An improved DNA coding image encryption algorithm

Combining entropy and chaos

Yan Liu[1,2, a], Geng Zhao[2, b],Guangzhang Wei[1,2],Junlei Zhang[1]

[1]*Xidian University,Xi'an 710071,China*

[2]*Beijing Electronic Science and Technology Institute, Beijing 100070, China*

[a]*Luckyliuyan520@126.com*, [b]*zg@besti.edu.cn*

Abstract.

For the problem of lower safety performance in literature [1] , an improved chaotic map gray image encryption algorithm based on information entropy has been proposed.The algorithm includes three portions: first,chaotic mapping generates random matrices to diffuse plaintext image matrix ; Second, DNA encoding the addition and subtraction as well as complement arithmetic rule makes plain image matrix better confusion; Third, information entropy modulation parameters of chaotic systems to resist chosen plaintext attack. Based on [1], a combination of information entropy, while maintaining a good efficacy and safety, but also successfully solved the problem can resist the literature [2] attack methods.

Keywords: chaos map; DNA coding; image encryption; entropy; information security

Introduction

With the development of communication technology, digital image transmission network is becoming increasingly popular. However, this open digital images, poses a serious threat in the transmission process. Therefore, the design for the image encryption scheme is very necessary.

Because the pseudo-random chaotic map, the sensitivity of the initial value and unpredictability etc.other characteristics.Specific performance of chaos[3,4], such as sensitivity to initial conditions and system parameters, pseudo-randomness, ergodicity, etc., have been awarded chaotic dynamics as a promising alternative to traditional encryption algorithms.Entropy relates to the probability of information occurrence, it can represent the value of information, which information entropy can reflect how much information is contained in a picture. DNA (Deoxyribonucleic acid) encoding is a new area of computer science and molecular biology combining and development. [5,6,7] which use massively parallel DNA coding ability, successfully resolved, such as Hamilton

path, maximum Clique and other NP (Non-deterministic Polynomial) problems.

Related work

1.Information Entropy**.**From the perspective of information dissemination, the information entropy can represent the value of information. This way we have a measure of the level of the standard value of information can be made more inferences about knowledge circulation problems. The formula is

$$\mathrm{H} = \sum p(i) \log_2 \frac{1}{p(i)}, \quad i = i,2 \cdots n$$

2.Chaotic System.One-dimensional logistic mapping from mathematical point of view is a very simple form of chaotic map, the system is extremely complex dynamical behavior of the application in a very wide field of confidentiality. In this paper, we use of one-dimensional logistic chaotic map,defined as follows: F（x）：$x_{n+1} = ux_n(1-x_n)$,for $0 < u < 4, 0 < x_n < 1, n = 0,1,2,3\cdots$,The sequence generated by the chaotic system is the pseudo-random sequence.

2.DNA coding.A DNA sequence comprising a nucleic acid with four kinds (A: adenine, G: guanine, C:cytosine, T: thymine).In this paper C, A, T, G is represented 00,01,10,11 respectively. For each of the pixel values of an 8-bit gray image can be a DNA sequence of length 4 to represent. For example: If you get a gray image is 123 pixels, its binary representation for 01111011. After DNA encoding rules they are coded as AGTG.

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

Table 1.DNA addition operation

—	A	C	G	T
A	C	A	T	G
C	G	C	A	T
G	T	G	C	A
T	A	T	G	C

Table 2.DNA subtraction operation

Proposed image encryption scheme

In this paper, there are three parts of image encryption scheme ,first is DNA encoding,complement and decoding of plaintext image.Secondly,calculating the entropy of the image, and the third part, matrix Z is generated by chaotic Logistic mapping for DNA ciphertext state confused . Where Z is a two-dimensional matrix generated by chaotic Logistic map. For a given gray image P which size defined as $\mathrm{m} \times n$ .A detailed analysis of the encryption process of plaintext image P can be decomposed into the following steps:

1.The plaintext image is transformed into two-dimensional matrix for each pixel 0-255,denoted $\mathrm{P_b}$.Decimal tow-dimensional matrix $\mathrm{P_b}$ is transformed into Binary two-dimensional matrix $\mathrm{P'_b}$.And then using the given DNA encoding rules above,00,01,10,11 correspond respectively C, A, T, G DNA encoding the matrix $\mathrm{P'_b}$. Then the two-dimensional matrix encoded size is $\mathrm{m}\times 4n$. denoted the matrix DNA_{Pb}.

2.Image entropy calculation.Calculate the information entropy H of decimal two-dimensional matrix, by the following formula:

$$\mathrm{H}=\sum_{i\in\{0,1\cdots,255\}} p(i)\log_2\frac{1}{p(i)} \tag{1}$$

Where $p(i)$ is the probability of i appearing in $\mathrm{P_b}$, and then calculate:

$$x_0^H=\begin{cases} H-\lfloor H\rfloor, if & H-\lfloor H\rfloor\neq 0 \\ x_0, if & H-\lfloor H\rfloor=0 \end{cases} \tag{2}$$

x_0^H is the initial value of Logistic chaotic map, x_0^H will be converted into 64-bit long binary sequence H_{binary} as follow: $H_{binary}=\mathrm{D}ec2Bin(x_0^H,64)$.Conversely, the binary sequence H_{binary} into a decimal $H_{decimal}$ as follows: $H_{decimal}=Bin2Dec(H_{binary})$.Noted that the because of impact of computer's finite precision calculations, $H_{decimal}$ may not be equal to x_0^H.Image permutation, calculate $u=3.75+0.25H_{decimal}$. $H_{decimal}$ is considered ciphertext entropy.

3.For logistic chaotic map,given $x_0=0.62$ with the calculated u in previous step, obtained through research when selecting a precision of 16 of Logistic map, selecting the sequence of eighth will make randomness best.In this paper logistic chaotic map is selected eighth for each item,notes L. and given the judgment conditions:if $\mathrm{L}>5$,then let $\mathrm{L}=1$;if $\mathrm{L}<5$,then let L=0.And the value of L as an element of the matrix, until the size of the selected matrix Z is $m\times 8n$.From a given initial value, the series of number between (0,1) iterations out by mapping.

For instance,when $\mathrm{u}=3.9, x_0=0.62$ can obtain the corresponding sequence:

$x_i = (\cdots\cdots; 0.804374867512651; 0.613688166103959; 0.924592503462883;$
$0.271912703412174; 0.772107122027503; 0.686235085153447; \cdots\cdots)$

Then, the corresponding expressed as follows $L_i = (\cdots\cdots; 6; 6; 0; 0; 2; 8; \cdots\cdots)$.After a judge to draw the appropriate matrix Z, $Z_i = (\cdots\cdots; 1; 1; 0; 0; 0; 1; \cdots\cdots)$.Then the matrix is encoded by given DNA encoding rules, denote the matrix as DNA_Z.

4.DNA addition.For matrices DNA_{Pb} and DNA_Z, add two matrices according to DNA encoding rules, and get matrix Q.Next, we just need decode the two-dimensional nuclear matrix Q and convert it to decimal matrix of each pixel within 0 to 255 to obtain a ciphertext image.

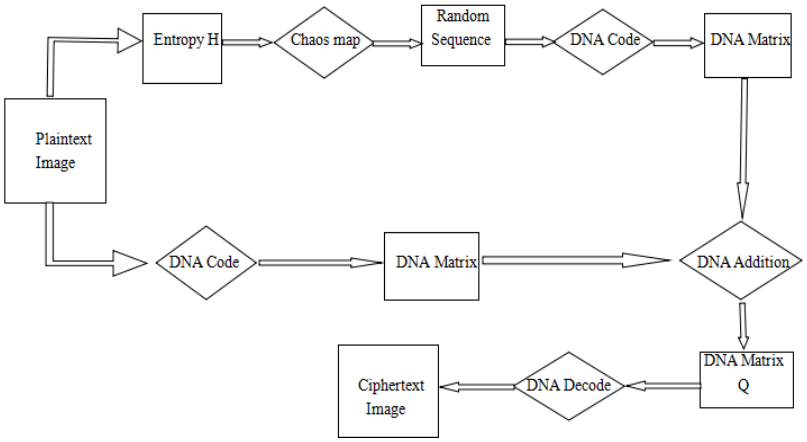


Fig. 1 flow chart of entire encryption

The image decryption algorithm

The article can be the inverse of the above operations, the original image is decrypted from the ciphertext state. Specific operations as follows:

1. Ciphertext image transform to a binary matrix, which will be coded according to the DNA coding rule to obtain a DNA matrix Q.

2 After entropy $H_{decimal}$ of ciphertext calculates Logistic chaotic system parameters,we encode the random sequence generated by Logistic chaotic map, in accordance with the corresponding DNA encoding rules ,and get nucleic matrix.

3. We make use of DNA subtraction operation to add DNA encoding matrix of random sequence which generated Logistic chaotic map and the matrix Q and obtain a new matrix P_b.

4 The result of decoding P_b is a binary matrix, then the matrix is converted to decimal matrix, so that is plaintext image.Figure 2 is a flowchart showing the entire decryption.

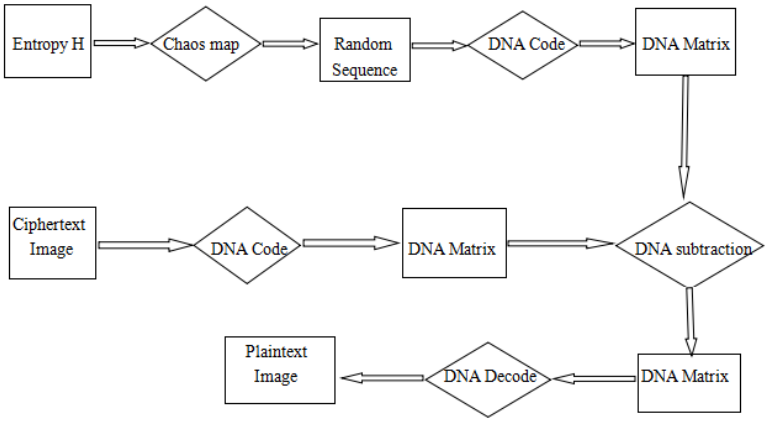
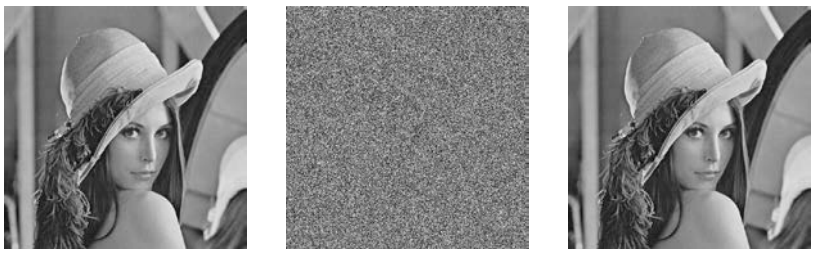


Fig. 2 flow chart of entire decryption

The experimental results

Analyzing performance of image encryption scheme, we implemented the algorithm in Matlab 7.0. Picture Lena and full black image as a plaintext being encrypted, the following figures are three pictures including plaintext image, ciphertext image and decrypted image,we can clearly see that the effect of encrypt and decrypt the image is quite satisfactory .The ciphertext can not be identified the original image information, and decrypted image can accurately restores the original image.



a. plaintext image b. ciphertext image c. decrypted image

Fig. 3 Lena

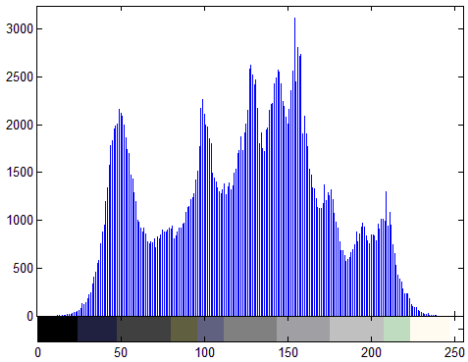
a. plaintext image b. ciphertext image c. decrypted image

Fig. 4 Black image

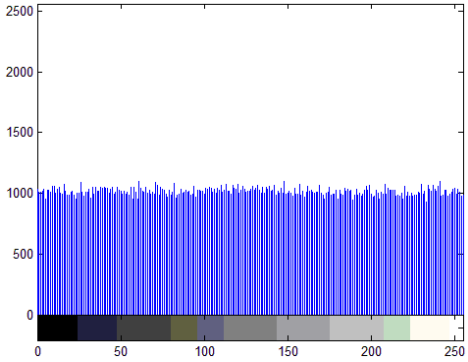
security and performance analysis

A good image encryption scheme should be designed for different types of attacks, such as violent attacks, differential attack,chosen-plaintext attack [8]. In this section, we will briefly analyze the security of the proposed encryption scheme.

1.histogram analysis.Histogram displays distribution of pixel values of gray images. Histogram of the encrypted image should be sufficiently smooth, otherwise the information may leak and result in statistical attack. This makes it possible to cause ciphertext-only attack by analyzing the statistical characteristics of the encrypted image . Figure 5, shows histograms of the gray image "Lena," and the corresponding encrypted image.Through comparing two histograms respectively we can see the pixel values of the original "Lena" image is centered on almost one value, also it's histogram of the encrypted image is very uniform, which makes statistical attacks impossible. It can be more intuitive to see the performance of the proposed algorithm.



a. Plaintext image histogram



b.Ciphertext image histogram

Fig. 5.Image "Lena" histogram

2. Resistance to chosen-plaintext attack.In the image encryption scheme, we use image information entropy to resist chosen plaintext attack referencing in[9].

Make DNA coding after calculating original image entropy and process by DNA addition. According to formula (1) and (2), entropy is determined by while the original image and a secret key. Information entropy is diffused through sensitivity of Logistic map and chaotic systems to affect the entire encrypted image.

Conclusions

In this paper, a improved and novel gray image encryption scheme is proposed, which takes the advantage of image information entropy,Logistic chaotic system and DNA encoding.Through the analysis of the algorithm feasibility and security ,we consider that the algorithm is brief,beautiful, good flexibility and application prospect.

Reference

[1] Guangzheng Wei.An improved image encryption method based on DNA coding and chaotic

map.Application Research of Computers[J]

[2] Houcemeddine Hermassi ,Akram Belazi ,Rhouma ,Safya Mdimegh Belghith. Security analysis

of an image encryption algorithm based on a DNA addition combining with chaotic maps[J].

Multimed Tools Appl. DOI 10.1007/s11042-013-1533-6(2013)SCI

[3] Lian S G, Sun J S and Wang Z Q 2005 Chaos Soliton. Fract. 26 117

[4] Huang C K and Nien H H 2009 Opt. Commun 282 2123

[5] Qiang Zhang,Ling Guo,Xiaopeng Wei. Image encryption using DNA addition combing with

chaotic maps. Mathematical and Computer Modelling[J]52(11-12) :2028-2035 SCI

[6] Xiaoling Huang , Guodong Ye. An image encryption algorithm based on hyper-chaosand DNA

sequence[J]. Multimed Tools Appl .DOI 10.1007/s11042-012-1331-6(2012) SCI

[7] YushuZhang,DiXiao,WenyingWen,MingLi. Cryptanalyzing a novel image cipher based on

mixed transformed logistic maps[J]. Multimed Tools Appl .DOI10.1007/s11042-013-1684

-5(2013) SCI

[8] Wang X Y and Bao X M 2013 Chin. Phys. B 22 050508

[9] Hermassi H, Belazi A, Rhouma R and Belghith S M 2013 Multimed. Tools Appl. 1