A Review on DNA Based Cryptography

Ruby Chandrakar[#1], Kirti Nahak[#2]

M.Tech Student, Bharti College of Engineering Technology, Durg, India[#1]

Assistant Professor, Bharti College of Engineering Technology, Durg, India[#2]

ABSTRACT Biotechnological ways may be used for cryptography to boost security of information. Steganography is that the act of hiding messages within a picture. Combining these two ways could be a topic of high relevancy since secure communication is inevitable for humankind. This paper provides an summary of deoxyribonucleic acid based steganographic ways. Hidden message is within the type of DNA sequence, image, audio and video, that is employed to stop necessary information from the intruders. in this paper, a new cryptography technique is projected using symmetrical Key Exchange, one-time pad scheme and dna pairing to reduce time complexness symmetrical Key Exchange is presenting a secure key generation scheme. This methodology is incredibly economical in encrypting, hiding, transmission and preventing powerful attacks

KEYWORDS: DNA, Steganography, Cryptography

I. INTRODUCTION

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.
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).

II. LITERATURE SURVEY BASED ON THE JOURNALS

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 2005, Kazuo Tanaka et al. [5] conferred cryptanalytic algorithmic program supported public key. this is often useful for coding and decoding technique. when generating public key message are encoded in DNA sequence. They used immobilization method and PCR amplification to decrypt the conceded DNA sequence.

In 2006, Sherif T. Amin et al.[6] used regular key algorithmic program in DNA cryptanalytic approach, wherever secret is calculable in DNA sequences square measure obtained from ordination and hold on massive DNA sequence in compact house. DNA cryptanalytic approach has nice storing capabilities than alternative standard cryptography algorithmic program. during this Author represented regular DNA based mostly cipher approach and effectively ascendible for big digital info product.

In 2008, Guangzhao Cui et al. [7] projected the coding theme using DNA writing, PCR amplification and DNA synthesis. The PCR amplification 2 primers combine was used as key and doesn't style by sender and receiver. This coding algorithmic program is employed for increase security purpose. using this methodology we are able to get completely different cipher text, which may stop from trespasser as PCR primers. This coding theme shows that top confidential strength.

In 2008, Lai Xin-she et al. [8] explained novel generation key theme supported DNA cryptanalytic approach. It uses mathematical operation to extend machine speed. They generated key enlargement matrix M and generate coding between 2 key using XOR operations. during this paper they uses the DNA sequence as a randomised info, scale back the computation and influence of mathematical operation to the computed speed.

In 2009, Xing Wang, et al. [11] applied cryptography approach in several field and solve several onerous drawback. during this paper author applied new technique to figure cryptography with DNA computing and RSA algorithmic program is employed to attach with DNA computing to cipher message with efficiency. DNA computing may be a methodology to unravel some onerous drawback and work quicker than information processing system. This paper introduced a brand new coding algorithmic program mix with RSA algorithmic program. DNA computing and model can't utilized in laboratory however this methodology of parallel computing may be a new methodology of computation.

In 2010, Lai, XueJiaet al. [9] projected DNA sequence as uneven coding and signature methodology with DNA technology matrix is obtained for encryption the image. Divide the DNA sequence matrix into block and addition operation is performed between block. during this paper original image square measure disorganised by addition and complement operation, that provides massive secret key house and high sensitive to secret key of coding algorithmic program. This algorithmic program resists complete attack, statistical attack and differential attack.

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.
.

III. CONCEPT OF DNA DATA HIDING

DNA Structure - deoxyribonucleic acid (DNA) sequence consisting of 4 alphabets: A, C, G and T. it's 2 base pairs (A, T) and (C, G) a sugar and phosphate cluster. the mix of 2 base pairs is created helix like structure of deoxyribonucleic acid containing double chemical bond with (A, T) and triple chemical bond with (C, G). WatsonCrick base
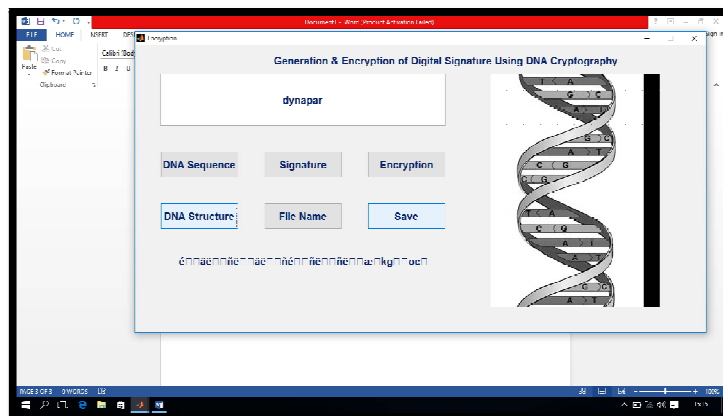
complementary principle (A, T) and (C, G) are complement to every alternative. the mix of the bases leads to purines and pyrimidines. The sequence of those bases stores info of living organisms, that is exclusive for all living organisms. There ar 2 strands of polymer sequence represent a private strand as single stranded deoxyribonucleic acid (ssDNA) and double stranded polymer (dsDNA) . an ssDNA will form double strand polymer (dsDNA) with alternative ssDNA. SsDNA and dsDNA ar complementary with one another. This method is termed hybridisation. the 2 strands deoxyribonucleic acid molecules are opposed parallel to every alternative.

DNA Technologies- deoxyribonucleic acid cryptography uses totally different style of technologies to write knowledge through secure channel, as for example- polymer enzyme chain reaction (PCR), bio molecular, one-time-pad. Polymer cryptography technology determines the order of 4 polymer sequence (A, C, T, G). OTP is generated key which is employed only 1 time for secret writing and it's to be modified for an additional time. PCR could be a biology technique to amplify many copies of polymer up to order of magnitude of specific deoxyribonucleic acid.

DNA secret writing Method- polymer secret writing methodology could be a procedure for conversion of plain text to computer code code and future conversion of computer code code to polymer sequence. There are 2 ways to write a noticeable text. Plain text is encoded to binary range, that is expressed in eight bits. as an example computer code code for plain text 'S' is eighty three, that is additional convert into binary range (83)2= 01010011.   Binary plain text 'S'=01010011is born-again into deoxyribonucleic acid sequence mistreatment table 2given below. for instance, scanning 2 left most bits within the binary sequence and additional convert to deoxyribonucleic acid sequence consistent with table two. A=00, C=01, G=10, T=11 [15]

IV. RESULT AND CONCLUSION

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
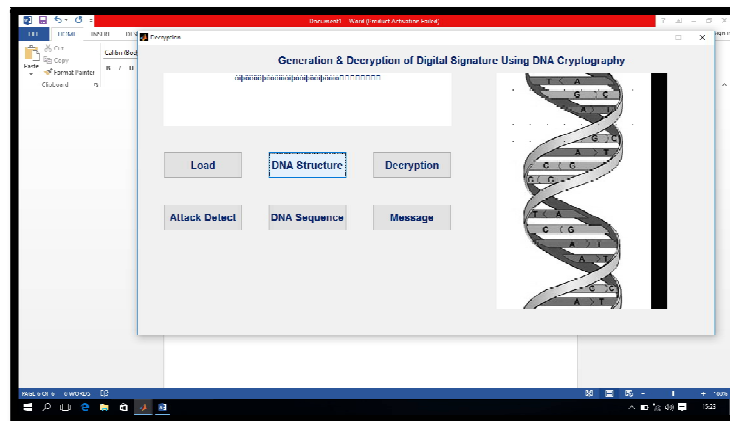
REFERENCES

[1] Alattar M., "Reversible Watermark Using the Difference Expansion of a Generalized Integer Transform," Computer Journal of IEEE Transactions on Image Processing, vol. 13, no. 8, pp. 1147-1156, 2004.

[2] Chang C., Lu T., Chang Y., and Lee C., "Reversible Data Hiding Schemes for DEOXYRIBONUCLEIC ACID Medium," International Journal of Innovative Computing, Information and Control, vol. 3, no. 5, pp. 1-16, 2007.

[3]Chen T., A Novel Biology-Based Reversible Data Hiding Fusion Scheme, Springer-Verlag, 2007.

[4]Coltuc D. and Chassery J., "Very Fast Watermarking by Reversible Contrast Mapping," Computer Journal of IEEE Signal Processing Letters, vol. 14, no. 4, pp. 144-146, 2007.

[5]Coltuc D. and Tremeau A., "Simple Reversible Watermarking Schemes," Computer Journal of SPIE: Security, Steganography, Watermarking Multimedia Contents, vol. 5681, no. 214, pp. 561-568, 2005.

[6] L. M. Ad leman, "Molecular computation of solution to combinatorial problems Science, (1994) 11, (266): 1021-1024

[7] Chen Jie, "A DNA-based bio molecular cryptography design," Proceedings of IEEE International Symposium, Vol. 3, pp. III-822, (2003).

[8] Borda, Monica, and Olga Tornea, "DNA secret writing Techniques," In Communications (COMM), 8th IEEE International Conference on, pp. 451-456, (2010).

[9] 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).

[10] 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).

[11] Sherif T. Amin, MagdySaeb and El-Gindi Salah, "A DNA-based implementation of YAEA encryption algorithm," In Computational Intelligence, pp. 120-125, (2006).

[12]Coltuc D. and Chassery J., "Very Fast Watermarking by Reversible Contrast Mapping," Computer Journal of IEEE Signal Processing Letters, vol. 14, no. 4, pp. 144-146, 2007.