Study of secure steganography method based on image compression

Neha Shekhawat
Computer Science & engineering, MTECH, ITS, Bhiwani, Haryana, India

Kiran Siwach
HOD, Computer Science & engineering, ITS, Bhiwani, Haryana, India

Sonia Rana
Assistant Professor, Computer Science & engineering, ITS, Bhiwani, Haryana, India

Abstract- Cryptography and steganography are the two popular methods available to provide security for communication. Cryptography is a type of Steganography, but are very different from each other. Steganography is a method of hiding secret messages in a cover objects for example digital images, audio, video or TCP/IP header file, while communication takes place between sender and receiver. In the same way cryptography is a technique of encrypting messages on an open environment, so that only subjected person receives the message. In this paper, a review report is presented for combining both the techniques.

Keywords: Cryptography, Steganography, Strength, Factor, Future

I. INTRODUCTION

A lot of work has been done for encrypting messages as well as for hiding presence of information, but it can provide enough security, if we can implement both the techniques together. Alone, they cannot provide sufficient security. If we simply use steganography it will be security by obscurity, if anyone suspects information, it can be detected. So we need to work on a method, through which we can implement secure steganography.

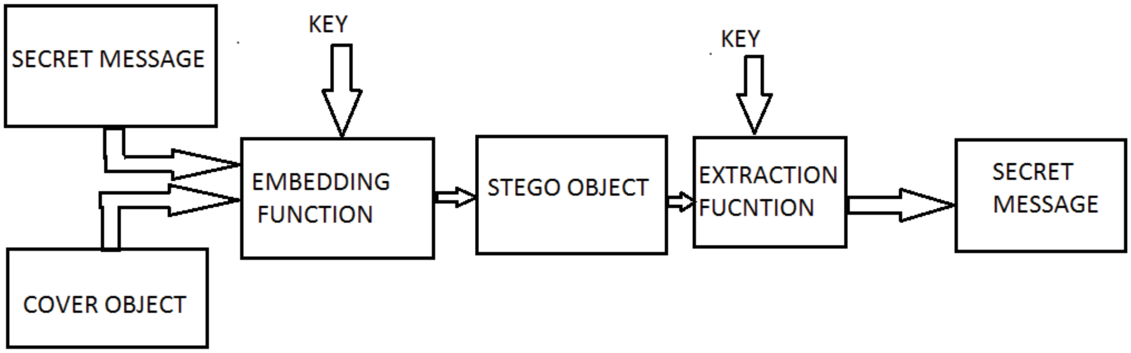


Fig: A model depicting combination of steganography and cryptography

II. SURVEY OF LITERATURE

Information sharing through open channel has come up fast and in the same way requirement of information security has drastically changed. Many techniques have come up and each of them has some positives and negative. Cryptography and steganography are the two common and popular methods provided for information security. Steganography is a type of cryptography, but are quite different from each other. Steganography is a method of hiding secret messages in a cover object while communication takes place between sender and receiver. Security of confidential information has always been a major issue from the past times to the present time. It has always been an interesting topic for developers to develop secure techniques to send data without revealing it to anyone other than the receiver. Hence many developers have come up with the techniques to fulfil secure transfer of data and steganography is one of them.

III. MAIN CONCEPTS OF STEGANOGRAPHIC SYSTEMS

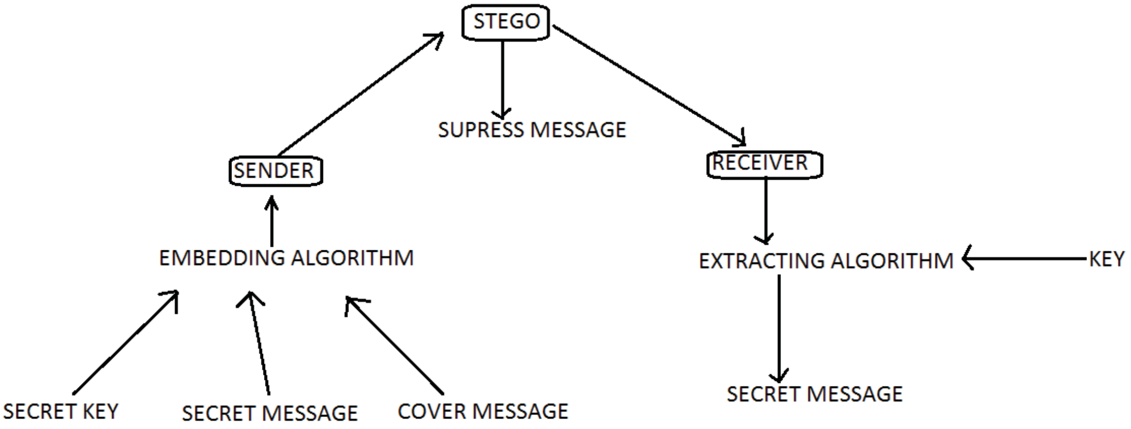
Steganographic systems rely on common principle explained as follows.

A stego file is a combination of cover file and hidden message in the cover file. The Objective here is to make our message unpredictable by intruder that there is a message inside. The sender will send a secret message to the recipient, so he will select a cover file. Later, receiver will take the object file out from cover and will use a stego key known as password. Stego key should be created such that neither computer not a human being can determine that there is a file inside.

It is kerchoff's principle, on which the whole stego systems rely. It states that stego system should be open for all, it should be the only key, which remains secret, so even if you have message, but does not have stego key, then that message will be of no use to you. This is the application, this projects move around. This is call secure steganographic systems. In the beginning only the transmitter and the intended recipient should have the stego key. Therefore, most of steganographic systems prompt users to provide a stego key or password when they try to embed information in a cover file. It is possible attackers can detect a hidden message in a stego file and determine how the message was embedded, but they are unable to extract the hidden message. Therefore the total strength of the system depends on how strong our key is.

Cryptanalysis: While designing the stego system, it is important to that we consider the skill sets of attackers. Generally attacker are highly skilled and experienced programmers. So it is only our key which can protect the message from hijacked.

IV. TECHNIQUES FOR STEGANOGRAPHY



1. Spatial Domain Methods: In this technique the secret information is embedded directly in the intensity of pixels i.e. Pixel values of the image are changed directly during hiding data. This technique is classified into following categories:

i) Least significant bit (LSB)
ii) Pixel value differencing (PVD)
iii) Edges based data embedding method (EBE)
iv) Random pixel embedding method (RPE)
v) Mapping pixel to hidden data method
vi) Labelling or connectivity method
vii) Pixel intensity based

i) LSB: LSB is the most common technique used for hiding data. Data is implemented by replacing the least significant bits of image pixels with the bits of secret data. Final image is almost similar to the earlier image, as change in LSB of the image does not affect the basic properties and looks of image.

ii) BPCP: In this method, complexity of image are used to determine the noisy factor, then these blocks of noise bit plan are replaced by the binary patterns mapped from a secret data. So noise factor is determined from image complexity, in reverse noise factor will not bring any change in appearance of image.

ii) PVD: In this method, two consecutive pixels are selected for embedding the data. Whether the two pixels are from smooth area or curved area, is determined. This is done by calculating the difference of two regular pixels.

2. Spread Spectrum Technique: This technique is widely used in military. Data is spread over a wide spectrum of noise. The number of bits of data must be small to detect the presence of data. Spectrum is wide, so after removing information from spectrum loads of information could be left in the spectrum. Thus it is a robust technique as it is difficult to remove the data completely without entirely destroying the cover.

3. Statistical Technique This technique utilizes the characteristics of the cover file. It is divided in to blocks. Then bit by bit messages are inserted into these blocks. This transmission is done at basic level of storage of file.

If the message contains a 1 then bit is inserted into block, if there is zero block is left blank. So quiet hard to break.

4. Transform Domain Technique: In this technique, frequency domain of the cover object is used to transform the original message. This is quiet complex and rare usage but this one is the most secured also as it is very difficult to decode it, per frequency. There are many techniques as

i) Discrete Fourier transformation technique (DFT)
ii) Discrete cosine transformation technique (DCT)
iii) Discrete Wavelet transformation technique (DWT)
iv) Lossless or reversible method (DCT)
iv) Embedding in coefficient bits

5. Distortion Techniques: This method is about distorting the message. A sequence of changes is applied and these changes are recorded sequence wise. The receiver should have knowledge about these distortions and the changes. And then at receiver these distortions are carried in reverse order and the real message could be retrieved.

6. Masking and Filtering: This method is basically used for 24-bit and grey scale images. These techniques hide information by marking an image. Steganography only hides the information whereas watermarks becomes a portion of the image. These techniques inserts the information in the more significant areas rather than hiding it into the noise level. This technique is more trustworthy, because watermarks are much inserted into image. This method is generally used for 24-bit and grey scale images.

V. OBJECTIVES

This paper focuses on combining the strength of cryptography and steganography, and how information could be encrypted and hided. Sequence of operation matters while combining both the operations, because first presence of information should be hided, and if broken it will be further secured by encrypted message. But it also depends on the type of information and security method. Also size of carrier data is important.

VI. WORK

In this paper we propose a technique of combining cryptography and steganography to solve the problem of unauthorized data access. Steganography also can be implemented to cryptographic data so that it increases the security of data. In this method we first encrypt a message. The combination of these two methods will enhance the security of the data embedded and will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. Furthermore, if an attacker were to defeat the steganographic technique to detect the message from the stego-object, he would still require the cryptographic method to decipher the encrypted message. The intended receiver should be able to recover the embedded data successfully, without any errors

Factors affecting the process of combining

1. Robustness: Robustness refers to the property that data will remain intact even after going many transformation like encrypting and decrypting, cropping or decimation, sharpening or blurring of spectrum, adding random noise, linear and non-linear filtering, scaling and rotations or loss compression.
2. Imperceptibility: The algorithm should be strong enough so that it can go un-noticed by a human eye. If anybody notices any difference in the image then the main aim of stego-object goes to failure. Although encrypted message will be there to protect it but even then steganography aim will be compromised.
3. Payload Capacity: It is important that we consider what size can be transmitted without being noticed, because first stego file will be created and then cryptography will be applied, so size may increase in large figure, so enough of space should be provided.
4. PSNR (Peak Signal to Noise Ratio): PSNR is used to measure the quality of steganography by measuring the difference between the original and a compressed image. PSNR is the ratio between the maximum possible power of a signal and the power of corrupting the message with the noise that affects the identification of message. AS much high the value of PSNR, will be, message embedded will harder to detect.
5. MSE (Mean Square Error): For an efficient system we should get low MSE. Mean Squared Error is the value of average squared difference between a reference image and a distorted image. It is computed pixel-by-pixel by sequencing up the squared differences of all the pixels and dividing by the total pixel count.
6. SNR (Signal to Noise Ratio): It compares the level of a desired signal to the level of background noise and is known as the ratio of signal power to the noise power.

7. NCC (Normalized Cross-Correlation): Normalized cross-correlation is a template matching technique, and is used to determine the alignment of images. Templates are matched in a particular pattern in the image to take out the message.
8. BER (Bit Error Rate): Bit error ratio (BER) is the count of bit errors divided by the total number of transferred bits while an observed time interval.

VII. APPLICATIONS OF SECURE STEGANOGRAPHY

- Data protection from alteration
- Electronic transactions
- Secret data and confidential information sharing
- Mobile banking
- Against fraudulent behaviors

VIII. CONCLUSION

Digitized communication has a vast scope and great future, because new algorithms will be discovered and will be broken. After studying many research papers published so far it has been realized that most of the work on steganography has been done after 2012. In the future we will see more combined versions of steganography and cryptography, for providing harder security.

Future aspects

This thesis has a vast scope of further combinations and analysis. There is vast scope of studying for particular type of images and for developing technique for transferring large messages. Also in future, need to work on the efficiency of the algorithm designed.

REFERENCES

[1] http://airccse.org/journal/ijsptm/papers/3114ijsptm02.pdf International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1, February 2013 DOI : 10.5121/ijcses.2013.4102 23 AN OVERVIEW OF DIGITAL IMAGE STEGANOGRAPHY R.Poornima and R.J.Iswarya2, Department Of Advanced Computing,

[2] http://www.cscjournals.org/manuscript/Journals/IJCSS/volume6/Issue3/IJCSS-670.pdf. Authors as Nagham Hamid, Abid Yahya, R. Badlishah Ahmad M. Al-Qershi Provides different techniques of stegenography and history of stegenography.

[3] http://repository.root-me.org/St%C3%A9ganographie/EN%20-%20Image%20Steganography%20Overview.pdf,A paper from south Africa provides knowledge about attacks on cryptography and steganography.

[4] http://www.ijsrm.in/v2-i12/2%20ijsrm.pdf.An internal paper submitted by students of MIT, Aurangabad provides details techniques of steganography through LSB technique.

[5] https://www.schneier.com/paper-blowfish-fse.html.provids information about different old cryptography algorithms that has been broken and provides information about latest algorithms like blowfish that has still not been broken.

[6] http://security.stackexchange.com/questions/5734/is-steganography-a-safe-method-to-store-secret-data

[7] http://www.airccse.org/journal/ijcses/papers/4113ijcses02.pdf Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay And Sugata Sanyal, SteganographyandSteganalysis

[8] Different Approaches Available from: http://arxiv.org/ftp/arxiv/papers/1111/1111.3758.pdf

[9] http://www.ermt.net/docs/papers/Volume_3/5_May2014/V3N5-190.pdf this is a review paper submitted in steganography , author as JKaur and deepankar verma.

[10] http://airccse.org/journal/ijcis/papers/2312ijcis14.pdf SECURE DATA TRANSMISSION USING STEGANOGRAPHY AND ENCRYPTION TECHNIQUE Shamim Ahmed Laskar1 and Kattamanchi Hemachandran2 Department of Computer Science Assam University, Silchar, India

[11] B. B. Zaidan, A. A. Zaidan, A.K. Al-Frajat and H.A. Jalab, “On the Differences between Hiding Information and Cryptography Techniques: An Overview”, Journal of Applied Sciences, Vol.10, No.15, pp.1650-1655, 2010.

[12] M. Kharrazi, H. T. Sencar and N. Memon, “Performance study of common image steganography and steganalysis techniques”, Journal of Electronic Imaging, SPIE Proceedings Vol. 5681.15(4), 041104 (Oct–Dec 2006). SPIE and IS&T., 2006

[13] http://www.sersc.org/journals/IJSIP/vol7_no3/4.pdf A New Image Steganographic Approach Based on Mod Factor for RGB Images