Adaptive Steganography scheme based on LDPC codes

I.DIOP[1];S.M FARSS[1], K TALL[1] , P. A. FALL[2],M .L .DIOUF[1]; A K DIOP[1];
[1] Polytechnic School of Cheikh Anta Diop University
[2] Gaston Berger University
idydiop@yahoo.fr, farsism@yahoo.com, papa-alioune.fall@ugb.edu.sn

***Abstract*— Steganography is the art of secret communication. Since the advent of modern steganography, in the 2000s, many approaches based on the error correcting codes (Hamming, BCH, RS, STC ...) have been proposed to reduce the number of changes of the cover medium while inserting the maximum bits. The works of I.Diop and al [1], inspired by those of T. Filler [2] have shown that the LDPC codes are good candidates in minimizing the impact of insertion. This work is a continuation of the use of LDPC codes in steganography. We propose in this paper a steganography scheme based on these codes inspired by the adaptive approach to the calculation of the map detectability. We evaluated the performance of our method by applying an algorithm for steganalysis.**

***Index Terms*—Adaptative steganography, complexity, detectability, steganalysis.**

I. INTRODUCTION

Steganography is the art of secret communication. It consists of inserting a message into a harmless medium such as an image, a video, a sound so that insertion is statistically undetectable. One of the assumptions made before 2011 was to say it was enough to minimize the number of changes of the medium to ensure maximum security of the scheme. This assumption is questionable since the BOSS competition [3]. That said, the study of error correcting codes to insert a message while minimizing the number of changes is an interesting problem. Many steganographic schemes based on the principle of "embedding matrix" (there use hijacked correcting codes) have been proposed in the past BCH, RS ... [4] [5]. These patterns are usually far from the terminal efficiency [1].

Our work is a continuation of the use of LDPC codes in steganography. Our approach is based on the consideration of the map of detectability upon insertion of the secret message. To approach this problem, we first present in section 2 the notion of detectability map in steganography. In section 3, we describe the steganalysis that consist to taking into account the system's attack. In section 4, we present the principle of the proposed method. And finally we conclude in section 5 with the presentation and analysis of results.

II. THE NOTION OF DETECTABILITY MAP

Let **x** be a cover image, **x** = $(x_1, \ldots, x_n)$. The goal of steganography by minimizing the impact of embedding is to provide the minimum of alterations to the roof sheathing **x** to produce a stego object **y** = $(y_1, \ldots, y_n)$ that communicate the message **m** = $(m_{1, \ldots,} m_n)$. To do this, we rely on the principle of HUGO scheme [6] which models the impact of embedding while minimizing the distortion function $D(x, y)$.

$$D(x,y) = \sum_{i=1}^{n} \rho_i |x_i - y_i| \qquad (1)$$

the we minimize. This distortion function is based on the use of a map detectability ρ_i which assigns to each cover element x_i with $i \in \{1, \ldots, n\}$ a cost of detectability $\rho_i > 0$ modeling the impact of the safety due to the modification of this element.

For each pixel x_i, we compute each its own map of detectability. The detectability ρ_i of the pixel x_i is defined by HUGO [6]:

$$\rho_i = \min(\rho_i^{(+)}, p_i^{(-)}) \qquad (2)$$

with $\rho_i^{(+)}$ (respectively $\rho_i^{(-)}$) the detectability after modification +1(respectively -1) of the pixel x_i.

$$\rho_i^{(+)} = \sum_{l=1}^{L} \rho_i^{(l)(+)} \qquad (3)$$

$$\rho_i^{(-)} = \sum_{l=1}^{L} \rho_i^{(l)(-)} \qquad (4)$$

To calculate these detectabilities, we use the method proposed in the works of S.Kouider and al [7]. The authors propose to calculate the detectability through an oracle consisted of L classifier FLD of Kodovsky and al [8].

$$\rho_i^{(l)(+)} = \frac{w^{(l)}\left(f_x^{(l)(+)} - f_x^{(l)}\right)}{S^{(l)}} \qquad (5)$$

$$\rho_i^{(l)(-)} = \frac{w^{(l)}\left(f_x^{(l)(-)} - f_x^{(l)}\right)}{S^{(l)}} \qquad (6)$$

with $s^{(l)} \in \mathbb{R}_+$ the scaling factor of l^ht classfier, $w^{(l)}$ the orthogonal vector to the hyper plane separating the two classes cover and stego classifier, $f_x^{(l)}$ the feature vector to classify by the classifier, et $f_x^{(l)(+)}$ (respectively $f_x^{(l)(-)}$) the feature vector after modification +1 (respectively -1) of the pixel x_i.

III. THE STEGANALYSIS

Steganalysis is the dual discipline of steganography. His principle differs from cryptanalysis as steganography differs from cryptography [9]. The initial goal of steganalysis isn't to get the hidden message in the media coverage, but only to the simple detection of the presence of this one. There are two categories of attack to classify the steganalysis:

- Passive attacks: The steganalyst not affect the signals traveling over the communication channel. They seek to identify the presence of a message in order to reconstitute secondary thereafter. These attacks can take many forms: reading or listening to the file, comparing with the original file (if available), statistical attacks (attack on LSB for example), the signature detection software used (study hexadecimal code)...
- Active attacks: The steganalyst can attack signals by various methods for the purpose of nullifying or impairing the embedded message so that the receiver can't grasp its meaning. They consist destroy the hidden message without paying attention to its meaning. The goal is to delete the message or make it unusable. This destruction will often take place through changes in the media. For example in the case of the method of steganography in LSB, overwrite all bits by placing 0 or 1 clears any message concealed.

It is usually placed in the case of passive steganalysis steganography. Active steganalysis is rather applied in the case of watermaking.

Although the main goal of steganalysis is the simple detection of the presence of a message in a suspect environment, the field has evolved to some improvements, such as to estimate its size. One speaks in this case of quantitative steganalysis [10]. Binary classification between medium coverage and stego medium steganalysis could be described qualitatively, although this terminology is not really used. In this category, there are two types of steganalyses as the type of measurements. If the measures depend on algorithms that we are trying to detect, the steganalysis is called specific [11]. But on the other hand, when the measurement is independent of the algorithm that is to be detected, the steganalysis is called universal [12].

IV. PRINCIPLE OF THE METHOD PROPOSED

Let $\boldsymbol{x}$ be a sheathing containing n elements $\mathbf{x} \in \mathbb{F}_2^n$, $\boldsymbol{m}$ the secret message, $\mathbf{m} \in \mathbb{F}_2^m$ with $\boldsymbol{m}$<$\boldsymbol{n}$$C(\mathrm{m}) = \{\mathbf{y} \in \mathbb{F}_2^n | \mathrm{H}\mathbf{y} = \boldsymbol{m}\}$ is the coset (all the code words that have the same syndrome). The goal of steganography by minimizing the impact of integration is to provide the minimum change in host support $\boldsymbol{x}$ to produce the stego object $\mathbf{y}$, $\mathrm{y} \in \mathbb{F}_2^n$.

In general, to encode a code word, we use a generator matrix G. But in the case of LDPC codes, the parity check matrix H is used for encoding and decoding. The insertion and extraction of the message is determined by:

$$\mathrm{y} = Emb(\mathrm{x}, \mathrm{m}) \tag{7}$$

$$Ext(\mathrm{m}) = \mathrm{Hy} = \mathrm{m} \tag{8}$$

Our embedding scheme based on the principle of minimizing of impact insertion correlated with the detectability. HUGO [6] models the embedding impact by a mesure of distortion additive and positive $D: \mathcal{X} \times \mathcal{X} \to [0; +\infty[$.

$$D(x, y) = \sum_{i=1}^{n} \rho_i |x_i - y_i| \tag{9}$$

The minimal distortion that we provide and obtained by hiding **m** bits in an object of coverage of n pixels is given by T.Filler and J. Fridrich [13] in the following theorem.

Theorem:

Let ρ = $(\rho_i)_{i = 1 \text{ to } n}$, $0 < \rho_i < \infty$, the set of constants defining the additive distortion measure for $i = 1$ *to* n. Let $0 \le m \le n$, the number of bits that we want to communicate using an operation of binary insertion.

The minimal distortion expected can be written in the following form:

$$D_{min}(m, n, p) = \sum_{i=1}^{n} p_i \rho_i \tag{10}$$

where

$$p_i = \frac{e^{-\lambda \rho_i}}{1 + e^{-\lambda \rho_i}} \tag{11}$$

is the probability of change of i^{th} pixel. The parameter λ is obtained by solving

$$-\sum_{i=1}^{n} (p_i \log_2 p_i + (1 - p_i) \log_2 (1 - p_i)) = m \tag{12}$$

The importance of this problem lies in the separation of the image model (requiring the calculation of the detectability map ρ_i) and the encryption algorithm used in the scheme of insertion. The optimal encoding can be simulated by switching each pixel with a probability ρ_i. Details of use of this theorem are given in the HUGO scheme [6].

We use this principle to bury the message in the media coverage while having minimum distortion on the decking.

Example of application:

Suppose that the sender wishes to communicate a message of length on $\alpha_p = p/(2^p -1)$, $p \ge 0$, which means that messages of p bits, *m[1], ..., m[p]*, must be integrated into 2^p - 1 pixels of the cover image. The sender modifies the values of the pixels so that the pixel is the smallest value of ρ_i satisfies the equation **m=Hy.**

In practice, if you want to insert a message in minimizing the impact of insertion (detectability map ρ is known) with the constraint of a fixed payload, it is possible to simulate the optimal insertion seeking parameter λ (solving the equation (12)), and then modifying each pixel according to the probability ρ_i defined in equation (11).

A. The embedding scheme

To embed the secret message in the cover medium, we use the parity check matrix to find the vector **y** such H**y** = **m**.

The processing algorithm of parity check matrix is described as follows:

Input: Invertible parity check matrix **H**,

Output: Parity matrix equivalent of form $\begin{pmatrix} A & B & T \\ C & D & E \end{pmatrix}$.

Step1. Triangulation (Run permutations of rows or columns to an approximation of the matrix H as lower triangular).

Step2. Control rank (Use gaussian elimination to actually execute the pre-multiplication).

Calculating detectability map allow us to use the pixels on which the message is inserted. We presented below the algorithm of the proposed scheme.

Input: The cover medium,

Output: The stego medium

Step1. Processing of the control parity check matrix.

Step2. Calcul of the vector **y** member of the coset

$\boldsymbol{y} = P^T.(\boldsymbol{m},\bar{0})$ with P^{T} transposed of the matrix P (matrix obtained from the treatement of the parity check matrix) and $\bar{0}$ a concatenated vector to **m** for that the matrix multiplication is possible.

Step3. Calculation of ρ_i for each pixel of the medium coverage.

Step4. Choice of the pixel that has the smallest value of ρ_i and the targeting vector.

Step5. Insertion of the message **m.**

Our adaptative scheme insertion is summarized by the following figure:

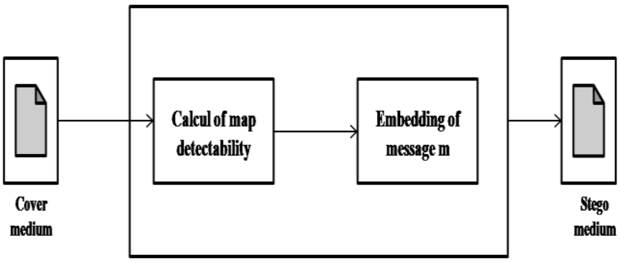

Figure 1. Adaptative integration scheme

B. Extraction scheme

To retrieve the message, we calculate the syndrome by using the parity check matrix. The algorithm is described as follows:

Input: The Stego medium

Output: The message m

Step1. Read the vector of the stego medium

Step2. Calcul of syndrome y

Step3. Retrieve the message with the relation $Hy = m$.

The retrieve process is summarized by the following figure:

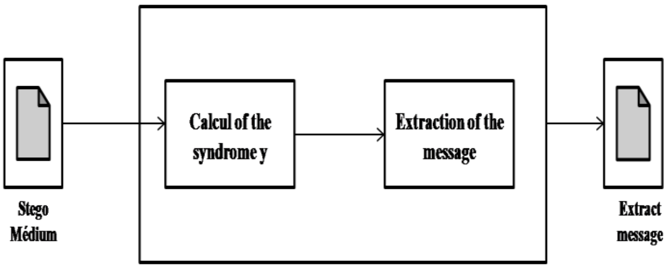

Figure 2. The extraction scheme

V. PRESENTATION AND ANALYSIS OF RESULTS

To evaluate the performance of our scheme, we measure the complexity first and then take the place of the attacker. The goal of steganography is primarily stealth. Regarding security schemes themselves, it is important that the goal is reached and an attacker cannot harm our system.

A. Complexity

Complexity is the number of computation and algorithmic nature of the instructions needed to perform the insertion of the message and its extraction. It also shows the computation time required for the operation of steganography. In the patterns of insertion secret message, it is preferable to use a low complexity algorithm for landfill operations and extraction is not expensive in computation time. This is why we have optimized our algorithm best to reinforce its rules.

To assess the complexity of our algorithm, we conducted an experiment on our diagram by varying the rate steganographic and noted the time each run. So we get the graph below:

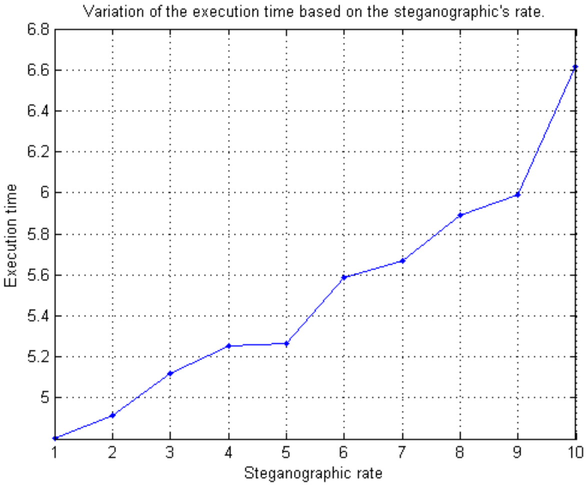

Figure 3. Variation of the execution time depending on the rate steganographic

This curve shows the execution time of our algorithm based on the rate steganographic inserted into the medium. In each run, we varied the size of the secret message inserted in an image. The curve shows that when the message size increases, the execution time increases. At t = 6.6 seconds, we reached the maximum message size to fit into the medium. This size corresponds to a text file of 625 characters for an image size $434 \times 567\ pixels$.

B. *Steganalysis of the method*

We show in this section that our algorithm is resistant to visual and statistical attacks. The first opponent a scheme of steganography is visual attack. No difference should be visible to the human eye between an original image and the reconstructed. The experiment below allowed us to test the invisibility criterion of our algorithm.

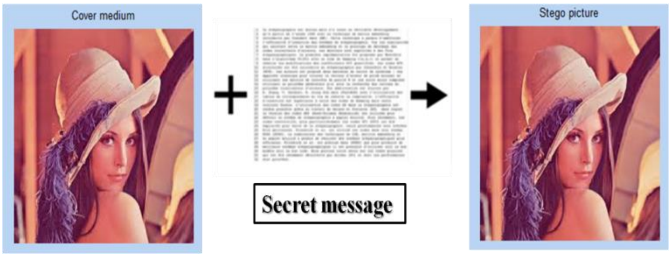

Figure 4. Visual comparison of the cover and the stego medium

We buried by our optimized algorithm, the message «Secret Message» on figure 3 in the original image (medium coverage). The visual system shows that there is no difference between the original image and the reconstituted. So we can say that the primary goal of steganography imperceptibility is achieved.

To measure the performance of our scheme in terms of statistics, we use the difference histograms. We experience as our algorithm by applying it to some pictures from our database. Figure 5 shows the histograms of the original image and stéganographied.

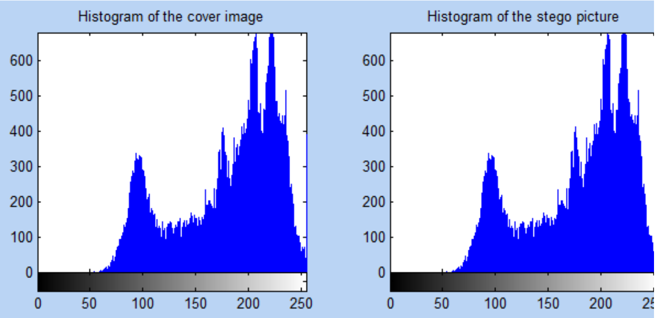

Figure 5. Histograms of the cover medium and the steganographied medium

Thus we see that the analysis of histograms before and after burying the secret message shows a small difference between the histogram of the original image and the reconstructed. The difference is more noticeable if the message size increases inserted.

C. *Measure of image distorsion*

To measure the distortion of steganographic images, we use the PSNR (Peak Signal to Noice Ratio). It allows measuring the distortion between the original image and the reconstructed. The unit of measurement is the decibel *dB*. PSNR is calculated using the MSE (Mean Square Error). Are I_o, an original image and a reconstructed image I_r, size $M \times N$. PSNR and MSE are given by the following relations :

$$PSNR(I_o, I_r) = 10 \log_{10} \frac{D^2}{MSE(I_o, I_r)} \qquad (13)$$

$$MSE(I_o, I_r) = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [I_o(i,j) - I_r(i,j)]^2 \qquad (14)$$

with *D* the dynamics of the signal (the maximum possible value for a pixel). In the standard case of an image where the components of a pixel are coded on 8 bits, *D = 255*. More the value of PSNR is great, more the images being compared are similar. When the value of PSNR between two images is greater than *35 dB*, this means that there is no visible difference between the two. If it is below *20 dB* means that the two images are very different.

For our experiment, we inserted 10 messages of different sizes in different images of the same size (512 × 512). By calculating the MSE and the PSNR for each pair of image (stego and clean), we obtain the curve of variation of PSNR based on the inverse of the load following relative:

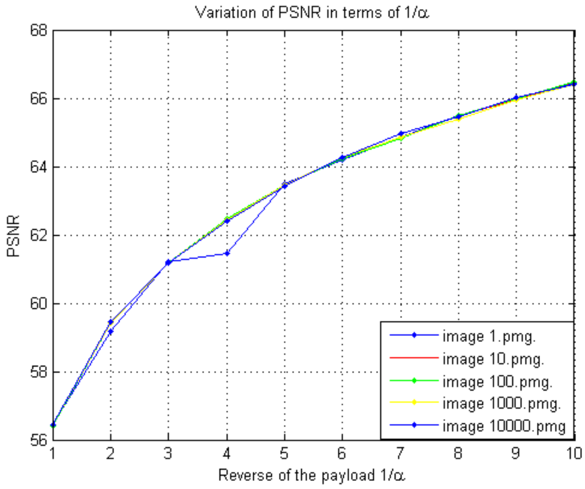

Figure 6. Variation of the PSNR depending on the direction of the payload

PSNR measurement on some images (.pmg) of the BOSS base [12], our algorithm experienced helped plot the above. We have 56.418 *dB* ≤ PSNR ≤ 66.4198 *dB*.

These values are well above 35 *dB*. This means that there is a difference between the trivial and clean images stégos images.

Then we can conclude that we have a good distortion performance.

VI. Conclusion

In this paper, we first recalled the notion of detectability map. We then presented steganalysis for even the behavior of the system to an attacker. The principle of the proposed method is then described before the presentation and analysis of results.

The proposed approach is based on taking into account the detectability map, we tested the performance of the scheme through the complexity, the specific steganalysis and the distortion of original and steganographic images. The complexity study showed that at t = 6.6 seconds, the maximum size of the message to insert is reached and corresponds to 625 characters. The attack on the scheme has enabled us to successfully face an opponent and shows that there's a slight difference between the histograms of the cover image and those steganographic images. The measure of images distortion showed that the distortion increases as the payload increases. In fact, more than the message size inserted increase, the change in the medium coverage (distortion) is important. PSNR values found are higher than 35 *dB*, which allowed us to confirm that the original image is very close to the steganographic image.

The future vision of our study focuses on the implementation of a specific steganalysis scheme to detect the presence of a secret message on a medium that steganographied with an algorithm based on LDPC codes.

References

[1] Diop, S. M. Farssi, M. Chaumont, O. Khouma, et H. B. Diouf, “Utilisation des codes LDPC en stéganographie, ” CORESA’2012, COmpression et REprésentation des Signaux Audiovisuels, Lille, France, 24-25 mai, 2012, 7 pages.

[2] Tomáš Filler, “Minimizing embedding impact in steganography using low density codes,” Thesis, Department of Electrical and Computer Engineering, SUNY Binghamton, USA, 2006/2007.

[3] P. Bas, T. Filler, T. Pevny, “Break Our Steganographic System --- the ins and outs of organizing BOSS,” In proceedings of Information Hiding Conference, Prague, 2011.

[4] Rongyue Zhang, Vasiliy Sachnev, Hyoung Joong Kim, “Fast BCH syndrome coding for steganography,” S. Katzenbeisser and A.-R. Sadeghi (Eds.), IH 2009, LNCS 5806, pp. 44-58, Springer-Verlag Berlin Heiderbelg 2009.

[5] F. Galand, C. Fontaine, “How can reed-solomon codes improve steganographic schemes.” In Information Hidding, Rennes, France, 2007.

[6] Tomáš Pevnỳ, Tomáš Filler and Patrick Bas, “Using high-dimensional image models to perform highly undetectable steganography,” Czech Technical University in Prague, Czech Republic; State University of New York in Binghamton, NY, USA; CNRS-LAGIS, Lille, France, 2010.

[7] S. Kouider, M. Chaumont, et W. Puech, “Stéganographie Adaptative par Oracle (ASO),” CORESA’2012, COmpression et REprésentation des Signaux Audiovisuels, Lille, France, 24-25 mai, 2012, 6 page.

[8] J. Kodovský et J.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, volume 7880, paper. 21, pages L 1–12, San Francisco, CA, January 23-26 2011.

[9] C. Tavernier, “Testeurs, problèmes de reconstruction univariés et multivariés et application à la cryptanalyse du DES, ” Thèse de doctorat, soutenu le 15, Janvier 2004 à l’Ecole Polytechnique, France.

[10] Sanjay Kumar Jena, G. V. V. Krishna, “Blind Steganalysis, Estimation of Hidden Message Length”.

[11] A. Westfeld, A. Pfitzmann, “Attacks on steganographic Systems, breaking the steganographic utilities Eztego, Jsteg, Steganos, and S-Tools ---- and Some Lessons Learned”.

[12] B. ROUE, P.BAS, J.M CHASSERY, “Influence des vecteurs caractéristiques en stéganalyse par Séparateurs à Vastes Marges”.

[13] J. Fridrich and T.Filler, “Pratical methods for minimizing embedding impact in steganography.” In:Proceddings SPIE, EL, Security, Steganography, and Watermaking of Multimedia Contents IX. Vol. 6505, pp. 02-03. San Jose, CA (January, 29-Feburary 1 2007).

[14] T.J. Richardson and R.L Urbanke, “Efficient Encoding of Low-DensityParity-Check Codes,” IEEE Trans. Inform. Theory, vol. 47, pp. 638-656, February 2001.