Application of Steganography for Anonymity through the Internet

Jacques M. Bahi, Jean-François Couchot, Nicolas Friot, and Christophe Guyeux*
FEMTO-ST Institute, UMR 6174 CNRS
Computer Science Laboratory DISC
University of Franche-Comté
Besançon, France
{jacques.bahi, jean-francois.couchot, nicolas.friot, christophe.guyeux}@femto-st.fr

** Authors in alphabetic order*

***Abstract*—In this paper, a novel steganographic scheme based on chaotic iterations is proposed. This research work takes place into the information hiding security framework. The applications for anonymity and privacy through the Internet are regarded too. To guarantee such an anonymity, it should be possible to set up a secret communication channel into a web page, being secure. To achieve this goal, we propose an information hiding scheme being stego-secure, which is the highest level of security in a well defined and studied category of attacks called "watermark-only attack". This category of attacks is the best context to study steganography-based anonymity through the Internet. The steganalysis of our steganographic process is also studied in order to show its security in a real test framework.**

***Keywords*-Privacy; Internet; Steganography; Security; Chaotic iterations.**

I. INTRODUCTION

In common opinion or for non specialists, anonymity through the Internet is only desirable for malicious use. A frequent thought is that individuals who search or use anonymity tools have something wrong or shameful to hide. Thus, as privacy and anonymity software as proxy or Tor [1] are only used by terrorists, pedophiles, weapon merchants, and so on, such tools should be forbidden. However, terrorism or pedophilia existed in the absence of the Internet. Furthermore, recent actualities recall to us that, in numerous places around the world, to have an opinion that diverges from the one imposed by political or religious leaders is something considered as negative, suspicious, or illegal. For instance, Saudi blogger Hamza Kashgari jailed, may face execution after tweets about Muhammad. Generally speaking, the so-called Arab Spring, and current fighting and uncertainty in Syria, have taught to us the following facts. First, the Internet is a media of major importance, which is difficult to arrest or to silence, bearing witness to the need for democracy, transparency, and efforts to combat corruption. Second, claiming his/her opinions, making journalism or politics, is dangerous in various states, and can lead to the death penalty (as for numerous Iranian bloggers: Hossein Derakhshan [2], Vahid Asghari, etc.).

Considering that the freedom of expression is a fundamental right that must be protected, that journalists must be able to inform the community without risking their own lives, and that to be a defender of human rights can be dangerous, various software have emerged these last decades to preserve anonymity or privacy through the Internet. Excepting of the Mix-Network principle [3], the most famous tool of this kind is probably Tor, the onion router. Tor client software routes Internet traffic through a worldwide volunteer network of servers, in order to conceal a user's location or usage from anyone conducting network surveillance or traffic analysis. Another example of this kind is given by Perseus [4], a firefox plugin that protect personal data, without infringing any national crypto regulations, and that preserve the true needs of national security. Perseus replaces cryptography by coding theory techniques, such that only agencies with a strong enough computer power can eavesdrop traffic in an acceptable amount of time. Finally, anonymous proxy servers around the world can help to keep machines behind them anonymous: the destination server (the server that ultimately satisfies the web request) receives requests from the anonymizing proxy server, and thus does not receive information about the end user's address.

These three solutions are not without flaws. For instance, when considering anonymizers, the requests are not anonymous to the anonymizing proxy server, which simply moves the problem on: are these proxy servers worthy of trust? Perseus can be broken with enough computer power. And due to its central position and particular conception, Tor is targeted by numerous attacks and presents various weaknesses (bad apple attack, or the fact that Tor cannot protect against monitoring of traffic at the boundaries of the Tor network).

Considering these flaws, and because having a variety of solutions to provide anonymity is a good rule of thumb, a steganographic approach is often regarded in that context [5]. Steganography can be applied in several ways to preserve anonymity through the Internet, encompassing the creation of secret channels through background images of websites, into Facebook photo galleries, on audio or video streams, or in non-interpreted characters in HTML source codes. The authors' intention is not to describe precisely these well-known techniques, but to explain how to evaluate their security. They applied it on a new algorithm of steganography based on chaotic iterations and data embedding in least significant coefficients. This state-of-the-art in information hiding security is organized as follows.

In Section II, some basic reminders concerning both mathematical notions and notations, and the Most and Least Significant Coefficients are given. Our new steganographic process called $\mathcal{DI}_3$ which is suitable to guarantee anonymity of data for privacy on the Internet is presented in Section III. In Section IV, a reminder about information hiding security is realized. The attacks classification in a steganographic framework are given, and the level of security of $\mathcal{DI}_3$ is studied. In the next section the security of our new scheme is evaluated. Then, in Section- VI the steganalysis of the proposed process is realized, and it is compared with other steganographic schemes in the literature. This research work ends by a conclusion section, where our contribution is summarized and intended future researches are presented.

II. BASIC REMINDERS

A. Mathematical definitions and notations

Let S^n denotes the n^{th} term of a sequence S, and V_i the i^{th} component of a vector V. For $a, b \in \mathbb{N}$, we use the following notation: $[\![a;b]\!] = \{a, a+1, a+2, \dots, b\}$.

Definition 1: *Let* $\mathsf{k} \in \mathbb{N}^*$. *The set of all sequences which elements belong into* $[\![1;\mathsf{k}]\!]$, *called* strategy adapters *on* $[\![1;\mathsf{k}]\!]$, *is denoted by* $\mathbb{S}_\mathsf{k}$. ☐

Definition 2: *The* support of a finite sequence *S of n terms is the finite set $\mathscr{S}(S) = \left\{S^k, k < n\right\}$ containing all the distinct values of S. Its cardinality is s.t. $\#\mathscr{S}(S) \leqslant n$.* ☐

Definition 3: *A finite sequence $S \in \mathbb{S}_\mathsf{N}$ of n terms is* injective *if $n = \#\mathscr{S}(S)$. It is* onto *if $N = \#\mathscr{S}(S)$. Finally, it is bijective if and only if it is both injective and onto, so $n = N = \#\mathscr{S}(S)$.* ☐

Remark 1: *On the one hand, "S is injective" reflects the fact that all the n terms of the sequence S are distinct. On the other hand, "S is onto" means that all the values of the set $[\![1;\mathsf{N}]\!]$ are reached at least once.* ☐

B. The Most and Least Significant Coefficients

We first notice that terms of the original content x that may be replaced by terms issued from the watermark y are less important than other: they could be changed without be perceived as such. More generally, a *signification function* attaches a weight to each term defining a digital media, depending on its position t.

Definition 4: *A* signification function *is a real sequence $(u^k)^{k\in\mathbb{N}}$.* ☐

Example 1: *Let us consider a set of grayscale images stored into portable graymap format (P3-PGM): each pixel ranges between 256 gray levels, i.e., is memorized with eight bits. In that context, we consider $u^k = 8 - (k \mod 8)$ to be the k-th term of a signification function $(u^k)^{k\in\mathbb{N}}$. Intuitively, in each group of eight bits (i.e., for each pixel) the first bit has an importance equal to 8, whereas the last bit has an importance equal to 1. This is compliant with the idea that changing the first bit affects more the image than changing the last one.* ☐

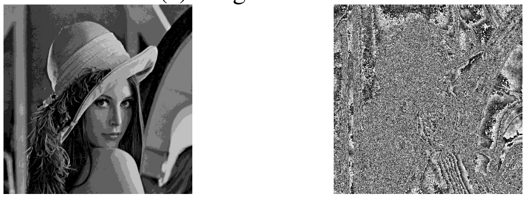
Definition 5: *Let $(u^k)^{k\in\mathbb{N}}$ be a signification function, m and M be two reals s.t. $m < M$.*

- *The* most significant coefficients (MSCs) *of x is the finite vector*
$$u_M = \left(k \mid k \in \mathbb{N} \text{ and } u^k \geqslant M \text{ and } k \leq \mid x \mid\right);$$
- *The* least significant coefficients (LSCs) *of x is the finite vector*
$$u_m = \left(k \mid k \in \mathbb{N} \text{ and } u^k \leq m \text{ and } k \leq \mid x \mid\right);$$
- *The* passive coefficients *of x is the finite vector*
$$u_p = \left(k \mid k \in \mathbb{N} \text{ and } u^k \in]m; M[\text{ and } k \leq \mid x \mid\right).$$

For a given host content x, MSCs are then ranks of x that describe the relevant part of the image, whereas LSCs translate its less significant parts.

Example 2: *These two definitions are illustrated on Figure 1, where the significance function (u^k) is defined as in Example 1, $m = 5$, and $M = 6$.*

(a) Original Lena.



(b) MSCs of Lena. (c) LSCs of Lena (×17).

Figure 1. Most and least significant coefficients of Lena.

Using the concept described in this section, it is now possible to expose our new steganographic scheme.

III. THE NEW PROCESS: $\mathcal{DI}_3$

In this section, a new algorithm, which is inspired from the scheme $\mathcal{CIS}_2$ described in [6], is presented. Unlike $\mathcal{CIS}_2$ which require embedding keys with three strategies, only one is required for $\mathcal{DI}_3$. Thus it is easyer to implement for Internet applications, especially in order to guarantee anonymization. Moreover, because in $\mathcal{DI}_3$ there is no operation to mix the message, this new scheme seems to be faster than $\mathcal{CIS}_2$, which is a major advantage to have fast response times on the Internet.

Let us firstly introduce the following notations. $\mathsf{P} \in \mathbb{N}^*$ is the width, in term of bits, of the message to embed into the cover media. $\lambda \in \mathbb{N}^*$ is the number of iterations to realize, which is s.t. $\lambda > \mathsf{P}$. The initial state $x^0 \in \mathbb{B}^\mathsf{N}$ is for the N LSCs of a given cover media C supposed to be uniformly distributed. $m \in \mathbb{B}^\mathsf{P}$ is the message to hide into x^0. Finally, $S \in \mathbb{S}_\mathsf{P}$ is a strategy such that the finite sequence $\left\{S^k, k \in [\![\lambda - \mathsf{P} + 1; \lambda]\!]\right\}$ is injective.

Remark 2: *The width P of the message to hide into the LSCs of the cover media x^0 has to be far smaller than the number of LSCs.* $\square$

The proposed information hiding scheme is defined by an iterative process applied on LSCs of the cover media as follow:

Definition 6 ($\mathcal{DI}_3$ Data hiding scheme): $\forall (n, i) \in \mathbb{N}^* \times [\![0; \mathsf{N}-1]\!]$*:*

$$x_i^n = \begin{cases} x_i^{n-1} & \text{if } S^n \neq i \\ m_{S^n} & \text{if } S^n = i. \end{cases} \qquad \square$$

The stego-content is the Boolean vector $y = x^\lambda \in \mathbb{B}^\mathsf{N}$, which will replace the former LSCs (LSCs of the cover media are replaced by the vector y).

Remark 3: *The implementation of this data hiding scheme is exposed in a complementary work [7].* $\square$

IV. DATA HIDING SECURITY AND ROBUSTNESS

A. Security and robustness

Even if security and robustness are neighboring concepts without clearly established definitions [8], robustness is often considered to be mostly concerned with blind elementary attacks, whereas security is not limited to certain specific attacks. Indeed, security encompasses robustness and intentional attacks [9], [10]. The best attempt to give an elegant and concise definition for each of these two terms was proposed in [9]. Following Kalker, we will consider in this research work the two following definitions:

Definition 7 (Security [9]): *Watermarking security refers to the inability by unauthorized users to have access to the raw watermarking channel [...] to remove, detect and estimate, write or modify the raw watermarking bits.* $\square$

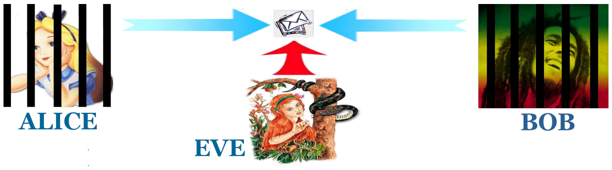


Figure 2. Simmons' prisoner problem [11]

Definition 8 (Robustness [9]): *Robust watermarking is a mechanism to create a communication channel that is multiplexed into original content [...] It is required that, firstly, the perceptual degradation of the marked content [...] is minimal and, secondly, that the capacity of the watermark channel degrades as a smooth function of the degradation of the marked content.* $\square$

In this article, we will focus more specifically on the security aspects, which have been formalized in the Simmons' prisoner problem.

B. The prisoner problem

In the prisoner problem of Simmons [11], Alice and Bob are in jail, and they want to, possibly, devise an escape plan by exchanging hidden messages in innocent-looking cover contents (Fig. 2). These messages are to be conveyed to one another by a common warden, Eve, who over-drops all contents and can choose to interrupt the communication if they appear to be stego-contents.

C. Classification of Attacks

In the steganography framework, in the Simmons' prisoner problem context, attacks have been classified in [12] as follows.

Definition 9 (Classes of attacks):

WOA:	*A* Watermark-Only Attack *occurs when an attacker has only access to several watermarked contents.*
KMA:	*A* Known-Message Attack *occurs when an attacker has access to several pairs of watermarked contents and corresponding hidden messages.*
KOA:	*A* Known-Original Attack *is when an attacker has access to several pairs of watermarked contents and their corresponding original versions.*
CMA:	*A* Constant-Message Attack *occurs when the attacker observes several watermarked contents and only knows that the unknown hidden message is the same in all contents.* $\square$

A synthesis of this classification is given in Table I.

In this article, we will focus more specifically on the "Watermark-Only Attack" situation, which is the most relevant category when considering anonymity and privacy protection through the Internet.

Class	Original content	Stego content	Hidden message
WOA		×	
KMA		×	×
KOA	×	×	
CMA			×

Table I
WATERMARKING ATTACKS CLASSIFICATION IN CONTEXT OF [9]

D. Reminder about Stego-Security

The stego-security, defined in the *Watermark-Only Attack* (WOA) framework, is the highest security level that can be defined in this setup [12].

Definition 10 (Stego-Security): *Let $\mathbb{K}$ be the set of embedding keys, $p(X)$ the probabilistic model of N_0 initial host contents, and $p(Y|K_1)$ the probabilistic model of N_0 watermarked contents. Moreover, each host content has been watermarked with the same secret key K_1 and the same embedding function e. Then e is said* stego-secure *if:*

$$\forall K_1 \in \mathbb{K}, p(Y|K_1) = p(X).$$

Until now, only three schemes have been proven stego-secure. On the one hand, the authors of [12] have established that the spread spectrum technique called Natural Watermarking is stego-secure when its distortion parameter η is equal to 1. On the other hand, we have proposed in [13] and [6] two other data hiding schemes satisfying this security property.

V. SECURITY STUDY

Let us prove that,

Proposition 1: *$\mathcal{DI}_3$ is stego-secure.* □

Proof: Let us suppose that $x^0 \sim \mathbf{U}\left(\mathbb{B}^\mathsf{N}\right), m \sim \mathbf{U}\left(\mathbb{B}^\mathsf{P}\right)$, and $S \sim \mathbf{U}\left(\mathbb{S}_\mathsf{P}\right)$ in a $\mathcal{DI}_3$ setup, where $\mathbf{U}(X)$ describes the uniform distribution on X. We will prove by a mathematical induction that $\forall n \in \mathbb{N}, x^n \sim \mathbf{U}\left(\mathbb{B}^\mathsf{N}\right)$. The base case is obvious according to the uniform repartition hypothesis.

Let us now suppose that the statement $x^n \sim \mathbf{U}\left(\mathbb{B}^\mathsf{N}\right)$ holds for some n ($P\left(x^n = k\right) = \frac{1}{2^N}$).

For a given $k \in \mathbb{B}^N$, we denote by $\tilde{k_i} \in \mathbb{B}^N$ the vector defined by:
$\forall i \in [\![0; \mathsf{N}-1]\!]$, if $k = (k_0, k_1, \dots, k_i, \dots, k_{\mathsf{N}-2}, k_{\mathsf{N}-1})$, then $\tilde{k_i} = \left(k_0, k_1, \dots, \overline{k_i}, \dots, k_{\mathsf{N}-2}, k_{\mathsf{N}-1}\right)$, where $\overline{x}$ is the negation of the bit x.

Let p be defined by: $p = P\left(x^{n+1} = k\right)$. Let E_j and E be the events defined by: $\forall j \in [\![0; \mathsf{P}-1]\!], E_j = (x^n = \tilde{k_j}) \wedge (S^n = j) \wedge (m_{S^n} = k_j)$,$E = (x^n = k) \wedge (m_{S^n} = x_{S^n})$. So, $p = P\left(E \vee \bigvee_{j=0}^{\mathsf{N}-1} E_j\right)$.

On the one hand, $\forall j \in [\![0; \mathsf{P}-1]\!]$, the event E_j is a conjunction of the sub-events $(S^n = j)$ and other sub-events. $\forall j \in [\![0; \mathsf{P}-1]\!]$, all the sub-events $(S^n = j)$ are clearly pairwise disjoints, so all the evente E_j are pairwise disjoints too.

On the other hand, $\forall j \in [\![0; \mathsf{P}-1]\!]$, the events E_j and E are disjoints, because in E_j, a conjunction of the sub-event $(x^n = \tilde{k_j})$ with other sub-events appears, whereas in E a conjunction of the sub-event $(x^n = k)$ with other sub-events appears, and the two sub-events $(x^n = \tilde{k_j})$ and $(x^n = k)$ are clearly disjoints.

As a consequence, using the probability law concerning the reunion of disjoint events we can claim that: $p = P(E) + \sum_{j=0}^{N} P(E_j)$.

Now we evaluate both $P(E)$ and $P(E_j)$.

1) *The case of $P(E)$*: As the two events $(x^n = k)$ and $(m_{S^n} = x_{S^n})$ concern two different sequences, they are clearly independent.
Then, by using the inductive hypothesis: $P(x^n = k) = \frac{1}{2^N}$. So,

$$\begin{array}{rcl} p(E) & = & P(x^n = k) \times P(m_{S^n} = x_{S^n}) \\ & = & \frac{1}{2^\mathsf{N}} \times [P(m_{S^n} = 0)P(x_{S^n} = 0) \\ & & + P(m_{S^n} = 1)P(x_{S^n} = 1)] \\ & = & \frac{1}{2^\mathsf{N}} \times [P(m_{S^n} = 0)P(x_{S^n} = 0) \\ & & +P(m_{S^n} = 1)(1 - P(x_{S^n} = 0))] \\ & = & \frac{1}{2^\mathsf{N}} \times \left[\frac{1}{2}P(x_{S^n} = 0) + \frac{1}{2}(1 - P(x_{S^n} = 0))\right] \\ & = & \frac{1}{2^{\mathsf{N}+1}}. \end{array}$$

2) *Evaluation of $P(E_j)$*: As the three events $(x^n = \tilde{k_j})$, $(S^n = j)$, and $(m_n = k_j)$ deal with three different sequences, they are clearly independent. So

$$\begin{array}{rcl} P(E_j) & = & P(x^n = \tilde{k_j}) \times P(S^n = j) \times P(m_{S^n} = k_j) \\ & = & \frac{1}{2^\mathsf{N}} \times \frac{1}{\mathsf{P}} \times \frac{1}{2} \\ & = & \frac{1}{\mathsf{P}} \times \frac{1}{2^{\mathsf{N}+1}}, \end{array}$$

due to the hypothesis of uniform repartition of S and m.

$$\begin{array}{lrcccc} \text{Consequently,} & p & = & P(E) & + & \sum_{j=0}^{\mathsf{P}} P(E_j) \\ & & = & \frac{1}{2^{\mathsf{N}+1}} & + & \sum_{j=0}^{\mathsf{P}} \left(\frac{1}{\mathsf{P}} \times \frac{1}{2^{\mathsf{N}+1}}\right) \\ & & = & \frac{1}{2^\mathsf{N}}. & & \end{array}$$

Finally, $P\left(x^{n+1} = k\right) = \frac{1}{2^N}$, which leads to $x^{n+1} \sim \mathbf{U}\left(\mathbb{B}^\mathsf{N}\right)$. This result is true $\forall n \in \mathbb{N}$, we thus have proven that the stego-content y is uniformly distributed in the set of possible stego-contents: $y \sim \mathbf{U}\left(\mathbb{B}^\mathsf{N}\right)$ when $x \sim \mathbf{U}\left(\mathbb{B}^\mathsf{N}\right)$. ■

Remark 4 (Distribution of LSCs): *We have supposed that $x^0 \sim \mathbf{U}\left(\mathbb{B}^\mathsf{N}\right)$ to prove the stego-security of the data hiding process $\mathcal{DI}_3$. This hypothesis is the most restrictive one, but it can be obtained at least partially in two possible manners. Either a channel that appears to be random (for instance, when applying a chi squared test) can be found in the media. Or a systematic process can be applied on the images to obtain this uniformity, as follows. Before embedding the hidden message, all the original LSCs must be replaced by randomly generated ones, hoping so that* *such cover media will be considered to be noisy by any given attacker.*

Let us remark that, in the field of data anonymity for privacy on the Internet, we are in the "watermark-only attack" framework. As it has been recalled in Table I, in that framework, the attacker has only access to stego-contents, having so no knowledge of the original media, before introducing the message in the random channel (LSCs). However, this assumption of the existence of a random channel, natural or artificial, into the cover images, is clearly the most disputable one of this research work. The authors' intention is to investigate such hypothesis more largely in future works, by investigation the distribution of several LSCs contained in a large variety of images chosen randomly on the Internet. Among other things, we will check if some well-defined LSCs are naturally uniformly distributed in most cases. To conduct such studies, we intend to use the well-known NIST (National Institute of Standards and Technology of the U.S. Government) tests suite, the DieHARD battery, or the stringent TestU01 [14]. Depending on the results of this search for randomness in natural images, the need to introduce an artificial random channel could be possibly removed. □

Remark 5 (Distribution of the messages m): *In order to prove the stego-security of the data hiding process $\mathcal{DI}_3$, we have supposed that $m \sim \mathbf{U}\left(\mathbb{B}^{\mathsf{P}}\right)$. This hypothesis is not really restrictive. Indeed, to encrypt the message before its embedding into the LSCs of cover media if sufficient to achieve this goal. To say it different, in order to be in the conditions of applications of the process $\mathcal{DI}_3$, the hidden message must be encrypted.* □

Remark 6 (Distribution of the strategies S): *To prove the stego-security of the data hiding process $\mathcal{DI}_3$, we have finally supposed that $S \sim \mathbf{U}\left(\mathbb{S}_{\mathsf{P}}\right)$. This hypothesis is not restrictive too, as any cryptographically secure pseudorandom generator (PRNG) satisfies this property. With such PRNGs, it is impossible in polynomial time, to make the distinction between random numbers and numbers provided by these generators. For instance,* Blum Blum Shub (BBS) *[15],* Blum Goldwasser (BG)*, or* ISAAC*, are convenient here.* □

VI. STEGANALYSIS

The steganographic scheme detailed along these lines has been compared to state of the art steganographic approaches, namely YASS [16], HUGO [17], and nsF5 [18].

The steganalysis is based on the BOSS image database [19] which consists in a set of 10 000 512x512 greyscale images. We randomly selected 50 of them to compute the cover set. Since YASS and nsF5 are dedicated to JPEG support, all these images have been firstly translated into JPEG format thanks to the `mogrify` command line. To allow the comparison between steganographic schemes, the relative payload is always set with 0.1 bit per pixel. Under that constrain, the embedded message m is a sequence of 26214 randomly generated bits. This step has led to distinguish four sets of stego contents, one for each steganographic approach.

Next we use the steganalysis tool developed by the HugoBreakers team [20] based on AI classifier and which won the BOSS competition [19]. Table II summarizes these steganalysis results expressed as the error probabilities of the steganalyser. The errors are the mean of the false alarms and of the missed detections. An error that is closed to 0.5 signifies that deciding whether an image contains a stego content is a random choice for the steganalyser. Conversely, a tiny error denotes that the steganalyser can easily classify stego content and non stego content.

Steganographic Tool	$\mathcal{DI}_3$	YASS	HUGO	NsF5
Error Probability	0.4133	0.0067	0.495	0.47

Table II
STEGANALYSIS RESULTS OF HUGOBREAKERS STEGANALYSER

The best result is obtained by HUGO, which is closed to the perfect steganographic approach to the considered steganalyser, since the error is about 0.5. However, even if the approach detailed along these lines has not any optimization, these first experiments show promising results. We finally notice that the HugoBreakers's steganalyser should outperform these results on larger image databases, *e.g.*, when applied on the whole BOSS image database.

VII. CONCLUSION AND FUTURE WORK

Steganography is a real alternative to guarantee anonymity through the Internet. Unlike the principle of onion routers or Mix-networks, such a protocol using steganography doesn't require any third party potentially corrupted. Only the two parties who want to anonymously communicate are involved in the protocol. Each one holds a secret key for embedding and extraction of the message in the cover media. So to guaranty the anonymity of the communication, only the stealth and the undetectability of the message is required. It is assured by the security of the steganographic process. For instance, the scheme presented in this article offers a secure solution to achieve this goal, thanks to its stego-security. Even if this new scheme $\mathcal{DI}_3$ does not possess topological properties (unlike the $\mathcal{CIS}_2$), its level of security seems to be sufficient for Internet applications. Indeed, we take place into the *Watermark Only Attack (WOA)* framework, where stego-security is the highest level of security. Additionally, this new scheme is faster than $\mathcal{CIS}_2$. This is a major advantage for an utilization through the Internet, to respect response times of web sites. Moreover, for this first version of the process, the steganalysis results are promising.

In future work, various improvements of this scheme are planed to obtain better scores against steganalysers. For instance, LSCs will be embedded into various frequency domains. The robustness of the proposed scheme will be evaluated too [21], to determine whether this information hiding algorithm can be relevant in other Internet domains interesting by data hiding techniques, as the semantic web. Finally a cryptographic approach of information hiding security is currently investigated, enlarging the Simmons' prisoner problem [22], and we intend to evaluate the proposed scheme in this framework.

REFERENCES

[1] www, "Tor: Anonymity online - protect your privacy. defend yourself against network surveillance and traffic analysis." 02 2012, [On line - 2012.02.22]. [Online]. Available: https://www.torproject.org/

[2] Wikipedia, "Hossein derakhshan — wikipedia, the free encyclopedia," 2012, [Online; accessed 1-May-2012]. [Online]. Available: http://en.wikipedia.org/w/index.php?title=Hossein_Derakhshan&oldid=488149891

[3] ——, "Mix network — wikipedia, the free encyclopedia," 2012, [Online; accessed 2-May-2012]. [Online]. Available: http://en.wikipedia.org/w/index.php?title=Mix_network&oldid=478408804

[4] ESIEA, "Perseus technology for anonymity through the internet," 02 2012, [On line - 2012.02.22]. [Online]. Available: http://www.esiea-recherche.eu/perseus.html

[5] C. Guyeux and J. Bahi, "An improved watermarking algorithm for internet applications," in *INTERNET'2010. The 2nd Int. Conf. on Evolving Internet*, Valencia, Spain, Sep. 2010, pp. 119–124. [Online]. Available: http://dx.doi.org/10.1109/INTERNET.2010.29

[6] N. Friot, C. Guyeux, and J. M. Bahi, "Chaotic iterations for steganography - stego-security and chaos-security," in *SECRYPT*, J. Lopez and P. Samarati, Eds. SciTePress, 2011, pp. 218–227.

[7] J. M. Bahi, F. Couchot, N. Friot, and C. Guyeux, "A robust data hiding process contributing to the development of a semantic web," in *INTERNET'2012, The Fourth International Conference on Evolving Internet*, Venice, Italy, Jun. 2012, pp. ***–***, to appear.

[8] L. Perez-Freire, P. Comesanñ, J. R. Troncoso-Pastoriza, and F. Perez-Gonzalez, "Watermarking security: a survey," in *LNCS Transactions on Data Hiding and Multimedia Security*, 2006.

[9] T. Kalker, "Considerations on watermarking security," in *Multimedia Signal Processing, 2001 IEEE Fourth Workshop on*, 2001, pp. 201–206.

[10] P. Comesaña, L. Pérez-Freire, and F. Pérez-González, "Fundamentals of data hiding security and their application to spread-spectrum analysis," in *IH'05: Information Hiding Workshop*, ser. Lecture Notes in Computer Science, M. Barni, J. Herrera-Joancomartí, S. Katzenbeisser, and F. Pérez-González, Eds., vol. 3727. Lectures Notes in Computer Science, Springer-Verlag, 2005, pp. 146–160.

[11] G. J. Simmons, "The prisoners' problem and the subliminal channel," in *Advances in Cryptology, Proc. CRYPTO'83*, 1984, pp. 51–67.

[12] F. Cayre, C. Fontaine, and T. Furon, "Kerckhoffs-based embedding security classes for woa data hiding," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 1–15, 2008.

[13] C. Guyeux, N. Friot, and J. Bahi, "Chaotic iterations versus spread-spectrum: chaos and stego security," in *IIH-MSP'10, 6-th Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing*, Darmstadt, Germany, October 2010, pp. 208–211. [Online]. Available: http://dx.doi.org/10.1109/IIHMSP.2010.59

[14] P. L'ecuyer and R. Simard, "Testu01: A software library in ansi c for empirical testing of random number generators," *Laboratoire de simulation et d'optimisation. Université de Montréal IRO*, 2009.

[15] P. Junod, *Cryptographic secure pseudo-random bits generation: The Blum-Blum-Shub generator*. August, 1999.

[16] K. Solanki, A. Sarkar, and B. S. Manjunath, "Yass: Yet another steganographic scheme that resists blind steganalysis," in *Information Hiding*, ser. Lecture Notes in Computer Science, T. Furon, F. Cayre, G. J. Doërr, and P. Bas, Eds., vol. 4567. Springer, 2007, pp. 16–31.

[17] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Information Hiding*, ser. Lecture Notes in Computer Science, R. Böhme, P. W. L. Fong, and R. Safavi-Naini, Eds., vol. 6387. Springer, 2010, pp. 161–177.

[18] J. J. Fridrich, T. Pevný, and J. Kodovský, "Statistically undetectable jpeg steganography: dead ends challenges, and opportunities," in *MM&Sec*, D. Kundur, B. Prabhakaran, J. Dittmann, and J. J. Fridrich, Eds. ACM, 2007, pp. 3–14.

[19] P. Bas, T. Filler, and T. Pevný, "Break our steganographic system — the ins and outs of organizing boss," in *Information Hiding, 13th International Workshop*, ser. Lecture Notes in Computer Science, T. Filler, Ed. Prague, Czech Republic: Springer-Verlag, New York, May 18–20, 2011.

[20] J. Kodovský, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," *IEEE Transactions on Information Forensics and Security*, vol. PP Issue:99, pp. 1 – 1, 2011, to appear.

[21] J. Bahi, J.-F. Couchot, and C. Guyeux, "Steganography: a class of secure and robust algorithms," *The Computer Journal*, pp. ***–***, 2011, available online. Paper version to appear. [Online]. Available: http://dx.doi.org/10.1093/comjnl/bxr116

[22] J. M. Bahi, C. Guyeux, and P.-C. Héam, "A complexity approach for steganalysis," *CoRR*, vol. abs/1112.5245, 2011.