Computers in Biology and Medicine 45 (2014) 111–117

Contents lists available at ScienceDirect

Computers in Biology and Medicine

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

Chaos-based color pathological image encryption scheme using one-time keys

Guoyan Liu [a], Jie Li [b], Hongjun Liu [c,*]

[a] Department of Dermatology, Affiliated Hospital of Weifang Medical University, Weifang 261031, China
[b] Department of Obstetrics, Affiliated Hospital of Weifang Medical University, Weifang 261031, China
[c] School of Information Engineering, Weifang Vocational College, Weifang 261041, China

ARTICLE INFO

Article history:
Received 20 September 2013
Accepted 18 November 2013

Keywords:
Image encryption
SHA-2
Avalanche effect
One-time keys
Chebyshev maps

ABSTRACT

This paper proposes an improved chaos-based color pathological image encryption algorithm, using SHA-2 to generate one-time keys. In order to send different ciphered images to different recipients, the hash value of the plain image and a random number are applied to generate one-time initial conditions for Chebyshev maps, to make the key stream change in every confusion process without changing the common initial values. The permuted image is divided into 256-bit long blocks, the avalanche effect is applied to diffuse the blocks, i.e., each block is XORed with the hash value of the prior block. Simulation results demonstrate that the proposed algorithm is robust against common attacks.

1. Introduction

In recent years, some image encryption schemes based on discrete chaotic maps have been designed. Liu et al. [1–3] proposed some image encryption and image hiding schemes by using chaotic maps. In Ref. [1], an opto-digital image encryption by Baker mapping and 1-D fractional Fourier transform is designed. In Ref. [2], a color image encryption algorithm by using Baker mapping and Hartley transform is presented, the coordinates composed of the scrambled monochrome components are converted from Cartesian coordinates to spherical coordinates, and the data of azimuth angle is normalized and regarded as the key. In Ref. [3], a mixed scrambling operation is defined by the use of Arnold transform and Baker mapping. Following a designed sequence, the combined scrambling operation is utilized for changing the pixel position of secret image under the control of a random matrix. At the same time, the pixel value is altered by random bit shift for obtaining an encrypted image encoded in N-bit data.

The security of digital image attracts much attention. Zhang et al. [4] designed a text encryption algorithm for one-way hash function construction based on the chaotic map with changeable-parameter. Cheddad et al. [5] designed a novel way of encrypting digital images with password protection using 1D SHA-2 algorithm coupled with a compound forward transform.

Deng et al. [6] attacked the algorithm proposed by Ref. [5], in their scheme, they assume that the key is unknown, and a black image is fed into the encryption system to generate the substituted key stream, after reversing the substituted key stream using the rule M, the new key stream before substitution can be obtained, which is equal to the key stream XORed with the plain image, and finally they proposed an improved algorithm coupled with the self-adaptive algorithm to achieve ideal encryption result.

Although the algorithm in Ref. [6] is better than the previous one, there still exist two flaws inside. Firstly, they use the Arnold cat map to shuffle the positions of the pixels, one weakness of this map is that the parameters of a, b and k are constant, and the limited iteration times are easily led to violent attacks, the solution is to employ the variable control parameters [7]; the other weakness is that the width and height of the plain image must be equal, or the image cannot be directly permuted. Secondly, for each time the user is required to enter the password, so it is difficult to ensure the password to be never duplicated, according to Shannon's theory of secure communication, only the one-time key is theoretically unbreakable [8].

To make chosen plaintext attack and known plaintext attack become invalid, the best way is to change the key stream each time [9]. The traditional way is to use the one time pad [10], although the cryptosystem can be ensured secure, it is impractical in the real secure communication for the problem of key distribution. The other practical way is to generate the key stream dependent on the plain text or the cipher text, so the key stream automatically changes in each encryption process.

This paper proposes an improved scheme to encrypt pathological image. We use the hash value of the plain image and a random number instead of the user's password, and employ the Chebyshev maps to confuse the pixels instead of the Arnold cat map, to send different ciphered images to different recipients. Furthermore, we take two measures to produce the avalanche

* Corresponding author. Tel.: +86 18265690365.
E-mail address: smithliu@126.com (H. Liu).

0010-4825/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.compbiomed.2013.11.010

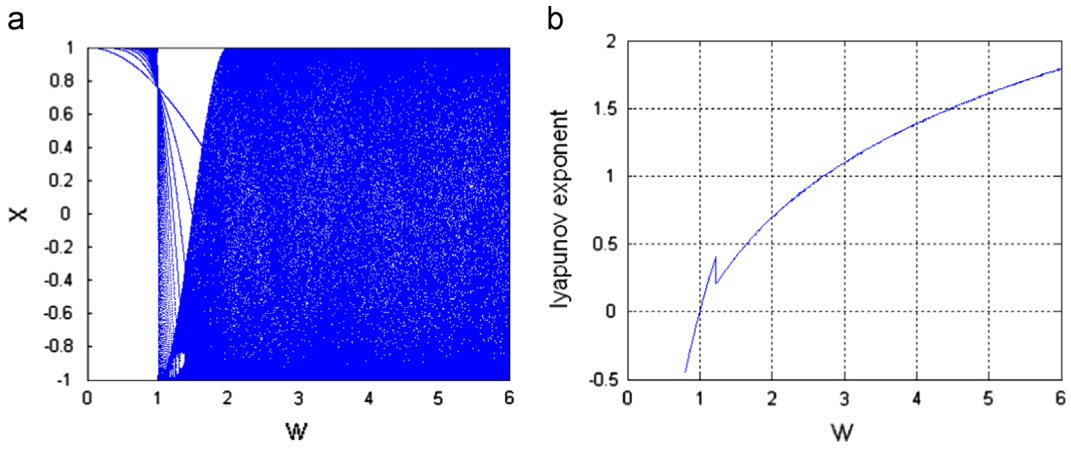

Fig. 1. (a) The bifurcate image and (b) the Lyapunov exponent image of Chebyshev maps.

effect to further diffuse the permuted image. Firstly, the initial value and parameter of the chaotic map are served as one-time keys, for each time the hash value is applied to modify them before encryption. Secondly, the permuted image is divided into 256-bit long blocks, and each block is XORed with the hash value of the prior block. Simulation results demonstrate that the proposed algorithm can be better than the existing ones.

2. SHA-256 and chaotic map

2.1. Using SHA-256 to generate initial values

SHA-2 is the one way hash function like SHA-1, but no collision has been found until now. SHA-2 hash standard underlies four secure hash algorithms of SHA-224, SHA-256, SHA-384, and SHA-512. The ECRYPT2 Yearly Report on Algorithms and Keysizes (2008–2009) [11] announced that, the security of SHA-256, SHA-384 and SHA-512 with complexity of the best attack as 2^{128}, 2^{192} and 2^{256} respectively. Here we choose the hash algorithm of SHA-256.

For the external secret keys in most of the cryptosystems remain unchanged, and Shannon proved that only the one-time key is theoretically unbreakable, so we use the hash value of the plain image and a random number to serve as the one-time key. We can send different ciphered pathological images to different recipients with different external secret keys by the following means:

(1) For each recipient, generate a random number R with the precision of 10^{-16}.
(2) Generate the 256-bit hash value $S(I,R)$ of the plain image I and R, which will be served as the external secret key.

Firstly, we use $S(I,R)$ to generate the new initial value and parameter of the Chebyshev maps. Secondly, we divide the pixels of the permuted image P' into blocks with equal size, and then use $S(I,R)$ to encrypt the first block.

Before permuting the plain image, we divide $S(I,R)$ into four blocks with the same length, and each block has sixteen hexadecimal numbers, i.e. $h_{j1}h_{j2}h_{j3}h_{j4}$, $j=1, 2, \ldots, 16$. For each group, we convert it into a floating decimal number $d_j \in (0,0.1)$ by Eq. (1).

$$d_j = \text{hex2}dec(h_{j1}h_{j2}h_{j3}h_{j4}) \times 10^{-6}, \tag{1}$$

where the function hex2dec(x) is employed to convert the hexadecimal number x to a decimal number.

For the Chebyshev maps, suppose the common initial value is z_0, and the parameter is w, we randomly separate d_j into two groups, such as $\{d_1, d_3, d_5, d_7, d_9, d_{11}, d_{13}, d_{15}\}$ and $\{d_2, d_4, d_6, d_8, d_{10}, d_{12}, d_{14}, d_{16}\}$, to compute the new initial value z'_0 and parameter w' by Eq. (2).

$$\begin{cases} z'_0 = z_0 + d_1 + d_3 + d_5 + d_7 + d_9 + d_{11} + d_{13} + d_{15} + \sum_{i=1}^{16} d_i \\ w' = w + d_2 + d_4 + d_6 + d_8 + d_{10} + d_{12} + d_{14} + d_{16} + \sum_{i=1}^{16} d_i \end{cases}. \tag{2}$$

For two images with even only one bit difference, their hash values will be completely different. By these measures, the initial conditions of the Chebyshev maps will dynamically change in each encryption process, so the results of confusion and diffusion can be unique.

2.2. Using Chebyshev maps to generate the permutation array

Chebyshev maps have important properties for designing excellent cryptosystem [12]. The expression for Chebyshev maps can generally be described in Eq. (3):

$$z_{i+1} = \cos(w \cos^{-1} z_i), \quad -1 \le z_i \le 1, \tag{3}$$

where w is the degree of Chebyshev maps, its corresponding invariant density is as follows:

$$\rho(z) = 1/(\pi\sqrt{1-z^2}). \tag{4}$$

If $w \in [2,6]$, the Lyapunov exponent of Chebyshev maps is positive, which predicates that the Chebyshev maps enter into chaotic state. The bifurcate image and Lyapunov exponent image are shown in Fig. 1.

Suppose the size of the color image is $M \times N$, we iterate Eq. (3) for $3MN$ times to get the sequence $Z = \{z_1, z_2, \ldots, z_{3MN}\}$ with the new initial value z'_0 and parameter w' by Eq. (2).

In order to confuse all the pixels, we will generate the array of $L = \{1, 2, \ldots, 3MN\}$ to donate the serial numbers of the pixels sorted by rows in ascending order.

Then we permute the array L by Eq. (5) to get L'.

$$L'(i) = L((z_i \times 3MN) \bmod i), \quad z_i \in Z, \quad i = 3MN, 3MN-1, \ldots, 2. \tag{5}$$