ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 10, October 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Image Encryption using DNA Encoding Techniques : a brief overview

Dr. Asoke Nath[1]
Department of Computer Science
St. Xavier's College(Autonomous)
Kolkata, West Bengal – India

Deborupa Roy[2]
Department of Computer Science
St. Xavier's College(Autonomous)
Kolkata, West Bengal – India

Rishov Nag[3]
Department of Computer Science
St. Xavier's College(Autonomous)
Kolkata, West Bengal – India

Abstract: ***The field of digital communication and information exchange technology are experiencing a rapid growth and hence data security is becoming a major field of concern. Images being the most basic elements that are shared on various networks - safe and unsafe, thus play a vital role in information hiding to protect confidential information from illicit access. Various encryption methods are used for image encryption. Now with the advancement in the field of DNA computation and information storage, DNA sequences along with other methods are being used for image encryption with much higher image security. In the given paper, we survey on already existing image encryption technique using DNA encryption and draw a comparison between two papers previously published in this field.***

Keywords: DNA sequence ; DNA computation; DNA encoding; DNA complementary rule; Chaotic system.

I. INTRODUCTION

With the increase in digitalization, large chunk of data is being exchanged on the internet and hence data security plays a significant role. In cryptography, only an authorized party can access a message or information which is encrypted. An unauthorized party can intercept the message or information but cannot access the content. The plaintext is the original message or information that is encrypted using various encryption schemes generating a cipher text which has to be decrypted in order to retrieve the contents. Usually, pseudorandom encryption keys generated from algorithms are used for this purpose.

In this paper, the authors have divided the contents into four sections. 'Section II' which deals with the general guidelines regarding DNA computation and DNA complementary rule. 'Section III' gives a detailed study of the various works done in the field of image encryption using DNA encoding. 'Section IV' contains a detailed study of two previously published and well accepted DNA encryption schemes. In 'Section V' contains conclusions and future scope of development in this field.

II. DNA COMPUTATION AND DNA COMPLEMENTARY RULES

A DNA is a long polymer chain comprising of repeating units called nucleotides which are made up of a nitrogenous base, a five-carbon sugar, and one or more phosphate group. The nitrogenous bases can be grouped as purines comprising of Guanine (G) and Adenine (A), and pyrimidine which comprises of Cytosine (C) and Thymine(T). While Adenine and Thymine form one complementary pair, Guanine and Cytosine forms the other.

DNA computing involves computations using biological molecules, instead of using silicon chips. American physicist Richard Feynman in 1959 first proposed the idea of using individual molecules for the process of computation. However, it was physically achieved in 1994 by American computer scientist Leonard Adleman who showed molecules can be used to solve a computational problem.

DNA computing uses the four-character genetic alphabet - A, G, C and T for representing information instead of using the 1's and 0's. This is feasible because short DNA molecules of any desired sequence may be synthesized. Thus an algorithm takes as input DNA molecules with specific sequences, and various laboratory operations are carried out on the molecules, such as sorting them according to length or chopping strands containing a certain subsequence etc.

The procedure of DNA computation can be partitioned into three stages:

1. Encoding information in the DNA sequence
2. Computation (molecular operation)
3. Extraction of solution

For a general 8 bit grey image we allocate 2 bits for each of the nucleotides. We assume, C represents 00, which implies G will be 11. A represents 01 and hence T will represent 10. It can be clearly seen that these nucleotides represent the numbers 0, 1, 2 and 3 in the decimal system. Using this transformation, the pixels of any 8-bit grey image will correspond to a nucleotide string of length four.

TABLE I

Binary Value	DNA Nucleotide Base
00	C
01	T
10	A
11	G

In the above system, there are 4! =24 number of ways in which we can encode the nucleotide string, but only 8 of them will follow the complementary rule.[6]

With rapid advancements in the DNA computing scheme, we try to apply algebraic operations on the DNA sequence. The addition and subtraction operation are the most common of the operations that can be applied to a DNA sequence.

The DNA addition operation is analogous to the binary addition operation since10+11=01 is same as A + G = T. Similarly, we can compute the subtraction operation. While the addition operation is used for the encoding purpose, the subtraction operation is used for decryption purpose mostly.

TABLE II ADDITION TABLE

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

TABLE III SUBTRATCTION TABLE

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

One of the most used concepts in image encryption using DNA encoding is the DNA complementary rule proposed by Watson and Crick. There exists a hydrogen bond between A and T, G and C. Complementarity is achieved by the distinct interaction between nucleobases. DNA cryptography is emerging as the new cryptographic field where DNA is used to store information. This is possible because of the exceptional energy efficiency, vast parallelism and extraordinary information density in DNA. Various algorithms have been developed for image encryption using DNA encoding for secure image encryption and have been discussed in the following section.

III. SURVEY OF LITERATURE

1. *"Image encryption using DNA addition combining with chaotic maps",2010:*

Qiang Zhang et al. [1] used DNA addition operations along with a chaotic map to encrypt image. Initially, a DNA sequence matrix is acquired by encoding the actual image, which is divided into some equal blocks and DNA sequence addition operation is used to add these blocks. DNA sequence complement operation using two Logistic maps is then applied on the resulting added block. Finally, the DNA sequence matrix is decoded while leads to the generation of the encrypted image. The simulation experimental results and the security analysis show that the scheme achieves a good encryption as well as can resist exhaustive, statistical and differential attack.

2. *"A novel image encryption scheme based on DNA coding and multi-chaotic maps",2010:*

Qiang Zhang et al. [2] proposed an original image encryption method using DNA coding and multi-chaotic maps. In the paper, it is shown that the security of the encryption algorithm is improved effectively, by combining bit shift, XOR, XNOR with certain biologic operations. The proposed paper makes use of two chaotic maps, one is to control the operations which should be operated, and the other is used in computing. Initially, the pixel values of the original image are converted into 8-bit binary numbers and are encoded by four alphabets biological coding as 'A T C G' and these codes are divided into multiple blocks. The same operation is also performed by the chaotic sequence. Then, various operation rules are defined which acts as an intermediary between explicit and chaotic sequences. The encryption algorithm can defend against the statistical and differential attacks effectively, has a large key space and it's effectiveness has been proved by numerical simulations.

3. *"A Novel Image Encryption Approach using an Index based Chaos and DNA Encoding and its Performance Analysis",2012:*

Aradhana Soni et al. [3] have put forth an image encryption algorithm that uses index based chaos for generating keys and permuation and DNA addition operation for substitution. This is a cross between DNA encoding procedures for image encryption and chaos. The chaos sequence is employed for the diffusion process. Index based chaotic sequence is generated using one dimensional logistic map for permutation and the DNA sequence matrix is obtained by encoding the permuted image and index based chaotic sequence using DNA encoding rule. The DNA matrix addition is done using the DNA addition operation and a new matrix is generated. We decode the generated matrix using DNA decoding rule and thus the encrypted image is produced. The proposed approach has two distinctive characteristics:

i. The method in which the integer sequence is generated from the real valued chaotic logistic sequence.

ii. The formation of encoded DNA key matrix

The simulation results show that the given algorithm is highly secure and is resilient to statistical attacks and has a large key space.

4. *"Image encryption using DNA complementary rule and chaotic maps",2012:*

Hongjun Liu et al. [4] used a DNA complementary rule for image encryption where piecewise linear chaotic map is used for permutation. Complementary rule is used for performing substitution. The four nucleotides of the DNA are used to encrypt each pixel of the original image. Complementary rule is used to transform nucleotides into its base pair for random times(s), the time being generated using Chebyshev's maps. Experiments show it's a good encryption method and has a large key space to resist against common attacks.

5. *"A new image encryption algorithm based on DNA approach",2014:*

An image encryption algorithm was put forward by Ritu Gupta et al. [5], which was based on the DNA computation technology. It encrypts the original image by means of DNA computation and complementary rule. Modular arithmetic operations are performed on a DNA sequence to generate the secret key. Each pixel value of the image is then considered for the encryption process. This process makes use of the secret key and the DNA computation method. The algorithm's validity has been proved by researchers through thorough simulation and theoretical analysis on the various parameters such as sensitivity, histogram analysis, correlation analysis which includes bio-security as well as math-security.

IV. DETAILED STUDY

The aim of this section, as we have mentioned before, is to study two previously published and well accepted DNA image encryption technique. We are referencing "*Image encryption using DNA addition combining with chaotic maps",2010* by Qiang Zhang et al. [1] and *"A new image encryption algorithm based on DNA approach",2014* by Ritu Gupta et al. [5]. The previous paper is one of the pioneer research paper in the field of image encryption using DNA encoding. We aim to study the progress that has been made in this field of image encryption over the time gap and with the development of newer technology.

Qiang Zhang et al. [1] in their paper "*Image encryption using DNA addition combining with chaotic maps"* have utilised the concept of 2D and 1D logistic maps.

A 2D logistic map can be described as:

$x_{i+1}=\mu_1 x_i(1-x_i) + \gamma_1 y_i^2$

$y_{i+1}=\mu_2 y_i(1-y_i) + \gamma_2(x_i^2 + x_i y_i)$

when ,

$2.75< \mu_1 \leq 3.4$ $2.75< \mu_2 \leq 3.45$

$0.15<\gamma_1<0.21$ $0.13<\gamma_2<0.15$

The system is said to be in a chaotic state and generates two chaotic sequences in the region (0,1]. This paper sets the value of the parameters of $\gamma_1=0.17$ and $\gamma_2=0.14$ and the rest of the parameters are included in the secret keys.

A 1D logistic map can be expressed as:

$X_{n+1} = \mu x_n(1-x_n)$

Where $\mu \epsilon [0,4]$, $x_n \epsilon (0,1)$, n=0,1,2….

Research results show that the system is in a chaotic state under the condition that $3.56994 < \mu \leq 4$.

The overall steps involved are:

i. Firstly, the secret key is generated.

ii. Secondly the original image is divided into blocks and are added using DNA addition operation.

iii. DNA sequence complement operation is carried out in the resulting added matrix using two logistic maps.

iv. Lastly decoding the result from the third stage we obtain the encrypted image.

The key generation is performed as follows:

A 8 bit grey image A is accepted such that a_{ij} if the value of the image pixel. The following formula is used to calculate k_1 and k_2.

$k_1= \frac{1}{256} mod(\sum_{i=1}^{m/2} \sum_{j=1}^{n} a_{ij}, 256)$

$k_2 = \frac{1}{256} mod(\sum_{i=m/2}^{m} \sum_{j=1}^{n} a_{ij}, 256)$

Two initial values x_1, y_2 and four system parameter $\mu_1, \mu_2, \mu_3, \mu_4$ are chosen.

$x_0 \longleftarrow x_1 + k_1$

if $x_0 > 1$ then

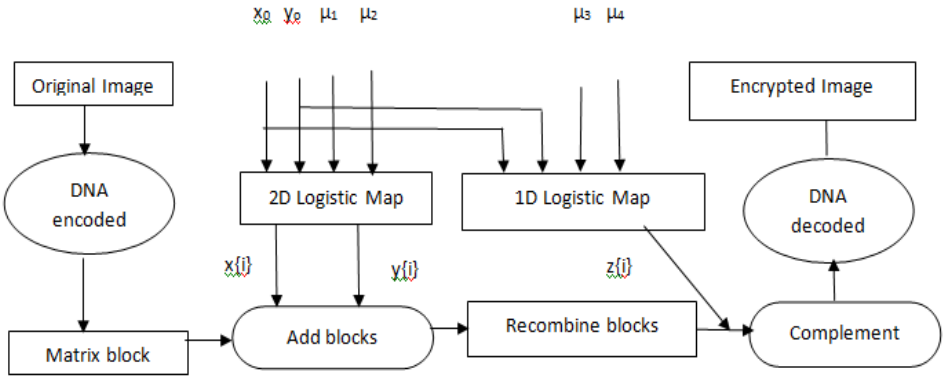
$x_0 \longleftarrow mod(x_0, 1)$

else

$x_0 \longleftarrow x_0$

end if

The above pseudo code is used to calculate x_0, y_0. x_0, y_0, μ_1, μ_2 are chosen as parameter for 2D logistic map and x_0, y_0, μ_3, μ_4 as the parameters of two 1D logistic maps. Thus these parameters can be seen as secret keys. The complete process can be represented by the diagram shown below:



The second paper being discussed here is presented by Ritu Gupta et al. [5] where the original image is encrypted using DNA computation and DNA complementary rule. The various steps involved are as follows:

The key for encryption is generated using the pseudo random sequence with certain modifications. According to the Wikipedia, a pseudorandom binary sequence (PRBS) is a binary sequence that, while generated with a deterministic algorithm, is difficult to predict and exhibits statistical behavior similar to a truly-random sequence.

Key Generation:-

A special gene sequence is taken of length 4n which is divided into substrings of length of 4, the starting and ending points being chosen at random. Each substring is converted into binary using DNA encoding. If we have n number of substrings, the binary numbers generated from the given DNA Sequence is denoted by N where $N=\{N_0, N_1, N_2, N_3, \ldots..N_{n-1}\}$. The key is generated using the formula $k=[((y_i \text{ XOR } N_i) \times A) + B] \bmod 2^8$, where $0 \leq i \leq n$. Where, y_0 is 8-bit seed value, $y_i = k_{i-1}$ for i = 1 to n- 1, A & B are two large prime numbers and $K = \{k_0, k_1, k_2, \ldots\ldots\ldots, k_{n-1}\}$ is the key sequence generated.

Key Expansion:-

The elements of the key sequence are encoded into the gene sequence using the DNA encoding method. The resulting DNA sequence is copied four times and then substring generation takes place. The first string is subdivided into strings of length 4 leaving the first character. Similarly, we generate the second string where the first character is left and the third string where the first two characters are left and so on. Then from all the strings only those substrings are taken into consideration as elements of the expanded key whose length is 4. Finally, all the substrings are converted back into its numerical form. Let the DNA code of the key sequence be "AGTCTACGACGTGACT". This DNA code is copied four times to generate the substring

- The first substring AGTC/TACG/ACGT/GACT. Here no character is discarded.
- The second substring A/GTCT/ACGA/CGTG/ACT. Here the first character is discarded.
- The third substring AG/TCTA/CGAC/GTGA/CT. Here the first two characters are discarded.
- The fourth substring AGT/CTAC/GACG/TGAC/T. Here the first three characters are discarded.

Pseudo Random sequence generation:-

- If the original grey scale image has MxN pixels in it, the pseudo random sequence will be of length MN.
- A state array S is declared of length 256 along with the key sequence K. The values of the array are filled from 0 to 255, i.e. s[0]=0, s[1]=1, s[2]=2,…….s[255]=255.
- Now a 256 byte temporary array T is created which stores all the values of K and the remaining positions of T are again filled with the values of K.
- Finally the pseudo random sequence Z of length MN is generated using the following logic: Initialize j=0;

```
For i= 1 To MN
    For j=0 To 255
        j=(j+s[i]+t[i]) mod 255;
        z[i]= j mod 8;
        s[i]=s[j];
```

Encryption:-

Here CBC mode of encryption is used. At first the original grey image is converted into a 2D matrix containing the pixel values. Then a 1D array is generated which is used for the encryption process. Before the encryption process begins a 8-bit number known as the Initialization Vector (IV) is randomly chosen and XOR-d with the first pixel value of the first block of the plain text. The purpose of the IV is to generate unique messages. The encryption algorithm takes the original grayscale image, the key sequence and the pseudo random sequence as input and generates the encrypted image. The Encryption Algorithm is as follows:

- After converting the original image into a matrix of pixel values, a 1D sequence P is generated.
- We then perform the following operation-

$C_0 = [(IV \text{ XOR } p_0)+k0] \bmod 8$

$C_i = [(C_{i-1} \text{ XOR } p_i)+(k_i \bmod n)] \bmod 2\text{^}8$ where $1 \le i < MN$

Where p_i subset of the plain text sequence $P = \{p_0, p_1, \ldots\ldots, p_{MN-1}\}$,

K_i subset of the key sequence $K=\{k_0,k_1,k_2,\ldots\ldots..,k_{n-1}\}$

$C=\{c_0, c_1,\ldots..,c_{MN}.1\}$ forms the intermediate cipher values

- Each value of the sequence C is encoded into the DNA code and the encrypted sequence $X=\{x_0,x_1,\ldots..,x_{MN}\}$ is generated using the following operation-

$x_1=\text{DnaAdd}(c1, \text{Comp}(\text{Rotate}(c_{MN})))$

$x_i=\text{DnaAdd}(c_i,\text{Comp}(\text{Rotate}(x_i\text{-}1)))$ where $2 \le i \le MN$

where DnaAdd is a function to do DNA addition using the addition table

Comp is used to generate the complementary code of a DNA code using Complementary rule

Rotate is a function to do bitwise left rotation of the DNA code, the number of bits rotated at the i^{th} iteration being same to the value of the pseudo random sequence

- Finally the sequence X is converted to a two dimensional matrix which is used to generate the decimal pixel values which forms the encrypted image.

V. Conclusion and Future Scope of dEvelopment

In the digital world nowadays data storage and information interchange plays an important role. Various forms of images are shared over the network. In most cases the images sent via communication networks are private to the sender and the recipient. Hence image encryptions play a very important role in securing images from intruders. In the given paper various existing image encryption techniques using DNA encryption techniques has been studied. The table below discusses the results of papers discussed above:

Name of the paper	Discussions
➢ Image encryption using DNA addition combination with chaotic maps[3]	▪ Has large secret key space to resist exhaustive attack. ▪ Encryption algorithm is sensitive to secret key value. ▪ All the different performance tests have been applied on the said algorithm and it has passed through all these tests with complete efficiency. The resistivity of the algorithms have been found to the various exhaustive, statistic and differential tests.
➢ A new image encryption algorithm based on DNA approach[11]	▪ Eliminate the requirements of sending the lengthy key sequence via a secure channel. ▪ Also a lot of combinations are possible making this algorithm all the more versatile. ▪ The algorithms produced a good avalanche effect thus proving to be secured from all kinds of external, brute forces. ▪ Histogram analysis shows resistance from statistical attack. ▪ Provides a large key space as they use DNA shotgun sequence which are generally large, thus providing protection from all kind of brute force attack.

Each technique is unique in its own way. Furthermore, we can see recent researches on image encryption algorithms have been increasingly based on chaotic systems[6][7][8][9] which lead to much secure image encryption because of its randomness and unpredictability. Other methods such as residue number systems[10] along with DNA sequence can also be used. Hence we conclude that all the techniques are useful for real time image encryption.

Acknowledgement

The authors would like to thank Prof. Shalabh Agarwal , Head of the Department of Computer Science and Dr. J. Felix Raj, Principal, St. Xavier's College(Autonomous), Kolkata for their support in helping the authors to do research in Network Security.

References

1. Qiang zhang, Ling Guo, Xiaopeng Wei, "Image encryption using DNA addition combining with chaotic maps", Mathematical And Computer Modelling 52 (2010) 20282035.
2. Qiang zhang, Qian Wang, Xiaopeng Wei, " A novel image encryption scheme based on DNA coding and multi chaotic maps", Journal Of Computational And Theoretical Nanoscience 3(4):447-451, December 2010.
3. 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.

4. Hongjun Liu, Xingyuan Wang, Abdurahman Kadir ,"Image encryption using DNA complementary rule and chaotic maps", Applied Soft Computing 12 (2012) 1457–1466.
5. Ritu Gupta, Anchal Jain – "A new image encryption algorithm based on dna approach" – International Journal Of Computer Application (0975-8887), Volume 85 – No 18, January 2014
6. 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
7. 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
8. Morteza SaberiKamarposhti, Mohd Shafry bin Mohd Rahim, 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
9. 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
10. 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

AUTHOR(S) PROFILE

Dr. Asoke Nath, is Associate Professor in the Department of Computer Science, St. Xavier's College(Autonomous), Kolkata, India. Apart from his teaching assignment he is actively envolved in doing research work in Computer Science and Engineering. His research areas include Data eccryption and Cryptography, Steganogarphy, DNA Cryptography, Big data analytics, Data science, Cognitive radio, Green computing, MOOCs, e-learning methodologies, Mathematical modelling of Social Networks, Li-Fi technology and so on. He has already published more than 201 research publications in Journals and Proceedings of International conferences.

Deborupa Roy, is a Final year student of B.Sc. Computer Science Honours, St. Xavier's College(Autonpomous<Kolkata, India. Apart from her normal graduation studies she is also engaged in doing research work in the field of DNA Cryptography and DNA Steganography. She is also interested to work in the field of VLSI and nanotechnology.

Rishov Nag, is a Final year student of B.Sc. Computer Science Honours, St. Xavier's College(Autonpomous< Kolkata, India. Apart from his normal graduation studies he is also engaged in doing research work in the field of DNA Cryptography and DNA Steganography.He is also interested to work in the field of Cloud Computing and Big Data Analysis.

