Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Image encryption using a synchronous permutation-diffusion technique

Rasul Enayatifar[a,*], Abdul Hanan Abdullah[b], Ismail Fauzi Isnin[b], Ayman Altameem[c], Malrey Lee[d,*]

[a] *Department of Computer Engineering, Firoozkooh Branch, Islamic Azad University, Firoozkooh, Iran*
[b] *Faculty of Computing, Universiti Teknologi Malaysia (UTM), Johor Bahru, Malaysia*
[c] *College of Applied Studies and Community Services, King Saud University (KSU), Riyadh 12372, Saudi Arabia*
[d] *The Research Center for Advanced Image and Information Technology, School of Electronics and Information Engineering, ChonBuk National University, JeonJu, ChonBuk 561-756, Republic of Korea*

ARTICLE INFO

Keywords:
Image encryption
DNA sequence
Permutation
Diffusion
Chaotic map

ABSTRACT

In the past decade, the interest on digital images security has been increased among scientists. A synchronous permutation and diffusion technique is designed in order to protect gray-level image content while sending it through internet. To implement the proposed method, two-dimensional plain-image is converted to one dimension. Afterward, in order to reduce the sending process time, permutation and diffusion steps for any pixel are performed in the same time. The permutation step uses chaotic map and deoxyribonucleic acid (DNA) to permute a pixel, while diffusion employs DNA sequence and DNA operator to encrypt the pixel. Experimental results and extensive security analyses have been conducted to demonstrate the feasibility and validity of this proposed image encryption method.

1. Introduction

Transmitting of secure information has been becoming vital since popularity of the Internet has increased dramatically. Nowadays, digital images play a relatively significant role not only throughout the Internet, but also in smart phones and cellular networks [1]. Although, the prevalence of digital images makes human life greatly easier, at the same time it brings security problems. For the sake of this reason, many researchers have been concentrated on proposing different types of image encryption schemes based on chaotic map [2–9], transform domain [10,11], cellular automata [12–16], evolutionary algorithm [2–4], deoxyribonucleic acid (DNA) sequence [3,7,12,17] and others [17–24].

Image encryption methods based on chaotic map has been considered by researchers due to its specific characteristics, including ergodicity, sensitivity to initial condition, and control parameters. The primary permutation-diffusion algorithm for chaos based image encryption is proposed by Fridrish in 1998 [25]. In his work, at first, a two-dimensional chaotic map is used to shuffle plain-image pixels and then in diffusion step those pixel gray-level are altered sequentially using a one-dimensional chaotic function. Since then, Many chaotic based image encryption algorithms have been inspired by Fridrich's method, therefore this architecture has become most well-known [26]. Although security of an efficient image encryption method is fundamental issue in an image encryption algorithm, recent cryptanalytical studies have proven that some chaos-based algorithms are not adequately secure to resist against common attacks [27,28].

Recently, some researchers have been successfully suggesting DNA-based image encryption algorithms due to its new way for encrypting a pixel [3,7,29–32]. These approaches make the algorithm fairly resistant against different types of attacks. The main idea of these methods is to employ DNA sequence and operators to alter a pixel value in diffusion part.

In this study, a novel synchronous permutation-diffusion has been proposed to make encryption process faster and rather secure.

In the proposed scheme the permutation operation disturbs plain-images dramatically in such a way that the correlation between two adjacent pixels is extremely low, and the diffusion operation makes the values of diffused images randomly distributed such that it makes statistical attacks hard to succeed. In the proposed method, a Three-dimenssional chaotic function, namely 3-D logistic map, which is improved by Pawan et al. [33], is used to perform synchronous permutation-diffusion. First dimension of the logistic map and DNA sequence are used to permute a pixel, while second and third dimensions are associated with the DNA operator to alter the pixel value. The encryption process is quite difficult to break by hackers due to the logical combination of DNA and chaotic map. In addition, the proposed algorithm is potentially fast because permutation and diffu-

[*] Corresponding authors.
E-mail addresses: R.enayatifar@gmail.com (R. Enayatifar), mrlee@chonbuk.ac.kr (M. Lee).

http://dx.doi.org/10.1016/j.optlaseng.2016.10.006
Received 15 June 2016; Received in revised form 2 September 2016; Accepted 6 October 2016

sion have been performed in one clock.

The rest of this study is organized as follows. The preliminaries of the work are introduced in Section 2. In Section 3, our proposed method is explained in details. Experimental results are obtained to check the performance of the proposed algorithms in Section 4. In Section 5, the conclusion remark is given briefly.

2. Preliminary

In this section, two main tools which are the source of our proposed method are explained.

2.1. 3-D logistic map

Chaotic maps are completely sensitive to the initial value, which is one of the characteristics making this process difficult to predict. In this sort of function, a sudden change can occur in the number sequence produced by the evolution function if a slight change is made in the initial value [4]. Researchers have employed Different types of chaotic maps, nonetheless one of the most well-known map is the logistic map described in Eq. (1).

$$X_{n+1}=RX_n(1-X_n) \tag{1}$$

This one-dimensional logistic map can be extended to a 3-dimensional one as stated in Eq. (2) [33].

$$\begin{aligned} X_{n+1}&=RX_n(1-X_n)+\beta Y_n^2X_n+\alpha Z_n^3\\ Y_{n+1}&=RY_n(1-Y_n)+\beta Z_n^2Y_n+\alpha X_n^3\\ Z_{n+1}&=RZ_n(1-Z_n)++\beta X_n^2Z_n+\alpha Y_n^3 \end{aligned} \tag{2}$$

This nonlinear system presents chaotic behavior when its parameters are valued in the range $0.53<R<3.81$, $0<\beta<0.022$, $0<\alpha<0.015$ where X_0, Y_0 and Z_0 are in [0,1].

2.2. Deoxyribonucleic Acid (DNA)

Knowledge of Deoxyribonucleic Acid (DNA) sequences has become vital for basic biological research, and applied in numerous fields such as diagnostics, biotechnology, forensics, and biological systematics. There are four different nucleic acids in a DNA sequence which are named A (adenine), T (thymine), C (cytosine), and G (guanine). Regarding the rules of base pairing, the purine adenine (A) always pairs with the pyrimidine thymine (T), and the pyrimidine cytosine (C) always pairs with the purine guanine (G). It can be concluded that A and T are complementary, G and C are also complementary [3,34]. These relationships are often called the rules of Watson-Crick base pairing, named after the two scientists who discovered their structural basis [34]. There is the fact that in the binary system, 0 and 1 are complementary, hence, it can be observed that 00 and 01 are complementary with 11 and 10, respectively.

Table 1 is released as a coding and decoding rule of the DNA sequence in order to satisfy the Watson-Crick base pairing rule. As an example, $(11000101)_2$ is the binary format for number 197 and it could be encoded considering Rule 3 (see Table 1) to (ATGG).

Due to the extensive development of DNA computing, it seems that investigating some algebraic and biological operators is essential [3,34]. Table 2 denotes the XOR operator which is used in this paper.

3. Proposed scheme

To tackle the proposed method, synchronous permutation-diffusion technique is employed as explained further in the following sub-sections.

3.1. Initialization

The proposed method starts by generating a secret key since the 3-D logistic map needs it to generate its deterministic sequence string. For doing so, initial values of X_0, Y_0 and Z_0 in Eq. (2) have been taken from a 240-bit secret key as stated by Eqs. (3)–(6).

$$Key=\{K_1,\ K_2,\ldots,\ K_{30}\} \tag{3}$$

$$X_0=\left((K_1\bigoplus K_2\bigoplus\ldots\bigoplus K_5)+\sum_{i=6}^{10}K_i\right)/2^6 \tag{4}$$

$$Y_0=\left((K_{11}\bigoplus K_{12}\bigoplus\ldots\bigoplus K_{15})+\sum_{i=16}^{20}K_i\right)/2^6 \tag{5}$$

$$Z_0=\left((K_{21}\bigoplus K_{22}\bigoplus\ldots\bigoplus K_{25})+\sum_{i=26}^{30}K_i\right)/2^6 \tag{6}$$

where K_i and $\bigoplus$ denote an 8-bit character and exclusive OR operation, respectively. Regarding to Eqs. (4)–(6) the initial values of X_0, Y_0 and Z_0 are placed in the range of [0, 1], hence 3-D logistic map enables to generate the string of chaotic number iteratively.

In this study, plain-image and cipher-image with M rows and N columns are converted to one dimension array as shown in Eq. (7):

$$NEW\_IMAGE\,[P_{(x-1)\times N+y}]_{M\times N}\leftarrow IMAGE\,[P_{x,y}]_{M,N} \tag{7}$$

where $P_{x,y}$ denotes pixel P in location x and y.

3.2. Permutation (First part)

In the first part of permutation, to determine new location of P_i, X_i (Eq. (4)) is scaled in the range of $[1,\ M\times N]$ as stated in Eq. (8).

$$Location\_P_i\leftarrow Round\,(X_i\times(M\times N))+1 \tag{8}$$

3.3. Diffusion

In order to have a better understanding of diffusion process, a pseudo-code is listed in Table 3 which is marked by Line 1–9.

To diffuse P_i which is permuted in the Section 3.2 (Line1),$Y_i(Eq.\ 5)$ is scaled between 1 and 8 (Line 3) to choose one of the rules in Table 1 in order to encode P_i to DNA sequence (Line 6). In addition, a random number in the range of [0, 255] is generated (Line 5) and encoded (Line 4 and Line 6) at the same time, according to $Z_i(Eq.\ 6)$ and Table 1. As it clearly observed from Line 7, encoded P_i and encoded random number created new DNA sequence number when they are affected by DNA's XOR ($\bigoplus$) which is introduced in Table 2. Line 8 is to generate new rule number based on exist X_i where this new rule number is employed to decode new P_i(Line 9). To have a more secure diffusion process, obtained DNA sequence is changed when got XOR again to REPOSITORY which contains $New\_P_{(i-1)}$ (pervious diffused pixel) (Line 8).

Table 1
Encoding and decoding map rule of DNA sequence.

	A	T	C	G
Rule 1	00	11	10	01
Rule 2	00	11	01	10
Rule 3	11	00	10	01
Rule 4	11	00	01	10
Rule 5	10	01	00	11
Rule 6	01	10	00	11
Rule 7	10	01	11	00
Rule 8	01	10	11	00