CityU Scholars

Research on Image Encryption Based on DNA Sequence and Chaos Theory

Zhang, Tian Tian; Yan, Shan Jun; Yan Gu, Cheng; Ren, Ran; Liao, Kai Xin

Published in:
Journal of Physics: Conference Series

Online published: 25/04/2018

Document Version:
Final Published version, also known as Publisher's PDF, Publisher's Final version or Version of Record

License:
CC BY

Publication record in CityU Scholars:
Go to record

Published version (DOI):
10.1088/1742-6596/1004/1/012023

Publication details:
Zhang, T. T., Yan, S. J., Yan Gu, C., Ren, R., & Liao, K. X. (2018). Research on Image Encryption Based on DNA Sequence and Chaos Theory. *Journal of Physics: Conference Series*, *1004*(1). https://doi.org/10.1088/1742-6596/1004/1/012023

Citing this paper
Please note that where the full-text provided on CityU Scholars is the Post-print version (also known as Accepted Author Manuscript, Peer-reviewed or Author Final version), it may differ from the Final Published version. When citing, ensure that you check and use the publisher's definitive version for pagination and other details.

General rights
Copyright for the publications made accessible via the CityU Scholars portal is retained by the author(s) and/or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights. Users may not further distribute the material or use it for any profit-making activity or commercial gain.

Publisher permission
Permission for previously published items are in accordance with publisher's copyright policies sourced from the SHERPA RoMEO database. Links to full text versions (either Published or Post-print) are only available if corresponding publishers allow open access.

Take down policy
Contact lbscholars@cityu.edu.hk if you believe that this document breaches copyright and provide us with details. We will remove access to the work immediately and investigate your claim.

Download date: 27/11/2021

Journal of Physics: Conference Series

PAPER • OPEN ACCESS

Research on Image Encryption Based on DNA Sequence and Chaos Theory

To cite this article: Tian Tian Zhang *et al* 2018 *J. Phys.: Conf. Ser.* **1004** 012023

View the article online for updates and enhancements.

Related content

- Advanced Secure Optical Image Processing for Communications: Compressive optical image security
  A Al Falou
- Implementation of digital image encryption algorithm using logistic function and DNA encoding
  MT Suryadi, Yudi Satria and Muhammad Fauzi
- Image encryption using the Gyrator transform and random phase masks generated by using chaos
  Juan M. Vilardy, Carlos J. Jimenez and Ronal Perez

IOP ebooks™

Bringing you innovative digital publishing with leading voices to create your essential collection of books in STEM research.

Start exploring the collection - download the first chapter of every title for free.

This content was downloaded from IP address 144.214.124.122 on 22/01/2019 at 06:32

Research on Image Encryption Based on DNA Sequence and Chaos Theory

Tian Tian Zhang[1,2,*], Shan Jun Yan[2,3], Cheng Yan Gu[1], Ran Ren[1]and Kai Xin Liao[4]

[1]City University of Hong Kong, Hong Kong, China
[2]School of Information and Electrical Engineering, Xuzhou University of Technology, Xuzhou Jiangsu, China
[3] China University of Mining and Technology, Xuzhou Jiangsu, China
[4] Nanjing Institute of Technology, Nanjing Jiangsu, China

*e-mail: ttzhang9-c@my.cityu.edu.hk

Abstract. Nowadays encryption is a common technique to protect image data from unauthorized access. In recent years, many scientists have proposed various encryption algorithms based on DNA sequence to provide a new idea for the design of image encryption algorithm. Therefore, a new method of image encryption based on DNA computing technology is proposed in this paper, whose original image is encrypted by DNA coding and 1-D logistic chaotic mapping. First, the algorithm uses two modules as the encryption key. The first module uses the real DNA sequence, and the second module is made by one-dimensional logistic chaos mapping. Secondly, the algorithm uses DNA complementary rules to encode original image, and uses the key and DNA computing technology to compute each pixel value of the original image, so as to realize the encryption of the whole image. Simulation results show that the algorithm has good encryption effect and security.

1. Introduction

In recent years, contributed by the rapid development of information technology and data processing, the problem concerning image secrecy has become more and more important. Encryption is an efficient way to keep image data free from attackers. In these encryption techniques, the chaotic image encryption method is more and more concerned because of the unpredictability of chaotic signals, the sensitivity to control parameters, the presence of the initial value, etc[1]. Many scholars are engaged in the research on the application of the combination of chaos theory and cryptography in encrypting image and improving the encryption level of cipher. Chaos theory has been widely applied to many subjects and become an important frontier science. However, the security of some existed algorithms has to be improved. At present, many proposed encryption methods simply utilize chaotic encryption, which have some drawbacks[2]-[6].

Today, researchers have proposed a number of encryption schemes based on DNA. DNA encryption is a combination of DNA technology and cryptography, thereby generating a new cryptographic technology and providing secure and efficient encryption service. The interesting feature lies in DNA structure is the complementary rules proposed by Watson and Crick. This principle has been widely used in different domains[7]-[9].

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd

2. The basic concept and the results of the study

2.1. Chaos theory

Chaotic system is a kind of peculiar motion form, which has a very good randomness. We often use this property to generate random sequences, thus disrupting the original image and getting satisfactory results. In this paper, we will choose one-dimensional logistic mapping as the chaotic system.
One-dimensional logistic mapping is a typical chaotic mapping, which is demonstrated below:

$$x_{n+1} = \mu x_n (1 - x_n), \mu \in [0,4], x_n \in (0,1), n = 0,1,2\cdots. \quad (1)$$

The results of study show that the system reaches chaos under the following criteria:

$$3.569945 < \mu \le 4 . \quad (2)$$

2.2. DNA

DNA is like the human body's password, its code word is A, T, C, G appearing with pairs. In image encryption, we can apply this rule to the encoding. Figure 1 shows the coding depending on DNA. Figure 2,3 propose DNA addition and subtraction rules.

0	1	2	3	4	5	6	7
A−00	A−00	C−00	C−00	G−00	G−00	T−00	T−00
C−01	G−01	A−01	T−01	A−01	T−01	C−01	G−01
G−10	C−10	T−10	A−10	T−10	A−10	G−10	C−10
T−11	T−11	G−11	G−11	C−11	C−11	A−11	A−11

Figure 1. Eight encoding rules for DNA sequences

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

Figure 2. DNA addition rule

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

Figure 3. DNA subtraction rule

3. The proposed algorithm program

3.1. Flow chart

This flow chart of this algorithm is shown as figure 4, which uses DNA encoding and DNA sequence:

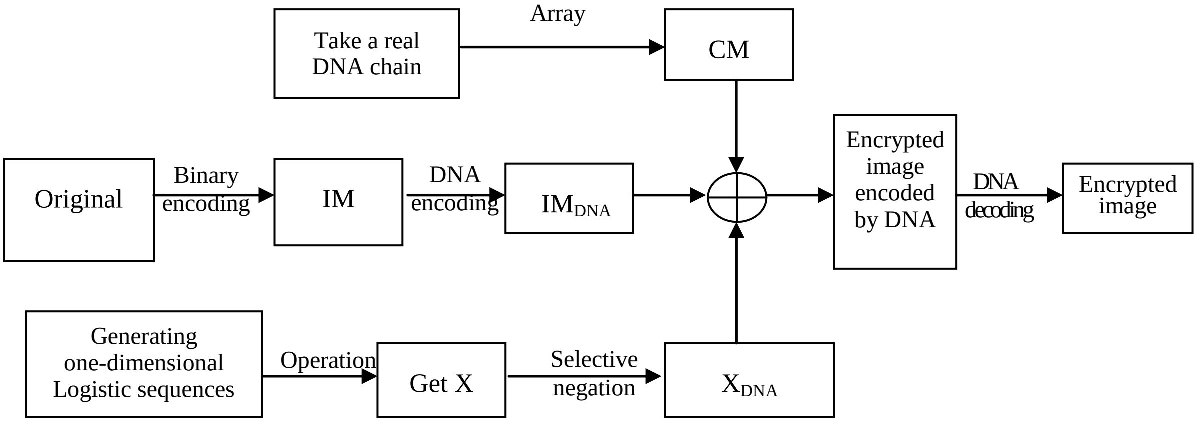


Figure 4. Flow chart of algorithm

3.2. Key generation

Input: Original image, DNA, value of Logistic mapping
Output: Encrypted image

3.2.1. Pretreatment

Step1： Choose a real DNA sequence.

Step2： Arrange the sequence into a matrix(512*4*512), which is named CM.

Step3： Using a programmer to produce a sequence of a one-dimensional logistic chaotic mapping, which is given initial value:

$$\mu = 4, X_0 = 0.53.$$

Step4： Choose the eighth bit of each number, named as X. If X is even, change the value into 0, or into 1.

Step5： Using the former DNA method to encode X, then we get X_{DNA}.

3.2.2. Encryption

Step6: Convert the image into a matrix, whose grey value is between 0-255, named as IM.(two-dimensional)

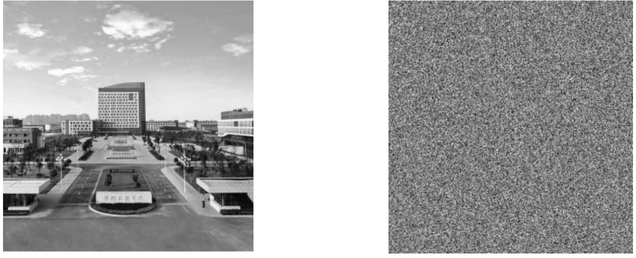
Step7: Using the DNA encoding method again to encode the matrix IM. The result is named as IM_{DNA}.

Step8: Adding the previous three matrices, which is from step2, step5 and step7, the result is called matrix P.

Step9: Applying the selective transformation into P. Define the formula of supplemental transformation: (it is the key step in the algorithm)

$$\text{Complement}_z\left(Y\right) = \begin{cases} Y, \text{if } X_i = 0, \\ \text{Complement}\left(Y\right), \text{if } X_i = 1, \end{cases} \tag{3}$$

End: Obtain the encrypted image, which is shown in figure 5.



(a) (b)

Figure 5. The result using the MATLAB software (a) original image (b) encrypted image

This algorithm can also reverse the above operations and obtain the original image.

4. Results analysis

We know that if the image encryption algorithm is security, it should be very exquisite and reasonable. In this part, the algorithm is allowed to face many attacks to test its security.

4.1. Resist brute force attack

If we want to resist brute force attacks, enlarging the key space should be an effective method. This requires designer to plan long key space or the keys will be destroyed for an exhaustive search within a limited time. In the encryption scheme, $\{x_0, \mu\}$ is the key, $\mu \in (3.56995, 4)$. 64-bit double precision 64 is 2^{64}, so the key space is about 2^{64}. In the DNA sequence portion, a 2559 DNA sequence was taken, the key space is 4^{2559}, The two key spaces added equal to the key space of this algorithm, much larger than the AES's practical symmetric encrypted maximum key space 2^{256}. After testing, it is big enough to stand up to brute force attacks.

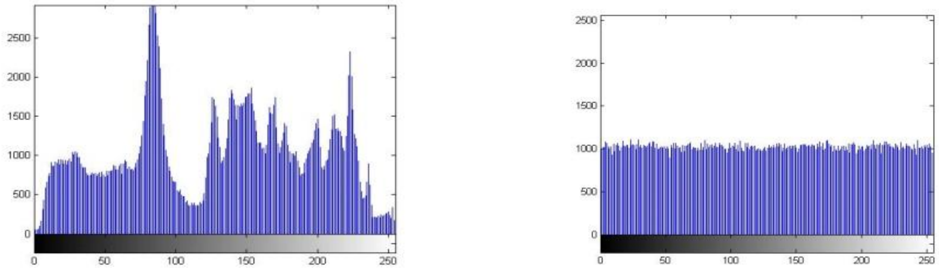
4.2. Anti-statistical attack

4.2.1. Information entropy. We often use information entropy to evaluating the gray pixel values distribution in the image. If the image is more chaotic, it's information entropy will be higher. Therefore, information entropy can be regarded as a measure of the ordering of the system. In image encryption, if the image encryption effect is very good, then the pixel is chaotic, it is equivalent to the system is disorder. Under ideal conditions, if the entropy of the image is 8, means that the encrypted image is chaotic. The information entropy of the encrypted image we calculate is H(M)= 7.9979.

$$H = \sum_{i \in \{A,T,G,C\}} P(i) \log_2 \frac{1}{p(i)}. \tag{4}$$

This result is very close to 8, so we can roughly think this algorithm can achieve the goal of encryption well.

4.2.2. Histogram analysis. In image encryption, the distribution of the gray pixel values is often displayed on histogram. The histogram of the encrypted image should change into a flat pattern. Figure 6 shows the histogram of two images. As they vividly show below, in the original image, the pixels concentrate in some values. In contrast, pattern of the encrypted image histogram is very flat, and almost every pixel is divided into each value. This way can resist statistical attack effectively.



(a) (b)

Figure 6. histogram (a) original image (b) encrypted image

4.2.3. Correlation analysis. Correlation analysis refers to the analysis of two or more variables, so as to measure the correlation degree of two variables. In the original image, the correlation between two adjacent pixels is very tight.

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, D(x) = \frac{1}{N\sum_{i=1}^{N}\left(x_i - E(x)\right)^2}, \tag{5}$$

$$\operatorname{cov}(x,y) = E\left(x - E(x)\right)E\left(y - E(y)\right), r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{6}$$

The encryption to do is to break or reduce the correlation, so that the attacker can't adopt the pixel analysis to restore the original picture, in order to achieve the effect of encryption. The smaller the correlation between two adjoining pixels, the more secure the cryptographic image. We randomly selected 1000 pairs of adjacent pixels from the original image comparing with encrypted images. The correlation through the MATLAB software to run the original two adjacent pixels is 0.8214, 0.0060 after encryption. We can see the correlation was significantly reduced.

4.3. Resist the chosen plaintext attacks

In the chosen plaintext attack, attacker can arbitrarily select a certain number of plaintext, let the algorithm to encrypt it, and get the corresponding ciphertext. In the worst case, the attacker can get the key for decryption directly. We analyse a chosen plaintext attack named differential attack.

The difference analysis involves the comparison of ciphertext pairs and plaintext with some characteristic. NPCR(Numbers of Pixel Change Rate), UACI(Unified Average Changing Intensity) are used to judge the effect of resisting differential attack.

$$\mathrm{NPCR} = \frac{\sum_{ij} D(i,j)}{m \times n} \times 100\%\,, \quad \mathrm{UACI} = \frac{1}{m \times n}\left[\sum_{ij} \frac{\left|C_1(i,j) - C_2(i,j)\right|}{255}\right] \times 100\%\,, \tag{7}$$

$C_1 \sim C_2$ represent the encrypted image after changing the gray value of a pixel respectively. m represents the size of the row, n represents the size of the column.

For the figure of 512*512, We select 5 representative points, which are located in the four corners and centres of the image, slightly change pixel values to test.

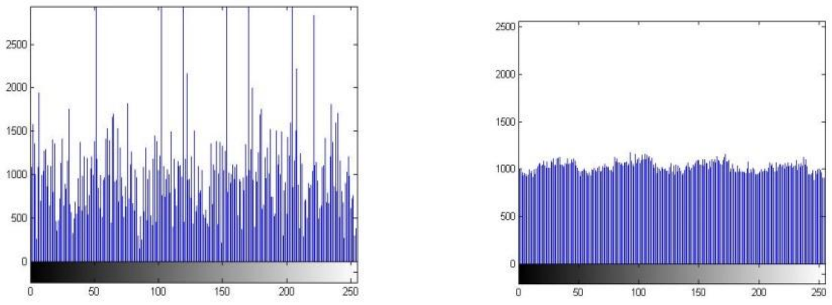
We can see the results in the table 1, the values of NPCR are all close to 100%, the values of UACI are about 33%.

Table 1. Encryption scheme anti-differential attack capability

Location	Primitive pixels	Changed pixels	NPCR	UACI
(1,1)	172	171	99.57%	33.41%
(1,512)	84	85	99.61%	33.44%
(256,256)	224	225	99.66%	33.35%
(512,1)	131	132	99.73%	33.47%
(512,512)	48	49	99.24%	33.46%

4.4. Comparison of algorithms

The algorithm compilation of references 8 and 9 are compiled in figure 7. The correlation of reference 8 and 9 is 0.0254 and -0.0106, while the correlation of this paper is 0.0060.



(a) (b)

Figure 7. Histogram of encrypted image from the reference (a) from reference 8(b) from reference 9

5. Conclusion

This paper proposed an algorithm combining DNA and Logistic chaotic mapping. The paper first shows that how to put the real DNA chain into the image and introduces logistic chaotic mapping, which is used for image encryption. Then a new algorithm is proposed which combines the logistic method and DNA sequence to encrypt the grayscale image. And a random matrix is generated on the basis of logistic chaotic mapping and DNA sequence, so that the addition and complement operations are performed on it. This algorithm successfully solves irreversible problems and expands the key space. It can resist attacks, such as the chosen plaintext attack, brute force attack and statistical attack.

References

[1] Peng J, Jin S J, Lei L and Han Q. Research on a Novel Image Encryption Algorithm Based on the Hybrid of Chaotic Maps and DNA Encoding 2013 *J. IEEE International Conference on Cognitive Informatics & Cognitive Computing*, p 403-8.

[2] Wang Q, Zhang Q and Zhou C J. A Multilevel Image Encryption Algorithm Based on Chaos and DNA Coding 2009 *J. International Conference on Bio-inspired Computing*, p 1-5.

[3] Liu H J, Wang X Y, Abdurahman K. Image Encryption Using DNA Complementary Rule and Chaotic Maps 2012 *J. Applied Soft Computing*, **12**(5) p 1457-66.

[4] Zhang Q, Xue X L, Wei X P. A Novel Image Encryption Algorithm Based on DNA Subsequence Operation 2012 *J. The Scientific World Journal*, **6736** p 286.

[5] Kar N, Majumder A, Saha A, Jamatia A, Chakma K and Pal M C. An Improved Data Security using DNA Sequencing 2013 *J. ACM Mobihoc Workshop on Pervasive Wireless Healthcare*, p13-8.

[6] Zhang Q, Guo L, Wei X P. Image Encryption Using DNA Addition Combining with Chaotic Maps 2010 *J. Mathematical and Computer Modeling*, **52**(11-12) p 2028-35.

[7] Hermassi H, Belazi A, Rhouma R, Wei X. Security Analysis of An Image Encryption Algorithm Based on A DNA Addition Combining with Chaotic Maps 2014 *J. Multimedia Tools Application*, **72**(3) p 2211 -24.

[8] Ritu G, Anchal J. A New Image Encryption Algorithm based on DNA Approach 2013 *J. International Journal of Computer Applications*(0975-8887), **85**(18) p 27-31.

[9] Jin X., Tian Y L, Song C G, Wei G Z, Li X D, Zhao G and Wang H C. An invertible and anti-chosen plaintext attack image encryption method based on DNA encoding and chaotic mapping 2016 *J. Chinese Automation Congress,* p 1159-64.