ISSN: 2321-7782 (Online)

Volume 3, Issue 6, June 2015

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Enhanced DNA Based Cryptography

Manisha[1]
M.Tech CSE Student
R. N. College of Engineering & Management
Maharshi Dayanand University
Rohtak, Haryana - India

Pooja Ahlawat[2]
Assistant professor
Department of Computer Science and Engineering
R. N. College of Engineering & Management
Maharshi Dayanand University, Rohtak, Haryana - India

Abstract: Traditional cryptography technique uses English words. Due to the limited dictionary of the English unauthorized entity can guess the cipher text. The DNA sequences do not follow such properties. It means the conversion of message to DNA sequences make it robust against attacks. This paper performs the DNA cryptography and then hides the DNA sequence in to the random frame of a video. The result analysis shows that the frame is imperceptible the video seems to be same. The enhancement in PSNR value and reduction in MSE shows the effectiveness of the technique.

Keywords: Cryptography, DNA cryptography, video, frame, PSNR, MSE.

I. Introduction

DNA stands for "Deoxyribose Nucleic Acid". It is a polymer of nucleotides. Each nucleotide contains three things: a 5-carbon sugar molecule, nitrogenous base and phosphate group. Depending upon nitrogenous base, nucleotides of DNA can be of four types: Adenine (A), Guanine (G), Cytosine (C), Thymine (T).

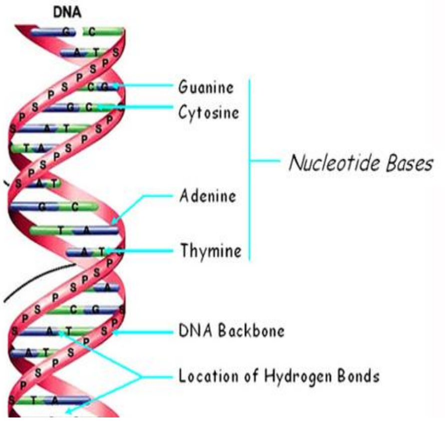

Fig 1: Structure of DNA

Where Adenine and Guanine are purines and Cytosine and thymine are pyrimidines. DNA is a double-helical structure with both strands running in opposite direction with the pairing of bases such that Guanine always pairs with Cytosine and Adenine always pairs with Thymine. The sugar molecule and phosphate group links together to form the backbone of each strand. The 3'carbon of sugar molecule connects to 5'carbon of next sugar molecule through phosphate group [25]. In DNA cryptography, the four bases Adenine (A), Guanine (G), Cytosine(C) and Thymine (T) are used to capture the information.

II. Operations on DNA

L. Kari[7] in her article, break down the process of DNA computing into several steps which are considered as the primitive operations for DNA computation. These operations are as follows:

DNA Synthesis: Encoding of text written in any language is done over four alphabets {A, C, G, T} to obtain a single strand of DNA.

Hybridization: Based on the complementary theory of Watson- Crick, single strands of DNA with opposite orientation join together in order to form a double helical structure. This operation is also known as *annealing.*

Cutting: A specific short length sequence of DNA is selected called restriction enzyme. This restriction enzyme is mapped with the double-stranded DNA. The site where the occurrence of this restriction enzyme found in a double-stranded DNA sequence is known as restriction site. The enzyme cuts the DNA sequence from that location in a specific sequence which is same as that of the enzyme. As a result, two “blunt-ended” double strands of DNA are left or two double-stranded DNA with single-stranded overhangs known as “sticky-ends” are left.

Ligation: This operation is reverse of cutting. In this, an enzyme known as DNA ligase, repairs and rejoins the resultant double-stranded DNA sequences of cutting operation.

Separation: This operation is carried out by using *gel electrophoresis* technique. In this, DNA molecules are filtered out according to their size (small or large).

Extraction: A single stranded DNA molecule that contains the targeted subsequence of bases is extracted by a process of affinity purification.

DNA replication: It is done with the help of *polymerase chain reaction* and a *primer*. In this, multiple copies of the complemented segment of DNA template which starts with primer sequence are produced.

All these operations can be performed in parallel.

III. DNA Cryptography

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.

IV. Results and Discussion

The parameters evaluated are PSNR, MSE and the total percentage of bit change. PSNR is the measure of the image quality. Generally when PSNR is 40db or greater, then the original and the stego images are virtually indistinguishable by human observer.

PSNR and MSE are defined as follows:

$$\mathrm{PSNR} = 10\log_{10}\frac{255^2}{\mathrm{MSE}} \quad \text{and} \quad \mathrm{MSE} = \frac{1}{n}\sum_{i=1}^{n}\left(I_m(i) - I_s(i)\right)$$

Where I_m and I_s are the original and watermarked image, respectively, n is the number of pixels.

Higher the PSNR means better image quality.

The total percentage of the bit change represents the amount of bits change in the cover data to get the stego data. Lower the bit change better is the technique.

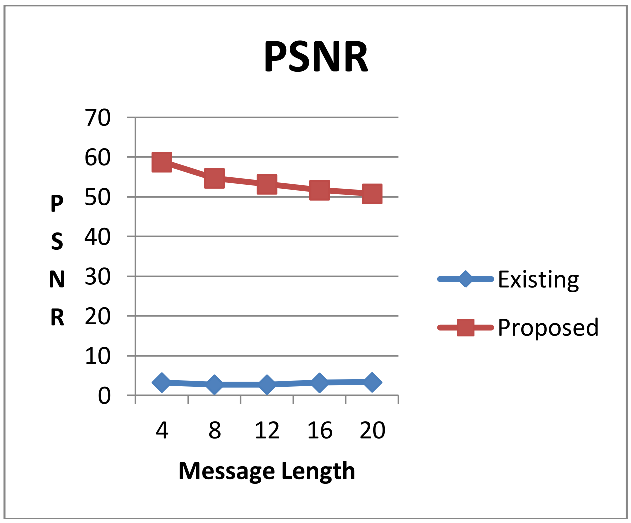

Figure 4: Comparison of PSNR Values

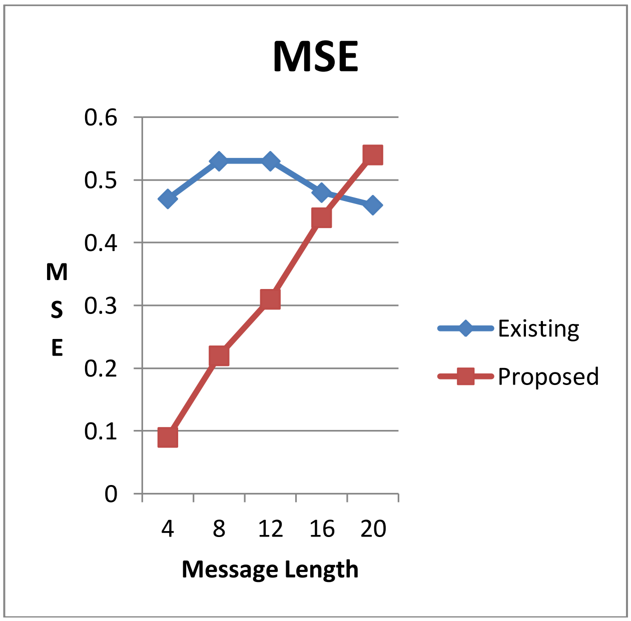

Figure 5: Comparison of MSE Values

The result comparison clearly shows that the amount of bit change reduced drastically. This signifies the importance of the proposed technique. The amount of the bit change reduced means both data that is original data and the stego data seems to be same. The higher values of the PSNR also show the effectiveness of the technique.

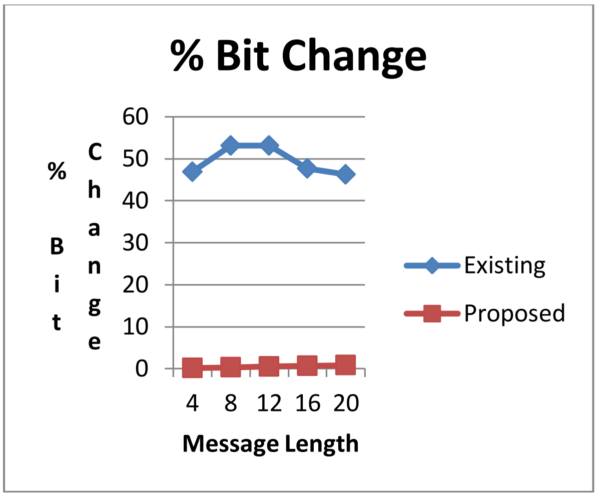

Figure 6: Comparison of % Bit change Values

V. Conclusion and Future Scope

The paper proposed a cascaded cryptography and Steganography by using the DNA cryptography and video Steganography. The work is implemented using the MATLAB and PNSR and MSR along with the % bit change is analysed. The increase in the PSNR and decrease in the MSE shows the effectiveness of the technique. The % bit change reduces a lot i.e. the resultant seems to be same as the original. It increases the imperceptibility. In future the work can be extended by using the audio cover media.

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. L. Kari, "DNA Computing: Arrival of Biological Mathematics," The Mathematical Tntelligencer, vol. 19, pp. 9–22, 1997.

Author(s) Profile

Manisha, received the B.Tech (Computer Science) Matu Ram Engineering and Management College affiliated to M. D. University in 2013 and M.Tech degree in Computer Science and Engineering from R. N. College of Engineering & Management affiliated to M. D. University in 2015, respectively