

Steganography: a Class of Algorithms having Secure Properties

Jacques M. Bahi, Jean-François Couchot, and Christophe Guyeux*

University of Franche-Comté, Computer Science Laboratory, Belfort, France

Email: {jacques.bahi, jean-francois.couchot, christophe.guyeux}@univ-fcomte.fr

Abstract—Chaos-based approaches are frequently proposed in information hiding, but without obvious justification. Indeed, the reason why chaos is useful to tackle with discretion, robustness, or security, is rarely elucidated. This research work presents a new class of non-blind information hiding algorithms based on some finite domains iterations that are Devaney’s topologically chaotic. The approach is entirely formalized and reasons to take place into the mathematical theory of chaos are explained. Finally, stego-security and chaos security are consequently proven for a large class of algorithms.

I. INTRODUCTION

Chaos-based approaches are frequently proposed to improve the quality of schemes in information hiding [1]–[4]. In these works, the understanding of chaotic systems is almost intuitive: a kind of noise-like spread system with sensitive dependence on initial condition. Practically, some well-known chaotic maps are used either in the data encryption stage [2], [3], in the embedding into the carrier medium, or in both [1], [5].

This work focus on non-blind binary information hiding scheme: the original host is required to extract the binary hidden information. This context is indeed not as restrictive as it could primarily appear. Firstly, it allows to prove the authenticity of a document sent through the Internet (the original document is stored whereas the stego content is sent). Secondly, Alice and Bob can establish an hidden channel into a streaming video (Alice and Bob both have the same movie, and Alice hide information into the frame number k iff the binary digit number k of its hidden message is 1). Thirdly, based on a similar idea, a same given image can be marked several times by using various secret parameters owned both by Alice and Bob. Thus more than one bit can be embedded into a given image by using dhCI dissimulation. Lastly, non-blind watermarking is useful in network’s anonymity and intrusion detection [6], and to protect digital data sending through the Internet [7].

Methods referenced above are almost based on two fundamental chaotic maps, namely the Chebychev and logistic maps, which range in \mathbb{R} . To avoid justifying that functions which are chaotic in \mathbb{R} still remain chaotic in the computing representation (*i.e.*, floating numbers) we argue that functions should be iterated on finite domains. Boolean discrete-time dynamical systems (BS) are thus iterated.

Furthermore, previously referenced works often focus on discretion and/or robustness properties, but they do not consider security. As far as we know, stego-security [8] and chaos-security have only been proven on the spread spectrum watermarking [9], and on the dhCI algorithm [10], which is notably based on iterating the negation function. We argue that other functions can provide algorithms as secure as the dhCI one. This work generalizes thus this latter algorithm and formalizes all its stages. Due to this formalization, we address the proofs of the two security properties for a large class of steganography approaches.

This research work is organized as follows. Section II first recalls the BS context. The new class of algorithms, which is the first contribution, is firstly introduced in Sec. III. Section IV shows how secure is our approach: this is the second contribution of the present paper. Instances of algorithms guaranteeing that desired properties are presented in Sec. V. Discussion, conclusive remarks, and perspectives are given in the final section.

II. BOOLEAN DISCRETE-TIME DYNAMICAL SYSTEMS

In this section, we first give some recalls on Boolean discrete dynamical Systems (BS). With this material, next sections formalize the information hiding algorithms based on chaotic iterations.

Let n be a positive integer. A Boolean discrete-time network is a discrete dynamical system defined from a *Boolean map* $f : \mathbb{B}^n \rightarrow \mathbb{B}^n$ s.t.

$$x = (x_1, \dots, x_n) \mapsto f(x) = (f_1(x), \dots, f_n(x)),$$

and an *iteration scheme* (*e.g.*, parallel, serial, asynchronous...). With the parallel iteration scheme, the dynamics of the system are described by $x^{t+1} = f(x^t)$ where $x^0 \in \mathbb{B}^n$. Let thus $F_f : \llbracket 1; n \rrbracket \times \mathbb{B}^n \rightarrow \mathbb{B}^n$ be defined by

$$F_f(i, x) = (x_1, \dots, x_{i-1}, f_i(x), x_{i+1}, \dots, x_n),$$

with the *asynchronous* scheme, the dynamics of the system are described by $x^{t+1} = F_f(s_t, x^t)$ where $x^0 \in \mathbb{B}^n$ and s is a *strategy*, *i.e.*, a sequence in $\llbracket 1; n \rrbracket^{\mathbb{N}}$. Notice that this scheme only modifies one element at each iteration.

Let G_f be the map from $\llbracket 1; n \rrbracket^{\mathbb{N}} \times \mathbb{B}^n$ to itself s.t.

$$G_f(s, x) = (\sigma(s), F_f(s_0, x)),$$

where $\sigma(s)_t = s_{t+1}$ for all t in \mathbb{N} . Notice that parallel iteration of G_f from an initial point $X^0 = (s, x^0)$ describes

* Authors in alphabetic order

the “same dynamics” as the asynchronous iteration of f induced by the initial point x^0 and the strategy s .

Finally, let f be a map from \mathbb{B}^n to itself. The *asynchronous iteration graph* associated with f is the directed graph $\Gamma(f)$ defined by: the set of vertices is \mathbb{B}^n ; for all $x \in \mathbb{B}^n$ and $i \in \llbracket 1; n \rrbracket$, $\Gamma(f)$ contains an arc from x to $F_f(i, x)$.

III. FORMALIZATION OF STEGANOGRAPHIC METHODS

The data hiding scheme presented here does not constrain media to have a constant size. It is indeed sufficient to provide a function and a strategy that may be parametrized with the size of the elements to modify. The *mode* and the *strategy-adapter* defined below achieve this goal.

Definition 1 (Mode) A map f , which associates to any $n \in \mathbb{N}$ an application $f_n : \mathbb{B}^n \rightarrow \mathbb{B}^n$, is called a *mode*.

For instance, the *negation mode* is defined by the map that assigns to every integer $n \in \mathbb{N}^*$ the function $\neg_n : \mathbb{B}^n \rightarrow \mathbb{B}^n$, $\neg_n(x_1, \dots, x_n) \mapsto (\overline{x_1}, \dots, \overline{x_n})$.

Definition 2 (Strategy-Adapter) A strategy-adapter is a function S , from \mathbb{N} to the set of integer sequences, that associates to n a sequence $S \in \llbracket 1, n \rrbracket^{\mathbb{N}}$.

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

Let us notice that the terms of x that may be replaced by terms issued from 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, w.r.t. its position t :

Definition 3 (Signification function) A signification function is a real sequence $(u^k)_{k \in \mathbb{N}}$.

For instance, let us consider a set of grayscale images stored into 8 bits gray levels. In that context, we consider $u^k = 8 - (k \bmod 8)$ to be the k -th term of a signification function $(u^k)_{k \in \mathbb{N}}$.

Definition 4 (Significance of coefficients) Let $(u^k)_{k \in \mathbb{N}}$ be a signification function, m and M be two reals s.t. $m < M$. Then the most significant coefficients (MSCs) of x is the finite vector u_M , the least significant coefficients (LSCs) of x is the finite vector u_m , and the passive coefficients of x is the finite vector u_p such that:

$$\begin{aligned} u_M &= (k \mid k \in \mathbb{N} \text{ and } u^k \geq M \text{ and } k \leq |x|) \\ u_m &= (k \mid k \in \mathbb{N} \text{ and } u^k \leq m \text{ and } k \leq |x|) \\ u_p &= (k \mid k \in \mathbb{N} \text{ and } u^k \in]m; M[\text{ and } k \leq |x|) \end{aligned}$$

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. We are then ready to decompose an host x into its coefficients and then to recompose it. Next definitions formalize these two steps.

Definition 5 (Decomposition function) Let $(u^k)_{k \in \mathbb{N}}$ be a signification function, \mathfrak{B} the set of finite binary sequences, \mathfrak{N} the set of finite integer sequences, m and M be two reals s.t. $m < M$. Any host x may be decomposed into

$$(u_M, u_m, u_p, \phi_M, \phi_m, \phi_p) \in \mathfrak{N} \times \mathfrak{N} \times \mathfrak{N} \times \mathfrak{B} \times \mathfrak{B} \times \mathfrak{B}$$

where

- u_M , u_m , and u_p are coefficients defined in Definition 4;
- $\phi_M = (x^{u_M^1}, x^{u_M^2}, \dots, x^{u_M^{|u_M|}})$;
- $\phi_m = (x^{u_m^1}, x^{u_m^2}, \dots, x^{u_m^{|u_m|}})$;
- $\phi_p = (x^{u_p^1}, x^{u_p^2}, \dots, x^{u_p^{|u_p|}})$.

The function that associates the decomposed host to any digital host is the decomposition function. It is further referred as $\text{dec}(u, m, M)$ since it is parametrized by u , m and M . Notice that u is a shortcut for $(u^k)_{k \in \mathbb{N}}$.

Definition 6 (Recomposition) Let

$$(u_M, u_m, u_p, \phi_M, \phi_m, \phi_p) \in \mathfrak{N} \times \mathfrak{N} \times \mathfrak{N} \times \mathfrak{B} \times \mathfrak{B} \times \mathfrak{B} \text{ s.t.}$$

- the sets of elements in u_M , elements in u_m , and elements in u_p are a partition of $\llbracket 1, n \rrbracket$;
- $|u_M| = |\phi_M|$, $|u_m| = |\phi_m|$, and $|u_p| = |\phi_p|$.

One may associate the vector

$$x = \sum_{i=1}^{|u_M|} \varphi_M^i \cdot e_{u_M^i} + \sum_{i=1}^{|u_m|} \varphi_m^i \cdot e_{u_m^i} + \sum_{i=1}^{|u_p|} \varphi_p^i \cdot e_{u_p^i}$$

where $(e_i)_{i \in \mathbb{N}}$ is the usual basis of the \mathbb{R} -vectorial space $(\mathbb{R}^{\mathbb{N}}, +, \cdot)$. The function that associates x to any $(u_M, u_m, u_p, \phi_M, \phi_m, \phi_p)$ following the above constraints is called the recomposition function.

The embedding consists in the replacement of the values of ϕ_m of x 's LSCs by y . It then composes the two decomposition and recomposition functions seen previously. More formally:

Definition 7 (Embedding media) Let $\text{dec}(u, m, M)$ be a decomposition function, x be a host content, $(u_M, u_m, u_p, \phi_M, \phi_m, \phi_p)$ be its image by $\text{dec}(u, m, M)$, and y be a digital media of size $|u_m|$. The digital media z resulting on the embedding of y into x is the image of $(u_M, u_m, u_p, \phi_M, y, \phi_p)$ by the recomposition function rec .

Let us then define the *dhCI* information hiding scheme:

Definition 8 (Data hiding dhCI) Let $\text{dec}(u, m, M)$ be a decomposition function, f be a mode, S be a strategy adapter, x be an host content, $(u_M, u_m, u_p, \phi_M, \phi_m, \phi_p)$ be its image by $\text{dec}(u, m, M)$, q be a positive natural number, and y be a digital media of size $l = |u_m|$.

The dhCI dissimulation maps any (x, y) to the digital media z resulting on the embedding of \hat{y} into x , s.t.

- We instantiate the mode f with parameter $l = |u_m|$, leading to the function $f_l : \mathbb{B}^l \rightarrow \mathbb{B}^l$.
- We instantiate the strategy adapter \mathcal{S} with parameter y (and some other ones eventually). This instantiation leads to the strategy $S_y \in \llbracket 1; l \rrbracket^{\mathbb{N}}$.
- We iterate G_{f_l} with initial configuration (S_y, ϕ_m) .
- \hat{y} is the q -th term.

To summarize, iterations are realized on the LSCs of the host content (the mode gives the iterate function, the strategy-adapter gives its strategy), and the last computed configuration is re-injected into the host content, in place of the former LSCs.

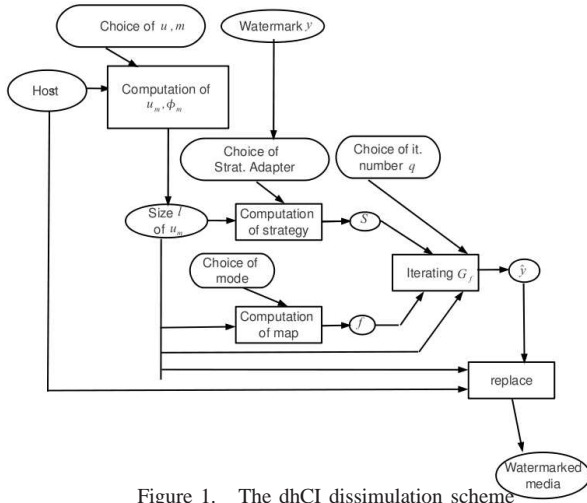


Figure 1. The dhCI dissimulation scheme

We are then left to show how to formally check whether a given digital media z results from the dissimulation of y into the digital media x .

Definition 9 (Marked content) Let $dec(u, m, M)$ be a decomposition function, f be a mode, \mathcal{S} be a strategy adapter, q be a positive natural number, and y be a digital media, $(u_M, u_m, u_p, \phi_M, \phi_m, \phi_p)$ be the image by $dec(u, m, M)$ of a digital media x . Then z is marked with y if the image by $dec(u, m, M)$ of z is $(u_M, u_m, u_p, \phi_M, \hat{y}, \phi_p)$ where \hat{y} is the right member of $G_{f_l}^q(S_y, \phi_m)$.

Various decision strategies are obviously possible to determine whether a given image z is marked or not, depending on the eventuality that the considered image may have been attacked. For example, a similarity percentage between x and z can be computed, and the result can be compared to a given threshold. Other possibilities are the use of ROC curves or the definition of a null hypothesis problem. The next section recalls some security properties and shows how the *dhCI dissimulation* algorithm verifies them.

IV. SECURITY ANALYSIS

Stego-security [8] is the highest security class in Watermark-Only Attack setup. 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 s.t. each host content has been marked with the same key K and the same embedding function.

Definition 10 (Stego-Security [8]) The embedding function is stego-secure if $\forall K \in \mathbb{K}, p(Y|K) = p(X)$ is established.

Let us prove that,

Theorem 1 Let ϵ be positive, l be any size of LSCs, $X \sim \mathbf{U}(\mathbb{B}^l)$, f_l be an image mode s.t. $\Gamma(f_l)$ is strongly connected and the Markov matrix associated to f_l is doubly stochastic. In the instantiated *dhCI dissimulation* algorithm with any uniformly distributed (u.d.) strategy-adapter which is independent from X , there exists some positive natural number q s.t. $|p(X^q) - p(X)| < \epsilon$.

Proof: Let $deci$ be the bijection between \mathbb{B}^l and $\llbracket 0, 2^l - 1 \rrbracket$ that associates the decimal value of any binary number in \mathbb{B}^l . The probability $p(X^t) = (p(X^t = e_0), \dots, p(X^t = e_{2^l-1}))$ for $e_j \in \mathbb{B}^l$ is thus equal to $(p(deci(X^t) = 0, \dots, p(deci(X^t) = 2^l - 1))$ further denoted by π^t . Let $i \in \llbracket 0, 2^l - 1 \rrbracket$, the probability $p(deci(X^{t+1}) = i)$ is

$$\sum_{j=0}^{2^l-1} \sum_{k=1}^l p(deci(X^t) = j, S^t = k, i =_k j, f_k(j) = i_k)$$

where $i =_k j$ is true iff the binary representations of i and j may only differ for the k -th element, and where i_k abusively denotes the k -th element of the binary representation of i .

Next, due to the proposition's hypotheses on the strategy, $p(deci(X^t) = j, S^t = k, i =_k j, f_k(j) = i_k)$ is equal to $\frac{1}{l} \cdot p(deci(X^t) = j, i =_k j, f_k(j) = i_k)$. Finally, since $i =_k j$ are $f_k(j) = i_k$ are constant during the iterative process and thus does not depend on X^t , we have

$$\pi_i^{t+1} = \sum_{j=0}^{2^l-1} \pi_j^t \cdot \frac{1}{l} \sum_{k=1}^l p(i =_k j, f_k(j) = i_k).$$

Since $\frac{1}{l} \sum_{k=1}^l p(i =_k j, f_k(j) = i_k)$ is equal to M_{ji} where M is the Markov matrix associated to f_l we thus have

$$\pi_i^{t+1} = \sum_{j=0}^{2^l-1} \pi_j^t M_{ji} \text{ and thus } \pi^{t+1} = \pi^t M.$$

First of all, since the graph $\Gamma(f)$ is strongly connected, then for all vertices i and j , a path can be found to reach j from i in at most 2^l steps. There exists thus $k_{ij} \in \llbracket 1, 2^l \rrbracket$ s.t. $M_{ij}^{k_{ij}} > 0$. As all the multiples $l \times k_{ij}$ of k_{ij} are such that $M_{ij}^{l \times k_{ij}} > 0$, we can conclude that, if k is the least common multiple of $\{k_{ij}/i, j \in \llbracket 1, 2^l \rrbracket\}$ thus $\forall i, j \in \llbracket 1, 2^l \rrbracket, M_{ij}^k > 0$ and thus M is a regular stochastic matrix.

Let us now recall the following stochastic matrix theorem:

Theorem 2 (Stochastic Matrix) *If M is a regular stochastic matrix, then M has an unique stationary probability vector π . Moreover, if π^0 is any initial probability vector and $\pi^{t+1} = \pi^t M$ for $t = 0, 1, \dots$ then the Markov chain π^t converges to π as t tends to infinity.*

Thanks to this theorem, M has an unique stationary probability vector π . By hypothesis, since M is doubly stochastic we have $(\frac{1}{2^l}, \dots, \frac{1}{2^l}) = (\frac{1}{2^l}, \dots, \frac{1}{2^l})M$ and thus $\pi = (\frac{1}{2^l}, \dots, \frac{1}{2^l})$. Due to the matrix theorem, there exists some q s.t. $|\pi^q - \pi| < \epsilon$ and the proof is established. ■

Since $p(Y|K)$ is $p(X^q)$ the method is then stego-secure.

Let us focus now on chaos-security properties. An information hiding scheme S is said to have such a property if its iterative process has a chaotic behavior, as defined by Devaney, on this topological space. This problem has been reduced in [11] which provides the following theorem.

Theorem 3 *Functions $f : \mathbb{B}^n \rightarrow \mathbb{B}^n$ such that G_f is chaotic according to Devaney, are functions such that the graph $\Gamma(f)$ is strongly connected.*

We immediatly deduce:

Corollary 1 *All the dhCI dissimulation algorithms follow hypotheses of theorem 1 are chaos-secure.*

V. INSTANTIATION OF STEGANOGRAPHIC METHODS

Theorem 1 relies on a u.d. strategy-adaptor that is independent from the cover, and on an image mode f_l whose iteration graph $\Gamma(f_l)$ is strongly connected and whose Markov matrix is doubly stochastic.

The CHS strategy adaptor [10] has the required properties: it does not depend on the cover, and the proof that its outputs are u.d. on $\llbracket 1, l \rrbracket$ is left as an exercise for the reader (a u.d. repartition is generated by the piecewise linear chaotic maps and is preserved by the iterative process). Finally, [12] has presented an iterative approach to generate image modes f_l such that $\Gamma(f_l)$ is strongly connected. Among these maps,

it is obvious to check which verifies or not the doubly stochastic constrain.

VI. CONCLUSION

This work has presented a new class of information hiding algorithms which generalizes algorithm [10] reduced to the negation mode. Its complete formalization has allowed to prove the stego-security and chaos security properties. As far as we know, this is the first time a whole class of algorithm has been proven to have these two properties.

In future work, our intention is to study the robustness of this class of dhCI dissimulation schemes. We are to find the optimized parameters (modes, strategy adapters, signification coefficients, iterations numbers...) giving the strongest robustness (depending on the chosen representation domain), theoretically and practically by realizing comprehensive simulations. Finally these algorithms will be compared to other existing ones, among other things by regarding whether these algorithms are chaotic or not.

REFERENCES

- [1] X. Wu, Z.-H. Guan, and Z. Wu, "A chaos based robust spatial domain watermarking algorithm," in *ISNN '07: 4th international symposium on Neural Networks*, ser. LNCS, vol. 4492. Springer, 2007, pp. 113–119.
- [2] Z. Liu and L. Xi, "Image information hiding encryption using chaotic sequence," in *KES '07: Knowledge-Based Intelligent Information and Engineering Systems*, ser. LNCS, vol. 4693. Springer, 2007, pp. 202–208.
- [3] J. Cong, Y. Jiang, Z. Qu, and Z. Zhang, "A wavelet packets watermarking algorithm based on chaos encryption," in *Computational Science and Its Applications ICCSA 2006, International Conference*, ser. LNCS, vol. 3980. Springer, 2006, pp. 921–928.
- [4] Z. Congxu, L. Xuefeng, and L. Zhihua, "Chaos-based multipurpose image watermarking algorithm," *Wuhan University Journal of Natural Sciences*, vol. 11, pp. 1675–1678, 2006.
- [5] X. Wu and Z.-H. Guan, "A novel digital watermark algorithm based on chaotic maps," *Physics Letters A*, vol. 365, no. 5-6, pp. 403 – 406, 2007.
- [6] A. Houmansadr, N. Kiyavash, and N. Borisov, "Rainbow: A robust and invisible non-blind watermark for network flows," in *NDSS'09: 16th Annual Network and Distributed System Security Symposium*, 2009.
- [7] G.S.El-Taweel, H. Onsi, M.Samy, and M. Darwish, "Secure and non-blind watermarking scheme for color images based on dwt," *ICGST International Journal on Graphics, Vision and Image Processing*, vol. 05, pp. 1–5, April 2005.
- [8] F. Cayre and P. Bas, "Kerckhoffs-based embedding security classes for woa data hiding," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 1–15, 2008.

- [9] I. J. Cox, S. Member, J. Kilian, F. T. Leighton, and T. Shamoan, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, pp. 1673–1687, 1997.
- [10] C. Guyeux, N. Friot, and J. M. Bahi, "Chaotic iterations versus spread-spectrum: Chaos and stego security," in *IIH-MSP '10: the 2010 Sixth International Conf. on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE, 2010, pp. 208–211.
- [11] C. Guyeux, "Le désordre des itérations chaotiques et leur utilité en sécurité informatique," Ph.D. dissertation, Université de Franche-Comté, 2010.
- [12] W. Qianxue, J. Bahi, J.-F. Couchot, and C. Guyeux, "Class of trustworthy pseudo-random number generators," in *INTER-NET'2011. The 3rd Int. Conf. on Evolving Internet*, 2011.