Signal Processing: *Image Communication* 29 (2014) 887–901

Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

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

A new hyperchaotic map and its application in an image encryption scheme

Radu Boriga [1], Ana Cristina Dăscălescu, Iustin Priescu

Informatics Departament, Titu Maiorescu University, Văcăreşti Avenue 187, Bucharest, Romania

ARTICLE INFO

Article history:
Received 11 November 2013
Received in revised form
2 March 2014
Accepted 30 April 2014
Available online 24 May 2014

Keywords:
Hyperchaos
Lyapunov exponents
Random permutation
Image encryption scheme

ABSTRACT

Recently, the hyperchaotic maps have been investigated in order to develop more secure encryption schemes. In this paper we propose a new hyperchaotic map derived from parametric equations of the serpentine curve. Its complex behavior was proven theoretically and numerically, using Lyapunov exponents, bifurcation diagram and correlation dimension of the attractor. The proposed map is then used in a new image encryption scheme with a classic bi-modular architecture: a diffusion stage, in which the pixels of the plain image are shuffled using a random permutation generated with a new algorithm, and a confusion stage, in which the pixels are modified with a XOR-scheme based on the proposed map. The results of its statistical analysis show that the proposed image encryption scheme provides an efficient and secure way for image encryption.

1. Introduction

Image encryption schemes have been increasingly studied in order to ensure real-time secure images transmission through the Internet or other communication networks. To meet this challenge, many new encryption schemes based on classical algorithms (i.e. AES, DES, Blowfish, etc.) have been proposed in the last years [1–7]. Starting from 1989, when Robert Matthews proposed the first chaos based cryptosystem in which he used the logistic map, the chaotic maps became a new direction to develop image encryption schemes which have, in many aspects, similar properties to the conventional ones [8–12].

In the last decade, many researchers proposed different encryption schemes based on chaotic maps, being encouraged by the chaotic properties of dynamical systems such as high sensitivity to the initial conditions, ergodicity, high complexity induce by their simple analytic expressions, etc. [13–21]. Mostly, those proposed chaos based encryption schemes used chaotic maps to generate a random permutation for shuffling the pixels from plain image and to generate a pseudorandom bit sequence for substituting the pixels, in order to obtain an encrypted image. The secret key consist from the control parameters of the chaotic map and its initial conditions, so it's necessary to use maps which are chaotic for a large interval of parameters' values. Meanwhile, in some cryptanalysis work it was proven that some chaos based image encryption schemes are insecure against various conventional attacks, such as chosen plain images or know plain image attacks [22–26]. Some general approaches evaluating security of chaos based encryption schemes were summarized in [27–29].

Recently, the hyperchaotic maps have been investigated in order to develop more secure image encryption schemes [30–32] due the fact that the hyperchaotic maps have more complex characteristics than the chaotic ones. In [33] and in [34] novel image encryption schemes based on improvement hyperchaotic sequences were proposed, where a pseudorandom number sequence generated by a

E-mail addresses: radu.boriga@prof.utm.ro (R. Boriga), cristina.dascalescu@prof.utm.ro (A.C. Dăscălescu), iustin.priescu@prof.utm.ro (I. Priescu).

[1] Tel.: +40724565388.

http://dx.doi.org/10.1016/j.image.2014.04.001
0923-5965/© 2014 Elsevier B.V. All rights reserved.

4D hyperchaotic map was used to modify the values of the pixels with a XOR-scheme. In [31] the Chinese remainder theorem is used to diffuse and compress an image shuffled with a 2D hyperchaos discrete nonlinear dynamic system and in [32] is presented a new cryptosystem with coupled map lattices and time-varying delay, using a linear hyperbolic chaotic system of partial differential equations with nonlinear boundary conditions. Also, in [30] an ergodic matrix of one hyperchaotic sequence is used to diffuse a permutated image and in [35] the hyperchaotic sequences are modified to generate the key stream, while in [36] a new image encryption algorithm based on fractional-order hyperchaotic Lorenz system is proposed. Still, there is little work about the study of encryption algorithms based on hyperchaos.

In this paper, we proposed a new hyperchaotic 2D map, derived from the serpentine parametric equations. Using the Lyapunov exponents, bifurcation diagram and fractal dimensions of the attractor, we prove theoretically and numerically that the proposed map has a complex behavior, being a hyperchaotic map. The proposed map is then used in a new image encryption scheme which has two stages: a diffusion stage, in which the pixels of plain image are shuffled using a random permutation generated with a new, and the confusion stage, in which the pixels are modify using a XOR–scheme based on the proposed map.

The paper is organized as follows: in Section 2 we presents the design of the newly proposed hyperchaotic 2D map, including its hyperchaotic behavior assessment; Section 3 presents a new image encryption scheme based on the map proposed in Section 2; Section 4 presents the performance analysis of the proposed image encryption scheme. Finally, Section 5 concludes the work carried out.

2. The proposed hyperchaotic map

The proposed 2D map is derived from the parametric equations of serpentine curve, defined by L'Hopital and Huygens [37]:

$$\begin{cases} x &= actgt \\ y &= b\ \sin\ t\ \cos\ t \end{cases} \tag{1}$$

where parameter $t \in [0, 2\pi]$.

Restricting the values of x and y in the interval $[-(\pi/2), (\pi/2)]$, we obtained the following 2D map, hereinafter referred as *serpentine map*:

$$\begin{cases} x_{n+1} &= \operatorname{arctg}(\operatorname{ctg}(2^r x_n)) \\ y_{n+1} &= \sin(2^r y_n)\cos(2^r y_n) \end{cases} \tag{2}$$

where $r > 0$ is the control parameter.

The evolution rule of the map (2) is:

$$\begin{gathered} f_S\colon \left[-\tfrac{\pi}{2}, \tfrac{\pi}{2}\right]\ \{0\} \times \left[-\tfrac{1}{2}, \tfrac{1}{2}\right] \to \left[-\tfrac{\pi}{2}, \tfrac{\pi}{2}\right] \times \left[-\tfrac{1}{2}, \tfrac{1}{2}\right], \\ f_S(x, y) = (\operatorname{arctg}(\operatorname{ctg}(2^r x)),\ \sin(2^r y)\cos(2^r y))\ ,\ r > 0 \end{gathered} \tag{3}$$

2.1. Dynamics of the proposed map

Next, we study the long time behavior of serpentine map according to the control parameter r and to the initial condition (x_0, y_0).

Theorem 1. Let $f_S\colon [-(\pi/2), (\pi/2)]\ \{0\} \times [-(1/2), (1/2)] \to [-(\pi/2), (\pi/2)] \times [-(1/2), (1/2)]$ be the serpentine map, defined by the relation (3). Then the f_S map has unstable periodic orbits with period $k \geq 2$ for any control parameter $r > 0$.

Proof. The stability of a periodic orbit $P = \{P_1(x_1, y_1), \dots, P_k(x_k, y_k)\}$ whit $k \geq 2$ period can be studied using the eigenvalues of the Jacobi matrix [38]. Thus, we calculated the Jacobi matrix associate to the k iteration of the serpentine map:

$$\begin{aligned} Df_S^k(P_1) &= Df_S(P_k) \times Df_S(P_{k-1}) \cdots Df_S(P_1) = \\ &= \begin{pmatrix} -2^r & 0 \\ 0 & 2^r\ \cos\ 2^{r+1} y_k \end{pmatrix} \\ &\times \begin{pmatrix} -2^r & 0 \\ 0 & 2^r\ \cos\ 2^{r+1} y_{k-1} \end{pmatrix} \cdots \begin{pmatrix} -2^r & 0 \\ 0 & 2^r\ \cos\ 2^{r+1} r y_1 \end{pmatrix} \Rightarrow \\ Df_S^k(P_1) &= \begin{pmatrix} (-1)^k 2^{kr} & 0 \\ 0 & 2^{kr}\ \cos\ 2^{r+1} y_k \cdots\ \cos\ 2^{r+1} y_1 \end{pmatrix} \end{aligned} \tag{4}$$

The eigenvalues of Df_S^k are:

$$\begin{cases} v_1 = (-1)^k 2^{kr} \\ v_2 = 2^{kr}\ \cos(2^{r+1} y_k) \cdots\ \cos(2^{r+1} y_1) \end{cases} \tag{5}$$

so, the absolute values of the eigenvalues are:

$$\begin{cases} |v_1| = 2^{kr} \\ |v_2| = 2^{kr} |\ \cos(2^{r+1} y_k) \cdots\ \cos(2^{r+1} y_1)| \end{cases} \tag{6}$$

The stability of the periodic orbit P depends on the value of the parameter r, thus:

1. if $r < 0 \Rightarrow |v_1| < 1$ and $|v_2| < 1$, then the orbit T is an attractor;
2. if $r \in \left(0, \log_2\left(1/\sqrt[k]{\left|\cos(2^{r+1} y_k) \cdots\ \cos(2^{r+1} y_1)\right|}\right)\right) \Rightarrow |v_1| > 1$ and $|v_2| < 1$, then the orbit T is a saddle;
3. $r > \log_2\left(1/\sqrt[k]{\left|\cos(2^{r+1} y_k) \cdots\ \cos(2^{r+1} y_1)\right|}\right) \Rightarrow\ |v_1| > 1$ and $|v_2| > 1$, then the orbit T is a source.

In conclusion, the map has unstable periodic orbits with period $k \geq 2$ for any control parameter $r > 0$. ■

Theorem 1. shows that f_S map possess unstable periodic orbits with period $k \geq 2$. Using the numerical methods we plotted in Fig. 1 the bifurcation diagram for parameter $r \in [0, 20]$. It can be notice that for values of parameter r very close to 0, the orbits of serpentine map are sources.

Another strong instrument used in our analysis are Lyapunov exponents, which indicate the exponential divergence of two orbits starting from two close points in the phase space. The 2D maps have two Lyapunov exponents. If the map has one exponent positive, then the map is in a chaotic regime and if the both exponents are positive, then the map exhibits a hyperchaotic behavior [38]. In practice, those Lyapunov exponents can be calculated numerically using the Wolf algorithm [39]. In Fig. 2