DNA Cryptography with Chaotic Mapping on Images: A Comparative Study

Siyamol Chirakkarottu
Assistant Professor
FISAT

Anil Johny
Assistant Professor
FISAT

Sheena Mathew, Ph.D
Reader
Dept. of Computer Science
CUSAT

ABSTRACT
Information in the form of digital images circulated over the networks is gaining popularity and great concern due to its enormous applications and necessities. in many of the applications, the images contain confidential information. the best method to protect images from unauthorized access is image encryption. Recent researches of image encryption algorithms have been increasingly based on chaotic systems. With the research of DNA computing has began, DNA cryptography is born as a new cryptographic field, in which DNA is used as information carrier and the modern biological technology is used as an implementation tool. Dna cryptography can be applied along with chaotic encryption for better performance.

Keywords
Image encryption, DNA cryptography, chaotic mapping.

1. INTRODUCTION
Security issues in medical data transmission are growing rapidly because most of the data to be transmitted are confidential. Several security algorithms are existing in recent trends for safer transmission of data. Moreover, the information that has to be transmitted must be encrypted to reduce the size of the data and increase processing speed. Most of the traditional text based encryption algorithms such as AES and IDEA are not suitable for image encryption[1].
Chaotic method reduces the correlation factor of adjacent pixels to a low value. Chaotic sequences produced by chaotic maps are pseudo-random sequences; their structures are very complex and difficult to be analyzed and predicted[2]. Chaotic systems can improve the security of encryption systems. The chaotic based systems are highly sensitive to initial condition[1], i.e.: a small change in the initial condition can drastically change the long-term behavior of the system. This makes a person impossible to predict a data, if gets a partial information. a chaotic system can be regenerated only if the initial parameters and the system conditions are known. Hence chaotic encryption is well suited for digital images. Dna cryptography offers efficient and low-complexity encryption can provide security for information against intrusion and sophisticated threats that abound now[4]. in this paper some of the dna encryption methods which uses chaotic encryption are described and compared.

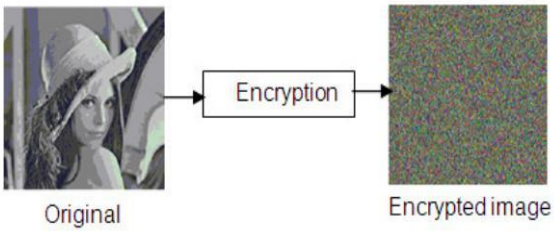

Fig 1. Image Encryption

2. LITERATURE REVIEW

2.1 Image Encryption Approach using an Index based Chaos and DNA Encoding
Here hybrid approach of chaos and DNA encoding is used for image encryption method has two phases: a permutation phase and diffusion phase. Using a 1D logistic map, the image is permuted. in the permutation phase, the pixel values are shuffled.
The 1D logistic map generates real numbers which are converted in to integer values. The chaotic sequence is represented as {a0,a1....an}. The indices of the values in this array are stored in an array b, in the ascending order. These index values are used in the phase of permutation. In the permutation phase the pixel values are rearranged based on the integer values in the array a[1]. The permuted image is converted in to DNA form by using DNA digital coding[1] method. Thus the image is now in DNA form. A secret key array is generated using the pixel values of the image. the key array also is converted in to DNA form. In the second phase of diffusion phase, the key array is added with image using DNA addition rule[1]. The obtained array should be converted in to binary and then reconstructed in to image, which is the encrypted image. the method is used for gray scale image. Key sensitivity , gray histogram and correlation coefficient analysis show that the method is efficient and less time consuming.

2.2 Image Encryption Algorithm Based on DNA Subsequence Operation
The paper suggests using the idea of DNA subsequence operations combining with the logistic chaotic map to scramble the location and the value of pixel points from the image[2]. A logistic map and 2D logistic map are used to improve the security. Using a dna encoding rule, the bases A, T, G, and C are encoded as 01, 10,00, and 11, respectively, satisfies the Watson-Crick complement rule.

Here five kinds of DNA subsequence operations are used. they are elongation, truncation, deletion, insertion and transformation. The inverse operation of elongation operation is truncation operation and the inverse operation of deletion operation is insertion operation. elongation, truncation,

deletion and transformation operations are used along with logistic mapping for encryption and insertion operation is for decryption. The method is implemented for gray image. Each pixel is converted in to 8 bit binary format. then each of the bit plane is extracted. The first and eight bit planes are composed to get a bit plane P1. Similarly, second and seventh are composed to get P2, third and sixth to get P3 and fourth and fifth to get P4. The obtained four bit planes are converted in to DNA sequence by applying DNA encoding rule. Then the dna sequence is divided in to dna subsequences of length 128,64,32 and 8.Then, to disturb the position and the value of pixel points from image by combining the logistic map, generate chaotic sequences and DNA subsequence operations (such as elongation operation, truncation operation, deletion operation and transformation. Finally the encrypted image is obtained by DNA decoding and recombining bit-planes. Image decryption is the reverse process of encryption.

2.3 Hybrid Method for Image Encryption using DNA Sequence and Chaotic Logistic Map

In this method, a chaotic logistic map is used to generate a secret key. the pixel levels of the gray image are altered by using dna sequences. the four bases of dna A, C, G and T can be encoded with binary codes to satisfy Watson and crick complementarity. Eight types of codes can be assigned to the bases which satisfies this rule. Each of the pixel value of the gray image is represented in binary and in dna form. Two chaotic sequences are generated using logistic mapping. The two chaotic sequences produced are multiplied to get a matrix k' which also should be represented in dna format. The obtained dna sequence is added with the original image, which is also in dna format. For addition, a dna addition rule is used.

The obtained dna sequence is converted in to binary and to decimal and represent it as image. The obtained one will be the encrypted image. The method based on chaotic shuffling and changing the gray value is resistive via different attacks like cryptanalytic, brute-force and statistical attacks.

2.4 Image Encryption using Chaotic Maps and DNA Addition Operation

The method is implemented for gray images. Here the image is encrypted using chaotic mapping. Four chaotic mappings- Cross chaotic map, Henon map, Ikeda map and logistic map are used for encryption and the performance are compared[5]. The image is converted to binary image and then to dna format. For this a digital coding technology is used. The bases are represented as A=00, T=11, G=10 and C=01.

Two chaotic squences are generated. One is represented as row matrix and the other in column matrix. Both are multiplied and represented in dna format, using the same coding rule. Both sequences are added using a dna addition rule[5]. The dna addition rule should satisfy the binary addition rules. Again a chaotic sequence is generated and the elements are compared with a threshold value. Based on this, the obtained sequence is complemented according to Watson and Crick complementarity. The complimented sequence is converted in to binary form and then represent as an image. The obtained image is the encrypted image. For decryption, the same steps are performed in the reverse order. the performance of various mapping are compared and cross chaotic mapping shows the best performance[5].

2.5 A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system

In this paper, a novel color image encryption algorithm based on DNA sequence operation and hyper- chaotic system is proposed. In this method, Chen's hyper-chaotic system is used to scramble the position of the pixels.

The color image is converted into three matrices for R, G and B which are further transformed nto binary matrices. Then these matrices are encoded according to DNA encoding rule[6]. The Chen's hyper-chaotic sequence is used to scramble the R ,G and B. the scrambled R,G and B are converted into blocks and then DNA addition operation is performed on the blocks. Now, the blocks are recombined and DNA decoding operation is performed to get the binary matrices. These binary matrices are further combined to get the encrypted image. The method improves the ability to resist differential attack by using hamming distance to generate the secrete keys. Furthermore, experimental results and security analysis shows that the algorithm has good encryption effect. Larger secret key space and high sensitive to the secrete key.

2.6 A new secure image encryption algorithm using chaotic maps, dna sequence and cellular automata

In this thesis, a novel confusion and diffusion method for image encryption using DNA sequences and cycling chaos and cellular automata is proposed[6]. Long secret key is used to obtain the initial value of cycling chaos and also to increase security of the proposed method. Cellular automata are used for changing key during the encryption process. Cycling chaos and DNA Sequences is used for scrambling image pixel's positions and then adjusting the pixels gray values by using a Mask DNA sequence matrix that it is generated using Cycling Chaos. The method is examined against cryptanalytic, exhaustive and statistical attacks. encrypted image's histograms are obtained and correlation coefficients are calculated. Experimental results show that this method has high security, and it is resistant to several different known attacks such as exhaustive attack, differential attack and statistical attack.

3. COMPARISONS

Various properties of different methods are studied and compared. Comparison of the existing methods is listed in Table 1.

The comparative study shows that chaotic mapping has advantageous properties over other methods for image encryption. The method can be used for both gray and color images.

Table 1 Comparison of Various Techniques

Methodology	Properties
Image Encryption Approach using an Index based Chaos and DNA Encoding	Satisfies key sensitivity, less time consuming and efficient

Image Encryption Algorithm Based on DNA Subsequence Operation	Applying the concepts of dna operations like insertion, deletion, elongation and truncation.Hence difficult for unauthorized access.
Hybrid Method for Image Encryption using DNA Sequence and Chaotic Logistic Map	Based on chaotic shuffling. Resistant to cryptanalytic, brute-force and statistical attacks.
Image Encryption using Chaotic Maps and DNA Addition Operation	Method compares the performance of more than chaotic mappings.
A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system	Larger key space and highly key sensitive
A new secure image encryption algorithm using chaotic maps, dna sequence and cellular automata	Resistant to exhaustive attack,differential attack and statistical attack.

4. CONCLUSION

DNA cryptography is an art of securing data using DNA sequences. Dna cryptography is combined with chaotic mapping for better performance[8]. Here the existing methods are studied and compared. Each technique is unique in its own way and this make it suitable for its many application. This survey provide a way to realize the different aspects that are used in chaotic mapping with dna cryptography. This survey shows that the method is well suited for image encryption

5. REFERENCES

[1] Aradhana Soni, Anuja Kumar Acharya,, "A Novel Image Encryption Approach using an Index based Chaos and DNA Encoding and its Performance Analysis," International Journal of Computer Applications (0975 – 8887)Volume 47– No.23, June 2012)

[2] Qiang Zhang, Xianglian Xue, and Xiaopeng Wei, " A Novel Image Encryption Algorithm Based on DNA Subsequence Operation*"* The Scientific World Journal Volume 2012, Article ID 286741, 10 pages doi:10.1100/2012/286741

[3] Morteza SaberiKamarposhti, Ibrahim AlBedawi, Dzulkifli Mohamad, "A New Hybrid Method for Image Encryption using DNA Sequence and Chaotic Logistic Map,"Australian Journal of Basic and Applied Sciences, 6(3): 371-380, 2012, ISSN 1991-8178

[4] M. I. Youssef, A. E. Emam, S. M. Saafan, M. Abd Elghany, "Secured Image Encryption Scheme Using both Residue Number System and DNA Sequence,"International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-12, October 2013

[5] Kuldeep Singh , Komalpreet Kaur, "'Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it," International Journal of Computer Applications (0975 – 8887) Volume 23– No.6, June 2011

[6] Morteza SaberiKamarposhti, Dr. Mohd Shafry bin Mohd Rahim, Prof. Dr. Dzulkifli B. Mohamad, "Developing a new secure image encryption algorithm using chaotic maps, dna sequences and cellular automata," Pattern Recognition, vol 40, issue 5, pp. 1621-1631, 2007. doi: 10.1016/j.patcog.2006.1 1.011

[7] Xiaopeng Wei, Ling Guo, QiangZhanga,Jianxin Zhang and ShiguoLian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system" journals of systems and software, volume 85, issue2,February 2012, Pages 290–299

[8] Prasenjit Kumar Das, Mr. Pradeep Kumar and Manubolu Sreenivasulu, "Image Cryptography: A Survey towards its Growth" ,Advance in Electronic and Electric Engineering, ISSN 2231-1297, Volume 4, Number 2 (2014), pp. 179-184