Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 3, March 2016, pg.827 – 832

Security and Information Hiding based on DNA Steganography

Mrs. Aditi Sharma
New Delhi
s.aditi02@gmail.com

Abstract
DNA cryptography is a new field which has emerged with progress in the research of DNA computing. As a special cryptography, DNA steganography is safer than ordinal cryptography, only if the primer sequences are concealed from an adversary however this is not easy . DNA cryptography and steganography differs from the conventional cryptology in the terms that the keys and the cipher texts are all biological molecules. The security of DNA-PKC relies on difficult biological problems instead of computational problems. We have researched on how to overcome the security deficiency of DNA steganography and developed a message hiding method based on DNA steganography. We designed some procedures to encrypt a message and then decompose the cipher text into two parts. The sender uses DNA steganography to send one part. If the microdot is assumed or contaminated, the message will be encrypted and decomposed again and again until the microdot is not assumed or contaminated. If the microdot is not assumed or contaminated, the corresponding part will be publicly sent. The novelty of the proposed method is that introduced message decomposing to solve the security problem of DNA steganography.

I. Introduction

Steganography is the science of hiding a confidential message in an innocent looking container file e.g. an image in a way that does not introduce perceptible distortions to the carrier file . It helps to conceal the existence of data. By use of steganography, confidential details can be embedded in a cover file and transmitted to the intended person without creating suspicion. A successful steganographic system embeds information imperceptibly in a cover file making sure that the exact information is extractable at the other end. Biometric based authentication system makes use of personal attributes data or body data e.g. iris , dna or finger prints etc[1]. . The biometric data is not only unique to the individual concerned but it also remains throughout the individual's life span. The growth in the Information Technology industry and the continued embracing of the same in every facet of life makes it very necessary to have reliable and secure identification.

DNA steganography is a research direction of DNA cryptography, which came true in 1999 [2] Cryptography is a branch of science which studies the encoding of information for the purpose of hiding messages. The development of cryptography is strongly related to human's information-processing capabilities and computing capacities .

Biological computing (e.g. DNA computing) and quantum computing are two most promising technologies under development [3].
In this process the principle is basically to Encrypting and hiding a message in a large number of DNA strands to prevent an adversary from reading and deciphering it. If the primer sequences are kept from an adversary, DNA steganography is safer than common cryptography. However, it is not easy. If the primer sequences are all the same, the security will be weak. If the primer sequences are different every time, the management will be hard. Even worse is that it is possible for an adversary to decipher DNA steganography without the primer sequences and also the main purpose is to solve the security problem of DNA steganography.[4]

II. Elements of DNA

DNA is the abbreviation of deoxyribonucleic acid which is the germplasm of all life forms. A typical DNA molecule has two anti-parallel strands consisting four types of nucleotides (or bases), which are adenine (A), thymine (T), cytosine (C) and guanine (G). Complementary DNA strands are held together by forming hydrogen bonds between bases (base pairing) from each strand specifically with A bonding only to T and G only bonding to C. In that the double helix structure DNA was discovered by Watson[5] and Crick, . and one of the greatest scientific discoveries in the 20th century. Complementary base pairing is also the basis of DNA chip technology, called gene chip, microarray, oligo-chips or biochips. DNA chip is fabricated with *in situ* synthesized oligo nucleic acids or spotted c DNA probes. Tens of thousand DNA probes are arranged on glass or silicon matrix and numerousTens of thousand DNA probes are arranged on glass or silicon matrix and numerous labeled complementary probes are annealed on the chip to get various hybridization spectrums, revealing the genetic information. [6]
Like conventional cryptography, a biological cryptosystem also consists of the sender Alice, the receiver Bob, and the challenger Eve. Biological cryptosystem differentiates it from conventional cryptosystem as follows:

1) Instead of a copy of data, keys in biological cryptosystem are biological molecules and some other secret information, such as hybridization condition, rules of reading the information, etc.

2) The ciphertext is in the form of biological molecules, in a mixture or on a chip.

3) One obtains the ciphertext and the key physically, or in other possible way in the future, not overelectronic communication.

4) Just like conventional public-key cryptosystem, encryption key and decryption key in a biological cryptosystem are also different.

III. OVERVIEW

Biological computing (e.g. DNA computing) and quantum computing are two most promising technologies under development. However, new crypto technology does not always follow the development in novel computation technology. Since Wisner [1] first proposed the premature idea of quantum cryptology in the 1970s, the quantum cryptology has been studied for nearly 40 years. Today, quantum cryptology is still far from changing the domination of the conventional cryptology, while significant progresses have been achieved in the field of quantum communication [7–10]. Although quantum computing is also a potential threat to current cryptology, there is stila long way to go before we can implement its potential power [11,12]. On the other hand, since Adleman [13] demonstrated the first DNA computing model, 15 DNA computing conferences have been held annually, different algorithms have been proposed and the computational power in laboratory environment was expanded extensively [14–20]. In 1999, Clelland succeeded in achieving DNA steganography. According to Clelland the message can be encrypted in a DNA strand, and then the strand is flanked by polymerase chain reaction (PCR) primer sequences and further hidden in a microdot. According to the encryption key and the primer sequences, the strand can be extracted from the microdot and then the message can be read and deciphered.

IV. Encryption Process

A. Encrypting the Message to Be Sent in a DNA Strand

Here, encryption is to encrypt a message in DNA and the encryption key is not of primary importance. A simple substitution cipher can be used to encrypt characters in DNA Triplets. (Table 1).

TABLE I. ENCRYPTION KEY
A=CGA I=ATG Q=AAC Y=AAA 6=TTA
B=CCA J=AGT R=TCA Z=CTT 7=ACA
C=GTT K=AAG S=ACG O=ACT 8=AGG
D=TTG L=TGC T=TTC I=ACC 9=GCG
E=GGC M=TCC U=CTG 2=TAG =ATA
F=GGT N=TCT V=CCT 3=GCA ,=TCG
G=TTT O=GGA W=CCG 4=GAG .=GAT
H=CGC P=GTG X=CTA 5=AGA :=GCT

B. **Hiding the Strand in a Microdot**

A DNA-encrypted message is first blanketed up by the enormous complexity of human genomic DNA and then further hidden by confining this sample to a microdot. In the interest of extracting the DNA-encrypted message simply, the strand containing the encrypted message should be flanked by PCR primer sequences. For the sake of sending the microdot conveniently, the microdot is carried in an ordinary paper. Then the sender sends the paper to the intended recipient.

C. Reading and Deciphering the Message

The encryption key and the primer sequences are shared by the sender and the intended recipient beforehand. Having received the paper, the intended recipient can lightly amplify the DNA strand through PCR and then read and decipher the message.

D. Security Problem

DNA steganography is safer than ordinary cryptography in sending a message. One microdot contains a huge number of DNA strands. It is hard for an adversary to pick out the strand containing the encrypted message without the primer sequences. Researchers have worked on how to conceal the primers from an adversary. However, it is almost impossible to succeed. Tf they were to succeed one day, DNA steganography could be deciphered all the same for its potential limitations. Measures should be taken to surmount the security deficiency.

V. THE HIDING METHOD BASED ON DNA STEGANOGRAPHY

In this section, we analyze the communication process of DNA steganography, present a new hiding method to solve the security problem of DNA steganography present a new hiding method to solve the security problem of DNA steganography and explain with an example.

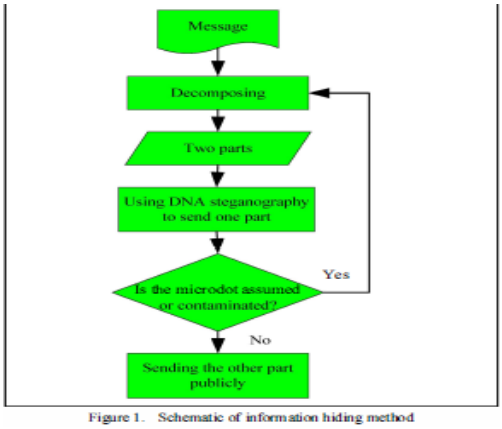

Figure 1. Schematic of information hiding method

The Communication Process of DNA Steganography

When the sender uses DNA steganography to send a message to the intended recipient, an adversary may intercept the paper containing the microdot. If an adversary intercepts the paper, the message to be sent may be read and deciphered. And then a paper containing an assumed or contaminated microdot may be sent to the intended recipient. It is easy to know that the microdot is assumed or contaminated according to the percentage of each DNA strand. If the microdot is assumed or contaminated, the message may have been read and deciphered by an adversary. If the microdot is not assumed or contaminated, an adversary does not intercept the paper and then the message is sent absolutely in secret. The communication process of DNA steganography can be utilized to send a message in private (Figure 1). The process is like that a message is decomposed into two parts and then one part is hidden in a microdot and sent. Apparently, decomposing a message should achieve the purpose that an adversary can not read and decipher the message until he or she intercepts both the two parts. If the microdot is assumed or contaminated, the process will be repeated until the microdot is not assumed or contaminated. If the microdot is not assumed or contaminated, the remaining part will be sent publicly.

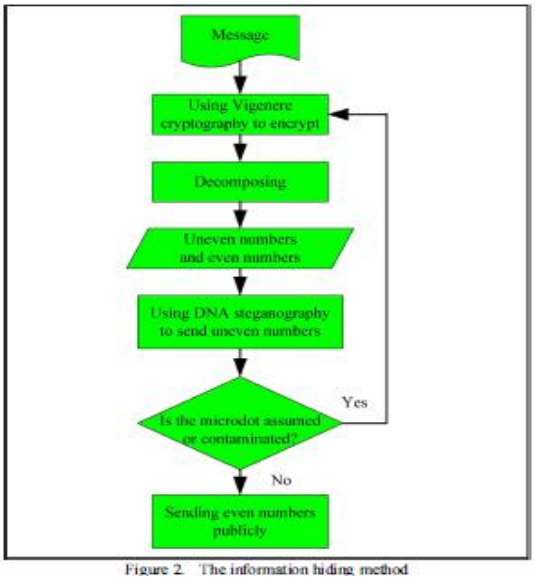

Figure 2 The information hiding method

A. The Process of Information Hiding

Having introduced the communication process of DNA steganography, we are ready to explain the proposed information hiding method (Figure 2). The steps are as follows.

- ✓ Use Vigenere cryptography to encrypt the message to be sent. As mentioned before, a message can be decomposed. into two But we can not decompose a message directly. If we did so, an adversary would get some information directly to the message as long as he or she intercepts the paper containing the microdot. Further more, if the message is decomposed many times, an adversary will get enough information to summarize the message sent to the intended recipient. In order to avoid this phenomenon, a message should be encrypted before being decomposed and the cipher texts of the same message should be different every time. Vigenere cryptography can make this lightly. So the first step is using Vigenere cryptography to encrypt a message.

- ✓ Convert the Vigenere cipher text to ASCII code. The Vigenere cipher texts are English letters. It is not very easy to decompose letters and achieve the purpose that an adversary can not read and decipher the message until he or she intercepts both the two parts. However, ASCII code

- ✓ Use DNA Steganography to send the uneven numbers into the intended recipient. If the microdot is assumed or contaminated, repeat the above steps until the microdot is not assumed or contaminated. If the microdot is not assumed or contaminated, send the corresponding even numbers publicly.

- ✓ Read and decipher the message. Decipher DNA steganography and then get the uneven numbers.

VI. Conclusions and Future scope

- The newborn DNA cryptography is far from mature both in theory and realization. Current DNA technology is still in a period of laboratory exploration and focused on experiments, while there is not a general theory about applying DNA molecules in cryptography. Also, it is a multidisciplinary area which not only demands the coupling of biological and cryptography technologies, but also requires researchers from both areas to work in a new cooperative way. As an example, some key technologies in DNA research, such as polymerase chain reaction (PCR), automatic sequencing, and DNA chip (microarray), have only been developed and well accepted in recent years. Plus, it takes time for cryptologists to fully understand them

- The DNA chip (microarray) technology is one of the most important inventions in modern biology. With this technology, the new data storing method, encoding method and reading method can be achieved in this paper. Moreover, synthesizing DNA strands is not necessary in the encryption process and sequencing DNA strands is no longer needed in the decryption process, which makes the applications like DNASC much easier to achieve.

- Due to current limitation of DNA technology it is not easy to design a cryptosystem which will replace DES or AES at once. It is still too early to do that . The aim is to show that DNA has the great potential of application in cryptography. As a future direction, DNA cryptography mig be one of the next generation's cryptography technologies.

- In DNA-PKC, DNA probes are used as keys and chips are used as ciphertexts and they are transmitted physically. Because of its biological nature, DNA-PKC is fitter for secure data storage of huge capacity, identity recognition, payment system and bioinformatics, etc. Particularly, the ciphertext in DNA-PKC are hard to replicate, which makes it possible to prevent data from being cloned and monitored. The security of the current public-key cryptosystem is based on some computationally difficult problems. These problems have long been assumed to be secure without strict proofs; therefore these cryptosystem might be threatened with super computational power in future. In contrast, the security of DNA-PKC is based on the research of genetic engineering, which provides some other possibility for security.

- In the aspect of practicality, DNA computing and DNA cryptography still cannot compete with the electronic computing technology and the mathematical cryptography. However, the DNA molecule has the potential to be used in the fields of information science.

- The study of DNA computing and the DNA cryptography are still at its early stages; thus it is too early to judge its future. However, with the development of the biotechnology, the exploration of the biological cryptography, such as DNA PKC and DNASC, will go much further, and it may have particular advantages over the conventional mathematical cryptology and the future quantum cryptology.

References

1. I. Chang, K.. W. Bowyer, and P. J. Flynn. An Evaluation of Multimodal 2D+3D Face Biometrics. IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.27, No.4, 2005, pp. 619-624.
2. C. T. Clelland, V. Risca and C. Bancroft, " Hiding messages in DNA microdots,"Science, 1999,vol. 39, pp.533-534.
3. G. Xiao, M. Lu, L. Qin and X. Lai, "New field of cryptography: DNA cryptography," Chinese Science Bulletin, 2006,vol. 51, pp.14
4. A. Gehani, T. LaBean and J. Reif ,"DNA-based Cryptography," Lecture Notes in Computer Science, 2004, vol. 2950, pp. 167-188.
5. A. Leier, C. Richter, W. Banzhaf and H. Rauhe, "Cryptography with DNA binary strands," Biosystems, 2000, vol. 57, pp. 13-22.
6. Chou C W, Laurat J L, Deng H, et al. Functional quantum nodes for entanglement distribution over scalable quantum networks. Science, 2007, 316: 1316–1320.

7. Bennett C H, Brassard G. Quantum cryptography: public-key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, India: Bangalore Press, 1984,175–179
8. G. Xiao, M. Lu, L. Qin and X. Lai, "New field of cryptography: DNA cryptography," Chinese Science Bulletin, 2006, vol. 51, pp.1413-l420.
9. M. Lu, X. Lai, G. Xiao and L. Qin, " Symmetric-key cryptosystem with DNA technology," Science China Information Sciences, 2007, vol. 50,pp. 324-333
10. Z. Chen and 1. Xu, "One-Time-Pads encryption in the tile assembly model," Bio-Inspired Computing: Theories and Applications, 2008, pp.23-30. (references).
11. Shor P W. Algorithms for quantum computation: discrete log and factoring. In: Goldwasser S, ed. Proceedings of the 35th Symposium on Foundations of Computer Science. Los Alamitos, CA: IEEE Computer Society Press, 1994. 124–134.
12. Adleman L. Molecular computation of solutions to combinatorial problems. Science, 1994, 266: 1021–1023
13. Leier A, Richter C, Banzhaf W, et al. Cryptography with DNA binary strands. Biosystems, 2000, 57: 13–22.
14. Schena M, Shalon D, Ronald W, et al. Quantitative monitoring of gene expression patterns with a complementary DNA microarray. Science, 1995, 270: 467–470.
15. Gabig M, Wêgrzyn G. An introduction to DNA chips: principles, technology, applications and analysis. Acta Biochim Polon,2001, 48: 615—622.
16. Liu Q, Wang L, Frutos A G, et al. DNA computing on surfaces. Nature, 2000, 403: 175–179
17. Roweis S, Winfree1 E, Burgoyne R, et al. A sticker based model for DNA computation. J Comput Biol, 1998, 5: 615–629
18. Gifford D K. On the path to computation with DNA. Science, 1994, 266: 993–994

