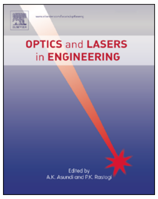
Optics and Lasers in Engineering 71 (2015) 33–41

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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



# A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata

Rasul Enayatifar [a], Hossein Javedani Sadaei [a], Abdul Hanan Abdullah [b], Malrey Lee [c,*], Ismail Fauzi Isnin [b]

[a] Graduate Program in Electrical Engineering, Federal University of Minas Gerais, MG, Brazil
[b] Faculty of Computing, Universiti Teknologi Malaysia, Johor, Malaysia
[c] The Research Center for Advanced Image and Information Technology, School of Electronics & Information Engineering, ChonBuk National University, ChonBuk, JeonJu 561-756, Republic of Korea

ARTICLE INFO

*Article history:*
Received 24 December 2014
Received in revised form
3 March 2015
Accepted 9 March 2015
Available online 30 March 2015

*Keywords:*
Image encryption
Deoxyribonucleic acid (DNA)
Cellular automata (CA)
Chaotic map
Tinkerbell map

ABSTRACT

Currently, there are many studies have conducted on developing security of the digital image in order to protect such data while they are sending on the internet. This work aims to propose a new approach based on a hybrid model of the Tinkerbell chaotic map, deoxyribonucleic acid (DNA) and cellular automata (CA). DNA rules, DNA sequence XOR operator and CA rules are used simultaneously to encrypt the plain-image pixels. To determine rule number in DNA sequence and also CA, a 2-dimension Tinkerbell chaotic map is employed. Experimental results and computer simulations, both confirm that the proposed scheme not only demonstrates outstanding encryption, but also resists various typical attacks.

## 1. Introduction

Nowadays, to send information such as digital images and videos through the internet and other kind of innovation technologies have become a significant task and protecting content of these data is quite a serious problem, as well [1,2]. In recent years, to protect the security of these types of information, numerous image encryption methods have been developed [1–15]. Although preliminary encryption methods such as IDEA, AES, RSA and DES focused on the high correlation among adjacent pixels in digital image, these methods are not efficient enough for suitable encryption [16,17]. To have almost a comprehensive algorithm, different categories of image encryption are introduced by scientists.

The first group is an optical image encryption approach, which is inspired by domain transform techniques such as discrete fractional Fourier transform (DFrFT) [18,19], fractional Fourier transform (FrFT) [7,15], gyrator transform [10,20] and Arnold transform [21,22].

Second group focuses on chaos-base image encryption, which satisfies confusion and diffusion strategy [13,14,23,24]. This group is well-known due to the specific features of a chaotic map which causes many attentions among scientists. This type of image encryption normally contains permutation and diffusion step [17,25]. All pixel position is reallocated by using chaotic map in the permutation step while gray-level of pixels not changed. Unlike the permutation, in diffusion step all pixels gray-level will be changed with the help of chaotic map.

One of the latest encryption methods is based on optimization algorithm [1,2,13]. In almost all of these kinds of methods two sequential steps are performed. At first, chaotic map is employed to specify numbers of cipher images which are extracted from the plain image. In the second step, optimization algorithm exhibits an evolutionary trend to improve the quality of cipher images and finally demonstrate the best cipher image as the output of the encryption algorithm.

Another popular image encryption method is based on deoxyribonucleic acid (DNA) which has excellent inherent feature that cause DNA appears to be suitable for high-security encryption [1,26–29]. The DNA-based approach includes two phases where the first phase applied DNA theory to encode plain image pixels to a DNA sequence and those rules are also used to generate the key image. In the next phase, DNA operation rules affect encoded plain-image pixels and finally generate cipher-image.

The last main category that we would to explain is using cellular automata (CA) for secure image encryption [8,30–33]. The CA

[*] Corresponding author.
*E-mail addresses:* Hanan@utm.my (A.H. Abdullah), Mrlee@chonbuk.ac.kr (M. Lee).

http://dx.doi.org/10.1016/j.optlaseng.2015.03.007
0143-8166/© 2015 Elsevier Ltd. All rights reserved.

normally uses to generate secret key and public key in encryption theory. Many image encryption algorithms employ CA to generate a pseudorandom bit to create the encryption sequence.

Nowadays, researchers attempted to combine different mentioned categories in order to propose a more secure image encryption scheme [1,13,29,34,35]. In this work, we investigated an image encryption method which is created using the chaotic map, CA and DNA, simultaneously. Firstly, all the plain-image pixels should be converted to DAN nucleic acids by standard rules which are defined in DNA sequence, then, CA and its 256-standard rules are employed to generate a new sequence for encrypting plain-image pixels. In order to choose standard rules in DAN sequence, we need proper tool which has likely randomness behavior and in this case 2 dimension chaotic map, namely Tinkerbell map [36] seems quite suitable for our purpose. Combination of CA, DNA and Tinkerbell map make proposed algorithm very strong against common attack in the image encryption method.

The rest of paper is organized as follow: Section 2 presents preliminary algorithm of this work. Proposed algorithm will be described in Section 3. Simulation results and security analysis are drawn in Section 4. The conclusion is provided in Section 5.

## 2. Preliminaries

There are three preliminary concepts contain Tinkerbell chaotic map, DNA sequence and CA, which are significant for understanding the proposed method.

### 2.1. Tinkerbell chaotic map

A group of functions which are quite sensitive to initial parameters value called chaotic maps. These functions show chaotic behavior where a slight change in initial parameters causes huge alteration in those values which are generated by chaotic function. There are various types of chaotic functions, whereas one of them is Tinkerbell chaotic map. It is 2-dimension function that is defined as

$$
\begin{aligned}
x_{n+1} &= x_n^2 - y_n^2 + a x_n + b y_n \\
y_{n+1} &= 2 x_n y_n + c x_n + d y_n \qquad (1)
\end{aligned}
$$

Fig. 1 shows the Tinkerbell chaotic map behavior with $n=1,\ldots,1000$ and $x_1=-0.5;\ y_1=-0.5$ and $a=0.9;\ b=-0.6013;\ c=2;\ d=0.5$.

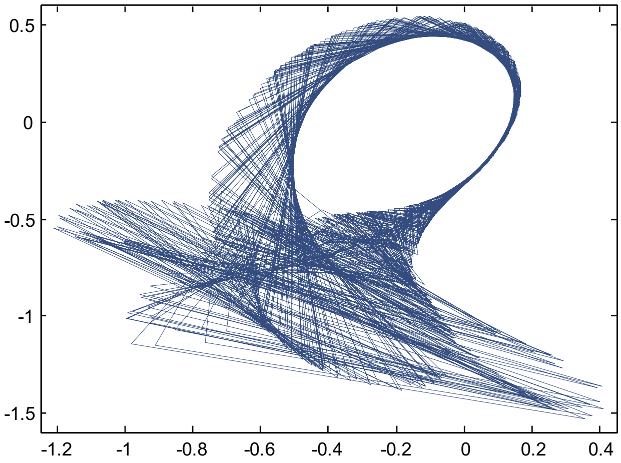


**Fig. 1.** Tinkerbell chaotic map with starting $x_1=-0.5;\ y_1=-0.5$ and parameters value $a=0.9;\ b=-0.6013;\ c=2;\ d=0.5$.

### 2.2. Cellular automata

Cellular automata (CA) is a non-linear dynamical system in which time and space are discrete and it can be expounded as mathematical model for systems containing a large set of simple identical components [37,38]. A CA is composed of a regular grid of cells where each cell has a finite number of states, such as on and off. In one dimension CA, each cell has two neighborhoods which are situated on the left side and right side of it. Each CA will update its next state synchronously based on existing rules in the database. These rules are generated according to the current state of each cell and its neighborhoods states and these rules are typically fixed throughout the iterations. For each cell there are two values, 0 and 1. Therefore, $2\times2\times2=2^3$ possible binary states for the three cells neighboring a given cell, there are a total $2^8=256$ cellular automata, each of which can be indexed with an 8-bit binary number [39]. For instance, rule number $45=(00101101)_2$ can be defined in Fig. 2.

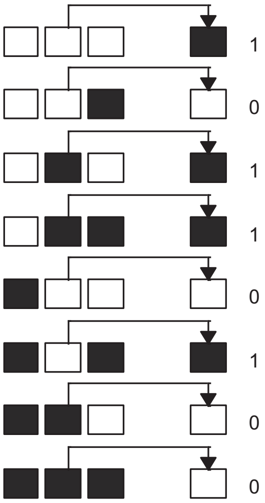


**Fig. 2.** Expanding 45 in CA.

### 2.3. Deoxyribonucleic acid sequence

The huge deoxyribonucleic acid (DNA) usage in biological science and others applied fields such as biotechnology; diagnostic and forensic make it very vital for scientists [1]. The DNA contains four types of nucleic acids, namely, A (adenine), T (thymine), C (cytosine), and G (guanine). There is an important rule in base pairing that mention (A) and (C) are always pair with (T) and (G), respectively [40]. Therefore, it is obvious that A and T are complementary, and also G and C are complementary [40,41]. These relationships are known Watson–Crick base pairing rules [42]. Beside of these rules, in the binary numbering system, 0 and 1 are complementary. Therefore, it can be concluded that 00 and 01 are complementary with 11 and 10, respectively. Table 1 introduces coding and decoding map rules of the DNA sequence, in order to satisfy the Watson–Crick base pairing rule. For better understanding, we have given an example for a pixel with grayscale $229 = (11100101)_2$. The DNA code for all existing rules in Table 1 is as follows: Rule1 (TCGG), Rule2 (TGCC), Rule3 (ACGG), Rule4 (AGCC), Rule5 (GATT), Rule6 (GTAA), Rule7 (CATT) and Rule8 (CTAA).

Considering the development of DNA computing, some algebraic and biological operators are released [43,44]. The operation exclusive OR $(\oslash)$ for DNA sequence is drawn in Table 2.