Volume 3, No. 12, December 2012
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

Steganography, Cryptography, Watermarking: A Comparative Study

Hardikkumar V. Desai (B.Sc., MCA)
Research Scholar, Singhania University,
Pacheri Beri, Distt. Jahunjhunu Raj.
hardik4dreamz@yahoomail.com

***Abstract*—** The definitions of passing data from one side to other side by a traditional way is been changed due to Internet and Communication Technology. Development is so much fast so the issue lies of security and integrity of data. Now a day's digital communication has become an essential part of (passing data), There are so many Internet application is used to communicate secretly. As a result, the security of information against unauthorized access has become a prime objective. This leads to lots of development of various techniques for data hiding. Steganography, Cryptography and Water marking are the popular techniques available to hide data securely.

INTRODUCTION

Steganography, Cryptography and Watermarking are well known and widely used to hide the original message. Steganography is used to embed message within another object known as a cover work, by tweaking its properties; By using Cryptography sender convert plaintext to 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 (visible or invisible).

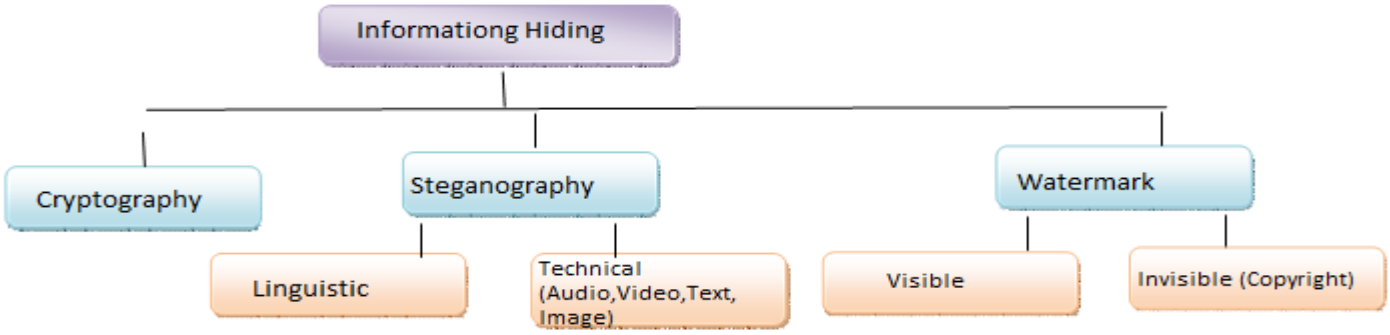

Figure 1 : Information Hiding

Today most of communication occurs electronically
There have been advancements utilizing digital multimedia signals as vehicles for steganographic communication These signals, which are typically audio, video or still imagery are cover signals. Schemes where the original cover signal is needed to reveal the hidden information are known as cover escrow [1].

A data hiding scheme 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 accommodates 2 KB of hidden 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 ratio of 1:6 is obtained 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].

DEFINITION AND TERMINOLOGY

One of the oldest examples of Steganography dates back to around 440 BC in Greek History. Herodotus, a Greek historian from the 5th century BC, revealed. Some examples of its use in his work entitled "The Histories of Herodotus". One elaborate example suggests that Histaeus, ruler of Miletus, tattooed a secret message on the shaven head of one of his most trusted slaves. After the hair had grown back, the slave was sent to Aristagorus where his hair was shaved and the message that commanded a revolt against the Persians was revealed [3].

The most common approaches to information hiding in images are

a. Least significant bit(LSB) insertion
b. Masking and Filtering techniques
c. Algorithms and Transformations.

Each of these can be applied to various images, with varying degrees of success. Each of them suffers to varying

degrees from operations performed on images, such as cropping or resolution decrementing or decrease in the colour depth [4].

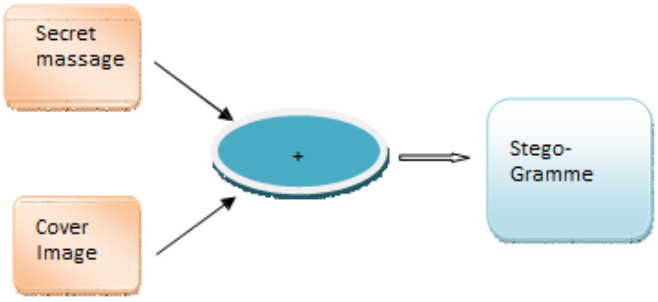

Figure 2 : Steganography.

Steganography:

The term steganography refers to the art of covert communications. The message is embedded within another object known as a cover work, by tweaking its properties. The resulting output is known as stegogramme.

Water Marking:

Digital watermarking is a technique for inserting information (the watermark) into an image (visible or invisible). Visible water marking

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 water marking is concerned to authentication copyrighting of image.

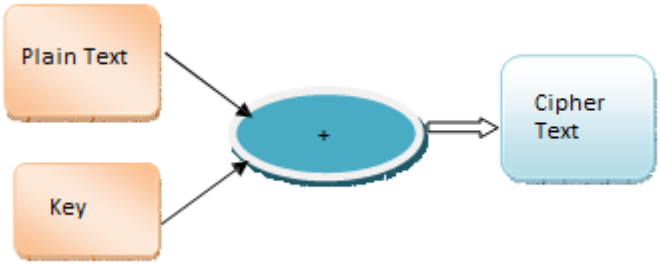

Figure 3: Cryptography.

SCOPE OF STUDY

CRYPTOGRAPHY

Cryptography means sender convert plaintext to cipher text by using Encryption key and other side receiver decrypt cipher text to plain text by using 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.

ANALYSIS

The researcher found following analysis

Table: 1

	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

CONCLUSION

Now a day's water mark majorly used for copyright the image, the researcher found that combination of steaganography and cryptography generate most secure data hiding technique.

Researcher found that steganography and cryptography are not same; security of data is a challenge for computer user. Combination of cryptography and steganography 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.

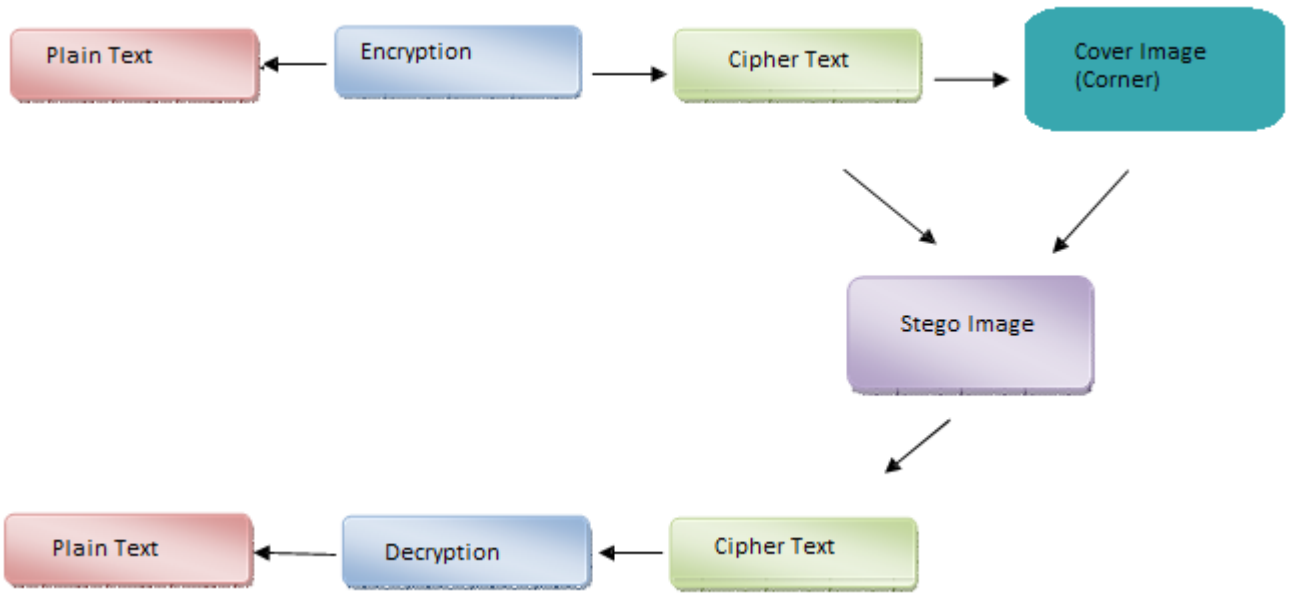

Figure 4 : Steganography & Cryptography.

The goal of information hiding is achieved through combinationation of steganography and cryptography because steganography main feature is that message never sought (shown by naked eye) and cryptography is about concealing the content of the message.At the same time encrypted data itself evidence of existence of data .

REFERENCES

[1]. 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.

[2]. 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.

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

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