Optik 126 (2015) 2474–2480

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

A new encryption algorithm for color images based on total chaotic shuffling scheme

Elaheh Vaferi, Reza Sabbaghi-Nadooshan*

Department of Electronics, Central Tehran Branch, Islamic Azad University, Terhran, Iran

ARTICLE INFO

Article history:
Received 26 April 2014
Accepted 4 June 2015

Keywords:
Security
Image encryption
Quantum chaotic map
Nearest-neighboring coupled-map lattices

ABSTRACT

This paper proposes a novel image encryption algorithm based on a quantum chaotic map, nearest-neighboring coupled-map lattices and permutation-diffusion architecture. First, a keystream generated by a quantum chaotic map is used to permute the pixels of the R, G and B components concurrently and make the three components affect one other. Next, the random circular shift operation was performed, resulting in permuted pixels to rearrange bits of each pixel. Finally, the new algorithm employs keystreams generated by the nearest-neighboring coupled-map lattices to diffuse the relationship between the cipher image and the plain image. To generate the initial conditions and parameters of the chaotic maps, a 128 bit long external secret key is used. The results of several experimental analyses on the randomness, sensitivity, and correlation of the cipher images show that the proposed algorithm has a high security level and high sensitivity and can be adopted for network security and secure communications.

1. Introduction

Thanks to the rapid development of information technology and network communication, the transmission of a wide range of digital data, from digital images to audio and video files, over the internet or via wireless networks has increased. In this virtual environment, problems associated with image security are becoming progressively important. In recent years, many image encryption methods have been suggested [1–5]. Image encryption architectures generally consist of two processes: pixel permutation and diffusion [6,7]. The permutation process changes the position of the image pixels. This process confuses the high correlation among pixels and does not alter the frequency distribution of pixel color values. The diffusion process modifies pixel values so that a tiny change for one pixel can be distributed to most pixels in the whole image. Because varied characteristics such as ergodicity and sensitivity exist in the initial conditions [8], the chaotic system can be considered a good candidate of a source of randomness in permutation and diffusion operations.

A chaos-based cryptographic scheme is an efficient encryption method first presented by Matthews [9]. It has several excellent characteristics that differ from other algorithms, such as sensitive dependence on initial conditions, non-periodicity, non-convergence, and control parameters [10]. In recent years, various encryption schemes based on a chaotic map have been proposed [11–21]. Fridrich [11] demonstrated a symmetric image encryption algorithm based on a 2D standard baker map.

Three basic steps to encrypt the data have been suggested to fit invertible chaotic 2D maps on a torus or rectangle. First, a chaotic map is selected, generalized by introducing parameters, and discretized to a finite rectangular lattice of points. In the last step, the map is extended to 3D chaotic baker maps to obtain a more complicated substitution cipher. Lately, an efficient image encryption algorithm based on a skew tent map and permutation-diffusion architecture has been suggested [12]. Mazloom and Eftekhari-Moghadam [13] designed a color image encryption algorithm based on a coupled nonlinear chaotic map. Seyedzadeh and Mirzakuchaki [14] showed that Mazloom's scheme [13] cannot resist sensibility attacks. Gao et al. [15] proposed a hyper chaotic cryptosystem based on the Chen system to encrypt a grayscale image. Rhouma et al. [16] presented cryptanalysis of a new image encryption algorithm based on hyper-chaos and two different attacks.

Other research [17,18] has also revealed good experimental results. Chaotic image encryption algorithms tend to have flaws. Some algorithms utilize Arnold cat maps to confuse pixels. This map [19,20] has two fundamental weaknesses [21]. One is that the iteration times are very limited, usually not more than 1000 times; the other is that the width and height of the original image must

* Correspondence to: Niayesh Building, Emam Hassan Blvd., Pounak, Tehran, Iran. Tel.: +98 21 44600047; fax: +98 21 44600071.
E-mail addresses: e.vafery@gmail.com (E. Vaferi), R_sabbaghi@iauctb.ac.ir (R. Sabbaghi-Nadooshan).

http://dx.doi.org/10.1016/j.ijleo.2015.06.012
0030-4026/

be identical, otherwise pre-operations must be performed on the image. Some algorithms encrypt color components independently and neglect correlations between R, G and B components, making them more vulnerable to attack. To obtain a perfect encryption effect, the algorithm must ensure that encryption procedures are related to a plain image, but some researchers have not realized that encryption procedures have little relevance for a plain image. Some algorithms only encrypt square images, so, if the image height and width are not equal, the image cannot be directly permuted.

Quantum chaos can be characterized by the sensitivity to parameters in the Hamiltonian that governs chaotic dynamics [22–24]. This is an interesting property that can be used in cryptography. This study proposes a novel image encryption algorithm based on a quantum chaotic map, nearest-neighboring coupled-map lattices, and permutation-diffusion architecture. First, a keystream generated by a quantum chaotic map is used to permute the pixels of the R, G and B components concurrently and make the three components affect one other. Next, a random circular shift operation is performed that results in permuted pixels to rearrange the bits of each pixel. Finally, the new algorithm employs keystreams generated by nearest-neighboring coupled-map lattices to diffuse the relationship between the cipher-image and the plain image. A 128-bit long external secret key is used to generate the initial conditions and parameters of the chaotic maps.

In the rest of the paper, Section 2 briefly describes the quantum chaotic map and nearest-neighboring spatiotemporal chaos system. In Section 3, the proposed cryptosystem is explained. Simulation results and security analysis are provided in Section 4. Conclusions are discussed in Section 5.

2. Basic theory of the proposed cryptosystem

2.1. Quantum Chaotic Map

Dissipative quantum systems are often described as a system coupled to a path of harmonic oscillators to construct a quantum logistic map [23,24] with quantum corrections. Akhshani and Akhavan [24] analyzed the effects of quantum corrections and state $a = \langle a \rangle + \delta a$, where δa shows a quantum fluctuation about $\langle a \rangle$. They proved that the very lowest-order quantum corrections can yield a chaotic map as follows:

$$\begin{aligned} X_{n+1} &= r\left(X_n - \left|X_n\right|^2\right) - ry_n \\ y_{n+1} &= -y_n e^{-2\beta} + e^{-\beta} r\left[(2 - X_n - X_n^*)y_n - X_n Z_n^* - X_n^* Z_n\right] \\ Z_{n+1} &= -Z_n e^{-2\beta} + e^{-\beta} r\left[2(1 - X_n^*)Z_n - 2X_n y_n - X_n\right] \end{aligned} \quad (1)$$

Where $x = \langle a \rangle$, $y = \langle \delta a \dagger \delta a$, r is an adjustable parameter and β is the dissipation parameter. Generally, x_n, y_n, and z_n are complex numbers, x_n^* is the complex conjugate of x_n and z_n^* is the complex conjugate of z_n. Akhshani and Akhavan [24] set $r = 3.9$, $\beta = 4.5$, and iterate Eq. (1) with real initial parameters x_0, y_0, z_0^*, x_0^*, z_0^*; thus, all successive values for x_n, y_n, and z_n will be real for all n.

2.2. Nearest-neighboring coupled-map lattices

A general nearest-neighboring spatiotemporal chaos system, also called a nearest-neighboring coupled-map lattice (NCML) [25], can be defined as follows:

$$Z_{n+1}(j) = (1 - \varepsilon) f(Z_n(j)) + \varepsilon f(Z_n(j+1)) \quad (2)$$

Where, $j = 1,2,..,T$ is the lattice state index; $n = 1, 2, 3, \ldots$, is the time index; f is a chaotic map, and $\varepsilon \in (0,1)$ is the coupling coefficient. The periodic border condition $z_n(j+T) = z_n(j)$ is required for this system.

3. The proposed cryptosystem

In the proposed algorithm, the keystream generation is combined with the spatial, random circular shift, and diffusion processes into a single coherent encryption platform.

3.1. Generation of initial conditions and parameters

Based on the analysis presented in Section 2, three initial inputs x_0, y_0, z_0, and x_0^* and z_0^* generate pseudo-random keystreams using a the quantum chaotic map. The proposed cryptosystem utilizes a 128 bit external secret key (K) divided into 8 bit blocks (k_i) referred to as session keys. The K is defined as:

$$K = K_1, K_2, K_3, \ldots, K_{16} \quad (3)$$

For an image of size W × H, the initial inputs are derived as follows:

$$\begin{aligned} X_0 &= \left(\left((K_1 \oplus \ldots \oplus K_4) + \sum_{i=1}^{i=16} K_i\right) \bmod 256\right) /256 \\ X_0^* &= \left(\left((K_5 \oplus \ldots \oplus K_8) + \sum_{i=1}^{i=16} K_i\right) \bmod 256\right) /256 \\ y_0 &= \left(\left((K_9 \oplus \ldots \oplus K_{12}) + \sum_{i=1}^{i=16} K_i\right) \bmod 256\right) /256 \\ Z_0 &= \left(\left((K_{13} \oplus \ldots \oplus K_{16}) + \sum_{i=1}^{i=16} K_i\right) \bmod 256\right) /256 \\ Z_0^* &= \left(X_0 + X_0^* + y_0 + Z_0\right) \bmod 1 \end{aligned} \quad (4)$$

The proposed algebraic transform is very sensitive to K and a change in K produces completely different results. As a result, the proposed algorithm with a total complexity of 2^{128} can resist any key sensitivity attack and any brute-force attack.

For the quantum chaotic map in Eq. (1), because β is located in a negative exponent of e, if β is a large number, z and y variables tend toward zero. In this case, a 3D quantum logistic map will transform to a one-dimensional logistic map, which has a smaller key space, lower complexity, and lower randomness than the logistic map [24]. On the quantum chaotic map, after several iterations (for example, 500 iterations), the value of y decreases until it reaches zero. This can lead to a reduction in the complexity of the encryption key and ultimately reduces the sensitivity of the algorithm to the secret key. To reduce the adverse effects in the proposed algorithm, after generating the initial parameters of the quantum chaotic map, x_n, y_n and z_n variables are coupled using the nearest-neighboring coupled-map lattice. The keystream of the encryption is thus generated, the complexity of the random keystream is ensured and also avoids z and y falling to zero over the next periods. Fig. 1 illustrates the key generation process.

3.2. Proposed encryption algorithm

For a color image of size $W \times H$, its components are treated as one-dimensional: $R = r_1, r_2, \ldots r_{W \times H}$; $G = g_1, g_2, \ldots g_{W \times H}$; $B = b_1, b_2, \ldots b_{W \times H}$. The three components are combined to the R, G and B matrices vertically and produce matrix P with $3W$ rows and H columns. The detailed encryption steps for the proposed algorithm are:

Step 1: Apply K and set $n = 0$, $L = W \times H$, $r = 3.9$ and $\beta = 4.5$ and generate the initial conditions as in Eq. (4).

Step 2: Apply these initial values to Eq. (1). Because initial values are real values, therefore, real three keystreams x_{n+1}, y_{n+1}, and z_{n+1} are obtained in each round. In order to increase the