On the interest and realization of chaos-based information hiding schemes: a review

Christophe Guyeux, Jean-François Couchot, and Jacques M. Bahi
{christophe.guyeux,jean-francois.couchot,jacques.bahi}@univ-fcomte.fr
Institut Femto-st, Université de Franche-Comté, France

October 27, 2013

Abstract

Information hiding schemes are studied Spread-spectrum data-hiding techniques have been widely studied in recent years under the scope of security. These techniques encompass several schemes, such as Improved Spread Spectrum (ISS), Circular Watermarking (CW), and Natural Watermarking (NW). Some of these schemes have revealed various security issues. On the contrary, it has been proven in [14] that the Natural Watermarking technique is stego-secure. This stego-security is one of the security classes defined in [14], where probabilistic models are used to categorize the security of data hiding algorithms in the Watermark Only Attack (WOA) framework.

We have explained in our previous research works [9] that any algorithm can be rewritten as an iterative process, leading to the possibility to study its topological behavior. As a concrete example, we have shown that the security level of some information hiding algorithms (of the spread-spectrum kind) can be studied into a novel framework based on unpredictability, as it is understood in the mathematical theory of chaos [9]. The key idea motivating our research works is that: *if artificial intelligence (AI) tools seem to have difficulties to deal with chaos, then steganalyzers (software based on AI that try to separate original from stego-contents) may be proven defective against chaotic information hiding schemes*. Our work has thus constituted in showing theoretically that such chaotic schemes can be constructed. We are not looking to struggle with best available information hiding techniques and we do not focus on effective and operational aspects, as our questioning are more locating in a conceptual domain. Among other things, we do not specify how to chose embedding coefficients, but the way to insert the hidden message in a selection of these "least significant coefficient" in an unpredictable manner. To say this another way, our intention is not to realize an hidden channel that does not appear as sleazy to a steganalyzer, but to construct an information hiding scheme whose behavior cannot be predicted: supposing that the adversary has anything (algorithm, possible embedding coefficient, etc.) but the secret key, we want to determine if he can predict

which coefficients will be finally used, and in which order. To do so, a new class of security has been introduced in [7], namely the topological security. This new class can be used to study some categories of attacks that are difficult to investigate in the existing security approach. It also enriches the variety of qualitative and quantitative tools that evaluate how strong the security is, thus reinforcing the confidence that can be added in a given scheme.

In addition of being stego-secure, we have proven in [23] that Natural Watermarking (NW) technique is topologically secure. Moreover, this technique possesses additional properties of unpredictability, namely, strong transitivity, topological mixing, and a constant of sensitivity equal to $\frac{N}{2}$ [22]. However NW are not expansive, which is in our opinion problematic in the Constant-Message Attack (CMA) and Known Message Attack (KMA) setups, when we consider that the attacker has all but the embedding key [22]. Since these initial investigations, our research works in that information hiding field have thus consisted in searching more secure schemes than NW, regarding the concerns presented in the first paragraph of this introduction. The objective of this review paper is to list the results obtained by following such an approach.

This article is organized as follows. Notations and terminologies are firstly recalled in the next section. Then the formerly published $\mathcal{CIW}_1$ chaotic iteration based one-bit watermarking process is recalled in detail in Section 3. Its steganographic version $\mathcal{CIS}_2$ is then explained in Section 4, while Section 5 presents the $\mathcal{DI}_3$ process, whose aims is to merge the two previous approaches. This review article of chaotic iterations based information hiding algorithms ends by a conclusion section containing intended future works.

1 Introduction

Information hiding has recently become a major digital technology [27, 42], especially with the increasing importance and widespread distribution of digital media through the Internet. Spread-spectrum data-hiding techniques have been widely studied in recent years under the scope of security. These techniques encompass several schemes, such as Improved Spread Spectrum (ISS), Circular Watermarking (CW), and Natural Watermarking (NW). Some of these schemes have revealed various security issues. On the contrary, it has been proven in [14] that the Natural Watermarking technique is stego-secure. This stego-security is one of the security classes defined in [14], where probabilistic models are used to categorize the security of data hiding algorithms in the Watermark Only Attack (WOA) framework.

We have explained in our previous research works [9] that any algorithm can be rewritten as an iterative process, leading to the possibility to study its topological behavior. As a concrete example, we have shown that the security level of some information hiding algorithms (of the spread-spectrum kind) can be studied into a novel framework based on unpredictability, as it is understood in the mathematical theory of chaos [9]. The key idea motivating our research

works is that: *if artificial intelligence (AI) tools seem to have difficulties to deal with chaos, then steganalyzers (software based on AI that try to separate original from stego-contents) may be proven defective against chaotic information hiding schemes*. Our work has thus constituted in showing theoretically that such chaotic schemes can be constructed. We are not looking to struggle with best available information hiding techniques and we do not focus on effective and operational aspects, as our questioning are more locating in a conceptual domain. Among other things, we do not specify how to chose embedding coefficients, but the way to insert the hidden message in a selection of these "least significant coefficient" in an unpredictable manner. To say this another way, our intention is not to realize an hidden channel that does not appear as sleazy to a steganalyzer, but to construct an information hiding scheme whose behavior cannot be predicted: supposing that the adversary has anything (algorithm, possible embedding coefficient, etc.) but the secret key, we want to determine if he can predict which coefficients will be finally used, and in which order. To do so, a new class of security has been introduced in [7], namely the topological security. This new class can be used to study some categories of attacks that are difficult to investigate in the existing security approach. It also enriches the variety of qualitative and quantitative tools that evaluate how strong the security is, thus reinforcing the confidence that can be added in a given scheme.

In addition of being stego-secure, we have proven in [23] that Natural Watermarking (NW) technique is topologically secure. Moreover, this technique possesses additional properties of unpredictability, namely, strong transitivity, topological mixing, and a constant of sensitivity equal to $\frac{N}{2}$ [22]. However NW are not expansive, which is in our opinion problematic in the Constant-Message Attack (CMA) and Known Message Attack (KMA) setups, when we consider that the attacker has all but the embedding key [22]. Since these initial investigations, our research works in that information hiding field have thus consisted in searching more secure schemes than NW, regarding the concerns presented in the first paragraph of this introduction. The objective of this review paper is to list the results obtained by following such an approach.

This article is organized as follows. Notations and terminologies are firstly recalled in the next section. Then the formerly published $\mathcal{CIW}_1$ chaotic iteration based one-bit watermarking process is recalled in detail in Section 3. Its steganographic version $\mathcal{CIS}_2$ is then explained in Section 4, while Section 5 presents the $\mathcal{DI}_3$ process, whose aims is to merge the two previous approaches. This review article of chaotic iterations based information hiding algorithms ends by a conclusion section containing intended future works.

2 Notations and Terminologies

In what follows, $\mathbb{B}$ denotes the Boolean set $\{0, 1\}$, S^n stands for the n^{th} term of a sequence S, V_i is for the i^{th} component of a vector V, and $[\![0; N]\!]$ is the integer interval $\{0, 1, \ldots, N\}$.

Compléter éventuellement les notations.

2.1 The mathematical theory of chaos

From a mathematical point of view, deterministic chaos has been thoroughly studied these last decades, with different research works that have provided various definitions of chaos. Among these definitions, the one given by Devaney [16] is perhaps one of the most established ones.

Consider a topological space $(\mathcal{X}, \tau)$ and a continuous function f on $\mathcal{X}$. Topological transitivity occurs when, for any point, any neighborhood of its future evolution eventually overlap with any other given region. More precisely,

Definition 1 *f is said to be* topologically transitive *if, for any pair of open sets $U, V \subset \mathcal{X}$, there exists $k > 0$ such that $f^k(U) \cap V \neq \emptyset$.*

This property implies that a dynamical system cannot be broken into simpler subsystems. It is intrinsically complicated and cannot be simplified. Besides, a dense set of periodic points is an element of regularity that a chaotic dynamical system has to exhibit.

Definition 2 *An element (a point) x is a* periodic element *(point) for f of period $n \in \mathbb{N}^*$, if $f^n(x) = x$.*

Definition 3 *f is said to be* regular *on $(\mathcal{X}, \tau)$ if the set of periodic points for f is dense in $\mathcal{X}$: for any point x in $\mathcal{X}$, any neighborhood of x contains at least one periodic point.*

This regularity "counteracts" the effects of transitivity. Thus, due to these two properties, two points close to each other can behave in a completely different manner, leading to unpredictability for the whole system. Then,

Definition 4 (Devaney's chaos) *f is said to be* chaotic *on $(\mathcal{X}, \tau)$ if f is regular and topologically transitive.*

The chaos property is related to the notion of "sensitivity", defined on a metric space $(\mathcal{X}, d)$ by:

Definition 5 *f has* sensitive dependence on initial conditions *if there exists $\delta > 0$ such that, for any $x \in \mathcal{X}$ and any neighborhood V of x, there exist $y \in V$ and $n \geq 0$ such that $d\left(f^n(x), f^n(y)\right) > \delta$.*

δ is called the constant of sensitivity *of f.*

Indeed, Banks *et al.* have proven in [11] that when f is chaotic and $(\mathcal{X}, d)$ is a metric space, then f has the property of sensitive dependence on initial conditions (this property was formerly an element of the definition of chaos).

2.2 Chaotic iterations and watermarking scheme

Let us consider a *system* with a finite number $\mathsf{N} \in \mathbb{N}^*$ of *cells*, so that each cell has a Boolean *state*. A sequence which elements belong into $[\![1; \mathsf{N}]\!]$ is a *strategy*. Finally, the set of all strategies is denoted by $[\![1, \mathsf{N}]\!]^{\mathbb{N}}$.

Definition 6 *The set* $\mathbb{B}$ *denoting* $\{0,1\}$*, let* $f : \mathbb{B}^{\mathsf{N}} \longrightarrow \mathbb{B}^{\mathsf{N}}$ *be a function and* $S \in [\![1, \mathsf{N}]\!]^{\mathbb{N}}$*. The* chaotic iterations *(CIs) are defined by* $x^0 \in \mathbb{B}^{\mathsf{N}}$ *and*

$$\forall n \in \mathbb{N}^*, \forall i \in [\![1; \mathsf{N}]\!], x_i^n = \begin{cases} x_i^{n-1} & \text{if } S^n \neq i \\ \left(f(x^{n-1})\right)_{S^n} & \text{if } S^n = i. \end{cases}$$

In other words, at the n^{th} iteration, only the S^n-th cell is "iterated". Let us now recall how to define a suitable metric space where chaotic iterations are continuous [10].

Let δ be the *discrete Boolean metric*, $\delta(x, y) = 0 \Leftrightarrow x = y$. Given a function f, define the function:

$$\begin{array}{rl} F_f : & [\![1; \mathsf{N}]\!] \times \mathbb{B}^{\mathsf{N}} \longrightarrow \mathbb{B}^{\mathsf{N}} \\ & (k, E) \longmapsto \left(E_j.\delta(k, j) + f(E)_k.\overline{\delta(k, j)}\right)_{j \in [\![1;\mathsf{N}]\!]} \end{array}$$

Consider the phase space $\mathcal{X} = [\![1; \mathsf{N}]\!]^{\mathbb{N}} \times \mathbb{B}^{\mathsf{N}}$, and the map defined on $\mathcal{X}$ by:

$$G_f\left(S, E\right) = \left(\sigma(S), F_f(i(S), E)\right), \tag{1}$$

where $\sigma : (S^n)_{n\in\mathbb{N}} \in [\![1, \mathsf{N}]\!]^{\mathbb{N}} \longrightarrow (S^{n+1})_{n\in\mathbb{N}}$ and $i : (S^n)_{n\in\mathbb{N}} \in [\![1, \mathsf{N}]\!]^{\mathbb{N}} \longrightarrow S^0$. Then chaotic iterations can be described by the following discrete dynamical system:

$$\begin{cases} X^0 \in \mathcal{X} \\ X^{k+1} = G_f(X^k). \end{cases} \tag{2}$$

To study whether this dynamical system is chaotic [16], a distance between $X = (S, E), Y = (\check{S}, \check{E}) \in \mathcal{X}$ has been introduced in [10] as follows: $d(X, Y) = d_e(E, \check{E}) + d_s(S, \check{S})$, where

- $d_e(E, \check{E}) = \sum_{k=1}^{\mathsf{N}} \delta(E_k, \check{E}_k)$,
- $d_s(S, \check{S}) = \frac{9}{\mathsf{N}} \sum_{k=1}^{\infty} \frac{|S_k - \check{S}_k|}{10^k}$.

This distance has been introduced to satisfy the following requirements. If the floor value $\lfloor d(X, Y) \rfloor$ is equal to n, then the systems $E, \check{E}$ differ in n cells. In addition, its floating part is less than 10^{-k} if and only if the first k terms of the two strategies are equal. Moreover, if the k^{th} digit is nonzero, then the k^{th} terms of the two strategies are different. With this metric, it has been proven that [10],

Theorem 1 G_{f_0} *is continuous and chaotic in* $(\mathcal{X}, d)$*.*

3 The $\mathcal{CIW}_1$ Chaotic Iteration based Watermarking Process

3.1 Using chaotic iterations as information hiding schemes

3.1.1 Presentation of the dhCI process

We have proposed in [4, 23] a data hiding protocol based on chaotic iterations. The process, referred as dhCI, consisted in iterating $\mathcal{G}_{f_0}$ on least significant coefficients of a cover medium. Each property exhibited by the dynamical system will then be possessed too by the watermarking scheme.

The same original image was supposed to be shared by the sender and the receiver, the sender either iterates or not CIs on these coefficients, depending on whether the binary information to transfer was 0 or 1, while the receiver computed the differences between its stored image and the received one. For further explanations, see [4, 23].

The first deepened study of such a dhCI algorithm was published in [8]. The aims were to prove that a particular instance of the dhCI algorithm, called the $\mathcal{CIW}_1$ process, is stego-secure and topologically secure, to study its qualitative and quantitative properties of unpredictability, and then to compare it with Natural Watermarking: the topological study has been realized in [22] while the stego-security has been proven later in [23]). To be able to recall the $\mathcal{CIW}_1$ scheme, we must firstly define the significance of a given coefficient.

3.1.2 Most and least significant coefficients

We first notice that terms of the original content x that may be replaced by terms taken 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 7 *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 8 *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*

$$u_M = \left(k \;\middle|\; k \in \mathbb{N} \text{ and } u^k \geqslant M \text{ and } k \leq \mid x \mid\right);$$

- *The* least significant coefficients (LSCs) *of x is the finite vector*

$$u_m = \left(k \;\middle|\; k \in \mathbb{N} \text{ and } u^k \leq m \text{ and } k \leq \mid x \mid\right);$$

- *The* passive coefficients *of x is the finite vector*

$$u_p = \left(k \;\middle|\; k \in \mathbb{N} \text{ and } u^k \in]m; M[\text{ and } k \leq \mid x \mid\right).$$

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. 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) Lena. (b) MSCs of Lena. (c) LSCs of Lena ($\times 17$).

Figure 1: Most and least significant coefficients of Lena.

3.1.3 Presentation of the $\mathcal{CIW}_1$ dhCI scheme

We have proposed in SECRYPT10 [8] to study a particular instance of the dhCI class, which considers the negation function as iteration mode. The resulting chaotic iterations watermarking[1] process has been denoted by $\mathcal{CIW}_1$ in this publication. It operates as follows. Let:

- $(K, N) \in [0; 1] \times \mathbb{N}$ be an embedding key,
- $X \in \mathbb{B}^{\mathsf{N}}$ be the N least significant coefficients (LSCs) of a given cover media C,
- $(S^n)_{n\in\mathbb{N}} \in [\![1, \mathsf{N}]\!]^{\mathbb{N}}$ be a strategy, which depends on the message to hide $M \in [0; 1]$ and K,
- $f_0 : \mathbb{B}^{\mathsf{N}} \to \mathbb{B}^{\mathsf{N}}$ be the vectorial logical negation.

So the watermarked media is C whose LSCs are replaced by $Y_K = X^N$, where:

[1] Watermarking means here that only a binary information, like the presence of a copyright, can be extracted.

(a) Original Lena.

(b) Watermark.

(c) Watermarked Lena.

Figure 2: Data hiding with chaotic iterations

$$\begin{cases} X^0 = X \\ \forall n < N, X^{n+1} = G_{f_0}\left(X^n\right). \end{cases}$$

In the following section, two ways to generate $(S^n)_{n\in\mathbb{N}}$ are given, namely Chaotic Iterations with Independent Strategy (CIIS) and Chaotic Iterations with Dependent Strategy (CIDS). In CIIS, the strategy is independent from the cover media X, whereas in CIDS the strategy will be dependent on X. These strategies have been introduced in [23]. Their stego-security are studied in Section 3.2 and their topological security in Section 3.3.2.

3.1.4 Examples of strategies

CIIS strategy Let us first introduce the Piecewise Linear Chaotic Map (PLCM, see [37]), defined by:

Definition 9 (PLCM)

$$F(x,p) = \begin{cases} x/p & \text{if} \quad x \in [0;p] \\ (x-p)/(\frac{1}{2}-p) & \text{if} \quad x \in \left[p;\frac{1}{2}\right] \\ F(1-x,p) & \text{else.} \end{cases}$$

where $p \in \left]0;\frac{1}{2}\right[$ is a "control parameter". Contrary to well-known chaotic maps like the logistic map, this PLCM is unbiased and does not present obvious security flaws [37].

We define the general term of the strategy $(S^n)_n$ in CIIS setup by the following expression: $S^n = \lfloor \mathsf{N} \times K^n \rfloor + 1$, where:

$$\begin{cases} p \in \left[0;\frac{1}{2}\right] \\ K^0 = M \otimes K \\ K^{n+1} = F(K^n,p), \forall n \leq N_0 \end{cases}$$

in which $\otimes$ denotes the bitwise exclusive or (XOR) between two floating part numbers (*i.e.*, between their binary digits representation). Lastly, to be certain to enter into the chaotic regime of PLCM [37], the strategy can be preferably defined by: $S^n = \left\lfloor \mathsf{N} \times K^{n+D} \right\rfloor + 1$, where $D \in \mathbb{N}$ is large enough.

CIDS strategy The same notations as above are used. We define CIDS strategy as in [23]: $\forall k \leqslant N$,

- if $k \leqslant \mathsf{N}$ and $X^k = 1$, then $S^k = k$,
- else $S^k = 1$.

In this situation, if $N \geqslant \mathsf{N}$, then only two watermarked contents are possible with the scheme proposed in Section 3.1, namely: $Y_K = (0, 0, \cdots, 0)$ and $Y_K = (1, 0, \cdots, 0)$.

Before being able to present the security study we performed on it, we must firstly recall the notion of security usually considered in information hiding and its difference with robustness.

3.2 Security versus robustness

3.2.1 Presentation

Even if security and robustness are neighboring concepts without clearly established definitions [31], 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 [15, 26]. The best attempt to give an elegant and concise definition for each of these two terms was proposed in [26]. Following Kalker, we will consider in this article the two following definitions:

Definition 10 (Security [26]) *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.*

Definition 11 (Robustness [26]) *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.*

3.2.2 Classification of attacks

In the security framework, attacks have been classified in [14] as follows.

Definition 12 *Watermark-Only Attack (WOA) occurs when an attacker has only access to several watermarked contents.*

Definition 13 *Known-Message Attack (KMA) occurs when an attacker has access to several pairs of watermarked contents and corresponding hidden messages.*

Definition 14 *Known-Original Attack (KOA) is when an attacker has access to several pairs of watermarked contents and their corresponding original versions.*

Definition 15 *Constant-Message Attack (CMA) occurs when the attacker observes several watermarked contents and only knows that the unknown hidden message is the same in all contents.*

A synthesis of this classification is given in Table 1.

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

Table 1: Watermarking attacks classification in context of [26]

3.2.3 Definition of stego-security

In the Simmons' prisoner problem [38], Alice and Bob are in jail and they want to, possibly, devise an escape plan by exchanging hidden messages in innocent-looking cover contents. These messages are to be conveyed to one another by a common warden named Eve, who eavesdrops all contents and can choose to interrupt the communication if they appear to be stego-contents.

Stego-security, defined in this well-known context, is the highest security class in Watermark-Only Attack setup, which occurs when Eve has only access to several marked contents [14].

Let $\mathbb{K}$ be the set of embedding keys, $p(X)$ the probabilistic model of N_0 initial host contents, and $p(Y|K)$ the probabilistic model of N_0 marked contents such that each host content has been marked with the same key K and the same embedding function.

Definition 16 (Stego-Security [14]) *The embedding function is* stego-secure *if* $\forall K \in \mathbb{K}, p(Y|K) = p(X)$ *is established.*

Stego-security states that the knowledge of K does not help to make the difference between $p(X)$ and $p(Y)$. This definition implies the following property:

$$p(Y|K_1) = \cdots = p(Y|K_{N_k}) = p(Y) = p(X)$$

This property is equivalent to a zero Kullback-Leibler divergence, which is the accepted definition of the "perfect secrecy" in steganography [13].

3.3 Security evaluation

3.3.1 Evaluation of the stego-security

We have proven in [23] the following proposition.

Proposition 1 *CIIS is stego-secure, while CIDS does not satisfy this security property.*

3.3.2 Evaluation of the topological security

To check whether an information hiding scheme S is topologically secure or not, we have proposed in [23], to write S as an iterate process $x^{n+1} = f(x^n)$ on a metric space $(\mathcal{X}, d)$. As recalled previously, this formulation is always possible. So,

Definition 17 *An information hiding scheme S is said to be topologically secure on $(\mathcal{X}, d)$ if its iterative process has a chaotic behavior according to Devaney.*

Due to the chaos properties of the so-called chaotic iterations, we have then deduced in [23] that,

Proposition 2 *CIIS and CIDS are topologically secure.*

We have then deduced qualitative and quantitative properties of topological security for this information hiding scheme in [23]: it is expansive (with a constant of expansiveness equal to 1), topologically mixing, etc. These properties can measure the disorder generated by our scheme, giving by doing so an important information about the unpredictability level of such a process, which helps to compare it to other data hiding methods. Such a comparison is outlined in the next section [23].

3.4 Comparison between spread-spectrum and chaotic iterations

The consequences of topological mixing for data hiding are multiple. Firstly, security can be largely improved by considering the number of iterations as a secret key. An attacker will reach all of the possible media when iterating without this key. Additionally, he cannot benefit from a KOA setup, by studying media in the neighborhood of the original cover. Moreover, as in a topological mixing situation, it is possible that any hidden message (the initial condition), is sent to the same fixed watermarked content (with different numbers of iterations), the interest to be in a KMA setup is drastically reduced. Lastly, as all of the watermarked contents are possible for a given hidden message, depending on the number of iterations, CMA attacks will fail.

The property of expansiveness reinforces drastically the sensitivity in the aims of reducing the benefits that Eve can obtain from an attack in KMA

or KOA setup. For example, it is impossible to have an estimation of the watermark by moving the message (or the cover) as a cursor in situation of expansiveness: this cursor will be too much sensitive and the changes will be too important to be useful. On the contrary, a very large constant of expansiveness ε is unsuitable: the cover media will be strongly altered whereas the watermark would be undetectable. Finally, spread-spectrum is relevant when a discrete and secure data hiding technique is required in WOA setup. However, this technique should not be used in KOA and KMA setup, due to its lack of expansiveness.

3.5 Lyapunov exponent evaluation

The Lyapunov exponent of the $\mathcal{CIW}_1$ algorithm has been computed in [5], to improve our knowledge of its topological security. It is equal to $\ln \mathsf{N}$, where N stands for the number of LSCs chosen in the implementation of the algorithm.

To evaluate this Lyapunov exponent, chaotic iterations must be described by a differentiable function on $\mathbb{R}$. To do so, a topological semiconjugacy between the phase space $\mathcal{X}$ and $\mathbb{R}$ has been written. As this proof is simply a rewriting in the digital watermarking field of an unpublished result on chaotic iterations obtained in [22], and as Section 4.7 provides a Lyapunov exponent evaluation for a completely different algorithm, we will not say any more about this publication.

4 The $\mathcal{CIS}_2$ Chaotic Iteration based Steganographic Process

After the introduction of $\mathcal{CIW}_1$ in [23], there were only two information hiding schemes being both stego-secure and topologically secure. The first one is based on a spread spectrum technique called Natural Watermarking. It is stego-secure when its parameter η is equal to 1 [14]. Unfortunately, this scheme is neither robust, nor able to face an attacker in KOA and KMA setups, due to its lack of expansiveness [21]. The second scheme both topologically secure and stego-secure has been presented in the previous section. However, this $\mathcal{CIW}_1$ process allows to embed securely only one bit per embedding parameters. The objective of [20] was to improve the scheme studied in [23], in such a way that more than one bit can be embedded. Such a study led to the definition of the $\mathcal{CIS}_2$ scheme presented here.

4.1 The improved algorithm

Let us firstly recall the notations and terminologies introduced in [20].

Definition 18 *Let* $\mathsf{k} \in \mathbb{N}^*$. *A* strategy adapter *is a sequence which elements belong into* $[\![0, \mathsf{k}-1]\!]$. *The set of all strategies with terms in* $[\![0, \mathsf{k}-1]\!]$ *is denoted by* $\mathbb{S}_\mathsf{k}$.

Intuitively, a strategy-adapter aims at generating a strategy $(S^t)^{t\in\mathbb{N}}$ where each term S^t belongs to $[\![1,n]\!]$.

Definition 19 *Let $k \in \mathbb{N}^*$. The* initial function *is the map i_k defined by:*

$$\begin{array}{rccc} i_k: & \mathbb{S}_k & \longrightarrow & [\![0,\mathsf{k}-1]\!] \\ & (S^n)_{n\in\mathbb{N}} & \longmapsto & S^0 \end{array}$$

Definition 20 *Let $k \in \mathbb{N}^*$. The* shift function *is the map σ_k defined by:*

$$\begin{array}{rccc} \sigma_k: & \mathbb{S}_k & \longrightarrow & \mathbb{S}_k \\ & (S^n)_{n\in\mathbb{N}} & \longmapsto & (S^{n+1})_{n\in\mathbb{N}} \end{array}$$

Let us additionally recall the following notations.

- $x^0 \in \mathbb{B}^{\mathsf{N}}$ the N least significant coefficients of a given cover media C.
- $m^0 \in \mathbb{B}^{\mathsf{P}}$ is the watermark to embed into x^0.
- $S_1 \in \mathbb{S}_N$ is a strategy called **place strategy**, giving the location (LCS) where to insert the message at each iteration.
- $S_2 \in \mathbb{S}_P$ is a strategy called **choice strategy**, providing which bits from the message must be inserted at the given iteration.
- Lastly, $S_3 \in \mathbb{S}_P$ is a strategy called **mixing strategy**, as it is required for chaos to mix the message at each iteration.

The information hiding scheme published in [20] was formerly called Steganography by Chaotic Iterations and Substitution with Mixing Message (SCISMM in short), and has been renamed $\mathcal{CIS}_2$ in later publications. It is defined by $\forall (n,i,j) \in \mathbb{N}^* \times [\![0;\mathsf{N}-1]\!] \times [\![0;\mathsf{P}-1]\!]$:

$$\begin{cases} x_i^n = \begin{cases} x_i^{n-1} & \text{if } S_1^n \neq i \\ m_{S_2^n} & \text{if } S_1^n = i. \end{cases} \\ \\ m_j^n = \begin{cases} m_j^{n-1} & \text{if } S_3^n \neq j \\ \overline{m_j^{n-1}} & \text{if } S_3^n = j. \end{cases} \end{cases}$$

The stego-content is the Boolean vector $y = x^P \in \mathbb{B}^{\mathsf{N}}$.

4.2 Security study of the $\mathcal{CIS}_2$

After having introduced the $\mathcal{CIS}_2$, we have studied its security in [20].

4.2.1 Stego-security

We have proven in [20] that,

Proposition 3 *$\mathcal{CIS}_2$ is stego-secure.*

Proof 1 *See [20].*

4.2.2 Topological security

Topological model We have firstly proven in [20] that $\mathcal{CIS}_2$ can be modeled as a dynamical system in a topological space, as follows. Let

$$\begin{array}{rl} F: & [\![0;\mathsf{N}-1]\!] \times \mathbb{B}^{\mathsf{N}} \times [\![0;\mathsf{P}-1]\!] \times \mathbb{B}^{\mathsf{P}} \longrightarrow \mathbb{B}^{\mathsf{N}} \\ & (k,x,\lambda,m) \longmapsto \left(\delta(k,j).x_j + \overline{\delta(k,j)}.m_\lambda\right)_{j\in[\![0;\mathsf{N}-1]\!]} \end{array}$$

where + and . are the boolean addition and product operations.

Consider the phase space $\mathcal{X}_2$ defined as follow:

$$\mathcal{X}_2 = \mathbb{S}_N \times \mathbb{B}^{\mathsf{N}} \times \mathbb{S}_P \times \mathbb{B}^{\mathsf{P}} \times \mathbb{S}_P,$$

where $\mathbb{S}_N$ and $\mathbb{S}_P$ are the sets introduced in Section 4.1.

We define the map $\mathcal{G}_{f_0} : \mathcal{X}_2 \longrightarrow \mathcal{X}_2$ by:

$$\mathcal{G}_{f_0}\left(S_1, x, S_2, m, S_3\right) =$$
$$\left(\sigma_N(S_1), F(i_N(S_1), x, i_P(S_2), m), \sigma_P(S_2), G_{f_0}(m, S_3), \sigma_P(S_3)\right)$$

$\mathcal{CIS}_2$ can be described by the iterations of the following discrete dynamical system:

$$\left\{ \begin{array}{l} X^0 \in \mathcal{X}_2 \\ X^{k+1} = \mathcal{G}_{f_0}(X^k). \end{array} \right.$$

Then, by comparing $\mathcal{X}_2$ and the phase space $\mathcal{X}$ formerly introduced in this document, we have verified in [20] that.

Proposition 4 *The phase space $\mathcal{X}_2$ has, at least, the cardinality of the continuum.*

A new distance on $\mathcal{X}_2$ We have defined in [20] a new distance on $\mathcal{X}_2$ as follows: $\forall X, \check{X} \in \mathcal{X}_2$, if $X = (S_1, x, S_2, m, S_3)$ and $\check{X} = (\check{S_1}, \check{x}, \check{S_2}, \check{m}, \check{S_3})$, then:

$$\begin{array}{rcl} d_2(X,\check{X}) & = & d_{\mathbb{B}^{\mathsf{N}}}(x,\check{x}) + d_{\mathbb{B}^{\mathsf{P}}}(m,\check{m}) \\ & + & d_{\mathbb{S}_N}(S_1,\check{S_1}) + d_{\mathbb{S}_P}(S_2,\check{S_2}) + d_{\mathbb{S}_P}(S_3,\check{S_3}). \end{array}$$

Continuity of $\mathcal{CIS}_2$ To prove that $\mathcal{CIS}_2$ is another example of topological chaos in the sense of Devaney, $\mathcal{G}_{f_0}$ must be continuous on the metric space $(\mathcal{X}_2, d_2)$. We thus have proven in [20] that,

Proposition 5 *$\mathcal{G}_{f_0}$ is a continuous function on $(\mathcal{X}_2, d_2)$.*

$\mathcal{CIS}_2$ is chaotic Then, in [20], $(\mathcal{X}_2, \mathcal{G}_{f_0})$ has been proven to be topologically transitive, regular, and sensitive dependence on initial conditions. We thus have the result [20]:

Theorem 2 *$\mathcal{G}_{f_0}$ is a chaotic map on $(\mathcal{X}_2, d_2)$ in the sense of Devaney.*

So we can claim that $\mathcal{CIS}_2$ is topologically secure.

4.3 Correctness and completeness studies

Without attack, the $\mathcal{CIS}_2$ scheme has to ensure that the user can always extract a message and that this latter is the watermark, provided the user has the correct keys. These two demands correspond respectively to the study of completeness and of correctness for the proposed approach, which have been investigated in [3]. We have firstly established that,

Proposition 6 *Let $\Im(S_p)$ be the set (without repetitions) $\{S_p^1, S_p^2, \ldots, S_p^l\}$ of cardinality k, $k \leq l$. This set contains all the elements of x that have been modified along the $\mathcal{CIS}_2$ iteration process. Let us consider $\Im(S_c)_{|D}$ defined by $\{S_c^{d_1}, S_c^{d_2}, \ldots, S_c^{d_k}\}$ where d_i is the last iteration that has modified the element $i \in \Im(S_p)$.*

Message can be extracted from the stego-content if and only if $\Im(S_c)_{|D} = [\![0; \mathsf{P}-1]\!]$.

Under this condition, one bit of index j of the original message m^0 is thus embedded at least twice in x^l. By counting the number of times this bit has been switched in S_m, the value of m_j can be deduced in many places. Without attack, all these values are equal and the message is immediately obtained. After an attack, the value of m_j is obtained as mean value of all its occurrences. The scheme is thus complete. Notice that if the cover is not attacked, the returned message is always equal to the original due to the definition of the mean function.

4.4 Deciding whether a possibly attacked media is watermarked

Let us consider a first media y that is watermarked with a message m and a second one, namely y', which is an altered version of y, *i.e.*, where some bits have been modified. Let m' be the message that is extracted from y'.

We have checked in [3] how far the extracted message m' is from m. To achieve this, we have considered the set $M = \{i | m_i = 1\}$ of the Boolean vector message m and similarly the set M' for the message m'. Most of similarity measures depend on the functions a, b, c, and d, all from $\mathbb{B}^{\mathsf{P}} \times \mathbb{B}^{\mathsf{P}}$ to $\mathbb{N}$, and respectively equal to $a(m, m') = |M \cap M'|$, $b(m, m') = |M \setminus M'|$, $c(m, m') = |M' \setminus M|$, and $d(m, m') = |\overline{M} \cap \overline{M'}|$ ($|S|$ and $\overline{S}$ respectively denote the cardinality and the complementary of any set S). In what follows a, b, c, and d respectively stand for $a(m, m')$, $b(m, m')$, $c(m, m')$, and $d(m, m')$.

According to [35] the Fermi-Dirac measure S_{FD} is the one that has the highest discrimination power, *i.e.*, which allows a clear separation between correlated vectors and uncorrelated ones. The measure is recalled hereafter with respect to the previously defined scalars a, b, and c.

$$S_{FD}(\varphi) = \frac{F_{FD}(\varphi) - F_{FD}(\frac{\pi}{2})}{F_{FD}(0) - F_{FD}(\frac{\pi}{2})},$$
$$F_{FD}(\varphi) = \frac{1}{1 + \exp(\frac{\varphi - \varphi_0}{\gamma})},$$

where $\varphi = \arctan(\frac{b+c}{a})$, φ_0 is $\pi/4$, and γ is 0.1.

The distance between m and m' is then computed in [3] as $1 - S_{FD}(m, m')$ and is thus a real number in $[0; 1]$. We have proposed in [3] that, if such a distance is lower than a given threshold, y' will be declared as watermarked and not watermarked otherwise. Next section presents a practical robustness evaluation of $\mathcal{CIS}_2$ using this decision rule.

4.5 Robustness study of the process

This section is devoted to the recall of the robustness study of the $\mathcal{CIS}_2$ scheme realized in [3]. For the whole experiments, a set of 100 images has been randomly extracted from the database taken from the BOSS contest [34]. In this set, each cover is a 512×512 grayscale digital image. The considered watermark m is given in Fig. 2(b). Testing the robustness of the approach is achieved by successively applying on watermarked images attacks like cropping, compression, geometric transformations,... Differences between m and m' have been computed as described in the previous section.

We have firstly evaluate the robustness of the $\mathcal{CIS}_2$ approach by applying different percentages of cropping, from 0.25% to 90%. Results are recalled in Fig. 3, which presents effects of such an attack. All the percentage differences are so far less than 97% and thus robustness is established.

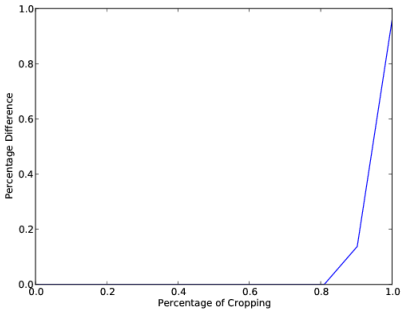
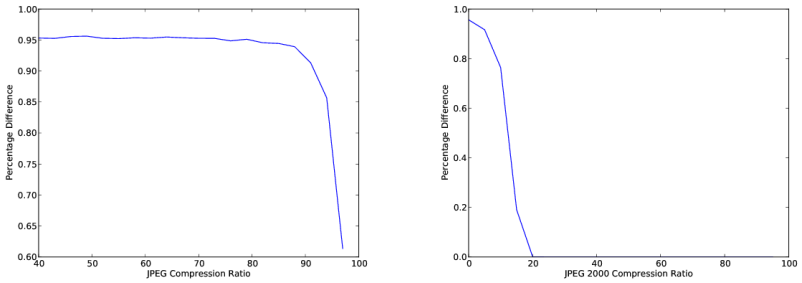


Figure 3: Cropping Results

Robustness against compression has then been addressed in [3], by studying both JPEG and JPEG 2000 image compressions. Results are respectively

presented in Fig. 4(a) and Fig. 4(b). It is not hard to see that robustness is well established for JPEG2000 compression: for all the ratios larger than 10%, the watermark is retrieved. However, as stated in [3], this scheme is not robust against JPEG compression for a ratio inferior to 90%. Remark that a potential solution can be to insert the watermark in least significant coefficient of the image described in frequency domain, for instance using either discrete cosine or with wavelet transform.



(a) JPEG Effect (b) JPEG 2000 Effect

Figure 4: Compression Results

Among geometric transformations, we then focused on rotations, *i.e.*, when two opposite rotations of angle θ are successively applied around the center of the image. In these geometric transformations, angles range from 2 to 60 degrees. Results are presented in Fig. 5: thanks to an efficient embedding, our scheme is resistant to all that type of attacks.

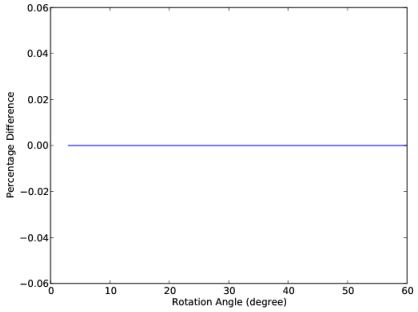
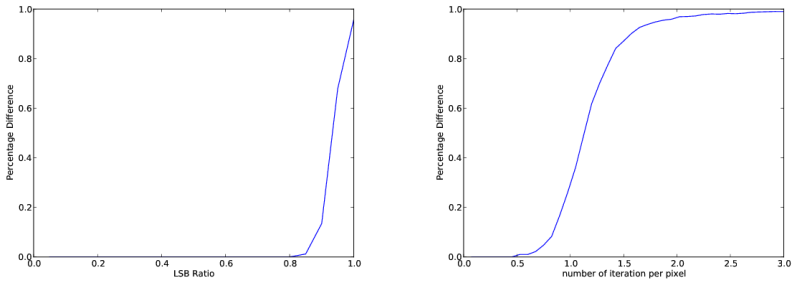


Figure 5: Rotation Attack Results

The first step of the $\mathcal{CIS}_2$ scheme studied in this subsection has defined x as the LSBs of the host image, it is thus based on LSB modifications. We have then considered in [3] two types of attacks modifying these LSB sets (see Fig 6). The former consists in setting to zero a subset of this one. Results are expressed

in Fig. 6(a) and show that the scheme is robust, unless 95% of the LSB is erased. In this case the image is really damaged. The latter consists in applying again this scheme on the watermarked image but with another message. Results of Fig. 6(b) show that this scheme is robust against that type of attack, provided the number of iterations is lesser than 1.75 times the number of pixels. With more iterations, the image is dramatically modified: more than 50% of the LSB is switched.



(a) LSB erasing effects (b) Applying algorithm twice

Figure 6: LSB Modifications

4.6 Evaluation of the embeddings

A Receiver Operating Characteristic (ROC) approach has finally been implemented in [3], to find the most adapted threshold w.r.t. the separation between watermarked images and other ones.

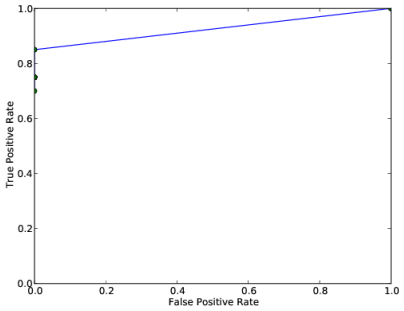


Figure 7: ROC Curves for DWT or DCT Embeddings

Figure 7 recalls the obtained ROC curve. This latter is close to the ideal one that is without False Positive and False Negative answer. The threshold with

best results is a distance equal to 0.97. With such a value, we can give some confidence intervals for most of evaluated attacks. The approach is resistant to all the cropping where percentage is less than 90%, to a JPEG2000 compression where quality ratio is greater than 5%, to all the rotation attacks, and to LSB erasing when less than 95% LSBs are set to 0.

4.7 Lyapunov evaluation of $\mathcal{CIS}_2$

We finally close the study of the $\mathcal{CIS}_2$ process by recalling the way we evaluated its Lyapunov exponent in Secrypt13 [6].

4.7.1 A topological semi-conjugacy between $\mathcal{X}_2$ and $\mathbb{R}$

In this section, by using a topological semi-conjugacy, we recall that $\mathcal{CIS}_2$ modeled by $\mathcal{G}_{f_0}$ on $\mathcal{X}$ can be described as iterations on a real interval. To do so, new notations and terminologies must be introduced.

Let $\mathcal{X}_{(\mathsf{N};\mathsf{P})} = \mathbb{S}_N \times \mathbb{B}^{\mathsf{N}} \times \mathbb{S}_P \times \mathbb{B}^{\mathsf{P}} \times \mathbb{S}_P$. In what follows and for easy understanding, we will assume that $\mathsf{N} = 3$ and $\mathsf{P} = 2$. So $\mathsf{N} + \mathsf{P} = 5$ and $\mathsf{NP}^2 = 12$. However, an equivalent formulation of the following can be easily obtained by replacing the bases 5 and 12 by any base $(\mathsf{N}+\mathsf{P})$ and (NP^2). N has only to be greater than P.

Definition 21 *The function* $\psi : [\![1, \mathsf{N}]\!] \times [\![1, \mathsf{P}]\!] \times [\![1, \mathsf{P}]\!] \to [\![0, \mathsf{NP}^2 - 1]\!]$ *is defined by:* $\psi\left(S_p^i, S_c^i, S_m^i\right) = (S_p^i - 1)\mathsf{P}^2 + (S_c^i - 1)\mathsf{P} + (S_m^i - 1)$.

This function aims to convert a strategy of triplets in a simple strategy of integers expressed in a different basis, see Table 2. Obviously, ψ is a bijective function, the reverse operation will be denoted by ψ^{-1}. The three projections of ψ^{-1} are denoted by: $\psi_1^{-1}\left(\psi\left(S_p^i, S_c^i, S_m^i\right)\right) = S_p^i$, $\psi_2^{-1}\left(\psi\left(S_p^i, S_c^i, S_m^i\right)\right) = S_c^i$, and $\psi_3^{-1}\left(\psi\left(S_p^i, S_c^i, S_m^i\right)\right) = S_m^i$.

Definition 22 *Let us define* $\varphi : \mathcal{X}_{(3;2)} = \mathbb{S}_3 \times \mathbb{B}^3 \times \mathbb{S}_2 \times \mathbb{B}^2 \times \mathbb{S}_2 \longrightarrow \left[0, 2^5\right[$, *as follows. If* $(S_p, E, S_c, M, S_m) = \left((S_p^0, S_p^1, \ldots); (E_0, E_1, E_2, E_3); (S_c^0, S_c^1, \ldots); (M_0, M_1); (S_m^0, S_m^1, \ldots)\right)$, *then* $\varphi\left(S_p, E, S_c, M, S_m\right)$ *is the real number:*

- *whose integral part* e *is* $\displaystyle\sum_{k=0}^{2} 2^{4-k} E_k + \sum_{k=3}^{4} 2^{4-k} M_{k-3}$, *that is, the binary digits of* e *are* $E_0\ E_1\ E_2\ M_0\ M_1$.
- *whose decimal part* s *is equal to:* $s = 0, \psi\left(S_p^0, S_c^0, S_m^0\right)\ \psi\left(S_p^1, S_c^1, S_m^1\right)\ \psi\left(S_p^2, S_c^2, S_m^2\right)\ \ldots = \sum_{k=1}^{+\infty} 12^{-k} S^{k-1}$. s *is thus expressed in base* 12.

As notified in [6], φ realizes the association between a point of $\mathcal{X}_{(3;2)}$ and a real number into $\left[0, 2^5\right[$. We must now translate the steganographic process $\mathcal{CIS}_2$, which is represented by $\mathcal{G}_{f_0}$, as iterations on this real interval. To do so, two intermediate functions over $\left[0, 2^5\right[$ denoted by e and s has been introduced in [6].

Base $\mathsf{N}=3$	Base $\mathsf{P}=2$	Base $\mathsf{P}=2$	Base $\mathsf{NP}^2=12$
S_p^i	S_c^i	S_m^i	$\psi\left(S_p^i, S_c^i, S_m^i\right)$
1	1	1	0
1	1	2	1
1	2	1	2
1	2	2	3
2	1	1	4
2	1	2	5
2	2	1	6
2	2	2	7
3	1	1	8
3	1	2	9
3	2	1	10
3	2	2	11

Table 2: Some values for ψ (see Definition 21).

Definition 23 *Let $x \in \left[0, 2^5\right[$ and:*

- *$e_0, \ldots, e_4$ the binary digits of the integral part of x: $\lfloor x \rfloor = \sum_{k=0}^{4} 2^{4-k} e_k$.*
- *$(s^k)_{k\in\mathbb{N}}$ the digits of x, expressed in base 12, where the chosen decimal decomposition of x is the one that does not have an infinite number of 11: $x = \lfloor x \rfloor + \sum_{k=0}^{+\infty} s^k 12^{-k-1}$.*

e and s are thus defined as follows:

$$\begin{array}{rccc} e: & \left[0, 2^5\right[& \longrightarrow & \mathbb{B}^3 \times \mathbb{B}^2 \\ & x & \longmapsto & ((e_0, e_1, e_2); (e_3, e_4)) \end{array}$$

and

$$\begin{array}{rccc} s: & \left[0, 2^5\right[& \longrightarrow & [\![0, 11]\!]^{\mathbb{N}} \\ & x & \longmapsto & (s^k)_{k\in\mathbb{N}} \end{array}$$

We have thus been able to define the function g, whose goal is to translate the steganographic process $\mathcal{CIS}_2$ represented by $\mathcal{G}_{f_0}$ on an interval of $\mathbb{R}$ [6].

Definition 24 *$g : \left[0, 2^5\right[\longrightarrow \left[0, 2^5\right[$ is such that $g(x)$ is the real number of $\left[0, 2^5\right[$ defined below:*

- *its integral part has a binary decomposition equal to $e'_0, \ldots, e'_4$, with $\forall i \in [\![0, 2]\!]$:*

$$e'_i = \begin{cases} e(x)_i & \text{if } i \neq \psi_1^{-1}\left(s^0\right) \\ e(x)_{2+\psi_2^{-1}(s^0)} & \text{if } i = \psi_1^{-1}\left(s^0\right) \end{cases}$$

and $\forall i \in [\![3,4]\!]$*:*

$$e'_i = \begin{cases} e(x)_i & \text{if } i \neq \psi_3^{-1}\left(s^0\right) \\ e(x)_i + 1 \ \textit{(mod 2)} & \text{if } i = \psi_3^{-1}\left(s^0\right), \end{cases}$$

- *whose decimal part is* $s(x)^1, s(x)^2, \ldots$

In other words, if $x = \sum_{k=0}^{4} 2^{4-k} e_k + \sum_{k=0}^{+\infty} s^k \ 12^{-k-1}$, then:

$$g(x) = \sum_{k=0}^{2} 2^{4-k} \left[e_k \left(\delta(k, \psi_1^{-1}(s^0)) + 1 \pmod 2 \right) + e_{2+\psi_2^{-1}(s^0)} \left(\delta(k, \psi_1^{-1}(s^0)) \right) \right]$$

$$+ \sum_{k=3}^{4} 2^{4-k} (e_k + \delta(k, \psi_3^{-1}(s^0) \pmod 2)) + \sum_{k=0}^{+\infty} s^{k+1} 12^{-k-1},$$

where δ is the discrete Boolean metric introduced previously.

Numerous metrics can be defined on the set $\left[0, 2^5\right[$, the most usual one being the Euclidian distance $\Delta(x,y) = |y-x|^2$. However, this Euclidian distance does not reproduce exactly the notion of proximity induced by distance d_2 on $\mathcal{X}_2$ introduced in a previous section, which is more relevant for the targetted applications. Indeed d_2 is richer than Δ, this is why we have introduced the following map in [6].

Definition 25 *Given* $x, y \in \left[0, 2^5\right[$*,* D *denotes the function from* $\left[0, 2^5\right[^2$ *to* $\mathbb{R}^+$ *defined by:* $D(x,y) = D_e\left(e(x), e(y)\right) + D_s\left(s(x), s(y)\right)$*, where:*

$$D_e(e, \check{e}) = \sum_{k=0}^{4} \delta(e_k, \check{e}_k), \quad \textit{and} \quad D_s(s, \check{s}) = \sum_{k=1}^{\infty} \frac{|s^k - \check{s}^k|}{12^k}.$$

We have thus proven in [6] that,

Proposition 7 D *is a distance on* $\left[0, 2^5\right[$.

The convergence of sequences according to D is not the same than the usual convergence related to the Euclidian metric. For instance, if $x^n \to x$ according to D, then necessarily the integral part of each x^n is equal to the integral part of x (at least after a given threshold), and the decimal part of x^n corresponds to the one of x "as far as required". D is richer and more refined than the Euclidian distance, and thus is more precise.

φ has been constructed in order to be continuous and onto, so we obtained the following theorem in [6].

Theorem 3 *The steganographic process $\mathcal{CIS}_2$ represented by $(\mathcal{G}_{f_0}, \mathcal{X}_2)$ can be considered as simple iterations on $\mathbb{R}$, which is illustrated by the semi-conjugacy given below:*

$$\begin{array}{ccc} \left(\mathcal{X}_{(3;2)}, d_2 \right) & \xrightarrow{\mathcal{G}_{f_0}} & \left(\mathcal{X}_{(3;2)}, d_2 \right) \\ \varphi \downarrow & & \downarrow \varphi \\ \left(\left[0, 2^5\right[, D \right) & \xrightarrow[g]{} & \left(\left[0, 2^5\right[, D \right) \end{array}$$

In other words, $\mathcal{X}_2$ is approximately equal to $\left[0, 2^{\mathsf{N}+\mathsf{P}}\right[$. We have thus remarked in [6] that,

Proposition 8 *The process $\mathcal{CIS}_2$ represented by g defined on $\mathbb{R}$ has derivatives of all orders on $\left[0, 2^5\right[$, except on the 385 points in I defined by: $I = \left\{ \dfrac{n}{12} \ / \ n \in [\![0; 2^5 \times 12]\!] \right\}$.*

Furthermore, on each interval of the form $\left[\dfrac{n}{12}, \dfrac{n+1}{12} \right[$, with $n \in [\![0; 2^5 \times 12[\![$, g is a linear function having a slope equal to 12: $\forall x \notin I, g'(x) = 12$.

We are now able to recall the way to evaluate the Lyapunov exponent of $\mathcal{CIS}_2$.

4.7.2 Topological security of $\mathcal{CIS}_2$ on $\mathbb{R}$

$\mathcal{CIS}_2$ represented by the function $\mathcal{G}_{f_0}$ on $\mathcal{X}_2$ is topologically secure, that is to say $(\mathcal{G}_{f_0}, \mathcal{X}_2)$ is chaotic in the sense of Devaney. We can deduce the same property for $\mathcal{CIS}_2$ represented by the g function on $\mathbb{R}$ for the order topology. Indeed $(\mathcal{G}_{f_0}, \mathcal{X}_2)$ and $\left(g, [0, 2^5[_D\right)$ are semi-conjugate by φ as recalled below. So $\left(g, [0, 2^5[_D\right)$ is a chaotic system according to Devaney, because the semi-conjugacy preserves this character [17]. However the topology generated by D is finer than the topology generated by the Euclidean distance Δ, which is the order topology. This is why we have proven in [6] that,

Theorem 4 *Let $\mathcal{X}$ be a set, and τ, τ' two topologies on $\mathcal{X}$ such that τ' is finer than τ. Let $f : \mathcal{X} \to \mathcal{X}$, continue for both τ and τ'.*

If $(\mathcal{X}_{\tau'}, f)$ is chaotic in the sense of Devaney, then $(\mathcal{X}_{\tau}, f)$ is also chaotic.

Finally, according to Theorem 4, we have deduced in [6] that the steganographic process $\mathcal{CIS}_2$ represented by g is chaotic in the sense of Devaney, for the order topology on $\mathbb{R}$. Having these assertions in mind, we have then formulated the following theorem:

Theorem 5 *The steganographic process $\mathcal{CIS}_2$ represented by g on $\mathbb{R}$ is chaotic in the sense of Devaney, when the usual topology of $\mathbb{R}$ is used (the order topology).*

This result is weaker than Theorem 2, which establishes the chaotic property of $\mathcal{CIS}_2$ for a finer topology. It is as if the chaos observed using usual tools like the Euclidian distance is still preserved when considering more powerful tools (higher resolution, *i.e.*, finer topologies). The result contained in Theorem 5 is however interesting, as it confirms that approach followed in [6] does not lead to deflated properties.

Indeed, our studies take place in a system other than the one usually considered in computer science ($\mathcal{X}_2$ instead of $\mathbb{R}$), in order to be as close as possible to the targetted computer machines. By doing so, we prevent from any loss of chaotic properties when computing the scheme written in mathematical terms. However, it might be feared that the choice of a discrete mathematics approach leads to a disorder of lower quality. In other words, perhaps we have avoided a situation of great disorder *lost* during the computation into finite machines. But the cost of such success may be to obtain a weaker disorder ? Theorem 5 proves exactly the contrary.

4.7.3 Evaluation of the Lyapunov exponent

Let $\mathcal{L} = \left\{x^0 \in \left[0, 2^5\right[\ / \ \forall n \in \mathbb{N}, x^n \notin I\right\}$, where I is the set of points in the real interval where g is not differentiable (as it is explained in Proposition 8). Then [6].

Theorem 6 *$\forall x^0 \in \mathcal{L}$, the Lyapunov exponent of $\mathcal{CIS}_2$ having x^0 for initial condition is equal to $\lambda(x^0) = \ln(12) > 0$.*

Rem 1 *The set of initial conditions for which this exponent is not calculable is countable. This is indeed the initial conditions such that an iteration value will be a number having the form $\frac{n}{12}$, with $n \in \mathbb{N}$. Moreover, for a system having $\mathsf{N} + \mathsf{P}$ cells (a number of LSCs equal to N and a secret message to embed of width equal to P), we will find,* mutatis mutandis*, an infinite uncountable set of initial conditions $x^0 \in \left[0; 2^{\mathsf{N}+\mathsf{P}}\right[$ such that $\lambda(x^0) = \ln(\mathsf{NP}^2)$.*

So, it is possible to make the Lyapunov exponent of the scheme $\mathcal{CIS}_2$ as large as possible, depending on the number of least significant coefficients of the cover media we decide to consider, and on the width of the message to embed. As proven in [23], a large Lyapunov exponent makes it impossible to achieve the well-known "Estimated Original Attacks" [14].

5 The $\mathcal{DI}_3$ Steganographic Process

In [1,2], a new steganographic algorithm named $\mathcal{DI}_3$ is presented. It is inspired from $\mathcal{CIW}_1$ and $\mathcal{CIS}_2$ respectively published in [20] and [23], and recalled previously in this article. Compared to the first one, $\mathcal{DI}_3$ is a steganographic scheme, not just a watermarking technique. That is, in our understanding, it can embed more than one bit. Unlike $\mathcal{CIS}_2$, which requires embedding keys with three strategies, only one sequence is required for $\mathcal{DI}_3$, so it is easier to implement.

Indeed $\mathcal{DI}_3$ is a faster instance of $\mathcal{CIS}_2$, as there is no message mixing in it. $\mathcal{DI}_3$ is well-defined mathematically and its security is evaluated in [1], whereas [2] provides algorithms and investigates its robustness, comparing it to some well-known watermarking schemes, namely the YASS [39], nsF5 [19], MMx [28], and HUGO [32] algorithms detailed in the Appendix 7.

5.1 Mathematical definitions and notations

New notations and terminologies must be introduced another time in order to be able to define mathematically the $\mathcal{DI}_3$ steganographic process. They are provided thereafter.

Definition 26 *The* support of a finite sequence S *of* n *terms is the finite set* $\mathsf{S}(S) = \left\{S^k, k < n\right\}$ *containing all the distinct values of* S*. Its cardinality is s.t.* $\#\mathsf{S}(S) \leqslant n$.

Definition 27 *A finite sequence* $S \in \mathbb{S}_{\mathsf{N}}$ *of* n *terms is* injective *if* $n = \#\mathsf{S}(S)$*. It is* onto *if* $N = \#\mathsf{S}(S)$*. Finally, it is bijective if and only if it is both injective and onto, so* $n = N = \#\mathsf{S}(S)$.

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

5.2 The new $\mathcal{DI}_3$ process

In this section, the new algorithm introduced in [1] and studied in [2] is recalled. Let $\mathsf{P} \in \mathbb{N}^*$ be 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. $\lambda > \mathsf{P}$. $x^0 \in \mathbb{B}^{\mathsf{N}}$ 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.

Rem 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.*

The proposed information hiding scheme is defined by:

Definition 28 ($\mathcal{DI}_3$ Data hiding scheme) $\forall (n, i, j) \in \mathbb{N}^* \times [\![0; \mathsf{N} - 1]\!] \times [\![0; \mathsf{P} - 1]\!]$*:*

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

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

5.3 Security study

A security study of the $\mathcal{DI}_3$ steganographic process has been realized in [1]. Conclusion of this study is summarized thereafter.

Proposition 9 *$\mathcal{DI}_3$ is stego-secure.*

This proof of this proposition, provided in [1], holds for the following restrictive hypotheses:

Distribution of LSCs. We have supposed that $x^0 \sim \mathcal{U}\left(\mathbb{B}^{\mathsf{N}}\right)$ to prove the stego-security of the data hiding process $\mathcal{DI}_3$. This hypothesis of the uniform distribution of the least significant coefficients is obviously 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 or for test batteries) 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 1, in that framework, the attacker has only access to stego-contents, having so no knowledge of the original media (*i.e.*, before introducing the message in the LSCs random channel).

Distribution of the messages m. In order to prove the stego-security of the data hiding process $\mathcal{DI}_3$, we have supposed that $m \sim \mathcal{U}\left(\mathbb{B}^{\mathsf{P}}\right)$. This hypothesis of the uniform distribution of the message to hide is not really restrictive. Indeed, to encrypt the message before its embedding into the LSCs of cover media, which is usually required for obvious security reasons, is 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.

Distribution of the strategies S. To prove the stego-security of the data hiding process $\mathcal{DI}_3$, we have finally supposed that $S \sim \mathcal{U}\left(\mathbb{S}_{\mathsf{P}}\right)$. This hypothesis is not restrictive too, as any cryptographically secure pseudo-random 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)* [25], *Blum Goldwasser (BG)* [40], or *ISAAC* [24] are convenient here.

After this theoretical study of the $\mathcal{DI}_3$ steganographic process realized in [1], we have investigated practical aspects, discussing about its concrete implementation and evaluating its robustness in [2], while article [1] already mentioned deals with its ability to face steganalyzers. These practical aspects are summarized below.

5.4 Implementing the $\mathcal{DI}_3$ scheme

In the algorithms recalled here, the following notations are used: S denotes the embedding and extraction strategy, H the host content or the stego-content depending of the context. LSC stands for the old or new LSCs of the host or stego-content H depending of the context too. N denotes the number of LSCs, λ the number of iterations to realize, M the secret message, and P the width of the message (number of bits).

The $\mathcal{DI}_3$ scheme theoretically presented in [1] has been practically described by three main algorithms in [2]:

1. Algorithm 1 generates the embedding strategy, part of the embedding key (with the LSCs and the number of iterations).
2. Algorithm 2 embeds the message into the LSCs of the cover media using the strategy. The strategy has been generated by the first algorithm and the same number of iterations is used.
3. Algorithm 3 extracts the secret message from the LSCs of the media (the stego-content) using the strategy, which constitutes with the message length the extraction key.

Two other complementary functions must be used:

1. Algorithm 4, which allows to extract MSCs, LSCs, and passive coefficients from the host content. Its implementation is based on the concept of signification function described previously.
2. Algorithm 5 rebuilds the new host content (the stego-content) from the corresponding MSCs, LSCs, and passive coefficients. This function realizes the opposite operation of Algorithm 4.

Rem 3 *These two algorithms depend of the definition of the MSCs, LSCs, and passive coefficients, which can correspond to a spatial or frequency description of the host content. This is why they are not documented here.*

5.5 Evaluation against steganalyzers

The steganographic scheme detailed in [1] has been compared to state of the art steganographic approaches, namely YASS [39], HUGO [32], and nsF5 [19] detailed in the Appendix 7. This study, realized in [1], is summarized thereafter.

The steganalysis is based on the BOSS image database [12], which consists in a set of 10 000 512x512 greyscale images. We have 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

Algorithm 1: *strategy*(N, P, λ)

```
/* S is a sequence of integers into [[0, P − 1]], such that
   (S_{n_0}, ..., S_{n_0+P−1}) is injective on [[0, P − 1]].   */
```

Result: S: The strategy, integer sequence $(S_0, S_1, \ldots)$.

begin

- $n_0 \longleftarrow L - P + 1$;
- **if** $P > N$ *OR* $n_0 < 0$ **then**
  - **return** *ERROR*
- $S \longleftarrow$ Array of width λ, all values initialized to 0;
- $cpt \longleftarrow 0$;
- **while** $cpt < n_0$ **do**
  - $S_{cpt} \longleftarrow$Random integer in $[\![0, P-1]\!]$.;
  - $cpt \longleftarrow cpt + 1$;
- $A \longleftarrow$ We generate an arrangement of $[\![0, P-1]\!]$;
- **for** $k \in [\![0, P-1]\!]$ **do**
  - $S_{n_0+k} \longleftarrow A_k$;
- **return** S

Algorithm 2: *embed*(LSC, M, S, λ)

Result: New LSCs with embedded message.

begin

- $N \longleftarrow$ Number of LSCs in LSC;
- $P \longleftarrow$ Width of the message M;
- **for** $k \in [\![0, \lambda]\!]$ **do**
  - $i \longleftarrow S_k$;
  - $LSC_i \longleftarrow M_i$;
- **return** LSC

bits. This step has led to distinguish four sets of stego contents, one for each steganographic approach.

We have next used in [1] the steganalysis tool developed by the HugoBreakers team [29, 30] based on AI classifier and which won the BOSS competition [12]. Table 3 summarizes these steganalysis results expressed as the error probabilities of the steganalyser, as they are given in [1]. The errors are the mean of the false alarms and of the missed detection. 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.

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 in [1] has no optimization, these first experiments shown promising results.

Algorithm 3: $extract(LSC, S, \lambda, P)$

Result: The message to extract from LSC.
begin
  $RS \longleftarrow$ The strategy S written in reverse order.;
  $M \longleftarrow$ Array of width P, all values initialized to 0;
  for $k \in [\![0, \lambda]\!]$ **do**
    $i \longleftarrow RS_k$;
    $M_i \longleftarrow LSC_i$;
  return M

Algorithm 4: $significationFunction(H)$

Data: H: The original host content.
Result: MSC: MSCs of the host content H.
Result: PC: Passive coefficients of the host content H.
Result: LSC: LSCs of the host content H.
begin
  `/* Implemented by the user. */`
  return (MSC, PC, LSC)

5.6 Robustness study

This section summarizes the robustness study presented in [2]. Each experiment is build another time on a set of 50 images, which are randomly selected among database taken from the BOSS contest [12]. Each cover is a 512×512 greyscale digital image. The relative payload is always set with 0.1 bit per pixel. Under that constrain, the embedded message m still remains a sequence of 26214 randomly generated bits.

According to previous similar work in the field of information hiding, we have conducted in [2] our evaluation following a same canvas than other robustness studies documented previously in this article. We have firstly chosen some classical attacks like cropping, compression, and rotation ones. The robustness of $\mathcal{DI}_3$ has then been tested by successively applying on stego content these attacks. Differences between the message that is extracted from the attacked image and the original one are then computed and expressed as percentage.

Different percentage of cropping (from 1% to 81%) have been firstly applied on the stego image in [2], Fig. 8 (c) recalls effects of such attacks. We have then addressed robustness against JPEG and JPEG 2000 compression, and results are summarized in Fig. 8 (a-b). Attacks based on geometric transformations have finally been addressed through rotations: as presented previously in this article, two opposite rotations of angle θ are successively applied around the center of the image. In these geometric transformations, angles range from 2 to 20 degrees. Effects of such attacks are also recalled in Fig. 8 (d).

From all these experiments, one can conclude that the steganographic scheme

Algorithm 5: $buildFunction(MSC, PC, LSC)$)

Result: H: The new rebuilt host content.
begin
  `/* Implemented by the user. */`
  return (MSC, PC, LSC)

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

Table 3: Steganalysis results of HugoBreakers steganalyser applied on steganographic scheme

does not present obvious drawback and resists to all the attacks: all the percentage differences are so far less than 50%.

All researches presented in previous sections have started from the $\mathcal{CIW}_1$ process, proceeding by successively correcting its drawbacks. By doing so, we have had a retreat from chaotic iterations. At the same time, the chaotic iterations based information hiding (dhCI) process, whose the $\mathcal{CIW}_1$ scheme historically arises from, continued to be investigated in parallel. Results of these investigations are detailed in the next section.

6 Conclusion

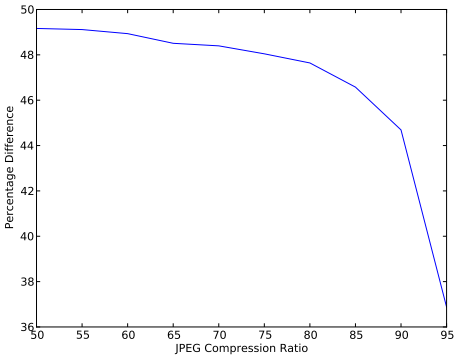
7 Appendix

We recall in this appendix some state of the art information hiding schemes. One should find more details in [18].

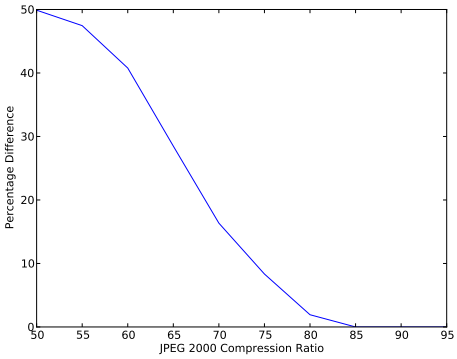
7.1 YASS

YASS (*Yet Another Steganographic Scheme*) [39] is a steganographic approach dedicated to JPEG cover. The main idea of this algorithm is to hide data into 8×8 randomly chosen inside $B\times B$ blocks (where B is greater than 8) instead of choosing standard 8×8 grids used by JPEG compression. The self-calibration process commonly embedded into blind steganalysis schemes is then confused by the approach. In the paper [36], further variants of YASS have been proposed simultaneously to enlarge the embedding rate and to improve the randomization step of block selecting. More precisely let be given a message m to hide, a size B, $B \geq 8$, of blocks . The YASS algorithm follows:

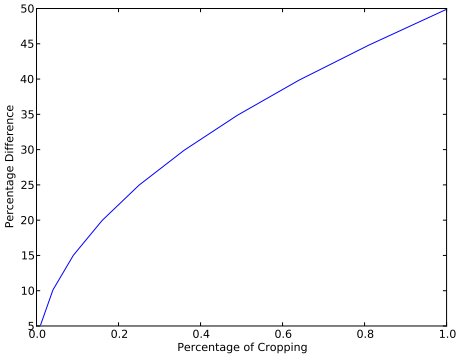
1. computation of m' which is the Repeat-Accumulate error correction code of m



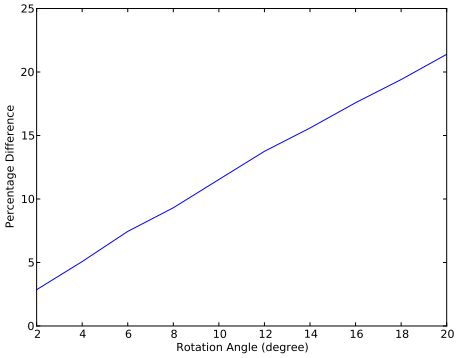
(a) JPEG effect.



(b) JPEG 2000 effect.



(c) Cropping attack.



(d) Rotation attack.

Figure 8: Robustness of $\mathcal{DI}_3$ scheme facing several attacks (50 images from the BOSS repository)

2. in each big block of size $B \times B$ of cover, successively:
   (a) random selection of an 8×8 block b using w.r.t. a secret key.
   (b) two-dimensional DCT transformation of b and normalisation of coefficient w.r.t a predefined quantization table. Matrix is further referred to as b'.
   (c) a fragment of m' is embedded in some LSB of b'. Let b'' be the resulting matrix.
   (d) The matrix b'' is decompressed back to the spatial domain leading to a new $B \times B$ block.

7.2 nsF5

The nsF5 algorithm [19] extends the F5 algorithm [41]. Let us first have a closer look on this latter

First of all, as far as we know, F5 is the first steganographic approach that solves the problem of remaining unchanged a part (often the end) of the file. To achieve this, a subset of all the LSB is computed thanks to a pseudorandom number generator seeded with a user defined key. Next, this subset is split into blocks of x bits. The algorithm takes benefit of binary matrix embedding to increase it efficiency. Let us explain this embedding on a small illustrative example where a part m of the message has to be embedded into this x LSB of pixels which are respectively a 3 bits column vector and a 7 bits column vector. Let then H be the binary Hamming matrix

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

The objective is to modify x to get y s.t. $m = Hy$. In this algebra, the sum and the product respectively correspond to the exclusive *or* and to the *and* Boolean operators. If Hx is already equal to m, nothing has to be changed and x can be sent. Otherwise we consider the difference $\delta = d(m, Hx)$ which is expressed as a vector :

$$\delta = \begin{pmatrix} \delta_1 \\ \delta_2 \\ \delta_3 \end{pmatrix} \text{ where } \delta_i \text{ is 0 if } m_i = Hx_i \text{ and 1 otherwise.}$$

Let us thus consider the jth column of H which is equal to δ. We denote by $\overline{x}^j$ the vector we obtain by switching the jth component of x, that is, $\overline{x}^j = (x_1, \ldots, \overline{x_j}, \ldots, x_n)$. It is not hard to see that if y is $\overline{x}^j$, then $m = Hy$. It is then possible to embed 3 bits in only 7 LSB of pixels by modifying on average $1 - 2^3$ changes. More generally, the F5 embedding efficiency should theoretically be $\frac{p}{1-2^p}$.

However, the event when the coefficient resulting from this LSB switch becomes zero (usually referred to as *shrinkage*) may occur. In that case, the recipient cannot determine whether the coefficient was -1, +1 and has changed to 0 due to the algorithm or was initially 0. The F5 scheme solves this problem first by defining a LSB with the following (not even) function:

$$LSB(x) = \begin{cases} 1 - x \mod 2 \text{ if } x < 0 \\ x \mod 2 \text{ otherwise.} \end{cases} .$$

An next, if the coefficient has to be changed to 0, the same bit message is re-embedded in the next group of x coefficient LSB.

The scheme nsF5 focuses on steps of Hamming coding and ad'hoc shrinkage removing. It replaces them with a *wet paper code* approach that is based on a random binary matrix. More precisely, let D be a random binary matrix of

size $x \times n$ without replicate nor null columns: consider for instance a subset of $\{1, 2^x\}$ of cardinality n and write them as binary numbers. The subset is generated thanks to a PRNG seeded with a shared key. In this block of size x, one choose to embed only k elements of the message m. By abuse, the restriction of the message is again called m. It thus remains $x - k$ (wet) indexes/places where the information shouldn't be stored. Such indexes are generated too with the keyed PRNG. Let v be defined by the following equation

$$Dv = \delta(m, Dx). \tag{3}$$

This equation may be solved by Gaussian reduction or other more efficient algorithms. If there is a solution, one have the list of indexes to modify into the cover. The nsF5 scheme implements such a optimized algorithm that is to say the LT codes.

7.3 MMx

Basically, the MMx algorithm [28] embeds message in a selected set of LSB cover coefficients using Hamming codes as the F5 scheme. However, instead of reducing as many as possible the number of modified elements, this scheme aims at reducing the embedding impact. To achieve this it allows to modify more than one element if this leads to decrease distortion.

Let us start again with an example with a $[7, 4]$ Hamming codes, *i.e*, let us embed 3 bits into 7 DCT coefficients, $D_1, \ldots, D_7$. Without details, let $\rho_1, \ldots, \rho_7$ be the embedding impact whilst modifying coefficients $D_1, \ldots, D_7$ (see [28] for a formal definition of ρ). Modifying element at index j leads to a distortion equal to ρ_j. However, instead of switching the value at index j, one should consider to find all other columns of H, j_1, j_2 for instances, s.t. the sum of them is equal to the jth column and to compare ρ_j with $\rho_{j_1} + \rho_{j_2}$. If one of these sums is less than ρ_j, the sender has to change these coefficients instead of the j one. The number of searched indexes (2 for the previous example) gives the name of the algorithm. For instance in MM3, one check whether the message can be embedded by modifying each time 3 pixel or less.

7.4 HUGO

The HUGO [32] steganographic scheme is mainly designed to minimize distortion caused by embedding. To achieve this, it is firstly based on an image model given as SPAM [33] features and next integrates image correction to reduce much more distortion. What follows discuss on these two steps.

The former first computes the SPAM features. Such calculi synthesize the probabilities that the difference between consecutive horizontal (resp. vertical, diagonal) pixels belongs in a set of pixel values which are closed to the current pixel value and whose radius is a parameter of the approach. Thus a fisher linear discriminant method defines the radius and chooses between directions (horizontal, vertical...) of analyzed pixels that gives the best separator for detecting embedding changes. With such instantiated coefficients,

HUGO can synthesize the embedding cost as a function $D(X, Y)$ that evaluates distortions between X and Y. Then HUGO computes the matrices of $\rho_{i,j} = \max(D(X, X^{(i,j)+})_{i,j}, D^-(X, X^{(i,j)-})_{i,j})$ such that $X^{(i,j)+}$ (resp. $X^{(i,j)+}$) is the cover image X where the the (i, j)th pixel has been increased (resp. has been decreased) of 1.

The order of modifying pixel is critical: HUGO surprisingly modifies pixels in decreasing order of $\rho_{i,j}$. Starting with $Y = X$, it increases or decreases its (i, j)th pixel to get the minimal value of $D(Y, Y^{(i,j)+})_{i,j}$ and $D^-(Y, Y^{(i,j)-})_{i,j}$. The matrix Y is thus updated at each round.

References

[1] Jacques Bahi, Jean-François Couchot, Nicolas Friot, and Christophe Guyeux. Application of steganography for anonymity through the internet. In *IHTIAP'2012, 1-st Workshop on Information Hiding Techniques for Internet Anonymity and Privacy*, pages 96–101, Venice, Italy, June 2012.

[2] Jacques Bahi, Jean-François Couchot, Nicolas Friot, and Christophe Guyeux. A robust data hiding process contributing to the development of a semantic web. In *INTERNET'2012, 4-th Int. Conf. on Evolving Internet*, pages 71–76, Venice, Italy, June 2012.

[3] Jacques Bahi, Jean-François Couchot, Nicolas Friot, Christophe Guyeux, and Kamel Mazouzi. Quality studies of an invisible chaos-based watermarking scheme with message extraction. In *IIHMSP'13, 9th Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing*, pages ***_***, Beijing, China, October 2013. To appear.

[4] Jacques Bahi, Jean-François Couchot, and Christophe Guyeux. Steganography: a class of algorithms having secure properties. In *IIH-MSP-2011, 7-th Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing*, pages 109–112, Dalian, China, October 2011.

[5] Jacques Bahi, Nicolas Friot, and Christophe Guyeux. Lyapunov exponent evaluation of a digital watermarking scheme proven to be secure. In *IIH-MSP'2012, 8-th Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing*, pages 359–362, Piraeus-Athens, Greece, July 2012. IEEE Computer Society.

[6] Jacques Bahi, Nicolas Friot, and Christophe Guyeux. Topological study and lyapunov exponent of a secure steganographic scheme. In Javier Lopez and Pierangela Samarati, editors, *SECRYPT'2013, Int. Conf. on Security and Cryptography. SECRYPT is part of ICETE - The International Joint Conference on e-Business and Telecommunications*, pages ***_***, Reykjavik, Iceland, July 2013. SciTePress. 8 pages. To appear.

[7] Jacques Bahi and Christophe Guyeux. A new chaos-based watermarking algorithm. In *SECRYPT'10, Int. conf. on security and cryptography*, pages 455–458, Athens, Greece, July 2010. SciTePress.

[8] Jacques Bahi and Christophe Guyeux. A new chaos-based watermarking algorithm. In *SECRYPT'10, Int. conf. on security and cryptography*, pages 455–458, Athens, Greece, July 2010. SciTePress.

[9] Jacques Bahi and Christophe Guyeux. *Discrete Dynamical Systems and Chaotic Machines: Theory and Applications.* Chapman & Hall, CRC Press, June 2013. 212 pages.

[10] Jacques M. Bahi and Christophe Guyeux. Topological chaos and chaotic iterations, application to hash functions. In *WCCI'10, IEEE World Congress on Computational Intelligence*, pages 1–7, Barcelona, Spain, July 2010. Best paper award.

[11] J. Banks, J. Brooks, G. Cairns, and P. Stacey. On Devaney's definition of chaos. *Amer. Math. Monthly*, 99:332–334, 1992.

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

[13] Christian Cachin. An information-theoretic model for steganography. In *Information Hiding*, volume 1525 of *Lecture Notes in Computer Science*, pages 306–318. Springer Berlin / Heidelberg, 1998.

[14] F. Cayre and P. Bas. Kerckhoffs-based embedding security classes for woa data hiding. *IEEE Transactions on Information Forensics and Security*, 3(1):1–15, 2008.

[15] Pedro Comesaña, Luis Pérez-Freire, and Fernando Pérez-González. Fundamentals of data hiding security and their application to spread-spectrum analysis. In Mauro Barni, Jordi Herrera-Joancomartí, Stefan Katzenbeisser, and Fernando Pérez-González, editors, *IH'05: Information Hiding Workshop*, volume 3727 of *Lecture Notes in Computer Science*, pages 146–160. Lectures Notes in Computer Science, Springer-Verlag, 2005.

[16] Robert L. Devaney. *An Introduction to Chaotic Dynamical Systems.* Addison-Wesley, Redwood City, CA, 2nd edition, 1989.

[17] Enrico Formenti. *Automates cellulaires et chaos : de la vision topologique à la vision algorithmique.* PhD thesis, École Normale Supérieure de Lyon, 1998.

[18] Jessica Fridrich. *Steganography in Digital Media: Principles, Algorithms, and Applications.* Cambridge University Press, New York, NY, USA, 1st edition, 2009.

[19] Jessica J. Fridrich, Tomás Pevný, and Jan Kodovský. Statistically undetectable jpeg steganography: dead ends challenges, and opportunities. In Deepa Kundur, Balakrishnan Prabhakaran, Jana Dittmann, and Jessica J. Fridrich, editors, *MM&Sec*, pages 3–14. ACM, 2007.

[20] Nicolas Friot, Christophe Guyeux, and Jacques Bahi. Chaotic iterations for steganography - stego-security and chaos-security. In Javier Lopez and Pierangela Samarati, editors, *SECRYPT'2011, Int. Conf. on Security and Cryptography. SECRYPT is part of ICETE - The International Joint Conference on e-Business and Telecommunications*, pages 218–227, Sevilla, Spain, July 2011. SciTePress.

[21] Christophe Guyeux. *Le désordre des itérations chaotiques et leur utilité en sécurité informatique.* PhD thesis, Université de Franche-Comté, 2010.

[22] Christophe Guyeux. *Le désordre des itérations chaotiques - Applications aux réseaux de capteurs, à la dissimulation d'information, et aux fonctions de hachage.* Éditions Universitaires Européennes, 2012. ISBN 978-3-8417-9417-8. 362 pages. Publication de la thèse de doctorat.

[23] Christophe Guyeux, Nicolas Friot, and Jacques 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*, pages 208–211, Darmstadt, Germany, October 2010.

[24] R. J. Jenkins. ISAAC. *Fast Software Encryption*, pages 41–49, 1996.

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

[26] T. Kalker. Considerations on watermarking security. In *Multimedia Signal Processing, 2001 IEEE Fourth Workshop on*, pages 201–206, 2001.

[27] Andrew D. Ker, Tomáš Pevný, Jan Kodovský, and Jessica Fridrich. The square root law of steganographic capacity. In *MMSec '08: Proceedings of the 10th ACM workshop on Multimedia and security*, pages 107–116, New York, NY, USA, 2008. ACM.

[28] Younhee Kim, Zoran Duric, and Dana Richards. Modified matrix encoding technique for minimal distortion steganography. In Jan Camenisch, Christian S. Collberg, Neil F. Johnson 0001, and Phil Sallee, editors, *Information Hiding*, volume 4437 of *Lecture Notes in Computer Science*, pages 314–327. Springer, 2006.

[29] J. Kodovský and J. Fridrich. Steganalysis in high dimensions: fusing classifiers built on random subspaces. In *Proc. SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics XIII, San Francisco, CA,*, January 2011.

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

[31] Luis Perez-Freire, Pedro Comesana, Juan Ramon Troncoso-Pastoriza, and Fernando Perez-Gonzalez. Watermarking security: a survey. In *LNCS Transactions on Data Hiding and Multimedia Security*, 2006.

[32] Tomás Pevný, Tomás Filler, and Patrick Bas. Using high-dimensional image models to perform highly undetectable steganography. In Rainer Böhme, Philip W. L. Fong, and Reihaneh Safavi-Naini, editors, *Information Hiding*, volume 6387 of *Lecture Notes in Computer Science*, pages 161–177. Springer, 2010.

[33] Tomás Pevný, Patrick Bas, and Jessica J. Fridrich. Steganalysis by subtractive pixel adjacency matrix. *IEEE Transactions on Information Forensics and Security*, 5(2):215–224, 2010.

[34] Tomáš Pevný, Tomáš Filler, and Patrick Bas. Break our steganographic system, 2010. available at `http://www.agents.cz/boss/`.

[35] Maria Rifqi, Marcin Detyniecki, and Bernadette Bouchon-Meunier. Discrimination power of measures of resemblance. In *IFSA'03*, 2003.

[36] Anindya Sarkar, Kaushal Solanki, and B. S. Manjunath. Further study on yass: Steganography based on randomized embedding to resist blind steganalysis.

[37] Li Shujun, Li Qi, Li Wenmin, Mou Xuanqin, and Cai Yuanlong. Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding. *Proceedings of the 8th IMA International Conference on Cryptography and Coding*, 1:205–221, 2001.

[38] Gustavus J. Simmons. The prisoners' problem and the subliminal channel. In *Advances in Cryptology, Proc. CRYPTO'83*, pages 51–67, 1984.

[39] Kaushal Solanki, Anindya Sarkar, and B. S. Manjunath. Yass: Yet another steganographic scheme that resists blind steganalysis. In Teddy Furon, François Cayre, Gwenaël J. Doërr, and Patrick Bas, editors, *Information Hiding*, volume 4567 of *Lecture Notes in Computer Science*, pages 16–31. Springer, 2007.

[40] Umesh Vazirani and Vijay Vazirani. Efficient and secure pseudo-random number generation (extended abstract). In George Blakley and David Chaum, editors, *Advances in Cryptology*, volume 196 of *Lecture Notes in Computer Science*, pages 193–202. Springer Berlin / Heidelberg, 1985. 10.1007/3-540-39568-7_17.

[41] Andreas Westfeld. F5-a steganographic algorithm. In Ira S. Moskowitz, editor, *Information Hiding*, volume 2137 of *Lecture Notes in Computer Science*, pages 289–302. Springer, 2001.

[42] F. Xie, T. Furon, and C. Fontaine. Better security levels for 'broken arrows'. In *Proc. of SPIE Electronic Imaging on Media Forensics and Security XII*, San Jose, CA, USA, jan 2010.