Technical Points About Adaptive Steganography by Oracle (ASO)

Sarra Kouider, Marc Chaumont, William Puech

TECHNICAL POINTS ABOUT ADAPTIVE STEGANOGRAPHY BY ORACLE (ASO)

Sarra Kouider[2]*, Marc Chaumont*[1,2]*, William Puech*[2]

[1]University of Nîmes, F-30021 Nîmes Cedex 1, France

[2]LIRMM Laboratory, UMR 5506 CNRS, University of Montpellier II,
161, rue Ada, 34095, Montpellier Cedex 05, France

{sarra.kouider, marc.chaumont, william.puech}@lirmm.fr

ABSTRACT

ASO [1] is an adaptive embedding scheme that has proved its efficiency compared to HUGO [2] algorithm. It is based on the use of a detectability map that is correlated to the security of the embedding process. The detectability map is calculated using the *Kodovský's ensemble classifiers* [3] as an oracle, which preserves the distribution of the cover image and of the sender's database. In this article, we give the technical points about ASO. We give the details of the detectability map computation, then we study the security of the communication phase of ASO through *the paradigm of the steganography by database*. Since the introduced paradigm allows the sender to choose the most secure stego image(s) during the transmission of his message, we propose some security metrics that can help him to distinguish between secure and insecure images. We thus significantly increase the security of ASO.

Index Terms— Steganography, Detectability map, Ensemble classifiers, Oracle, Steganography by database.

1. INTRODUCTION

Steganography is the art of secret communication. The goal is to hide a secret message in an unsuspicious object in such a way that no one can detect it. With the Internet spread, several philosophies of designing steganographic methods were proposed. One of the most used embedding methods for real digital images is the steganography by minimizing of the embedding impact[1].

Let $\mathbf{x} = (x_1, ..., x_n)$ be a cover support composed of n elements. The goal of steganography by minimizing the embedding impact is to communicate a secret message $\mathbf{m} = (m_1, ..., m_m)$ by making small perturbations of cover object $\mathbf{x}$ to produce a stego object $\mathbf{y} = (y_1, ..., y_n)$. For this, we define a distortion function $D(\mathbf{x}, \mathbf{y})$ that we minimize under the constraint of a fixed payload. This distortion function is generally based on the use of a detectability map $\rho \in \mathbb{R}_+^n$ which assigns to each cover element x_i with $i \in \{1, ..., n\}$, a detectability cost $\rho_i \in \mathbb{R}_+$ that models the impact on the security caused by the modification of the i^{th} element.

The HUGO algorithm [2] used during the BOSS[2] competition [5] uses a detectability map, which attributes to each pixel of a cover image a detectability cost $\rho_i \in [0, \infty]$, as suggested in [6]. The calculation of the detectability cost is based on the use of high-dimensional features, which are calculated from the cover image. These features correspond to the conditional probabilities in each pixel of the filtered image. The MOD[3] algorithm proposed in 2011 [7], extends the HUGO proposal by defining a parametric detectability cost $\rho_i \in [0, \infty]$, which is parametrized by a high number of parameters. The ASO[4] embedding algorithm that we proposed in [1], improves the concept of the detectability map introduced by HUGO. It uses a non parametric detectability map whereas MOD use a parametric approach. The detectability map $\rho = \{\rho_i \in [0, \infty[\}_{i=1}^n$ is defined by using the functionalities of the *Kodovský's ensemble classifiers* [3] as an oracle. This preserves not only the cover image distribution, but also the distribution of the sender's database. Thus, ASO introduces a new paradigm in steganography which is *the steganography by database* that, furthermore, offers to the sender the possibility to choose the most secure image(s) during the transmission phase.

In this paper, we pursue the study about the adaptive steganography by oracle [1]. We give the technical points about the embedding algorithm (ASO), and we discuss about the security of the ASO's embedding process thanks to *the steganography by database paradigm*. For this, we propose some new security measures that reflect the security level of the stego images.

The rest of this paper is organized as follows. In Section 2.1, we recall some notions about the ASO algorithm. In Sec-

[1]The principle of minimizing the embedding impact was proposed in 2007 [4]. It is based on the adaptivity of the embedding operation by the use of a detectability map.

[2]BOSS (Break Our Steganography System) is the first challenge on Steganalysis. The challenge started the September 9th 2010 and ended the 10th of January 2011. The goal of the player was to figure out, which images contain a hidden message and which images do not. The steganographic algorithm was HUGO [2]. http://www.agents.cz/boss/BOSSFinal/.

[3]MOD: Model Optimized Distortion.

[4]ASO: Adaptive Steganography by Oracle [1].

tion 2.2, we give the technical points about the detectability map construction. In Section 2.3, we discuss the paradigm of *the steganography by database* and we propose the security metrics. We give experimental results in Section 3, and we conclude in Section 4.

For the sake of simplicity, we denote by $\mathbf{x} = (x_1, ..., x_n) \in \mathcal{X} = \{0, ..., 255\}^n$ and $\mathbf{y} = (y_1, ..., y_n) \in \mathcal{Y} = \{0, ..., 255\}^n$ grayscale cover and stego images with n pixels. The use of any other digital media is also possible.

2. ADAPTIVE STEGANOGRAPHY BY ORACLE (ASO)

2.1. General scheme

ASO[5] [1] is an adaptive embedding scheme that is based on the principle of minimizing embedding impact [4, 6]. It strives to hide a given message $\mathbf{m}$ in a cover support $\mathbf{x}$, while minimizing an ad hoc distortion measure that is correlated to the security of the embedding process. The embedding is either simulated [4], or done by using the STC[6] approach [6]. These embedding algorithms require to define a detectability map ρ that model the statistical detectability. In ASO an oracle is used to calculate a detectability map $\rho = \{\rho_i \in \mathbb{R}\}_{i=1}^n$ that assigns a detectability costs ρ_i to each pixel x_i:

$$\rho_i = min\left(\rho_i^{(+)}, \rho_i^{(-)}\right), \tag{1}$$

with $\rho_i^{(+)}$ (resp. $\rho_i^{(-)}$) the detectability cost of changing the i^{th} pixel by $+1$ (resp. -1).

Since the *Kodovský's FLD ensemble classifiers* [3] allows to split the features space into cover and stego regions, ASO [1] uses this separation as an oracle to define the detectability costs $\rho_i^{(+)}$ and $\rho_i^{(-)}$:

$$\rho_i^{(+)} = \sum_{l=1}^{L} \rho_i^{(l)(+)}, \quad \text{and} \quad \rho_i^{(-)} = \sum_{l=1}^{L} \rho_i^{(l)(-)}, \tag{2}$$

where $\rho_i^{(l)(+)}$ (resp. $\rho_i^{(l)(-)}$) is the detectability cost provided by the l^{th} classifier, and L is the number of the FLD classifiers.

For each FLD classifier F_l, with $l \in \{1, ..L\}$, that performed its learning on a subspace of d_{red} dimension, the detectability cost $\rho_i^{(l)(+)}$ is defined as:

$$\rho_i^{(l)(+)} = \frac{\mathbf{w}^{(l)}.\left(\mathbf{f}_{\mathbf{x}_{\sim x_i}}{}^{(l)(+)} - \mathbf{f}_{\mathbf{x}}{}^{(l)}\right)}{s^{(l)}}, \tag{3}$$

and the detectability cost $\rho_i^{(l)(-)}$ by:

$$\rho_i^{(l)(-)} = \frac{\mathbf{w}^{(l)}.\left(\mathbf{f}_{\mathbf{x}_{\sim x_i}}{}^{(l)(-)} - \mathbf{f}_{\mathbf{x}}{}^{(l)}\right)}{s^{(l)}}, \tag{4}$$

[5]For more details about the ASO embedding algorithm, please refer to [1], available on: http://www.lirmm.fr/∼kouider/Publications.html.

[6]STC: Syndrome Trellis Codes.

with $\mathbf{w}^{(l)}$ the vector orthogonal to the hyperplane separating the two classes calculated by the classifier F_l, $\mathbf{f}_{\mathbf{x}}{}^{(l)}$ the feature vector that we wish to classify by the classifier F_l, $\mathbf{f}_{\mathbf{x}_{\sim x_i}}{}^{(l)(+)}$ (resp. $\mathbf{f}_{\mathbf{x}_{\sim x_i}}{}^{(l)(-)}$) the feature vector obtained after the modification of the i^{th} pixel by $+1$ (resp. -1), and $s^{(l)} \in \mathbb{R}_+$ the normalization factor of the l^{th} classifier F_l (see [1]).

By using the functionalities of the *Kodovský's ensemble classifiers* [3] and the acquired knowledge of the learning phase, ASO [1] manages to preserve not only the distribution model of the current cover image, but also the distribution model of the sender's database. It thus improves the security of the embedding process.

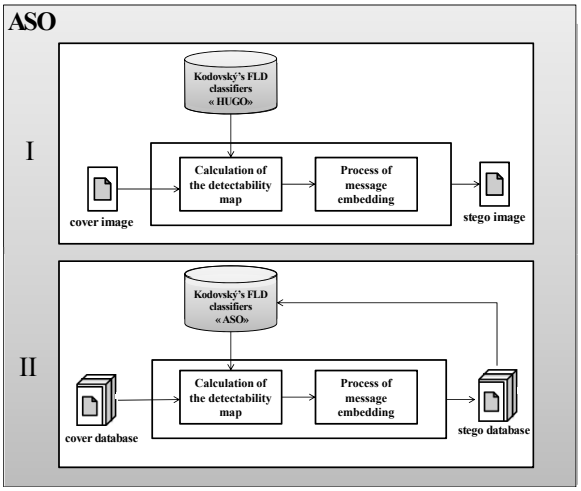


Fig. 1. General scheme of the Adaptive Steganography by Oracle (*ASO*) [1].

As shown in Figure 1, the embedding process of ASO [1] consists of two steps. The first step (labeled I in Figure 1) aims to produce a first draft of ASO's stego images. In this step, the computation of the detectability map ρ (Eq. 1) is performed by using the *Kodovský's ensemble classifiers* [3] that is trained to distinguish between cover and the stego images embedded with HUGO [2]. The second step (labeled II in Figure 1) is an iterative step that aims to improve the security of ASO. The detectability map is calculated using a *Kodovský's ensemble classifiers* [3] that is trained to distinguish between the cover and the ASO's stego images from the previous iteration.

At the end of the embedding process, ASO allows to obtain a set of a stego images, rather than only one stego image.

2.2. Technical points about detectability map computation

The computation of a feature vector $\mathbf{f}_{\mathbf{x}} \in \mathbb{R}^d$, with vector dimension $d \gg d_{red}$, is CPU consuming. In our case $\mathbf{f}_{\mathbf{x}}$ is obtained by first applying many high-pass filter and then count the m-uplets co-occurrences in the different high-pass images. In the ASO algorithm, the computation of the detectability map ρ requires to compute the values $\rho_i^{(l)(+)}$ and $\rho_i^{(l)(-)}$ for each pixel x_i, which involves the calculation of the

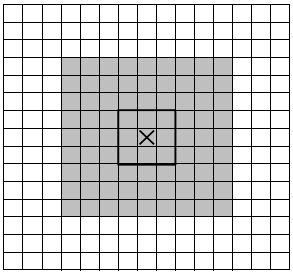


Fig. 2. Computation of the feature variations on a square window area of $r = 9$ width. The residual 1-Dimension filter used to compute the features has a size (s = 3).

two new feature vectors ${\mathbf{f}_{\mathbf{x}_{\sim x_i}}}^{(l)(+)}$ and ${\mathbf{f}_{\mathbf{x}_{\sim x_i}}}^{(l)(-)}$ resulting from the modification $+1$ or -1 of the i^{th} pixel (see Eq. 3 and Eq. 4). Since the vector $\mathbf{w}^{(l)}$ and the normalisation factor $s^{(l)}$ are calculated during the learning phase of the classifier, we do not need to calculate them again during the computation of $\rho^{(l)(+)}$ and $\rho^{(l)(-)}$. The computational complexity for the construction of the detectability map ρ comes mainly from the computation of ${\mathbf{f}_{\mathbf{x}_{\sim x_i}}}^{(l)(+)}$ and ${\mathbf{f}_{\mathbf{x}_{\sim x_i}}}^{(l)(-)}$. To address this problem, instead of calculating separately the feature vectors ${\mathbf{f}_{\mathbf{x}_{\sim x_i}}}^{(l)(+)}$ and ${\mathbf{f}_{\mathbf{x}_{\sim x_i}}}^{(l)(-)}$, we propose to only calculate, on a reduced area, the variation $({\mathbf{f}_{\mathbf{x}_{\sim x_i}}}^{(l)(+)} - {\mathbf{f}_{\mathbf{x}}}^{(l)})$ and $({\mathbf{f}_{\mathbf{x}_{\sim x_i}}}^{(l)(-)} - {\mathbf{f}_{\mathbf{x}}}^{(l)})$ introduced by the modification $+1$ or -1 of each pixel x_i.

We thus define for each pixel x_i a square window area of r width centred on x_i. This window area gives the set of pixels responsible of the changes between the vectors ${\mathbf{f}_{\mathbf{x}}}^{(l)}$ and ${\mathbf{f}_{\mathbf{x}_{\sim x_i}}}^{(l)(+)}$ (resp. ${\mathbf{f}_{\mathbf{x}_{\sim x_i}}}^{(l)(-)}$ and ${\mathbf{f}_{\mathbf{x}}}^{(l)}$). The pixels that are outside of this area do not introduce change between ${\mathbf{f}_{\mathbf{x}}}^{(l)}$ and ${\mathbf{f}_{\mathbf{x}_{\sim x_i}}}^{(l)(+)}$ (resp. ${\mathbf{f}_{\mathbf{x}_{\sim x_i}}}^{(l)(-)}$ and ${\mathbf{f}_{\mathbf{x}}}^{(l)}$). We thus do not consider those pixels during the computation of the feature variations.

The width r of the square window area depends on the size s of the high-pass 1-Dimension filter, and the order m of the co-occurrence matrice used to calculate the feature vectors [8]. The size of the window area, on which we calculate the variations $({\mathbf{f}_{\mathbf{x}_{\sim x_i}}}^{(l)(+)} - {\mathbf{f}_{\mathbf{x}}}^{(l)})$ and $({\mathbf{f}_{\mathbf{x}_{\sim x_i}}}^{(l)(-)} - {\mathbf{f}_{\mathbf{x}}}^{(l)})$, must be large enough to cover all possible modifications involved by changing the pixel x_i. Knowing that changing a given pixel x_i by $+1$ or -1 may affect (non pathological case) the m-uplets $(x_{i+a}, x_{i+(a+1)}, ..., x_{i+(a+m)})$, with $a \in \{-\lfloor \frac{r}{2} \rfloor, ..., \lfloor \frac{r}{2} \rfloor - m\}$, in all directions, choosing $r = s + 2(m-1)$ guarantees a valid result for the computation of the feature variations $({\mathbf{f}_{\mathbf{x}_{\sim x_i}}}^{(l)(+)} - {\mathbf{f}_{\mathbf{x}}}^{(l)})$ and $({\mathbf{f}_{\mathbf{x}_{\sim x_i}}}^{(l)(-)} - {\mathbf{f}_{\mathbf{x}}}^{(l)})$.

To take an example, for a residual 1-Dimension filter with $s = 3$ size and $m = 4$ (Figure 2), the involved variations $({\mathbf{f}_{\mathbf{x}_{\sim x_i}}}^{(l)(+)} - {\mathbf{f}_{\mathbf{x}}}^{(l)})$ and $({\mathbf{f}_{\mathbf{x}_{\sim x_i}}}^{(l)(-)} - {\mathbf{f}_{\mathbf{x}}}^{(l)})$ are calculated on a square window area of width $r = 9$.

Our implementation of ASO, for $d = 5330$, $L = 30$, $d_{red} = 250$, and $N = 10000$ images of 512×512, using the parallel OpenMP library on an architecture of 8 processors *Quad-Core AMD Opeteron(tm) Processor 8384*, at 2.69 GHz, took less than one day and half. Knowing that on a monoprocessor, without the trick of the square window (Eq. 3 and Eq. 4), the calculation of one feature vector $\mathbf{f}_{\mathbf{x}}$ took about 0.013s, the computation time of the detectability map ρ of the 10000 images would take $0.013s \times 2 \times 512 \times 512 \times 10000 = 68157440s$ (more than two years).

2.3. Paradigm of the steganography by database

As mentioned in Section 2.1, ASO introduces the new "*steganography by database*" paradigm. The embedding process of ASO takes into account not only the model distribution of the current cover image, but also the distribution of the sender's database, thus improving the security of the embedding process. Moreover, it allows to obtain a set of stego images instead of just one stego image, which offers to the sender the opportunity to choose the most secure image(s) during the transmission of his secret message.

Choosing the most reliable image(s) during the transmission phase can improve the security of ASO. In order to select the less detectable stego image(s), we compute for each stego image a score value that reflects its security level. One possible powerful method that offers ASO consists to compute for each stego image the number of FLD classifiers that have classified it as cover instead of stego, from the *Kodovský's ensemble classifiers* [3]. We thus define the security score as:

$$\begin{array}{rccl} S_{\mathbf{f}}^{FLD}: & \mathbb{R}^d & \rightarrow & \{0, ..., L\} \\ & \mathbf{x} & \rightarrow & S_{\mathbf{f}}^{FLD}(\mathbf{x}), \end{array}$$

$$\text{where:} \qquad S_{\mathbf{f}}^{FLD}(\mathbf{x}) = L - \sum_{l=1}^{L} F_l(\mathbf{f}_{\mathbf{x}}), \tag{5}$$

with $F_l(\mathbf{f}_{\mathbf{x}})$ the decision of the classifier F_l (1 for stego and 0 for cover), and $\mathbf{f}_{\mathbf{x}}$ the feature vector of the stego image $\mathbf{x}$. The higher the score $S_{\mathbf{f}}^{FLD}(\mathbf{x})$ is, the greater is the security of the stego image. Note that with that measure, we obtain several stego images with the same score.

For more finer granularity of the score value, we may use the sparsity measures that are generally used with the One Class Neighbor Machine (OC-NM) steganalyzer [9, 10].

Let us assume that we have K cover images from which we compute K d-dimensional features. By taking the set of cover images as a training base, the OC-NM computes for each samples $\mathbf{x}$ a sparsity measure $S_{\mathbf{f}}^{oc}(\mathbf{x})$ that characterizes the closeness of $\mathbf{x}$ to the cover images. The OC-NM steganalyzer strives to identify the best threshold γ so that all samples $\mathbf{x}$ with $S_{\mathbf{f}}^{oc}(\mathbf{x}) > \gamma$ are classified as stego.

Several types of sparsity measures are proposed in the original publication on OC-NM [9]. One of the most used measure that can be adopted as a security score, is the so-called Hilbert kernel density estimator:

$$\begin{array}{rccl} S_{\mathbf{f}}^{oc}: & \mathbb{R}^d & \rightarrow & \mathbb{R} \\ & \mathbf{x} & \rightarrow & S_{\mathbf{f}}^{oc}(\mathbf{x}), \end{array}$$

where:

$$S_{\mathbf{f}}^{oc}(\mathbf{x}) = \log\left(\frac{1}{\sum_{k=1}^{K} 1/\left(\parallel \mathbf{f}_{\mathbf{x}} - \mathbf{f}_k \parallel_2^{hd}\right)}\right), \qquad (6)$$

with $\mathbf{f}_{\mathbf{x}}$ the feature vector of the stego image $\mathbf{x}$, $\mathbf{f}_k$ the feature vector of the k^{th} cover image of the training set, $\parallel . \parallel_2$ the L_2 norm, d the feature vectors dimension, and h a parameter of smoothness.

Intuitively, since the sparsity measures reflect the closeness of a given image to the covers, using these measures as a security score allows us to evaluate the detectability of the used stego image(s). The smaller is the sparsity $S_{\mathbf{f}}^{oc}(\mathbf{x})$ of a given stego image, the greater is its security.

3. EXPERIMENTAL RESULTS

Our experiments were conducted using the BossBase v1.00 cover database[7] containing 10000 512×512 grayscale cover images in the pgm format, and the same 10000 images embedded with ASO[8] for each payload from 0.1 bpp to 0.5 bpp.

Each image is represented by a feature vector of $d = 5330$ MINMAX features. The set of features comes from the 1458 dimensional MINMAX vector with the truncation threshold $T = 4$, and the 3872 dimensional SUM3 vector from the HOLMES features [8].

To evaluate the necessity and the importance of the introduced paradigm of *the steganography by database*, we have built for each payload α from 0.1 bpp to 0.5 bpp two testing databases of 500 ASO's stego images. The base $\mathcal{B}_1^{(\alpha)}$ consists of 500 ASO's stego images that have been randomly selected from the BossBase v1.00 ASO's stego images. The base $\mathcal{B}_2^{(\alpha)}$ is composed of the most secure 500 ASO's stego images selected from the BossBase v1.00 ASO's stego images using the security measure $S_{\mathbf{f}}^{FLD}$ (see Eq. 5). Once calculated, for each payload, the two testing databases are then steganalyzed using the One-Class Support Vector Machine (OC-SVM) of LIBSVM[9]. The OC-SVM was trained on the BossBase v1.00 cover database using the Gaussian kernel $k(\mathbf{x}, \mathbf{y}) = \exp(-\gamma\|\mathbf{x} - \mathbf{y}\|^2)$ with $\gamma = 0.181526$ and $\nu = 0.01$ which is the desired false positive rate. The training data were scaled before, so that all features were in the range $[-1, +1]$ (the scaling parameters were derived from cover images only).

By using the OC-SVM for the steganalysis of the two testing databases ($\mathcal{B}_1^{(\alpha)}$ and $\mathcal{B}_2^{(\alpha)}$) for each relative payload α from 0.1 bpp to 0.5 bpp, we seek to test if the stego images that have been selected using the security measure criterion (Eq. 5 and Eq. 6) are more secure than those selected randomly by the sender. In other words, we want to prove the importance of choosing the most reliable image(s) during the secret communication phase (*i.e.* prove the additional security feature of *the steganography by database* paradigm).

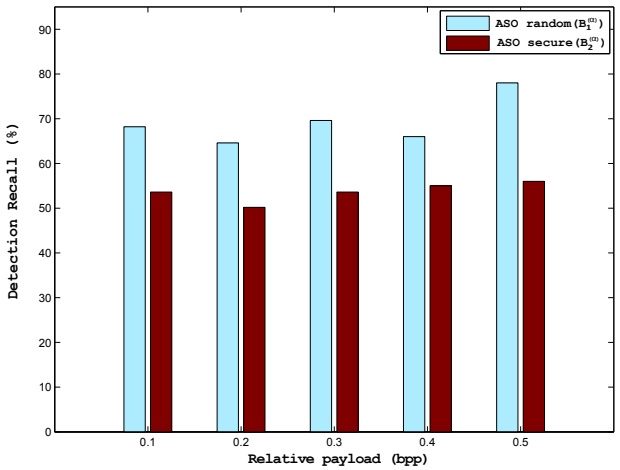


Fig. 3. Detection Recall (R) of $\mathcal{B}_1^{(\alpha)}$ and $\mathcal{B}_2^{(\alpha)}$ for five relative payloads.

From the results shown in Figure 3, for the five relative payloads from 0.1 bpp to 0.5 bpp the security of the stego database $\mathcal{B}_2^{(\alpha)}$ built using the security measure criterion $S_{\mathbf{f}}^{FLD}$, is better than the security of the randomly selected stego database $\mathcal{B}_1^{(\alpha)}$. For all relative payloads the detection recall[10] R of the OC-SVM steganalyzer on $\mathcal{B}_2^{(\alpha)}$ is lower than that on $\mathcal{B}_1^{(\alpha)}$. For instance, for $\alpha = 0.5$ bpp, the detection recall R on $\mathcal{B}_1^{(\alpha)}$ is 78%, whereas it is only 56% on $\mathcal{B}_2^{(\alpha)}$. Similarly, the detection recall R on $\mathcal{B}_2^{(\alpha)}$ at 0.4 bpp is less than that on $\mathcal{B}_1^{(\alpha)}$; 55% compared to 66%. In brief , the detection recall R on $\mathcal{B}_2^{(\alpha)}$ for all relative payloads is close to 50-55%. The OC-SVM steganalyzer classifies incorrectly one out of two times a given stego image as cover image. In other words, on $\mathcal{B}_2^{(\alpha)}$, the OC-SVM has a random behaviour, since it can not distinguish between the cover and stego images. This confirms that the stego database $\mathcal{B}_2^{(\alpha)}$ is more secure than the stego base $\mathcal{B}_1^{(\alpha)}$

Note that the detection recall R of $\mathcal{B}_2^{(\alpha)}$ at 0.1 bpp is higher than that at 0.2 bpp. It is 53.6% at 0.1 bpp, whereas it is 50.2% at 0.2 bpp. Indeed, for payloads under 0.2 bpp, the ASO embedding algorithm does not perform as well as at higher payloads, since the oracle used for computing the detectability map (Section 2.1) can not manage to distinguish between secure and insecure areas [1].

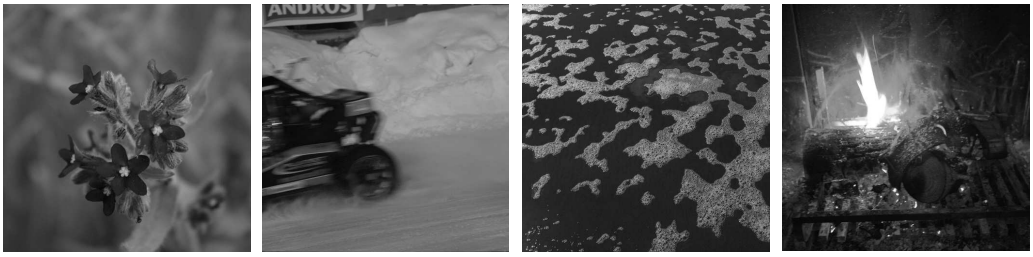
The obtained results show that the set $\mathcal{B}_2^{(\alpha)}$ of the stego images selected using the security measure $S_{\mathbf{f}}^{FLD}$ are more secure than those of $\mathcal{B}_1^{(\alpha)}$ that have been randomly selected.

[7] BossBase v1.00: A database of 10000 images available on http://agents.cz/boss/BOSSFinal/.

[8] The embedding process of ASO was done using $L = 30$ classifiers, $d = 5330$, and $d_{red} = 250$ [1].

[9] LIBSVM: A Library for Support Vector Machines, available on http://www.csie.ntu.edu.tw/ cjlin/libsvm/.

[10] The detection recall $R = \frac{\textit{number of stego images correctly classified}}{\textit{total number of stego images}}$.



$S_{\mathbf{f}}^{\mathrm{FLD}}(\mathbf{x}) = 30$ $S_{\mathbf{f}}^{\mathrm{FLD}}(\mathbf{x}) = 29$ $S_{\mathbf{f}}^{\mathrm{FLD}}(\mathbf{x}) = 28$ $S_{\mathbf{f}}^{\mathrm{FLD}}(\mathbf{x}) = 27$

Fig. 4. Some exemples of the selected stego images using the security measure $S_{\mathbf{f}}^{FLD}$ criterion ($\alpha = 0.5$ bpp, and $L = 30$).

By using a simple security metrics, such as $S_{\mathbf{f}}^{FLD}$, we obtain a strong security. The used steganalyzer can not distinguish between cover and stego images. This confirms the relevance of choosing the most reliable image(s) during the transmission phase of the secret message. Moreover, we believe that using a more finer security measure such as $S_{\mathbf{f}}^{oc}$ (Eq. 6) may improve even more the security of the message communication[11].

Some examples of the stego images that have been selected using the security measure $S_{\mathbf{f}}^{FLD}$ criterion are given in Figure 4. As we can see, the selected stego images that have been judged as the most secure images correspond to the noisy and textured images.

4. CONCLUSION

In this paper, we present the technical points about the adaptive steganography by oracle (ASO). First, we discuss about the detectability map computation of ASO that reduce significantly its computational complexity. Then, we study the security of ASO thanks to the paradigm of *the steganography by database*. Since our embedding ASO algorithm allows to obtain a set of stego images instead of just one stego image, we offer to the sender the opportunity to choose the most undetectable stego image(s) during the transmission of his secret message. To do this, we propose some security metrics that help him to select the most reliable stego image(s). Experimental results show that using a simple security metric, such as $S_{\mathbf{f}}^{FLD}$ (Eq. 5), for choosing the most secure stego image(s), improves significantly the security of the communication phase of ASO.

ACKNOWLEDGMENTS.

This work was supported by the "Ministry of Higher Education and Scientific Research of Peoples Democratic Republic of Algeria".

5. REFERENCES

[1] Sarra Kouider, Marc Chaumont, and William Puech, "Adaptive Steganography by Oracle (ASO)," in *submission*.

[2] Tomáš Pevný, Tomáš Filler, and Patrick Bas, "Using High-Dimensional Image Models to Perform. Highly Undetectable Steganography," in *Information Hiding - 12th International Conference*, Berlin, Heidelberg, October 01 2010, vol. 6387 of *Lecture Notes in Computer Science, IH'10*, pp. 161–177, Springer-Verlag.

[3] Jan Kodovský and Jessica J. Fridrich, "Steganalysis in High Dimensions: Fusing Classifiers Built on Random Subspaces," in *Media Watermarking, Security, and Forensics XIII, part of IS&T SPIE Electronic Imaging Symposium*, San Francisco, CA, January 23-26 2011, vol. 7880, paper. 21, pp. L 1–12.

[4] Jessica J. Fridrich and Tomáš Filler, "Practical Methods for Minimizing Embedding Impact in Steganography," in *Security, Steganography, and Watermarking of Multimedia Contents IX, part of IS&T SPIE Electronic Imaging Symposium*, San Jose, CA, January 29-February 1 2007, vol. 6505, pp. 02–03.

[5] Patrick Bas, Tomáš Filler, and Tomás Pevný, "Break Our Steganographic System — the ins and outs of organizing BOSS," in *Information Hiding - 13th International Workshop*, Prague, Czech Republic, May 18-20 2011, vol. 6958 of *Lecture Notes in Computer Science, IH'11*, pp. 59–70, Springer-Verlag.

[6] Tomáš Filler, Jan Judas, and Jessica J. Fridrich, "Minimizing Embedding Impact in Steganography using Trellis-Coded Quantization," in *Media Forensics and Security II, part of IS&T SPIE Electronic Imaging Symposium*, San Jose, CA, USA, January 18-20 2010, vol. 7541, paper. 05.

[7] Tomáš Filler and Jessica J. Fridrich, "Design of Adaptive Steganographic Schemes for Digital Images," in *Media Watermarking, Security, and Forensics XIII, part of IS&T SPIE Electronic Imaging Symposium*, San Francisco, CA, January 23-26 2011, vol. 7880, paper. 13, pp. F 1–14.

[8] Jessica J. Fridrich, Jan Kodovský, Vojtech Holub, and Miroslav Goljan, "Steganalysis of Content−Adaptive Steganography in Spatial Domain," in *Information Hiding - 13th International Conference*, Tomás Filler, Tomás Pevný, Scott Craver, and Andrew D. Ker, Eds., Prague, Czech Republic, May 18-20 2011, vol. 6958 of *Lecture Notes in Computer Science, IH'11*, Springer.

[9] Alberto Munoz and Javier M. Moguerza, "Estimation of high-density regions using one-class neighbor machines," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28(3), pp. 476–480, March 2006.

[10] Tomás Pevný and Jessica J. Fridrich, "Novelty detection in blind steganalysis," in *workshop on Multimedia and security, part of MM&Sec'08 Proceedings of the 10th ACM multimedia*, New York, NY, USA, September 22-23 2008, pp. 167–176, ACM.

[11] Because of lack of time, we did not test the $S_{\mathbf{f}}^{oc}$ security measure criterion.