
$$\rho_i^{(+)} = \sum_{l=1}^{L} \rho_i^{(l)(+)}$$

The detectability map computation

Our proposed approach :

For each FLD classifier (F_l)

- $\rho_i^{(l)(+)} = \dfrac{\mathbf{w}^{(l)} \cdot \left(\mathbf{f}_{\mathbf{x} \sim x_i}{}^{(l)(+)} - \mathbf{f}_{\mathbf{x}}{}^{(l)} \right)}{s^{(l)}}$
- $\rho_i^{(l)(-)} = \dfrac{\mathbf{w}^{(l)} \cdot \left(\mathbf{f}_{\mathbf{x} \sim x_i}{}^{(l)(-)} - \mathbf{f}_{\mathbf{x}}{}^{(l)} \right)}{s^{(l)}}$

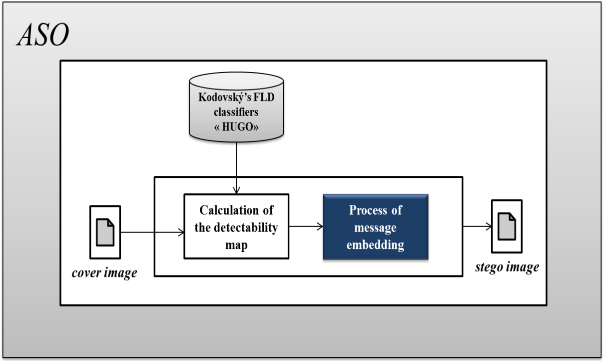


where

$\mathbf{f}_{\mathbf{x}}{}^{(l)}$: Feature vector before modification.

$\mathbf{f}_{\mathbf{x} \sim x_i}{}^{(l)(\pm)}$: Feature vector after a pixel modification ± 1.

Embedding process



Embedding Process

- Defining the embedding impact:
  $D(\mathbf{X}, \mathbf{Y}) = \| \mathbf{X} - \mathbf{Y} \|_\rho = \sum_{i=1}^{n} \rho_i \mid x_i - y_i \mid .$
- Find the stego object $\mathbf{Y}$ that minimizes the distortion function D under the constraint of a fixed payload: $\mathbf{Y} = Emb(\mathbf{X}, m) = \arg\min D(\mathbf{X}, \mathbf{Y})$.

  $\Rightarrow$ Simulating the optimal embedding algorithm.

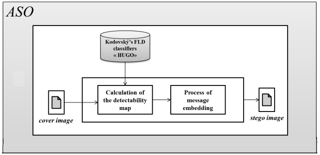
  or

  $\Rightarrow$ Using the practical STC algorithm.

T. Filler, J. Judas, and J. Fridrich
Minimizing embedding impact in steganography using trellis-coded quantization. In SPIE. San Jose, CA, January 18-20, 2010.

ASO's design

- Oracle learns on 5000 covers and 5000 HUGO stego images from BOSSBase v1.00.
- Each image is represented by a vector of $d = 5330$ MINMAX features [Fridrich et al., 2011].
- Personal implementation of the FLD ensemble classifiers with $d_{red} = 30$, and $L = 30$ classifiers.
- Complexity reduction trick (from 2 years to 1.5 days) for 10000 images.



General scheme of ASO.

J. Fridrich, Kodovský, V. Holub, and M. Goljan
Breaking HUGO - the Process Discovery. In IH. Prague, Czech Republic, May 18-20, 2011.

1. Introduction
2. The proposed ASO scheme
3. Steganography by database
   - The steganography by database paradigm
   - Security measure
4. Experimental results
5. Conclusion

The steganography by database paradigm

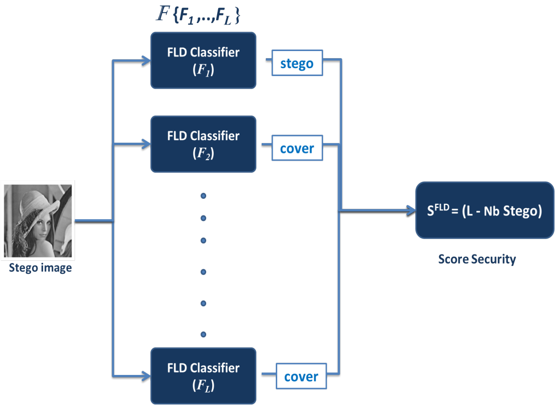
Paradigm:

- Requires a cover database at the input of the embedding process, instead of just one image.
- Preserves both cover image and sender's database distributions.

May output:

- One stego images with the secret message (one-time database).
- Or multiple stego images with different messages (batch steganography).

The proposed security measure



high score S^{FLD} $\Rightarrow$ high stego image security.

1. Introduction

2. The proposed ASO scheme

3. Steganography by database

4. Experimental results
    - ASO's security performance
    - Security measure performance

5. Conclusion

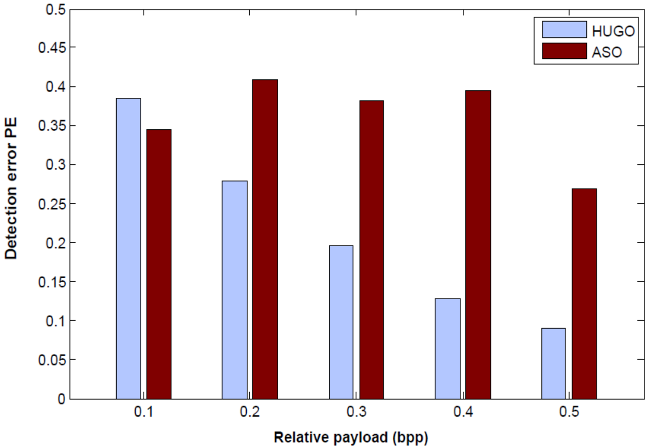
Evaluation protocol: ASO's security performance

- Blind steganalysis (ASO vs HUGO)
  - Kodovský ensemble classifier.
  - BossBase v1.00 database with 10000 512×512.
  - Rich Model SRMQ1 of 12753 features [Fridrich et al., 2012].
- Detection Error:

$$P_E = \min_{P_{FA}} \frac{1}{2} \left(P_{FA} + P_{MD} \left(P_{FA} \right) \right).$$

J.J. Fridrich, and J. Kodovský
Rich Models for steganalysis od Digital Images. *In IEEE Transactions on Information Forensics and security*. 2012.

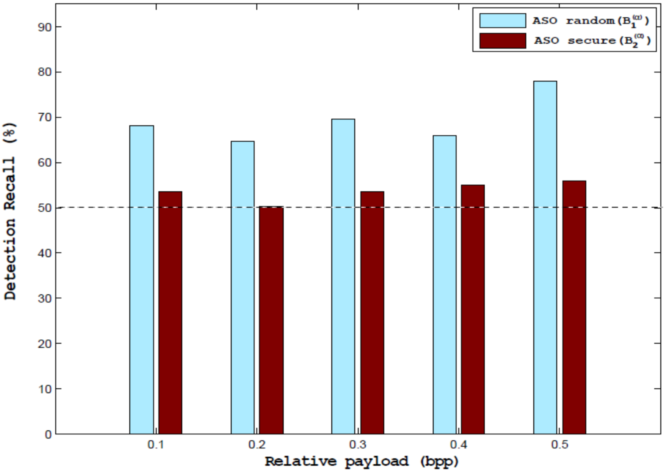
ASO's security performance



Evaluation protocol: Security measure performance

- OC-SVM machine learning with Gaussian kernel.
- Learning phase conducted on BossBase v1.00 cover images.
- $\mathcal{B}_1^{(\alpha)}$: 500 randomly selected ASO's stego images.
- $\mathcal{B}_2^{(\alpha)}$: 500 selected ASO's stego images using the S^{FLD} security criterion.

Security measure performance



Conclusion

Summary

- A new secure adaptive embedding algorithm: ASO.
- Presentation of the steganography by database paradigm.
- A selection criterion for the stego images.

Future work

- Security evaluation with a pooled steganalysis.
- Other security criterion.
- Position with game theory aspects.


Thanks
for your attention