A Comparable Analysis of Steganography, Cryptography and Watermarking

[1]Arbind Tiwary, [2]Dr. A. K. Gupta, Dr. [3](Prof) Rajesh Kr. Tiwary

[1]Research Scholar, Department of Computer Application, Vinoba Bhave University, Hazaribag, India
[2]Associate Professor, Department of Physics, Vinoba Bhave University, Hazaribag, India
[3] Dean, Deparment of CSE , R.V.S. College of Engg. & Tech., Jamshedpur, India.

Abstarct: The descriptions of passing data from one side to other side by a outdated way is been changed due to Internet and Communiqué Technology. Expansion is so much fast so the issue lies of security and integrity of data. Now a day's digital message has become an essential part of (transitory data), There are so many Internet application is used to communicate secretly. As a result, the security of information against unlawful access has become a prime objective. This leads to lots of expansion of various techniques for data hiding. Steganography, Cryptography and Water marking are the popular methods available to hide data strongly.

Keyword: Steganography, Cryptography, Watermarking, StegoImage, Encryption, Decryption

1. Introduction

Steganography, Cryptography and Watermarking are well identified and broadly used to hide the original message. Steganography is used to implant message within another object known as a concealment work, by alteration its properties. The Cryptography is a technique in which, sender convert plaintext into cipher text by using Encryption key and other side receiver decrypt cipher text to plain text. Digital watermarking is a technique for inserting information (the watermark) into an image (seen or unseen). Today most of communication occurs digitally. There have been progresses exploiting digital multimedia signals as vehicles for steganographic communication. The cover signal inclue audo,video & imagery signal. Patterns where the unique cover signal is required to disclose the concealed information are known as concealment escrow [1]. A data hiding pattern using the statistical properties of dithered imagery is proposed by Tanka, in this method, the dot patterns of the ordered dither pixels are controlled by the information bits to be concealed. This system adopts 2 KB of concealed information for a bi-level 256 x 256 image, yielding a payload of data or information hiding ratio of one information bit to four cover image bits. An information hiding proportion of 1:6 is acquired for tri-level image of the same size, the method has high payload but is restricted to dithered images and is not resistant to errors in stego image [2]

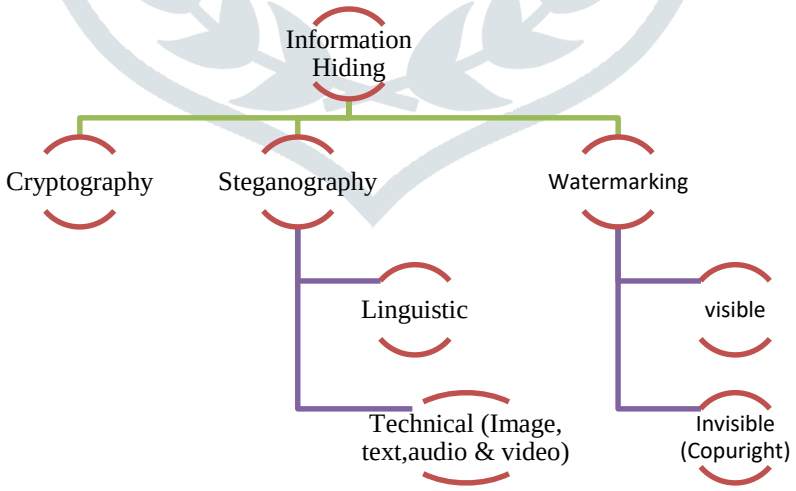

Figure 1: Information Hiding

2. Definition and Terminology

One of the ancient examples of Steganography periods back to around 440 BC in Greek History. Herodotus, a Greek historian from the 5th century BC, discovered. In those examples of its use in his work entitled "The Histories of Herodotus". One extravagant example suggests that Histaeus, ruler of Miletus, tattooed a secret message on the shaven head of one of his most trusted slaves. Later

the hair had grownup back, the slave was sent to Aristagorus where his hair was hairless and the message that commanded a revolt against the Persians was revealed [3]. The furthermost common methodologies to information hiding in images are

a. Least significant bit(LSB) insertion.

b. Masking and filtering techniques.

c. Algorithms and Transformations.

All of these can be applied to numerous images, with changeable degrees of achievement. All of them agonize to varying degrees from operations performed on images, such as cropping or resolution decrementing or decrease in the colour depth [5].

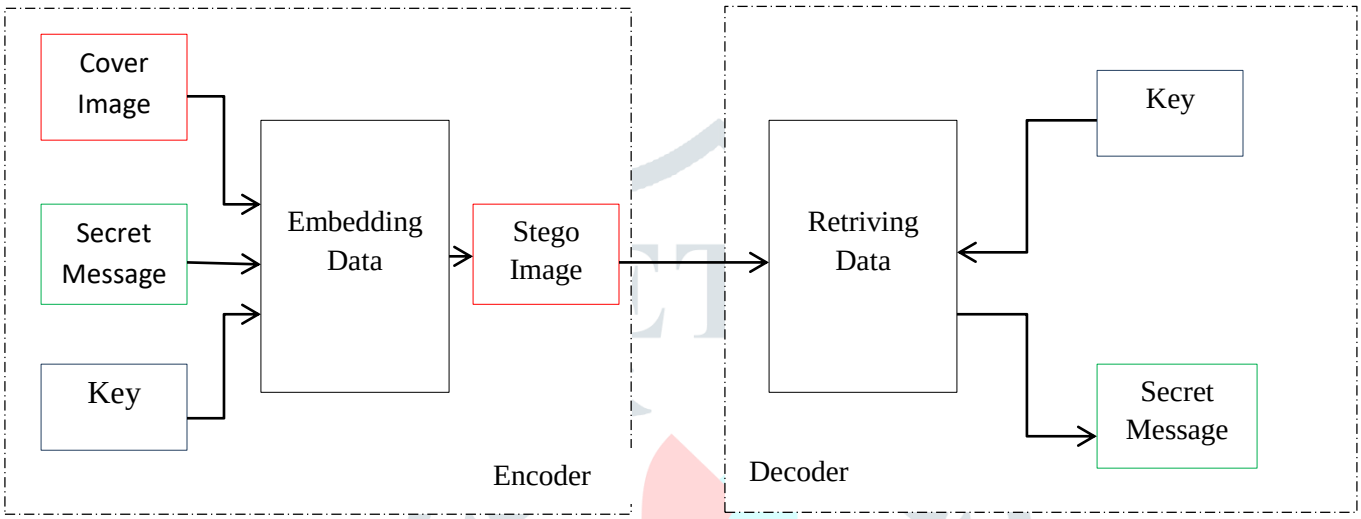

Figure 2: Steganography Model

2.1 Steganography

The term steganography refers to the art of concealed communications. The message is embedded within another object known as cover work, by changing its properties [1]. The resulting output is known as stego-gram. Steganography is data concealed within data. Steganography procedures can be applied to images, a video file or an audio file [7]. Usually, however, steganography is transcribed in characters including hash pattern, but its usage within images is also common. At any rate, steganography protects from pirating copyrighted materials as well as aiding in illegal viewing.

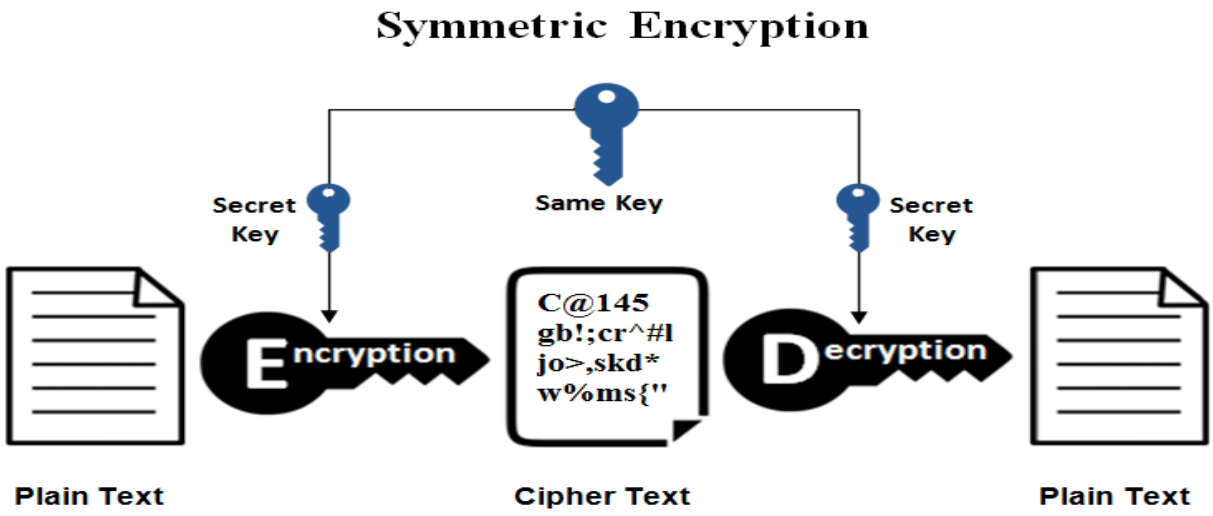

Figure 3: Cryptography Model

2.2 Cryptography

Cryptography is the skill of encrypting and decrypting written communication. It's comes from the Greek word "krypo", meaning hidden, and "graphia", meaning writing. Cryptography [8] is a scheme of storing and transmitting data in a form that only those it is intended for can read and process. It is a skill of protecting information by encoding it into an unreadable format. Cryptography is an operative way of protecting sensitive information as it is stored on media or transmitted through network communication paths.

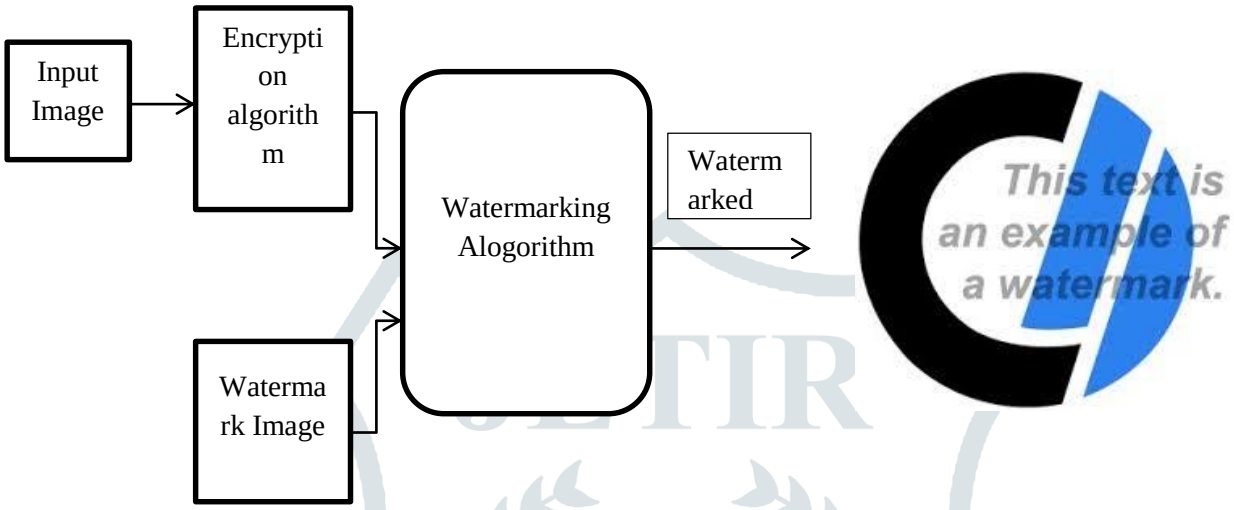

Figure 4: Watermarking Model and Example

2.3 Watermarking

Digital watermarking is a method for inserting information (the watermark) into an image (visible or invisible). Visible watermarking Decryption Key. The idea is to change the text in to format which is not easy to decrypt without decryption key .changing the alphabets with another alphabets or make a key to arrange the alphabets. Generally, organization put there logo or seal which holds rights of the organization of image. Invisible water marking invisible watermarking is concerned to authentication copyrighting of image.

The area of research emphasize on which technique is best suited as individual or together for data hiding .So analyzing all three techniques and derived the result best suited.

3. Scope of Study

3.1 Analysis

After analysis of these three techniques, the following thing we got,

Table 1: Comparison table of three techniques

Attribute	Steganography	Cryptography	Water Marking
Techniques	LSB, Spatial Domain, Jsteg, Outguess	Transposition, Substitution, RSA	compensated prediction, DCT
Naked eye Identification	No, as message is Hide within other carrier (cover image)	Yes, as message is convert in Other way, which sough something is hidden	Yes, as actual message is hiding by some watermark
Capacity	Differs as different Technology usually low hiding capacity	Capacity is so high, but as message is long it chances to be decrypt	Capacity depends on the size of hidden data.
Detection	Not easy to detect because to find steganographic image is hard.	Not easy to detect ,depend on technology used to generate	Not easy to detect
Strength	Hide message without altering the message, it conceals information	Hide message by altering the message by assigning key	Extend information and become an attribute of the cover image
Imperceptibility	High	High	High
Applicability	Universally	Universally	Universally
Robust	Yes	Yes	Yes

Researcher obtained that steganography and cryptography are not similar. Security of data is a challenge for computer user. Amalgamation of cryptography and steganography [6] enhance the security and reliability of message as first message is encrypt and the using steganography hide it to other carrier like digital image, video file or any other.

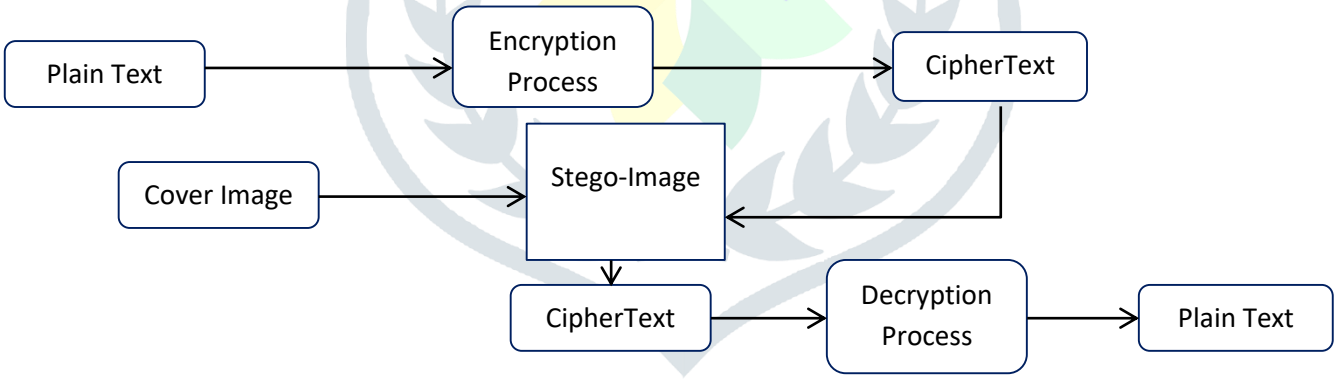

Figure 5: Amalgamation of cryptography and steganography

4. Conclusion and Future Work

Presently watermark majorly used for copyright the image; we have found that a combination of steganography & cryptography generates the most secure data hiding technique. The goal of information hiding is achieved through the combined action of steganography and cryptography because steganography main feature is that message never sought (shown by the naked eye) and cryptography is about masking the content of the message. At the same time encrypted data itself evidence of the existence of data. In future we can say, the proposed analysis of three technique the best technique steganography and cryptography will secure information over un-secure channel of communication.

5. References

[1]. Arbind Tiwary1, A K Gupta2 and Rajesh Kumar Tiwari3,"DIFFERENT IMAGE STEGANOGRAPHY TECHNIQUES: AN OVERVIEW", International Journal of Computer Engineering and Applications, Volume XI, Issue IX, September 17, www.ijcea.com ISSN 2321-3469, pp1-13

[2]. B. P Fitzmann, "Trials of traced traitors." Information hiding, first international work shop, Lecture notes in computer science R. Anderson, Ed. Berlin, Germany: Springer Verlag 1996, vol. 1, pp- 49-64.

[3]. K. Tanaka, Y. Nakamura and K. Matsui, "Embedding Secret Information in to a Dithered Multi Level Image," in Proc IEEE Military communications conf., Monterey, CA, 1990, pp- 216-220.

[4]. Neil F. Johnson and sushil Jajodia Exploring Steganography: seeing the unseen IEEE computer, 31(2)26-34, 1998.

[5]. N. Proros and P. Honeyman. "Hide and seek: An Introduction to Steganography ", IEEE: security & Privacy, vol. 10, pp. 32-44, 2003.

[6] Amanpreet Kaur,Renu Dhir and Geeta Sikka, "A New Image Steganography Based On First Component Alteration Technique", International Journal of Computer Science and Information Security,Vol. 6, No. 3, pp 53-56,2009

[7] Mansi S. Subhedar,Vijay H. Mankar "Current status and key issues in image steganography: A survey, Computer Science review,13-14, pp 95-113,2014

[8] Image Steganography, https://en.wikipedia.org/wiki/Steganography