A Comparative Study on Cryptography, Steganography and Watermarking Techniques used for Data Security

Lalit Mohan
Department of Computer Engineering
Graphic Era Hill University, Bhimtal, Uttarakhand, India

Abstract- *Cryptography, Steganography and Watermarking are three popular ways of sending information in a secret way. Now a day's computer applications are developed to handle financial and personal data, the real need for data security. Data security means protecting Data from unauthorized access. It is very challenging task to transmit data from sender to authorized receiver with full security through an insecure media. This paper is an attempt to analyze the data protecting techniques such as steganography, cryptography and watermarking.*

Keywords- Steganography, Cryptography, Watermarking, Symmetric key cryptography.

I. INTRODUCTION

In the past few years due to the fast development in cyberspace field, now it is needed to protect the information so that it is secret and confidential information from intruder. This is achieved through a hiding of data. The Greek word Steganography is combination of two words "stegos" meaning mean "cover" and "grafia" meaning means "writing" defining it as "covered writing" [1]. Communication over internet is surely efficient but intruder can steal the private information. Many communications such as video-chat or electronic mail and even web browser are Cryptography, Steganography and Watermarking techniques are widely used to hide the original message for secure communication. Cryptography means sender convert plaintext to cipher text by using encryption key and receiver side require receiver to decrypt cipher text to plain text by using a technique known as cryptanalysis [3].
Steganography is a data hiding technique, in which message is kept secret inside another media whereas in Watermarking special information is secretly inserted in the image not totally secure over the internet for exchanging the information [2]. Sometimes, information may include the personal or financial details such as bank related details which may be intercepted by intruder so user requires third party which do not access and alter the original content.

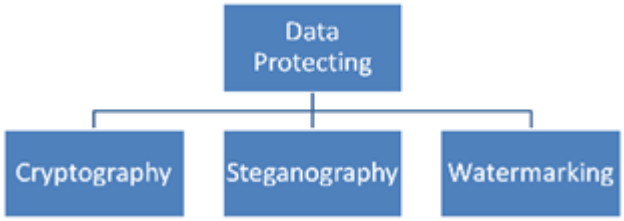

Fig. 1 Types of Data Protecting techniques

II. CRYPTOGRAPHY

It is the art of secret writing between two entities who want the communication over an insecure channel by converting original messages into a different form to exchange messages between them [3]. Without the exact knowledge of the key unauthorized access cannot be possible. In cryptography the data is converted from plain text to cipher text [10]. The Sender codifies the data with a key using any suitable scheme and converts the text in to cipher text which is a scrambled text. This cipher text is transmitted at the receiver end. The receiver transforms cipher text message back to plain text. Cryptography schemes include symmetric key cryptography, asymmetric key cryptography [3].

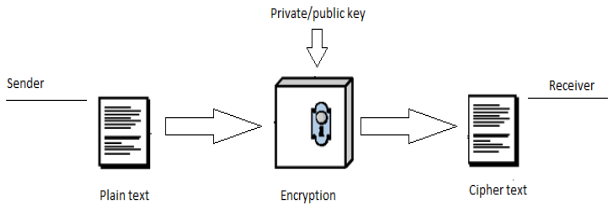

Fig. 2 Process of Encryption

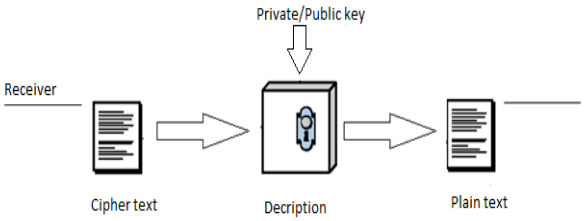

Fig. 3 Process of Decryption

Symmetric key cryptography

In symmetric key cryptography, single key is used to encrypt the message and same key is used to decrypt the message. The symmetric key cryptography takes place in two modes either as the block ciphers or as the stream ciphers. Symmetric key cryptosystems are much faster than the asymmetric key cryptosystems [13].This technique is also called as symmetric key, private key and single key encryption.

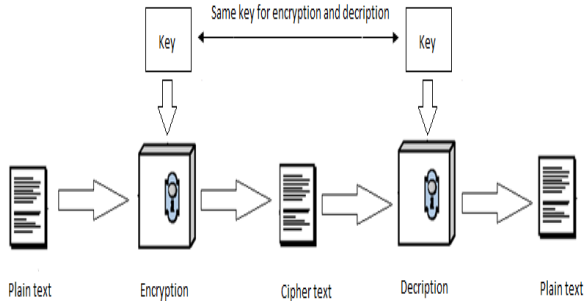

Fig. 4 Symmetric key cryptography

Asymmetric key cryptography

In asymmetric key cryptography key pair is used one key is used for encryption and another key is used for decryption. The two keys are a private key and a public key. The public key is announced to the public and it is available to anyone on the network, whereas the private key is kept by the receiver. The sender uses the public key of the receiver for encryption and the receiver uses his private key for decryption [14].

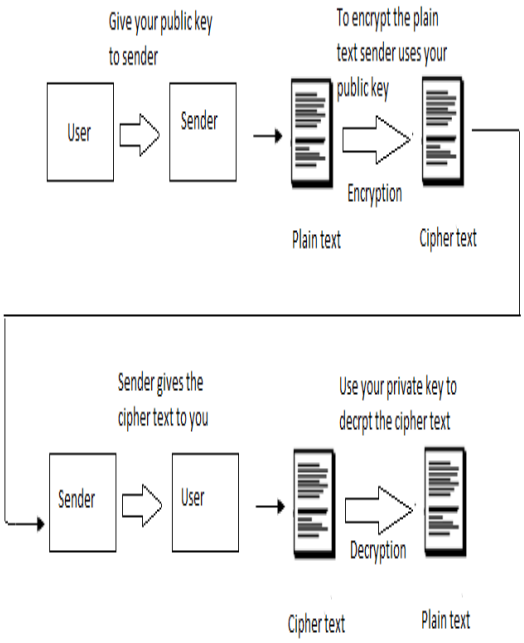

Fig. 5 Asymmetric key cryptography

III. STEGANOGRAPHY

Steganography is the study of invisible communication. Steganography means hiding of secret message behind any media files. The media file with confidential information is called stego media file and without secret information is called cover media file. Steganography is totally dependent on the type of media file being used to hide the information [9]. Steganalysis is a technique of extracting information from the stego media file [4]. The exact nature of embedding should be known in order to extract the message [7]. In sender side confidential message is embedded into some media file like text or audio and then it is transmitted so it will very difficult to an opponent from guessing that any confidential message is being transmitted [5].This embedded media file is transferred to the receiver end and the secret message is extracted by the recipient if he knows the key. There are two types of steganography which are Fragile and Robust [6].

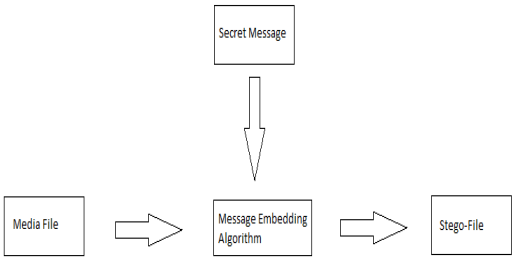

Fig. 6 Steganography

IV. WATERMARKING

Digital watermarking is the technique of hiding a message related to a digital signal (i.e. an image) within the signal itself. Watermarking is concept similar to steganography, in which both hide a message inside a digital signal. Watermarking tries to hide a message related to the actual content of the digital signal. Watermarking is a process for adding message (the watermark) into the image [8]. If anybody tries to copy the watermarked image, the watermark is copied along with the image. So watermarking is help to verify the authenticity and identity of the genuine owner of the digital image [12].

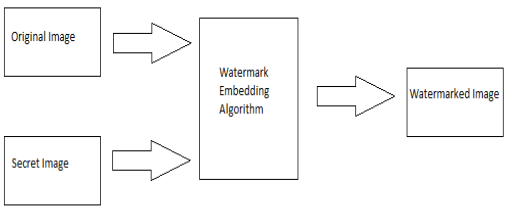

Fig. 7 Watermarking

V. COMPARATIVE STUDY OF STEGANOGRAPHY, CRYPTOGRAPHY AND WATERMARKING

FACTORS	Steganography	Cryptography	Watermarking
Definition	Steganography is art of hiding information behind the media file.	Cryptography is art of achieving security by encoding message to make them non readable.	Watermarking is an art of inserting information into image secretly.
Techniques	LSB, Spatial Domain, Jsteg, Outguess	Transposition, substitution, Stream ciphers, Block ciphers	Spatial domain, Fragile watermarking, DCT.
Carrier	Any digital media	Usually text	Usually Image
Secret key	Not necessary	Necessary	Not necessary
Robustness	Yes	Yes	Yes
Type of attack	Steganalysis	Cryptanalysis	Synchronization attacks, stochastic attacks
Output	Stego file	Cipher text	Watermarked image
Fails	When it is detected	De-ciphered	When it is detected
Key length	Small	Very large	Small
Naked eye Identification	No, cannot be possible because message is kept hidden within media file.	Yes, can be possible because original message is converted into cipher text.	Yes, as actual message is hidden by some watermark.

VI. CONCLUSION

This paper provides a comparative study of three techniques which are widely accepted for the transmission of the confidential data from one side to the other side. We can evaluate from the table that since the key length is high in cryptographic technique thus it is very difficult to decipher the code. When it comes to naked eye identification steganography is a better technique but once it is detected the secret message can be easily decoded. The same happens in the case of watermarking. But in the case of cryptography the naked eye identification can be easily done because during this technique original message is converted into cipher text but due to large number of secret key combination it is very difficult to de-cipher it again. Finally, we conclude that cryptography is a better technique as it offers more secure service but it has some limitation in the case of naked eye identification and it can only be applied in case of text formats whereas steganography and watermarking technique is applied on various formats. Thus, to solve this problem further enhancement in the cryptography and steganography technique is very important and both these techniques have to be integrated together for better security results.

REFERENCES

[1] Ashitosh S. Thorat, G. U. Kharat, "Steganography based navigation of missile", International Journal of Advanced Research in Electronics and Communication Engineering, ISSN: 2278 – 909X, Volume 4, Issue 6, 2015

[2] Pranali R. Ekatpure, Rutuja N Benkar, "A Comparative Study of Steganography & Cryptography", International Journal of Science and Research (IJSR), ISSN (Online): 2319-7064, Volume 4, Issue 7, 2015

[3] Latika, "A Comparative Study of Cryptography, Steganography & Watermarking", Journal of Emerging Technologies and Innovative Research, ISSN-2349-5162, Volume 2, Issue 5, 2015

[4] R.Srinivasan, V. Saravanan, G. Selvananthi, "A Comparative Study on Cryptography and Steganography", International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753, Vol. 3, Issue 12, 2014

[5] Ratul Choudhury, Samir Kumar Bandyopadhyay, "LSB Based Audio Steganography Using Pattern Matching Student", Journal of Multidisciplinary Engineering Science and Technology (JMEST), ISSN: 3159-0040, Vol. 2, 2015

[6] R. Poornima, R. J. Iswarya, "AN OVERVIEW OF DIGITAL IMAGE STEGANOGRAPHY", International Journal of Computer Science & Engineering Survey (IJCSES), Vol. 4, No. 1, 2013

[7] Preeti Singh, Charu Pujara, "Comparative study of various Techniques Employ in Image Steganography",

International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Volume 1, Issue-5, 2012

[8] Hardikkumar V. Desai, "Steganography, Cryptography, Watermarking: A Comparative Study", Journal of Global Research in Computer Science, ISSN: 2229-371X, Volume 3, No. 12, 2012

[9] Shaveta Mahajan, Arpinder Singh , "A Review of Methods and Approach for Secure Stegnography" , International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277-128X, Volume 4, Issue 5, 2014

[10] Sangeeta Raheja, Shradha Verma, "Comparative study of Hashing Algorithm Using Cryptographic and Steganography Using Audio Files", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277-128X, Volume 4, Issue 5, 2014

[11] Chin- Chen Chang, Yung- Chen Chou, 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

[12] D. Biswas, S. Biswas, P. P. Sarkar, D. Sarkar, S. Banerjee, A. Pal, "Comparison and Analysis of Watermarking Algorithms in Color Images – Image Security Paradigm", International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3, 2011

[13] Ritu Tripathi, Sanjay Agrawal, "Comparative Study of Symmetric and Asymmetric Cryptography Techniques", International Journal of Advance Foundation and Research in Computer (IJAFRC), ISSN 2348 – 4853, Vol 1, Issue 5, 2014

[14] Nivedita Bisht, Sapna Singh, "A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms", International Journal of Innovative Research in Science, Engineering and Technology, ISSN 2347 – 6710, Vol 4, Issue 3, 2015