



A Dual Mode DNA Cryptography: Bio Inspired Approach for Information Security

Fakhrayh Al Harrasi¹, Dr. M.S.Saleem Basha², Dr. A. Mohamed Abbas² and Mohamed Jameel Hashmi²

¹Post Graduate Student, Mazoon University College, Muscat, Sultanate of Oman.

²Assistant Professor, Mazoon University College, Muscat, Sultanate of Oman.

Abstract: Modern studies focused on Deoxyribonucleic acid (DNA) because that DNA have several important features including the random nature of the sequence of nitrogenous bases consisting the acid and large storage capability of the information that led to its usage in the field of encryption where the appearance of a new branch which is encryption of DNA. This research provided a new method to encrypt text files using DNA were building a set of coding tables and using them to obtain the cipher text in DNA form, also used a set of transposition cipher methods for the purpose of increasing the security of the resulted cipher text. Security is more important in the organization. The company's document information is encrypted to save the information. The Deoxyribonucleic Acid (DNA) cryptography is emerged with progress of new promising structure of DNA Computing. This concept is massive parallelism with large information of density and inherent the DNA molecule of exploited of cryptographic purposes. The requirement is high tech model bimolecular in laboratory of proposed structure of DNA molecular one time pad scheme structure with DNA hybridization techniques and it minimizes the complexity time. The DNA cryptography use of DNA nucleotides and it denoted by alphabet characters C, G, A and T to perform encoded with micro messages. It is transmitting the secrets and creates the encoding rule of DNA components.

Key words: DNA cryptography, PCR, Steganography

I. Introduction

Every company have Network and have Internet access, it will be worry of its data from unauthorized access, so the system Administrator will be responsible to implement all kinds of security to make the network in safety Place to make the Network in Perfect protection and defense for any type of hackers. The System Administrator have keep all the Network Device in secure place for example, he or she have collect the routers, Firewall and switches in rack and the rack should be block all the time by using key. To limit access to the device and make any update or change the configuration for the device. In addition the hardware device should have password to access it from all the ports. The network device and all servers in the Network should be collected in one room its call server room or data center. This room has on Authorized access for the people who have the permission to access for monitoring and fixing the network. This room should be blocking in all times and they can access it by using the key room or by using access card. For each employee in the company have user name and password to login his computer and before he leave his office he have to log of or make shutdown to limit any unauthorized access for the files and documents or any sensitive data by using the user accounts in the company. All the clients or the PCs in the company should have Software antivirus to protect the data from virus or others when they using USB. This DNA cryptography is to encrypt the textual information and maintain the security for the text message. The company important information like password, account number, employee password can encrypt. While encrypt the information can create the code and can decrypt the encrypted messages. The Nucleotides are quaternary source code and the each letter is denoted character string ATC and the letters B are ACC etc. The synthesize of secret message of are encoded into DNA sequence. According code synthesized of secret message of DNA with of secret messages. The secret messages are encoded to DNA sequence message 69 nucleotides and each word is PRC primers. The DNA message are physically can look the human DNA by nucleotides long and concealing DNA mixed, attached the common colorless form of microdots.

II. Literature Review

The DNA method is Biotechnological method and it has been wide class of developed for the operation of DNA and RNA standard. It includes site based and splicing operations. The Data Encryption standard (DES) are using vast parallelism are available via the recombinant of DNA to combinatorial to search the large number of various solutions of DNA standards. This method is solving various combinational method of search the problem and succeeds for various problems and intimately limited volume requirements. The research of DAN computing is re-combination of DAN technique and generally bimolecular computing (BMC) are using biotechnological computations [1]. The substitution method are using library to distinct pads and each method are specific randomly to generate pair the encryption of natural DNA and encryption to encrypt the binary data.

The present novel and chip based micro array technology are 2D data input and encrypted output. The DNA cryptography are secretly take are input in the DNA standard and collection of various DNA standard. The potential limitations of cryptography method are showing assumptions of entropy and plain text messages. The various combination of DNA are showing sufficient to allow the universal commutation of BMC method and solve the difficult re-combinatorial problems are such as Hamiltonian path Problem of data Encryption standards [2]. The cryptography are executing the further application and pure combinatorial search. The DNA and RNA media for data storage and very large amount of the data are store in the compact volume. The vastly exceed storage contain and conversational electronic optic media and store the applied concentrations of DNA standards and constitute biological data and it obtained more convention of binary storage media. The DNA data are moved to conventional binary storage media and varieties of techniques are included in DNA standard use of alphabet and short of alphanumeric sequence. It discussed method to get the fast associative and search the DNA database for hybridization. The BMC technique are perform more sophisticated database operations and database join architecture massively parallel operation of the DNA data. The various techniques are including in the DNA chip array and binary data are encoded DNA standards using alphabet short sequential of letters with continues sequence [3]. The data security and cryptography contain critical aspects and conventional computing is more important of DNA database application are provided the basic terminology are in the terminology. The sender and receiver wishes to send the message to encrypted format and over the finite alphabet. The encryption is the process of the plaintext message and transforming encrypted message of cipher text. The fixed code can be provide the initial mapping form he characters to the plaintext alphabet review process of physical system to encrypt and transformation of read out and unbreakable cryptosystem with successful of cryptanalysis and it is decryption algorithms. The two point of critical security of issues and it should be created about the codebooks and can be truly random to security of issues and randomly select the classical approach of random letter and secret code contain the cryptosystems and its absolutely unbreakable [4]. The DNA based cryptography are simulating the DNA using computers with Pseudo virtual DNA computing. The substitution method are using libraries and one time pad and define randomly pair-wise mapping the scheme are index random key string used in the encryption. The DNA sequences are matrix obtain and encode the original image and dividing into equal block of two logistic maps. The DNA sequence additional operations are use and the element in the block. The DNA matrix is decoded and get encrypted image. The plaintext are cipher pairs and constructed there complete coverage of lexicon on each pad and nearly unique word are mapping between the plain text and cipher pairs. The result of cipher word is plain text and assembled in random order. The DNA stand by the higher efficiency technique and hybridization of complemented Almena's original DNA experiment [5]. The two different cryptographic are based on the DNA binary potential interceptor and the decryption are using PCR with subsequent electrophorus. The DNA sequence are convert into spliced data and curing specified translated and converted mechanisms of DNA function. The method is pseudo DNA cryptography method. The DNA computing are full potential of DNA cryptography and the process are taking to molecular level and realized to outside of ultra-modern DNA laboratory. The DNA binary standard is more secured and satisfactory of multi-level and to resist exhaustive of statistical attack and differential kind of attack. The DNA Sequence of other related data are protein in the secure channel. The DES - Data Encryption Standard algorithm with approximately 72 types of quadrillion possible keys is can generate. The security of DES is based on difficulty while picking the rout key and 16 round nonlinear operations can do. Breaking the DES is difficult. The following picture are DNA based cryptography method and it contain repeating unit are contain sequence of world, bi from the set in the cipher of the code book are matching words. The unbreakable of the letter standards and one time pad are between the message sender and decryption of undesired interceptor features of DNA message. To share the advanced for the information to assumption and it require of standard and provide the nature of secret message and fascinated combination of data and large number of message to assemble. The sequence of word Contain and form the set of cipher of codebook. It is matching the words. The sequence word or each pair and uniquely associates of plaint text with the string word. The with B1 are correspond the complement of the cipher word of B1. It can use polymerase primer and the extended growing of DNA standard boundary of paired. Each individual strand from one time pad and it consist of cod book library of specified word pairings. The one time pad contain DNA Strand of length are provided in this picture [6]. The DNA cryptosystem for 2D image are using DNA chip and randomly assembled one time pad and system capable of data encryption and decryption to provide the input data and output data in the form of 2D image are recorded in the microscopic array of DNA chip. The basic DNA technology is previous use of the DNA chip of Input and output. This system are describe the data set to encrypted and the chip are bearing immobilized data sent to encrypted format and various of the method of encoding encrypting in the form of data type and encrypted information. This chip contain the addressable of array and nucleotide of sequence of immobilized and multiple copy of multiple sequence in the microscopic pixel. The DNA chip are currently commercially available and construction of method [7]. The DNA Stegnography technique are class of techniques in the information are hide using secret message and within another message. The Stegnography system is original plaintext and it is not actually encrypted and disguised of hidden message with another data.

The historical Stegnography are use of grills in the mask and the image except of secret message. The micro photographic are placed in the large images invisible En-cryptography are generally consider conventional method and low security. The plain text are encrypted and listed of other media with numbers cases are using Stegnography method. It was practice the appealing and simple bio technological method with secret keys are stands. The plain text are DNA are stands and random assemble the knowledge of recombinant of separation of methods. The plain text message is standard and separated of hybridization with magnetic surface. It support the separation of combined with amplification steps are included [8][9]. Cryptanalysis of DNA Stegnography System is true cryptographic cipher and security depended with secret key. The security system is deriving the format of Stegnography system and adversary of existence message in the form of medium and distinguishes of plain text message. This system can be generated and DNA Stegnography system is security and depended of DNA stands. It is more responsible of the distracter and strands are constructed in the form of random of assembly and generated format of additional source are generating with plain text message. The probability of source are generate with plain text message. The probability of distribution of source generator to establish the English text message and class of none coding standard to constant and protein coding standard. The plain text DNA source has entropy and constant of plain text with images are entropy, overall entropy are most classes of DNA. The range 1.2 to 2. The each round for the data separation and assume the mixture of tagged plain text. The mixed high concentration of distracter and size of the information are reduced with previous ration. The pour of faction's s of the volume of current and remaining faction volume into the test data [10][11]. Compression of Plain Text is another method to improve the DNA Stegnography system to recode plain text are using universal compression algorithm method and such also resulting redistribution of the recoded and assembled distracter sequence and suffice to provide and improved security . This system unlined conventional Stegnography method and recording to done by BMC recording method to similar discussed in this section summation to similar section are mapping Stegnography system and absolutely provide one time pads for equivalent decryption of text. The system are describe and consist of data set to encrypted in the chip are barking immobilized using DNA standards. The library of one time pads and encoded long DNA standard. The 2 dimensional images are various data type to incepted microscopic pixel. The DNA chip is currently commercially available and chemical method to construction of customer format [11]. The DNA chip are displayed analog and chemically added into the cipher worked using olio synthesis. The DNA chip complementary contains the plain text lexicon and fluorescent are labeled strands prepared to protect some pixels with plaintext of cipher words. The cipher word is stands and still labeled with decryption word pair strands and must be reconstructed appending the cipher words and proper plain text words. The decrypting process are fluorescent label and photo-labile based on unnecessary and cannot in the present image. The final to involve the bending reformed and word pair are stands to DNA chip with reading message of fluorescent. The following image is showing step by step procedure to encryption [12].

III. Proposed Method

In the proposed method there are three steps are implemented for the purpose of DNA cryptography. First, each alphabet in the English language is assigned with the short length of DNA sequence. Second, a random key value is applied to the output of the first process. Third, convert the resultant English alphabets to their corresponding position in the English Language alphabet list.

(A) Substitution Method:

The proposed method starts with defining with the substitution table with each alphabets in English language including upper case and lower case, is assigned with a short DNA codons consists of 3 nucleotides of DNA (A, G, C, T). So, there are sixty four different combination of codons is possible. The substitution of DNA codons to the equivalent English letters are based on the upper case and the lower case of the English language alphabets as shown in the Table 1.

Table 1: Mapping of English Letters to DNA codons

Alphabet	Codon	Alphabet	Codon	Alphabet	Codon	Alphabet	Codon
a	TTC	n	TTA	A	TTG	N	TCT
b	TCC	o	TCA	B	TCG	O	TAT
c	TAC	p	TGT	C	TGC	P	TGG
d	CTT	q	CTC	D	CTA	Q	CTG
e	CCT	r	CCA	E	CCG	R	CAT
f	CAC	s	CAA	F	CAG	S	CGT
g	CGC	t	CGA	G	CGG	T	ATT
h	ATC	u	ATA	H	ATG	U	ACT
i	ACC	v	ACA	I	ACG	V	AAT
j	AAC	w	AAG	J	AGT	W	AGC
k	AGA	x	AGG	K	GTT	X	GTC
l	GTA	y	GTG	L	GCT	Y	GCC
m	GCA	z	GCG	M	GAT	Z	GAC

(B) Key database and PCR:

To generate the key set for the secure communication PCR (Polymer Chain Reaction) is used to generate the random key to the each set of information which is to be sent secretly. PCR is the process of generating a

considerable random length of DNA string. In this proposed method it used the PCR to generate the random key. The random key length in the proposed method is same size to that of the out got from the substitution method referred with Table 1. To be agreed between the sender and the recipient of the series of information and these are available within key database, including the representation of random alphabet to the combination of DNA codons of the key and the output of the substitution method s shown in the Table 2.

Table 2: Codons Mapping with Alphabet

DNA	DNA	Alphabets	DNA	DNA	Alphabets
T	T	B	A	T	D
T	G	H	A	G	I
T	A	K	A	A	R
T	C	M	A	C	P
G	T	S	C	T	X
G	G	V	C	G	W
G	A	Y	C	A	Z
G	C	E	C	C	F

So, there are sixteen possibilities of the choosing two codons from the set of 4 codons with the repetition. Once, mapped these codons with the alphabets, Convert the alphabet to the numbers according to the alphabetical order. The binary number system is then used to convert the alphabetical order to binary representation. To represent twenty six English alphabet's position five binary bits is sufficient thus it may be considered a Re-Encryption.

Table 3: This table we used DNA Condon to Binary

Binary	Codon
00	A
01	C
10	G
11	T

Then the binary representation of the message is then converted to DNA codons with refer to the Table 3. Further the DNA codons are transmitted to the intended recipient. Five stage DNA cryptographic technique

A. **Encrypt Method Diagram**

The overall process of the proposed work is stated as a flow char as shown in figure 1.

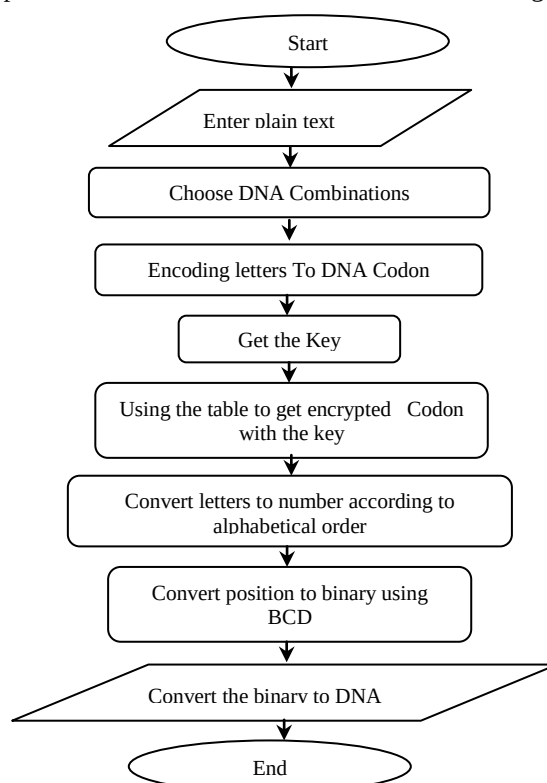


Figure 1: Encryption Method

B. Decrypt Method Diagram

The decryption of the proposed method is the reverse of all the operations of the encryption method is illustrated in the figure 2.

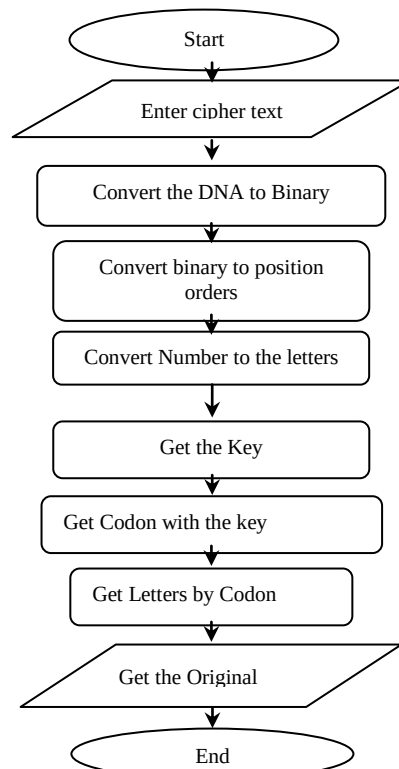


Figure 2: Decryption Method

IV. Implementation

The proposed method is implanted in C#. The screen shot is shown in Figure 3 and Figure 4 to illustrate the way how the proposed system works. To clarify the mechanism of proposed method a sample plane text is used as an example. Note that the decryption process are the same steps but in contrary way.

Table 4: Encryption of sample plain text.

The Plain Text	:	my name is fakhrrayh alharrasi
Convert letters DNA Codon	:	GCAGCCGGTTCTTTTCGATCCTGGTACCCGTGGTCAGTTCGTTATCCATTTCGCCA TCGGTTTCGCTATCTTGCCACATTTCCGTACC
Generate randomly key using PCR	:	GCCCCGGGATAAGTTTCACTACCGGATGTGCGACCGCTGGTGAAATGTCGACCC CATAATGCTGGGCGTCTAGGTTTGCTGCGACCG
Mapping with the key	:	VFPEFWVVBZKHBXSPKFXKEEHIZXWSHEVKFPVMBWVBHRKZXIBMHZEFPF KXYYBHMVWVHPHXM BYWDXDHMBWVFKPFW
Character coding	:	22-06-16-05-06-23-22-22-11-02-26-11-08-02-24-19-16-11-06-24-11-05-05-08-09-26-24- 23-19-08-05-22-11-06-16-22-13-02-23-22-02-08-18-11-26-24-09-02-13-08-26-05-06-06- 16-11-24-25-25-02-08-13-24-22-23-08-16-08-24-13-02-25-23-23-04-24-04-08-13-02-23- 06-22-11-16-06-23
Binary Representation	:	10110-00110-10000-00101-00100-01000-00110-00010-11000-00010-10000-01100-01000- 11001-00010-00100-01000-01000-10000-00100-01001-10000-10001-00001-01000-00001- 00010-01000
DNA coding	:	AGAGAACGACCGAACCAACGAGATAGAGAGAGACACAAAGAGCGACACAAGA AAAGAGCAACGCACCGACACAACGAGCAACACAACCAACCAAGAAAGCAGCG AGCAAGATACGCAAGAAACAGAGACACAACGACCGAGAGACATAAAGAGAT AGAGAAAGAAGAACGAACACAGCGAGCAAAGCAAAGACATAAGAAGCGAACC AACGAACGACCGACACAGCAAGCCAGCCAAAGAAGAACATAGCAAGAGAGAT AAGAACCGAAGAAGCAACATAAAGAGCCAGATAGATAACAAGCAAACAAGA ACATAAAGAGATAACGAGAGACACACCGAACGAGAT

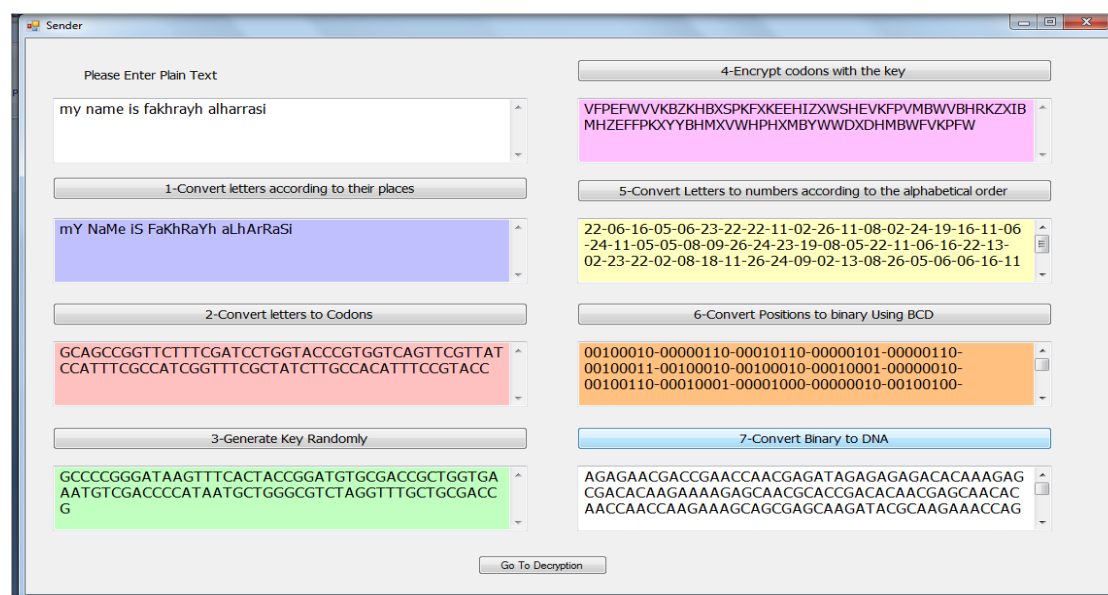


Figure 3: Screen Shot of Proposed Encryption Method

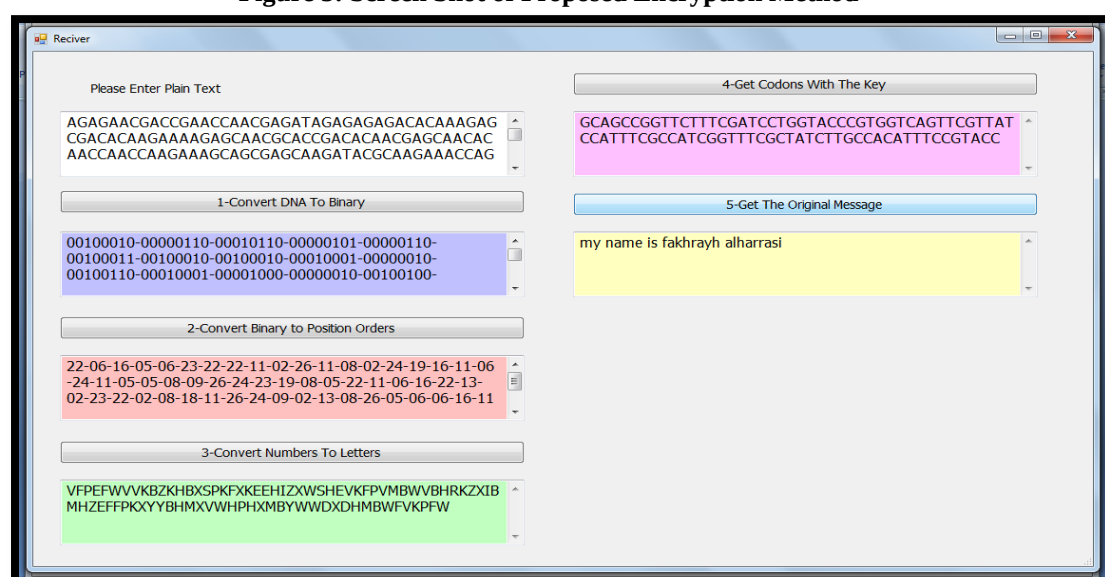


Figure 4: Screen Shot of Proposed Decryption Method

V. Conclusion

In the paper, we have stated a new encryption method for the secure communication. The key used in this proposed method is generated by the polymer chain reaction, which means the DNA sequence got from the Polymer Chain Reaction is highly random in nature and impossible to guess or brute force attack. Also, two times the plain message was encoded with DNA equivalent; hence it is called Dual Mode encryption. In the proposed method a symmetric key has been used. In near future public key will be used.

References

- [1] Barnes W.M, "PCR amplification of Up to 35 kb DNA with high fidelity and high yield form bacteriophage templates".
- [2] Adleman. L, "Molecular Computations of Solution to Combinational Problems", Science 266,1021 (1994)
- [3] Adleman. L, "On Constructing a Molecular Computer", Dept of CS., U.S.C., 1995. Available via anonymous FTP form.
- [4] Baum. E.B, "DNA sequence useful for computations, 2nd Annual Diamacs Meeting of DNA based computers", Princeton University, June 1996
- [5] Hagiya. M.M., Arita, and D.Kiga, "3rd DIMACS Meeting of DNA based Computers", University Penns, June 1997.
- [6] Head. T, "Splicing Schemes and DNA formulas with Molecules".
- [7] Mills. A, "Meeting of DNA based computing", Baltimore, Penns, June 1998
- [8] Wang L, Liue A and S. Gillmor, "Surface based DNA computing operations Destroy and Read"
- [9] Roberts S.S, "Turbocharged PCR", Journal of NIH Research, Meeting on DNA based computing Baltimore, Penns.
- [10] Schneier. B, "Applied Cryptography" 2nd Edition, Jonnwwally
- [11] J.Ziv and A.Lempel, A. "Universal Algorithm for Sequential Data Compression".
- [12] Mills, A.B.Yurke, P.Platzman, "Error-Tolerant massive DNA neural - Network computations".