ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

Survey On Encryption Algorithm Based On Chaos Theory And DNA Cryptography

Jyoti Chauhan[1], Anchal Jain[2]

Department of CSE, Inderprastha Engineering College, Ghaziabad, UP, India[1]

Department of CSE, Inderprastha Engineering College, Ghaziabad, UP, India[2]

Abstract: DNA Cryptography is a new born cryptography that overcomes the difficulties of traditional cryptography due to its extraordinary information density inherent in DNA molecules, exceptional energy efficiency and vast parallelism. A lot of work have been done in this area based on different techniques like –DNA synthesis, PCR, Electrophoresis etc. In this paper various trends in DNA Cryptography are surveyed, highlighting the merits and demerits of each.

Keywords: DNA,CHAOS ,PWLCM,HYPER-CHAOS.

I.INTRODUCTION

Transmission of digital image over the internet has become more and more popular. However, the openness and sharing of networks exposes the security of digital image to serious threats in the process of transmission. Traditional encryption algorithms such as DES, IDEA, AES etc. are not suitable for image encryption due to the different storage format of an image. DNA Cryptography is proposed for secure communication due to the vast parallelism and extraordinary information density that are inherent in any DNA molecule. The main objective of this method is to encrypt the plaintext and hide it in the DNA digital form. DNA Cryptography enables the confidentiality of data with the use of one time pad (OTP) keys and its size.

(i) DNA: An Overview

DNA stands for Deoxyribonucleic acid which store genetic information and consist of long polymer of small units called nucleotides. These nucleotides consist of three components: Nitrogenous bases, five carbon sugar and Phosphate group. Nitrogen base consist of four bases: Adenenine, Thymine, Cytosine and Guanine (A, T, C and G), Adenine and Guanine are called purines whereas Thymine and Cytosine are called pyrimidines. DNA is a double helix structure discovered by Watson and Crick, also known as Watson-Crick complementary structure where A and T form hydrogen bond with one another. Both the strands are antiparallel to each other means if one strand start from 3’ to 5’ then another strand start from 5’ to 3’.

(ii) Biological Background

Hybridization: This is the formation of double stranded DNA molecules using single stranded DNA molecules. In this process Adenine always pair with Thymine while Guanine always pair with Cytosine.

Polymerase Chain Reaction (PCR): This is a scheme which amplifies single or multiple copies of a piece of DNA. Primer: It functions as a beginning point for DNA synthesis.

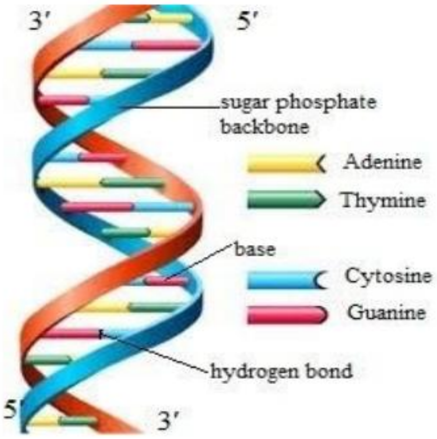

Figure 1. *Double helical structure of DNA*

Transcription and Splicing: In this process DNA segment that constitutes a gene is read from the beginning position of DNA segment. The non-coding areas are removed and coding areas are joined.

Translation: The mRNA sequence is translated into arrangement of amino acids.

II.HOTTEST ENCRYPTION METHODS

- DNA Cryptography Based Image Encryption
- Chaos Based Image Encryption

a)DNA Cryptography Based Image Encryption

In DNA Cryptography, DNA is used as information carrier and the modern biological technology is used as implementation tool, and the vast parallelism, exceptional energy efficiency and extraordinary information density inherent in DNA molecules are explored for cryptographic purpose. The main advantage of this scheme is that by using extended ASCII all kinds of digital data can be encrypted.

b)CHAOS Based Image Encryption

The chaotic image encryption can be developed by using deterministic properties of chaos including dynamics, unpredictable behavior and non-linear transform. Chaotic sequences produced by chaotic maps are pseudo random sequences, their structure are very complex and difficult to be analyzed and predicted.

III.LITERATURE SURVEY ON DNA TECHNIQUES

(i) Encryption using Chaotic Logistic Map

N.K. Pareek,Vinod Patidar,K.K. Sud [1], proposes a new scheme for image encryption that uses an external key of 80-bit and two chaotic logistic maps.The initial conditions of both logistic maps are derived by external key. Eight different types of operation are used to encrypt each pixel of an image and each operation for a particular pixel is decided by the outcome of second logistic map. To make the algorithm more robust and secure, after encrypting a block of sixteen pixel the secret key is modified.

Hongjun Liu, Xingyan Wang, Abdurrahman Kadir [2], permute the rows and columns of the image by the arrays generated by PWLCM. Algorithm makes an advantage of MD5 hash to generate initial values and parameters of chaotic map. By the DNA coding each pixel of a grayscale image is encoded into four nucleotides and then using complementary rule it is transformed into base pair for random times, generated by Chebyshev maps.

(ii) DNA Self-Assembly Technology

Shiua Zhou, Qiang Zhang, Xiaopeng advice the DNA Self-Assembly technology [3], to encrypt the image and enhance the security. DNA Self-Assembly technology is composed of the five groups of DNA tiles, namely DNA tiles of plaintext, DNA tiles of encryption, DNA tiles of ciphertext, DNA tiles of key and DNA tiles of decryption. Experimental result shows that algorithm is feasible to encrypt the image and can be implemented in DNA Computing in future.

(iii)DNA Biological Properties and Chaotic Systems

Qiang Wang, Qiang Zhang [4], proposes the algorithm that combines the biological properties of DNA and improved sequence of logistic map to scramble image pixel. Biological properties of DNA can better scramble image pixel and improved sequence of logistic map can better change pixel values. Experimental results show negative correlation of adjacent pixels.

(iv)DNA Sequences Based Algorithm

Shihua Zhou, Qiang Zhang and Xiaopeng [5], presented an image encryption algorithm based on DNA sequences to reduce big image encryption time. Proposed algorithm uses DNA sequence to generate scrambling sequences and another DNA sequence to generate DNA templates to accomplish pixel replacement. Experimental result demonstrates that algorithm is highly secured robust against all kinds of attacks.

In 2012, Qiang Zhang, Xianglian Xue [6], presented a novel image encryption algorithm based on DNA subsequence operations [6] combining with logistic chaotic map to scramble the location and value of pixel of an image. The experimental results and security analysis shows that proposed algorithm has larger key space, ability to resist statistic attack but can't resist differential attack.

In 2013, Nirmalya Kar, Atanu, Ashim Saha. [7], proposed encryption algorithm that uses the technology of DNA sequences and DNA Synthesis. Rather than sharing actual keys session keys are shared that bears the information about encryption keys. Extra padded bits presented in cipher make it more secure.

.

(v) DNA addition combining with Chaotic Maps.

Ling Guo, Xia OpengWei [8], presented a new image encryption scheme. The idea works in two steps 1) The original image is encoded to obtain DNA sequence matrix which is divided into equal blocks ,addition operation is used to add these blocks.2) By using Logistic map , DNA complement operation is performed to the added matrix. In the proposed algorithm pixel values are scrambled by DNA sequence addition operation and DNA complement operation.

In 2013, Houcemeddine Hermassi, Akram Belazi, Rhouma Safya [9], shows the cryptanalysis to the encryption scheme proposed in [8]. Authors demonstrate that algorithm proposed in [8] is non-invertible and attacker can determine the key only by temporary access to the encryption machinery. Moreover proposed algorithm is weak against chosen plaintext attack.

Wiang Hai-Chun , Wang Xiao-Xian [10], presented a new algorithm of " one –packet-one cipher " that takes advantages of both block cipher and one – time pad cipher in one encryption scheme. A new AES algorithm based on chaos map has created in which keys are generated from chaotic sequences that are used as sub-keys for AEs cipher. The proposed scheme has a good future on M-commerce security.

(vi) DNA Fractal Based

Qiang Zhang, Xianglian, Shihua Zhou [11], use DNA sequences as a secret keys. The permutation process is implemented by Halo's fractal sequence [11] and diffusion process is carried out to alter the gray values. Since DNA sequences are natural one time pad they are used as a main key which makes algorithm more secure and effectively resist exhaustive attacks.

(vii)Index Based Symmetric DNA

This scheme [12, 13, 17], are proposed where DNA gene bank is used for key which avoids sending the long keys over the channel. Author selects the special DNA sequences as encryption index and divides the plaintext into different groups. The key is created by chaos key generator based on logistic map that will take XOR operation with block plaintext.

(viii)Object identification

Mohammad Osiur, Hassaan Bari [14], tried to overcome the large computational time which is the major drawback of template matching by designing the object identification algorithm using DNA molecular operations. The paper also describes the application of DNA computing in recyable waste paper sorting.

(ix) Hyper Chaos Based Image Encryption

Hyper-chaos has more complex positive Lyapunov exponent and there are more complex dynamical characteristics than the chaos, therefore study of hyper-chaos based encryption algorithm may be more valuable.

Jun Peng, Shangzhu, Jin Hiang Lei and Qia Han [15], proposes an encryption algorithm with a 192-bit key by utilizing the hyper chaotic system and combination with DNA complementary rule. Author uses the Arnold cat map for obtaining the better confusion, and then it is encoded into DNA image. After that, each nucleotide of DNA image is transformed into its base pair by means of the complementary rule and XORED with a hyper-chaotic binary sequence.

Chen Zaipang, Li Haifen, Dong Enzeng, Du yang [16], uses Chen's hyper-chaotic system to shuffle the position of the image pixel and to confuse the relationship between the original image and cipher images. The encryption algorithm of image has the advantages of large key space and high security.

CONCLUSION

DNA encryption based on PCR amplification, one time pad, DNA synthesis, DNA hybridization makes it unique from traditional cryptographic techniques due to molecular properties inherent in it. Research of DNA cryptography lacks practical implementation but it is becoming a new and promising direction in the domain of cryptography research.

REFERENCES

[1] N.K.Pareek, Vinod Patidar, K.K.Sud," Image Encryption using Chaotic logistic Map",(0262-885) 2006, Image and Vision Computing.

[2] Hongjun Liu, Xingyacn Wang Abdurahman kadir,"Image Encryption using DNA complementary rule and chaotic maps", Applied soft Computing 12(2012) 1457-1466.

[3] Shiua Zhon, Qiang Zhang,Xia openg,"DNA Self-Assembly Technology", 978-1-4244-6585-9, 2010 IEEE.

[4] Qian Wang, Qiang Zhang, Xiaopeng Wei, "Image Encryption Algorithm based on DNA biological Properties and Chaotic Systems", 978-1-4244-6439-5, 2010 IEEE.

[5] Shihua Zhou, Qiang Zhang, Xiaopeng Wei, " Image Encryption Algorithm Based on DNA Sequences for the Big Image ," 978-0-7695-4, 2010 IEEE..

[6] Qiang Zhang, Xianglian Xue, Xiaopeng, Wei, " A Novel Image Encryption Algorithm Based on DNA Subsequence Operation ",The Scientific World Journal Volume 2012, Article ID 286741.

[7] Nirmalya Kar, Atanu Majumder, Ashim Saha , Anupam Jamalia, Kunnal Chakma, Dr.Mukul Chandra Pal," An Improved Data Security using DNA sequencing", 2013 ACM 978-1-4503-2207-2.

[8] Qiang Zhang, Ling Guo, Xiaopeng Wei, Image encryption using DNA addition combining with chaotic maps, Mathematical and computer Modelling 52(2010) 20282035.

[9] Houcemeddine Hermassi, Akram Belazi, Rhouma Rhouma,Safya Mdimegh Belghith ,"Security Analysis of An Image Encryption Algo Based on A DNA Addition Combining with Chaotic Maps", Multimedia Tools Application, june 2013 Springer Science.

[10] Wang Hai-Chun,Wang Xiao-Xian,"Research On Applications of Chaos Cryptography to M-Commerce Security", IEEE

[11] Qiang Zhang, Shihua Zhou and Xiaopeng Wei," An Efficient Approach for Dna Fractal Based Image Encryption",Applied Mathematics & Information Sciences 5(3) (2011), 445-459-An International Journal.

[12] Zhang Yunpeng, Zhu Yu, Wang Zhong, Richard o. Sinnott," Index-Based Symmetric DNA encryption Algo", 2011 4th International Congress on Image and Signal Processing , IEEE.

[13] Ritu Gupta, Anchal Jain" A New Image Encryption Algorithm baesd on DNA Approach", International Journal of Computer Applications(0975-8887) Volume 85-No 18, International Journal of Computer Applications (0975-8887), Volume 47- No.23, June 2012.

[14] Mohammad Osiur Rahman, Aini Hussain, Edgar Scavino, M A Hannan Basri,"Object Identification Using DNA Computing Algorithm",2012 IEEE.

[15] Jun Peng,Shangzhu Jin, Liang Lei and Qi Han,"Research a Novel Image Encryption Algorithm Based on the Hybrid of Chaotic maps and DNA Encoding",2013 IEEE.

[16] Chen Zaiping, Li Haifen, Dong Enzeng, Du Yang,"A Hyper Chaos Based Image Encryption Algorithm",978-0-7695-4151, 2010 IEEE.

[17] Guangzhao Cui, Limin Qin, Yanfeng Wang, Xuncai Zhang, "An Image Encryption scheme using DNA Technology". 2008 IEEE.

[18] Qian Wang, Qiang Zhang, Xiaopeng Wei, "Image Encryption Algorithm based on DNA biological Properties and Chaotic Systems", 978-1-4244-6439-5, 2010 IEEE.

[19] Shihua Zhou, Qiang Zhang, Xiaopeng Wei, " Image Encryption Algorithm Based on DNA Sequences for the Big Image ," 978-0-7695-4, 2010 IEEE..

[20] Qiang Zhang, Xianglian Xue, Xiaopeng, Wei, " A Novel Image Encryption Algorithm Based on DNA Subsequence Operation ",The Scientific World Journal Volume 2012, Article ID 286741.

[21] Nirmalya Kar, Atanu Majumder, Ashim Saha , Anupam Jamalia, Kunnal Chakma, Dr.Mukul Chandra Pal," An Improved Data Security using DNA sequencing", 2013 ACM 978-1-4503-2207-2.

[22] Qiang Zhang, Ling Guo, Xiaopeng Wei, Image encryption using DNA addition combining with chaotic maps, Mathematical and computer Modelling 52(2010) 20282035.

[23] Houcemeddine Hermassi, Akram Belazi, Rhouma Rhouma,Safya Mdimegh Belghith ,"Security Analysis of An Image Encryption Algo Based on A DNA Addition Combining with Chaotic Maps", Multimedia Tools Application, june 2013 Springer Science.

[24] Wang Hai-Chun,Wang Xiao-Xian,"Research On Applications of Chaos Cryptography to M-Commerce Security", IEEE

[25] Qiang Zhang, Shihua Zhou and Xiaopeng Wei," An Efficient Approach for Dna Fractal Based Image Encryption",Applied Mathematics & Information Sciences 5(3) (2011), 445-459-An International Journal.

[26] Zhang Yunpeng, Zhu Yu, Wang Zhong, Richard o. Sinnott," Index-Based Symmetric DNA encryption Algo", 2011 4th International Congress on Image and Signal Processing , IEEE.

[27] Ritu Gupta, Anchal Jain" A New Image Encryption Algorithm baesd on DNA Approach", International Journal of Computer Applications(0975-8887) Volume 85-No 18, International Journal of Computer Applications (0975-8887), Volume 47- No.23, June 2012.

[28] Mohammad Osiur Rahman, Aini Hussain, Edgar Scavino, M A Hannan Basri,"Object Identification Using DNA Computing Algorithm",2012 IEEE.

[29] Jun Peng,Shangzhu Jin, Liang Lei and Qi Han,"Research a Novel Image Encryption Algorithm Based on the Hybrid of Chaotic maps and DNA Encoding",2013 IEEE.

[30] Chen Zaiping, Li Haifen, Dong Enzeng, Du Yang,"A Hyper Chaos Based Image Encryption Algorithm",978-0-7695-4151, 2010 IEEE.

[31] Guangzhao Cui, Limin Qin, Yanfeng Wang, Xuncai Zhang, "An Image Encryption scheme using DNA Technology". 2008 IEEE.