A NEW CHAOS-BASED WATERMARKING ALGORITHM

Christophe Guyeux, Jacques M. Bahi
Computer Science Laboratory, University of Franche-Comté (LIFC)
Rue Engel-Gros, BP 527, 90016 Belfort Cedex, France
christophe.guyeux@univ-fcomte.fr, jacques.bahi@univ-fcomte.fr

Keywords: Watermarking, Chaotic iterations, Topological chaos, Information hiding.

Abstract: This paper introduces a new watermarking algorithm based on discrete chaotic iterations. After defining some coefficients deduced from the description of the carrier medium, chaotic discrete iterations are used to mix the watermark and to embed it in the carrier medium. It can be proved that this procedure generates topological chaos, which ensures that desired properties of a watermarking algorithm are satisfied.

1 INTRODUCTION

Information hiding has recently become a major security technology, especially with the increasing importance and widespread distribution of digital media through the Internet. It includes several techniques, among which is digital watermarking. The aim of digital watermarking is to embed a piece of information into digital documents, like pictures or movies for example. This is for a large panel of reasons, such as: copyright protection, control utilization, data description, integrity checking, or content authentication. Digital watermarking must have essential characteristics including imperceptibility and robustness against attacks. Many watermarking schemes have been proposed in recent years, which can be classified into two categories: spatial domain (Wu et al., 2007) and frequency domain watermarking (Cong et al., 2006), (Dawei et al., 2004). In spatial domain watermarking, a great number of bits can be embedded without inducing too clearly visible artifacts, while frequency domain watermarking has been shown to be quite robust against JPEG compression, filtering, noise pollution, and so on. More recently, chaotic methods have been proposed to encrypt the watermark, or embed it into the carrier image for security reasons.

In this paper, a new watermarking algorithm is given. It is based on the commonly named chaotic iterations and on the choice of relevant coefficients deduced from the description of the carrier medium. This new algorithm consists of two basic stages: a mixture stage and an embedding stage. At each of these two stages, the proposed algorithm offers additional steps that allow the authentication of relevant information carried by the medium or the extraction of the watermark without knowledge about the original image.

This paper is organized as follows: firstly, some basic definitions concerning chaotic iterations is recalled. Then, the new chaos-based watermarking algorithm is introduced in Section 3. Section 4 is constituted by the evaluation of our algorithm: a case study is presented, some classical attacks are executed and the results are presented and commented on. The paper ends by a conclusion section where our contribution is summarized, and planned future work is discussed.

2 BASIC RECALLS: CHAOTIC ITERATIONS

In the sequel S^n denotes the n^{th} term of a sequence S, V_i denotes the i^{th} component of a vector V and $f^k = f \circ ... \circ f$ denotes the k^{th} composition of a function f. Finally, the following notation is used: $[\![1;N]\!] = \{1,2,\dots,N\}$.

Let us consider a *system* of a finite number N of *cells*, so that each cell has a boolean *state*. Then a sequence of length N of boolean states of the cells corresponds to a particular *state of the system*. A sequence which elements belong in $[\![1;\mathsf{N}]\!]$ is called a *strategy*. The set of all strategies is denoted by $\mathbb{S}$.

Definition 1 Let $S \in \mathbb{S}$. The *shift* function is defined by $\sigma : (S^n)_{n\in\mathbb{N}} \in \mathbb{S} \longrightarrow (S^{n+1})_{n\in\mathbb{N}} \in \mathbb{S}$ and the *initial function* i is the map which associates to a sequence, its first term: $i : (S^n)_{n\in\mathbb{N}} \in \mathbb{S} \longrightarrow S^0 \in [\![1;\mathsf{N}]\!]$.

Definition 2 The set $\mathbb{B}$ denoting $\{0,1\}$, let $f : \mathbb{B}^{\mathsf{N}} \longrightarrow \mathbb{B}^{\mathsf{N}}$ be a function and $S \in \mathbb{S}$ be a strategy. Then, the so-called *chaotic iterations* are defined by $x^0 \in \mathbb{B}^{\mathsf{N}}$ and $\forall n \in \mathbb{N}^*, \forall i \in [\![1;\mathsf{N}]\!]$,

$$x_i^n = \begin{cases} x_i^{n-1} & \text{if } S^n \neq i \\ \left(f(x^{n-1})\right)_{S^n} & \text{if } S^n = i. \end{cases} \quad (1)$$

3 A NEW CHAOS-BASED WATERMARKING ALGORITHM

3.1 Most and Least Significant Coefficients

Let us first introduce the definitions of most and least significant coefficients of an image.

Definition 3 For a given image, the most significant coefficients (in short MSCs), are coefficients that allow the description of the relevant part of the image, *i.e.* its most rich part (in terms of embedding information), through a sequence of bits.

For example, in a spatial description of a grayscale image, a definition of MSCs can be the sequence constituted by the first three bits of each pixel.

Definition 4 By least significant coefficients (LSCs), we mean a translation of some insignificant parts of a medium in a sequence of bits (insignificant can be understand as: "which can be altered without sensitive damages").

The LSCs are used during the embedding stage: some of the least significant coefficients of the carrier image will be chaotically chosen and replaced by the bits of the (possibly mixed) watermark.

The MSCs are only useful in case of authentication, mixture and embedding stages will then depend on them. Hence, a coefficient should not be defined at the same time both as a MSC and a LSC: the LSC can be altered, while the MSC is needed to extract the watermark (in case of authentication).

3.2 Stages of the Algorithm

Our watermarking scheme consists of two classical stages: the mixture of the watermark and its embedding into a cover image.

3.2.1 Watermark mixture

For security reasons, the watermark can be mixed before its embedding. A common way to achieve this stage is to use the bitwise exclusive or (XOR), for example, between the watermark and a logistic map. In this paper, we will introduce a mixture scheme based on chaotic iterations. Its chaotic strategy will be highly sensitive to the MSCs, in case of an authenticated watermark (Bahi and Guyeux, 2010). For the details of this stage see the Paragraph 4.1.2 in Section 4.

3.2.2 Watermark Embedding

This stage can be done either by applying the logical negation of some LSCs, or by replacing them by the bits of the possibly mixed watermark.

To choose the sequence of LSCs to be changed, a number of integers, less than or equals to the number N of LSCs, corresponding to a chaotic sequence $\left(U^k\right)_k$, is generated from the chaotic strategy used in the mixture stage and possibly the watermark. Thus, the U^k-th least significant coefficient of the carrier image is either switched, or substituted by the k^{th} bit of the possibly mixed watermark. In case of authentication, such a procedure leads to a choice of the LSCs which are highly dependent on the MSCs.

On the one hand, when the switch is chosen, the watermarked image is obtained from the original image, whose LSCs $L = \mathbb{B}^{\mathsf{N}}$ are replaced by the result of some chaotic iterations. Here, the iterate function is the vectorial boolean negation, defined by $f_0 : \mathbb{B}^{\mathsf{N}} \longrightarrow \mathbb{B}^{\mathsf{N}}, (x_1,\ldots,x_{\mathsf{N}}) \longmapsto (\overline{x_1},\ldots,\overline{x_{\mathsf{N}}})$, the initial state is L and strategy is equal to $\left(U^k\right)_k$. In this case, it is possible to prove that the whole embedding stage satisfies topological chaos properties (Bahi and Guyeux, 2010), but the original medium is needed to extract the watermark.

On the other hand, when the selected LSCs are substituted by the watermark, its extraction can be done without the original cover. In this case, the selection of LSCs still remains chaotic, because of the use of a chaotic map, but the whole process does not satisfy topological chaos (Bahi and Guyeux, 2010): the use of chaotic iterations is reduced to the mixture of the watermark. See the Paragraph 4.1.3 in Section 4 for more details.

3.2.3 Extraction

The chaotic sequence U^k can be regenerated, even in the case of an authenticated watermarking: the MSCs have not been changed during the stage of embedding watermark. Thus, the altered LSCs can be found. So, in case of substitution, the mixed watermark can be rebuilt and "decrypted". In case of negation, the result of the previous chaotic iterations on the watermarked image, is the original image.

If the watermarked image is attacked, then the MSCs will change. Consequently, *in case of authentication* and due to the high sensitivity of the embedding sequence, the LSCs designed to receive the watermark will be completely different. Hence, the result of the decrypting stage of the extracted bits will have no similarity with the original watermark.

4 A CASE STUDY

4.1 Stages and Details

4.1.1 Images Description

Carrier image is the famous Lena, which is a 256 grayscale image and the watermark is the 64×64 pixels binary image depicted in Fig. 1a. The embedding domain will be the spatial domain. The selected MSCs are the four most significant bits of each pixel and the LSCs are the three following bits (a given pixel will at most be modified by four levels of gray by an iteration). The last bit is then not used. Lastly, LSCs of Lena are substituted by the bits of the mixed watermark.

(a) Watermark. (b) Watermarked Lena.

Figure 1: Watermark and watermarked Lena.

4.1.2 Mixture of the Watermark

The initial state x^0 of the system is constituted by the watermark, considered as a boolean vector. The iteration function is the vectorial logical negation f_0 and the chaotic strategy $(S^k)_{k\in\mathbb{N}}$ will depend on whether an authenticated watermarking method is desired or not, as follows. A chaotic boolean vector is generated by a number T of iterations of a logistic map ((μ, U_0) parameters will constitute the private key). Then, in case of unauthenticated watermarking, the bits of the chaotic boolean vector are grouped six by six, to obtain a sequence of integers lower than 64, which will constitute the chaotic strategy. In case of authentication, the bitwise exclusive or (XOR) is made between the chaotic boolean vector and the MSCs and the result is converted into a chaotic strategy by joining its bits as above. Thus, the mixed watermark is the last boolean vector generated by the chaotic iterations.

4.1.3 Embedding of the Watermark

To embed the watermark, the sequence $(U^k)_{k\in\mathbb{N}}$ of altered bits taken from the M LSCs must be defined. To do so, the strategy $(S^k)_{k\in\mathbb{N}}$ of the mixture stage is used as follows

$$\left\{ \begin{array}{lll} U^0 & = & S^0 \\ U^{n+1} & = & S^{n+1} + 2 \times U^n + n \pmod{\mathsf{M}}. \end{array} \right. \tag{2}$$

To obtain the result depicted in Fig. 1b.

Remark that the map $\theta \mapsto 2\theta$ of the torus, which is a famous example of topological Devaney's chaos (**?**), has been chosen to make $(U^k)_{k\in\mathbb{N}}$ highly sensitive to the chaotic strategy. As a consequence, $(U^k)_{k\in\mathbb{N}}$ is highly sensitive to the alteration of the MSCs: in case of authentication, any significant modification of the watermarked image will lead to a completely different extracted watermark.

4.2 Simulation Results

To prove the efficiency and the robustness of the proposed algorithm, some attacks are applied to our chaotic watermarked image. For each attack, a similarity percentage with the watermark is computed, this percentage is the number of equal bits between the original and the extracted watermark.

4.2.1 Zeroing Attack

In this kind of attack, some pixels of the image are put to 0. In this case, the results in Table 1 have been obtained. We can conclude that in case of unauthentication, the watermark still remains after a cropping attack: the desired robustness is reached. In case of authentication, even a small change of the carrier image leads to a very different extracted watermark. In

UNAUTHENTICATION		AUTHENTICATION	
Size (pixels)	Similarity	Size (pixels)	Similarity
10	99.08%	10	89.81%
50	97.31%	50	54.54%
100	92.43%	100	52.24%

Table 1: Zeroing attacks.

UNAUTHENTICATION		AUTHENTICATION	
Angle	Similarity	Angle	Similarity
5	94.67%	5	59.47%
10	91.30%	10	54.51%
25	80.85%	25	50.21%

Table 2: Rotation attacks.

this case, any attempt to alter the carrier image will be signaled.

4.2.2 Rotation Attack

Let r_θ be the rotation of angle θ around the center $(128,128)$ of the carrier image. So, the transformation $r_{-\theta} \circ r_\theta$ is applied to the watermarked image. The good results in Table 2 are obtained.

4.2.3 JPEG Compression

A JPEG compression is applied to the watermarked image, depending on a compression level. Let us notice that this attack leads to a change of the representation domain (from spatial to DCT domain). In this case, the results in Table 3 have been found. A good authentication through JPEG attack is obtained. As for the unauthentication case, the watermark still remains after a compression level equal to 10. This is a good result if we take into account the fact that we use spatial embedding.

4.2.4 Gaussian Noise

Watermarked image can be also attacked by the addition of a Gaussian noise, depending on a standard deviation. In this case, the results in Table 4 have been found.

UNAUTHENTICATION		AUTHENTICATION	
Ratio	Similarity	Ratio	Similarity
2	82.95%	2	54.39%
5	65.23%	5	53.46%
10	60.22%	10	50.14%

Table 3: JPEG compression attacks.

UNAUTHENTICATION		AUTHENTICATION	
Standard dev.	Similarity	Standard dev.	Similarity
1	74.26%	1	52.05%
2	63.33%	2	50.95%
3	57.44%	3	49.65%

Table 4: Gaussian noise attacks.

5 DISCUSSION AND FUTURE WORK

In this paper, a new way to generate watermarking methods is proposed. The new procedure depends on a general description of the carrier medium to watermark, in terms of the significance of some coefficients we called MSC and LSC. Its mixture and also the selection of coefficients to alter are based on chaotic iterations, which generate topological chaos in the sense of Devaney. Thus, the proposed algorithm possesses expected desirable properties for a watermarking algorithm. For example, strong authentication of the carrier image, security, resistance to attacks, and discretion.

The algorithm has been evaluated through attacks and the results expected by our study have been experimentally obtained. The aim was not to find the best watermarking method generated by our general algorithm, but to give a simple illustrated example to prove its feasibility. In future work, other choices of iteration functions and chaotic strategies will be explored. They will be compared in order to increase authentication and resistance to attacks. Lastly, frequency domain representations will be used to select the MSCs and LSCs.

REFERENCES

Bahi, J. and Guyeux, C. (2010). Topological chaos and chaotic iterations, application to hash functions. In *WCCI'10, IEEE World Congress on Computational Intelligence*, pages ***–***, Barcelona, Spain. To appear.

Cong, J., Jiang, Y., Qu, Z., and Zhang, Z. (2006). A wavelet packets watermarking algorithm based on chaos encryption. *Lecture Notes in Computer Science*, 3980:921–928.

Dawei, Z., Guanrong, C., and Wenbo, L. (2004). A chaos-based robust wavelet-domain watermarking algorithm. *Chaos, Solitons and Fractals*, 22:47–54.

Devaney, R. L. (2003). *An Introduction to Chaotic Dynamical Systems, 2nd Edition*. Westview Pr.

Wu, X., Guan, Z.-H., and Wu, Z. (2007). A chaos based robust spatial domain watermarking algorithm. *Lecture Notes in Computer Science*, 4492:113–119.