International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 11, November - 2013

Summarization on DNA cryptography

Siyamol Chirkkarottu
FISAT, Angamaly

Dr. Sheena Mathew
CUSAT

***Abstract*—Large storage capacity of DNA can be used for applications like cryptography, cryptanalysis and steganographic problems. Several DNA computing algorithms exist in the area and they are quite powerful. Both real DNA and principles of DNA can be used for encryption. The traditional encryption algorithms have shortcomings and they are not considered as ideal for image applications, because of their low level efficiency when dealing with large and redundant blocks of image data. DNA encryption makes a bridge between existing and new technology. The power of DNA computing will strengthen the existing security system by opening up a new possibility of hybrid cryptosytstem. The method can be extended to video applications also.**

Index Terms*—DNA cryptography, image encryption,,DNA computing.*

I. Introduction

Encryption is a common technique to uphold security of both text and image data. However there are many classical encryption technologies like DES and RSA, they can be broken by some attack problems. This information states that the modern cryptography encryption methods, which are solely based on mathematical computations are not so reliable as before. To achieve the above purpose researchers look for more secure cryptography incessantly. Independently of the future technological success of DNA computing[1], this area has led already to interesting new computing paradigms which certainly enriched our understanding of the nature of computation. The Hamiltonian path problem[9] is already solved by applying DNA computing. The conventional algorithms for encryption, including DES, IDEA and one time pad are already shown improved performance by applying DNA cryptography. The vast storage capability of DNA can be used to store both text and image data. Using one gram of DNA about 108 terrabytes of data can be stored[13].

The rest of the paper is organized as follows. Section II describes the structure and functions of DNA which can be applied for computational analysis. Section III and section IV describe the different DNA cryptography technologies in both text and image data respectively. Section V states the analysis of DNA cryptography methods. Finally the conclusion is drawn in section VI.

II. Biological Study

DNA[1] molecules are polymers constructed from monomers called nucleotides, made up of three components: sugar, phosphate and base. There are four distinct bases: adenine, guanine, cytosine and thymine, abbreviated A; G; C and T , respectively. Single-stranded DNA molecules are simply chains of nucleotides where two consecutive nucleotides are bound together by a strong covalent bond along a sugar-phosphate backbone. Each single strand has, according to chemical convention, a 5 and a 3 end, thus any single strand has a natural orientation. DNA has a double helical structure with two anti parallel strands as shown in figure 1.

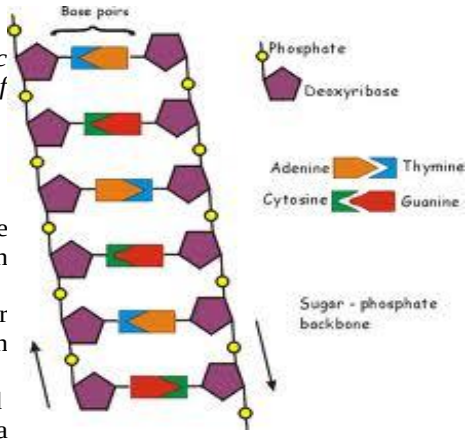

Fig. 1. *structure of DNA*

DNA can be used as an information carrier and it can be considered as a measure in the conversion of plain text to cipher text. Both the storage capacity and biological functions of DNA can be used for cryptography technologies. DNA chip technology [9], DNA fragment assembly and PCR technology are some of the methods which can be applied in cryptography.

III. Encryption of Text Data

DNA cryptography can be applied along with both symmetric and asymmetric encryption, in the case of text data. In symmetric encryption[2], both the sender and receiver use the same key for encryption and decryption. Asymmetric cryptography uses public key for encryption and receivers private key for decryption. The section follows describes the

various methods which use DNA cryptography for text encryption.

A. Pseudo DNA cryptography

The principles of biological operations transcription and translation are applied in the method[9]. Information is stored in binary form and can be transformed in to DNA form, by mapping the binary numbers to the bases A,C,G and T. Analogous to RNA splicing, the fragments of sentences, which are identified by predetermined starting codes and patterns, are removed. Using the concept of translation, the plain text is converted in to protein form.

The starting and pattern codes, removed introns and the gene mapping table together should be send along a secure path as the key. The advantage of the method is, only a little information need to be send securely. It is easy for the sender to encrypt the message. The size of the key is small compared to the size of the plain text. The method can be improved by including multiple rounds of intron splicing. The difficulty with the method is, if the key becomes complex, it will affect the speed of decryption also. The intruder must be aware of biological principles, to decrypt the message.

B. One time pad

The method uses a substitution one time pad[8] cryptosystem. The plain text, which is represented in the form of DNA, is partitioned in to words of fixed length. A substitution one time pad table is used which randomly maps all possible plain text word to cipher text words. The method is implemented for the encryption of 2D images using DNA chip.

Another method of one time pad is an XOR scheme, which uses molecular computations. Either the original DNA or DNA encoded message can be encrypted using this one time padding.

C. JAVA - DNA cryptography encryption

The Java - DNA encryption includes both symmetric and asymmetric methods for encryption[2].The algorithm includes mainly 3 steps: key generation, encryption and decryption. The key using for encryption and decryption should have same length of the plain text block.

In the symmetric approach, the key is translated in to DNA form by assigning the bases A,C,G and T to each of the number 0 to 3[2] using a translation table. Because of the huge size of the plain text and the key, the text is divided in to fixed sized blocks, and each block is encrypted using same sized key. If the text size is not multiple of block size, padding is implemented. Encryption is implemented by double encryption. The first encryption step uses substitution technique. Here plain text is represented as DNA language by using a substitution table. The obtained result is converted in to byte array, and XOR with the key to get the double encrypted message. The algorithm was developed using Open JDK, which is based on the JDK 7.0 version of JAVA.

IV. Encryption of Image Data

Since image encryption has various applications in areas like medical imaging, internet communications, telemedicine and military communications, it is important to hide the contents of a message when it enters in an insecure channel. The traditional image encryption schemes, except one time pad, own only computational security [1]. DNA encryption makes a bridge between the existing methods and a new encryption technology for images. Due to the enormous storage capacity of DNA sequence, it is very useful to store the information of images. Since asymmetric encryption uses different keys for encryption and decryption, it is a time consuming process[2]. Image encryption includes large amount of data and hence asymmetric methods are not commonly recommended[12]. The section follows describes the various existing DNA encryption methods of two dimensional images.

A. Uncompressed image encryption algorithm

The algorithm uses DNA as information carrier and thus reduces the time for encryption. This facilitates encryption of big image without compression[5]. In this method, two levels of encryption are used. In the first level, the image is scrambled by applying any discrete system like Arnold cat map [4]. The pixels of the discrete image are represented in terms of DNA bases using DNA digital coding. Three DNA templates are created using a key DNA sequence. The third image template is the encrypted image. The key DNA sequence and the frequency for scrambling together are transmitted through a secure channel as the key.

The algorithm is extended to video also. In the case of video data, since the number of frames is large, a scrambling method which needs less time, should be used.

B. Image encryption using transforms

The algorithm uses two levels of encryption. In the first level, the original image is divided in to a number of blocks. Each block is transformed with DWT, DCT and a combination of DCT and DWT transforms[3]. In DCT, the blocks of image are transformed from spatial domain to frequency domain. In DWT, the blocks are transformed in to wavelets[3]. This makes the image distorted. Using DNA digital coding each base is assigned a four bit binary code. For key generation, DNA sequence and size of the image are used. The key is added with the transformed image to get the encrypted image.

As a result, the encrypted image is highly uncorrelated to the original image, and hence it ensures security of the image.

C. DNA fractal based image encryption

The algorithm does not use any biological operations, but DNA sequences are used as secret keys for image encryption. The security depends on the variety of real DNA sequences. Hao. et.al [6],[8] proposed a DNA fractal sequence representation approach. The method is based on counting the frequency of appearance of a given string of a given length in a sequence. When this method is applied to all the known genome sequences, it reveals a fractal like pattern.

Any DNA string is composed of repeated units of A,C,G,T. In order to count the frequency of occurrence of a

four word string , 4^k counters are needed. In this encryption method, a modified permutation approach is used to improve the security of permutation approach. A gray image is considered with size a X b. the values of counters k1 and k2 are calculated using Hao's fractal principle. Then k1 and k2 are converted in two binary strands. Length of the two sequences are represented as bk1 and bk2. A secret permutation key sequence is also converted in binary sequence. The sequences bk1 and bk2 are enlarged to the length of permutation key sequence. Now input bk1 and bk2 in the reverse order to get Bk1 and Bk2. Finally bk, Bk1 and Bk2 are XORed bit by bit to get a binary strand bm. The obtained binary strand , bm , can be represented as a DNA sequence.

The image is converted to binary matrix, and then carry out DNA encoding. By using the secret key and applying Hao's principle and logistic mapping, a scrambled image is produced[8]. The encrypted image can be send through insecure channel and secret key through secure channel. The method is more secure than most of the existing chaos based algorithms.

D. Image encryption using chaotic maps and DNA addition.

The method uses four chaotic maps on a two dimensional image as first level of encryption. Then uses DNA addition[10] operation to produce the encrypted image. For encryption the secret keys are calculated using the original 8 bit grey image. The chaotic maps used are 2D logistic map, cross chaotic map, henon map and ikeda map. The DNA bases are represented using digital coding as assigning the bases A as 00, C as 01, G as 10 and T as 11.

For encryption initially the original image is converted in to binary image and DNA image. Then divide the image in to small blocks of size 4x4. Apply chaotic mapping functions and the obtained chaotic sequences are reconstructed to raw and column matrices X and Y respectively. X and Y matrices are multiplied to get a matrix k' , which is then converted in to binary matrix. Using DNA encoding, the binary matrix is modified. The obtained DNA matrix is divided in to small cells. By applying DNA addition, chaotic mapping encryption is implemented. Addition and subtraction operations of DNA sequences are performed according to traditional addition and subtraction operations.

The method can be improved by removing the noise effects, in better way, by suitable noise filtering schemes.

V. Analysis of DNA Encryption

Table 1 and Table II describe an overview of existing DNA encryption methods for text data and 2D images respectively. The main difficulties o DNA cryptography based image encryption are the absence of the effective secure theory and simple realizable methods. Encryption and decryption based on biological problems are safer when compare to mathematical ones. DNA encryption owns vast parallelism, exceptional energy efficiency, and extra ordinary information density inherent in DNA molecules.

TABLE I
SUMMARY OF DNA ENCRYPTION METHODS FOR TEXT DATA

Cryptographic methods	Technology used	Remarks
Pseudo DNA encryption	Symmetric encryption method. Applying translation and transcription operations	Only a very little information is needed to be transmitted in secure way
One time pad	Symmetric encryption	Simple to implement. Successfully applied for image data also.
JAVA DNA encryption	Both symmetric and asymmetric encryption methods are implemented.	High security ensured for asymmetric encryption. The method is applied only for text data

TABLE II
SUMMARY OF DNA ENCRYPTION FOR 2D IMAGES

Encryption method	Technology used	Remarks
DNA encryption of big images	Applying Arnold cat mapping,Symmetric encryption, DNA templates of image are used	Encryption is applied for uncompressed image, hence less information loss.
DNA encryption with transforms.	DCT and DWT transforms are used. DNA sequence is used for key generation.	The encrypted image is highly uncorrelated with original image.
DNA fractal based image encryption	DNA sequences are used for key generation.	Applied for only Grey image
Encryption with DNA addition	Chaos based encryption. DNA sequence is used for key generation.	Applied for Grey image. Noise effects are not totally removed.

VI. Conclusion

DNA cryptography is a fast developing interdisciplinary area. Encryption using DNA is more secure. One gram of DNA can contain 108 terrabytes of data. A few grams of DNA may be sufficient to hold all the data stored in the world. The use of DNA reduces the necessity of signature authorization. Due to the vast storage capability of DNA, it can be used to store big images also. The method is powerful against most of the attacks, especially brute force attack [11].

References

[1] Martyn Amos, gheorghe Paun, Grzegorz Rozenberg, Arto Salomaa,'*Topics in the theory of computing*',Theoretical computer science 287, 2002,3-38.

[2] Radu Terec,Mircea Florin Vaida,Lenuta Alboaie,Ligia Chiorean, '*DNA security using symmetric and asymmetric cryptography*', International journal of new computer architectures and their applications,IJNCAA,vol 1,2011,

[3] K Sumathy and R Tamilselvi,'*Comparison of encryption levels for image security using various transforms'*, international conference on information and network technology,IPCSIT vol 4(2011).
[4] Anton and Howard,*Linear algebra and applications*, 7th edition,New York,John Willey and sons,1994.
[5] Shima Ramesh Maniyath and Supriya M,'*An uncompressed Image encryption algorithm based on DNA sequences'*, D.C Wyld,et al,(Eds):CCSEA 2011,CS & IT 02,pp 258-270,2011.
[6] Qiang Zhang,Shihua Zhoa and Xiaopeng Wei,'*An efficient approach for DNA fractal based Image encryption*',Applied mathemetics and information sciences, an international journal 5(3),(2011) 445-459.
[7] Bai Lin hao,H.C Lee and Shu Yu Zhang,'*Fractals related to long DNA sequences and complete genomes'*,Chaos, Solitons and fractals 11 (2000) 825-836.
[8] Ashish gehani,Thomas H Labean and John H Reif,*DNA based cryptography*,LNCS 2950Festscrift, Springer, pp 167-188, 2004
[9] Kang Ning,*A pseudo DNA cryptography method*, http://arxiv.org/abs/0903.2693
[10] kuldeep Sing,Komalpreet Kaur,'*Image encryption using Chaotic maps and DNA addition operation and noise effect on it*',International journal of computer applications (0975-8887) volume 23 – No.6,June 2011.
[11] S.Jeevidha,Dr.M.S.Saleem Basha,Dr.P Dhavachelan,*'Analysis on DNA based cryptography to secure data transmission'*, intenational journal of computer applications, (0975-8887) volume 29- No-8, september 2011.
[12] Shihua Zhou,Qiang Zhang,Xiaopeng Wei and Changjun Zhou,'A summarization on Image encrytpion',IETE technical review vol 27 issue 6, nov-dec 2010.