A Comparative Study of Cryptography, Steganography & Watermarking

Latika
M-Tech Scholar
PIET College, Panipat, India
latikaraheja01@gmail.com

Abstract- In this era of technology, the interpretation of transferring the data from one end to another via a conventional methods is been alternated due to the evolution of hyperspace. The advancements in the field of information and technology have produced the best outputs but problem lies in the security and integrity of data. There are various applications which are available on internet for communication but one or the other lacks in providing a secure way to transfer the data from source to destination. As an effect, the security of data from an unauthorized access or from unauthorized person has become a major objective. This issue lead to the development of various techniques for hiding data. Various popular techniques available are Steganography, Cryptography and Watermarking.

Index Terms: Steganography, Cryptography, Watermarking, public key cryptography, hash functions, private key cryptography

Introduction

With the advancement of technologies, the security is the main issue in the process of communication. In any form of communication, the terms like security, reliability, and robustness are a common issue. The extensive use of internet for communication increases the challenges of security. Sometimes challenges are managed by the advanced technologies for secure networks but every time these techniques may not provide a reliable and secure communication between two parties who may be at a longer distance. In this perspective, three techniques i.e. cryptography, steganography and watermarking are widely used to provide security. However, three said techniques provide secure communication but no one standalone techniques can provide secure communication. Each technique has its benefits and issues.

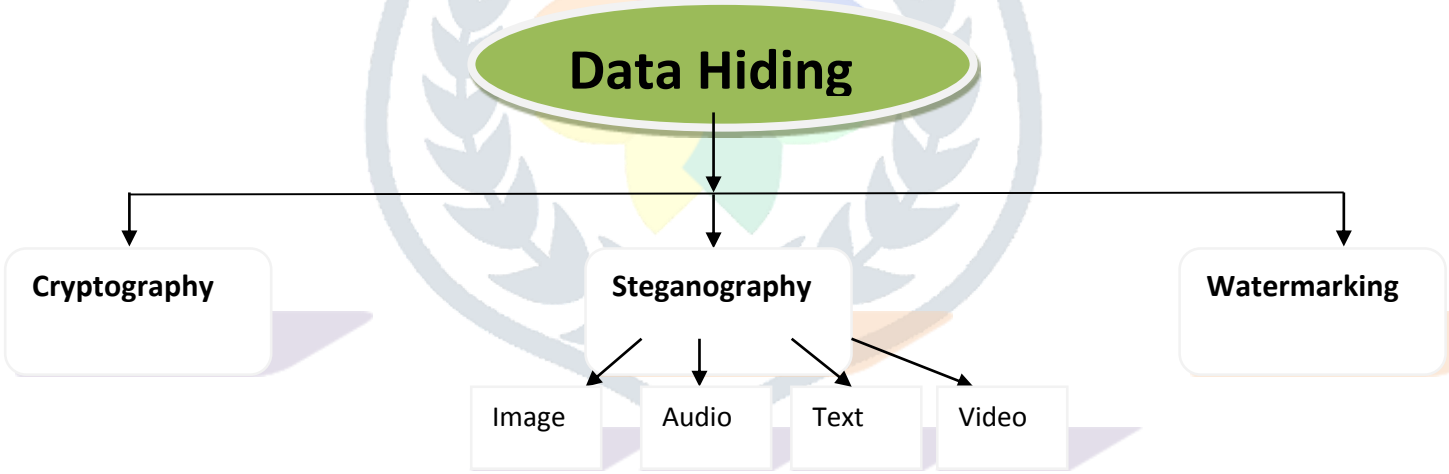

Figure 1 Overview of Data Hiding

I. Cryptography

It is the science of secret writing, converting messages or data into a different form to exchange messages between two parties who want the communication over an insecure channel. Without the right knowledge of the key no-one can access the correct information [1, 2]. The Sender encrypts the data with a key and converts the text in to cipher text which is a scrambled text. This cipher text is transmitted at the receiver end. The receiver decrypts the data with the key and gets the original text. Cryptography schemes include private key cryptography, public key cryptography and hash functions.

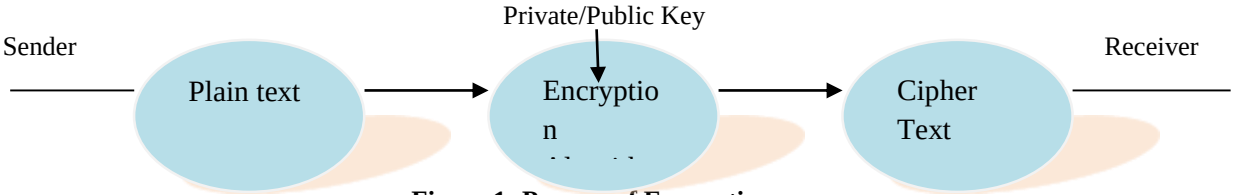

Figure 1: Process of Encryption

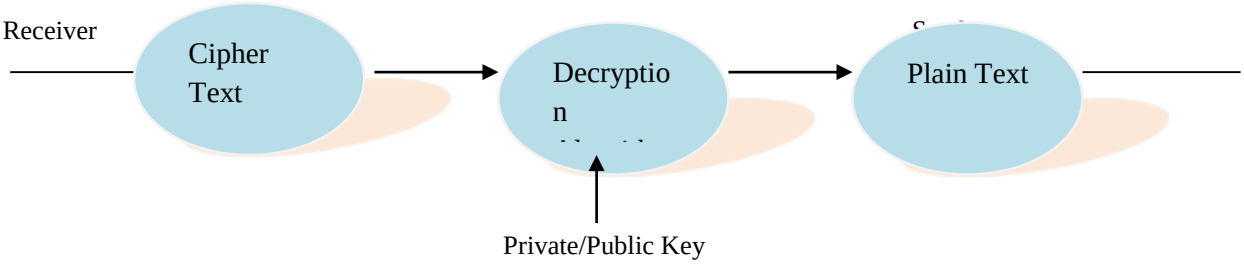

Figure 2: Overview of cryptography

A. Public key cryptography: In public key cryptography/asymmetric cryptography, two keys are used; one key for encryption and another key for decryption. The process can be described below:

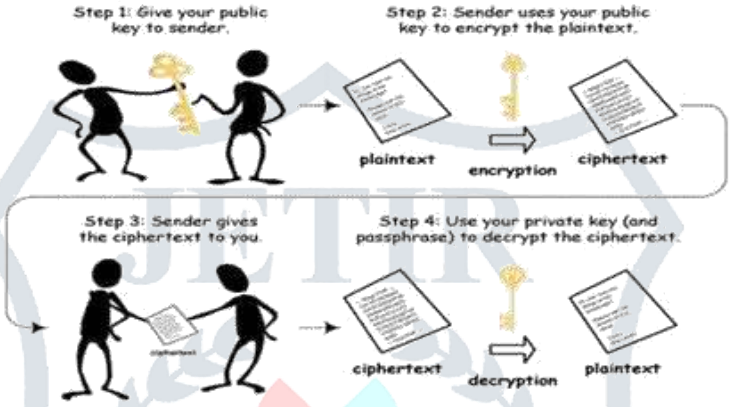

Figure 3: Public Key Cryptography [6]

B. Private Key cryptography: In private key cryptography / symmetric key cryptography, a single key is used to encrypt and decrypt the message. This technique is also called as single key , shared key and private key encryption.

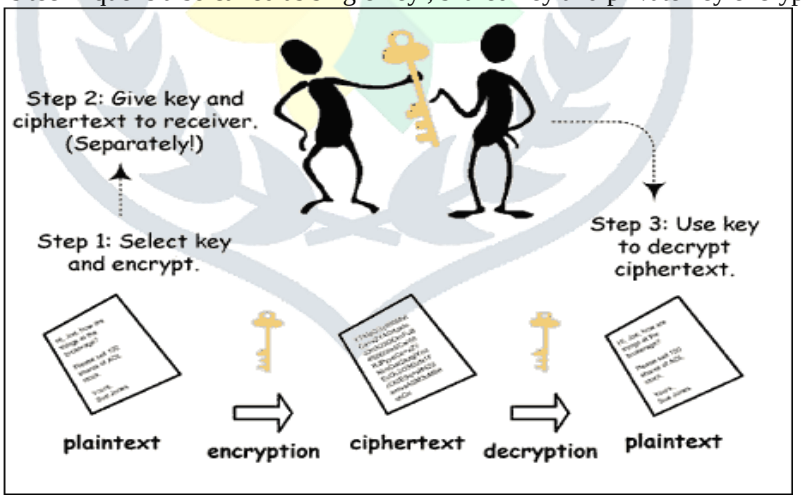

Figure 4: Public Key Cryptography [5]

C. Hash Function: In this technique, instead of using the concept of key , a fixed length hash value is computed based upon the plain text. Hash functions are used by various operating system to encrypt the passwords.

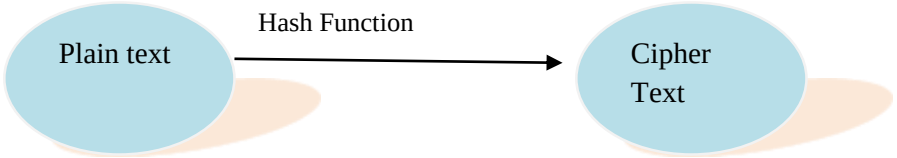

Figure 5 Hash Function

II. Steganography

Steganography is the art or practice of concealing a file, message, image, or video within another file, message, Image or video [3]. The steganography technique takes a cover image secret data,and a key, embeds the secret data into the cover image and produce a stego image. This stego image is transferred to the receiver end and the secret message is extracted by the recipient if he knows the key.

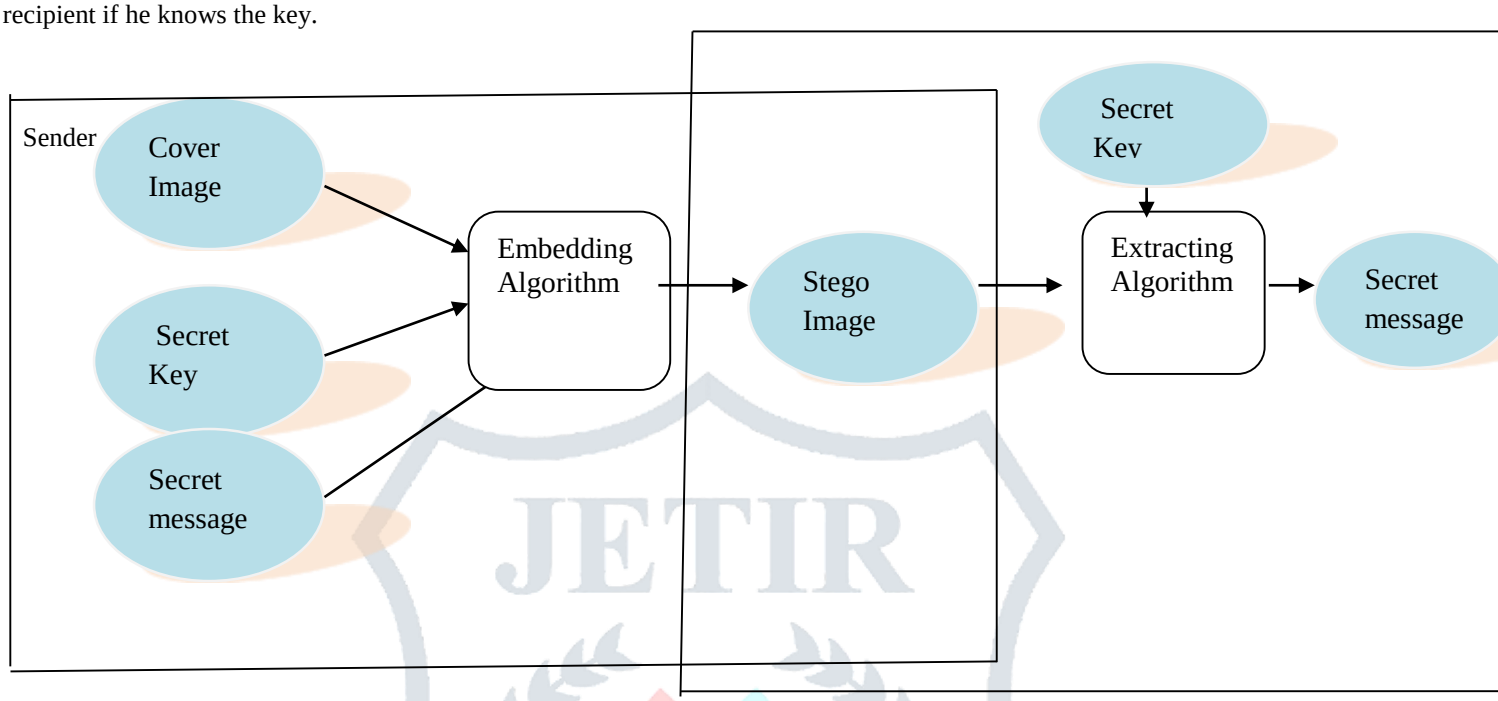

Figure 6: Overview of Steganography

III. Watermarking

The process of inserting information (the watermark) in the image (either visible or invisible form) is termed as digital watermarking.

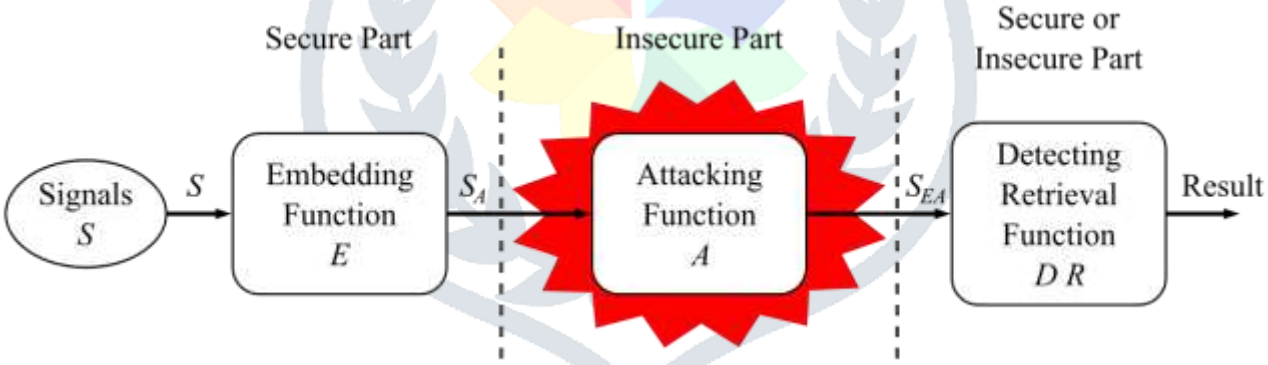

Figure 7: Digital Watermark Life cycle [4]

Comparative Study of Steganography, Cryptography and Watermarking

Table 1: Comparative Study

S No	Attributes	Steganography	Cryptography	Watermarking
1.	Definition	Steganography is called as cover writing	Cryptography is termed as hidden secret	A kind of marker covertly embedded in image or audio
2.	Techniques	LSB , Spatial, Block complexity, Transform Domain	Transposition, substitution, Stream ciphers, Block ciphers	Spatial domain, Fragile watermarking
3.	Carrier	Image, Audio, Video, Text	Text Files	Image
4.	Applicable	Cosmically	Cosmically	Cosmically
5.	Type of attack	Steganalysis i.e. if the intruder detects that steganography is performed then the security breaks	Cryptanalysis i.e. if the intruder cracks the cipher text then the security is broken as the original message is revealed	Watermark Drowning, synchronization attacks, stochastic attacks

6.	Secret Key	May be used	Necessary cannot work without key	May be used
7.	Motive	Conceal the existence of message	Conceal the contents of the message not its presence	Copyright protection
8.	Outcome	Stego image	Cipher text	Watermarked image
9.	Robustness	Yes	Yes	Yes
10.	Durability	Steganography basically hides the data under a cover i.e. it does not make any changes to the data	Cryptography , using an encryption algorithm converts the plain text in to cipher text i.e. it makes changes to the original data	Watermarking embed the data covertly in to the noise signals.
11.	Applications	Modern printers, intelligent services, distributed steganography	Integrity in storage, authenticity, Credentialing Systems, Electronic signatures	Copyright protection, Source Tracking, Video authentication

Conclusion

The paper provides a comparative study of three techniques which are widely accepted for the transmission of the confidential data from one end to the other end. The facts clearly state that neither of three can provide a secure transmission but if two techniques are combined then a robust system can be formed which can provide a secure data transmission. The study clearly states a simple concept i.e. if the cipher text formed from the cryptography process if is embedded in a cover image and then send for transmission then a secure and robust system can be formed. Future work can be done in a way to combine the cryptography and steganography techniques to provide a secure way to the confidential data.

References

[1] Gaetan Le Guelvouit, "Trellis-Coded Quantization for Public-Key Steganography," IEEE International conference on Acostics, Speech and Signal Processing, pp.108-116, 2008.

[2] Babita Ahuja and, Manpreet Kaur, "High Capacity Filter Based Steganography," International Journal of Recent Trends in Engineering, vol. 1, no. 1, pp.672-674, May 2009.

[3] Latika and Yogita Gulati, "A Review of Steganography Research and Development", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, 2015.

[4] http://en.wikipedia.org/wiki/Digital_watermarking

[5] Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay and Tai-hoon Kim, "Text Steganography: A Novel Approach," International Journal of Advanced Science and Technology, vol.3, pp.79-85, February2009.

[6] Chin- Chen Chang, Yung- Chen Chou and Chia- Chen Lin, "A steganography scheme based on wet paper codes suitable for uniformly distributed wet pixels," IEEE International Symposium on circuits and Systems, pp. 501-504, 2009.