Enhanced DNA Cryptographic Solution for Secured Data Transmission

Bahubali Akiwate, Latha Parthiban

Abstract: ***An enhanced technique to generate unique code using DNA sequences that encrypt and decrypt plaintext of characters, text file(.txt,.doc,.docx),image (jpg, jpeg), audio(.mp3) and video(.mp4) using a dynamic DNA key-based cryptography. Cryptography is always considered as secured way for transferring information over insecure channel by achieving confidentiality, privacy and integrity. Since last 10 years traditional cryptography approaches are been replaced with more efficient and effective cryptographic systems like DNA Cryptography. This system takes the DNA sequence as the input and generates a key randomly and is used to decrypt the data without non-integrity of data. This system provides two stages of data security using DNA sequences.***

Index Terms: DNA Cryptography, Encryption, Decryption, DNA Sequences, Confidentiality, DNA Digital Coding

I. INTRODUCTION

Cryptography converts information into encoded format then can be decoded back to original form. It is like handshake mechanism where sender produced encoded format data will be recovered at the receiver side with decoding. Even if information is available in between by other users it is unbreakable.

The more usage of the internet, lots of new technologies, resources are used by several users and organizations and the data load is heavily increasing on networks. It may leads to high probability of data theft, modification and several kinds of attacks both in wired and wireless networks. Obviously there is a need of robust technique addressing all these issues which can then able to provide high storage environment with modern era computing platforms including effective time complexity. The DNA computing is one such new field gaining popularity because of its randomness, high storage capabilities and enhanced security level.

The DNA Cryptography is evolved from biological meaning that four nucleotides such as Adenine, Thymine, Genuine and Cytosine Make DNA (Deoxyribo Nucleic Acid) strand. These four nucleotides with their first letters, we considering as key i.e ATGC to produce DNA sequences at the beginning stage and later it can be used to produce unique code, which is unbreakable[1]. The proposed work can be applicable to electronic data communication with secure fashion, digital transactions such as credit card payments, mobile banking [16].

II. DNA CRYPTOGRAPHY

The DNA cryptography was introduced by L.Adleman in the year 1994.He assumed that DNA has high storage and able to solve complex computational problems such as searching and Hamiltonian path problem. Lipton extended this work by solving NP-complete search problem. During 1995, Boneh et.al presented DNA based approach to break Data Encryption Algorithm (DES).Because of its huge storage capacity and vast parallelism DNA Cryptography evolved as new direction in the field [6]. The research includes genetic code i.e. the information encoded with DNA as genetic material and DNA sequence i.e. the order of nucleotides in the DNA molecule. The proposed enhanced DNA cryptographic technique has the following characteristics:

1. **Confidentiality**: Encoded data should not be deciphered by Unauthenticated/Unauthorized user.
2. **Dynamicity**: The sender and receiver should generate and use new encoding table during peculiar sessions.
3. **Robustness**: Difficult to recover original information.
4. **Randomness**: For every different transaction, different keys are produced and used.
5. This technique may be **unique** and able to support various forms of data.

III. OBJECTIVES

Aiming to enhance the security level this technique has the following objectives:

1. To develop a technique to generate unique code DNA sequence along with traditional techniques such as Diffie-Hellman Key exchange algorithm.
2. To secure the user data and avoiding the leakage of original data over the network.
3. To avoid illegal access of data from unauthorized users.
4. Providing better security with reduced storage and time complexities.

IV. SYSTEM REQUIREMENTS

To develop proposed approach, we need following requirements:

1. **Software Requirements:** Net Beans IDE, JDK 7.0 and above, Java Code.
2. **Hardware Requirements:** Windows XP and above system, Minimum 2GB RAM, Minimum 160 GB Hard Disk Drive.

Revised Manuscript Received on July 05, 2019.

Bahubali Akiwate, Computer Science, KLECET, Chikodi, India.
Dr.Latha Parthiban, Computer Science, Pondicherry University, Pondicherry, India.

3. **Functional Requirements:** User's Selection of file, pressing of encryption and decryptions buttons, sending encrypted file over network.
4. **Non-Functional Requirements:**
   i. **High performance:** The system should encode/decode information with reduced storage requirement.
   ii. **Reduced delay:** Sending of encrypted files over a network with minimum delay covering encryption and decryption processes.
   iii. **Reliable and secure.**
   iv. **User friendly** system interface.

V. SYSTEM DESIGN

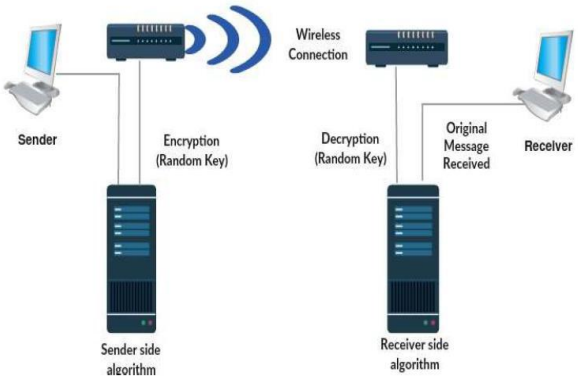


Fig.1 Transmission of data between sender and receiver

The above Fig.1 describes the transmission of data between the sender and receiver. The data that has to be transferred should be compulsorily encrypted and there should be random key generation take place. Later encrypted data and random key were passed over wireless network. The encrypted data must be decoded at the receiver side by using the received random key to make data more secure and should be visible at the intended receiver end only. Both the processes use DNA digital coding. The following steps show step by step process of its working:

1. First we consider the contents of data to be transmitted in wireless network; the data may be text, image, audio, video or gif files.
2. Next, it is necessary to encrypt the data that has to be transferred and generating random key while transmission.
3. A peculiar key generation algorithm/program is to be used for key generation. This key plays major role either at the stage of encryption or decryption. The main advantage of this key is it's a private by console, i.e., the key is never visible until end process.
4. In the next phase the decryption of encrypted data takes place at the receiver side. To see the original data that has been encrypted using key, the receiver needs to enter the decryption key to decrypt the encrypted data that is received from sender.
5. Now the data has been decrypted, the receiver gets the original information that has been transmitted from the sender.

A. Use Case Diagram

The following Fig. 2 shows the use case diagram, in which the original message selected by user. Later, start of encryption process, DNA digital coding can be used to encode the message. After the encryption the random key is generated, and cipher text is transmitted. In decryption process, the amplified message is received. Later, start of decryption process, using DNA digital coding and entering the randomly generated key to get the original message.

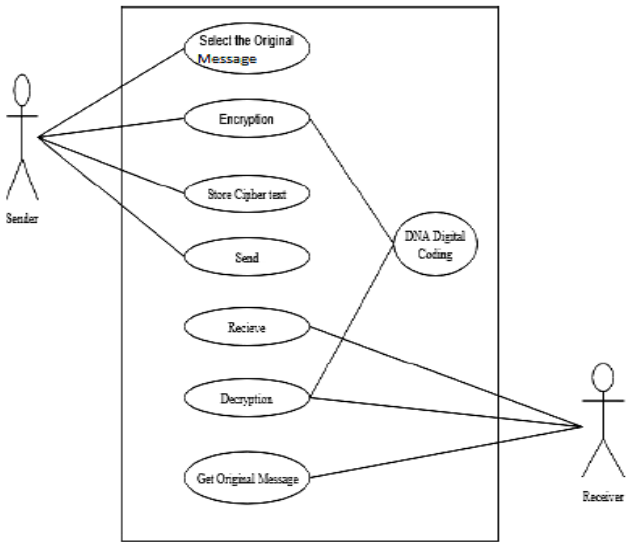


Fig.2 Use Case Diagram

B. Sequence Diagram

The following Fig.3 shows the sequence diagram of proposed approach which illustrates how the communication happens between sender and receiver [16].

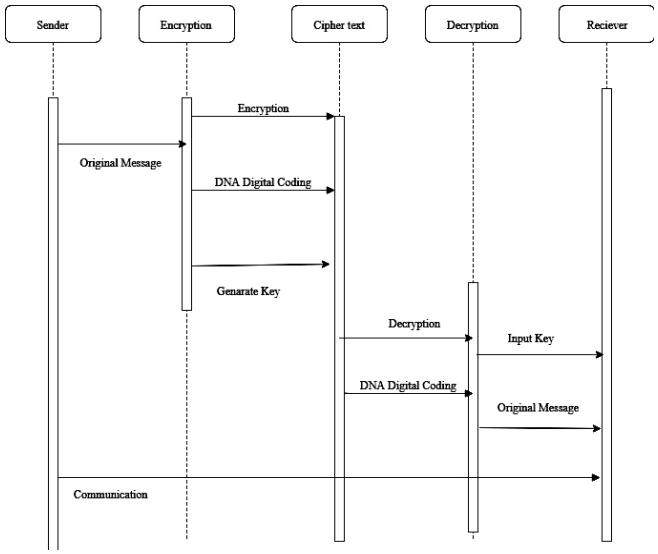


Fig.3 Sequence Diagram

VI. IMPLEMENTATION

Securing data network, the implementation over DNA cryptography is implemented through following modules.

1. Encryption Module
2. Decryption Module

Encryption Module

The following Fig. 4 shows the encryption process, in which the original message is converted to the ASCII character then converted into hexadecimal after that it converted it into binary format. By using DNA Digital coding shown in table 1 and Key Combinations shown in table 2, Ciphertext message will be generated [1].

Fig.4 Encryption Process

Decryption Module

The following Fig.5 shows the decryption process which is almost reverse process as that of encryption process.

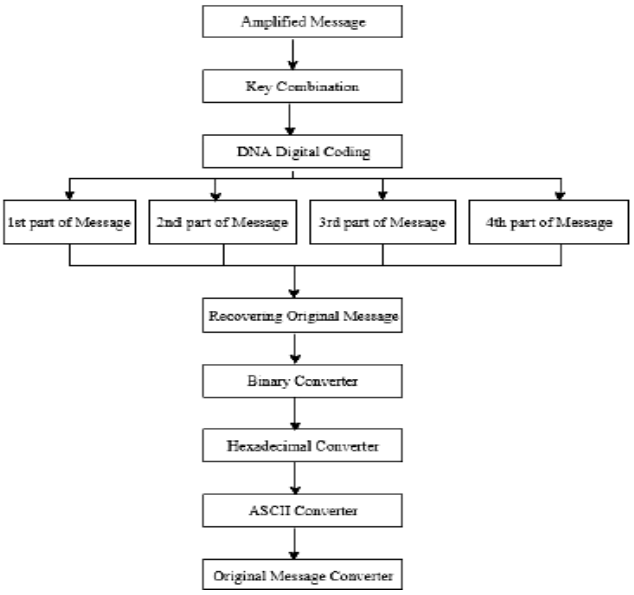


Fig.5 Decryption Process

The following table 1 shows DNA digital coding, where four codes namely A,T,G,C are assigned with binary values 00,01,10,11 respectively [17].

Table 1. DNA Digital Coding

Binary Value	DNA Digital Coding
00	A
01	T
10	G
11	C

Table 2. Key Combinations

Key Combinations	Patterns	Values
AA	0101	5
AT	0011	3
AG	0001	1
AC	0010	2
TA	0110	6
TT	1111	15
TG	0111	7
TC	1001	9
GA	1010	10
GT	0100	4
GG	1000	8
GC	1100	12
CA	1110	14
CT	1011	11
CG	0000	0
CC	1101	13

The above table 2 shows key combinations with their pattern values [1].

To understand the scenario of Encryption and Decryption process flow chart we consider one example. In this the example for plaintext is “Engineering”. Performing encryption and decryption operation yields the following :

Encryption Process

Plaintext: Engineering

We can convert the plaintext into ASCII format to get the cipher text.

ASCII:

691101031051101011011 4105110103

After that we need to convert ASCII value into the hexadecimal format.

Hexadecimal value:

456E67696E656572696E67

The hexadecimal value is converted into the binary form by using the key combination.

Binary value:

1000101110111011001111101001110111011001011100101 1110010110100111011101100111

After that we need to refer the DNA digital coding table.

DNA Digital coding:

From Table 2 we can write

GAGUCTCPCACUCTAUCTCPCAGUCAGUCGTPCTAU CTCPCACU

Now from table 2, by using the DNA digital coding we get the amplified message the DNA digital coding is convert to the key combination.

Amplified Message:

1010101101111011101111011001101111011101011110101 0000010101100110111101110111

Decryption Process

Now at the receiver side, the receiver receives the amplified message and the unique key for decryption.

Amplified Message:

1010101101111011101111011001101111011101011110101 0000010101100110111101110111

After receiving, the amplified message is converting into the DNA digital code using DNA digital coding table to retrieve original message.

DNA Digital coding:

GAGUCTCPCACUCTAUCTCPCAGUCAGUCGTPCTAU CTCPCACU

From the key combination table we can convert the DNA code into the binary form. For example TT is converted into 0101.

Binary value:

1000101110111011001111101001110111011001011100101 1110010110100111011101100111

After the binary representation the data is converted into the hexadecimal format. For example 0101 is converted into 5 in the hexadecimal format.

Hexadecimal value:

456E67696E656572696E67

The hexadecimal value is converting into the ASCII format to get original message.

ASCII: 691101031051101011011141051101 03

From the ASCII value receiver will get the original message.

Plaintext: Engineering

VII. RESULTS

During the execution, certain computations were derived and for these calculations specific analysis were made which are discussed below.

The table 11.1 shows the time taken to encrypt and decrypt the various file types and different sizes. It measures the time in terms of milliseconds.

Table 3. Encryption and decryption time required for various file types

Input Type	Size on Disk	Time Taken for Encryption (ms)	Time Taken for Decryption (ms)
Text	10KB	3564.5	2314.85
Image	2.5MB	12819.337	3441.589
Audio	10MB	10992.95	3502.510
Video	15MB	21680.316	2659.88

Below Fig .6 illustrates the graphical representation for the derived computations.

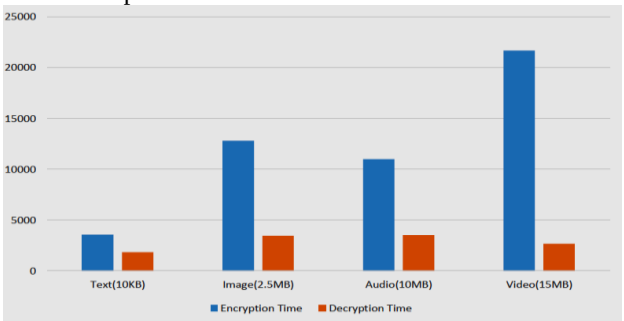


Fig.6 Representing table 3 in graphical format

The figure 6 shows the comparison between times that are taken for encryption and decryption processes for different file types and different file sizes. In that X-axis represents different types of files along with their sizes and Y-axis represents the time in terms of milliseconds. From the above table we conclude that the decryption process takes less time compared to encryption process.

The table 4 shown below represents the different file sizes of original, encrypted and decrypted files.

Table 4. Encryption and decryption of different file sizes (in bytes) for various file

Input	Original file size	Encrypted file size	Decrypted file size
Text	10240	10112	10239
Image	1366365	1366368	1366365
Audio	10810458	10810464	10810454
Video	16215828	16215832	16215827

The below Fig.7 shows the comparison between the file size of original file, encrypted file and decrypted file. These entire file sizes are mentioned in terms of bytes. In this graph X-axis represents the different file types and Y-axis represents the file size in bytes. The original file, encrypted file and decrypted files are represented in different colors as shown in the below figure.

From the table 4, we conclude that the encrypted file size is very few bytes larger compared to the original file size and the decrypted file size is comparatively similar size as the original file size for all the different types of files.

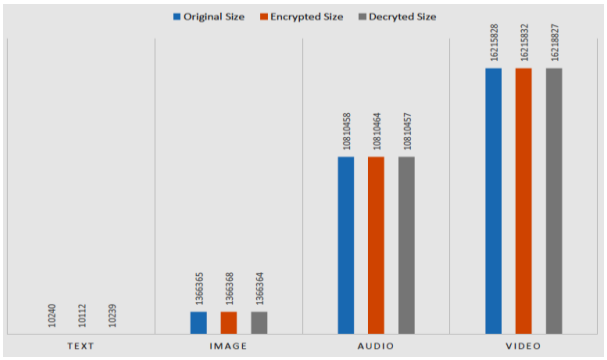


Fig.7 Representing table 4 in graphical format

VIII. ADVANTAGES AND DISADVANTAGES

The following are the advantages and disadvantages of the proposed work.

Advantages

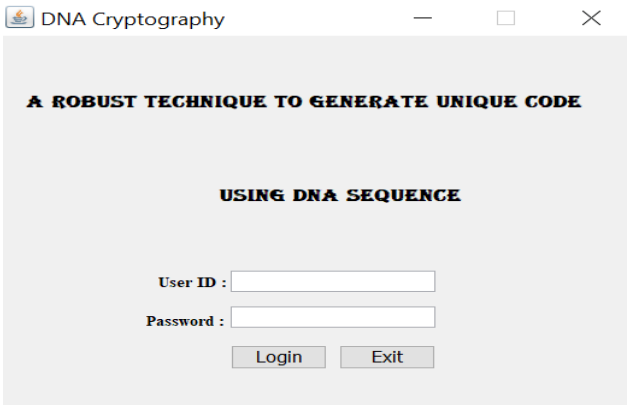
1. The data transfer takes place more securely.
2. There is a minute and immeasurable difference in variation of size of original file and decryption file which reduces storage complexity.
3. The time taken to transfer the secured data over a network is very less, which again reduces its time complexity.
4. Data transfer takes place wirelessly over two nodes reliably.
5. Transmission of files with larger size can be done with least complexity issues.

Disadvantages

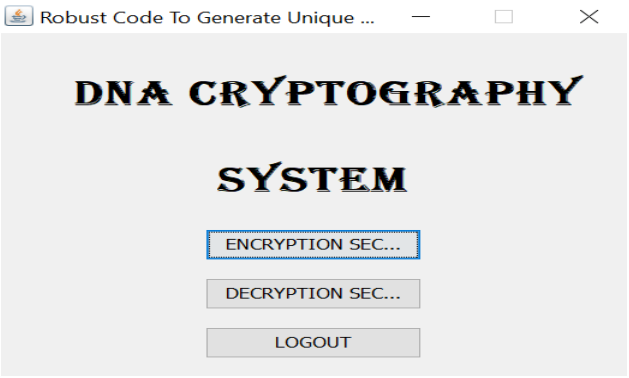
1. Sometimes system may show error while transferring very large files.
2. Connection may seem difficult over multiple nodes.

IX. SNAPSHOTS

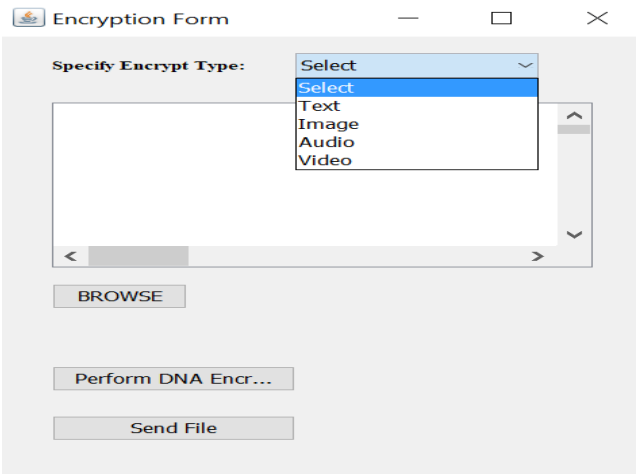
After implementing this work, these were the results that were observed.



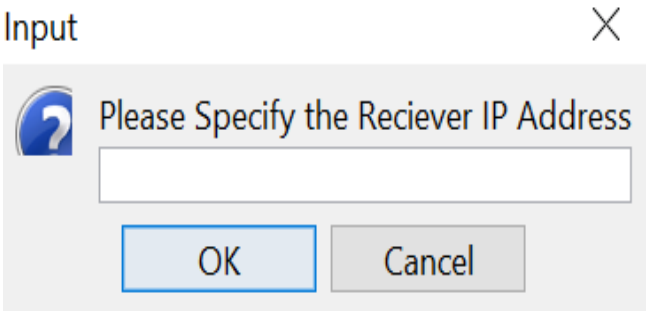
Snapshot 1: Describes the login page of the user, before performing the other operations, first user need to login into the system



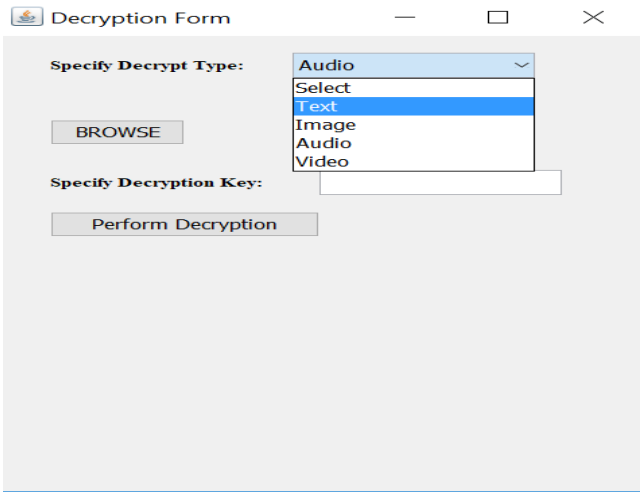
Snapshot 2: Describes the three different sections namely, encryption section, decryption section and logout. Based on the requirement of the sender and receiver they can select the particular section



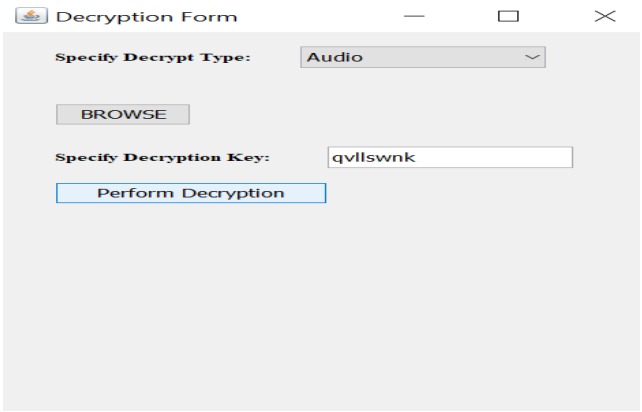
Snapshot 3: Indicates the encryption form, where sender needs to specify the encryption type. Once they select the type of the data, they can browse the file and then perform the encryption process



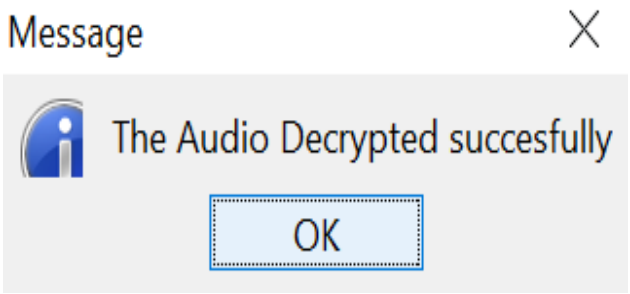
Snapshot 4: Indicates the input value which means the sender need to enter the IP address of the receiver's system to send the files



Snapshot 5: Indicates the decryption form. Here receiver needs to select the type of the file to decrypt the encrypted data and also needs to browse the encrypted file



Snapshot 6: Indicates the decryption form. Here receiver needs to enter the decryption key to perform the decryption process



Snapshot 7: Indicates the message which will appear after the successful decryption of the encrypted file

X. CONCLUSION

We proposed and implemented robust technique to generate unique code using DNA sequences, it implies that the user provide information security while on private communication on public network. In DNA cryptography user is able to send text, long text file, images, audio files, video files and GIF files. After encryption the random key is generated and it can be sent to the receiver. Later, the receiver receives the cipher text and enters the key to get the original data securely. The entire proposed algorithm has various complex procedures to get the original message from the encrypted file. So, any intruder who receives the intermediate message will never be able to retrieve the original message as intended by the sender. Message encryption using DNA sequence is a very new technique, still evolving and tried out for secure transmission and reception of hided messages. The method is deemed to be so secure that it would be very difficult for any intruder to break the encrypted message and retrieve the actual message. Only the intended receiver can decrypt and receive the original message.

REFERENCES

1. Prajapati Ashishkumar B and Prajapati Barkha, "Implementation Of DNA Cryptography In Cloud Computing and Using Socket Programming", IEEE, January 2016.
2. Naveen Jarold, P Karthigaikumar, N M Sivamangai, Sandhya R, Sruthi B Ashok, "Hardware Implementation of DNA based Cryptography", Conference on Information and Communication Technologies, IEEE,pp. 696-700,2013.
3. M R Saranya, Arun K Mohan and K.Anusudha, "Algorithm for Enhanced Image Security Using DNA and Genetic Algorithm", IEEE, April 2015.
4. Ajit Singh and Reena Singh, "Information Hiding Techniques Based on DNA Inconsistency: An Overview", IEEE, May 2015.
5. Deepak Singh Chouhan, R.P.Mahajan, "An Architectural Framework for Encryption & Generation of Digital Signature Using DNA Cryptography", IEEE, pp. 743-748, June 2014.
6. Tushar Mandge and Vijay Choudhary, "A DNA Encryption Technique
7. Based on Matrix Manipulation and Secure key Generation Scheme", IEEE, 2013.
8. Anchal Jain, "Adaptive Key Length Based Encryption Algorithm using DNA Approach", IEEE , 2013.
9. Zhang Yunpeng, Zhu Yu, Wang Zhong and Richard O.Sinnott, "Index-Based Symmetric DNA Encryption Algorithm" , IEEE,pp. 2290-2294, 2011.
10. G. Cui, L. Qin , Y. Wang , X. Zhang, "An Encryption Scheme Using DNA Technology", IEEE, 2008.
11. Hamza Hammami, Hanen Brahmi, Sadok Ben Yahia "Secured Outsourcing Towards a Cloud Computing Environment Based on DNA Cryptography", IEEE page no. 31-36,2018
12. S.V.Keerthana Priya, S.J.Saritha , "A Robust Technique to Generate Unique Code DNA Sequence", IEEE, page no.3815-3820,2017
13. Mona Sabry, Mohamed Hashem, Taymoor Nazmy, Mohamed Essam Khalifa , "Design of DNA-based Advanced Encryption Standard (AES)",IEEE, pp. 390-397,2015.
14. Deepak Kumar and Shailendra Singh ,"Secret Data Writing Using DNA Sequences", IEEE,pp. 402-405,2011.
15. Aqeel ur Rehman, "Block mode image encryption technique using two-fold operations based on chaos, MD5 and DNA rules", part of Springer Nature 2018.
16. Vikas Sagar and Krishan Kumar, "A Symmetric Key Cryptography using Genetic Algorithm and Error Back Propagation Network", IEEE, pp. 1396-1391,2015.
17. Bahubali Akiwate, Latha Parthiban, "A Dynamic DNA for Key-based Cryptography"- Accepted for publication, CTEMS, IEEE, 2018 to be published.
18. Ashish Prajapati, Amit Rathod, "Enhancing security in cloud computing using Bi-Directional DNA Encryption Algorithm", International Conference on Intelligent Computing, Communication & Devices. (ICCD-2014), Springer.
19. Hatem M. Bahig, Dieaa I. Nassr, "DNA-Based AES with Silent Mutations", Arabian Journal for Science and Engineering (2019) 44:3389–3403 (Springer).

AUTHORS PROFILE

Mr. Bahubali Akiwate received a Bachelor of Engineering degree in Computer Science and Engineering from Bahubali College of Engineering, Shravanabelagola, affiliated to VTU, Belagavi, during the year 2009. He completed M.Tech Degree in Digital Communication and Networking from Gogte Institute of Technology, Belagavi, from the same University during the year 2011. He is working as an Assistant Professor in Computer Science and Engineering Department of K. L. E. College of Engineering and Technology, Chikodi since from September-2011.Currently he is doing research in VTU-RRC, Belagavi, since 2014.

Dr. Latha Parthiban received a Bachelor of Engineering degree in Electronics and Communication from Madras University during the year 1994.She completed M.E degree in Computer Science and Engineering from Anna University during the year 2008.She completed Ph.D Degree from Pondicherry University during the year 2010.Currently she is working as Assistant Professor in Computer Science and engineering department in Pondicherry University, since 2012.