ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 7, Issue 5, May 2018

A REVIEW: SECURITY FOR DNA STEGANOGRAPHY USING HYPER ELLIPTIC CURVE CRYPTOGRAPHY

Laxmi devi[1] (laxmis4141@gmail.com)
Ms. Nishapandey[2]
Shri ram college of engineering & management (Delhi NCR), Faridabad

Abstract

Biotechnological methods can be used for cryptography to improve security of data. Steganography is the act of hiding messages inside an image.Digital communication witnesses a noticeable and continuous development in many applications in the Internet. Hence, a secure communication session must be provided. The security of data transmitted across a global network has turned into a key factor on the network performance measures. Cryptography and steganography are two important techniques that are used to provide network security.We survey a number of methods combining cryptography and steganography techniques in one system.

Keywords: Cryptography, encryption, decryption, steganography, stego-image.

I. Introduction

Steganography is originated in Greece which means "covered writing". During ancient times, steganography was used to trade personal secret messages, for sending political intelligence information [2].Here are some examples of steganography used in past, during World War II to send messages between Resistance cells, invisible ink was used by the French Resistance on couriers backs. In Greece, plain wood tablets with engraved message covered with wax were used to transmit messages. By the time tablet reached its destination, hidden message was revealed by melting the wax. But with times steganography has changed a lot. In order to send messages digital form of steganography is used these days.

Figure 1: Example of Steganography

Above example conceals message shown below. If above information is exposed to the intruder, it will not be possible to make decision whether it hides any hidden information.

Figure 2: Digital steganography message

In digital steganography message is hidden in carrier, such as photos, audio or video files, by adding or replacing bits with secret data. For transmitting sensitive personal or business information over the Web through e-mail, or through social channels such as Twitter or Facebook steganography is used because it is very hard to "crack".

Digital Carriers for Steganography

It has been noticed that digital file formats with a high degree of redundancy are best suited as carrier for steganography. As there is possibility that

duplicate bits can be substituted with secret data bits without embedded data being visually difference. Anderson and Petitcolas in [2] showed that redundant bits of an image are bits which can be altered without being detected easily. Images, Videos, Text, and Audio files have large number of duplicate data in binary form which goes with the need of steganography. Thus figure 3 shows carrier for steganography.

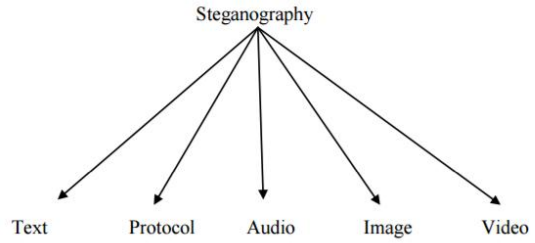

Figure 3: File formats used for steganography

Above shown file format categories make use of different data hiding techniques depending on the unique features of the file format and the delicacy of bits in the representation of the digital file [2].

Text Steganography

Data hiding in text steganography is done by making changes in the construct of the text document without making significant changes in the output. In Text steganography one text file is hidden into another text for the secure communication. Text steganography techniques are categorized into three types as shown below.

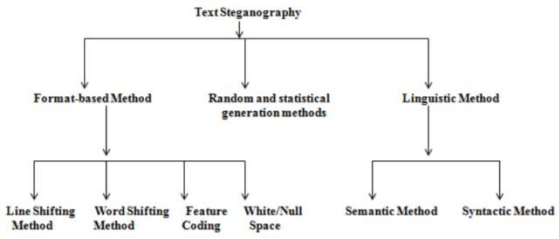

Figure 4: Categories for Text Steganography techniques

Format based

Information in format based methods is hidden using physical text formatting. No text value is changed in this type of method therefore no harm is done to the value of the cover text.

There are four types of Format Based Method:

Line shifting method: In this method, text lines are vertically shifted to fixed degree and unique structure of the text is used to hide the data. In one of the approach, the line is moved up or down, while the adjacent lines are left unmoved. These unmoved lines are used as reference locations during the decoding process. Memon in [3] showed that little variation as vertical shift of 1/300 inch up or 30 down goes un-noticed by human eye.

Word shifting method: In this method, to embed information in text, distances between the words are horizontally shifted by some value. The researchers have proved that humans while reading have tendency to accept a wide changes in text setting in one line and changes like shift of 1/150 inch horizontally go unnoticed by human eye. In this kind of method, a word is changed right, left while following adjacent words left unmoved. These unmoved words used as reference locations while extracting the data.

Feature coding: In this coding method feature of the text are selected and changed based on the message to be hidden. Alterations are done to change alphabets height or its position based on relative font of other alphabets. Changes are also done in vertical lines of the individual alphabet and the length may also be modified which cannot be noticed by the ordinary readers [3]

White/null /open space: In this method, cover message content is added with some extra white/null spaces in order to hide the secret data. At different position of cover message whitespaces are added such as end of each line, end of paragraph or sentence, between the words. This method is proved to be very secure as it does not catch reader's attention because whitespaces are added in any arbitrary text. But using this method is not used for large text messages but instead is used for very small

quantity of information to be hidden in cover document. This technique is popular and can be implemented with all kind of documents without revealing the existence of the hidden data.

II. SECURITY FEATURES

In order to run the organization effectively, several security products and policies are evaluated. The systematic way of defining the security requirements, methodologies and approaches are described by three aspects such as security services, security mechanisms and security attacks

- **Security Services**

The security service is a communication service which is provided by a system to give a specific kind of protection to system resources. The major role of security services is to enhance the security of data processing systems and information transfer of wireless systems. Many security policies are proved by security services using security mechanism. Security services includeAuthentication, Access Control, Data Confidentiality, Data Integrity, Non-Repudiation, and Availability.

- **Authentication**

The authentication service provides information about reality and reliability of both user and data. The main function of authentication service is to assure the recipients that the message is from the trusted source or not. It provides service either by authenticating the two entities during connection initiation or by authenticating the connection established between user and server to avoid unauthorized transmission and reception.

- **Access Control**

Access Control prevents the unauthorized user to utilize the resources. It permits only the user having access to the resources that is only the legitimate users.

- **Data Confidentiality**

Data Confidentiality is the protection of transmitted data from passive attacks. With respect to the content of a data transmission, several level of protection can be identified. The broadcast service protects all user data transmitted between two users over a period of time. The other aspect of confidentiality is the protection of traffic flow from analysis. This requires an attacker not to be able to detect the source and destination, frequency, length, or other characteristics of the traffic on a communication facility.

- **Data Integrity**

Data Integrity service is applied to a single message, stream of messages, or selected part of the message and provides assurance to the recipients about the originality of message. This is done by checking the characteristics of the received message for insertion, modification, duplication, reordering or replays and destruction of data.

- **Non-Repudiation**

Non-Repudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. Similarly, when a message is received, the sender can prove that the message was in fact received by the alleged receiver.

- **Availability**

It assures that the system works promptly and service is not denied to authorize users.

III. SECURITY MECHANISMS

A security mechanism is designed to detect, prevent or recover from a security attack. Examples of security mechanisms are key generation, encryption, decryption, digital signatures and authentication.

- **Encipherment**

Encipherment uses mathematical operations to transform the data into indeterminate form termed as cipher-text which is not readily intelligible. The transformation and subsequent recovery of the data depends on the algorithm and encryption keys used for transformation.

- **Digital Signature**

Digital signature is applied to a single message or stream of messages by using one's own private key.

- **Authentication Exchange**

A mechanism intended to ensure the identity of an entity by means of information exchange.

- **Traffic Padding**

The insertion of bits in a data stream to frustrate the traffic analysis attempts.

- **Routing Control**

Routing control enables the selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

- **Notarization**

The use of a trusted third party to assure certain properties of a data exchange in security.

III. LITERATURE SURVEY

Amritpal Singh, et al. (2015), [1] In this paper the author states that steganography is a method which hides the records in such a technique that it is not observable to user. Steganography has separated into numerous types like Audio, Video, Text, and Image. In case of image steganography data is secreted in arrears the image. In this covered input image is used to hide the data. The image acquired after implanting the data is recognized as stego image. Numerous approaches used for steganography are like LSB, Transform Domain, DFT and a lot of more. Entirely the methods have some advantages and disadvantages. In this paper improved LSB system is established by the author who overcomes the boundaries of other methods. LSB method for color images by inserting the data into 3 planes of Red, green, blue image in a method that improves the feature of image and attains high implanting volume. The PSNR significance of the planned system is enhanced than preceding steganography approaches.

Mehdi Hussain et al, (2013), [2]In this work the author describes steganography as a method which secures the confidential data from unauthorized user. It is used universal for the determination of securing the data while broadcast. With the increase in number of users for internet the use of the steganography is also amplified to amagnitude. It is also recognized as imperceptible communication among sender and receiver. This method deals with hiding the message presence for the determination of security. Usually the data can be entrenched in audio, video, image, sound, text etc. The request of steganography is martial communication. Steganography is also used in satisfied copyrighting. In this main in first cover image is used to insert the data behind it and next inserting the data the image developsstego image.

T. Morkel et al, [3]The states that steganography is a originality to hide the in formationafter an image, an audio, video or text. In former words it is similarly identified as the procedure of hiding the datainside other information. Numerous file organizations are used for steganography like .jpeg, .png. The digital image is other desirable for steganography due to its frequency completed the internet. There are numerousmethods for steganography. The optimal of the method is based on the wildlife of the application for which it is presence used like some application needs high level of privacy whereas particular demands for average level confidentiality in their submission. This work main attention is on proving the compatibility of the method of steganography for application and then the greatestappropriatesystem is functional to the submission for steganography.

Ushl et al. in [4] proposed an encrypting technique which combines stegnography and steganography for data hiding. The message is encrypted two times for providing data security. The cipher text is hidden inside the image. It makes use of a reference matrix in order to select passwords depending on the image properties.

Bharti and Soni [5] proposed a novel scheme to embed data in color images. This method shows its larger capacity for hiding data than other methods without loss of imperceptibility integer wavelet transform and Genetic algorithm. The method is very efficient, especially when applied to those images whose pixels are scattered homogeneously and for small data. Watada in [5], illustrate the current state of the art of DNA computing achievements and also explain new approaches or methods contributing to solve either theoretical or application problems. DNA computing approaches a new way to solve engineering or application problems. It also provides an overview of research achievements in DNA computing and touches on the achievements of improved methods. c Huang in [5] analysis the development of DNA and introduces the working principle, mathematical model using DNA molecules.

Catherine Taylor [6]suggested an indication in which data is programmed into DNA elements, and then transformed into microdots. A microdot is an extremely reduced photograph of a typewritten page. Industrialized DNA based particularly steganography technique. First done DNA encryption and before reduced it to a microdot. Simple substitution cipher is used for encryption. Because of the vast prospects of DNA nucleotides, it performances as a complex background for storage secret message. Arbitrary key is used for encryption.

Xing Wang in [7] applied computing theories in steganography which will solve many hard problems successfully. He proposes a new way to use Steganography with DNA Computing to transmit message securely and effectively. The RSA algorithm combined with DNA computing technique to encrypt and decrypt the message which requires more key size for providing same level of security as ECC.

Guozhen Xiao, Mingxin Lu, Lei Qin and XuejiaLai in [8], uses DNA or other biological macromolecules as computing hardware. It examines the possibilities of DNA computing and opens up the general molecular computation and achieves the problems faced by DNA computing technique.

Guangzhao Cui in [9] can realize several security technologies such as encryption, Steganography, signature and authentication by using DNA molecular as information medium. He introduces the basic idea of DNA computing, and then discusses the information security technology in DNA computing.

R.Poornima et al, [10] This paper is proposed that the hiding capacity for the important concern of data hiding or steganography. Steganography is a method which hides the data behind the image or audio, video etc. In this method that the original data can't be noticeable to the user. Only receiver can decrypt the data. Several methods for steganography are like audio, video, text or image. The image steganography is most widely used system for hiding data. In this methods used for this technique is alteration domain. The communication is also done by encrypting the PIN. But only sender and receiver have through the access of message

IV. Challenges in Cryptography and steganography

Information/data security is currently an essential issue in our today life. The security of private identity, individual finances is contingent on the protection of significant and unique information. Steganography is the knowledge of changing selected readable data into approximately in comprehensible setup, which is hard to decipher. In current times, stenography has accepted a new intermediate human DNA. At a time once conservative steganography has been mislaying asset to new progressive cryptanalysis, DNA steganography has new more elements of confusion and diffusion. The use of DNA classifications to encrypt data has supported the current classical encryption procedures. Thus, DNA steganography has added another dimension to conventional stenography.

V.Various method used in Cryptography and steganography

Round Least Significant Bit (R-LSB)

Instead of hiding data and damaging/altering the file, we can also hide data in data parts which are not important to the original carrier file. Every pixel of a colour image is expressed using three bytes, one for

each colour i.e. red, blue and green. Each byte consists of 8 bits. All of these 8 bits are not required to give information about the colour i.e. red, white or blue of the pixel. This makes it perfect spot to hide the secret data. Hiding data using R-LSB does not add size to the file. We can hide 3 bits of information in one pixel by replacing the R-LSB of each byte. Audio streams are even better medium to hide data. We can replace the noise and hissing in audio streams with secret data sounds.

Sequential DNA structure

Every living being, including humans, contains a molecule DNA which carries our genetic code. In 1953, Watson and Crick researched and identified molecule deoxyribonucleic acid for the first time. DNA structure is double helix which consists of two filament having four bases namely Adenine, Guanine, Cytosine and Thymine. These bases are found in combination of triplets. These filaments have a varying sequence where bases are repeated in a long and complex code. Each polymer filament is connected together with hydrogen bond. While polymer strands are formed, it will always bond with T and G will always bond with to C. A very powerful microscope is used to see a single cell of DNA molecule as strands are twisted densely together.

Researches on DNA Scientists have shown differences in human DNA with various ailments like cancer, heart disease etc. Studying DNA, we can also find differences related to different behavior, like personal ability and mental ability. Studying this emerging new field of complicated and unique code is creating wonders in medical science. Although implementation is controversial because of its consequences as it was with the development of atomic energy.

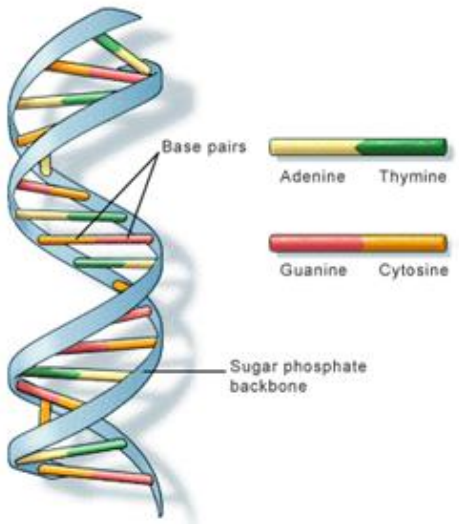

Fig 5: DNA Structure

Huffman coding

Huffman coding is a statistical coding technique, it aims to make the average code word length nearly equals to the entropy, to explain this coding technique

"This technique was developed by David Huffman as part of a class assignment; the class was the first ever in the area of information theory .The codes generated using this technique or procedure are called Huffman codes. These codes are prefix codes and are optimum for a given model "set of probabilities". The Huffman procedure is based on two observations regarding optimum prefix codes [11].

1. "In an optimum code, symbols that occur more frequently (have a higher probability of occurrence) will have shorter code words than symbols that occur less frequently".
2. "In an optimum code, the two symbols that occur least frequently will have the same length".

VI. Conclusion

In this paper, the concepts of cryptography, steganography and their applications in the security of digital data communication across network are studied. A comprehensive technical survey of recent methods which combined steganography and cryptography is presented. Combining these two

techniques is found to be more secure than applying each one of them separately.

REFERENCES

[1] Amritpal Singh, "An Improved LSB based Image Steganography Technique for RGB Images", Electrical,Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on. IEEE, 2015.,pp 1-4

[2] Mehdi Hussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology Vol. 54, May, 2013, pp 113-124

[3] T. Morkel, "AN OVERVIEW OF IMAGE STEGANOGRAPHY", ISSA. 2005, pp 1-11

[4] Usha, S., Kumar, G. A. S., and Boopathybagan, K., A secure triple level encryption method using cryptography and steganography, 0Computer Science and Network Technology (ICCSNT), International Conference,pp. 1017-1020.IEEE. 0 10000 20000 30000 40000 50000 Gray True color LSB Proposed Applied Computational Science ISBN: 978-960-474-368-1 133, Vol.2, No.2.11, 2011

[5] Bharti,P.,andSoni, R.,A New Approach of Data Hiding in Images using Cryptography and Steganography, International Journal of Computer Applications,Vol.58,No.18,pp1-5,2012.

[6] Catherine Taylor Clelland. Hiding Messages in DNA Microdots. Nature, 399:533–534, June 1999.

[7] Xing Wang and Qiang Zhang, "DNA computing-based cryptography", in the IEEE proceeding of BIC-TA '09. Fourth International Conference on Bio-Inspired Computing, Page(s): 1 - 3 , Oct. 2009.

[8] Guozhen Xiao, Mingxin Lu, Lei Qin and XuejiaLai , "New field of cryptography: DNA cryptography", in the Journal on Chinese Science Bulletin , vol.51, Issue 12 , pp.1413-1420, June 2006.

[9] Guangzhao Cui, Cuiling Li, Haobin Li and Xiaoguang Li, "DNA Computing and Its Application to Information Security Field", in the IEEE proceedings of Fifth International Conference on Natural Computation, pp.148-152, June 2007.

[10] R.Poornima, "AN OVERVIEW OF DIGITAL IMAGE STEGANOGRAPHY", (IJCSES) Vol.4, No.1,February 2013, pp 23-31.

[11] A. Ali and F. Moayad, "Arabic Text Steganography Using Kashida Extensions With Huffman Code," Journal of Applied Sciences, vol. 10, pp. 436-439, 2010.