Optics and Lasers in Engineering 110 (2018) 24–32

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices

Hossein Nematzadeh[a], Rasul Enayatifar[b,*], Homayun Motameni[b], Frederico Gadelha Guimarães[c], Vitor Nazário Coelho[d]

[a] Department of Computer Engineering, Sari Branch, Islamic Azad University, Sari, Iran
[b] Department of Computer Engineering, Firoozkooh Branch, Islamic Azad University, Firoozkooh, Iran
[c] Department of Electrical Engineering, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte, Brazil
[d] Institute of Computer Science, Universidade Federal Fluminense (UFF), Niterói, RJ, Brazil

ARTICLE INFO

Keywords:
Medical image encryption
Modified genetic algorithm
Coupled map lattices

ABSTRACT

Image data are considered as significant data in medical systems. The amount of medical image data available for analysis keeps increasing with the modernization of image devices and biomedical image processing techniques. To prevent from being hacked over an insecure network, medical images should be encrypted safely. This study aims at proposing a medical image encryption method based on a hybrid model of the modified genetic algorithm (MGA) and coupled map lattices. First, the proposed method employs coupled map lattice to generate the number of secure cipher-images as initial population of MGA. Next, it applies the MGA to both increase the entropy of the cipher-images and decrease the algorithm computational time. Experimental results and computer simulations both indicate that the proposed method that includes a hybrid algorithm not only performs excellent encryption but also is able to resist to various typical attacks.

1. Introduction

The technology of digital images has great impact in diagnosis of certain diseases in medical systems. With the combination of digital images and Internet, great improvement in health protection has been achieved [1]. Digital images have several usages in medical diagnostics such as computed tomography and magnetic resonance imaging. Moreover, there are several techniques that are used with digital images such as noise detection, noise deletion, feature extraction, image segmentation, watermarking, and image compression. Health care systems are among the medical systems that use patients' digital images with high privacy [1,2].

In medical images adjacent pixels are strongly correlated but current image encryption algorithms are not powerful enough for proper image encryption thus, researchers tend to propose highly reliable image encryption algorithms [1–10]. Optical Encryption approach is an efficient image encryption method, which has been inspired from mathematical transform techniques such as fractional Fourier, discrete fractional Fourier, Fresnel, and etc. [2,11–14].

There are many directions and trends for the usage of chaos-based image encryption methods in the literature [4,6,15–18], especially when security is a matter of concern. Permutation and diffusion are the two main steps in chaos-based image encryption [7]. In permutation pixels' gray level are not changed and chaotic map reallocates image pixels. Next, chaos sequence is used to change the value of each pixel in diffusion step. Most of the chaos-based encryptions algorithms assign the parameter μ of the logistic map close to 4 ($\mu = 3.99$), which can ensure the chaotic behavior of the logistic map. Thus, the limitation in the range of $\mu \in (0, 4]$ indicates that the keystream generated from the chaotic sequences in the logistic map is vulnerable. One of the recently proposed chaotic map is coupled lattice map (CLM) which is more secure in comparison with the conventional lattice maps [19].

There have recently been proposed evolutionary algorithm-based image encryption techniques [5,6,8]. Specifically, Abdullah et al. proposed a genetic algorithm-based optimization approach for finding the best solutions at the end of each iteration [5]. First, the presented approach has been initiated with certain number of cipher-images generated using chaotic maps. Next, GA has been used to modify the cipher-images in order to achieve a cipher-image with the highest entropy and lowest correlation coefficient. There are some other evolutionary algorithm-based approaches for image encryption using same patterns. The category of evolutionary algorithm-based image encryption approaches is time consuming due to alternating iterations, which is one of the main deficiencies of these methods.

[*] Corresponding author.
E-mail address: r.enayatifar@gmail.com (R. Enayatifar).

https://doi.org/10.1016/j.optlaseng.2018.05.009
Received 28 October 2017; Received in revised form 7 May 2018; Accepted 11 May 2018

In this paper a novel approach has been proposed based on a modified GA (MGA) and coupled lattice map. First, CLM is used for generating secure cipher-images from the plain-images to form the initial population in MGA. Then, GA has been modified by proposing a new local search method as well as determining an experimental stop condition (termination criterion). The proposed modification accelerates convergence in the GA.

The organization of the paper is as follows: First, Section 2 explains CLM and GA. Then, Section 3 introduces the proposed method. Next, Section 4 simulates and analyses the results. Finally, the paper is concluded with overall findings and future works in Section 5.

2. Coupled map lattices

Chaotic maps are widely sensitive to the initial configuration because of their intrinsic features. Coupled map lattices (CML) is a type of chaotic function that employs the logistic map to generate its sequence [19]. In comparison with one dimensional chaotic system, the CML system contains stronger chaotic behavior, better pseudo random chaotic sequences, wider range of parameters and less periodic windows in bifurcation diagrams. Therefore, the pseudo random chaotic sequences generated from the CML system are more secure than that from one dimensional chaotic system. CML uses adjacent lattices for coupling as stated in Eq. (1) [19]:

$$X_{n+1}(i) = (1-\varepsilon) f\left[x_n(i)\right] + \frac{\varepsilon}{2}\left\{ f\left[x_n(i+1)\right] + f\left[x_n(i-1)\right]\right\} \qquad (1)$$

in which ε is the coupling parameter and $f(x) = \mu\, x(1 - x)$ with $\mu \in (0, 4]$. Assuming $\mu \in (3.87,\ 3.999)$ and $\varepsilon = 0.1$ indicates that the system generates local chaotic behavior because some of the lattices are not in chaotic behavior [19]. It should be noted that the impact of the number of lattices on image encryption is important. Finally, lattices substitute their chaotic sequences for preventing potential attacks. This happens when the mutual information of chaotic sequences between any two lattices are not zero.

3. The proposed method

The proposed method includes three phases which are explained in detail as follows:

Phase 1: key generation

For reliable encryption a random key with a fixed length of 128 bits is defined as in Eq. (2).

$$Key = \left[K_1,\ K_2, \ldots, K_{16}\right] \qquad (2)$$

In which K_i is a random 8-bit character. In this paper, couple lattice map (CLM) is used as a chaos function for initial image encryption. As it was discussed in Section 2, CLM uses logistic map sequence to generate quasi random numbers [19]. The pseudo code for creating the initial value of the logistic map from the key has been shown in Table 1.

In which ⊕ denotes the exclusive OR.

Phase 2: initial population generation

Basically, the initial population in GA includes diverse cipher-images derived from the plain-image. To initialize encryption, the main image with $N \times M$ dimension should be transformed to a one dimensional vector $\{P_1, P_2, P_3, \ldots, P_{M\times N}\}$. Here P_i shows the ith pixel. Eq. (3) is used to generate each cipher-image from the main image.

$$P_i' = \begin{cases} \lfloor X_n \times 256 \rfloor \oplus P_i & if\ (i=1) \\ \lfloor X_n \times 256 \rfloor \oplus P'_{i-1} \oplus P_i & Otherwise \end{cases} \qquad (3)$$

In which P_i' is the encrypted P_i and X_n is the coupled lattice map result. To prevent similarities among encrypted images i should be reset unlike n. Using this approach the sufficient initial population for genetic algorithm is generated. A number is assigned to its image in accordance with its encryption order, that is, the first image is assigned 1, the second image is assigned 2 and etc.

Table 1
A pseudo code for creating initial value of the logistic map.

```
Input: Key stream
Output: $X_0$
$KEY \leftarrow [K_1,\ K_2, \ldots, K_{16}]$
$Binary\_Array \leftarrow Convert\ K_1\ to\ binary$
FOR I ← 2–9
    $Temp\_Array \leftarrow$ Convert $K_i$ to binary
    $Binary\_Array \leftarrow Binary\_Array \oplus Temp\_Array$
END FOR
$Decimal\_Num \leftarrow$ Convert $Binary\_Array$ to decimal
FOR $i$ ← 10 to size 16
    $Decimal\_Num \leftarrow Decimal\_Num + K_i$
END FOR
$X_0 \leftarrow \frac{Decimal\_Num}{2^{11}}$
```

For image decryption an encryption table containing the number of two parents that generate the cipher-image is needed besides the key. In this phase, since CLM is used for generating cipher-images, both numbers in the encryption table are the same in accordance with their respective order of cipher-images. The way of generating encryption table is mainly inspired by Enayatifar, et al. [8], which is shown in Table 2.

Phase 3: modified genetic algorithm (MGA)

The main steps of the proposed MGA are similar to original GA except in the initial stage in which the initial population is divided into specified number of groups firstly. This could reduce the number of comparisons drastically and as a result increase the performance. Next, selection and crossover operators are applied as explained in [5].

In the mutation step, a certain number of individuals (according to the mutation rate) are replaced with newly generated random individuals. Then, at the end of each iteration all of the solutions are excluded from their groups and are ranked based on their entropy fitness function. Finally, half of the best solutions are selected for the next iteration. The proposed algorithm will be terminated if after 10 consecutive iterations the fitness of solutions does not improve. The proposed MGA tackles the final encryption process as depicted in Fig. 1.

4. Simulation results

4.1. Experimental setup

The proposed method analysis is carried out in this section. Eight 256 × 256 medical images, as shown in Fig. 2, are used as a set of standard images. The experimental results have been calculated with MATLAB 2013 on a laptop with an Intel Core i7, 2.3 GHz CPU, 8 GB memory and 500 GB hard disk with a Windows 8 operating system. The introduced method parameters throughout the experiment are as follows. The number of initial population varies between 100 and 150 while crossover rate and mutation rate are set at 85% and 5%, respectively.

4.2. Entropy analysis

An outstanding feature to express degree of uncertainty in image is known as entropy which is calculated by Eq. (4) [20]. According to the equation, maximum possible entropy value for a 256 gray-scale image is 8, thus the entropy with closest value to 8 indicates the better uniform distribution.

$$H(s) = \sum_{i=0}^{2^M-1} P\left(s_i\right)\log_2 \frac{1}{P\left(s_i\right)} \qquad (4)$$

where $P(s_i)$ denotes the probability of the occurrence of variable s_i.

To perform the entropy test, the proposed study is run 30 times on each test image. The obtained entropy values of the cipher-images are listed in Table 3. As can be seen in Table 3, entropy values for all the test images are close to 8, which means the proposed method is effective.