Optik 127 (2016) 5812–5819

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Original research article

Asymmetric color pathological image encryption scheme based on complex hyper chaotic system

Hongjun Liu [a,b,*], Abdurahman Kadir [c], Yangling Li [a,b]

[a] School of Information Engineering, Weifang Vocational College, Weifang 261041, China
[b] Modern Logistics Information Engineering Technology Research Center of Weifang, Weifang 261041, China
[c] School of Computer Science and Engineering, Xinjiang University of Finance and Economics, Urumqi, 830012, China

ARTICLE INFO

Article history:
Received 19 October 2015
Accepted 6 April 2016

Keywords:
Hyper chaotic complex system
Asymmetric cryptosystem
Hash function
Dynamical step length

ABSTRACT

An asymmetric color image encryption scheme is proposed based on four-wing hyper chaotic complex system, whose initial values, parameter and step length depend on 512-bit hash value of the plain image. The encryption process is to transform three color components of red, green and blue into three 1D arrays, and then use three pairs of chaotic sequences to encrypt the elements of odd number and even number indexes respectively. The encryption algorithm and the decryption algorithm have different keys. Numerical results and security analysis demonstrate the feasibility and effectiveness of the asymmetric color image encryption scheme.

1. Introduction

In recent years, based on symmetric image encryption schemes, some asymmetric image encryption schemes have been proposed by researchers. Abuturab et al. [1] proposed an asymmetric single-channel color image encryption using Hartley transform and gyrator transform, the encoded image is modulated with a conjugate of random phase mask, the asymmetric (decryption) keys, random phase mask and transformation angle of gyrator transform serve as main keys. Li et al. [2] proposed a multiple-image cryptosystem based on the cascaded fractional Fourier transform, the encryption key is an indivisible part of the corresponding original image and it is still useful during decryption. Liu et al. [3] proposed a multiple-image encryption scheme with asymmetric keys, the original images are multiplexed and encoded into real-valued cipher text using only one public encryption key, and ciphered image can only be de-multiplexed by its private decryption key.

Chaotic map is discreted and can be expressed as difference equation, while chaotic system is continuous and can be expressed as differential equation, which can produce discreted value by setting step length of Runge-Kutta method. Besides chaotic map and chaotic system, fractional-order chaotic system also have been applied in image cryptosystems. Liu et al. [4] proposed an asymmetric color image cryptosystem based on Hénon map. Zhang et al. [5] proposed an improved image encryption based on coupled logistic map, self-adaptive permutation, S8 S-boxes transform and combined global diffusion. Wu et al. [6] proposed a color image encryption algorithm by using coupled-map lattices (CML) and a fractional-order chaotic system, an image division-shuffling process is put forward to make the encryption process more confusing and complex.

* Corresponding author.
E-mail address: smithliu@126.com (H. Liu).

http://dx.doi.org/10.1016/j.ijleo.2016.04.014
0030-4026/

Based on the classical integer-order chaotic system and fractional-order chaotic system, such as Lorenz system, Chen system, et al., the corresponding complex chaotic system [7–9] and hyper chaotic system [10,11] have been proposed and applied in secure communication.

In this paper, an asymmetric color image encryption scheme is designed based on four-wing hyper chaotic complex system. 512-bit hash value of the plain image and the initial values are combined to generate the one-time initial conditions of chaotic system. Each color component is transformed into a 1D array and encrypted by a pair of chaotic sequences produced by the hyper chaotic complex system. Statistical and security analysis demonstrate the effectiveness of the asymmetric image encryption scheme.

2. The Dadras complex hyper chaotic system

Dadras et al. [10] constructed a real 4D smooth autonomous hyper chaotic system, which can be expressed by Eq. (1):

$$\begin{cases} \dot{x} = ax - yz + w \\ \dot{y} = xz - by \\ \dot{z} = xy + xw - rz \\ \dot{w} = -y \end{cases}, \tag{1}$$

in which $[x, y, z, w]^T$ is the state vector, and a, b and r are positive parameters. If we set $a = 8$, $b = 40$ and $r = 14.9$, the system can generate a four-wing hyper chaotic attractor.

Liu et al. [11] proposed the corresponding complex hyper chaotic system of Eq. (1), which can be experssed by Eq. (2).

$$\begin{cases} \dot{z}_1 = az_1 - z_2 z_3 + z_4 \\ \dot{z}_2 = z_1 z_3 - bz_2 \\ \dot{z}_3 = 0.5[\bar{z}_1(z_2 + z_4) + z_1(\bar{z}_2 + \bar{z}_4)] - rz_3 \\ \dot{z}_4 = -0.5(z_2 + \bar{z}_2) \end{cases}, \tag{2}$$

where $z_1 = u_1 + ju_2$ and $z_2 = u_3 + ju_4$ are complex state variables, and $z_3 = u_5$ and $z_4 = u_6$ are real state varisbles. The complex hyper chaotic Dadras system of Eq. (2) can be re-expressed as a real first-order ordinary diferential equation of Eq. (3).

$$\begin{cases} \dot{u}_1 = au_1 - u_3 u_5 + z_6 \\ \dot{u}_2 = au_2 - u_4 u_5 \\ \dot{u}_3 = u_1 u_5 - bu_3 \\ \dot{u}_4 = u_2 u_5 - bu_4 \\ \dot{u}_5 = u_1(u_3 + u_6) + u_2 u_4 - ru_5 \\ \dot{u}_6 = -u_3 \end{cases}, \tag{3}$$

when we set the parameters of $a = 8$, $b = 40$ and $r = 39$, the 3D chaotic attractors are shown in Fig. 1.

We set the control parameter r dynamically change in some intervals, the system can still maintain hyper chaotic status. Six Lyapunov exponents of Eq. (3) with $r \in [0, 39]$ are shown in Fig. 2, in which two positive Lyapunov exponents demonstrate the hyper chaotic features. The initial values of six state variables and the control parameter r can serve as keys.

3. Generating one-time initial conditions

Here we calculate the hash value of the plain image, and transform it into the initial values of System (3). The SHA-512 is employed to generate the 512-bit hash value H of the plain image, and H can be divided into 128 heximal numbers and be expressed as Eq. (4).

$$\boldsymbol{H} = h_1, h_2, \ldots, h_{128}. \tag{4}$$