Color Image Encryption Depend on DNA Computing

Matheel Emadaldeen and Zena mohammad saadi

University of Technology-Computer science department

Abstract

DNA computing has prevailed in the field of cryptography. DNA cryptography uses DNA as an information transporter and gets benefit from biotechnology in order to achieve encryption. Encryption character algorithm proposed by Kang et al relying on pseudo-DNA operation, However, DNA encryption methods have defects such as expensive experimental equipment, complex operation and difficult to understand its biotechnology and remains cannot be effectively applied in encryption field. Also the chaos theories can generator dynamic system with random numbers. In this paper; a design new approach for encryption image was suggested depending on proposal DNA computing such as (coding, decoding) with multi-operation in festiel structure to increase more complexity when an attacker tries image retrieval. When used NLFSR as random generate system to mixing to increase complexity also was proposed new idea to generated secret key. A performance analysis in measurement test between the original image and encryption image was evaluated, the values rustle is big to depend on no correlation for a pixel in original and cipher image. Another test between plain image and clear image after decryption are good values for a statistical test. MSE is equal to zero and PSNR infinity number because no loss data or difference in this approach was found.

Keywords: color image, encryption, decryption, DNA, chaotic map.

تشفير الصورة الملونة بالأعتماد على حوسبةDNA

مثيل عماد الدين   و   زينه محمد سعدي

الجامعة التكنولوجية ـ قسم علوم الحاسوب

الخلاصة

حوسبة الـDNA قد تخللت في مجال التشفير. تشفير DNA استخدم DNA كحامل معلومات واستفاد من ميزة التكنولوجيا الحيوية لتحقيق التشفير . كانغ وآخرون اقترحو خوارزمية تشفير الأحرف بالأعتماد على عملية pseudo DNA ، ومع ذلك ، فأن طرق تشفير DNA لديها مساوئ مثل معداتها التجريبية الباهضة الثمن وعملياتها المعقدة وصعوبة فهم التكنولوجيا الحيوية لها والتي لاتزال لايمكن تطبيقها بكفاءة في مجال التشفير. ان نظريات الفوضى ممكن استخدامها كنظام ديناميكي ويعمل على توليد الارقام العشوائيه. في هذا البحث صمم نموذج لتشفير الصورة بالأعتماد على حوسبة DNA المقترحه مثل (الترميز وفك الترميز)وعمليات متعددة في النموذج الشبكي festiel لزيادة التعقيد عندما يحاول احد المهاجمين استرجاع الصورة. وعند استخدام NLFSR كنظام مقترح لتوليد الارقام العشوائيه اللتي تدمج مع بيانات الصوره يودي الى زياده التعقيد بالاضافه الى اقتراح طريقه جديده لتوليد المفتاح السري. وقد تم تقييم تحليل الأداء في اختبار القياس بين الصورة الاصلية والصورة المشفرة ، القيم هي كبيرة بالأعتماد على عدم وجود علاقة بين البكسل في الصورة الاصلية والمشفرة. أختبار آخر هو بين الصورة الاصلية والصوره بعد فك التشفير هي قيم جيدة لأختبار احصائي. MSEمساوي للصفر و PSNR هو عدد غير منتهي بسبب عدم وجود فقدان بالبيانات أو اختلاف بهذه الطريقة.

كلمات مفتاحية: صورة ملونة , التشفير,فك الشفرة , DNA , نظرية الفوضى**.**

Introduction

Information security is the act of defending information from any improper use and illegal access to the resources via different objectives. It has been developed over different stages through several past years. The rapid growth and huge demands indicate the need to invest into researches. Intensive research has passed through different phases in order to keep pace of the developments required over past 50 years. This included investigation of cryptographic methods, generic security of computing devices, operating systems and networks [1]. Information security objectives aim to assure that risk can be reduced to a lowest possible percentage. The major objectives of the information security can be expressed as confidentiality, integrity, authentication, identification and availability [2]. In various areas of

society, the digital images have become used on a large scale with the development of computer network technology. But due to the openness of the network, image security is exposed to serious threat by the attackers; therefore, the image encryption becomes the most effective way in order to guarantee to transmit security of images [3]. In DNA computing, also familiar as molecular computing, a DNA computer is basically a set of DNA strands correlated that solves some of the problems, relying on the problem, technology is currently available both to select the initial tracks and to filter the final solution. The DNA computing is massive parallelism: can solve huge problems with a particular system and enough DNA by using parallel search. This can be much faster than a classical computer that would require a large amount of hardware massive parallelism, not simply more DNA [4].

Related work

Several researches have used image encryption using DNA computing with chaos theory and other operations. Lili Liu, Qiang Zhang , Xiaopeng Wei,2012, have proposal ," A RGB image encryption algorithm based on DNA encoding and chaos map"[5]. In this paper, a RGB image encryption algorithm based on DNA encoding combined with chaotic map is proposed aiming at characteristics of RGB image. Song and Yulong Qiao ,2015,have proposed " A Novel Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos**"[6].** In this paper, we propose a novel image encryption scheme based on DNA encoding and spatiotemporal chaos. In particular, after the plain image is primarily diffused with the bitwise Exclusive-OR operation, the DNA mapping rule is introduced to encode the diffused image. Y. Allen Daniel , Harish. J , Aswin.S , S. Sankar,2015,have proposed" Encryption then Compression Based on Image Fusion, Chaotic Map and DNA Subsequence Operation"**,** [7]. This paper deals with image encryption and compression based on chaotic map and DNA Subsequence Operation and hence overcomes the drawback of existing techniques. The image initially undergoes image fusion where two or more similar images are combined into a single image and the fused image is more informative than the input images.

DNA Image Encryption

Of the most common methods to support the image security is encryption. There are many applications to encrypt image and video in several areas, including the multimedia systems,

tele-medicine, internet communication, medical imaging, and military communication and to achieve these purposes; Researchers are constantly looking for methods of encrypting more secure [8]. Since the vast parallelism, extraordinary information intensity, and exceptional energy efficiency all are inherent in DNA molecules. DNA cryptography is a new promising field of cryptography that has become an important direction with the development of DNA computing. As it is known the DNA cryptography has many benefits in the research of DNA computing, but is not equal to the DNA computing, because there is the main difference between them. In DNA computing, the DNA technology is used to solve difficult computational problems but in DNA cryptography, several difficult biological problems are used as the security of DNA cryptosystems. Can be considered the processes of cryptography as computation but not all DNA computations relate to cryptography. Cryptography-DNA is built on the information carrier of DNA and takes the advantage of biological technology, which has been proved good results in the image encryption. In last few years, a large amount of data computational and NP problem produced with the rapid development of the technology of science and social. But DNA computer has excellent properties to process efficient parallel and mass storage capacity problem [9] [10]. In 1994, Directed Hamilton path problem is resolved by Dr. Adleman by DNA computing that enhances the capabilities of the study area [11]. In digital image, it is not reasonable to use conventional encryption methods on it because a large data size and real-time requirements. Thus, a main trend is to minimize the computational requirements for secure multimedia distribution. There are a number of encryption algorithms available such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA) and RSA (developed by Rivest, Shamir, and Adleman).These traditional encryption algorithms have disadvantages and they are not considered as ideal for image applications, because of the low level of efficiency when dealing with large and excessive blocks of image data. In addition to, these algorithms require power and more than the ordinary expected computation time during the performance image encryption [12] [13].

Scheme for Encryption and Decryption of Image using DNA

The algorithm principally uses the encoded matrix of DNA sequence in implementation DNA addition, subtraction operations, and uses many functions to implement image encryption with special tables for DNA, can explain in the following figure [5].

+	A	C	G	T
A	A	C	G	T
C	C	G	T	A
G	G	T	A	C
T	T	A	C	G

-	A	C	G	T
A	A	T	G	C
C	C	A	T	G
G	G	C	A	T
T	T	G	C	A

Figure (1): Addition and Subtraction operations

Chaos Theory

A chaotic system is a simple, non-linear, dynamical, and deterministic system that shows completely unpredictable behavior and appears random. Moreover, it is a deterministic system with great sensitivity to initial conditions; for example computer system can give an amazingly different result when the value of an input parameter is changed. On the other hand, in classical science, small changes in an initial value might generate small differences in the result [14] [15]. A system is called a chaotic system if it is sensitive to initial conditions, topology mix, and if periodic orbits are dense [15].

1. Logistic Map

Discrete chaotic of logistic map is a simple non-linear dynamical map. A logistic map is one of the most popular and simplest chaotic maps .The logistic map is a polynomial mapping, a complex chaotic system, the behavior of which can arise from very simple non-linear dynamical equations. The logistic map is written as [16]:

$$Xn+1=Xn* r * (1-Xn) \qquad (1)$$

Where x_n is a number between zero and one, x_0 represents the initial population, and r is a positive number between zero and four. But when r between (3.5, 4) is good random. The logistic map is one of the simplest chaotic maps; it is highly sensitive to change in its parameter value, where a different value of the parameter will give a different map f, can explain in following figure [17].
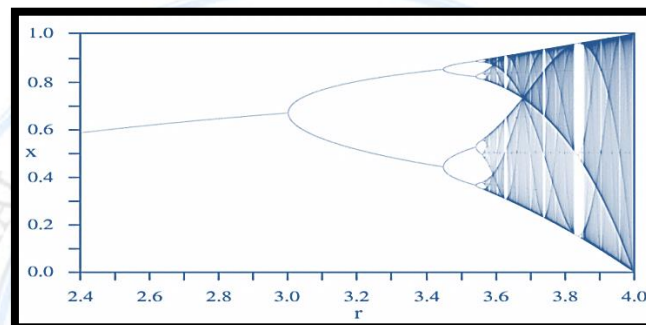

Figure (2): Bifurcation of the Logistic map[17]

Proposed a New Approach for Image Encryption depends on DNA computing

The proposed approach is designed depending on DNA computing and operation in DNA such as (encoding, decoding, addition, subtraction, and complement) to increase computation complexity used feistel structure as block cipher with multi operation in diffusion. This algorithm designed depends on numbers of proposal function difference with stander functions in DNA and block cipher. Figure (3) and figure (4) explain the general structure for the proposed algorithms.
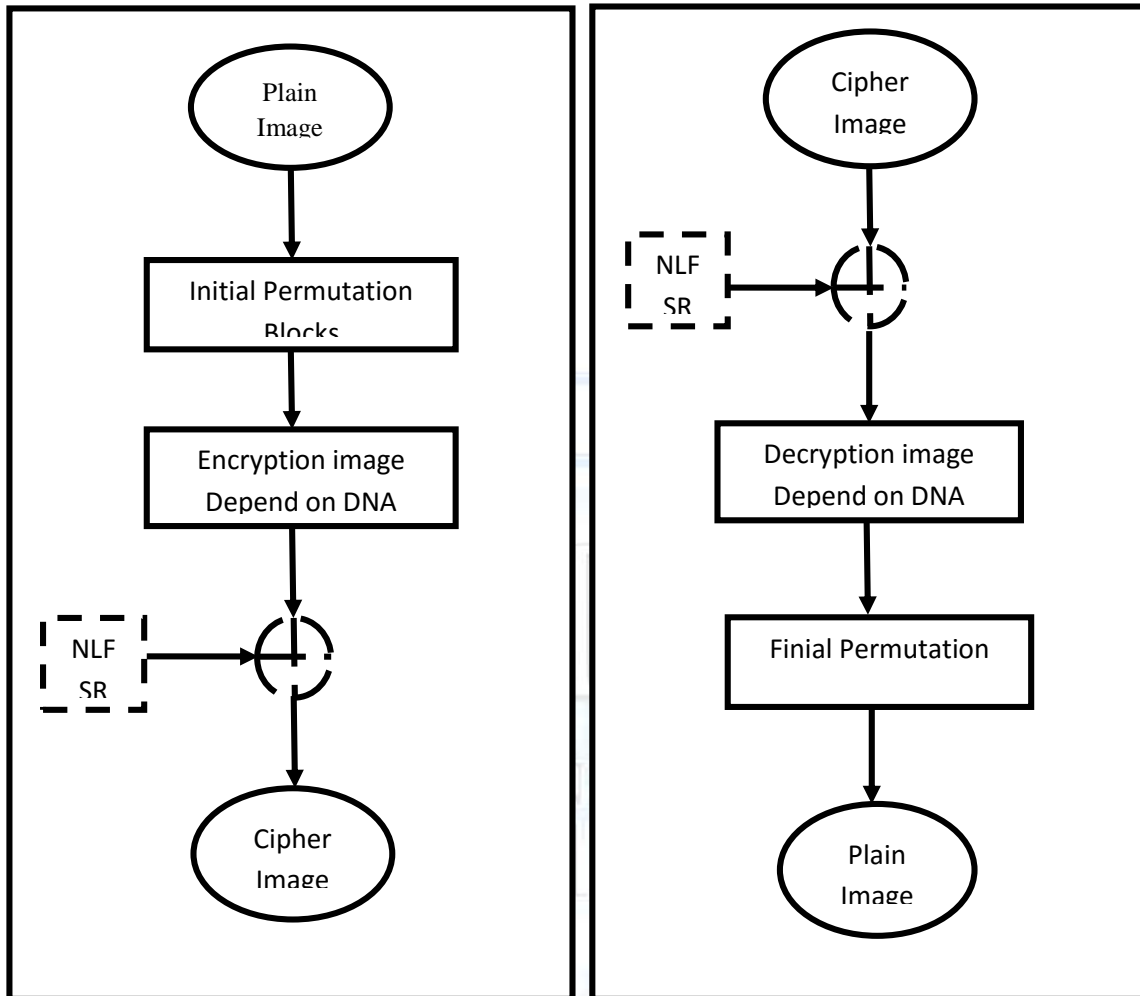
Figure (3): Encryption Structure.   **Figure (4):** Decryption Structure.

In the following figures the general algorithms for encryption and decryption:

Algorithm (1) :Encryption Algorithm	Algorithm (2) :Decryption Algorithm
Input: Plain image.	**Input:** Cipher image.
Output: Cipher image.	**Output:** Plain image.
Begin	**Begin**
Step1: Divide image into blocks, each block as 256 byte size in blocks array.	**Step1**:XOR operation between cipher image with NLFSR.
Step 2: Initial permutation was done for blocks array depending on shifting map.	**Step2**: DNA decryption was done.
Step 3: DNA encryption to blocks array is done.	**Step3**: Divide image into blocks, each Block as 256 byte size in blocks array.
Step 4: XOR operation between blocks array with NLFSR is done.	**Step4**: Final permutation was done for each block depend on inverse shifting.
End	**End**

In algorithm (1).The plain image was divided into many blocks with size 256 byte ,these blocks are permutation as reordered for location depending on symmetric values(secret map) as shifting of location (the same map in encryption and decryption but in reverse order). After IP-Block operated for blocks array, the blocks array is processed and encrypted using DNA encrypting operation. The last operation was the output from DNA encryption that enters to XOR operation to get cipher image. Algorithm (2) was the same structure of encryption with some inverse functions. The proposed structure consist of many algorithms in Initial Permutation (IP) and DNA operation (encoding, decoding, complement, addition and subtraction, DNA IP-Box) that can be explained in algorithms (3) and (4) as a secret mapping for diffusion in forward and backward. In the first process, convert image file to an array of the block each block has 256 bytes ,this array is processed by the first layer in above encryption algorithm (IP-blocks) and can explain in the algorithm(3).

Algorithm (3) :Permutation Algorithm

Input: Array of Block(),Length of Array Block

Output: IP-Block ().

Begin

Step 1: Count1=0,Count2=0

Step2: For i=0 to length of array Block -1

IP-Block(Count1)= Array of Block (i)

Count1=Count1+4

if (Count1> length of array Block) then

Count2=count2+1

Count1=Count2

End if

Next

End

Algorithm (4) :Final Permutation Algorithm

Input: Array of Block(),Length of Array Block

Output: IP-Block ().

Begin

Step 1: Count1=0,Count2=0

Step 2: For i=0 to length of array Block-1

 IP-Block(i)= Array of Block (Count1)

Count1=Count1+4

if (Count1> length of array Block) then

Count2=count2+1

Count1=Count2

End if

Next

End

Algorithm (3) for diffusion of blocks (Block locations re-order) was used to increase more complexity. When the first location in block array shifted to the first location in the new array, the second location from the original array is shifted to four locations depend on pulse fourth in each shifting and so on to reorder all location (shifting to left). The inverse of IP-blocks used in decryption algorithm can explain in the algorithm (4). The second layer in the proposed algorithm is DNA encryption depending on proposal multi-operation in DNA operation that can explain in figure (3). In this approach, the IP-blocks that were an input from the previous layer can divide in left part and right part, each part has different processes. The left and right part has three processes (DNA coding, DNA sum, and decoding) and the right part has a process

as (preprocess, DNA P-Box and complement).The proposed algorithm can explain in figure (5).
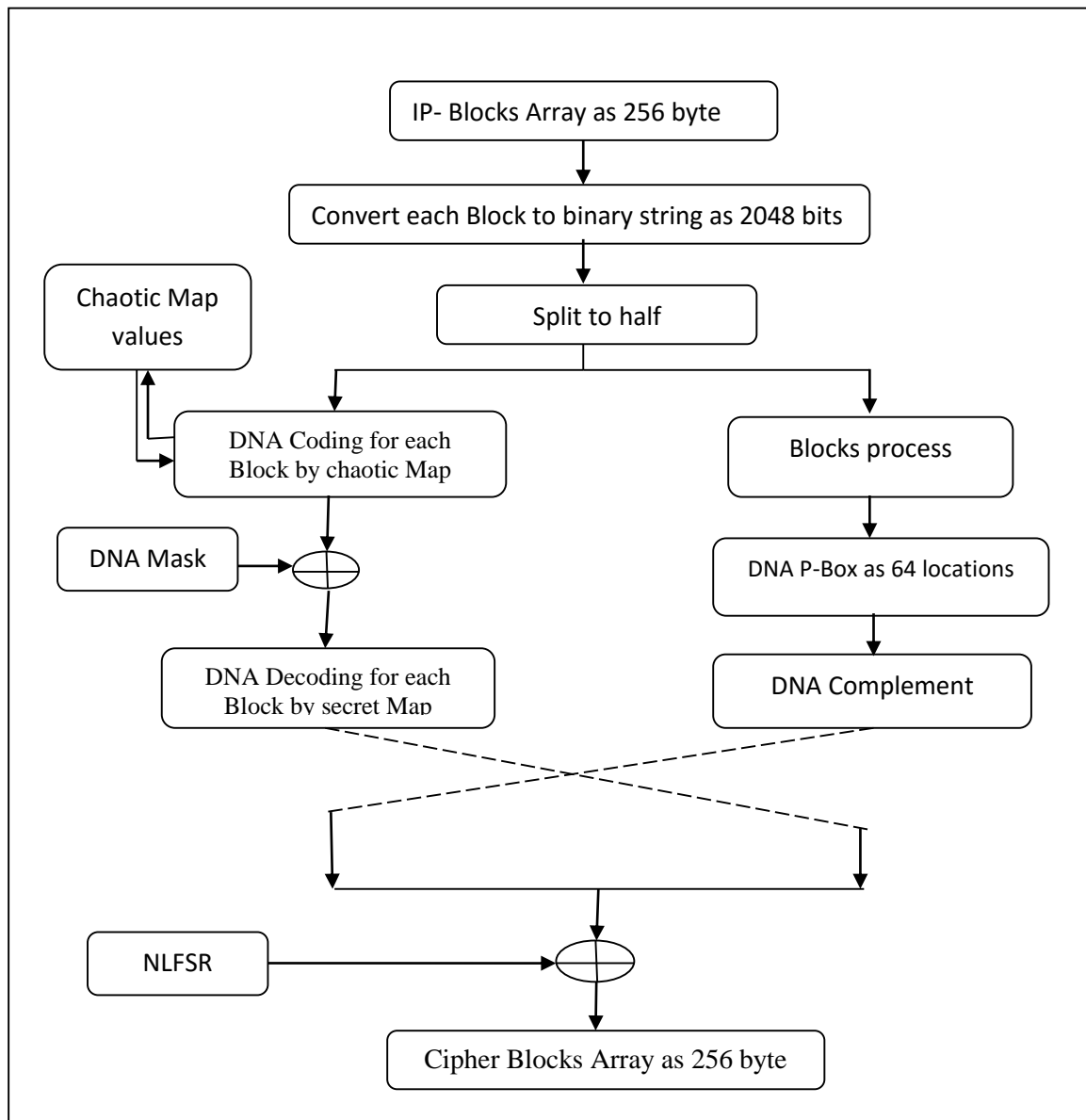

Figure (5): DNA Encryption Structure.

In the decryption process, all operation in encryption algorithm does in decryption but some in reverse order and directional but another operation as symmetric as XOR operation. To can explain the DNA decryption structure in figure (6).
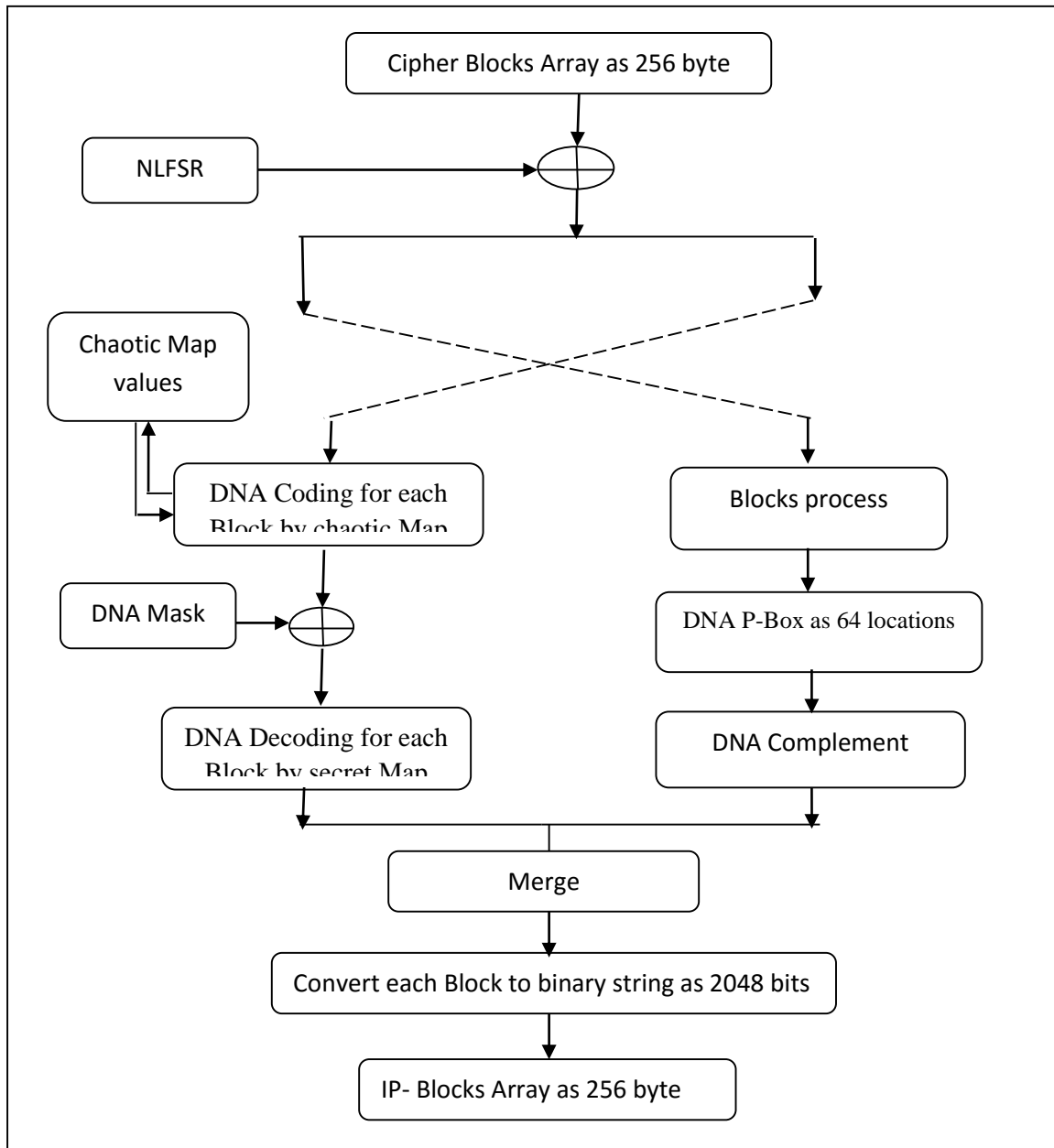
Figure (6): DNA Decryption Structure.

In the beginning, fetch block as size 256 byte from left part from the image, this block must be converted to DNA coding depend on of DNA table rule. This table consist of 8 columns for convert each two bit to (A, T, C, G), the first byte has 8 bits convert to 4 characters in the first column and second byte convert in the second column and so on. But in this structure we can a

proposed a new idea to select the number of columns depending on the chaotic equation to generate a number, this number used as security map. Each number in this map is present a number of a column from rule table to convert as DNA coding. This proposal algorithm depends on chaos theory as logistic map; this algorithm generates many of random numbers and chooses one number to select a number of columns for coding and decoding in DNA special table coding. The choose number must present a column between 1 to 8, sometimes the generating number in the proposal algorithm has number 0 or number 9 but in table DNA, it does not have this column numbers so it must process this number in delete manner.The mask generator algorithm depends on generating multi-keys from original key by using diffusion principle in feistel key generator, in the beginning input the security key as 16 bytes, the first process converts 16 bytes to 128 bits by binary process after that create 2-D array that has 16 row each row present array 1-D or vector as 128 bit, this 2-D array generated by shift and rotate to left 16 time each row has n^{th} time to get new row and put in 2-D new as binary array-Key(16,128) bits as mask key. To increase complexity in new binary array-Key we reordering of row location depend on security map to more diffusion. To get new array or string as 16 bits that can get by cut one bit from (i) location for each row in binary array-key to explain that cut and contacts each location (1) from all rows to get string1 as 16 bits size, in second cut location 2 from each rows in binary array 2 to get string 2 as 16 bit and so on, after end the process previous stage, one can has 128 string each one has 16 bits. To get DNA coding convert each row from 16 bits to 8 characters (A, C, G, and T) depending on DNA table coding. In the final step, one can have 128 rows each row has 8 characters so 1024 DNA coding using as mask or security key in addition (encryption) and subtraction (decryption) algorithm, the security key is symmetric in sender and receiver side. After ending the previous process one must convert the result by DNA decoding depending on DNA table in inverse operation. The new left side convert to binary and swap(as permutation operation) with old right and put in cipher file image. The right side has half size of the image, in begin fetch 265 bytes as a block and by using preprocess function convert to 16 locations each location has 16 bytes. Convert each cell from 16 bytes to binary as 128 bits depending on binary function, these 128 bits convert to DNA coding depending on DNA table to get 64 characters (A, D, T, C) the first string 64 characters permutation in location by proposal new IP-Box. After this process, to get new 64 characters, complement operation in

DNA used to complement final result depending on the complement table to get more confusion. Each 64 characters must decode to get binary as 128 bits for each block, and reverse operation. Each block as 256 bytes put on the right side and so on, so the right side is complete. When right side swap to the new left side, the exchange right and left side is done to increase more complexity for cryptanalysis. In the previous sections, the old P-Boxes function generates from linear equation, the P-box can breakable depend on a linear attacker, so can suggested new nonlinear P-Box depending on private equation, this equation has nonlinear principle but generator sometimes many repeated numbers. So, can execute this equation to more than size for needed P-Box, the size of P-Box are 64 location, and check the values must not repeated to insert in new P-Box. After complete building the secret map(P-Box) of reordering location in DNA input, (P-Box^{-1}) inverse map to use in decryption or reorder to the original location. This P-Box has more speed comparison with tradition a P-Box because in old P-Box the exchanging is done bit by bit but in proposals permutation as 2 bit in each time (2 bit as one character coding A, T, C, G) used to permutation for each location in the block. In decryption algorithm used the inverse DNA P-box inversed. After merge operation between the new left and new right side put in cipher image file to get cipher image ,but to more complexity, one can use the primitive and irreducible polynomials to generate big randomness string binaries, this final output string from generating XOR with cipher bytes and put in cipher image. Each polynomial has the big degree to max period to prevent output repeated; the first and second polynomial has LFSRs, the nonlinear filter combine between two output polynomials. The explanation was introduced in equations (2) and (3) to generate the output in equation (4):

$$F_1(x): \quad x^{16} + x^{11} + x^7 + x^5 + 1 \tag{2}$$

$$F_2(x): \quad x^{13} + x^9 + x^7 + x^5 + 1 \tag{3}$$

$$\textbf{Output} = (f_1(x) \text{ and } f_2(x)) \quad \text{XOR } f1(x) \tag{4}$$

Time and complexity of the Proposed Structure

In this part, one will try to find out some aspects of evaluation concerning speed, complexity and resistance against known attack as a comparative study with some blocks cipher system.

Color Image Encryption Depend on DNA Computing

Matheel Emadaldeen and Zena Mohammad Saadi

The speed of the proposed structure and run methods is design as feistel structure to more complexity in diffusion .Then they are applied to an image with different sizes. The image has a bitmap (BMP) type and with size K that is taken and encrypted and the running time of its operation is computed. Then the 66K, 117K, 168K, 198K, and 792K are taken and the running time of encryption and decryption of each image are calculated. Another type as JPEG, TIFF was used because it is higher resolution and lossless image can clear in tests, table (1) explains the running time evaluated.

Table (1): Compare between plain image and decryption

Image Dimension	Image size	Encryption time	Decryption time
150x150	66 k	3 sec.	3 sec.
200x200	117 k	5 sec.	5 sec.
240x240	168 k	7 sec.	7 sec.
260x260	198 k	7 sec.	8 sec.
520x520	792 k	25 sec.	25 sec.

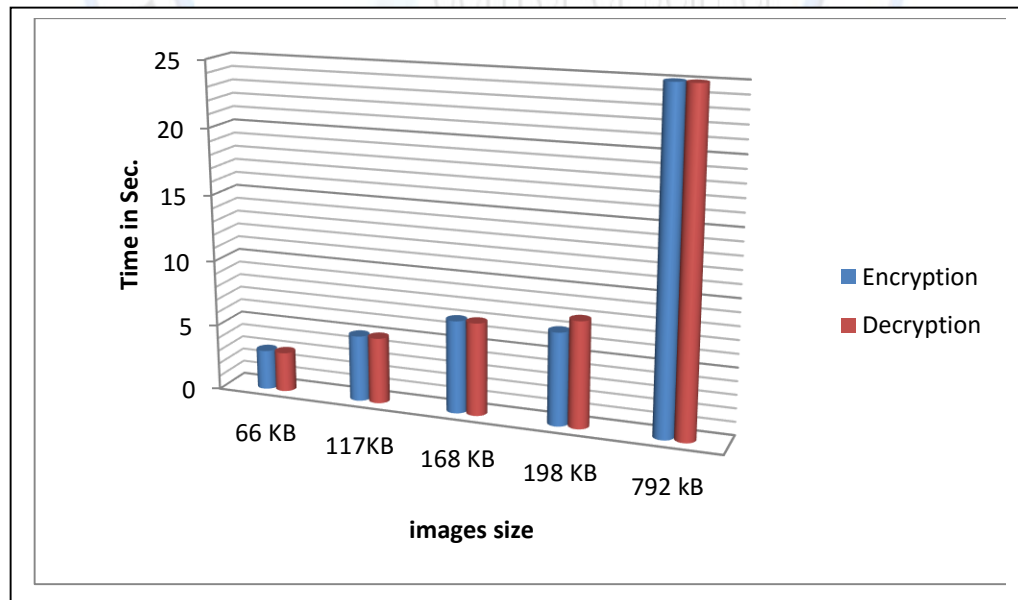Also, it can be explained in figure (5) for time encryption and decryption.

Figure (5): Encryption and Decryption Time.

The complexity of any encryption algorithm cipher depends on key length and operations in algorithm, but in the proposed structure the complexity is computed by addition operation such as DNA operation such as (encoding, decoding, addition, subtraction, and complement), DNA permutation operation and used linear operation between encryption block (from proposed structure) and reminder key from NLFSRs system. On the other hand, the complexity of the proposed structure has depended on the complexity of feistel network and DNA computing, measurement of proposed approach structure.

The proposed structure depends on:

- New table for DNA IP-Box DNA IP-Box^{-1} for permutation as DNA character to more speed by using nonlinear equation generator.
- Using a chaotic map to generate numbers of a column in DNA table coding.
- Using linear operation between the result from DNA encryption and all blocks has difficult decryption to get original blocks.

Key Space Analysis

One of the parameters used to measure the security of an image encryption algorithm is its key space. As the key space increases, the security of encryption improves. The method describes an encryption technique that uses a color image of different size pixels. This key space is large enough to resist exhaustive attacks. The technique uses an input key size of 128-bits as (2^{128}) to breakable in brute force attack. To increase complexity, the initial condition in chaotic as $X_0=0.99$ and $r=3.6$ must be symmetric to generate same values and used in send and receive (encryption and decryption) and modify any values that produced other numbers as column number in DNA table. Also, one can need same equations to generate symmetric keys for XOR operation, when modifying in equation one or two produce another output, this equation generate more bits to maximize period.
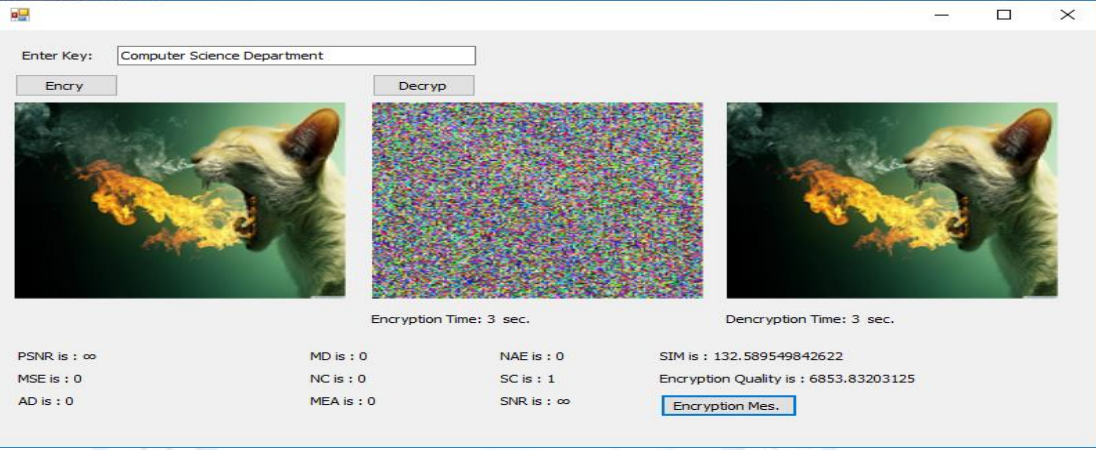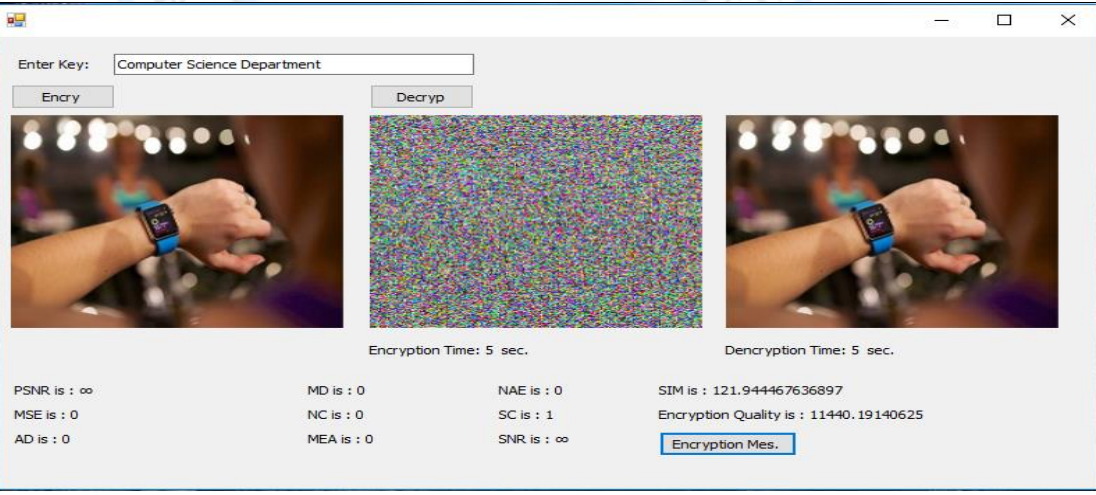
Implementation and Performance Analysis

In this section we are programming new block cipher depend on DNA computing and another mathematical. The implementation requirements to proposed approaches, the visual studio.net 2013 as software, the program have easy interface and many of tools to powerful of

programming, and used laptop computer C.P.U core I5 and RAM 4M, used different of images size, each image used unique key to encryption and decryption process,

The test images have different size. The results after encrypting to plain images using me proposed algorithm are given. The diffusion characteristics include PSNR, MSE, MD, AD, NC, MEA, NAE, SC, SNR, SIM, and EQ, that can explain the result in the table (2).

Table (2): Encryption and Decryption five Images

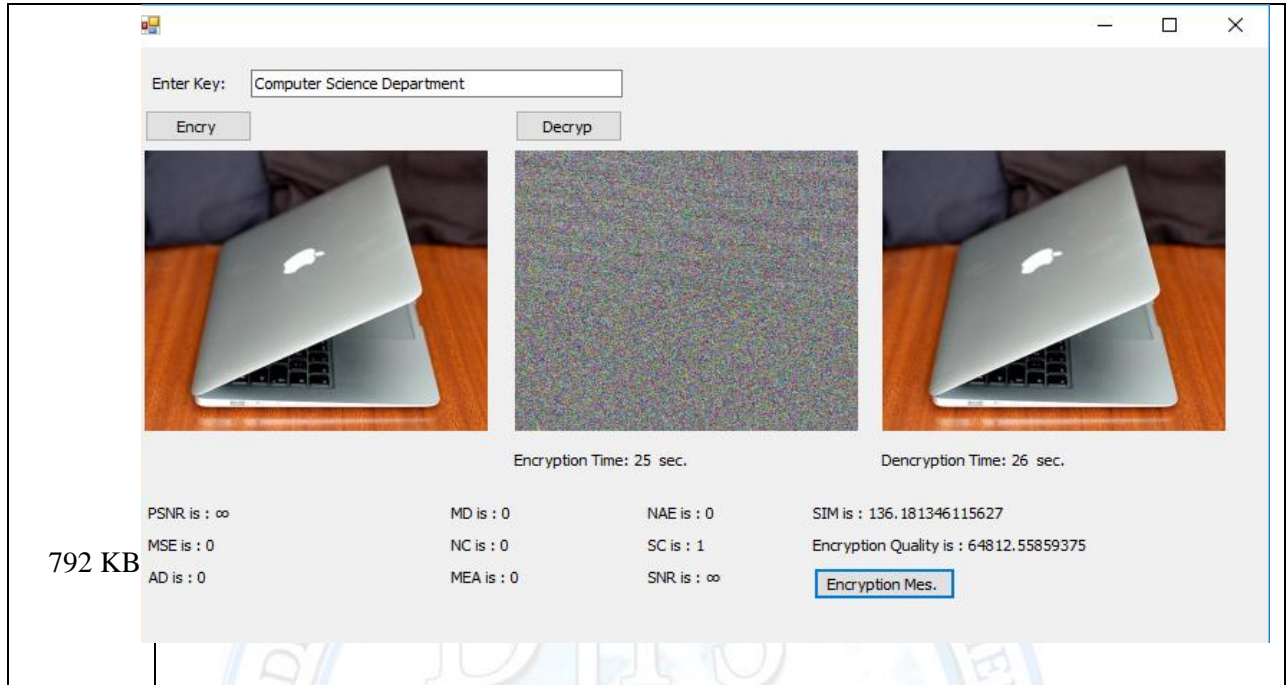| Image size	Interface encryption and decryption with different keys
66KB	
117KB	

168 KB

198 KB

Table (3): Compare between plain image(original) and decryption

Image size	150*150 66.2 KB	200*200 117 KB	240*240 168 KB	260*260 198 KB	520*520 792 KB
PSNR	100 or infinity	100 or infinity	100 or infinity	100 or infinity	100 or infinity
MSE	0	0	0	0	0
AD	0	0	0	0	0
MD	0	0	0	0	0
NC	0	0	0	0	0
MEA	0	0	0	0	0
NAE	0	0	0	0	0
SC	1	1	1	1	1
SNR	100 or infinity	100 or infinity	100 or infinity	100 or infinity	100 or infinity
SIM	132.5895	121.9444	189.4609	166.9186	136.1813
Quality encryption test is between plain images and cipher images					
EQ	6853.8320	11440.1914	18300.9032	18605.5859	64812.5585

When studying the tests performance, the PSNR values for many images are infinity because MSE as zero values because no difference in pixels in plain and decryption image. PSNR is a measure of return infinity values that depend on images size that can present as 100 percentages.

The remind characteristics as equal or near from size because no modify or loss information between plain and decryption image so that the result are equal to zero. In the last one (encryption quality) it must work between the plain and cipher images to test the powerful and quality encryption, the high values produce good encryption and difference in pixels. It also depends on image size and many of difference in pixels.

Conclusion

The proposed algorithm enhances two criteria of a standard block cipher, which are confusing and diffusion in feistel mode with DNA computing. The DNA operation such as (addition, subtraction, complement) has no more complexity because the operations are simple it. DNA permutation operation depends on the length of the string in DNA present. Also, DNA can storage more data in the string as each two bits presentation in one character. Encryption image of feistel network and DNA computing produce more complexity encryption. The secret key used to find many keys to encrypt blocks to increase quality encryption. The coding and decoding DNA consume more time. DNA permutation was used to make more difference in neighborhood pixel.

References

1.   Angelo A., Cancelli G. and Barni M. ,*" Watermark-Based Authentication"*, Springer-Verlag Berlin Heidelberg, Vol. 282, pp. 365 -402, 2010.

2.   Thien C. and Lin J., *"Secret Image Sharing"*, Elsevier, Computers and Graphics, Vol. 26, No. 5, pp. 765-770, 2002.

3.   Chong F. and Zhiliang Z., "A Chaotic Image Encryption Scheme Based on Circular Bit Shift Method", The 9th International Conference for Young Computer Scientists. (2008) 3057–306l.

4.   Weng-Long C., Shu-Chien H. and Weicheng L., "Fast parallel DNA-based algorithms for molecular computation: discrete logarithm", J Supercomputing 2011; 56:129–63.

5.   Lili Liu, Qiang Zhang , Xiaopeng Wei ," A RGB image encryption algorithm based on DNA encoding and chaos map", Computers and Electrical Engineering, elseveir,2012

6.   Chunyan Song and Yulong Qiao ," A Novel Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos", journal-entropy ISSN 1099-4300,2015

7. Y. Allen Daniel , Harish. J , Aswin.S , S. Sankar," Encryption then Compression Based on Image Fusion, Chaotic Map and DNA Subsequence Operation", International Journal of Emerging Technology and Advanced Engineering, Volume 5, Issue 3, March 2015.

8. Shihua Z., Qiang Z. and Xiaopeng W., "Image Encryption Algorithm Based on DNA Sequences for the Big Image" , 2010 International Conference on Multimedia Information Networking and Security.

9. Xiao G., Lu M., Qin L. and Lai X., "New Field of Cryptography: DNA Cryptography", Chinese Science Bulletin, vol. 51, pp.1413-1420, 2006.

10. Leier A., Richter C., Banzhaf W. and Rauhe H., "Cryptography with DNA Binary Strands", Bio Systems, vol. 57, pp.13-22, 2000.

11. Heider D. and Bamekow A., "DNA-based Watennarks Using the DNA-Crypt Algorithm", BMC Bioinfonnatics, vol. 8, pp.176-185, 2007.

12. Adleman L., "Molecular Computation of Solutions to Combinatorial problems", Science, vol. 226, pp. 1021-024, Nov. 1994.

13. Cui G. and Qin L., "Information Security Technology Based on DNA Computing", IEEE International, China, pp. 288 – 291, April 2007.

14. Hung K. , "A Study on Efficient Chaotic Image Encryption Schemes ", M.Sc. Thesis, Department of Electronic Engineering, City University of Hong Kong, September, 2007.

15. Maqableh M., " Analysis and Design Security Primitives Based on Chaotic Systems for eCommerce ", Ph.D Thesis, Durham University, School of Engineering and Computing Sciences, United Kingdom, 2012.

16. May R., "Simple mathematical models with very complicated dynamics", Nature Publishing Group, Vol. 261, pp. 459-67, 10 June 1976.

17. Tong X., Cui M., "Image encryption with compound chaotic sequence cipher shifting dynamically", Image Vision Computing, 6:843-50, 2008.