iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XII **Month of publication:** December 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 5 Issue XII December 2017- Available at www.ijraset.com

Telemedicine Cryptography using DNA Sequence

Ruby Chandrakar[1], Suman Kumar Swarnkar[2]
[1,2]*Bharti College of Engineering Technology,Durg*

Abstract: ***Today innovative methods of Data hiding are the most evolving platforms with new applications, authentications, protocols etc. Hiding secret data in deoxyribo nucleic acid is one such important and interesting research topic. The secret data in transcribed deoxyribo nucleic acid, translated ribo nucleic acid regions, or active coding segments where it doesn't mention to modify the original sequence, but others hide data in non-transcribed deoxyribo nucleic acid, non-translated ribo nucleic acid regions, or active coding segments. However the techniques to embed the secret data into the deoxyribo nucleic acid sequence without altering the functionalities is searched upon as sometimes schemes either alter the functionalities or modify the original deoxyribo nucleic acid sequences. This paper is a general study of DNA cryptography, its techniques, applications and result.***
Keywords: Security, steganography, DNA, and RCM

I. INTRODUCTION

Steganography schemes hide the key message thus it cannot be determined. The product of this scheme not solely purposeful however conjointly is also identical. Totally different ways of steganographic techniques were used from the earlier period. Nowadays, biology techniques become a lot wider, and that they area unit applied to several varieties of applications, authentication protocols, organic chemistry, cryptography and then on. One in all the foremost recently used biology techniques is Deoxyribo macromolecule (DNA). Deoxyribonucleic acid primarily based steganographic techniques were used. deoxyribonucleic acid has several characteristics that build it an ideal steganographic media. These techniques rely upon the high randomness of the deoxyribonucleic acid to cover any message while not being detected. During this scheme, secret message area unit hidden in a very deoxyribonucleic acid sequence in order that the hidden knowledge won't be detected. Moreover, the host deoxyribonucleic acid sequence is reconstructed once the reverse operation, which way differs from the previous schemes conjointly supported deoxyribonucleic acid. This property does not solely ensure the safety of the key knowledge however conjointly preserves the practicality of the initial deoxyribonucleic acid.

II. RELATED THEORY

DNA is 2 twisted strands composed of 4 bases, adenine (A), cytosine (C), thymine (T) and guanine (G). The four bases represent the genetic code. (A) bonds with the complementary (T), (G) bonds with the Complementary (C), and the other way around. so one strand and therefore the corresponding complementary strand represent polymer [17]. for instance, one strand is AACGTC, and therefore the different should be TTGCAG as shown in Figure one. The polymer sequence determines the arrangement of amino acids that type a macromolecule. Transcription is that the method to form RNA, AN mediator copy of the directions contained in polymer. RNA could be a single strand and contains nucleotide nucleotide (U), wherever thymine (T) would seem in polymer. For clarity, the four bases in RNA square measure adenine (A), C (C), nucleotide (U) and guanine (G)

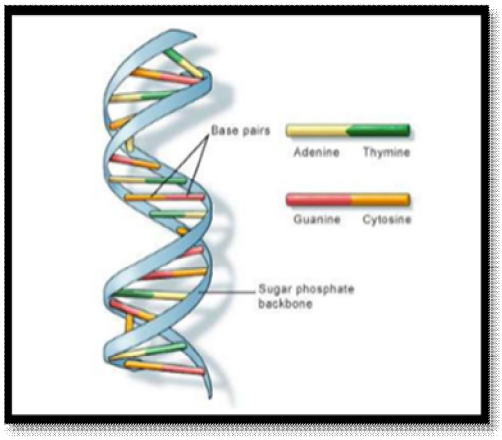


Figure 1. The structure of part of a DNA double helix.

III. LITERATURE SURVEY

In 2003, Jie chen [2] planned deoxyribonucleic acid cryptanalytic algorithmic program on carbon nano-tube and deoxyribonucleic acid based mostly system. deoxyribonucleic acid based mostly cryptosystems area unit accustomed convert message into segments. One-time-pad is employed code book to convert plain text into cipher text. Code book ought to be random and should be distinctive. Jie chen presenting a deoxyribonucleic acid coding and cryptography pictures bio-molecular methodology supported planned algorithmic program.

In 2004, Sabari Pramanik1 et al. [3] bestowed cryptography methodologies victimization deoxyribonucleic acid crossing and deoxyribonucleic acid digital writing, just the once pad, that minimize time quality. deoxyribonucleic acid technologies need large computing time, high procedure quality and extensively laboratory depended. They used parallel technique to rewrite the message in less time.

In 2011, Deepak Kumar et al. [10] conferred secret knowledge writing using deoxyribonucleic acid sequence. They centered on deoxyribonucleic acid computing, deoxyribonucleic acid sequence, that have massive storage capability, extraordinary data density. Author gift coding and cryptography algorithmic program supported just the once pad technique through that one will secure our knowledge in deoxyribonucleic acid sequence. Steganogaphy is employed in this paper to cover message in double strand deoxyribonucleic acid sequence microdots. Author designed knowledge concealment algorithmic program by using deoxyribonucleic acid sequence and ancient cryptography. This algorithmic program is simple to use and economical.

In 2012, Yunpeng Zhang et al. [12] planned deoxyribonucleic acid cryptanalytic approach supported deoxyribonucleic acid digital writing and deoxyribonucleic acid fragment assembly. they supply high security analysis and prove that the algorithmic program has high confidential strength. during this paper author style bilateral coding algorithmic program victimization deoxyribonucleic acid technology.DNA technology has distinctive benefits than ancient cryptography. it's low energy consumption and high storage capability.

In 2013, Wang Zhong et al. [13] planned a replacement index based mostly bilateral algorithmic program. This algorithmic program encrypts plain text victimization block cipher and index of string. algorithmic program converts every character into American Standard Code for Information Interchange code and in keeping with the nucleotide sequence convert into deoxyribonucleic acid sequence. This algorithmic program stores position as a cipher text. The researchers ought to prove potency and time quality of this algorithmic program through simulation and theoretical analysis.

IV. METHODOLOGY

Security is that the main concern of any style of communication. In secure communication aim is to boost the safety of information being changed between a pair of parties, say A and B. It is accomplished mistreatment many strategies. Cryptography or steganography is wont to improve the safety. Steganography even hides the presence of a message. polymer primarily based steganography is that the act of mistreatment steganography at the side of deoxyribonucleic acid encoding. it's the advantage of accelerating the randomness of message so it can not be extracted simply by a 3rd party. Cryptography provides a variety of options for data security. the most aspects treated by cryptography are: confidentiality, information integrity, authentication, and non repudiation. The objectives of this thesis were to target the confidentiality half and to search out new strategies (ciphers) to make sure privacy through the utilization of DNA

V. THE AES CIPHER

AES, is a symmetric block cipher. This means that it uses the same key for both encryption and decryption .However, AES is quite different form DES in a numberous ways. The algorithm Randel allow for a variety of block and key can and not just the 64 and 56 bits of DES, block and key size. The block and key can in fact be chosen independently form 128,160 192, 224,256 bits and need not be the same. However, the AES standard states that the algorithm can only accept a block size of 128 bits and choice of three key-128,192,256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192, and AES-256 respectively. As well as these different AES differs from DES in that it not a festal structure. Recall that in a festal structure, half of the data block is used to modify the other half of the data block and then the halves are swapped. In this case the entire data block is processed in parallel during each round the using substitutions and permutations. A number of AES parameter depend on the key length. For example if the key size used is 128 then number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. Present the most common key size likely to be used is the128 bits Key. This description of the AES algorithm therefore describes this particular implementation.

Randel was designed to have the following characteristics;

A. Resistance against all known attacks.
B. Speed and code compactness on a wide of platform.
C. Design simplicity

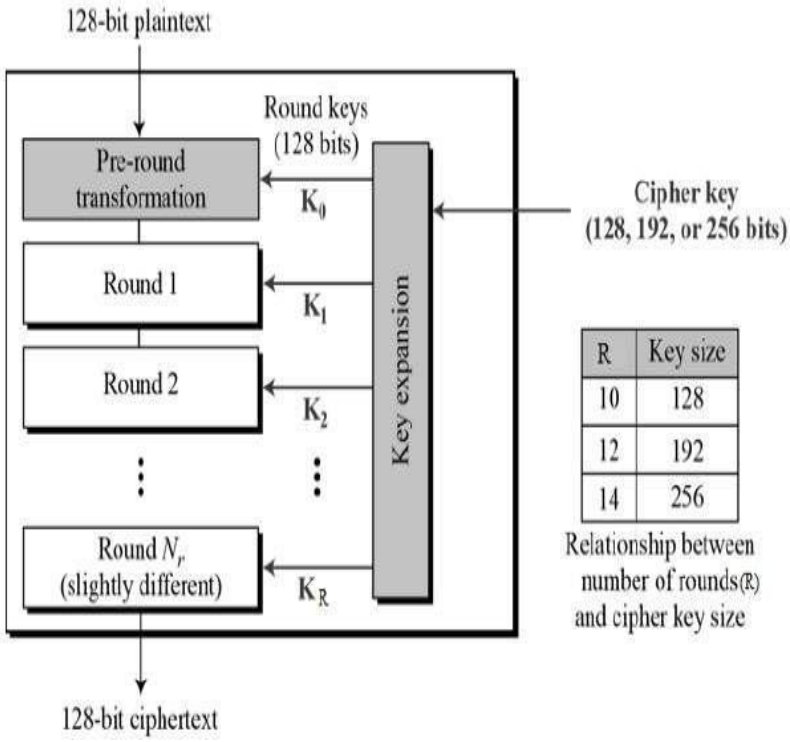


Fig 2 AES, algorithms

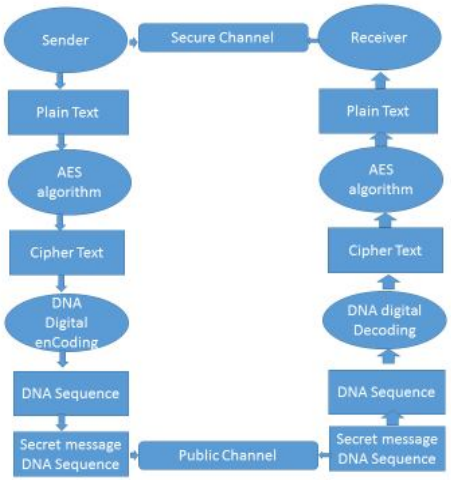


Fig 3 Flow chart of AES

VI. DATA HIDING SCHEME

The planned scheme adopts the reversible distinction mapping technique to cover the key message during a deoxyribonucleic acid sequence, severally. deoxyribonucleic acid sequence consists of 4 nucleotides A, C, G, and T. Hence, we want to remodel the illustration format of the nucleotides such the concealment techniques will be wont to conceal the key message during a deoxyribonucleic acid sequence. First, every nucleotide image of the deoxyribonucleic acid sequence is regenerate into a binary string. A convenient strategy is to encrypt every ester with 2 bits in alphabetical order.

The watermark substitutes the LSBs of the remodeled pairs of values. At detection, so as to extract the watermark and to revive the first values, every remodeled try ought to be properly known. The LSB of the primary price of every try is employed to point if a try was remodeled or not "1" for remodeled pairs and "0" otherwise.

The detail of the hiding procedure is illustrated in Figure 4

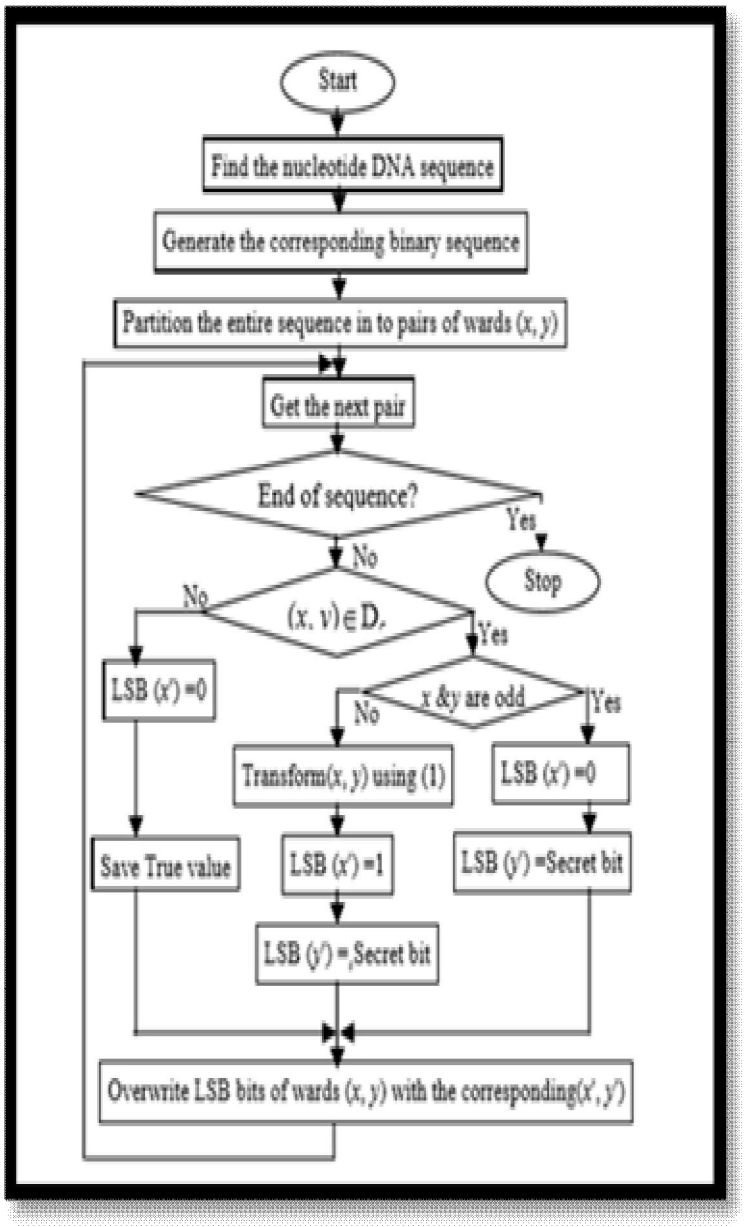


Figure 4 Flowchart of hiding scheme

VII. ENCRYPTION KEY EXCHANGE SCHEME

Algorithm planned algorithmic rule relies o symmetrical Key Exchange and XOR operation technique, that encrypts plain text message into polymer cipher text. To avoid attainable attacks on cipher text by intruders changed message area unit checked at the receiver side. 2 parties concerned in communication area unit sender and receiver. Sender encrypts the plain text using symmetrical key into polymer sequence and sends through insecure channels like web.

Sender→ E(Kdna,, P)= Cdna.

Receiver decrypts the cipher text into plain text using deoxyribonucleic acid key sequence.

Receiver→ D(Cdna, Kdna,,)= P

Flow chart for Encryption and Decryption techniques is shown in Fig 5

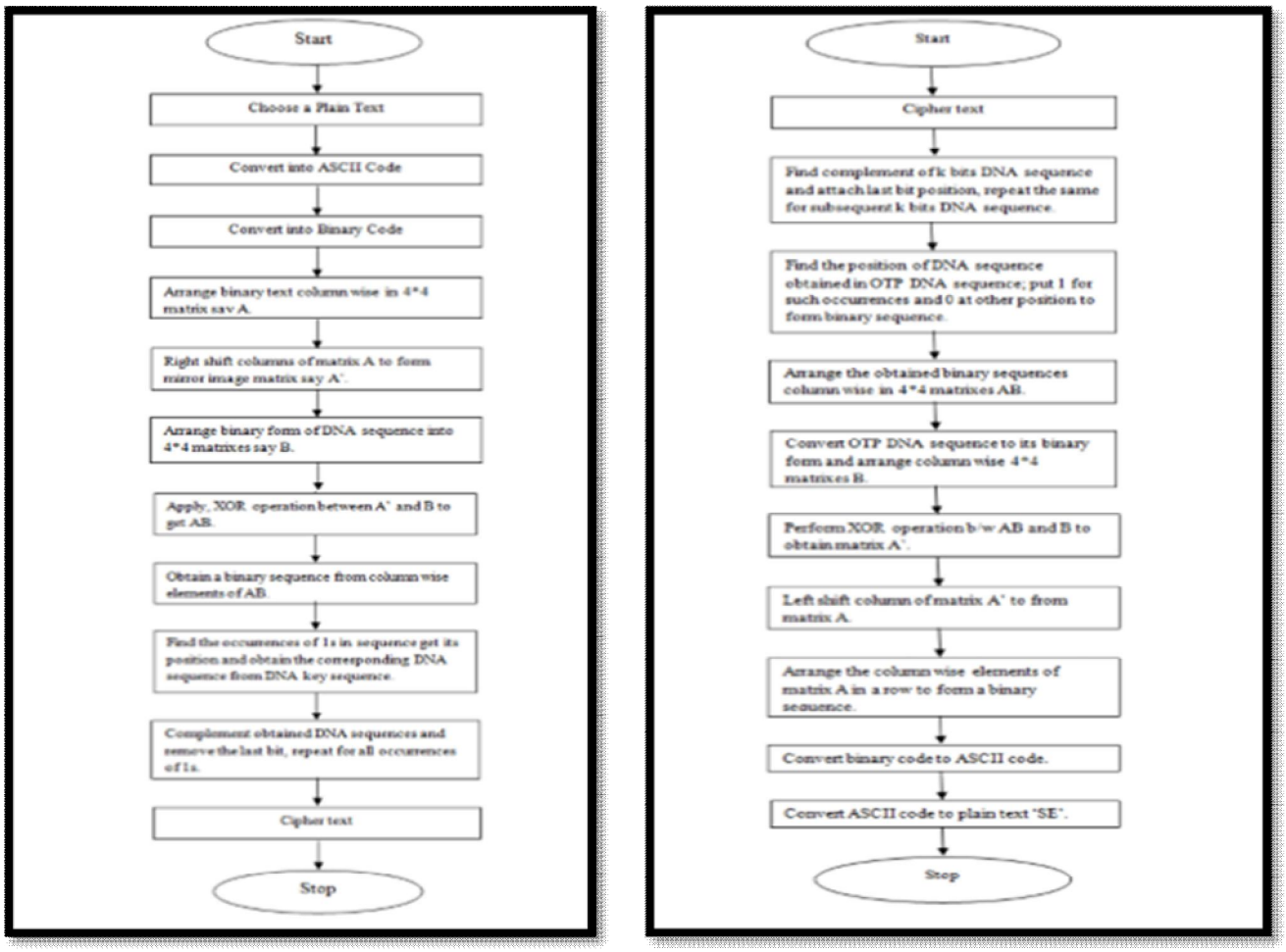


Figure 5 - Flow chart for Encryption and Decryption techniques

VIII. DNA COMPUTING

DNA is that the major data storage molecule in living cells, and billions of years of evolution have tested and refined each this wonderful data molecule and extremely specific enzymes which will either duplicate the data in deoxyribonucleic acid molecules or transmit this information to alternative deoxyribonucleic acid molecules rather than using electrical impulses to represent bits of data, the deoxyribonucleic acid laptop uses the chemical properties of those molecules by examining the patterns of combination or growth of the molecules or strings. Deoxyribonucleic acid will try this through the manufacture of enzymes, that area unit biological catalysts that might be referred to as the 'software', accustomed execute the specified calculation. A deoxyribonucleic acid computer, because the name implies, uses deoxyribonucleic acid strands to store data and taps the recombinative properties of deoxyribonucleic acid to per-form operations a little tube of deoxyribonucleic acid strands suspended during a answer might yield millions to billions of synchronous interactions at speeds — in theory — quicker than today's quickest supercomputers. Deoxyribonucleic acid computer uses the recombinative property of deoxyribonucleic acid to perform operations. The main good thing about using deoxyribonucleic acid computers to resolve advanced issues is that completely different potential solutions are created all right away. This can be called parallel processing. Humans and most electronic computers decide to solve the matter one method at a time (linear processing). Deoxyribonucleic acid itself provides the additional advantages of being an inexpensive, energy-efficient resource. During a completely different perspective, over ten trillion deoxyribonucleic acid molecules will work into a district no larger than one cc. With this, a deoxyribonucleic acid laptop might hold ten terabytes of information and perform ten trillion calculations at a time. During a ancient computer, information are drawn by and keep as strings of zeros and ones. With a deoxyribonucleic acid computer, a sequence of its four basic nucleotides — A, cytosine, guanine, and pyrimidine — is employed to represent and store information on a strand of deoxyribonucleic acid. Calculations during a traditional computer are performed by

moving information into a process unit wherever binary operations area unit performed. Primarily, the operations flip miniaturized circuits off or on admire the zeros and ones that represent the string of information

IX. RESULTS

We enforced a replacement DNA coding scheme supported on symmetrical key exchange, mathematical operation and XOR technique. Any message is regenerate in DNA sequence. DNA sequence hold on massive message in compact volume. during this paper, a replacement cryptography technique is planned using symmetrical Key Exchange, one-time pad theme and DNA hybridisation to reduce the time quality. Matrix kind operations cut back time quality of coding and secret writing. DNA cryptography will be combined with ancient cryptography to supply hybrid security. therefore there's plenty of scope for future works during this space. completely different ancient cryptography techniques combined with DNA cryptography could result in higher hybridisation. the employment of upper dimension matrices for coding and secret writing will additionally minimize the time quality and thus will be thought of as future scope of this work . Experiments were applied to guage the performance of the projected scheme. The projected scheme was tested on a 797 megahertz central processor. laptop computer with 256 RAMS. The system uses the Visual C++ perform random ( ) to come up with pseudo-random numbers and a secret message.

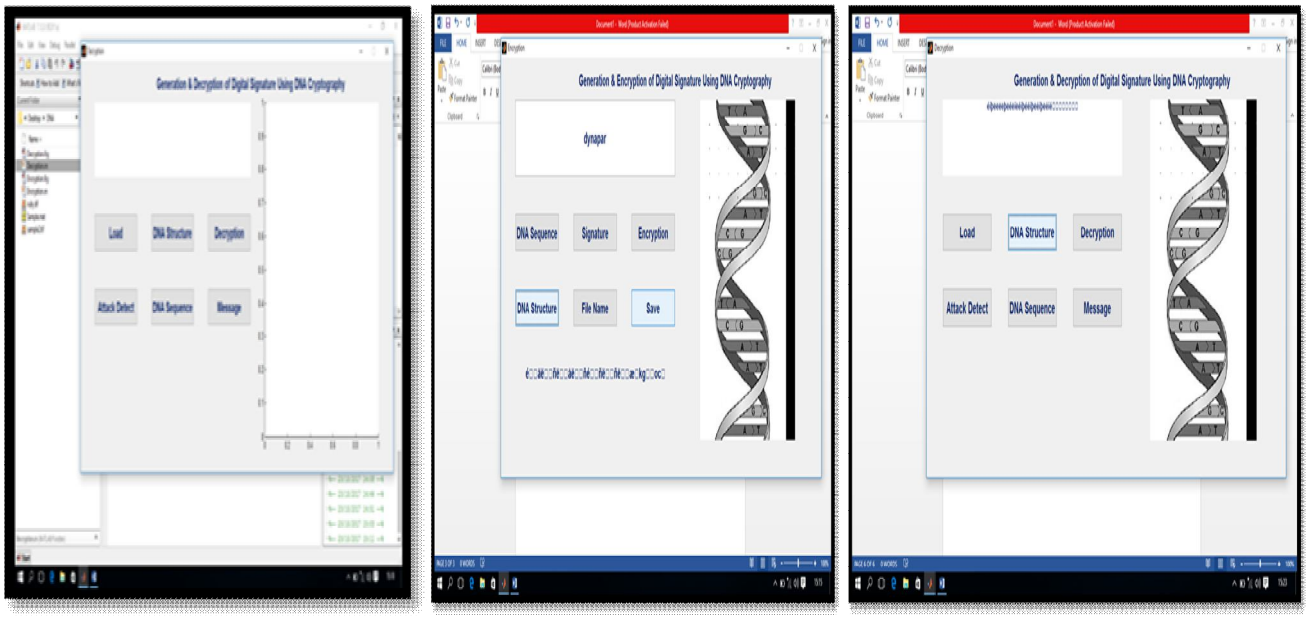


Figure 6 – Output DNA

X. ANALYSIS

The proposed procedures are implemented in MATLAB for its platform independence property and available in-built cryptography functionalities. The procedures are implemented successfully to specified sized input plain texts. Initially, there were constraints for large files such as image where the required primary memory of the system could create a problem in the execution and conversion of plain text into cipher text. But later on that problem are also resolved by extracting the byte code values of the compressed file of input plaintext and then dividing the compressed file into fixed sized chunks and then performing all the procedures of encoding and decoding by joining the chunked sub files. This algorithm is applicable for all most all documents. The results of generation of cipher text after encrypting the plaintext on few data sets are given below:

Dataset	Length of plain text bits	Encryption time (ms)	Decryption times(ms)	RSA algoritms
Test1	112	16	12	256
Test2	226	12	8	256

Test3	454	14	10	256
Test4	910	11	9	256
Test5	1822	14	9	256
Test6	3646	15	9	256
Test7	7294	19	10	256
Test8	10092	24	11	256

Table 1 Dataset for performance analysis

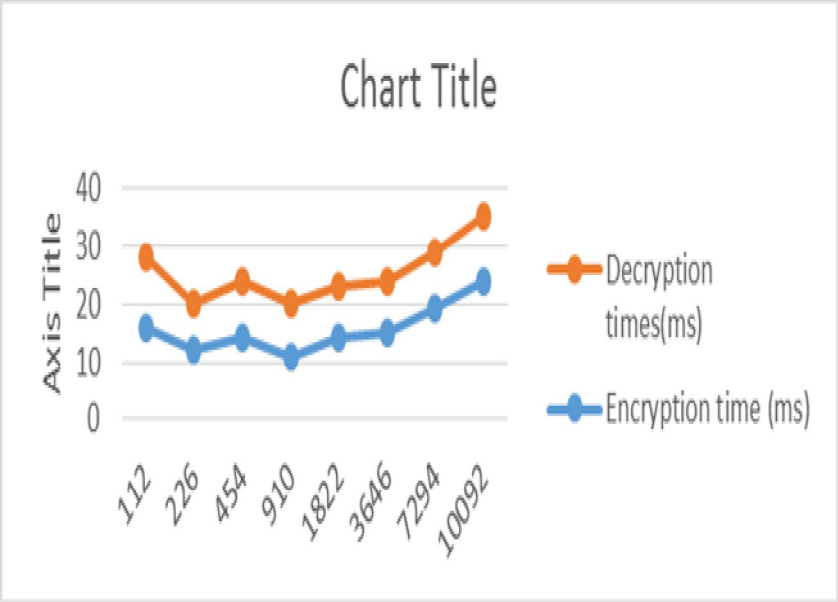


Fig 6 analysis of the time for the Encryption and Decryption with Plaintexts

Length of plain text bits	Previous Encryption time (ms)	Previous Decryption times(ms)	RSA algoritms	Proposed Encryption time (ms)	Proposed Decryption times(ms)	AES algoritms
112	32	31	512	16	12	256
226	33	32	512	12	8	256
454	48	46	512	14	10	256
910	79	78	512	11	9	256
1822	142	125	512	14	9	256
3646	235	203	512	15	9	256
7294	548	422	512	19	10	256
10092	1358	858	512	24	11	256

Table 2. Comparisons of the previous result

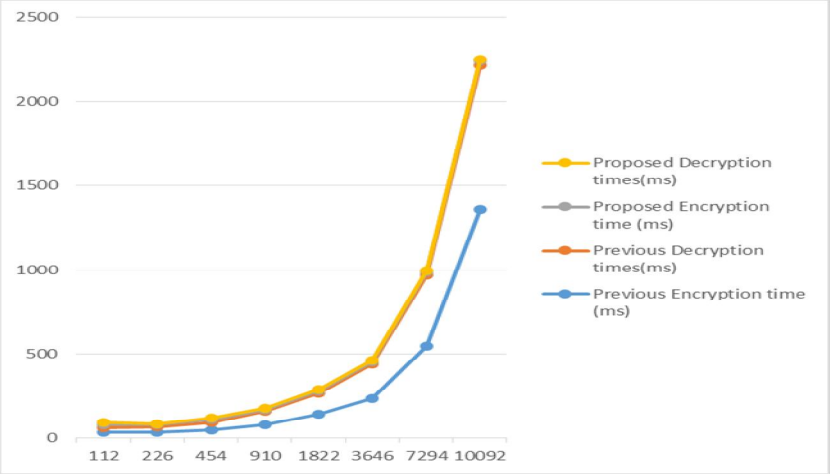


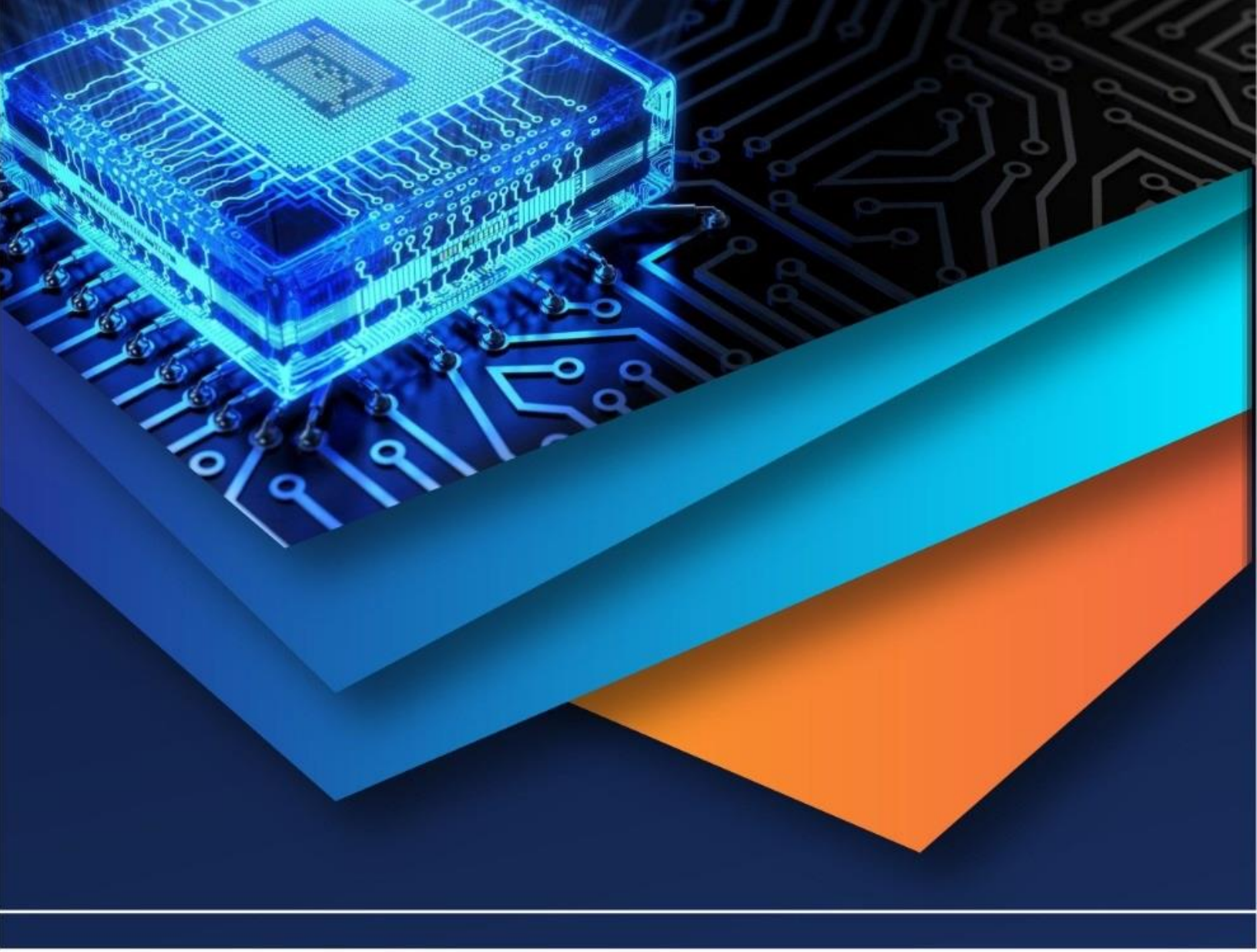
Fig 7 Compare result analysis of the time for the Encryption and Decryption with Plaintexts of different lengths

XI. CONCLUSIONS

This paper introduced a reversible data hiding scheme for deoxyribonucleic acid sequence supported reversible distinction mapping. The scheme uses 2 words of the sequence with the reversible distinction mapping to realize reversibility. DNA cryptography will be combined with ancient cryptography to supply hybrid security. Therefore there's plenty of scope for future works during this space. completely different ancient cryptography techniques combined with DNA cryptography could result in higher hybridisation. the employment of upper dimension matrices for coding and secret writing will additionally minimize the time quality and thus will be thought of as future scope of this work

REFERENCES

[1] L. M. Ad leman, "Molecular computation of solution to combinatorial problems Science, (1994) 11, (266): 1021-1024
[2] Chen Jie, “A DNA-based bio molecular cryptography design,” Proceedings of IEEE International Symposium, Vol. 3, pp. III-822, (2003).
[3] Borda, Monica, and Olga Tornea, "DNA secret writing Techniques," In Communications (COMM), 8th IEEE International Conference on, pp. 451-456, (2010).
[4] TusharMandge, Vijay Choudhary. “A DNA encryption technique based on matrix manipulation and secure key generation scheme”. Information Communication and Embedded Systems (ICICES), International Conference on 21-22 Feb. (2013).
[5] Kazuo Tanaka, Akimitsu Okamoto, and Isao Saito, “Public-key system using DNA as a one-way function for distribution”.Bios stems 81, 1, pp. 25-29, (2005).
[6] Sherif T. Amin, MagdySaeb and El-Gindi Salah, “A DNA-based implementation of YAEA encryption algorithm,” In Computational Intelligence, pp. 120-125, (2006).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY