DOUBLE LAYERED DNA BASED CRYPTOGRAPHY

Manisha[1], Parvinder Bangar[2], Mohit[3]

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

Abstract

DNA cryptography the new era of 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. The level of security can be increased by using the more than one cover medium. This paper discussed a technique that uses two cover medium to hide the message one is DNA and the other is image. The message is encrypted and converted to faked DNA then this faked DNA is hided to the image.

***Keywords**: DNA, cryptography, DNA cryptography*

----------***----------

1. INTRODUCTION

Redundancy of words and characters in English language helps cryptanalysts in guessing the cipher text. Acc. to Shannon theory, the entropy of printed English lies between 0.6 and 1.3 bpc based on successive character prediction level of a person [1]. Whereas, Cover and King [2], estimated the entropy as 1.25 bpc. Researchers [3-5] estimated the entropy of DNA sequences. After comparing it with the entropies of other natural languages, they concluded that expressing power of DNA is higher than any other natural language. Moreover, Tsonis et al. [6] in his study declared that DNA sequences do not follow any linguistic properties. Hence, translating any language first to DNA sequences and then applying cryptography technique upon it can prevent the attacks based on frequency analysis.

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.

2. RELATED WORK

The existing works are explained in the following table i.e. table 1:

Table 1: 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

3. EXISTING WORK

In this existing method, the algorithm first randomly selects a DNA sequence for example, TAGCATGACT. Each letter is then given a subscript index starting from 0. Message index is the first positional index value of the DNA sequence. As the next step, any complementary rule. As per the algorithm, a single letter is replaced with a specific letter defined by the complementary rule. For example, if the complementary rule 1 is selected, then, as a first bit (most significant bit) apart from the obtained sequence, a letter 'A' is inserted which implicitly tells the receiver that rule 1 is selected. Likewise, if letter 'C' is inserted, then it tells that rule 2 is used and 'G' is used for rule 3.

The message to be encoded is then taken and each letter in the faked DNA sequence is given subscript. Each letter in the message is converted into its ASCII equivalent and they are then converted into equivalent binary form. Each two digits in the converted binary sequence are converted. Then, the message index position (first position of each letter) in the faked DNA sequence is applied to each letter of the converted sequence. Each digit in the resultant sequence is replaced with its equivalent three digit binary value and the equivalent alphabet value is replaced for the binary value. For example, if the obtained binary value is 010 011 101 … , then it will be replaced as C D F… where A has the value 000, B has 001 and so on. The resultant sequence of alphabets is transmitted over to the receiver. In the receiver side, the reverse process is done in which the original receiver knows the complementary rules and the randomly selected DNA sequence. The message to be sent is then encoded with the fake DNA sequence and transmitted. It can also be elaborated by following diagram:

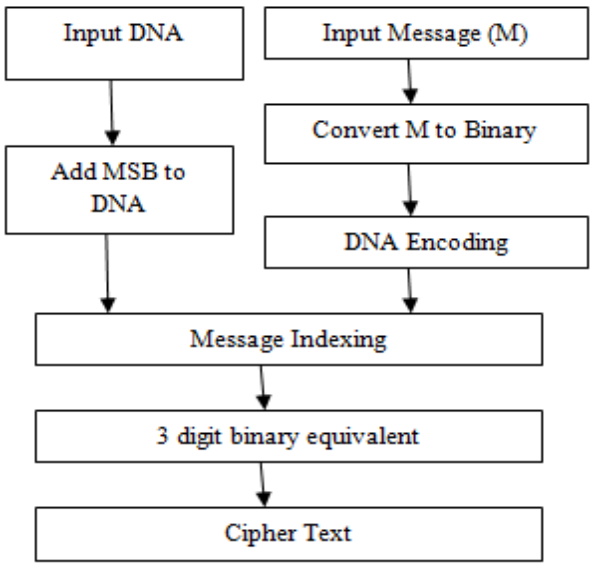
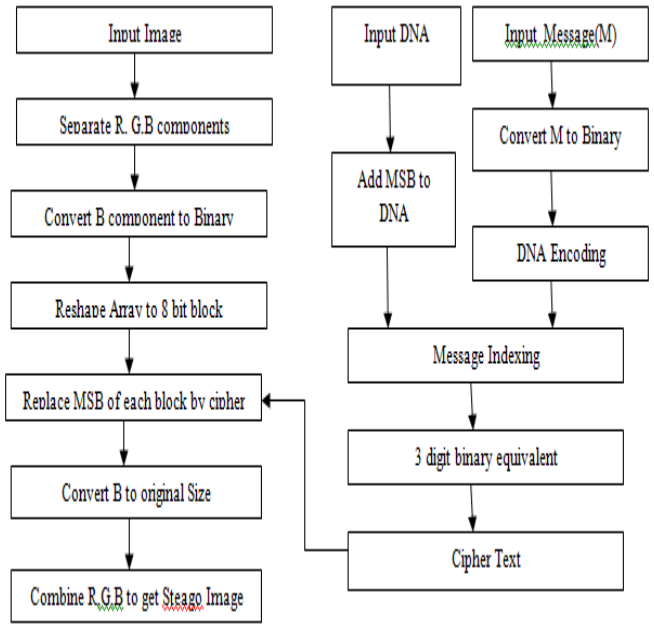


Fig 1: Encryption using Existing Technique

4. PROPOSED TECHNIQUE

In the existing system, if 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. In this work the input is an color image. The R, G, B component are extracted from the image. The extracted components are converted in to the binary format. Then the binary array is reshaped to the block of 8 bit. Then the secret message is encrypted to the DNA by using the indexing of the faked DNA. Then the encrypted message i.e. DNA is hided to blue component of the image by replacing the LSB of the each block by one bit. The present work can also be easily explained by the following diagram:



The decryption process is the reverse of the encryption process. This work is beneficial due to the double cover medium one is DNA and the other is image. Moreover, the DNA is hided to the blue component of the image that makes system imperceptible.

5. CONCLUSION

The paper proposes an imperceptible technique to secure the message while transmission. The technique is highly secured as it uses two cover medium to hide the message. The message is firstly encrypted to the DNA then the encrypted DNA is hided in to the blue component of the image. The system is highly secured and efficient. In future, the other cover medium can also be used to hide the message.

REFERENCES

[1]. Shannon, C. "Prediction and entropy of printed English*". Bell Systems Technical Journal*, vol. 30, pp. 50-64. 1951

[2]. Cover, T. & King, R. "A convergent gambling estimate of the entropy of English", *IEEE Transactions on Information Theory*, vol. 24, No. 4: pp. 413-421, 1978.
[3]. Lanctot, J., Li, M., & Yang, E. "Estimating DNA Sequence Entropy", *Symposium on Discrete Algorithms*, 2000.
[4]. Farach, M., Noordewier, M., Savari, S., Shepp, L., & Wyner, A. "On the entropy ofDNA: algorithms and measurements based on memory and rapid convergence, *Symposium on Discrete Algorithms, 1995.*
[5]. Behr, F., Fossum, V., & Mitzenmacher, M. "Estimating and Comparing Entropy across Written Natural Languages Using PPM Compression", *Technical Report TR-12-02*, Harvard University, 2002.
[6]. Tsonis, A., Elsner, J., &Tsoni, P. "Is DNA a language?" *Journal of Theoretical Biology*, Vol. 184, No.1, pp. 25-29, 1997
[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).