Contents lists available at SciVerse ScienceDirect

Computers and Electrical Engineering

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

A RGB image encryption algorithm based on DNA encoding and chaos map ☆

Lili Liu, Qiang Zhang *, Xiaopeng Wei

Key Laboratory of Advanced Design and Intelligent Computing, Dalian University, Ministry of Education, Dalian 116622, China

ARTICLE INFO

Article history:
Available online 5 March 2012

ABSTRACT

In this paper, a RGB image encryption algorithm based on DNA encoding combined with chaotic map is proposed aiming at characteristics of RGB image. The algorithm firstly carries out DNA encoding for R, G, B components of RGB image; then realizes the addition of R, G, B by DNA addition and carries out complement operation by using the DNA sequence matrix controlled by Logistic; three gray images are got after decoding; finally gets the encrypted RGB images by reconstructing R, G, B components which use image pixels disturbed by Logistic chaotic sequence. Simulation result shows that the proposed algorithm has a large secret key space and strong secret key sensitivity. Meanwhile, it can resist exhaustive attack, statistical attack, and thus it is suitable for RGB image encryption.

1. Introduction

With the development of computer network technology, digital image is widely used in various fields of society. However, due to openness of the network, the security of image is threatened seriously, so the image encryption becomes the most effective way to guarantee transmit security of images [1]. Chaos is seemingly a random movement of deterministic system. Chaos system has the properties of ergodicity, boundedness, sensitivity to initial conditions. Therefore, using chaotic system in image encryption can meet certain security requirements. However, the chaotic encryption algorithms [2–4] which utilize one-dimensional chaos map, multi-dimensional chaos map and ultra-dimensional chaos map are all to transform the image pixel position and pixel values, a lot of Refs. [5–7] point out that using encryption algorithms constituted by a single chaos map are vulnerable to be interpreted.

Nowadays, DNA computing has permeated the domain of cryptography. DNA cryptogram utilizes DNA as information carrier and takes advantage of biological technology to achieve encryption [8–11]. Kang et al. had proposed a character encryption algorithm based on pseudo DNA operation [12], it made use of central dogma which belongs to molecular biology to implement encryption. However, DNA encryption methods have disadvantages such as expensive experimental equipment, complex operation and difficult to grasp its biotechnology, and still cannot be efficiently applied in encryption field.

In order to overcome the defects of the situation that a single chaos encryption is easy to be decoded and DNA encryption needs biological experiment, we presents RGB image encryption algorithm based on DNA encoding and chaos map. The proposed algorithm utilizes DNA addition to scramble the pixel values of image R, G, B components and then encrypt the scrambled images. Experimental results show that the algorithm which is simple to implement, can resist a variety of attacks, and can be easily applied to color image to scramble encryption, very suitable to use in secure communication. This paper is organized as follows. In Section **2**, we introduce the basic theory of the proposed algorithm. The details of designing the

☆ Reviews processed and approved for publication by Editor-in-Chief Dr. Manu Malek.

* Corresponding author.
E-mail address: zhangq30@yahoo.com (Q. Zhang).

0045-7906/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compeleceng.2012.02.007

proposed image encryption are proposed in Section **3**. Section 4 is simulation results. In Section **5**, security analysis is discussed. Section **6** gives the conclusion.

2. Basic theory of the proposed algorithm

The algorithm mainly uses the encoded matrix of DNA sequence to carry out DNA addition operation, and uses Logistic mapping function to implement image encryption.

2.1. DNA encoding

DNA computing is a form of computing which uses DNA, biochemistry and molecular biology, instead of the traditional silicon-based computer technologies. DNA computing, or more generally, bimolecular computing, is a fast developing interdisciplinary area. With the rapid development of DNA computing, the researchers presented many biological operations and algebra operations based on DNA sequence [13]. Single-strand DNA sequence is composed by four bases, they are A, C, G and T, where A and T are complement to each other, so are C and G. In the modern theory of electronic computer, all information is expressed by binary system. But in DNA coding theory, information is represented by DNA sequences. So we use binary numbers to express the four bases in DNA sequence and two bits binary number to represent a base. In the theory of binary system, 0 and 1 are complementary, so we can obtain that 00 and 11, 01 and 10 are also complementary. We can use 00, 01, 10 and 11 to express four bases and the number of coding combination kinds is 4! = 24. Due to the complementary relation between DNA bases, there are only eight kinds of coding combinations that satisfy the principle of complementary base pairing in 24 kinds of coding combinations. Table 1 gives eight encoding rules:

Example: The binary pixel value of an image is [00111010], so the corresponding DNA sequence is [ATGG] according to the first encoding rule, similarly according to the seventh decoding rule, the decoding sequence is [11001010]. In the proposed algorithm, we put the eight encoding and decoding rules mapped to the eight sub-region of (0,1), and using the seed generated by random number to choose different rules.

2.2. The addition and subtraction operation of DNA sequence

Since the development of DNA computing, scholars have proposed using algebraic operation of DNA sequence to replace the traditional computer algebraic operation. Based on this, we use DNA addition operation to realize DNA sequence matrix computing for R, G, B components. The algorithm of this paper finds out DNA addition and subtraction rules by using mod 2 operations of binary figure when 01 – A, 10 – T, 00 – C, 11 – G, and you can find the rules in Table 2.

The Logistic map is a polynomial map (equivalently, recurrence relation) of degree 2, often cited as an archetypal example of how complex chaotic behavior can arise from very simple non-linear dynamical equations. The map was popularized in a seminal 1976 paper by the biologist Robert May, in part as a discrete-time demographic model analogous to the Logistic equation first created by Pierre François Verhulst [14]. One-dimensional Logistic map is the most widely applied chaos map currently. The chaotic models generated by it are also known as insect amount model. Its mathematical define is as follows:

$$x_{n+1} = \mu x_n(1 - x_n) \tag{1}$$

where $\mu \in [0,4], x_n \in (0,1), n = 0,1,2,\ldots$, and we can find from the bifurcation diagram of Fig. 1 that when $2.6 < \mu \leqslant 4$ this dynamic system forks and generates two times period or four times period from the steady state. Vast multi-periods appear in the interval of smaller μ, and after forking n times, the length of period is 2^n; when $3.569945 < \mu \leqslant 4$, the system accesses chaos state and the chaotic sequences generated by it are non-convergent, aperiodic and having certain sensitivity to initial value; when $\mu = 4$, the Logistic map is surjection and while $x_n \in (0,1)$ the chaotic sequences have ergodicity [15].

The chaotic sequence in the algorithm of this paper has generation ways as follows:

(1) The real value sequence is generated by Logistic map while initial value is g_0, μ_0: namely $\{x_n, n = 0,1,2,\ldots\}$, it is formed by the chaotic map track points.

(2) *Binary sequences:* The real value sequence generated by chaotic map while initial value is g_0, μ_0, through defining a threshold function $f(x)$ and the threshold is 0.5, the definition is as follows:

Table 1
Eight kinds of DNA map rules.

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