iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** III **Month of publication:** March 2015

DOI:

www.ijraset.com

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

Volume 3 Issue III, March 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Survey on DNA Based Cryptography

Mohit[1], Manisha[2], Parvinder Bangar[3]
M.Tech Scholar[1], Asstt.Prof.[2],H.O.D[3]
ECE Deptt., CBS Group of Institutions, Jhajjar, Haryana, India[1,3]
ECE Deptt., M.R.I.E.M., Rohtak, Haryana, India[2]

Abstract: DNA cryptography is a new era of enhanced security for the data transfer using the internet. DNA cryptography enhanced the cryptography in terms of time complexity as well as capacity. It uses the DNA strands to hide the information. The repeated sequence of the DNA makes highly difficult for unintended authority to get the message. This paper discusses DNA cryptography and the difference between the traditional and the DNA cryptography. This paper also brief the various work done in the field of the DNA cryptography.
Keywords: DNA , cryptography, DNA cryptography

I. INTRODUCTION

Cryptography is the science and art of secret writing [1][2]. It studies some mathematical techniques and provides mechanisms necessary to provide aspects related to information security like confidentiality, data integrity, entity authentication, and data origin authentication[2].
Symmetric algorithms are cryptosystems that either a secret key will be shared for both encryption and decryption [1][5]. The algorithms of symmetric cryptosystems are very strong against possible attacks, but mainly weakness of symmetric cryptosystems is brute-forcing the secret key. This characteristic creates the biggest critical act in any cryptosystem that uses symmetric algorithms which is distribution of the shared secret between the two parties like DES algorithms. Asymmetric algorithms use different values for encryption and decryption and do not need to share secret between two parties. Each party only has to keep a secret of its own. The earliest foundation of asymmetric algorithms known as public key cryptosystems comes from key exchange problem of symmetric algorithms. In 1976, Whitfield Diffie and Martin Hellman proposed a method were the sender and receiver do not have to share a secret. That was the first work on hybrid cryptosystem [1][2].
DNA stands for Deoxyribo Nucleic Acid. DNA represents the genetic blueprint of living creatures. DNA contains “instructions” for assembling cells. Every cell in human body has a complete set of DNA. DNA is unique for each individual. DNA is a polymer made of monomers called deoxyribo nucleotides. The structure of DNA is specified in figure 1. Each nucleotide consists of three basic items: deoxyribose sugar, phosphate group and a nitrogenous base. The nitrogenous bases are of two types: purins Adenine and Guanine) and pyrimidins (Cytosine and Thymine). They are represented as A, G, C and T. A binds with T and G binds to C. The various operations that can be performed on DNA are ligation, polymerase chain reaction (PCR), gel electrophoresis and affinity purification[4] .

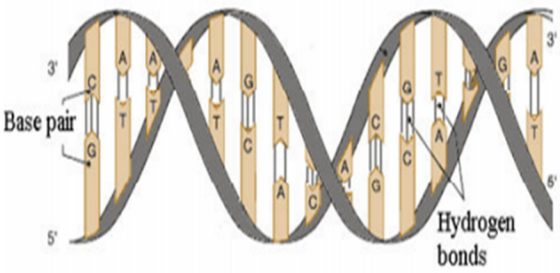


Figure 1: DNA Structure

DNA cryptography, a new branch of cryptography utilizes DNA as an informational and computational carrier with the aid of molecular techniques. It is relatively a new field which emerged after the disclosure of computational ability of DNA [5]. DNA cryptography gains attention due to the vast storage capacity of DNA, which is the basic computational tool of this field. One gram

of DNA is known to store about 108 tera-bytes. This surpasses the storage capacity of any electrical, optical or magnetic storage medium [5], [6]. Traditional cryptographic systems have long legacy and are built on a strong mathematical and theoretical basis. Traditional security systems like RSA, DES or NTRU are also found in real time operations. So, an important perception needs to be developed that the DNA cryptography is not to negate the tradition, but to create a bridge between existing and new technology. The power of DNA computing will strengthen the existing security system by opening up a new possibility of a hybrid cryptographic system. This needs the clear difference between the traditional and DNA based cryptography that is specified in the table 1.

Table 1: Comparison of traditional and DNA cryptography[4]

Characteristics	Traditional Cryptography	DNA cryptography
Security	less	more
Time	Minutes to hours	Hours to days
Storage capacity	In MB	In TB
Dependency	On Implementation environment	On environmental conditions

II. TECHNOLOGY USED IN DNA COMPUTAION

Today, various techniques are used to carry out DNA computation. Researchers use these techniques for performing the operations on informative DNA molecules. Some of these technologies are as follows:

A. Gel electrophoresis

It is a phenomenon used to separate the DNA fragments according to their length. A gel of polyacrylamide or agarose is prepared. The negatively charged DNA molecules are placed in the wells which are situated at one side of this gel. On the application of an electric current to the gel, the negatively charged DNA molecules will start moving towards the positive pole, where the shorter molecules travel faster than the larger ones. Hence, a separation between them can be detected easily [14].

B. Polymerase Chain Reaction (PCR)

As it is difficult to manipulate the small amount of DNA, an amplification process is carried out. PCR has very high amplification efficiency, hence, this technology is used to amplify and quantify the DNA. In DNA amplification using PCR, required DNA segments are cloned into vectors. For PCR amplification two things are required, a primer and a DNA template. DNA template is a single-stranded DNA sequence which contains the segment which is to be amplified and primer is a complement sequence of that segment. A primer is annealed with the DNA template. After that, DNA polymerase enzyme initiates DNA synthesis process by successively adding the nucleotides to 3' end of the primer, until the desired DNA strand is obtained. Primer always extends in the direction 5' to 3' only. The desired DNA strand starts with the primer and is always complementary to the DNA template. The whole PCR process can be divided into two steps:

1) Designing the two primers and loading them separately, one at the beginning and another at the end of target DNA.
2) Matching the primers with their complement sequences in template DNA [15].

C. DNA Chip technology:

With the help of DNA chip, a vast amount of genome-sequencing data can be manipulated [16]. It is used to find the expression of several genes in parallel. DNA chips stores data in the form of DNA sequences. In DNA chips, a huge number of spots are embedded on solid surface, generally a glass slide. Each and every spot of a chip consists of different type and number of probes. Probes are small single-stranded DNA sequences have the ability to bind with their complementary DNA sequences. Binded DNA sequences are labelled fluorescently which are observed under laser dye. Depending upon the ratio of binding between probe and DNA of each spot, data is calculated by electronic means[17].

III. DNA BASED CRYPTOGRAPHY

Adding or hiding data in chemical DNA sequences does not require us to be very clever For most tasks, a flat encoding of 2 bits/nucleotide, assigned in alphabetical order would be a sufficient starting point

. A=00 C=01 G=10 T=11

With this basic foundation, we can add binary segments to DNA that could be used to store interspersed hidden data, annotate existing DNA sequences, watermark a DNA computing solution, and so on. Depending on the task, different operations could be performed on the binary sequence while the DNA encoding scheme remains constant. For the purposes of data storage or transport, a compression step on the binary data would be useful. For a watermark, an encryption step would be appropriate. For annotation, plain text or simple codes could be used. After each important sequence, perhaps it would be useful to add a checksum to verify that the DNA strand hasn't degraded or been altered. In all cases, the application would drive the operations performed on the hidden data and in all cases, existing well-known binary techniques could be used for this purpose. The motivation for this is simple. The fewer complex and unprecedented steps are performed on data, the easier it is to process, embed, extract, and explain in court. Extending this notion to live DNA requires great care. Unlike, chemical DNA where changes can be made wherever necessary to hide data, with live DNA, besides the obvious dangers of active genetic segments, there are other complications. Although, only a small percentage of DNA codes directly for genes, in addition to genes, there are regulatory and structural regions. Altering or adding sequences that seem innocuous may have profound effects when processed by cellular machinery.

IV. RELATED WORK

Wael Adi et al. [7] showed a scenario to link e-DNA identity proposed in a former work to a dynamic, transaction dependant unit profile in its operating environment. The system attempts to link the unit identity to its interaction profile in the network. Lukas Kencl et al. [8] proposed that DNA contains repeats in order to solve the information concealing problem. They want to stress that even though their algorithm is inspired by the repeats in DNA, the output of the algorithm, aside of containing repeats, has no other similarities to the DNA structure as far as we know. Hayam Mousa et al. [9] introduced a reversible information hiding scheme for DNA sequence based on reversible contrast mapping. The scheme uses two words of the sequence with the reversible contrast mapping to achieve reversibility. Jin-Shiuh Taur et al. [10] proposed an improved algorithm named the Table Lookup Substitution Method (TLSM) to enhance the performance of an existing data hiding method called the substitution method. Moreover, a general form of the TLSM is discussed, which includes the original method as a special case.

Mohammad Reza Najaf Torkaman et al. [11] proposed to decrease the usage of asymmetric cryptography and introduced a novel cryptographic-steganography protocol. The main advantage of proposed cryptography protocol was using innovative DNA steganography techniques to conceal secret session key which is transferred among sender and receiver throughout unsecured channel. Ban Ahmed Mitras et al. [12] discussed a reference DNA sequence has been shared between sender and receiver. Not only this DNA reference sequence can be retrieved from EBI or NCBI databases but it can also be simply selected from any database. Therefore, by considering any sort of database, there are 163 million targets to select it. Virtually, guessing the correct DNA sequence by attacker is unachievable. M. Yamuna et al. [13] proposed four methods for encryption of a binary string. In practice finding the difference between a original DNA and fake one is not easy because lot of fake DNA sequences are already publicly available. So encrypting a binary string as a DNA sequence is very safe. K. Menaka et al. [4] proposed algorithm has many steps to break and to get the original message. So, any intruder who receives the intermediate message will never be able to retrieve the original message as intended by the sender. The random selection of DNA sequence can be increased to many numbers. The existing work is also explained in the following table i.e. table 2:

Volume 3 Issue III, March 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Table 2: Related Work

Author	Year	Contribution
Wael Adi et al. [7]	2008	link the unit identity to its interaction profile in the network
Lukas Kencl et al. [8]	2010	solve the information concealing problem
Hayam Mousa et al. [9]	2011	introduced a reversible information hiding scheme
Jin-Shiuh Taur et al. [10]	2012	proposed an improved algorithm named the Table Lookup Substitution Method (TLSM)
Mohammad Reza Najaf Torkaman et al. [11]	2012	decrease the usage of asymmetric cryptography
Ban Ahmed Mitras et al. [12]	2012	Increased Security
M. Yamuna et al. [13]	2013	Proposed four methods for encryption of a binary string

V. DRAWBACK OF EXISTING WORK

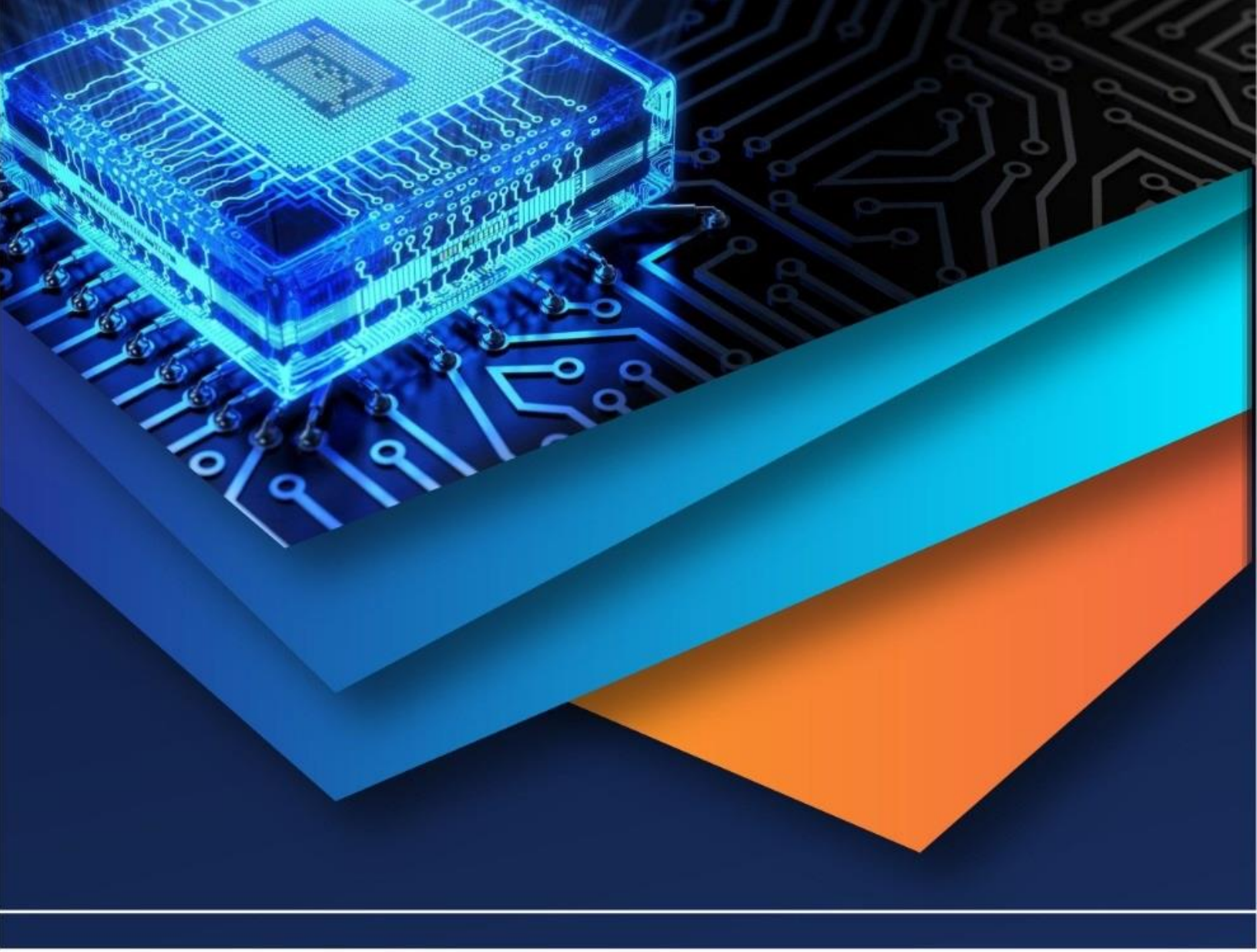
The unintended user gets to know that data is hided in the particular DNA then the extraction of data is possible in the DNA based Steganography. It is due to the fact the data is in plain form in the DNA. While the cryptography makes the data in encrypted form but the data is visible to the unintended user. To make the process more robust and secure the data must hided must be cascaded by cryptography and the Steganography.

VI. CONCLUSION

This paper discusses the structure of the DNA along with the DNA cryptography. This paper also briefs the work done in the area of the DNA cryptography. The difference between the traditional and DNA cryptography clears the importance of the DNA cryptography. The drawback of the previous work defines the open area of research in the field of DNA cryptography. In future an algorithm can be designed for DNA based cascaded Steganography and cryptography.

REFERENCES

[1] Torkaman M.R.N., Nikfard P., Kazazi N.S., Abbasy M.R., and Tabatabaiee S.F.: Improving Hybrid Cryptosystems with DNA Steganography. E. Ariwa and E. El-Qawasmeh (Eds.): DEIS 2011, CCIS 194, pp. 42–52, 2011
[2] Alia, M.A., Yahya, A.: Public–Key Steganography Based on Matching Method. European Journal of Scientific Research, 223–231 (2010)
[3] Kumar, S., Wollinger, T.: Fundamentals of Symmetric Cryptography. Embedded Security in Cars, 125–143 (2006)
[4] Menaka, K. (2014, February). Message Encryption Using DNA Sequences. InComputing and Communication Technologies (WCCCT), 2014 World Congress on (pp. 182-184). IEEE.
[5] Anam B., Sakib K., Hossain M.A., Dahal K.: Review on the Advancements of DNA Cryptography. arXiv:1010.0186v1 [cs.CR] 1 Oct 2010.
[6] G. Cui, Y. Liu, and X. Zhang,: New direction of data storage: DNA molecular storage technology. Computer Engineering and Application, vol. 42, no. 26, pp. 29–32, 2006.
[7] Adi, W. (2008, August). Clone-Resistant DNA-Like Secured Dynamic Identity. In Bio-inspired Learning and Intelligent Systems for Security, 2008. BLISS'08. ECSIS Symposium on (pp. 148-153). IEEE.
[8] Kencl, L., & Loebl, M. (2010). DNA-inspired information concealing: A survey. Computer Science Review, Volume4, Issue (4), pp. 251-262.
[9] Mousa, H., Moustafa, K., Abdel-Wahed, W., & Hadhoud, M. M. (2011). Data hiding based on contrast mapping using DNA medium. Int. Arab J. Inf. Technol., Volume- 8 Issue (2), pp 147-154.
[10] Taur, J. S., Lin, H. Y., Lee, H. L., & Tao, C. W. (2012). Data Hiding In Dna Sequences Based On Table LookUp Substitution. International Journal of InnovativeComputing, Information and Control, Volume 8 Issue (10).
[11] Torkaman, M. R. N., Kazazi, N. S., & Rouddini, A. (2012). Innovative approach to improve hybrid cryptography by using DNA steganography. International Journal of New Computer Architectures and their Applications (IJNCAA), Volume-2 Issue(1), pp. 224-235.
[12] Mitras, B. A., & Aboo, A. K. (2012). Proposed Steganography Approach Using Dna Properties. International Journal of Information Technology and Business Management, Volume-14 Issue 1.
[13] Yamuna, M., Dangi, M. K., & Singh, K. (2013). Encryption of a Binary String Using DNA Sequence. International Journal of Computer Science, Volume 2, Issue (02).
[14] H. Lodish, A. Berk, P. Matsudaira, C. A. Kaiser, M. Krieger, M. P. Scott, S. L. Zipursky, and J. Darnell “Molecular Cell Biology”, 5th ed. New York: W. H. Freeman and Co. 2003.
[15] G. Cui, L. Qin, Y. Wang, and X.Zhang, “An encryption scheme using DNA technology,” in IEEE 3rd International conference on Bio-Inspired Computing: Theories and Applications (BICTA08), Adelaid, SA,Australia, pp. 37–42, 2008
[16] P. Gwynne and G. Heebner, “Technologies in DNA chips and microarrays: I,” Science, vol. 4 May, p. 949, 2001.
[17] T. Tsukahara and H. Nagasawa, “Probe-on-carriers for oligonucleotide microarrays (DNA chips),” Science and Technology of Advanced Materials,Elsevier Science, vol. 5, pp. 359–362, 2004.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY