ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 6, June 2014

Steganography Process- A Review

Lovepreet Kaur

CGC Landran, Punjab, India.

ABSTRACT: In this paper we survey different steganography techniques for encrypting the data along with characteristics, difference with cryptography. Steganography is the art and science of hiding information by embedding messages within other, seemingly harmless messages. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images. This paper will help in using the best stegnography method for images

KEYWORDS: steganography, cryptography, DCT, DWT

I. INTRODUCTION

Steganography is the art or practice of concealing a message, image, or file within another message, image, or file. The word steganography combines the Ancient Greek words steganos meaning "covered, concealed, or protected", and graphein meaning "writing". The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages will appear to be (or be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter. Some implementations of steganography which lack a shared secretare forms of security through obscurity, whereas key-dependent steganographic schemes adhere to Kerckhoffs's principle.

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages—no matter how unbreakable—will arouse interest, and may in themselves be incriminating in countries where encryption is illegal.Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

II. DIFFERENCE BETWEEN CRYPTOGRAPHY AND STEGANOGRAPHY

With the increasing number of users and the number of unauthorized access has also increased. Hence, Information security plays an important role. Keeping this concept in mind cryptography and steganography both are used. Therefore, the main issue now is to mitigate and to lessen the impact of the chances of the information being detected during transmission. Cryptography deals message encryption but the communication is visible but on the other hand, steganography deals with secret message hiding but the communication is invisible. This is the major difference between cryptography and steganography. Although by encrypting the traffic, the communications will be secured but people become aware of the existence of information by observing coded information, although they are unable to comprehend the information. Steganography hides the existence of the message so that intruders can't detect the communication and thus provides a higher level of security than cryptography. Both steganographic and cryptographic systems provide secret communications but different in terms of system breaking. Steganography system is more fragile than cryptography systems in terms of system failure.

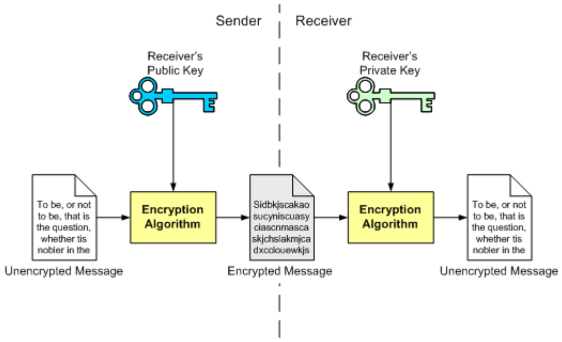
Sender
Receiver
Receiver's Public Key
Receiver's Private Key
To be, or not to be, that is the question, whether tis nobler in the
Encryption Algorithm
Sidbkjscakao sucyniscuasy ciascnmasca skjchslakmjca dxccioueywkjs
Encryption Algorithm
To be, or not to be, that is the question, whether tis nobler in the
Unencrypted Message
Encrypted Message
Unencrypted Message

Figure. 1 Image Cryptography

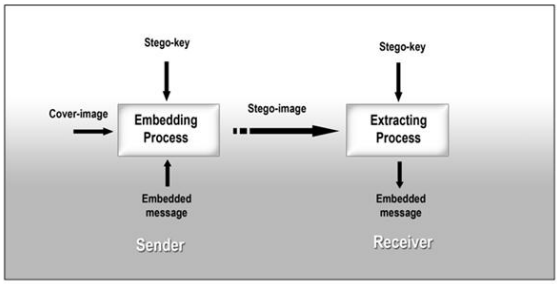

Figure. 2 Image Steganography

III. RELATED WORK

However, the majority of the development and use of computerized steganography only occurred in year 2000 [1]. The main advantage of steganography algorithm is because of its simple security mechanism. Because the steganographic message is integrated invisibly and covered inside other harmless sources, it is very difficult to detect the message without knowing the existence and the appropriate encoding scheme [2]. There are several steganography techniques used for hiding data such as batch steganography, permutation stehanography, least significant bits (LSB), bit-plane complexity segmentation (BPCS) and chaos based spread spectrum image steganography (CSSIS). Research in hiding data inside image using steganography technique has been done by many researchers, for example in [3-7]. Warkentin et al. [3] proposed an approach to hide data inside the audiovisual files. In their steganography algorithm, to hide data, the secret content has to be hidden in a cover message. El-Emam [4], on the other hand, proposed a nsteganography algorithm to hide a large amount of data with high security. His steganography algorithm is based on hiding a large amount of data (image, audio, text) file inside a colour bitmap (bmp) image. In his research, the image will be filtered and segmented where bits replacement is used on the appropriate pixels. These pixels are selected randomly rather than sequentially. Chen et al. [5] modified a method used in [6] using the side match method. They concentrated on hiding the data in the edge portions of the image. Wu et al. [7], on the other hand, used pixel-value differencing by partitioning the original image into non-overlapping blocks of two consecutive pixels.

IV. CHARACTERISTICS OF STEGANOGRAPHY

Steganographic techniques embed a message inside a cover. Various features characterize the strength and weaknesses of the methods. The relative importance of each feature depends on the application .

Capacity: The notion of capacity in data hiding indicates the total number of bits hidden and successfully recovered by the Stego system

Robustness: Robustness refers to the ability of the embedded data to remain intact if the stego-system undergoes transformation, such as linear and non-linear filtering; addition of random noise; and scaling, rotation, and loose compression .

Undetectable: The embedded algorithm is undetectable if the image with the embedded message is consistent with a model of the source from which images are drawn. For

Invisibility (Perceptual Transparency): This concept is based on the properties of the human visual system or the human audio system. The embedded information is imperceptible if an average human subject is unable to distinguish between carriers that do contain hidden information and those that do not.

Security: It is said that the embedded algorithm is secure if the embedded information is not subject to removal after being discovered by the attacker and it depends on the total information about the emb

V. TECHNIQUES

A. STEGANOGRAPHY IN IMAGE IN SPATIAL DOMAIN

Steganography techniques that modify the cover image and the secret image in the spatial domain are known as spatial domain methods. It involves encoding at the LSBs level.

Least Significant Bit Substitution (LSB) [3] is the most commonly used stenographic technique. The basic concept of Least Significant Bit Substitution includes the embedding of the secret data at the bits which having minimum weighting so that it will not affect the value of original pixel.

A new steganographic method to hide a secret message into a gray -valued cover image was proposed [4]. For embedding a secret message, a cover image is partitioned into non-overlapping blocks of two consecutive pixels. In each block, a difference value is calculated from the values of the two pixels. Then that difference value is replaced by a new value to embed the value of the secret message. This method produces a more imperceptible result than those obtained from simple least-significant-bit substitution methods. The embedded secret message can be extracted from the resulting stego-image without referencing the original cover image. Iuon-Chang Lin [5] proposed a Data hiding scheme with distortion tolerance which uses spatial domain for hiding data. This method provides distortion tolerance and gives better quality of processed image. This scheme provides effective results than other schemes in terms of distortion tolerance. As LSB insertion is simpler and good for steganography, we can try to improve one of its major drawbacks: the ease of extraction. We don't want that an eavesdropper be able to read everything we are sending.

B. STEGANOGRAPHY IN IMAGE IN FREQUENCY DOMAIN

The need for enhanced security, has led to the development of other algorithms. LSB technique has weak resistance to attacks. So to overcome this shortcoming, researchers found a better way for hiding information in areas of the image that are less exposed to compression, cropping, and image processing A lossless and reversible steganography scheme has been introduced that use each block of quantized discrete cosine transformation (DCT) coefficients in JPEG images for embedding secret data [6]. In this scheme, the two successive zero coefficients of the medium-frequency components in each block are used to hide the secret data. This method results in a high image quality of stego image and successfully achieves reversibility.

A reversible data hiding scheme that use the histogram shifting method based on DCT coefficients was proposed [7]. Cover images are partitioned into several different frequencies, and the high-frequency parts are used for embedding the secret data. For hiding secret data, this method of histogram shifting shifts the positive coefficients around zero to the right and the negative coefficients around zero to the lef . It improves the hiding capacity and quality of the stego-images. On reversing the frequency domain stego-image back to the spatial domain image may cause underflow and overflow problems.

Wavelets transform (WT) converts spatial domain information to the frequency domain information. Wavelets are used in the image steganographic model because the wavelet transform clearly partitions the high-frequency and low-frequency information on a pixel by pixel basis. Many practical tests propose to use the Wavelet transform domain for steganography because of a number of advantages. The use of such transform will mainly address the capacity and robustness of the Information Hiding system features.

A Haar discrete wavelet transformation (HDWT)- based reversible data hiding method was proposed in 2009 [8]. In this method a spatial domain image is transformed into a HDWT-based frequency domain image and then the high frequency coefficients are used to embed the secret data. This method provides a high hiding capacity and a good stego-image quality.

In the recent year DWT based algorithm for image data hiding has been proposed that uses CH band of cover image for hiding the secret message. Vijay kumar [9] proposed an algorithm in which secret message is embed in different bands of cover image. PSNR has been used to measure the quality of stegano image and it gives better PSNR by replacing error block with diagonal detail coefficients (CD) as compare to other coefficients.

A new image steganography technique based on Integer Wavelet Transform (IWT) and Munkres' assignment algorithm was introduced [10]. IWT converts spatial domain information to the frequency domain information. For embedding secret data, assignment algorithm is used for best matching between blocks. Stego image is subjected to various types of image processing attacks andit shows high robustness against these attac

VI. CONCLUSION

This paper reviewed the main steganographic techniques. Each of these techniques tries to satisfy the three most important factors of steganographic design (imperceptibility or undetectability, capacity, and robustness). LSB techniques in a spatial domain have a high payload capacity, but they often fail to prevent statistical attacks and are thus easily detected.

The promising techniques such as DCT, DWT and the adaptive steganography are not prone to attacks, especially when the hidden message is small. Working at some level like that of DCT turns steganography much more powerful and less prone to statistical attacks. Embedding in the DWT domain reveals a sort of constructive results and outperforms DCT embedding.

REFERENCES

[1] N.F. Johnson, S. Jajodia, Exploring steganography: seeing the unseen, IEEE Computer 31 (2) (1998) 26–34.

[2] J.C.Judge, Steganography: past, present, future. SANS Institute publication, <http://www.sans.org/ reading room/ whitepapers/ stenganography/ 552.php>, 2001

[3] F.A.P.Petitcolas, R.J.Anderson, M.G.Kuhn:"Information Hiding- A Survey", Process of IEEE, vol.87,no.7, pp.1062-1078, July, 1999.

[4] E. Cole, Hiding in Plain Sight: Steganography and the Art of Covert Communication, Indianapolis: Wiley Publishing, 2003.

[5] T. Jahnke, J. Seitz, (2008). An introduction in digital watermarking applications, principles and problems, in: H.
Nemati (Ed), Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 554-569.

[6] M. Warkentin, M.B. Schmidt, E. Bekkering, Steganography and steganalysis, Premier reference Source–Intellectual Property Protection for Multimedia Information technology, Chapter XIX, 2008, pp. 374-380.

[7] N.N. El-Emam, Hiding a large amount of data with high security using steganography algorithm, Journal of Computer Science 3 (2007) 223-232.

[8] K. Sullivan, Z. Bi, U. Madhow, S. Chandrasekaran, and B. S. Manjunath, Steganalysis of quantization index modulation data hiding, Proc. of 2004 IEEE International Conference on Image Processing, vol. 2, pp. 1165-1168, 2004.

[9]Jar no Mielikainen, "LSB Matching Revisited", Signal Processing Letters, IEEE, Publication Date: May 2006 Volume : 13, Issue : 5, pp. 285- 287

[10] K. Gopalan. Audio steganography using bit modification. In Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '03), volume 2, pages 421–424, 6-10 April 2003.

11] Xuping Huang, Ryota Kawashima, Norihisa Segawa, Yoshihiko Abe. "The Real-Time Steganograph Based on Audio-o-Audio Data Bit Stream",Technical report of IEICE, ISEC, vol.106 pp.15-22, September 2006.

[12] Haz Malik, Steganalysis of qim steganography using irregularity measure, Proc. of the 10th ACM workshop on Multimedia and security, ACM Press, pp. 149-158, 2008.

[13] A. Delforouz, Mohammad Pooyan, "Adaptive Digital Audio Steganography Based on Integer wavelet transform ", IEEE Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2007, 26-28 Nov 2007, pp 283-286.

[14] M. Goljan, J. Fridrich, and T. Holotyak, New blind steganalysis and its implications, IST/SPIE Electronic Imaging: Security, Steganography of Multimedia Contents VIII, vol. 6072, pp. 1-13, 2006.

[15] Y. Wang and P. Moulin, Optimized feature extraction for learning-based image steganalysis, IEEE Trans. Information Forensics and Security, vol. 2, no. 1, pp. 31-45, 2007.