Literature Review on DNA-based Audio Steganographic Techniques

Rashmi M. Tank[1] , Prof. Vikram Agrawal[2] , Prof. Hemant D. Vasava[3]

[1]*PG Student of Computer Department* , [2]*Assistant Prof. of IT Department* , [3]*Assistant Prof. of Computer Department,*

Gujarat Technological University,

B.V.M. Engineering college , Vallabh Vidhyanagar , Anand , Gujarat , India

Abstract **– Steganography is the technique of hiding secret message in a cover medium in such a way that only the sender and the intended recipient knows the existence of communication. DNA due to its immense storage capacity and high randomness is used now in the field of steganography. Though many algorithms have been developed for hiding the data, DNA sequences based data encryption seems to be a promising strategy for fulfilling the current information security needs. Audio steganography is concerned with hiding information in a cover (host) audio signal in an imperceptible way. In this paper, various techniques using DNA Sequences and audio files for data hiding is discussed for secure data transmission and reception.**

Keywords- **Steganography, Data hiding, Data Security , DNA Sequence , Audio Steganography**

I. INTRODUCTION

Digital communication has become an essential part of infrastructure nowadays and also lots of applications are internet based. So the communication made must be secret. Techniques such as cryptography are being used on a large scale for transmitting information secretly. Steganography is a new approach of providing secure data transmission. The term steganography is derived from two greek words, “stegano” means ”secret” and “graphy” means “writing” .So steganography literally means secret writing, hide the secret message in a cover medium so that it cannot be seen.

DNA computing is a new method of simulating biomolecular structure of DNA and computing by means of molecular biological technology which has a novel and potential growth. In a pioneering study, Adleman demonstrated the first DNA computing. It marked the beginning of a new stage in the era of information. DNA (Deoxyribonucleic Acid) is the germ plasm of all life styles. It is a kind of biological macromolecule made up of nucleotides. Each nucleotide contains a single base. There are four kinds of bases, which are adenine (A), thymine (U or T), cytosine (C) and guanine (G). In a double helix DNA string, two strands are complementary in terms of sequence, that is A to T and C to G according to Watson-Crick rules.A number of methods have been proposed over the last decade for encoding information using deoxyribonucleic acid (DNA), giving rise to the emerging area of DNA data embedding.

Audio Steganography hides the secret message in an audio signal called cover audio. Once the secret message is embedded in the cover audio, the resulting message is called stego message and stego message is transmitted to the receiver side. While hiding the secret data one has to be keep in mind that the header part of the wave file ie. first 44 byte should be unaltered because in case the header gets corrupted, the audio file will also corrupt. Another consideration that should be made is not to embed data into the silent zone as that might cause undesirable change to the audio file At present, there is lot of research is being made on audio steganography. This paper presents literature review of few of the methodologies of DNA based audio steganography.

II. HISTORY

The first steganographic technique was developed in ancient Greece around 440 B.C. The Greek ruler Histaeus employed an early version of steganography. He shaved the head of a slave and then tattooed the message on the slaves scalp, waited for the hair to grow to cover the secret message. Once the secret message is covered he sent the slave on his way to deliver the message. The recipient shaves the slave’s head to read the message.

Null ciphers were also used to send secret messages. Null ciphers are messages which contain secret messages embedded in the current text. An example of null cipher is: “Missing feel mind and boat strength admit masterful transparent randomness side moment proposed many step way.” By taking the third letter in each word we get the secret message as follows:

Send arms and money.

III. LITERATURE REVIEW

1. Shyamasree C M and Sheena Anees proposed the DNA based Audio Steganography method which works in three levels [1]. First level makes use of DNA based Playfair algorithm.The second level hides the secret message in a randomly generated DNA sequence.In the third level embedded DNA is hidden inside the Audio file.DNA digital

coding is used to convert the raw data in secret file into DNA sequence. Any DNA sequence can be encoded using binary coding scheme. They have used the coding pattern A(00) , C(01) ,G(10) and U(11) to encode 4 nucleotides.The sequence of three nucleotides is called codon. There are total 64 possible codons. These codons are mapped to 20 standard amino acids. They have used playfair encryption algorithm to encrypt the sequence of amino acids. The encrypted DNA sequence is hidden inside randomly generated DNA sequence using two-by-two complementary rule. Finally the embedded DNA sequence is hidden inside audio file using Least Significant Bit (LSB) modification technique.

2. Amal Khalifa proposed LSBase: A key encapsulation scheme to improve hybrid crypto-systems using DNA steganography [2].A hybrid crypto-system is public key system. They have used cryptography and steganography together to hide session key inside randomly generated DNA sequence. They have used codon degeneracy to hide information inside DNA sequences without affecting the type or structure of it. There are total 64 possible codons. These codons are mapped to 20 standard amino acids. Some amino acids are coded for more than one codon. This property is called codon degeneracy. This useful characteristic can be used to change the codon's last base while keeping its type (purine or pyrimidine).In other words, this algorithm changes the third nucleotide base of the codon into pyrimidine base or purine base if the secret bit is 0 or 1 respectively. Furthermore, the extraction process can be done blindly without any need to reference DNA sequence. The overall hiding payload is 1/3 bpn. It is showed to be the only blind technique that is capable of conserving the functionality of the carrier DNA .

3. K. Menaka proposed the indexing technique to hide the secret message inside the randomly generated DNA sequence [3]. They have used three complementary rules: based on Purine and Pyrimidines, based on Amino and Keto groups, based on Strong and Weak H-bonds. Each letter in the DNA sequence is given the subscript index starting from 0.Message is converted to DNA sequence using digital coding pattern. Then the message index position in the faked DNA sequence is applied to each letter of the converted sequence. In this paper it has been pointed out that there are many properties of DNA sequences that can be utilized for encryption purposes.

4. Bama R, Deivanai S, Priyadharshini K proposed DNA sequencing which ensures secured data authorization, storage and transmission [4]. DNA Sequencing for a Electronic Medical Record System has been introduced to access the patient□s medical record securely and instantly. The Substitution approach uses two schemes which are kept secret between sender and receiver. These two schemes are binary coding scheme and complementary pair rule. The proposed scheme of DNA Sequencing is more reliable, efficient and secured.

5. Siddaramappa V introduced data security by using random function in DNA sequencing [5]. They generate random numbers for each nucleotide and performs binary addition and subtraction on binary form of message and DNA sequence. This paper focus on the data security issues for providing a secure and effective encryption and decryption method by random number keys generation.

6. Rohit Tanwar, Bhasker Sharma and Sona Malhotra introduced the robust substitution technique to implement audio steganography [6]. It is robust to various intentional and unintentional attacks and improves data hiding capacity. The basic problem to the substitution technique is identified and the possible solutions are proposed too. One problem is that they are less robust against intentional attacks and the second having low robustness against distortion. They have provided solutions to the two problems of substitution technique which is to use the deeper layer bits for embedding and other bits should be altered willingly to decrease the amount of error induced.

7. Pratik Pathak, Arup Kr. Chattopadhyay and Amitava Nag proposed new steganography technique based on location selection [7]. The position for insertion of secret bit is selected from 0^{th} to 7^{th} LSB based on upper three MSB. If length of message is n then the complexity of the algorithm is O(n). It is more secure than simple LSB technique because it provides randomness while embedding secret message bits. This scheme provides high audio quality, robustness and lossless recovery from the cover audio.

8. Muhammad Asad, Junaid Gilani and Adnan Khalid proposed enhanced Least Significant Bit (LSB) modification technique to improve conventional LSB modification method [8]. First way is to randomize bit number of host message used for embedding secret message while second way is to randomize sample number containing next secret message bit. On average, the technique embeds one secret message bit per four samples of host message. In order to make sure the secret message is embedded, the sample of host message should be eight times the number of bits of secret message.

9. Anupam Kumar Bairagi, Saikat Mondal and Amit Kumar Mondal proposed the dynamic approach to audio steganography [9]. Using this approach host message bits are embedded into deeper layer. The robustness against intentional attacks is increased. In this approach if number of 1 bits are greater than or equal to two and less than total number of bits than that sample is candidate for substitution. The bit position in the counted number and the message bit is XORed and if result is 0 then no need to substitution and if the result is 1 then substitute the bit positioned by the message bit. This proposed method increases the robustness and reduces the distortion.

10. Ankur, Divyanjali and Vikas Pareek developed a new Pseudorandom number generator that can be used for non-cryptographic application [10]. It also includes its statistical

testing result and its related proofs. The algorithm works on summation of numbers from Z_m, chosen as multiples of number from previous iteration and mapped again to Z_m. The presented algorithm is tested on NIST statistical test suite *sts-2.1.1*, containing total of 15 tests, out of which several tests are performed several times.

IV. ADVANTAGES OF DNA COMPUTATION

Microprocessors made of silicon will eventually reach their limits of speed and miniaturization. Chip makers need a new material to produce faster computing speeds. DNA might one day be integrated into a computer chip to create a so called biochip that will push computers even faster the other computing devices [12].

Advantages of using DNA based computation methods are:

- Parallel Computing
- high storage capacity and light weight
- less power consumption
- fast computations.

TABLE I: BASIC COMPARISION BETWEEN TRADITIONAL AND DNA CRYPTOGRAPHY[11]

	Traditional Cryptography	**DNA based Cryptography**
Ideal System	Silicon chip based	DNA chip based
Information Storage	Silicon computer chips	DNA strands
Storage Capacity	1 gram silicon chip carries 16 Mega-bytes	1 gram DNA carries 10^8 Tera-bytes
Processing time	Less	High
Performance Dependancy	Implementation and system configuration	Environmental conditions

V. APPLICATIONS

DNA due to its immense storage capacity and high randomness is used now in the field of steganography.DNA based algorithms can be used in various fields such as job scheduling for clusters, GPU applications, multi-core architectures, etc. Audio files are considered to be excellent carriers for the purpose of steganography due to presence of redundancy [1].

In the business world steganography can be used to hide a secret chemical formula or plans for a new invention. Steganography can also be used for corporate espionage by sending out trade secrets without anyone at the company being any the wiser. Terrorists can also use steganography to keep their communications secret and to coordinate attacks. There are a number of peaceful applications. The simplest and oldest are used in map making, where cartographers sometimes add a tiny fictional street to their maps, allowing them to prosecute copycats. A similar trick is to add fictional names to mailing lists as a check against unauthorized resellers. Most of the newer applications use steganography like a watermark, to protect a copyright on information. Photo collections, sold on CD, often have hidden messages in the photos which allow detection of unauthorized use. The same technique applied to DVDs is even more effective, since the industry builds DVD recorders to detect and disallow copying of protected DVDs [13].

VI. CONCLUSION

Communicating secretly without giving away any kind of crucial information is very important now a days in many fields. In this paper we presented some DNA based audio steganographic techniques. There are multiple carriers for hiding data such as image, audio, video etc. Audio files are considered to be excellent carrier due to redundancy.DNA (Deoxyribonucleic Acid) is the germ plasma of all life styles. A number of methods have been proposed over the last decade for encoding information using deoxyribonucleic acid (DNA), giving rise to the emerging area of DNA data embedding. There are millions of DNA sequences available publicly. So guessing the correct DNA sequence by attacker is very difficult task. Furthermore, digital coding pattern used by sender is also not known to the attacker so it increases security of secret data .Due to randomness, high storage capacity and other advantages, DNA is now used in steganography and other applications. Hence, there is a need of more new techniques in this field.

ACKNOWLEDGMENT

I am very grateful and would like to thank my guide for their advice and continued support to complete this paper and help to think beyond the obvious.

REFERENCES

[1] Shyamasree C M, Sheena Anees “Highly Secure DNA-based Audio Steganography” International Conference on Recent Trends in Information Technology (ICRTIT) IEEE 2013.

[2] Amal Khalifa“LSBase: A key encapsulation scheme to improve hybrid crypto-systems using DNA steganography ” IEEE 2013

[3]] K. Menaka“Message Encryption Using DNA Sequences ”IEEE 2014

[4] Bama R, Deivanai S, Priyadharshini K“Secure Data Transmission Using DNA Sequencing” IOSR Journal of Computer Engineering (IOSR-JCE) Volume 16, Issue 2, Ver. II (Mar-Apr. 2014)

[5] Siddaramappa V“Data Security in DNA Sequence Using Random Function and Binary Arithmetic Operations”International Journal of Scientific and Research Publications, Volume 2, Issue 7, July 2012

[6] Rohit Tanwar, Bhasker Sharma and Sona Malhotra“A Robust Substitution Technique to implement Audio Steganography ” International Conference on Reliability, Optimization and Information Technology, IEEE 2014

[7] Pratik Pathak, Arup Kr. Chattopadhyay and Amitava Nag“A New Audio Steganography Scheme based on Location Selection with Enhanced Security”IEEE.

[8] Muhammad Asad, Junaid Gilani and Adnan Khalid"An Enhanced Least Significant Bit Modification Technique for Audio Steganography"IEEE 2011

[9] Anupam Kumar Bairagi, Saikat Mondal and Amit Kumar Mondal"A Dynamic Approach In Substitution Based Audio Steganography"IEEE/OSA/IAPR International Conference on Infonnatics, Electronics & Vision , 2012

[10] Ankur, Divyanjali and Vikas Pareek"A New Approach to Pseudorandom Number Generation" Fourth International Conference on Advanced Computing & Communication Technologies,IEEE 2014.

[11] Tushar Mandge , Vijay Choudhary "A DNA Encryption Technique Based on Matrix Manipulation and Secure key Generation Scheme"IEEE.

[12] Swarnendu Mukherjee, Debashis Ganguly, Swarnendu Bhattacharya, Partha Mukherjee"A Cognitive Study on DNA Based Computation" International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009

[13] Ronak Doshi, Pratik Jain, Lalit Gupta"Steganography and its Applications in Security"International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.6, Nov-Dec. 2012 pp-4634-4638