Engineering Technology Open Access Journal

Juniper Publishers key to the Researchers

Review Article
Volume 2 Issue 5 - March 2019

Eng Technol Open Acc

Secure Cyber Network to Sharing Information through Cryptography & Stenography

Yogesh Meena[1], Rohit Kumar Verma[2], Mahipal Singh Sankhla[3]* and Rajeev Kumar[4]

[1]*Students of Bachelor of Technology Computer Science and Engineering, Galgotias University, India*

[2]*Student of B.Sc. (Hons.) Forensic Science, Division of Forensic Science, Galgotias University, India*

[3]*Research Scholar, Division of Forensic Science, Galgotias University, India*

[4]*Associate Professor, Division of Forensic Science, Galgotias University, India*

Submission: January 22, 2019; **Published:** March 12, 2019

***Corresponding author:** Mahipal Singh Sankhla, Research Scholar, Division of Forensic Science, SBAS, Galgotias University, Greater Noida, India

Abstract

In this digital era the Information is our main assets. We have to keep secure our information and data, so we use different techniques to secure our data. Information transmits through various channels and this channel must be secure. To secure our information we use different techniques like stenography and cryptography. In this technique we hide original message by using encryption to secure our information and then use decryption to retrieve our original message. Lack of awareness has caused for such cryptography and stenography to people don't secure information and hacker are change information and read the information or data to commit crimes have been overlooked and treated as a major threat. In this review paper we mainly discuss cryptographic and Stenography various method to secure data or information.

Keywords: Digital; Cryptographic; Stenography; Security; Information

Introduction

Through the past few years there is an incredible change in information and communication technology. So, security in communication over internet has become a worry. Network security complications can be categorized roughly into four parts: secrecy, authentication, non-repudiation and integrity control [1]. Secrecy or Confidentiality concerns with keeping the data away from the unauthorized manipulators. That means unauthorized users should not be able to read and recognize the data [2]. Authentication supports to confirm the exact uniqueness of sender of the message. Attacker can pose as a diverse user and may attempt to connect with the target and try to gain the serious info [3]. Non-repudiation the sending and receiving parties of the information or data should guarantee that both identify about the interruption in sending and receiving of the data or information [4]. Integrity denotes to the honesty of information or resources [5]. An absence of integrity outcomes in dishonesty: when an approved party collects incorrect information and trusts it to be correct [6]. Integrity in CPS can therefore be observed as the capability to uphold the operative goals by preventing, detecting, or surviving deception attacks in the data sent and received by the sensors, the regulators, and the actuators [7] (Figure 1).

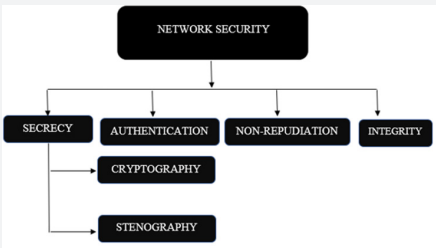

Figure 1: Classification of Network Security [2].

Types of Attacks

"Passive attack" when a network intruder intrudes data roaming concluded the network, and "Active attack" in which an intruder initiates instruction to interrupt the network's steady operation [8]. Cryptography is the science of securing data and analysing and breaking the secure communication is known as cryptanalysis [9].

Cryptography

Science of secret writing is known as cryptography. Through 3000 BC the public of Greece and Egypt used this art of confidential writing. The initial term of cryptography was hieroglyphics

derived from the Greek word "hieroglyphica" which means- sacred carvings. Later on, it was retitled as cryptography [10]. This process is the art of secret writing, which is used to encrypt the plaintext with a key into ciphertext to be transferred between parties on an uncertain network. Using an effective key, the ciphertext can be decrypted to the original plaintext. Without the information of the key, no one can retrieve the plaintext. Cryptography plays an important part in several services, alike: confidentiality, key exchange, authentication and non-repudiation. Cryptography runs these services for secure communication across insecure networks [11].

Classification of cryptography

Cryptographic algorithms can be classified as the number of keys used as. Figure 2 as shown below [12]

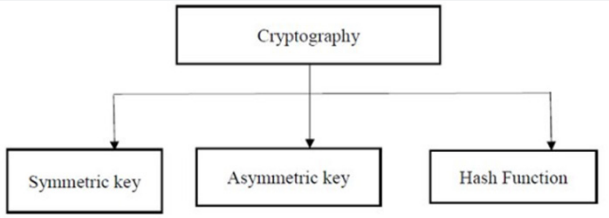

Figure 2: Types of Cryptography [12].

Basic terms used in cryptography

Plain text: The original message that the person needs to communicate with the other is defined as Plain Text. In cryptography the real message that has to be send to the other end is given a different name as Plain Text. For example, Alice is a person wants to send "Hi how are you" message to the person Bob. Here "Hi how are you" is a plain text message [13].

Cipher text: The message that cannot be understood by anybody or worthless message is what we call as Cipher Text. In Cryptography the original message is altered into non-readable message before the transmission of real message. For example, "Ajd672#@91ukl8*^5%" is a Cipher Text shaped [13].

Encryption: A procedure of transformed Plain Text into Cipher Text is termed as Encryption. Cryptography performs the encryption method to send close messages through an insecure network. The method of encryption requires two things- an encryption algorithm and a key. An encryption process means the method that has been used in encryption. Encryption takes place at the source side [13].

Decryption: A converse method of encryption is called as Decryption. It is a process of translating Cipher Text into Plain Text. Cryptography uses the decryption method at the receiver side to get the original message from non-readable message (Cipher Text). The process of decryption involves two things- a Decryption process and a key. A Decryption process means the method that has been used in Decryption. Usually, the encryption and decryption process are same [13].

Key: A Key is a numeric or alpha numeric script or may be a different sign. The Key is used at the period of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very significant since the security of encryption process depends directly on it. For example, if the Alice uses a key of 3 to encrypt the Plain Text "President" then Cipher Text produced will be "Suhvlghqw" [13].

Symmetric encryption or secret key cryptography

In symmetric Cryptography the key used for encryption is like to the key used in decryption. Thus, the key spreading has to be made prior to the spread of data. The key plays a very vital role in symmetric cryptography since their security directly depends on the nature of key i.e. the key length etc. There are many symmetric key algorithms for example DES, TRIPLE DES, AES, RC4, RC6, BLOWFISH [14,15] (Figure 3).

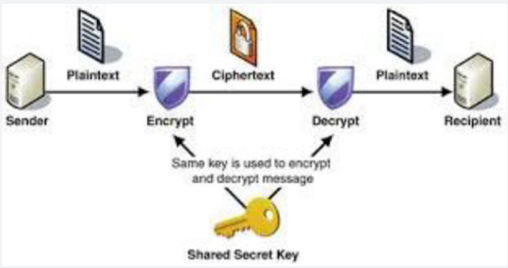

Figure 3: Symmetric key encryption process [15].

Asymmetric / public key cryptography:

The asymmetric cryptosystem (or public key cryptosystem), services two keys that are mathematically associated, use distinct for the encryption and decryption of information. Figure 4 shows the working steps of this process [11].

In this method with the single key, it is not likely to access the data or simply determine the other key. The both of keys are mandatory for the process to work. The key used for encryption is kept public and so named as public key, and the decryption key is kept secret and called private key. The keys are created in such a way that it is impossible to create the private key from the public key. Few examples of Asymmetric-Key Algorithms are RSA, Diffie-Hellman, Digital Signature Algorithm (DSA), Public-Key Cryptography Standards (PKCS), Key Exchange Algorithm (KEA) etc. [11,16] (Figure 4).

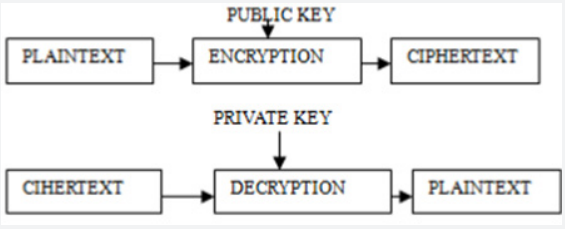

Figure 4: Symmetric key encryption process [16].

How to cite this article: Yogesh M, Rohit K V, Mahipal S S, Rajeev K. Secure Cyber Network to Sharing Information through Cryptography & Stenography. Eng Technol Open Acc. 2019; 2(5): 555598

Hash functions

A hash function is a one-way collision-free function with a fixed-length output. Hash functions are also named as message digests. A hash function is a process that does not use any key. However, a fixed-length hash value is compute based on the input information such that it computationally infeasible to get the input information from the hash value, or even any input string that matches the certain hash value. Hash functions are generally used to produce digital fingerprints of records and to promise the truthfulness of the records [11].

Stenography

Steganography is a method for hidden communication. This is attained by hiding data inside added data, thus hiding the existence of the linked data. The term steganography is resulting from the Greek words "stegos" means "cover" and "grafia" means "script". The knowledge and exercise of hiding data has a lengthy past. In Greece monarchs used to send info to their friend monarchs by script the letter on the head of a reliable soldier. During world war-2 steganography was used as a way of invisible communication. In modern steganography image, audio and video files are used as steganography carriers [17]. Steganography is the method of inserting hidden messages /information in such a way that nobody can perceive the existence of the messages, except the sender and planned receiver(s). The chief goal of steganography is to hide the secret message or info in such a way that nobody is able to perceive it. If they found any suspicion data, then goal is defeated [18].

The basic model of steganography comprises of three mechanisms

The carrier image: The carrier image is also named as cover object that will carry the note/information which is used to be concealed [2].

The message: A message can be everything like information, folder or image etc. [2].

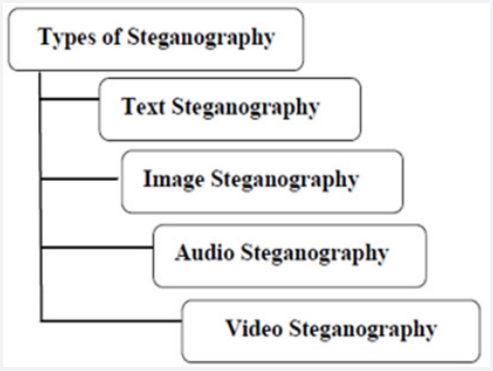

Figure 5: Types of Stenography [2].

The key: A key is used to decrypt/read the unseen message [2] (Figure 5).

Text stenography

Text steganography is the most complex stenography: this is typically due to the absence of a redundant data in a text file, which is not a problem in a image of sound or image file. The building of a text file is relatively close to what is visually detected, while other media cover types (audio, picture, video) vary from what we really see, which makes hiding data in them a lot easier than hiding it in a text cover type. The benefit of text steganography is its requirement for lesser memory and simpler communication, permitting it to send more data and lessening printing expenses [19]. It is also extremely trusting on linguistic, as each possess unique characteristics. For example, the symbols in English is not reliant on its relative place in a word, while Persian/Arabic letters display diverse forms created on the place of its symbols [20].

Image stenography

As the name suggests, Image Steganography refers to the process of hiding data within an image file. The image selected for this purpose is called the cover-image and the image obtained after steganography is called the stego-image [21]. Image Steganography is generally more preferred media because of its harmlessness and attraction. Image Steganography may classify according to working domain: (a) Spatial domain and, (b) Frequency domain. Spatial domain Steganography work on the pixel value directly and modify the pixel gray-value [22]. In Frequency domain-based methods [23], images are first transformed into the frequency domain and then message are embedded in the transform coefficients [24].

Audio stenography

Audio steganography method uses the audio file as a host (cover) file in inserting which is not simple and can be measured as a challenge due to the sensitivity of Human Auditory System (HAS). HAS senses the difference of audio file over a range of power larger than one billion to one and range of frequencies larger than one thousand to one. However, it has holes and a large dynamic range can contribute to information hiding (Bender *et al*., 1996). Audio files make suitable cover file for hiding because of its high level of redundancy and high data program rate in adding to the big size in contrast with other multimedia files. Somemethods are discussed later [25].

Video stenography

Although different multimedia files are used as carrier to protect information over internet. But among all methods, Video steganography has overcome various problems like imperceptibility, capacity, robustness. A video is a consecutive arrangement of fast-moving pictures and audio clips. Thus, it is very hard for attackers to disclose secret information without analyzing each single frame of video. Using this method, a usual property of human beings can be exploited due to dynamic nature of the video, it decreases the probabilities of secret message recognition in distinction with image steganography [26,28]. Video steganography

How to cite this article: Yogesh M, Rohit K V, Mahipal S S, Rajeev K. Secure Cyber Network to Sharing Information through Cryptography & Stenography. Eng Technol Open Acc. 2019; 2(5): 555598.

is extension of image steganography, but there is chief difference between threats on both for example, lossy compression, presentations update, increased or decreased frame rate, adding or removing of frames during video processing. Above all, inserting capacity in video is very high [26].

There are many kinds of methods used for video steganography. On basis of payload capacity, these are classified into following types [27,28].

a) Spatial Domain Techniques.

b) Transform Domain Techniques (Table 1).

Table 1: Comparison between Steganography and Cryptography [11].

S.no.	Context	Steganography	Cryptography
1	Host Files	Image, Audio, Text, etc.	Mostly Text Files
2	Hidden Files	Image, Audio, Text, etc.	Mostly Text Files
3	Result	Stego File	Cipher Text
4	Type of Attack	Steganalysis: Analysis of a file with an objective of finding whether it is stego file or not.	Cryptanalysis
5	Objectives	Keeping the existence of a message secret	Keeping the contents of a message secret
6	Applications	Used for securing information against potential eavesdroppers	Used for securing information against potential eavesdroppers
7	Security services offered	Confidentiality, Identification, Authentication	Confidentiality, Data Integrity Identification and authentication Non-repudiation
8	Technology specific problems	Steganalysis, Key distribution (except with keyless steganography	Key distribution, Law enforcement Cryptanalysis

Discussion

Nowadays internet is used by every person, government organization and various agencies and due to this some mischievous organization and persons try to leak information. The currently cybercrime plays major role in our society. Sharing information and data should be secure while sharing information. So, to secure information we use different Network Security. To secure information, we need to encrypt/decrypt data by using cryptography and Stenography. Both are art of hiding information through different techniques. Cryptography mean secreting the content of the data by encipherment. Stenography means covering the message itself by hiding it with something else. This both techniques are also used in information security. The importance of this techniques used to send confidential reports to investigation and government agencies by encrypting data.

Conclusion

Cryptography alter the arrangement and presentation of the information that cannot be understand by any unknown person. Steganography is the method of insert concealed messages / data in such a way that nobody can perceive the existence of the information, excepting the sender and intended receivers. Both techniques are very beneficial and secure data to achieve secrecy message. In Future, this method can be improved to embed secret data and hidden more information. This review paper is mainly focus on the all major methods given by different researchers are explain very briefly.

References

1. Tanenbaum AS (2006) Computer Networks, Fourth Edition, Pearson Education.
2. Babita EB, Er G K (2017) A Review: Network Security Based On Cryptography & Steganography Techniques. International Journal of Advanced Research in Computer Science 8(4).
3. Gupta B, Agrawal DP, Yamaguchi S (2016) Handbook of research on modern cryptographic solutions for computer and cyber security IGI Global.
4. Uma M, Padmavathi G (2013) A Survey on Various Cyber Attacks and their Classification IJ Network Security. 15(5): 390-396.
5. Bishop M (2003) Computer Security, Art and Science Addison-Wesley.
6. (2000) N W Group Internet security glossary.
7. Cardenas AA, Amin S, Sastry S (2008) Secure control: Towards survivable cyber-physical systems In Distributed Computing Systems Workshops. 2008 ICDCS'08 28th International Conference IEEE, pp. 495-500.
8. Pawar MV, Anuradha J (2015) Network security and types of attacks in network. Procedia Computer Science 48: 503-506.
9. Anjali Arora (2012) A Survey of Cryptanalytic Attacks on Lightweight Block Ciphers. International Journal of Computer Science and Information Technology & Security 2(2).
10. Bhaskar SM, Ahson SI (2008) Information Security A Practical Approach. Narosa Publishing House, India.
11. Kumar P, Sharma VK (2014) Information security based on steganography & cryptography techniques. A review International Journal 4(10).

How to cite this article: Yogesh M, Rohit K V, Mahipal S S, Rajeev K. Secure Cyber Network to Sharing Information through Cryptography & Stenography. Eng Technol Open Acc. 2019; 2(5): 555598

12. Shankar M, Akshaya P (2014) Hybrid Cryptographic Technique Using RSA Algorithm and Scheduling Concepts. International Journal of Network Security & Its Applications 6(6): 39.

13. Agrawal M, Mishra P (2012) A comparative survey on symmetric key encryption techniques. International Journal on Computer Science and Engineering 4(5): 877.

14. Salama D, Elminaam A, Mohamed H, Kader A, Hadhoud MM (2008) Performance Evaluation of Symmetric Encryption Algorithms. International Journal of Computer Science and Network Security 8(12): 280-286.

15. Saranya K, Mohanapriya R, Udhayan J (2014) A review on symmetric key encryption techniques in cryptography. International Journal of Science, Engineering and Technology Research 3(3): 539-544.

16. Sharma N (2017) A Review of Information Security using Cryptography Technique. International Journal of Advanced Research in Computer Science 8(4).

17. Swain G, Lanka S K (2012) A quick review of network security and steganography. International Journal of Electronics and Computer Science Engineering 1(2): 426-435.

18. Rahmani KI, Arora K, Pal N (2014) A Crypto-Steganography: A Survey. International Journal of Advanced Computer Science and Applications 5(7).

19. Memon AJ, Khowaja K, Hameedullah K (2008) Evaluation of Steganography for URDU /ARABIC. Journal of Theoretical and Applied Information Technology.

20. Shahreza MS, Shahreza MH (2008) An Improved Version of Persian/ Arabic Text Steganography Using "La" Word" Proceedings of IEEE. 2008 6th National Conference on Telecommunication Technologie.

21. https://wwwgeeksforgeeksorg/computer-network-image-steganography/.

22. A Westfield (2001) F5- A steganographic algorithm: High capacity Despite Better Steganalysis. Proceeding of 4th Int Information Hiding Workshop 21(37).

23. Cox I, Kilian J, Leighton T, Shamoon T (1997) Secure spread spectrum watermarking for multimedia. IEEE Transaction on Image processing 6(12): 1673-1687.

24. Karthik JV, Reddy BV (2014) Authentication of secret information in image stenography. International Journal of Computer Science and Network Security 14(6): 58.

25. Ali AH, George L (2016) A review on audio steganography techniques. Research Journal of Applied Sciences, Engineering and Technology 12(2): 154-162.

26. Mstafa RJ, Elleithy KM (2015) A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes. International journal of Multimedia Tools and Applications 75(17): 10311-10333.

27. Baby D, Thomsa J, Augustinea G, Georgea E, Michael NR (2015) A Novel DWT based Image Securing Method using Steganography. International Conference on Information and Communication Technologies, Procedia Computer Science 46: 216-218.

28. Ramalingam M, Mat NA (2014) A steganography approach for sequential data encoding and decoding in video images. International Conference on Computer, Control, Informatics and Its Application, pp. 120-125.

How to cite this article: Yogesh M, Rohit K V, Mahipal S S, Rajeev K. Secure Cyber Network to Sharing Information through Cryptography & Stenography. Eng Technol Open Acc. 2019; 2(5): 555598.