ISSN No. 0976-5697

Volume 8, No. 4, May 2017 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Review: Network Security Based On Cryptography & Steganography Techniques

Er. Babita[1]
M.tech Scholar, Deptt.of CSE[1]
Sant Baba Bhag Singh University[1]
Jalandhar, India[1]
babitakapoor405@gmail.com[1]

Er. Gurjeet Kaur[2]
Assistant Professor, Deptt. of CSE[2]
Sant Baba Bhag Singh University[2]
Jalandhar, India[2]
gurjeetminhas@gmail.com[2]

Abstract: **The communication technology is very advanced in these days. Digital Communication has become very important to secure the transmission of information between sender and receiver. Security is very important feature for exchange the information because it secures the information from intruders. In this paper we present a hierarchy of network security techniques such as: Secrecy, Authentication, Non-repudiation and Integrity control. There are two popular security mechanisms, namely Cryptography and Steganography. Both are well known and widely used techniques. Cryptography is used for send the data in encrypted form with using the encryption key. Encrypted data is transmitted from insecure public media. In which Decryption algorithm is also used for decrypt the message while using the decryption key. Steganography is used for hiding the data into another cover media.**

Keyword— Cryptography,Decryption, Encryption,Network Security, Steganography,.

I. INTRODUCTION

The transmission of information through internet may include sensitive personal data which may be attacked by intruders.. Also, there are many applications on the internet and many web sites which are require the user to fill the form which may include the sensitive personal data. User may need private and secure communication for many reasons such that protect their information from intruders who always wait for attack on sensitive data. So confidentiality and data integrity are required to protect the information against unauthorized access and use. Network security problems can be categorized into four parts: Secrecy, Authentication, Non-repudiation and integrity control [1]. Secrecy or Confidentiality concerns with keeping the information away from the unauthorized users. That means unauthorized users should not be able to read and understand the information.

Authentication means any party which may be sender or receiver can verify that the other party is who he or she claims to be, i.e., validate the identity of the other party.

Non-repudiation means the sender cannot deny having sent a given message. i.e., if a transaction has occurred between two parties, the non-repudiation service can prove that for any party, he/she really performed the transaction him/herself, not by any other person.

Integrity means the receiver can confirm that a message has not been altered during transmission, i.e., protect the information from tampering.

1. SECURITY REQUIREMENTS FOR TRANSMITTING INFORMATION:

*a) Confidentiality:*The information should be readable only by the intended receiver. i.e., protect the information from eavesdropping. There are two main techniques to achieve the security: Cryptography and Steganography. Cryptography is the science of secret or hidden writing of information. It has two main components: Encryption and Decryption. Cryptography algorithms are of two types: Public key cryptography and symmetric key cryptography. Steganography is a technique of covert communication in which the intruder cannot suspect that communication is going on. In steganography the secret information is hidden inside another file without affecting the quality of that file such that the intruder will not suspect that any communication is happening. The carrier file or cover file can be an image, audio, video or text file [2].

b) Authentication: Authentication means the process of identifying an individual based on a username and password. In security systems, authentication, which is the process of giving individuals access to system objects based on their identity. Authentication ensures that the individual is who he or she claims to be, but says nothing about the access right of the individual [2].

*c) Non-repudiation:*Non-repudiationis the assurance that someone cannot deny something. Typically, non-repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated [2].

d) Data integrity: Data integrity, in the context of networking, refers to the overall completeness, accuracy and consistency of data. Data integrity must be imposed when sending data through a network. This can be achieved by using error checking and correction protocols [2].

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

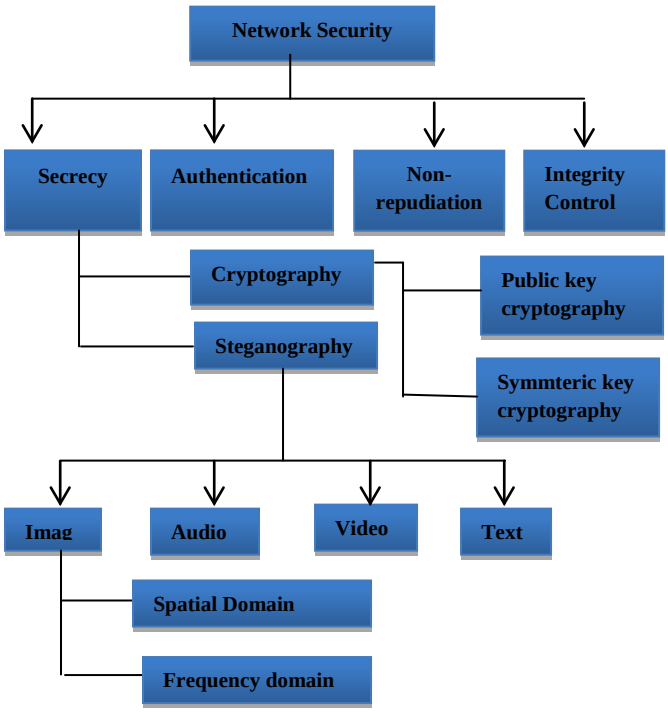

Fig-1: Classification Of Network security algorithm

A. CRYPTOGRAPHY:

Cryptography is the art of achieve the security by encode the messages to make them non-readable. Cryptography is an art of transmitting the data safely over the Internet by applying some cryptographic algorithms so that it will be difficult for intruders to attack some confidential or private information. Two basic terms used in cryptography are encryption and decryption; encryption process is the process of converting plain text into cipher text and decryption process is the reverse process of encryption. Plain text is the text which have the original message or data which is not encrypted and cipher text is the text which is ready to be sharedafter encryption of message. A key is needed for both encryption and decryption of the message [3].

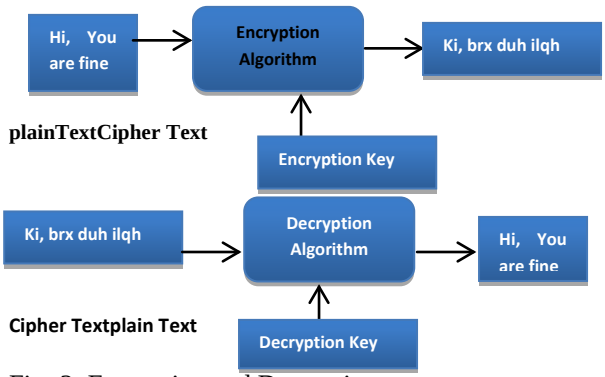

Fig -2: Encryption and Decryption

Plaintext - Unscrambled information to be transmitted. It could be a simple text document, a credit card number, a password, a bank account number, or sensitive information such as personnel information, or a secret formula being transmitted between organizations.

Cipher text- Represents plain text rendered unintelligible by the application of a mathematical algorithm. Cipher text is the encrypted plain text that is transmitted to the receiver.

Key-A mathematical value, formula, or process that determines how a plaintext message is encrypted or decrypted. The key is the only way to decipher the scrambled information.

Cryptographic Algorithm – A mathematical formula used to scramble the plain text to yield cipher text. Converting plain text to cipher text using the cryptographic algorithm is called encryption, and converting cipher text back to plain text using the same cryptographic algorithm is called decryption. Figure 1 depicting the tactic of cryptography.

Broadly cryptographic algorithms can be divided into two categories:

- **Stream algorithms–** Operate on plaintext one byte at a time, where a byte is a character, number, or special character. The process is inefficient and slow.
- **Block algorithms –** Operate on plaintext in groups of bytes, called blocks (hence the name block algorithms or block ciphers). Typical block sizes for modern algorithms are 64 bytes, small enough to work with but large enough to deter code breakers. Unfortunately, with the current speed of microprocessors, breaking a 64-byte algorithm using brute force is proving to be to relatively easy task.

1.TYPES OF CRYPTOGRAPHY:

*a) Secret Key Cryptography:*This algorithm is also known as Secret Key cryptography, where the sender and the receiver use the same keys to encrypt and decrypt the message. The algorithms known as the symmetric-key algorithm which is used for symmetric-key cryptography. The symmetric algorithms are classified into two types: stream cipher and block cipher. The stream cipher algorithms which are designed to accept a crypto key and a stream of plaintext which are use to produce a stream of cipher text. The block cipher algorithms operate on blocks of data where, the plaintext is broke into blocks and operates on every block independently.
List of Symmetric Algorithms:

- Data Encryption Standard(DES)
- Advanced Encryption Standard (AES)
- Triple Data Encryption Standard
- Blowfish Encryption Algorithm
- International Data Encryption Algorithm

*b) Public-Key Cryptography:*In the Public Key Cryptography, each user generates two keys: One is a Public key used by anyone for encrypting messages to be sent to the user and a

Private key which the user needs for decrypt the messages. List of Public- key Algorithms:

- Diffie-Hellman
- RSA
- DSA etc

*c) Hash Functions:*Hash functions use a mathematical transformation to irreversibly encrypt information. The primary application of hash functions in cryptography is message integrity. The hash value provides a digital fingerprint of a message's contents, which ensures that the message has not been altered by an intruder, virus, or by other means. Hash algorithms are effective because of the extremely low probability that two different plaintext messages will yield the same hash value. [4]
There are several well-known hash functions in use today:

- Hashed Message Authentication Code (HMAC)
- Message Digest 2 (MD2)
- MD4
- MD5
- Secure Hash Algorithm (SHA)

2. ADVANTAGES AND DISADVANTAGES OF CRYPTOGRAPHY:

a) Advantages:

- It hides the message and your privacy is safe.
- No one would be able to know what it says unless there's a key to the code.
- You can write whatever you want and however you want (any theme any symbol for the code) to keep your code a secret.
- You are able to use cryptography during lessons without the teacher knowing.

b) Disadvantages:

- Take a long time to figure out the code.
- It takes long to create the code.
- If you were to send a code to another person in the past, it will take long to get to that person.
- Overall it's a long process.

B. STEGANOGRAPHY:

Steganography is the technique of embedding hidden messages /data in such a way that no one can detect the existence of the messages, except the sender and intended receiver(s). The main aim of steganography is to hide the secret message or information in such a way that no one is able to detect it. If they found any suspicion data, then goal is defeated [3]. The various types of data in steganography can be audio, video, text and images etc. The basic model of Steganography consists of three components:

The Carrier image: The carrier image is also called the cover object that will carry the message/data which is used to be hidden.
The Message: A message can be anything like data, file or image etc.
The Key: A key is used to decode/decipher the hidden message.

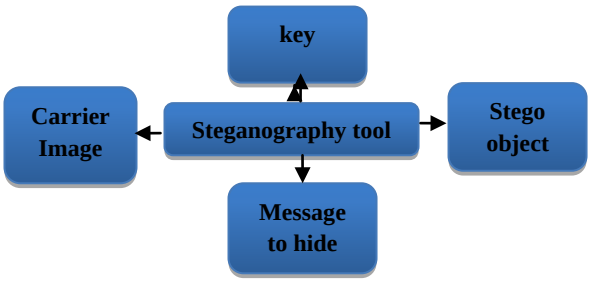

Fig. 3 Basic Model Of Steganography

1. TYPES FOR STEGANOGRAPHY:

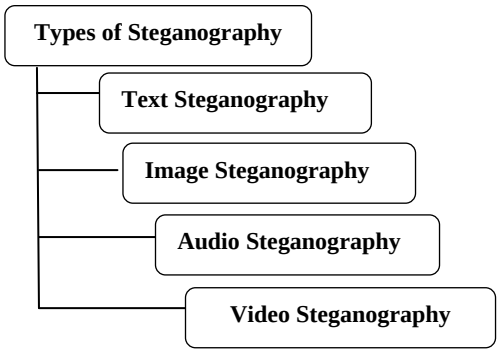

Fig-4:TechniquesOf Steganography

*a) Text Techniques:*The Steganography uses the text media to hide data known as text Steganography. It hides the text behind the other text file [5]. There are many techniques to embed the secret data in text files.

- Format Based Method
- Random and Statistical Method
- Linguistics Method

*b) Image Techniques:*In this method, images are used as cover object. Steganography is a two-step process: 1) Creating a stego image which is the combination of message and carrier. 2) Extracting the message image from the stego image. [6] In the image Steganography method, data hiding method can be classified into different categories.

- Spatial domain
- Frequency domain
- Masking
- Filtering

*c) Audio Steganography***:**When secret data is the embedded into sound which act as cover media, the technique is known as audio steganography. This method is embeds the secret message in WAV, AU and MP3 sound files. [7]. There are the different methods through which audio steganography are:

- Low Bit Encoding
- Phase Coding
- Spread Spectrum
- Echo hiding

d) Video Steganography: This technique is used for mixing of sound and image and sends it together in combine form over the transmission medium.There are different techniques to embed secret data in video:

- Least Significance Bit
- Spread Spectrum
- discrete cosine Transform
- Non-uniform rectangular partition
- Compressed video steganography
- Masking and filtering

II. STEGANOGRAPHY TECHNIQUES:

*a) Spatial Domain methods***:** These methods directly changed some bits in the image pixel values of hiding data. There are various spatial domain methods such as (i) Least significant bits(LSB) (ii) Pixel values differencing (PVD) (iii) Edges based data embedding method (EBE) (iv) Pixel intensity basedLSB

b) Transform Domain techniques: In this technique, the secret data is embedded in the transform or frequency domains of the cover object.In this many different algorithms and transformations are used for hiding information in an image. This technique is more robust and complex. There are some transform domain techniques such as (i) Discrete Fourier transformation technique (DFT), (ii) Discrete cosine transformation technique (DCT), (iii) Discrete wavelet transformation technique (DWT).

*c) Masking and Filtering:*The technique in which secret data/message is hidden in the more significant areas by marking an image. This method is more robust than LSB method. The main limitation of this technique is that this method can be applied only to gray scale images and 24 bits images.

3. ADVANTAGES AND DISADVANTAGES OF STEGANOGRAPHY:

a) Advantages:

- Difficult to detect and only receiver can detect.
- It can be done faster with large no. of software.
- Provides better security for sharing data in LAN, MAN and WAN.

C. DIFFERENCE BETWEEN CRYPTOGRAPHY AND STEGANOGRAPHY:

Table-1: Difference between cryptography and steganography

Steganography	Cryptography
Unknowing message passing	Knowing message passing
Steganography prevents discovery of the very existence communication	Encryption prevents an unauthorized party from discovering the contents of a communication
Little known technology	Common technology
Technology still being developed for certain formats	Most of algorithm known by all
Once detected message is known	Strong current algorithms are currently resistant to attack, larger expensive computing power is required for cracking
Steganography does not alter the structure of the secret message	Cryptography alter the structure of the secret message

III. CONCLUSION

In this paper we presented a classification/ hierarchy of network security techniques. Due to increasing demand for privacy and security, a need for various data hiding techniques which lead to the development of several techniques for embedding and extraction. we have discuss about the all the techniques of cryptography and steganography. Both are well known and widely used techniques. Both are very useful and secure techniques to achieve secrecy communication. If both the techniques: cryptography and steganography is combined used then the communication becomes double secured.

REFERENCES

[1] Marwa E. Saleh , Abdelmgeid A. Aly, Egypt Fatma A. Omara,"Data Security Using Cryptography and Steganography Techniques" in (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 6, 2016

[2] Gandharba Swain, "A Quick review of Network Security and Steganography" in (ijecse) International Journal of Electronics and Computer Science Engineering , ISSN: 2277-1956

[3] Md. Khalid Imam Rahmani and KamiyaArora, Naina Pal, "A Crypto-Steganography: A Survey in" in (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 7, 2014

[4] ShyamNandan Kumar, "Review on Network Security and Cryptography" in International Transaction of Electrical and Computer Engineers System, 2015, Vol. 3, No. 1, 1-11

[5]Rakhi1, Suresh Gawande2 "A REVIEW ON STEGANOGRAPHY METHODS", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 10, October 2013

[6] VidhyaSaraswathi, Mrs.SumathyKingslin, (Associate Professor)" Different Approaches to Text Steganography: A Comparison", International Journal of Emerging Research in Management &Technology (Volume-3, Issue-11)

[7] HilalAlmara'beh "Steganography Techniques - Data Security Using Audio and Video", International Journal of Advanced Research in Computer Science and Software Engineering Volume 6, Issue 2, February 2016
[8]Vishnu S babu and Prof. Helen KJ, "A study on combine cryptography and steganography" in IJRSCSE International Journal of Research Studies in Computer Science and Engineering, Volume 2, Issue 5, May 2015, PP 45-49
[9]NitinKaul and Nikesh Bajaj, "Audio in Image Steganography based on Wavelet Transform" in International Joural of Computer Applications (0975-8887), October 2013.
[10] Vijay Kumar and Dinesh Kumar, "Digital Image Steganography Based on Combination of DCT and DWT" inSpringer-Verlag Berlin Heidelberg, pp. 596–601, 2010.
[11] Vijay Kumar and Dinesh Kumar, "Digital Image Steganography Based on Combination of DCT and DWT" in Springer-Verlag Berlin Heidelberg 2010, pp. 596–601.
[12] Divya.Aynapur, S.Thenmozhi, "A SECURE STEGANOGRAPHY APPROACH OF MULTIPLE SECRET IMAGES USING ANN" in @IJRTER-2016
[13] A.E.Mustafa, A.M.F.ElGamal, M.E.ElAlmi, Ahmed.BD, "A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit" in Research Journal Specific Education Faculty of Specific Education Mansoura University Issue No. 21, April. 2011
[14] Harshitha K M and Dr. P. A. Vijaya , "secure data hiding algorithm using encrypted secret message" in International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012.
[15] Hemang A. Prajapati, Dr. Nehal G. Chitaliya, "Secured and Robust Dual Image Steganography: A Survey" in International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 1, January 2015
[16]AartiMehndiratta, "Data Hiding System Using Cryptography & Steganography: A Comprehensive Modern Investigation" in International Research Journal of Engineering and Technology (IRJET), Volume: 02 Issue: 01 | Apr-2015
[17] PiyushMarwaha, PareshMarwaha ,"Visual Cryptographic Steganography in Images" in proceedings of Second International conference on Computing, Communication and Networking Technologies, pp 1-6, 20104.