Applied Soft Computing 21 (2014) 481–490

Contents lists available at ScienceDirect

Applied Soft Computing

journal homepage: www.elsevier.com/locate/asoc

Design and implementation of coupled chaotic maps in watermarking

S. Behnia [a,*], S. Ahadpour [b], P. Ayubi [c]

[a] Department of Physics, Urmia University of Technology, Orumieh, Iran
[b] Department of Physics, University of Mohaghegh Ardabili, Ardabil, Iran
[c] Department of Computer Engineering, Islamic Azad University, Urmia Branch, Urmia, Iran

ARTICLE INFO

Article history:
Received 22 May 2011
Received in revised form 17 March 2014
Accepted 22 March 2014
Available online 18 April 2014

PACS:
05.45.Jn
05.45.Ra
05.45.Xt
65.40.Gr

Keywords:
Digital image watermarking
Chaotic map
Coupled map lattice
Ergodic theory

ABSTRACT

The present paper proposes a multidimensional coupled chaotic map as a pseudo random number generator. Based on an introduced dynamical systems, a watermark scheme is presented. By modifying the original image and embedding a watermark in the difference values within the original image, the proposed scheme overcomes the problem of embedding a watermark in the spatial domain. As the watermark extraction does not require the original image, the introduced model can be employed for practical applications. This algorithm tries to improve the problem of failure of embedding in small key space, embedding speed and level of security.

1. Introduction

Watermarking technique is one of the active research fields in recent years, which can be used in protection of multimedia information, content authentication, and so on. The two well-known research branches and applications in digital watermarking are fragile and semi-fragile watermarking [28,40,14]. In authentication watermarking, tamper localization and detection accuracy are two major issues. However, most methods in literature have not presented precise localization. A watermark typically contains information about origin, status, and/or destination of the host data [9,41,32]. Image scrambling is one of the most prevailing encryption algorithms these years [15,37,43,12]. However, the methods of scrambling are limited. By now most of the proposed watermarking schemes have used watermarks generated from pseudo random number sequences [19]. On the other hand, chaotic functions such as Markov Maps, Bernoulli Maps, Skew Tent Map and Logistic Map have been widely used to generate watermark sequences [3,29,30]. These types of watermark generation schemes require two values (the initial value and the function seed value) to recreate the same watermark at a later stage. An advantage of these watermarks is the possibility of analyzing and controlling the watermark spectral properties.

A watermark should be robust. That is, it should survive classic content processing. It should also remain imperceptible and convey as much information as possible. For real-time applications, it should have low complexity embedding and retrieval processes [38,20].

The present paper concentrates typically on the security of watermarking (key space) [13,24]. Specifically it aims at proposing a secure watermarking scheme based on spatiotemporal chaos. In order to enhance the security in watermarking process, spatiotemporal chaos is employed to select both the embedding positions for each watermark bit and for watermark encryption. In this article, a watermarking algorithm based on a multidimensional coupled chaotic map is proposed. The dimension of the introduced dynamical system regarding the level of the security and the extra dimension can be used to apply many logos in watermarking process.

The paper is organized as follows. Section 2 describes chaotic maps and the location of embedding position of watermark. Section 3 presents the synchronization condition and the ergodicity of the introduced model. The section studies the chaotic domain of the introduced model through Lyapunov exponents to generate

* Corresponding author. Tel.: +98 9141468515.
E-mail address: s.behnia@sci.uut.ac.ir (S. Behnia).

http://dx.doi.org/10.1016/j.asoc.2014.03.022
1568-4946/

the key space. The watermarking scheme based on chaotic maps is proposed in Section 4. The selected example and the simulation results are discussed in Sections 4 and 5. Section 6 concludes the paper.

2. Definition of model

The chaotic sequences exhibit some important characteristics. any change in control parameter of chaotic maps such as Logistic and Chebyshev maps can produce white-noise-like sequences [24,6,25]. For enhancing the security of discrete chaotic watermarking the paper introduces for the first time, the concept of using multidimensional coupled chaotic map with an invariant measure in watermarking (See Appendix A). Certain characteristics of our introduced watermarking method, make it distinctive compared to the other schemes.

These characteristics can be stated as follows:

- Presenting very large number of fully developed chaotic maps.
- Having complexity due to high dimensionality and chaoticity.
- Having large key space; It is obvious that the attack complexity is determined by the size of the key space and the complexity of the verification of each key.
- Having flexibility in attributing different values to the control parameters and the coupling parameter.

The multidimensional coupled chaotic map can be defined as:

$$\Phi = \begin{cases} x_1(n+1) = F(x_1(n), \ldots, x_N(n)) = \epsilon_1 f_1(x_1(n)) + \ldots + \epsilon_N f_N(x_N(n)) \\ \vdots \\ x_N(n+1) = F(x_1(n), \ldots, x_N(n)) = \epsilon_1 f_1(x_N(n)) + \ldots + \epsilon_N f_{N-1}(x_{N-1}(n)) \end{cases} \quad (1)$$

where, ϵ is the strength of the coupling $\{\epsilon_1 + \ldots + \epsilon_N = 1\}$. We introduce our map ensemble $\{f\}$ based on the one-parameter families of chaotic maps $\Phi_N(x, \alpha)$ with an invariant measure. They can be defined as the ratio of polynomials of degree N (see Appendix A). In fact, there is a multidimensional dynamical system which has the property of possessing an invariant measure at synchronized state [21].

3. Key space

Key space can be generated by control parameters and the initial conditions of chaotic maps. Many properties of the chaotic systems have their corresponding counterparts in traditional cryptosystems, such as: ergodicity and confusion, sensitivity to initial conditions, control parameter, and diffusion [26,27]. In this section, the ergodicity is explored by calculating the invariant measure. The Lyapunov exponents are also calculated to verify the chaotic domain. By considering the chaotic domain of the multidimensional coupled chaotic maps, the key space is arranged. One possibility to have an ergodic coupled map is to synchronize the introduced dynamical model.

Synchronization of two (or more) chaotic dynamical systems (starting with different initial conditions) means that their chaotic trajectories remain in step with each other during the temporal evolution. The key concept of complete synchronization refers to a state where the trajectories of dynamical systems approach each other[4,39]. The introduced model has a fast speed and robust synchronization properties.

3.1. Invariant measure

For multidimensional coupled chaotic map, we have tried to describe ergodicity from the invariant measure point of view [16,10]. Sinai–Ruelle–Bowen (SRB) is a measure which describes the ergodic properties with respect to typical initial conditions [16,11]. The difficulty in rigorous proving that a given coupled map exhibits spatio-temporal chaos lies in finding such an SRB measure.

Each symmetric transformation for generic model Eq. (1) should have the invariant measure. The suitable condition for the presentation of the invariant measure of the synchronized coupled map is choosing a one-dimensional map with an invariant measure as introduced in our previous paper [21]. We can rewrite the Frobenius–Perron (FP) integral for multidimensional coupled chaotic map as follows [16,11]:

$$\mu(x_1(n+1), \ldots, x_N(n+1)) = \int dx_1 \ldots \int dx_N \delta(x_1(n+1) - F_1(x_1(n), \ldots, x_N(n))) \ldots \delta(x_N(n+1) - F_N(x_1(n), \ldots, x_N(n)))\mu(x_1(n), \ldots, x_N(n)),$$

We will show that the invariant measure at synchronized state has the following form:

$$\mu(x_1, \ldots, x_N) = \delta(x_2 - x_1) \ldots \delta(x_N - x_1)\mu(x_1) \quad (2)$$

Relation 2 shows invariance under the permutation of synchronization coordinate $(x_1, x_2, \ldots)$, therefore, the measure is invariant at transverse direction and the stable direction follows $\mu(x_1)$. By considering the complete synchronization, the (FP) integral for multidimensional coupled chaotic map can be written as:

$$\mu = \int dx_1 \ldots \int dx_N \delta(x_1(n+1) - F_1(x_1(n), \ldots, x_N(n)))\delta(x_N(n+1) - F_N(x_1(n), \ldots, x_N(n))) \times \delta(x_2(n) - x_1(n)) \ldots \delta(x_N(n) - x_1(n))\mu(x_1),$$

which can be reduced to:

$$\mu = \delta(x_2(n+1) - x_1(n+1)) \ldots, \delta(x_N(n+1) - x_1(n+1)) \times \int dx_1 \delta(x_1(n+1) - F_1(x_1(n), \ldots, x_1(n)))\mu(x_1(n)),$$

Now, if the one-dimensional map $x(n+1) = F(x_1(n), \ldots x_1(n))$ possesses the invariant measure $\mu(x_1(n))$, then it satisfies:

$$\mu(x(n+1)) = \int \delta(x(n+1) - F(x_1(n), \ldots, x_1(n)) d\mu(x_1), \quad (3)$$

Then, we have:

$$\mu(x_1(n+1), \ldots, x_N(n+1)) = \delta(x_1(n+1) - x_2(n+1)), \ldots, \delta(x_N(n+1) - x_1(n+1))\mu(x_1(n+1)). \quad (4)$$

3.2. Lyapunov exponent spectra

The following properties make a deterministic algorithm suitable to generate a pseudo random sequence of numbers: high value of entropy, high dimensionality of the parent dynamical system, and very large period of the generated sequence [22,18,8]. There is a close correlation between the Lyapunov exponent of the underlying chaotic map and the "randomness". Since randomness is desired to be seen on a random number generator clearly, it must be correlated with the diverging nature of the trajectories of a chaotic map, which is tied to the existence of a positive Lyapunov exponent.

A spectrum of all the Lyapunov exponents with respect to the synchronization solution can be evaluated in a way similar to that of one-dimensional local maps [16,17]. At synchronized state, the Lyapunov exponents Λ_k of multidimensional