An Encryption and Decryption Algorithm for Image Based on DNA

Ranu Soni
Department of Computer Science & Engineering LNCT Indore, India
Indiaranusoni_8086@yahoo.co.in

Arun Johar
Department of Computer Science & Engineering LNCT Indore, India
arunjohar@gmail.com

Vishakha Soni
Department of Computer Science & Engineering PCST Indore, India
vishakhasoni@gmail.com

***Abstract*— A novel image encryption algorithm based on DNA sequence addition operation. This initiation and increasing escalation of Internet has caused the information to be paperless and the makeover into electronic compared to the conventional digital image distribution. In this paper we proposed and implement four phase. First phase, image is renovating into binary matrix. Afterward matrix is apportioning into equal blocks. Second phase, each block is then encoded into DNA sequences and DNA sequence addition operation used to add these blocks. For that result of added matrix is achieved by using two Logistic maps. At the time of decoding the DNA sequence matrix is complemented and we encrypt that result by using DES then we get encrypted image. Our paper includes a novel encryption technique for providing security to image. We have proposed an algorithm which is based on suitable encryption method.**

Keywords— DNA Computing ; DNA Sequence; Encryption ; Chaotic system ; DES .

I. INTRODUCTION

Since the computer networks have been extensively applied. The transmission for digital image over Internet has become explosive. However, due to the openness and sharing of networks, make the security of digital image has a serious threat in the process of communication. Image encryption is one of the most proficient methods for the protection of image information. Along with that the DNA image encryption method acting vital part in providing security to the image.

The chaotic system is a nonlinearity determinate system. It possesses of a variety of characteristics, such as high sensitivity to initial conditions, determinacy and so on. Chaotic sequences produced by chaotic maps and are pseudo-random sequences. Their structures are very complex and difficult to analysis and prediction. In other words, chaotic systems can develop the security of encryption systems.

Encryption algorithms are based on chaotic map. There is lot of research work publish by countless researchers, but most of them are overlaying a chaotic sequence and the pixel grey value from the image directly to implement encryption, which is easy to be attacked by the statistical attack or differential attack. And the resulted secret key space is limited.

With the rapid development of DNA computing, DNA cryptography has infiltrated into the field of cryptography. Catherine presented a method for hiding message in DNA microdots, for instance, letter "A" is expressed by DNA sequence "GGT", but the process must through complex biological experiments, it is not easy to implement. Recently, Kang Ning proposed a pseudo DNA cryptography method; it has better encryption result and not through real biological experiments.

II. BASIC THEORY OF THE PROPOSED ALGORITHM

A. Chaotic Map

In this paper, we used 2D Logistic map and one dimension Logistic map whose definition as follows. 2D Logistic map is described as (l) and (2):

$$X_{i+1} = x_i \mu_1 (1-x_i) + \gamma_1 y_{i2} ; \quad (1)$$

$$Y_{i+1} = y_i \mu_2 (1-y_i) + \gamma_2 (x_{i2} + x_i y_i); \quad (2)$$

When $2.75 < \mu_1 \leq 3.45$, $2.75 < \mu_2 \leq 3.45$, $0.15 < \gamma_1 \leq 0.21$, $0.13 < \gamma_2$ 12 ≤ 0.15 Where $\mu \in [0, 4]$, $x_n \in (0,1)$, n = 0, 1, 2,.. The research result shows that the system in chaotic state under the condition that $3.56994 < \mu \leq 4$.

B. DNA Sequence Encryption

1) *DNA Encoding and Decoding for Image:* A DNA sequence contains four nucleic acid bases A(Adenine), C(Cytosine), G(Guanine), T(Thymine), where A and T is complement, G and C is complement. In the binary, 0 and 1 is complement, so 00 and 11 is complement, 01 and 10 is also complement. In this paper, we use 00, 01, 10, 11 to denote C, A, T, G, respectively. For 8 bit grey images, each pixel can be expressed a DNA sequence whose length is 4.

   For example: If the first pixel value of the original image is 1 convert it into a binary steam is [10101101], by using DNA encoding rule to encode the steam, we can get a n sequence [TTGA]. Whereas use C, A, T, G to denote 00, 10, 11, respectively and to decode above DNA sequence, we can obtain a binary sequence as [10101101].

2) *Addition and Subtraction Algebraic Operation for DNA Sequences:* With the rapid developments of DNA computing some biological operations and algebraic operations presented by researchers based DNA sequence [7-8], such as addition operation. Addition and subtraction operations for DNA sequences are performed according to traditional addition and subtraction in the Z_2. For example, 11 + 10 = 01, 01-11 = 10. We use 00, 01, 10, 11 to denote C, A, T, G, respectively, the detail of addition and subtraction rules is shown in Table 1 and Table 2. From Table 1, we can see that any two rows are complementary, and Table 2 is in the same. In other words, the addition of algebraic operation table is a double helix structure which has satisfied by the Watson-Crick complement regulation. Subtraction is the inverse operation of addition, but whose structure is not double helix structure. However, we also find the complement of every base as shown in the Table 2. In this paper, we use this ideal addition rules to scramble the pixel value of the original image.

978-0-7695-4958-3/13 $26.00 © 2013 IEEE
DOI 10.1109/CSNT.2013.105

IEEE computer society

Authorized licensed use limited to: University of Petroleum & Energy Studies. Downloaded on February 17,2023 at 05:59:40 UTC from IEEE Xplore. Restrictions apply.

TABLE 1: ADITION RULE

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

TABLE 2: SUBSTRACTION RULE

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

III. ALGORITHM ILLUSTRATE

In this section, we perform detail study on the procedure of image encryption and which is based on DNA sequence addition operation. In First stage we produce secret keys. In Second stage we divide the original image into blocks and add these blocks by using DNA sequence addition operation. Finally we carry out DNA sequence complement operation for the result added matrix by using two Logistic maps. At the time of decode the result from the third part we get the encrypted image. The process of proposed image encryption algorithm is shown in Fig.1.

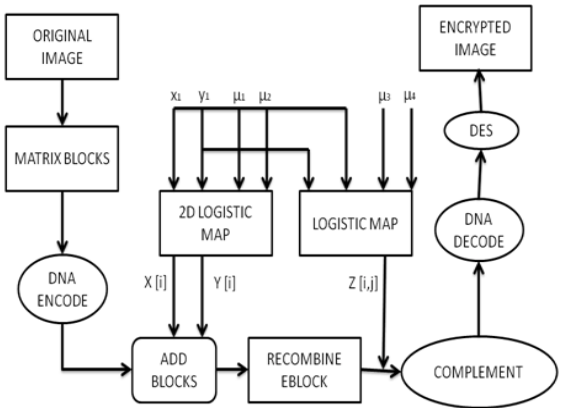

Figure 1: Block diagram for image encryption algorithm

A. Generation Of The Secret Key

We use the method to generate the secret key. Input a 8 bit grey image A as the original image, $A = A(a_{ij})$, $i = 1,2, \ldots, m$, $j = 1,2, \ldots, n$ .Here, a_{ij} is the pixel value of image, (i, j) is the position of image, and (m, n) is the size of image. We can use following equations to calculate K_1 and K_2.

$$K_1 = (1/256)\mathrm{mod}(\sum_{i=1}^{m/2} \sum_{j=1}^{n} a_{ij}, 256) \quad (3)$$

$$K_2 = (1/256)\mathrm{mod}(\sum_{i=m/2}^{m} \sum_{j=1}^{n} a_{ij}, 256) \quad (4)$$

Then choose two initial values x_1, y_2 and four system parameters μ_1, μ_2, μ_3, μ_4.

Image encryption algorithm based on DNA sequence addition

According to Fig. 1, the proposed encryption algorithm can be divided into the following steps in detail:

Step 1. Convert image into a binary matrix blocks , then carry out DNA encoding for the binary matrix blocks according to section II- B - 1, we will gain a coding matrix Ab, the size of Ab is $(m, n \times 4)$;

Step 2. Divide Ab into some equal blocks Ab{ i, j}, $i = 1,2, \ldots, m/4$, $j = 1,2, \ldots, n$, where the size of blocks is 4 x 4;

Step 3. Generate two chaotic sequences $X= \{x_1, x_2, x_3, x_4 \ldots\ldots\ldots x_{m/4}\}$, $Y= \{y_1, y_2, y_3, y_4, \ldots\ldots\ldots, Y_n\}$, through 2D Logistic map under the condition that initial values are x_0, y_0 and system parameters are μ_0, μ_2;

Step 4. To sort X, Y by ascending, we get two new sequences X', Y';

Step 5. Let the location value of sequences X', Y' as row coordinates and column coordinates of Ab{ i, j}, in other word, it can be expressed $Ab\{x_{p'}, y_{q'}\}$, where $\{x_{1'}, x_{2'}, \ldots, x_{p'}, \ldots, x')$ and $\{y_{1'}, y_{2'}, \ldots y_{n'}\}$ are the location values of sequences X', Y', respectively;

Step 6. Add Ab{i,j} and $Ab\{ x_{p'}, y_{p'}\}$ according to the section II -B-2, obtain the result of added blocks B{i,j}.

Step 7. Recombine these blocks B{i,j}, we will get a new sequence matrix C.

Step 8. Two chaotic sequences z_1 and z_2 are produced by two Logistic maps, whose lengths are m and n x 4. Reconstruct z_1 and z_2 to two matrices $z_{1(m,1)}$ and $z_{2(1,n \times 4)}$. Do multiply operation for $z_{1(m,\ 1)}$ and $z_{2(1,n \times 4),}$ we obtain the matrix Z whose size is m x n x 4. Map the value of Z into (0,1) by mod(Z, 1). Then using following threshold function f (x) to get a binary sequence matrix:

$$F(X) = \begin{cases} 0, & 0 < Z(I,J) \leqslant 0.5 \\ 1, & 0.5 < Z(i,j) \leqslant 1 \end{cases} \quad (5)$$

Step 9. If Z{i,j} = 1, C{i,j} is complemented, otherwise it is unchanged. After complementing operation, we get a new coding matrix C';

Step 10. Matrix C is encrypted by using DES (Data Encryption Standard). And we get encrypted image.

The process of decryption is an inverse process of encryption. Receivers obtain secret keys from sender. To decrypt the encrypted image according to contrary operation of above algorithm, where the addition operation is replaced subtraction operation in the step 6, other steps is unchanged.

Following figure 2 indicates the process of encryption of universal image i.e. Lena. Jpg. In this snap shot we browse for image and enter desired password for encryption of image. After that we clicked on encrypt button and in results our proposed method is applied over universal image.

Authorized licensed use limited to: University of Petroleum & Energy Studies. Downloaded on February 17,2023 at 05:59:40 UTC from IEEE Xplore. Restrictions apply.

Figure 2: Encryption process

Figure 3 shows the process of decryption of our encrypted image. In this process we browse our encrypted image and then we insert password for decryption of image. Once image is browse and password is inserted then click decrypt button. And this process in outcomes give two images as shown in figure 3 one is original image and another one is decrypted image. This figure also charted by output parameters. This output parameters are nothing but time taken by image for decryption process, memory used by the decryption process and last but least parameter is Matched it shows that the percentage of comparision between original or universal image and decrypted image.

Figure 3: Decryption Process.

Figure 4 shows the process of decryption using serial DNA method. In this process also we browse for encrypted file and then place password for decryption. Once this task is completed we process for decryption process. There is also output parameters as which shows results regarding time raken for decryption, memory used for decryption and matching percentage with original or universal image against decrypted image.

Figure 4: Serial DNA decryption process.

IV. Experimental Result

In this session we discussed about ressults obtained from our proposed method. Figure 5 shows the graph i.e. memory used in encryption which contains red line that indicates the memory required by the serial DNA encryption method. There is other blue color line that indicates the memory required by proposed method. Vertical values indicate the memory required by process in terms of MB. And horizontal values indicate number of execution required by encryption process.

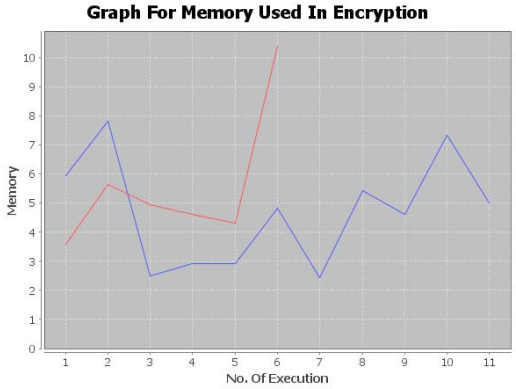

Figure 5: Memory used in Encryption.

Figure 6 shows graph for time taken in encryption by both methods.

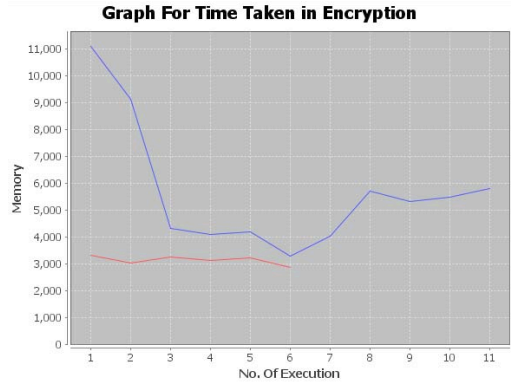

Figure 6: Time Taken in Encryption.

Following figure 7 shows graph of the parameter i.e. memory used during the decryption process for serial DNA decryption method and proposed decryption method.

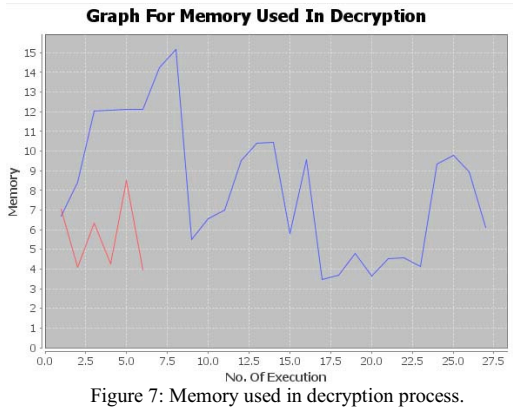

Figure 7: Memory used in decryption process.

Authorized licensed use limited to: University of Petroleum & Energy Studies. Downloaded on February 17,2023 at 05:59:40 UTC from IEEE Xplore. Restrictions apply.

Now one more parameter as similar to time taken by the process during encryption is shown in figure 8 i.e. time taken by decryption by both process.

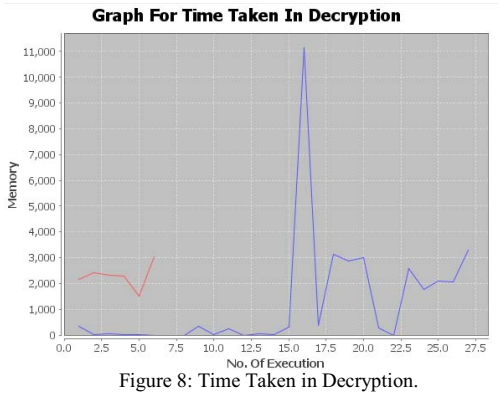

Figure 8: Time Taken in Decryption.

Now the following graph is also important as similar to above graph. This graphs shows the accuracy results.

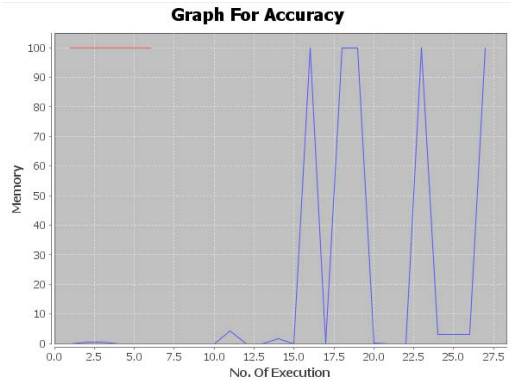

Figure 9: Accuracy by both process.

Now the following table contents methods and respective parameters values.

TABLE 3: PARAMETERS VALUES FOR RESPECTIVE METHODS

Parameters	Method	
	Serial DNA	Proposed Method
Encryption Time	3133.5 MS	5667.09 MS
Encryption Memory	5.58610026041 MB	4.70632102 MB
Decryption Time	2290.166666666 MS	1260.51851MS
Decryption Memory	5.68619791666 MB	8.17 MB
Accuracy	100%	100%

CONCLUSION

In this paper, we proposed a new image encryption algorithm based on DNA sequence addition. From above discussing, the pixel grey values of the original image are scrambled by DNA sequence addition operation and DNA complement operation completely. Through the experiment result we find that our algorithm has better encryption effect, larger secret key space and high sensitive to the secret key.

ACKNOWLEDGMENT

I, would like to acknowledge and extend sincere gratitude to acknowledge and extend my sincere gratitude to the principal of LNCT, Indore for his regular guidance and encouragement in all the aspects for successful completion of this work.

References

[1]. Chong Fu, Zhejiang Zhu, "A Chaotic Image Encryption Scheme Based on Circular Bit Shift Method", The 9th International Conference for Young Computer Scientists,2008,3057-306 l .

[2]. Yunpeng Zhang, Fei Zuo, Zhengjun Zhai, Cai Xiaobin, "A New Image Encryption Algorithm Based on Multiple Chaos System", International Symposium on Electronic Commerce and Security, 2008,347-350.

[3]. Liu Jin-mei, Qiu Shui-sheng, Xiang Fei, Xiao Hui-juan," A Cryptosystem Based on Multi-Chaotic Maps", International Symposiums on Information Processing, 2008, 740-743.

[4]. Catherine Taylor Clelland, Viviana Risca, Carter Bancroft. "Hiding Message in DNA Microdots Scientific Correspondence", Nature, 1999, 399.

[5]. Kang Ning," A Pseudo DNA Cryptography Method", arXiv: 0903.2693.

[6]. Hongjuan Liu, Zhiliang Zhu, Huiyan Jiang, Beilei Wang, "A Novel Image Encryption Algorithm Based on Improved 3D Chaotic Cat Map", The 9th International Conference for Young Computer Scientists, 2009,3016- 302l.

[7]. Allen P. Mills Jr., Bernard Yurke, Philip M. Platzman, "Article for analog vector algebra computation" , BioSystems 52, 1999,175-180.

[8]. Piotr Wasiewicz,lan J. Mulawka, Witold R. Rudnicki, Bogdan Lesyng, "Adding Numbers with DNA", International Conference on Systems",Man and Cybernetics,2000,265-270.

[9]. Dong enzeng, Chen zengqiang, Yuan zhuzhi, Chen zaiping, "A Chaotic Image Encryption Algorithm with The Key Mixing Proportion Factor", 2008 International Conference on Information Management, Innovation Management and Industrial Engineering, 2008,169-174.

[10]. Ling Wang, Qun Ye, Yaoqiang Xiao et aI, "An Image Encryption Scheme Based on Cross Chaotic Map", 2008 Congress on Image and Signal Processing, 2008,22-26.

[11]. Jun Peng, Shangzhu Jin, Yongguo Liu etc., "A Novel Scheme for image Encryption Based on Piecewise Linear Chaotic Map", Cybernetics and Intelligent Systems,2008, 1012-1016.

[12]. M.Sabery.K, M.Yaghoobi, "A New Approach for Image Encryption using Chaotic Logistic Map", 2008 International Conference on Advanced Computer T heory and Engineering, 2008,585-590.

[13]. Xu Shu-Jiang, Wang Ying-Long, Wang Ji-Zhi and Tian Min, "A Novel mage Encryption Scheme Based on Chaotic Maps", 2008.ICSP.9th International Conference on Signal Processing,2008, 10 14-1018.

[14]. Shannon, "Communication Theory of Security Systems", The Bell Syst Tech J 1949; 28: 656715.

[15]. Leonard. Adleman, "Molecular computation of solutions to combinatorial Problems", Sience: 266 :1021-1024, 1994.

[16]. Ashish Gehani, Thomas H. LaBean, John H. Reif, "DNA based cryptography", 5th Annual DIMACS Meeting on DNA Based Computers (DNA 5), MIT, Cambridge, MA, June 1999.

[17]. Lu MingXin, Lai XueJia, Xiao GuoZhen & Qin Lei. "Symmetric Key Cryptosystem with DNA Technology Department of Information Management", Cancer Research Institute, Queen's University, Kingston, Ontario, K7L3N6,Canada 2001.

[18]. Ning Kang, "A pseudo DNA cryptography Method", DBLP:journals/corr/abs-0903-2693,2009 http://arxiv.org/abs/0903.2693

[19]. Sherif T. Amin, Magdy Saeb, Salah El-Gindi, "A DNA-based Implementation of YAEA Encryption Algorithm," IASTED International Conference on Computational Intelligence (CI 2006), San Francisco, Nov. 20, 2006.

Authorized licensed use limited to: University of Petroleum & Energy Studies. Downloaded on February 17,2023 at 05:59:40 UTC from IEEE Xplore. Restrictions apply.