I. J. Computer Network and Information Security, **2019, 7, 13-20**
Published Online July 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2019.07.03

An improved DNA Based Security Model using Reduced Cipher Text Technique

Lalit Mohan Gupta
Vivekananda College of Technolgy & Management, Aligarh, India
E-mail: lalitmguptaamu@gmail.com

Dr. Hitendra Garg and Dr. Abdus Samad
Hindustan College of Science Technology, Mathura, India
Aligarh Muslim University, Aligarh, India
E-mail: {hitendra.garg, abdussamadamu}@gmail.com

Received: 03 May 2019; Accepted: 29 May 2019; Published: 08 July 2019

Abstract—An essential parameter of information security during data transmission is a secure cryptographic system. In this paper a new cryptographic security technique is proposed to secure data from un-authorized access. The proposed system incorporate cryptology technique of encryption inherits the concept of DNA based encryption using a 128-bit key. Besides this key, round key selection technique, random series of DNA based coding and modified DNA based coding are followed by unique method of substitutions. The proposed technique increases size of the cipher text by 33% as compared to conventional DNA and non DNA based algorithms where size of the cipher text becomes almost double of the original file. This reduction in cipher text improves memory utilization along with data security.

The paper is organized in six Sections. Section 1, gives the introduction and also briefly describes related work. In Section 2, the proposed model for solving the problem is described. Various steps involved during encryption and decryption are explained in Section 3, and the results obtained by implementing the proposed algorithm are presented and discussed in Section 4. The Section 5 concludes the work and brief outline of the future work is given in Section 6.

Index Terms—Deoxyribo Nucleic Acid, Reduced Cipher Text, Secure Access Control, Privacy, Security, Data Hiding.

I. Introduction

Due to rapid growth of Internet services, security of data during transmission has become the primary concern. When data belongs to the financial domain such as, bank transactions, e-commerce transactions etc., security becomes critical and the most essential factor related to confidentiality and integrity of the message.

Cryptography plays an important role in incorporating security by manipulating information. Computer revolution brought a new meaning of information and gave a new inclination in the development of security and cryptographic protocols. Computational power produced the possibility to build new and strong algorithms in cryptography, but strong tools are used by cryptanalysts to break cryptosystems. This means the challenge of developing new and powerful ciphers is always of interest and offers new directions to explore cryptography. The major aspects handled by cryptography are: confidentiality, data integrity, authentication, and non-repudiation. Various techniques have been proposed by researchers in the field of cryptography in the recent past [1-5].

De-oxyribo Nucleic Acid (DNA) cryptography is a modern trend in the cryptographic field in research of DNA computing where DNA works as the information carrier. DNA is used as the basic storage medium for information transmission as well as to perform computations. DNA can work either at molecular level (biological DNA) or with genetic databases (digital DNA). The advantages of digital DNA databases can be dilated to the information security domain through DNA cryptography. DNA cryptography is simply hiding of information in terms of DNA sequences. Several DNA cryptographic techniques have been proposed in literature [6-8]. DNA based symmetric key cryptography is another approach to handle the issue of security [9]. The authors performed practical implementation and theoretical analysis to show that their approach is efficient in computation, storage as well as in transmission of information.

An important technique for secure transmission is being data hiding where a secret message is embedded in the original message during transmission to maintain confidentiality of the message on the receiver side. To strengthen security of the data, various data hiding methods based on DNA sequences have been introduced by several researchers [10, 11]. Chang et al. introduced two DNA based reversible data hiding techniques in which sensitive data could be recovered by restoring the original DNA sequences [12]. These techniques require a compression method to embed sensitive data which needs

some extra efforts.

Atanu Majumder et al. proposed an efficient method of DNA based cryptography in which a key 256 bits is chosen randomly for encryption, and 16 characters in the formation of cipher text. This technique reports lesser execution time during the encryption–decryption process [13].

H. J. Shiu et al. [14] introduced DNA sequences based data hiding methods which are insertion method, complementary pair method and substitution method. In the insertion method, insert bits from binary converted secret message are arbitrarily in alienated positions within a DNA reference sequence. In the complementary pair technique, the greatest complementary pairs in a sequence are detected to conceal the message parts before making communication. Both insertion method and complementary pair method result in growth in length of the original sequence. Lastly, substituting some of the DNA nucleotides with others based on the message bits are to be done in substitution method. These three algorithms conceal data by changing the original DNA sequence, either by substituting or inserting some bases, without taking into consideration the operation's biological consequences, resulting in some distortion and dangerous effects on the biological characteristics of a specified organism. The robustness and tightly embedded capacity analysis of the mentioned methods have been demonstrated to show better performance of the methods as compared to competing methods on capacity, payload and number of bits hidden per character (bpn) parameters.

Peterson et al. also discussed a substitution method to hide data in DNA sequences [15]. Another method of data hiding is index based DNA encryption method that utilizes block cipher [16]. The author applied simulation and analytical analysis on the proposed technique to show better performance on the encryption and decryption processes which makes it difficult for attackers to breach security of the message. Ying-Husan Huang [17] proposed reversible data hiding techniques to strengthen the method of Shiu schemes [14].

Abir Awad et al. [18] used a Chaotic DNA substitution method, shuffling of image pixel positions incorporated to enhance high level of security of sensitive data. Similarly, Chaos based Symmetric Key technique for color images, scrambles images using Arnold Cat Map to create ambiguity and then convert to DNA Codes [19]. This method appears to be fruitful to encrypt and decrypt RGB color images using secret keys.

Nooral Hussain et al. [20] overcame the limitation of DNA cryptography that uses modular arithmetic in their attempt, but were unable to reduce memory size of the cipher text. Prior to DNA sequencing, embedding secret information into the host images is the traditional process for data hiding.

In the proposed work, security, confidentiality and integrity of the message are achieved by applying DNA based multilayer encryption technique. Each encryption layer provides more secure communication with reduction in size of the cipher text. Size of cipher text is improved and a reduction of approximately 33% in the obtained cipher text as been observed as compared to the size of cipher text obtained by traditional encryption techniques. The resulting cipher text becomes more secure because it is in the form of unreadable, unpredictable, ambiguous text which creates confusion to predict the decryption process for accessing the original message by unauthorized users.

II. The Proposed Model

The proposed model combines the approach of conventional cryptography with DNA based cryptography in order to provide multiple layers of encryption. Each following layer of encryption has its own method and is considered more secure than the previous state of encryption. The obtained cipher text (CT) at last becomes more secure than conventional DNA techniques because the resulting cipher text comes in the form of unreadable, unpredictable, ambiguous text that creates confusion during the decryption process. The resulting cipher text files are not only smaller in size but also enhance security of the data. The complete process of incorporating multi layers encryption is divided into two phases known as Preliminary Encryption and Secondary Level Encryption as described below.

A. Preliminary Encryption

Preliminary encryption is the first phase of the encryption process in which cipher text is obtained using the block method of plain text with some modification. Initially, any 128 bit strong key is arbitrarily selected which is further transformed into 4 ×8 matrixes, with each cell consisting of a 4-bit key value. Afterwards, the 128-bit key is converted into a matrix row wise. Then the key bits are read, one row at a time. This produces a sub-key of 32-bit, a total of four blocks of sub-keys will be generated. Each block of sub-keys is named with one of the four DNA bases namely, T, C, G, A. There are 24 possible combinations of length 4 such as, TGCA, AGTC etc. The algorithm selects one of the sequences randomly as the sub-key for round key selection. During the encryption process, these sub-key blocks are used in four rounds of encryption operation. The selected DNA sequences, secret key and position of extra coding are shared through a secret channel between the sender and receiver. In the data encryption phase, byte values are extracted from the input file or message.

a. Algorithm

The proposed algorithm works as follows. In the first step, encryption process is applied on byte values of the input file, which is termed as plaintext. Each character of the plaintext is converted into 8-bit binary values and 128-bit blocks are formed. Each block of binary stream will go through the encryption process. In the next step, the 128-bit binary stream is partitioned into four 32-bit blocks. The 32-bit block is Ex-OR with round 1-key, Key1. The output generated is Ex-OR with the next 32-bit block and so on. These four outputs of the 32-bit block move through a straight D-Box. The complete

algorithm with four rounds of encryption operations is shown in Fig.1.

B. Algorithm Presentation

The proposed preliminary encryption scheme consists of the following phases:

1111	1110	1011	1001	0100	1001	1110	1011
1001	1100	1011	1111	0000	1010	1110	1001
1101	1010	1110	1001	0101	1100	1010	1011
0000	1110	1111	1011	0100	1000	0110	1001

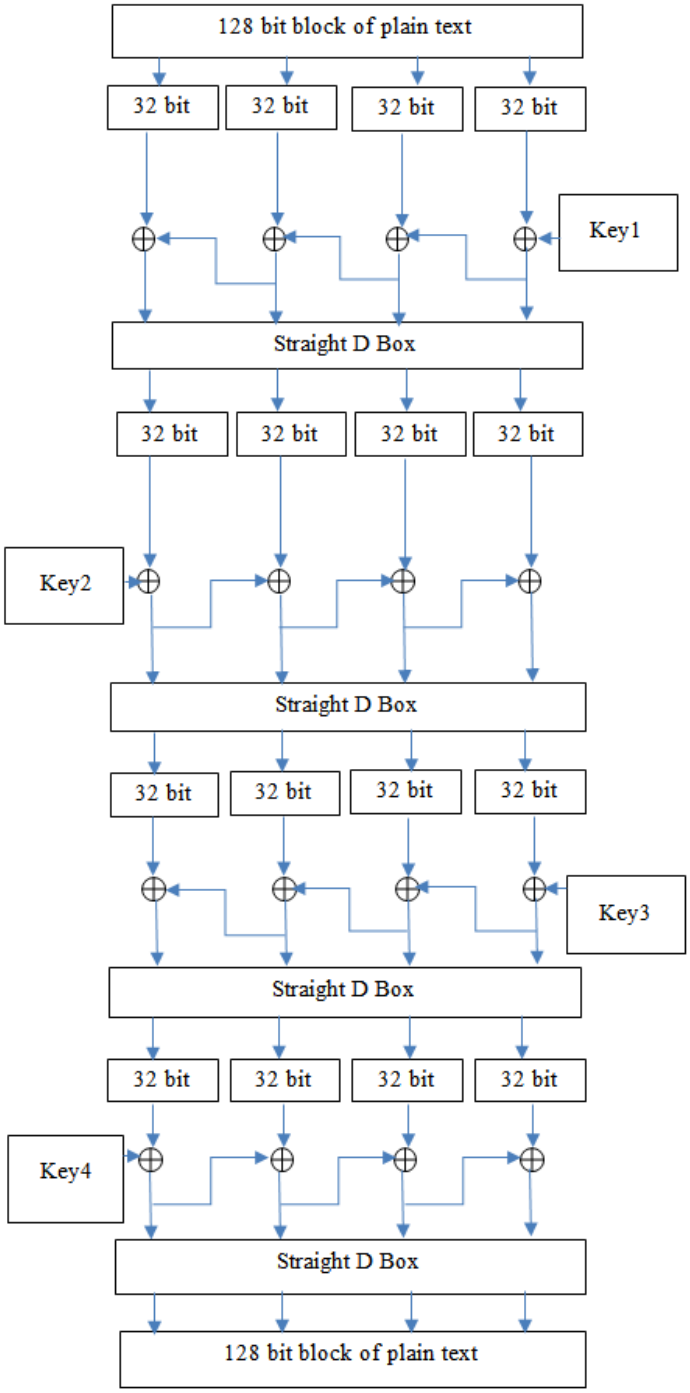

Fig.1. Algorithm with four round of encryption operations

a. Round Key Selection

In this phase, a key of size 128-bit is selected arbitrarily. This selected key is transmitted into an 8×8 matrix. Let, Key K= '1111 1110 1011 1001 0100 1000 1110 1011 1001 1100 1011 1111 0000 1010 1110 1001 1101 1010 1110 1001 0101 1100 1010 1011 0000 1110 1111 1011 0100 1000 0110 1001'

Convert key K into a matrix of 4×8 form (row wise), where each cell consists of 4 bits of key value and then read one row (32 bits) at a time that produce 4 subkeys. Each subkey is labelled with DNA bases (A, T, C, and G) as follows:

T='1111 11101011100101001001111010 11'
A='10011100101111110000101011101001'
C='1101 10101110100101011100101010 11'
G='00001110111110110100100001101001'

Let the arbitrarily selected DNA sequence with DNA bases be 'TGCA'; then,

Round 1 key, Key l =T;
Round 2 key, Key 2=G;
Round 3 key, Key 3=C;
Round 4 key, Key 4=A,

b. Message Encryption

Every 128-bit plain text block processes the 4 rounds of encryption. After completion of each round, the coded block further moves through a straight D-Box. The D-Box has four input and output terminals. The input terminals are labelled with DNA bases (A, T, C, and G). The D-Box works on the arbitrarily selected DNA sequence of length four. The encryption algorithm is given below:

Step 1: Read the byte values from the input file and transform each byte value into 8-bit binary representation.
Step 2: Convert 128-bit plain text blocks from the binary representation.
Step 3: Split the 128-bit block into four 32-bit blocks, namely M1, M2, M3, M4.

Round 1:

Temporary variables V11, V12, V13, V14;

$$V14= M4 \oplus Key1 \quad (1)$$

$$V13= M3 \oplus T14 \quad (2)$$

$$V12= M2 \oplus V13 \quad (3)$$

$$V11=M1 \oplus V12 \quad (4)$$

Let the arbitrarily selected DNA sequence be 'TGCA'.

Round 2:

Temporary variables V21, V22, V23, V24;

$$V2l= V11 \oplus Key2 \quad (5)$$

$$V22= VI2 \oplus V2l \quad (6)$$

$$V23= V13 \oplus V22 \quad (7)$$

$$V24= V14 \oplus V23 \quad (8)$$

Let the arbitrarily selected DNA sequence be 'AGTC'.

Round 3:

Temporary variables V3l, V32, V33, V34;

$$V34= V24 \oplus Key3 \quad (9)$$

$$V33= V23 \oplus V34 \quad (10)$$

$$V32= V22 \oplus V33 \quad (11)$$

$$V3l= V21 \oplus V32 \quad (12)$$

Let the arbitrarily selected DNA sequence be 'CGTA'.

Round 4:

Temporary variables V4l, V42, V43, V44;

$$V41= V31 \oplus Key4 \quad (13)$$

$$V42= V32 \oplus V4l \quad (14)$$

$$V43= V33 \oplus V42 \quad (15)$$

$$V44= V34 \oplus V43 \quad (16)$$

Let the arbitrarily selected DNA sequence be 'TACG'.

Step 4: Unite all 32-bit cipher blocks to form 128-bit cipher text block.
Step 5: Repeat steps 3 and 4 for each block of plain text.
Step 6: Club together all the 128-bit cipher text blocks.

After this, a fixed number of bits are to be added, both at the end of the coded message and at two specific positions within the coded message. After inserting extra coding, final form of the cipher text is associated to an altered DNA sequence. In order to form altered DNA coding, 8 characters are arbitrarily selected for making the altered DNA coding and all the 8 characters transformed into 2×4 matrix as follows:

	00	01	10	11
0	F	G	M	L
1	J	H	I	K

Fig.2. Middle Level Cipher Text

The first stage of cipher text in binary coded form is obtained by executing Steps 1-6 from Message Encryption Algorithm as: CT='01000001 01100010 01100100 01110101 01101100' 01110101 01101100'

Then, The final form of primary cipher text has obtained by replacing the three bits with unique character as per Fig. 2. In this sequence, pick three sequential bits from left side in which first bit represent column and remaining two bits represent the row (most significant bits) and so on and replace with corresponding characters mentioned in Table-1. For example, '010' is replaced by 'M', '000' by 'F' and so on as shown in Table 1. It is remembered that CT obtained from previous stage should be multiple of 3 if it does not so, then add extra bit in least significant bits to make it multiple of 3.

Table 1. Character representation corresponding to each 3 bits block

Binary 3 bits block	Corresponding character representation
010	M
000	F
010	M
110	I
001	G
001	G
100	J
100	J
011	L
101	H
010	M
110	I
110	I
011 (append 2 bits extra)	L

Therefore, after mapping all the bits, we obtain preliminary cipher text =' MFMIGGJJLHMIIL'. This preliminary cipher text works as an input for secondary level encryption as shown in Fig. 3.

C. Secondary Level Encryption

The secondary level cipher text is a substitution method to replace 4 characters blocks obtained in the preliminary encryption into sequences of two printable computer symbols.

Each block is replaced with a unique sequence of random characters. In this way, the final cipher text file is obtained after completion of secondary level encryption. The secondary level encryption process of resultant cipher text obtained in the preliminary phase is shown in Fig.3.0

Make 4 characters block.
MFMI GGJJ LHMI IL
(a) Make 4 character form

Assignment of two printable characters to each block
MFMI GGJJ LHMI ILHG (append 2 characters to make 4 character blocks)
@3 %$ &* (&
(b) Assignment of Printable characters

Final Cipher Text
@3%$&*&
(c) Final Cipher Text

Fig.3. Example of secondary level encryption process

To enhance security at secondary level of encryption, we randomly selected 8 distinct alphabet characters shown in Fig. 2 to convert the binary stream to form character. Then, read 4 characters at a time to form a four character block. These four characters as mentioned in Fig. 2 have been obtained by $2^3 \times 2^3 \times 2^3 \times 2^3 = 2^{12}$ (4096) way to form the said block of 4 characters. The constructed block of 4 character is replaced by the unique code of special characters as mentioned in Table 2. In Table 2, there is a unique code corresponding to each 4096 possible combination of 4 character block.

Table 2. Printable Character Database generated during encryption

S. No.	4-character block	Two Printable characters
1	MFMI	@3
2	GGJJ	%$
3	LHMI	&*
4	ILHG	(&
….	….	….
….	….	….

III. Steps Involved in the Proposed Encryption and Decryption Processes

In the proposed model, cipher text is generated after two levels of security applied on the original message. The final cipher text obtained is difficult to understand and therefore it is not easy for intruders to extract meaning of the original message.

The cipher text file through preliminary phase of encryption works as an input for the secondary level technique giving another cipher text file which is more complicated.

A. Experimental Evaluation

For first level of encryption the results are obtained by applying four level of encryption as given in algorithm shown in Fig. 1.

After obtained first level of encryption the input is applied for second level of encryption as demonstrated in Fig. 3. The steps involved during the encryption and decryption processes of the original message are shown under Encryption Process and Decryption Process respectively.

Encryption Process
Step 1: Read plain text from the file and first convert into ASCII code.
Step 2: Convert ASCII code into binary form.
Step 3: Design blocks of 128-bits at a time and apply encryption process on each 128-bits block as described in Preliminary phase.
Step 4: Convert the obtained file into randomly selected 8 characters using Fig. 3.
Step 5: Select four-character block and substitute it randomly with unique two printable character symbols.
Finally, this process generates the final cipher text and a printable character database.

Decryption Process
Step 1: Read two characters at a time from the cipher text and replace these characters into 4 characters alphabets according to Printable Character Database File.
Step 2: Convert each character into 3-bits binary form using Figure 3.
Step 3: Apply preliminary decryption process using the same 128-bit strong key.
Step 4: Convert the obtained binary file into ASCII code. Finally, convert ASCII code to plain text.

Applying second level of encryption the new cipher text is obtained. Therefore, generating a method for the decryption process is quite difficult for intruders because the resulting cipher text is in the form of unreadable, ambiguous text and creates confusion for unauthorized users to extract exact meaning of the original data.

IV. Result Analysis

A particular system may have total 0-255 special characters; however, some of them are printable and others are non-printable characters. In the proposed work, only combinations of printable characters are used so that they can be easily differentiated from each other. Here, we assign the unique value of each possible combination of sequence of two characters $64 \times 64 = 2^6 \times 2^6 = 2^{12}$ (4096) that represents a unique 4-character block. This technique decreases size of the cipher text file up to approximately 33%, in comparison to conventional techniques based on DNA sequences that gives almost double the size of the cipher text. We analyze execution time and cipher text size with the existing algorithms, algorithm proposed by Bibhash Roy et al. [9] and Atanu Majumder at el. [13]. Table 3 demonstrates the results of execution time of proposed encryption and decryption process, memory occupation on different data file sizes.

Table 3. Evaluation of Cipher Size and Execution Time

File Size (MB)	Proposed Technique		
	Cipher size (MB)	Encryption time (ms.)	Decryption time (ms.)
1	1.33	3208	3564
2	2.67	5589	7860
3	4	8000	15537
5	6.65	13138	17731
10	13.3	36969	53295

In order to authenticate the results in terms of execution time, we evaluated and compared our results with traditional work on DNA based techniques. Outcome shows that the planned encryption method is more secure and efficient in comparison with traditional DNA and non DNA based approaches because intruder has to access both Cipher Text file as well as Data Base Text file related to the final cipher text. The proposed method also improves memory utilization as compared to traditional approach (DNA Based and Non DNA Based approaches e.g., BlowFish, DES, 3DES, AES etc.) in which cipher text file size increased by 100% (double of original file size). The behaviour of results during the encryption and decryption process by applying the proposed technique is shown in Fig. 4 a-c.

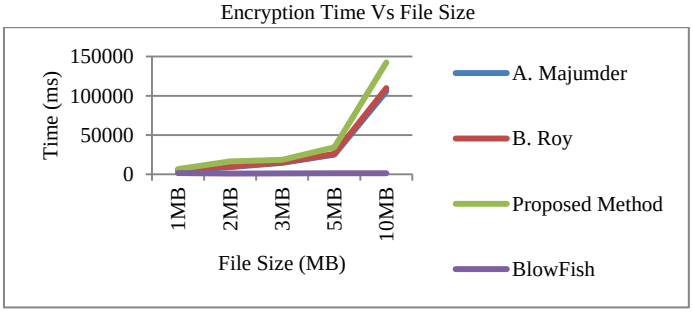

Fig.4a. Execution time analysis on different methods during encryption process

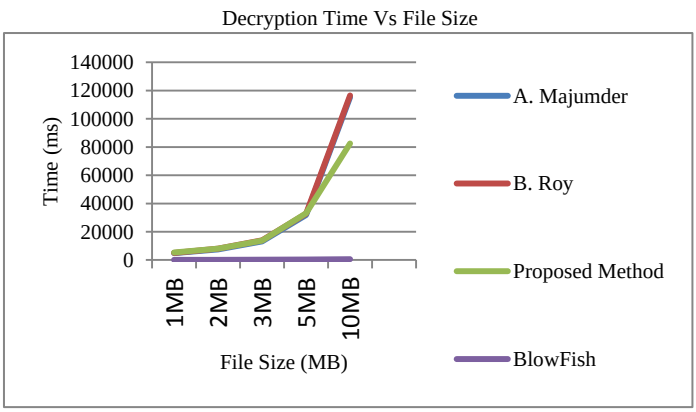

Fig.4b. Execution time analysis on different methods during decryption process

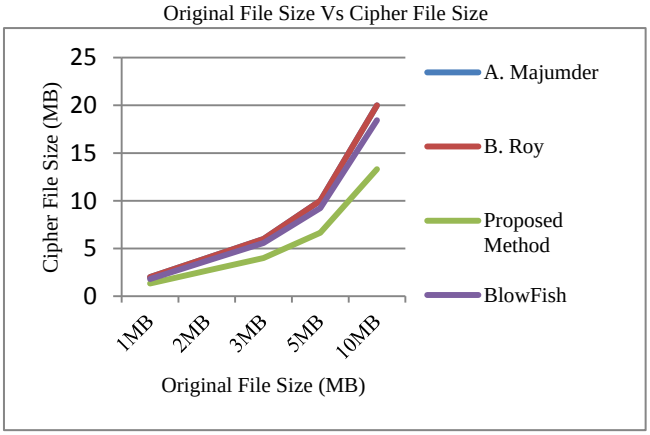

Fig.4c. File size analysis of cipher text for various methods

Table 4. Encryption Execution Time

1	Encryption Execution Time (in milliseconds)			
	A. Majumder	B. Roy	Proposed Method	Blow Fish
1	4637	5568	6553	1539
2	9097	10025	16514	1022
3	14676	15025	18569	1058
5	25051	26027	34387	1289
10	105500	109888	142469	1369

Table 5. Decryption Execution Time

File Size (MB)	Decryption Execution Time (in millisecond)			
	A. Majumder	B. Roy	Proposed Method	Blow Fish
1	4864	5028	5332	81
2	7494	7995	8044	109
3	13122	13925	13720	209
5	31830	32800	33132	357
10	115258	116556	82567	567

Table 4 and Table 5 show execution time during encryption and decryption processes using the proposed algorithms, Atanu Majumder (A. Majumder) [13], Bibhash Roy (B.Roy) [9] and non DNA based Blow fish algorithms, on different file sizes. We also found that encryption time slightly increased in the proposed method, but decryption time decreased for large data size as compared with conventional DNA based algorithms.

Table 6. Original File Size Vs. Cipher File Size

Original File Size (MB)	Cipher File Size (MB)			
	A. Majumder	B. Roy	Proposed Method	Blow Fish
1	2	2	1.33	1.80
2	4	4	2.67	3.70
3	6	6	4	5.58
5	10	10	6.65	9.23
10	20	20	13.3	18.43

V. Conclusion

It is observed from the obtained results that the proposed approach lessens the size of cipher text as compared to traditional methods. Decryption process requires the actual CPT table to obtain the original message; if any changes have been made in the CPT table, it gives incorrect message. Hence, the intruder would have difficulty to guess the actual CPT table that had been generated randomly during the encryption process. Consequently, intruders never get the original message without knowing the exact CPT table.

The proposed algorithm also takes less time to encrypt and decrypt large file size data; as a result, it takes less time for large database as compared to other algorithms. Finally, any DNA based cipher text size can be reduced and made secure by applying secondary level encryption to obtain the cipher text. From the comparative study carried out in Table 6, It is clear from the results that the proposed technique reduces the cipher text file size. The reduction is approximately 33% as compared to conventional techniques.

VI. Limitations & Future Work

We used the proposed approach and found that it enhances security level. A comparative study of cipher size obtained with the proposed technique as well as with the existing techniques is also carried out and demonstrated. The proposed algorithm may further be improved to obtain reduced cipher text with significant smaller encryption time for smaller as well as large file size data.

References

[1] Atul Kahate, “Computer and Network Security”, Third Edition,, 2013.

[2] Kumar, S., Wollinger, T.: Fundamentals of Symmetric Cryptography. Embedded Security in Cars, 125–143 (2006)

[3] Tom St Denis, Cryptography for Developers, Syngress Publishing, Inc., 2007.
[4] S. William, Cryptography and Network Security, 6/E, Pearson, 2013.
[5] W. Diffie, and M. Hellman, New Directions in Cryptography, Proceedings of the AFIPS National Computer Conference, June 1976.
[6] Ashish Gehani, Thomas LaBean and John Reif. DNA-Based Cryptography. DIMACS DNA Based Computers V, American Mathematical Society, 2000.
[7] Ashish Gehani et al , DNA-based cryptography, Lecture Notes in Computer Science, vol.2950, pp.167-188, 2004.
[8] Beenish Anam,Kazi Sakib,Md. Alamgir Hossain,Keshav Dahal, Review on the Advancements of DNA Cryptography arXiv:1010.0186v[cs.CR], 1st Oct 2010.
[9] Bibhash Roy, Gautam Rakshit, Pratim Singha, Atanu Majumder, Debabrata Datta, An improved Symmetric key cryptography with DNA Based strong cipher -ICDeCom-2011, Feb' 24-25'2011, pp.1-5
[10] C.C. Chang, C.C. Lin, C.S. Tseng, W.L. Tai, Reversible hiding in DCTbased compressed images, Information Sciences pp. 177 (2007).
[11] H.W. Tseng, C.P. Hsieh, Prediction-based reversible data hiding, Information Sciences pp. 179 (2009).
[12] Chang CC, Lu TC, Chang YF, Lee RCT "Reversible data hiding schemes for deoxyribonucleic acid (DNA) medium." in Int J Innov Comput Inf Control 3(5) (2007),pp. 1145–1160
[13] Atanu Majumder, Abhishek Majumdar, Tanusree Podder , Nirmalya Kar, Meenakshi Sharmas, Secure Data Communication and Cryptography Based on DNA Based Message Encoding in EEE International Conference on Advanced Communication Control and Computing Technologies 2014, pp.360-363
[14] H. J. Shiu,, K. L. Ng, J. F. Fang, R. C. T. Lee, and C. H. Huang, Data hiding based upon DNA sequences, Elsevier, Information Sciences, vol. 180, pp. 2196-2208, 2010.
[15] Peterson I (2001) Hiding in DNA. Muse: 22.
[16] Zhang Yunpeng, Zhu Yu, Wang Zhong and Richard O.Sinnott, Index-Based Symmetric DNA Encryption Algorithm in International Cong. on Image and Signal Processing, 2011, pp. 2290-2294.
[17] Y. Huang, C. Chang and C. Wu, A DNA-based data hiding technique with low modification rates, Multimedia Tools and Applications. Vol. 70, No. 3, pp. 1439-1451, 2014
[18] Abir Awad and Ali Miri, A New Image Encryption Algorithm Based on a Chaotic DNA Substitution Method in IEEE ICC-Communication and Information Systems Security Symposium, 2012, pp.1011-1015
[19] Sukalyan Som, Atanu Kotal, Ayantika Chatterjee, Soumista Dey, and Sarbani Palit, A Colour Image Encryption Based On DNA Coding and Chaotic Sequences in ICETACS, 2013, pp.108-114
[20] Noorul Hussain Ubaidpur Rahman, Chithralekha Balamurugan, Rajapandian Mariappan A Novel DNA Computing based Encryption and Decryption Algorithm in International Conference on Information and Communication Technologies (ICICT 2014)-2015

Authors' Profiles

Mr. Lalit Mohan Gupta is pursuing PhD. in Computer Science from A.K.T.U, LUCKNOW. He did his M.tech in Software Engineering from Aligarh Muslim University. He is presently working as HOD in Department of Computer Science & Engineering in Vivekananda College of Technology & Management, Aligarh. He has total experience of more than 10 years in the field of academics / administrations. The main research area of Mr. Gupta is Image processing and Security. He has published many research paper in national / international journals / conference of repute.

Dr Hitendra Garg did his PhD (CSE) from Motilal Nehru National Institute of Technology, Allahabad and Masters (Software Systems) from BITS-Pilani. He is presently working as Associate Professor in Department of Computer Science & Engineering. He has total experience of more than 17 years in the field of academics / research. He has more than 20 research papers in the international journals / conference of repute. His research areas are Image Processing, Cryptography, 3D data processing etc

Dr. Samad is working as an Associate Professor in Computer Engineering at University Women's Polytechnic, AMU, Aligarh and having teaching experience of more than 20 years.

He is currently serving as Head of the Section. He completed his Ph.D from Dept. of Computer Engineering, AMU, Aligarh in the year 2010. His research areas include Parallel and Distributed Systems, Algorithm Design, Microprocessor and Parallel System Design. He has supervised PhD as well as M.Tech. Dissertations.

He has contributed and attended various National and International Conferences in India and abroad, and published papers in reputed journals. He has also delivered keynote addresses and invited talks in Conferences and Workshops.

Dr. Samad is a Member of IE (India), IETE and also serving as Honorary Secretary of IETE Aligarh Centre. He is also a member of Curriculum Design Committee of University Polytechnic, JMI, New Delhi.

He sharing various responsibilities in the department and also actively participated in various positions in the University administration, such as Assistant Proctor, Warden of various Halls of residence.

How to cite this paper: Lalit Mohan Gupta, Hitendra Garg, Abdus Samad, "An improved DNA Based Security Model using Reduced Cipher Text Technique", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.7, pp.13-20, 2019. DOI: 10.5815/ijcnis.2019.07.03