EasyChair Preprint

№ 253

A Survey paper on different Steganography Techniques

Shashi Kant Singh, Seema Yadav, Ankur Raj and Priya Gupta

June 14, 2018

A Survey paper on different Steganography Techniques

Shashikant Singh [1], Seema Yadav [2], Ankur Raj[3] and Priya Gupta[4]

Assistant Professor
JECRC,Jaipur,Rajasthan,India
shashikant.cse@jecrc.ac.in [1], seemayadav.cse@jecrc.ac.in[2] , ankurraj.cse@jecrc.ac.in[3] , priyagupta.cse@jecrc.ac.in[4]

Abstract

With the rapid advance in digital network, information technology, digital libraries, and particularly World Wide Web services, many kinds of information could be retrieved any time. So in this digital scenario invisible communication between two parties is the prime concern. Steganography is the technique of hidden communication. It not only hides the message contents, instead it hides the existence of the message. In this paper, a new image steganography method based on spatial domain is proposed secret data hided in image segments using least significant bit (LSB) steganography is proposed. The color image is divided into four equal parts and the secret data is also divided into four equal parts and those divided data is hided in the image segments using least significant bit steganography. In this paper we have critically analyzed various steganographic techniques and also have covered steganography overview its major types, classification, applications.

Keywords: Steganography, least significant bit, Spatial Domain, MSE, PSNR, NC.

I. Introduction

1. The advancement in digital technology with the advent of computers and internet technology has brought a revolution by transforming the world into a digital village. Some illegal eavesdroppers every time try to hack that secret data. For providing security to this secret data in digital medium there are various techniques are available[1]. Like Cryptography, Steganography, Digital watermarking etc. Basically Steganography word is derived from two Greek words “Stegos” and “Grafia” i.e. Steganographic, where Stegos means covered and Grafia means writing it means covered writing. In this technique secret message is concealed inside a cover object. There are different types of Steganography Techniques are available based on the cover object. Cover Objects can be image, Audio, Video, Protocols etc. The secret information can be embedded in various types of covers. If information is embedded in a cover text (text file), the result is a stego-text object. Similarly, it is possible to have cover audio, video and image for embedding which result in stego-audio, stego-video and stego-image respectively. The proposed paper provide a systematic survey of existing Steganography research by categorizing existing methods according to the certain features and analysing the advantages of these features. The motive of the paper is to provide researchers with in-depth study of subject.

1.1 CLASSIFICATIONS OF DIGITAL STEGANOGRAPHY

Steganography can be classified according to its importance and goals. So different types of steganography are as follows:

a) Linguistic steganography: Linguistic steganography is concerned with hiding information in natural language text. One of the major transformations used in linguistic steganography is synonym substitution [2]. However, few existing studies have studied the practical application of this approach.

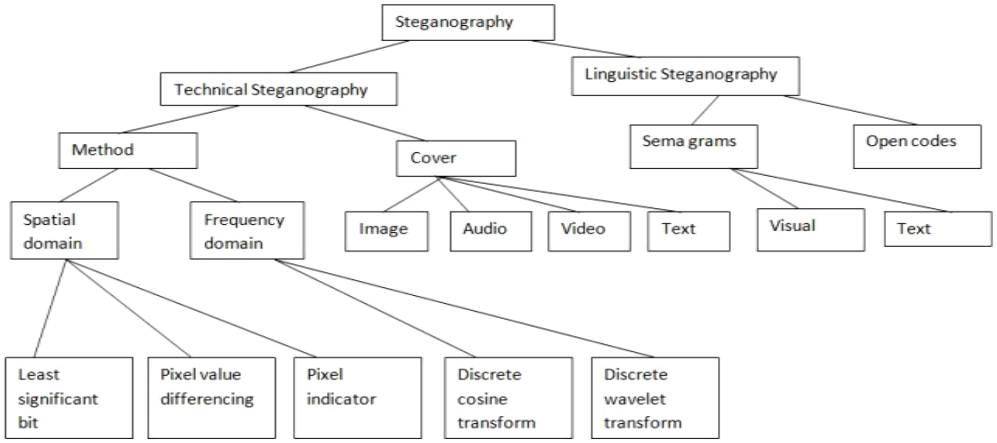

Fig.1. Types of Steganography[2]

b) Semagrams: It uses only symbols and signs to hide the information. It is further categorized into two ways:

i) Visual Semagrams: A visual semagrams uses physical objects used every day to convey a message. For example: the positioning of items on a particular website.

ii) Text Semagrams: This type is used to hides a message by modify the appearance of the carrier text, or by changing font size and type, or by adding extra space between words and by using different flourished in letters or handwritten text[3].

c) Image Steganography: Taking the cover object as image in steganography is known asimage steganography. Generally, in this technique pixel intensities are used to hide the information.

d) Network Steganography: When taking cover object as network protocol, such as TCP,UDP, ICMP, IP etc, where protocol is used as carrier, is known as network protocol steganography. In the OSI network layer model there exist covert channels where steganography can be achieved in unused header bits of TCP/IP fields[4&5]..

e) Video Steganography: Video Steganography is a technique to hide any kind of files orinformation into digital video format. Video (combination of pictures) is used as carrier for hidden information.

f) Audio Steganography: When taking audio as a carrier for information hiding it is calledaudio steganography. It has become very significant medium due to voice over IP (VOIP) popularity. Audio steganography uses digital audio formats such as WAVE, MIDI, AVI MPEG or etc for steganography[6].

g) Text Steganography: General technique in text steganography, such as number of tabs,white spaces, capital letters, just like Morse code and etc is used to achieve information hiding.

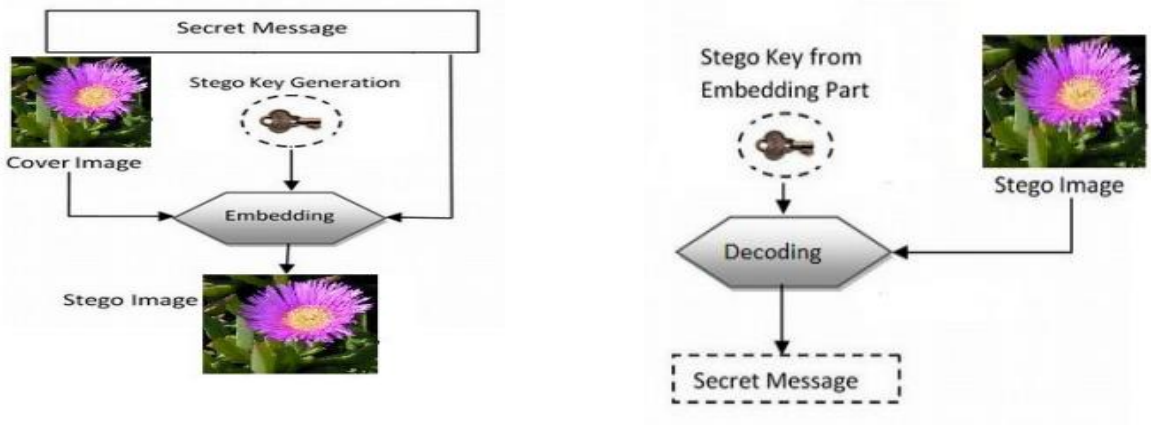

Fig.2. Block diagram of Image steganography[4]

II. LSB Method:

In LSB steganography, the least significant bits of the cover media's digital data are used to conceal the message. The simplest of the LSB steganography techniques is LSB replacement. LSB replacement steganography flips the last bit of each of the data values to reflect the message that needs to be hidden[7]. Consider an 8-bitgrayscale bitmap image where each pixel is stored as a byte representing a gray scale value. Suppose the first eight pixels of the original image have the following gray scale values.

11010010 01001010 10010111 10001100
00010101 01010111 00100110 01000011

To hide the letter C whose binary value is 10000011, we would replace the LSBs of these pixels to have the following new grayscale values:

11010011 01001010 10010110 10001100
00010100 01010110 00100111 01000011

In the above example only half the LSBs need to change. [12] The difference between the cover (i.e. original) image and the stego image will be hardly noticeable to the human eye. However, one of its major limitations is small size of data which can be embedded in such type of images using only LSB. LSB is extremely vulnerable to attacks. LSB techniques implemented to 24 bit formats for the color image are difficult to detect contrary to 8 bit format[8]. It is observed that there are little differences in the histograms of cover and stego image of Lena. For other images, similar characteristics are obtained.

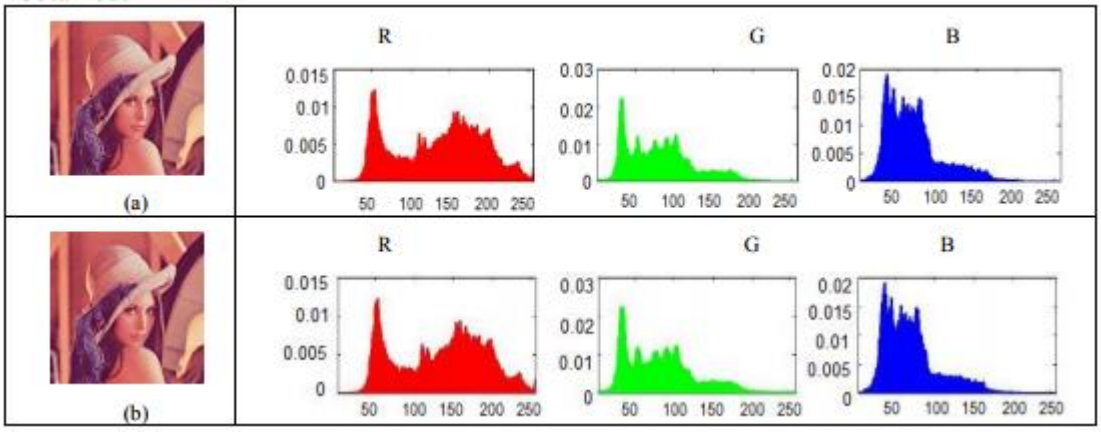

Fig.3. Cover and Stego Images of Halena: (a) Cover Image and RGB Histograms (b) Stego Image and RGB Histogram[3]

From above experimental results, it is apparent that each stego-image is almost analogous to corresponding cover image and shows better imperceptibility. That is, deterioration of the quality of images due to the embedding of the secret messages cannot be distinguished.

III. ADVANTAGES

Steganography has unique advantages for net-espionage agents. Even if a file is known or suspected to contain Steganographic software, it is almost impossible to extract the information until the correct password is obtained. Steganography is beneficial for securely storing sensitive data, such as hiding system passwords or keys within other files[9]. In places where standard cryptography and encryption is outlawed, Steganography can be used for covert data transmission.

IV. CONCLUSION

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. It is therefore a book on magic. It is emerging in its peak because it does not attract anyone by itself [24]. A Review of Comparison Techniques of Image Steganography LSB, DCT & DWT methods has been successfully implemented and results are delivered. The MSE and PSNR of the methods are also compared and also this paper presented a background discussion and implementation on the major algorithms of steganography deployed in digital imagin[10].

V . FUTURE SCOPE

Still efforts have to be made to increase the embedding capacity and maintain secrecy. In this method we can hide text file equal to the size of the image. Efforts can be made to hide text files having more size than image size. The secret keys have to be known to both sender and receiver. Keys are not sent in cover-images but are distributed separately. A technique can be evolved so that these keys can be generated and distributed covertly. The Transform Domain method can be utilized if more security is required[11]. If Steganography is used with Cryptography, it will prove to be an unbeatable tool in secure communication links. Security of the scheme can be improved by using advanced cryptography techniques and also improve the efficiency by using data compression techniques.

References:

[1]. A. A. Ali and A. H. Seddik, “Image Steganography Technique By Using Braille Method of Blind People (LSBraille)”, International Journal of Image Processing (IJIP), Vol. 7, Issue 1,PP. 81-89, 2013.

[2] A. Ahmed, N. Agrawal, and S. Banerjee, “Image steganography by closest pixel-pair mapping”, IEEE- International Conference On Computing, Communications and Informatics (ICACCI), PP. 1971 - 1975, 24-27 Sept. 2014.

[3] A. Nag, S. Ghosh, S. Biswas, D. Sakar, and P.P. Sakar, “An Image Steganography Technique using X-Box Mapping”, IEEE- International Conference On Advances In Engineering, Science and Management(ICAESM-2012), Vol. 3, Issue 12, PP. 709-713, March 2012.

[4] A. A. Ali and A. H. Seddik, “New Image Steganography Method By Matching Secret Message With Pixels Of Cover Image (SMM)”, International Journal of Computer Science Engineering and Information Technology Research (IJCSITR), Vol. 3, Issue 2 ,PP. 1-10, Jun 2013.

[5] S. Nazari, A-M. Eftekhari, and M. Sh. Moin, “Secure Information Transmission using Steganography and Morphological Associative Memory”, International Journal of Computer Applications, Vol. 61, No. 7, PP. 23-29, January 2013.

[6] K.Thangadurai and G.Sudha Devi, “An analysis of LSB based image Steganography techniques,” Computer Communication and Informatics (ICCCI), International Conference on 3-5 Jan. 2014, pp.1 – 4, Publisher: IEEE.

[7] Amritpal Singh and Harpal Singh, “An improved LSB based image Steganography technique for RGB images,” Electrical, Computer and Communication Technologies (ICECCT), IEEE International Conference on 5-7 March 2015, pp. 1- 4.

[8] Deepesh Rawat and Vijaya Bhandari, “ A Steganography Technique for Hiding Image in an image using LSB Method for 24 Bit color Image,” International Journal of Computer Application (0975-8887) Volume 64-No.20, February 2013.

[9] Rawat D., Bhandari V., Steganography Technique for Hiding Text Information in Color Image using Improved LSB Method, International Journal of Computer Applications 67(1) (2013), 22- 25.

[10] A. Saha, S. Halder and S. Kollya, “Image Steganography using 24-bit Bitmap Images”, Proceedings of the 14th International Conference on Computer and Information Technology (ICCIT), Bangladesh, (2011) Noveber 22-24.

[11] M. O. Islam, “A High Embedding Capacity Image Steganography using Stream Builder and Parity Checker”, Proceedings of the 15th International Conference on Computer and Information Technology (ICCIT), Dhaka, Bangladesh, (2012) Noveber 22-24.

[12] N. Akhtar, S. Khan and P. Johri, “An Improved Inverted LSB Image Steganography”, Proceedings of the International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), (2014) February 7-8.