Commun Nonlinear Sci Numer Simulat 15 (2010) 2469–2478

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

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

Multiple-watermarking scheme based on improved chaotic maps

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

[a] *Department of Physics, IAU, Ourmia, Iran*
[b] *Department of Elec. Eng., K.N Toosi University Technology, Tehran, Iran*
[c] *Department of Computer, IAU, Ourmi, Iran*

ARTICLE INFO

Article history:
Received 29 June 2009
Accepted 29 September 2009
Available online 8 October 2009

Keywords:
Pair-coupled maps
Pseudo random sequence
Ergodic theory
Robustness
Digital signature image
Key space
security

ABSTRACT

In this letter a new watermarking scheme for color image is proposed based on a family of the pair-coupled maps. Pair-coupled maps are employed to improve the security of watermarked image, and to encrypt the embedding position of the host image. Another map is also used to determine the pixel bit of host image for the watermark embedding. The purpose of this algorithm is to improve the shortcoming of watermarking such as small key space and low security. Due to the sensitivity to the initial conditions of the introduced pair-coupled maps, the security of the scheme is greatly improved.

1. Introduction

The majority of watermarking schemes proposed to date, use watermarks which are generated from pseudo random number sequences [1–3]. Chaotic oscillators with positive Lyapunov exponents can be viewed as information sources [3,4]. Previously, it has been demonstrated that an information signal can be encoded in the symbolic dynamics of a chaotic oscillator [5,6]. Recent works have introduced the application of chaotic functions such as Markov Maps, Bernoulli Maps, Skew Tent Map, Logistic Map [7–9]. Although theses maps have perfect dynamical properties and can be realized simply in both hardware and software with a widespread usage [10,11] but there are fundamental drawbacks in these chaotic cryptosystems, such as small key space, slow performance and weak security function [12,13].

Considering a symmetric two-dimensional map which possesses invariant measure in its diagonal and anti-diagonal invariant sub-manifolds, we have been able to propose a pair-coupled map that possesses ergodic property [14] at synchronized states [15,16].

Entropy and the Lyapunov exponents were calculated, at synchronized state. We propose a secure watermarking scheme based on the pair-coupled map. In order to enhance the security, chaos is employed to select the embedding positions for each watermark bit and for watermark encryption. The introduced dynamical system with the level of the security proposed can be applied to many logos in watermarking process. An advantage of these watermarks is the possibility to analyze and control their spectral properties.

* Corresponding author. Tel.: +98 441 3458902; fax: +98 441 3460980.
E-mail address: s.behnia@iaurmia.ac.ir (S. Behnia).

1007-5704/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.cnsns.2009.09.042

The rest of the Letter is organized as follows. Section 2 describes chaotic maps and the location of embedding position of watermark. In Section 3, the chaotic domain of the introduced model is studied via Lypaunov exponents in order to generate the key space. The watermarking scheme based on chaotic maps is proposed in Section 4. Also, the selected example and simulation results are discussed in Section 5. Section 6 is the conclusion. Two appendices are also provided, which contain all algebraic calculations and proofs.

2. Coupled maps

Coupled map lattices are arrays of states whose values are continuous, usually within the unit interval, or discrete space and time [17]. The pair-coupled map with ergodic behavior can be considered as a two-dimensional dynamical map defined as [18]:

$$\Phi(X,Y)=\begin{cases} X=F(x,y)=[(1-\epsilon)(f_1(x))^P+\epsilon(f_2(y))^P]^{\frac{1}{P}} \\ Y=F(y,x)=[(1-\epsilon)(f_1(y))^P+\epsilon(f_2(x))^P]^{\frac{1}{P}} \end{cases} \tag{1}$$

where, in general, P is an arbitrary parameter, ϵ the strength of the coupling, and the functions $f_1(x),\ f_2(x)$ are two arbitrary one-dimensional maps. Obviously, by choosing $P=1$, we get ordinary linearly coupled maps. But, in order to have a two-dimensional dynamical system associated with the pair-coupled map with the property of possessing an invariant measure at synchronized state [19,20], one needs to choose P as an arbitrary integer and the functions $(f_1(x), f_2(x))$ as measurable dynamical systems (see Appendix A). At completely synchronized state $x=y$, the pair-coupled map by considering A.1 reduces to:

$$X=F(x,x)=\bar{a}(\epsilon,a_1,a_2)\tan^2(N\arctan(\sqrt{x})) \tag{2}$$

with $\bar{a}(\epsilon,a_1,a_2)=((1-\epsilon)a_1^P+\epsilon a_2^P)^{\frac{1}{P}}$ which is discussed latter (see (B.6) and Appendix B).

3. Lyapunov characteristic exponent

A chaotic system is sensitive to small changes in the initial state. This tendency to amplify small perturbations is quantified by the Lyapunov exponent of the system [21]. For the one-dimensional mapping $x_{n+1}=\Phi(x_n,\alpha)$, the Lyapunov exponent can be computed from

$$\lambda(x_0)=\lim_{n\to\infty}\sum_{k=0}^{n-1}\ln\left|\frac{d\Phi_N(x)}{dx}\right|, \tag{3}$$

It is obvious that $\lambda(x_0)<0$ for an attractor, $\lambda(x_0)>0$ for a repeller and $\lambda(x_0)=0$ for marginal situation. Also, the Lyapunov number is independent of initial point x_0, provided that the motion inside the invariant manifold is ergodic, thus $\lambda(x_0)$ characterizes the invariant manifold of Φ_N as a whole [21,22].

The stability of the pair-coupled map can be assessed by computing its Lyapunov exponent spectrum. A spectrum of all the Lyapunov exponents with respect to the synchronization solution can be evaluated in a fashion similar to that of one-dimensional local maps [4]. At synchronized states, the Lyapunov exponents $(\Lambda_\pm)$ of the two-dimensional dynamical system described by the map (Eq. (2)) are defined as the $\lim_{n\to\infty}\frac{1}{n}|\lambda_\pm(x_n)|$, where $\lambda_\pm=h_1(x)\pm h_2(x)$ are eigenstates of the following matrix:

$$\begin{vmatrix} h_1(x_n) & h_2(x_n) \\ h_2(x_n) & h_1(x_n)) \end{vmatrix}=\begin{vmatrix} \frac{\partial x_{n+1}}{\partial x_n} & \frac{\partial x_{n+1}}{\partial y_n} \\ \frac{\partial y_{n+1}}{\partial x_n} & \frac{\partial y_{n+1}}{\partial y_n} \end{vmatrix}_{x_n=y_n}=\begin{pmatrix} (1-\epsilon)a_1^P & \epsilon a_2^P \\ \epsilon a_2^P & (1-\epsilon)a_1^P \end{pmatrix}^{n+1}\prod_{k=0}^{n}\left[((1-\epsilon)a_1^P+\epsilon a_2^P)^{\frac{1}{P}-1}g(x_k)\right]$$

which yields:

$$\Lambda_+=\lim_{n\to\infty}\frac{1}{n}\ln|\lambda_+(x_n)|=\Lambda\left[((1-\epsilon)a_1^P+\epsilon a_2^P)^{\frac{1}{P}}\tan^2(N\arctan\sqrt{x})\right] \tag{4}$$

$$\Lambda_-=\lim_{n\to\infty}\frac{1}{n}\ln|\lambda_-(x_n)|=\ln|(1-\epsilon)a_1^P-\epsilon a_2^P|-\ln|(1-\epsilon)a_1^P+\epsilon a_2^P|+\Lambda\left[((1-\epsilon)a_1^P+\epsilon a_2^P)^{\frac{1}{P}}\tan^2(N\arctan\sqrt{x})\right] \tag{5}$$

Result representing the general form of the Lyapunov characteristic exponent for the introduced family (Eq. (2)).

4. Watermark generation

Color is an important visual information which keeps humans fascinated since birth. The representation of color is based on the classical three-color theory where any color can be reproduced by mixing an appropriate set of three primary colors.