A new secure process for steganography: CI2. Stego and topological security

Nicolas Friot, Christophe Guyeux, Jacques Bahi

A new secure process for steganography: $\mathcal{CI}_2$

Stego-security and topological-security

Nicolas Friot[1], Christophe Guyeux[1], and Jacques M. Bahi[1]

Computer Science Laboratory LIFC
University of Franche-Comté
Besançon, France
http://lifc.univ-fcomte.fr/
-
nicolas.friot@lifc.univ-fcomte.fr
{christophe.guyeux, jacques.bahi}@univ-fcomte.fr

Abstract. In this paper is proposed a novel steganographic scheme based on chaotic iterations which offer a solution facing the main limitation of the previous one. This research work takes place into the information hiding security fields. We show that the proposed scheme is stego-secure, which is the highest level of security in a well defined and studied category of attack called "watermark-only attack". Additionally, we prove that this scheme presents topological properties so that it is one of the firsts able to face, at least partially, an adversary when considering the others categories of attacks defined in the literature.

Keywords: Steganography; Topology; Security; Chaotic Iterations

1 Introduction

Security is one of major concerns in the information hiding field. The security is defined in [7] as follows: "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."

In this field, it has been realized in [4] a classification of attacks into categories, according to the type of information the attacker has access to. One of the well known class is called Watermark Only Attack (WOA). Several levels of security have been recently defined in these setups. The highest level of security in this framework is called stego-security [3], whereas topological-security tends to improve the ability to withstand attacks in other setups [6].

To the best of our knowledge, there exist only two information hiding schemes that are both stego-secure and chaos-secure [3, 6] in some conditions. The first one called Natural Watermarking is based on a spread spectrum technique. Unfortunately, this scheme is neither robust, nor able to face an attacker in other setups than WOA, due to its lack of a topological properties[6]. The second one is based on chaotic iterations [1]. However, it allows to embed securely only one

bit per host content, which constitute the main limitation of this scheme. This is a one-bit-watermarking process.

This document has for main objective to present the interest of our research works accepted in the conference on Security and Cryptography Secrypt 2011 in Sevilla in Spain. Its main aim is to present a new process based on chaotic iterations which is stego-secure and topologically-secure too, and offer a solution to bypass the limitation of the previous one and so allow to embed securely more than one bit. This will be a real steganographic process.

The rest of this document is organized in the following way: in Section 2 it is down a reminder information hiding security. In Section 3 the new algorithm is presented. This documents ends by a conclusion section 4 where our contribution is summarized and intended future researches are presented.

2 Data hiding security

2.1 Classification of Attacks

In the steganography framework, attacks have been classified in [3] in several classes: Watermark-Only Attack (WOA) when an attacker has only access to several watermarked contents, Known-Message Attack (KMA) when an attacker has access to several pairs of watermarked contents and corresponding hidden messages, Known-Original Attack (KOA) when an attacker has access to several pairs of watermarked contents and their corresponding original versions, and Constant-Message Attack (CMA) when the attacker observes several watermarked contents and only knows that the unknown hidden message is the same in all contents.

2.2 Stego-Security

The stego-security is defined in the framework of the Simmons' [8] prisoner problem. It is the highest security level in WOA setup [3]. To remind it, we need the following notations: $\mathbb{K}$ is the set of embedding keys, $p(X)$ is the probabilistic model of N_0 initial host contents, and $p(Y|K_1)$ is the probabilistic model of N_0 watermarked contents. Furthermore, it is supposed in this context that each host content has been watermarked with the same secret key K_1 and the same embedding function e.

Definition 1 (Stego-Security). *The embedding function e is* stego-secure *if and only iff:* $\forall K_1 \in \mathbb{K}, p(Y|K_1) = p(X)$.

2.3 Topological-Security

To check whether an information hiding scheme S is topological-secure or not, S must be written as an iterate process $x^{n+1} = f(x^n)$ on a metric space $(\mathcal{X}, d)$. This formulation is always possible [2]. So,

Definition 2 (Topological-Security). *An information hiding scheme S is said to be topological-secure on $(\mathcal{X}, d)$ if its iterative process f check the three following topological properties:*

- ***Transitivity:*** *iff, for any pair of open sets $U, V \subset \mathcal{X}$, there exists $k > 0$ such that $f^k(U) \cap V \neq \varnothing$.*
- ***Regularity:*** *iff the set of periodic points of f is dense in $\mathcal{X}$.*
- ***Sensitivity:*** *iff there exists $\delta > 0$ such that, for any $x \in \mathcal{X}$ and any neighborhood V of x, there exist $y \in V$ and $n \geqslant 0$ such that $d\left(f^n(x), f^n(y)\right) > \delta$. ($\delta$ is called the* constant of sensitivity *of f).*

In the approach presented by Guyeux *et al.*, a data hiding scheme is secure if it is unpredictable. Its iterative process must satisfy the three topological properties and its level of topological-security increases with the number of other topological properties satisfied by it.

This new concept of security for data hiding schemes has been proposed in [2] as a complementary approach to the existing framework. It contributes to the reinforcement of confidence into existing secure data hiding schemes. Additionally, the study of security in KMA, KOA, and CMA setups is realizable in this context. Finally, this framework can replace stego-security in situations that are not encompassed by it. In particular, this framework is more relevant to give evaluation of data hiding schemes claimed as chaotic.

3 The improved algorithm: $\mathcal{CI}_2$

To describe $\mathcal{CI}_2$ we need the following notations: $x^0 \in \mathbb{B}^{\mathsf{N}}$ is the N LSCs (as defined in Figure 1 on the following page) of a given cover media C, $m^0 \in \mathbb{B}^{\mathsf{P}}$ is the watermark to embed into x^0, $S_p \in \mathbb{S}_N$ is a strategy called *place strategy*, $S_c \in \mathbb{S}_P$ is a strategy called *choice strategy*, and $S_m \in \mathbb{S}_P$ is a strategy called *mixing strategy*. So our information hiding scheme denoted by $\mathcal{CI}_2$ is defined by:

$$x_i^n = \begin{cases} x_i^{n-1} & \text{if } S_p^n \neq i \\ m_{S_c^n} & \text{if } S_p^n = i. \end{cases} \text{ and } m_j^n = \begin{cases} m_j^{n-1} & \text{if } S_m^n \neq j \\ \overline{m_j^{n-1}} & \text{if } S_m^n = j. \end{cases} \text{ with } \begin{cases} n \in \mathbb{N}^* \\ i \in [\![0; \mathsf{N}-1]\!] \\ j \in [\![0; \mathsf{P}-1]\!] \end{cases}$$

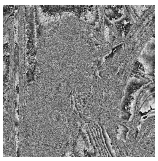
where $\overline{m_j^{n-1}}$ is the boolean negation of m_j^{n-1}, and the stego-content is $y = x^P$.

It has been described in details in [5] how to model the new process $\mathcal{CI}_2$ as a discreet dynamical system (an iterative process) $\mathcal{G}_{f_0}$ in a topological space, and in the same work it has been proven that:

Theorem 1. *$\mathcal{CI}_2$ is stego-secure and topologically-secure.*

(a) MSCs of Lena.
The richest part of Lena.

(b) Original Lena.



(c) LSCs of Lena ($\times 17$)
Details of Lena.
Can be altered without damages.

Fig. 1: Most and least significant coefficients of Lena. (MSCs and LSCs)

4 Conclusion and future works

In this research work, a new information hiding scheme has been introduced. It is topological-secure and stego-secure, and thus is able to withstand attacks in Watermark-Only Attack (WOA) and Constant-Message Attack (CMA) setups. These results have been obtained after having studied the topological behavior of this data hiding scheme. To the best of our knowledge, this algorithm is the third scheme that has been proven to be secure, according to the information hiding security field. In future work, we intend to study the robustness of this scheme, and to compare it with the two other secure algorithms. Additionally, we will investigate the topological properties of our scheme, to see whether it is secure in KOA and KMA setups.

References

1. Jacques Bahi and Christophe Guyeux. A new chaos-based watermarking algorithm. In *SECRYPT 2010, International conference on security and cryptography*, Athens, Greece, 2010. To appear.
2. Jacques M. Bahi and Christophe Guyeux. A chaos-based approach for information hiding security. arXiv N^o 0034939, April 2010.
3. Francois Cayre, Caroline Fontaine, and Teddy Furon. Kerckhoffs-based embedding security classes for woa data hiding. *IEEE Transactions on Information Forensics and Security*, 3(1):1–15, 2008.
4. Franois Cayre, Caroline Fontaine, and Teddy Furon. Watermarking security: theory and practice. *IEEE Transactions on Signal Processing*, 53(10):3976–3987, 2005.
5. Nicolas Friot, Christophe Guyeux, and Jacques Bahi. Chaotic iterations for steganography - stego-security and chaos-security. In *SECRYPT'2011, Int. Conf. on Security and Cryptography*, pages ***–***, Sevilla, Spain, July 2011. To appear.
6. 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.
7. T. Kalker. Considerations on watermarking security. pages 201–206, 2001.
8. Gustavus J. Simmons. The prisoners' problem and the subliminal channel. In *Advances in Cryptology, Proc. CRYPTO'83*, pages 51–67, 1984.