ISSN: 2321-7782 (Online)
Volume 2, Issue 11, November 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Hiding Image in Image by using FMM with LSB Substitution in Image Steganography

Praneeta Dehare[1]
M.E. (CTA) Scholar
Department of Computer Science and Engineering
SSGI, SSTC Bhilai
Bhilai (C.G.) – India

Padma Bonde[2]
Sr. Associate Professor
Department of Computer Science and Engineering
SSGI, SSTC Bhilai
Bhilai (C.G.) – India

Abstract: ***In this electronic era, communicate confidential information through a public network channel becomes an important task. So that sending any secret information can be done by using Steganography. Steganography refers to the process of hiding secret information inside an appropriate multimedia carrier e.g. image, audio and video files. Today, most of the electronic data send through the wireless network, so there is a chance of hacking from the medium where communication takes place. The main objective of using steganography is to transmit information securely, which is completely undetectable from the medium. In this paper image steganography has used to transmit secret image, where an image is used as medium to hide the secret image, called cover image. For implementing the image steganography where a secret image hides into cover image, method uses two techniques. The embedding of images done by using two algorithms, first algorithm called five modulus methods and second is LSB substitution technique. In embedding process, secret image apportioned into two parts. The first part have size of 75% of secret image that uses FMM algorithm and rest of the 25% of secret image uses LSB substitution to hide into cover image. To provide more security a private stego-key is also used with FMM algorithm so that detection of secret image from the cover image becomes more difficult for any unauthorized recipients. Therefore, nesting of two algorithm with a password make it difficult for any opponent (who has not involved in communication parties) to extract the hidden image from cover image.***

Key words: Image Steganography, Cryptography, Secret Key, Five Modulus Method, LSB, Security.

I. INTRODUCTION

In the field of digital communication, the exponential growth of information technology has been observed. This enhancement is useful for remote users but it has some drawback too is that the unintended recipients can also use this facility. So, the major problem comes when the digital communication need to send any secret message through a public cannel. In that case some technique may use to secure the secret information. In one of this popular mechanism is Steganography. In today's electronic era, steganography plays a major role for hidden communication. Steganography means as "concealed writing", i.e. a Greek Origin. It is made of Greek words originated as far back as 440(B.C.), where *steganos* stands for covered or protected and *graphei* is for writing. In the applied mechanism under steganography has ability to hide information in cover media, so that no one apart from the intendant recipients even knows that the message transmission is taking place. Now a day's the rapid growth of wireless communication has increased through the development of electronic devices. So when any secret message transmitted by using these electronic devices security and privacy has desired. When the data transmission placed on channel many hackers could try to extract the messages from channel, so that possibility of intrusion increased when the systems used internet extensively. Therefore, sharing information becomes major issue for user and developer when using wireless communication. To resolve this problem steganography used through various digital media like text, image, audio and video files. To secure secret data from any adversary, cryptography can also use, but the advantage of steganography over cryptography is that the steganography hides the existence of communication, where cryptography allowed the unintended

recipients to detect the transmission of information on channel; it only keeps the contents of a message secret. Steganography and Cryptography are counter parts in digital security [1]. Secret data can be hiding in any digital medium. To explain the procedure R. Doshi, P. Jain and L. Gupta [2] provides a generic description of the pieces of the steganographic process as:

cover_medium + hidden_data + stego_key = stego_medium.

II. Related Work

In the process of data hiding for embedding the information into any digital content can be done by using steganography techniques without causing perceptual. The popular techniques, which are used for data hiding, are watermarking, steganography and cryptography. In ancient Greek, research on steganography techniques has done. On that time a secret message tattooing on the shaved head of a messenger and before sending him to the destination letting his hair to grow back. In around 400 B.C. the famous method used is tradition steganography technique in which the document marked with invisible ink lie lemon juice.

Many techniques have been proposed for image steganography. The image steganography based on the image format. The image format is classified into two categories – (i) Spatial Domain, and (ii) Transform Domain. In the Spatial Domain format the most popular technique which is the simplest and widest known steganography method is Least Significant bit, which replaces the least significant bit of pixels selected to hide the content that holds information. Complete discussion on LSB could be found in [3]. Some more methodology has been proposed by using LSB substitution in [4] and [5]. Further an improved LSB substitution method used by V. K. Sharma and V. Shrivastava in [6], where MSB of secret image in to LSB of cover image get embedded. A. Sharma, A. Agrawal and V Kumar introduced a technique [7], where large amount of data could be hidden in enciphered with the help of secret key, which is then embedded at the end of image and then again deciphered with the help of same key. Many researcher have been discussed are several another steganography techniques to hide data inside in image in [8-11]. El-Sayed M. El-Alfy and Azzat A. Al-Sadi [8] used the pixel-value differencing method, where the grayscale/color changes by adopting the number of embedded bits, which leads to increase the capacity of embedding without losing quality of image. a randomization method has been proposed by Joyshree Nath and Asoke Nath [9] where the randomized key matrix generated by encryption and decryption. They used two methods (i) the secret message encrypted, and (ii) the encrypted secret message inserted into the cover file. Ajit Danti and Preethi Acharya [10] presented, a novel image steganography method based on randomized bit embedding. This method has done by using two processes; first the Discrete Cosine Transform (DCT) of the cover image obtained then the stego image constructed by hiding the secret image in Least Significant Bit of he cover image in random locations. Matus Jokay and Tomas Moravcık [11] deal with the steganographic algorithm LSB (Least Significant Bits) in images (JPEG), where the main concentration is to minimize the number of modified DCT coefficients using Hamming codes. Some good theoretical knowledge about steganography and steganalysis could be studied in [12-14].Times is specified, Times Roman or Times New Roman may be used. If neither is available on your word processor, please use the font closest in appearance to Times. Avoid using bit-mapped fonts if possible. True-Type 1 or Open Type fonts are preferred. Please embed symbol fonts, as well, for math, etc.

III. Basic of Implementation

Embedding of information or message like plain text, cipher text, images, audio or video through steganographic technique; is to be hidden into an another digital file. The information hiding is based on three different features: security, capacity and robustness. Capacity can say as to measure the amount of information that could be hidden in the cover media, security refers to as inability of an unauthorized recipients's to detect hidden information and robustness is on to the amount of modification on stego medium can withstand before an adversary can destroy hidden information [11].

This paper embeds the information and hides into a digital media by using image steganography. In image steganography, the image which holds the hidden information called cover image and second file is the message which is to be hidden. The second file or secret message could be any digital file. Watermarking and steganography both are work for information hiding, where watermarking concentrate on to the high level of robustness and steganography focuses on security and capacity of the embedded data. While embedding the data into cover media, it is necessary that the intended recipients knows the secret key when the steganography communication is taking place between them.

On the basis of image format many different ways and techniques used to hide information in image. Some known methods which included the secret data into image are;

- Least significant bit insertion,
- Masking and filtering and,
- Transformation techniques and algorithm.

These techniques could be applied with varying degrees of success on different image files [14].

IV. PROPOSED METHODOLOGY

For implementing image steganography this paper used two methods called Five Modulus Method proposed by Firas A. Jassim [15] and LSB Substitution method. The proposed method intends to use of image steganography, where an image (secret) can transfer in an image (cover) by nesting the methods five modulus method and LSB Substitution. In proposed technique,

- The secret image gets partitioned into two parts. The first part has 75% of the size of original secret image and hides into cover image by applying Five Modulus Method and second part has 25% of the size of original secret image which uses LSB substitution method to hides into cover image. Moreover, a private stego-key also combined with this algorithm to make it difficult for any unauthorized recipients to extract the secret image from the cover image.
- The Stego Image has sent through the channel to the authorized recipients to whom secret image needs to be transferred.
- On the receiver side the stego image receives, and by applying the same algorithm and private stego key the secret image extracted from the cover image. the procedure for proposed methodology is given in below figure –

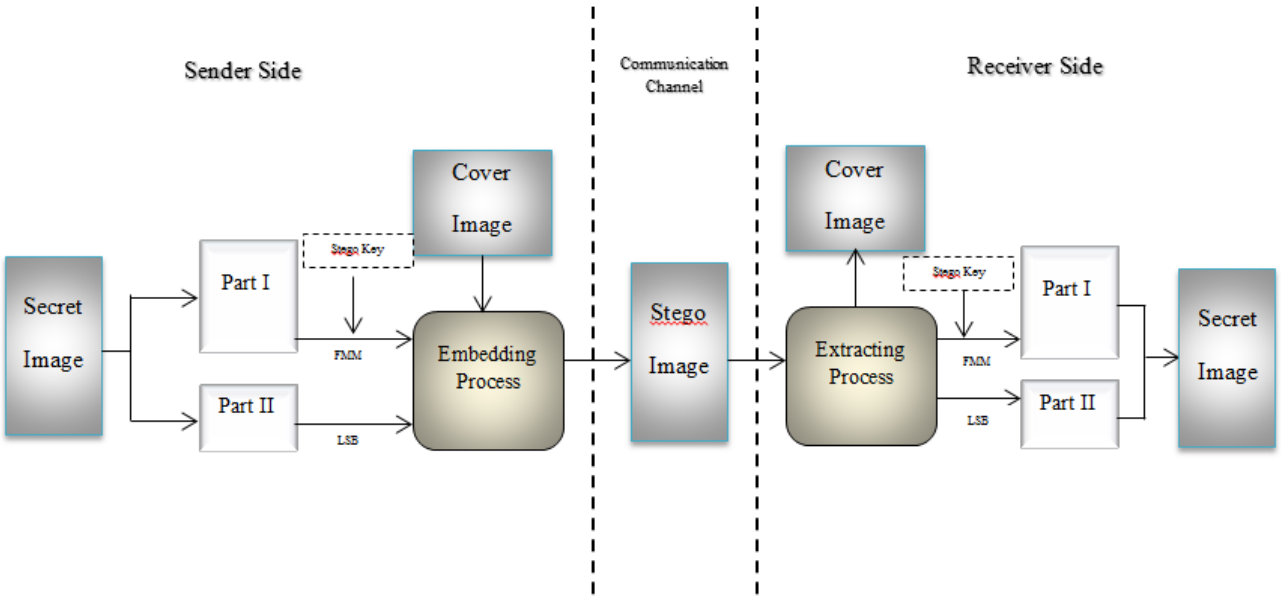

Figure – Implementation of Proposed Methodology

i. **Five Modulus Method**

The main objective of using FMM is to transform the whole image into multiples of five. This technique used a digital image. **Digital Image Background** – A Digital image is representing as a rectangular array of dots or pixels, arranged in M (rows) X N (columns) array. In color representation of image the Grey-scale image uses 1 byte to represent each pixel value whereas the digital color image's each pixel stored into three bytes; the pixel of array constructed by combining 3 different channel (RGB), where each channel represent a value from 0 to 255. So that applying FMM technique, transforms each pixel value of image in multiples of five. In that case the pixel value range 0…255 is reduces to range 0…51 with 52 distinct numbers, i.e. 0, 5, 10, 15… 200, 205 ….250, and 255. To find the pixels value and place we can partition the image in number of k x k windows. The FMM method will be applied for both the cover and the stego images.

ii. **Least Significant Bit Substitution Method**

It is the simplest and widest known technique for image steganography. This steganographic algorithm works for 8bit (grayscale) or 24 bit (colour image). By using of this algorithm the quality of image can be maintain by changing the negligible variations to each pixels of the image so that the visibility is indictable. Based on Logical operation the algorithm embeds 1 pixel value of secret image to the least significant bit of the pixel value of cover image. The efficiency can be enhanced by using this algorithm because the algorithm allows low computational complexity.

V. Expected Outcome

This paper introduced two methods for implementing image steganography and the methods nested to provide more security. The Five Modulus Method reduces the original pixels range from 0...255 into 0...51. This method provides a good image quality without any dissimilarity between the original image and constructed image, as well as the LSB provides a low data computation complexity. To provides more security a private stego key also used while using FMM algorithm that makes the extraction of secret image from the communication channel more difficult for unauthorized recipients. By using these two methods a good balance between the security and image quality can be achieved.

References

1. S. Sivasubramanian and J. Raju, Advanced Embedding of Information by Secure Key exchange via trusted third party using Steganography, International Journal of Latest Research in Science and Technology, vol. 2, issue 1, pp. 536-540, Jan – Feb 2013.
2. R. Doshi, P. Jain and L. Gupta, Steganography and Its Applications in Security, International Journal of Modern Engineering Research (IJMER), Vol. 2, issue 6, pp. 4634-4638, ISSN: 2249-6645, Dec 2012.
3. R. Chandramouli and N. Memon, Analysis of LSB based image steganography techniques, Proceedings 2001 International Conference on Image, Vol. 3, pp. 1019-1022.
4. M. Nosrati, R. Karimi and M. Hariri, Embedding Stego-Text in Cover Images Using linked List Concepts and LSB Technique, World Applied Programming, Vol 1, pp. 264-268, ISSN: 2222-2510, October 2011.
5. H. Al-Bahadili, A Secure Block Permutation Image Steganography Algorithm, International Journal on Cryptography and Information Security (IJCIS), Vol.3, No. 3, September 2013.
6. V. K. Sharma and V. Shrivastava, A steganography algorithm for hiding image in image by improved LSB substitution by minimizes detection, Journal of Theoretical and Applied Information Technology, Vol. 36, ISSN: 1992-8645, Feb. 2012.
7. A. Sharma, A. Agarwal and V. Kumar, A simple technique for steganography, arXiv: 1307.8385v1 [cs.MM] 31 Jul 2013.
8. El-Sayed M. El-Alfy and Azzat A. Al-Sadi, Pixel-Value Differencing Steganography: Attacks and Improvements, The Second International Conference on Communications and Information Technology (ICCIT), Feb 2012.
9. J. Nath and A. Nath, Advanced Steganography Algorithm using Encrypted secret message, International Journal of Advanced Computer Science and Applications, IJACSA, Vol. 2, No.3, March 2011.
10. A. Danti and P. Acharya, Randomized Embedding Scheme Based on DCT Coefficients for Image Steganography, IJCA Special Issue on Recent Trends in Image Processing and Pattern Recognition RTIPPR, 2010.
11. M. Jokay and T. Moravcik, Image-Based Jpeg Steganography, Tatra Mt. Math. Publ. 45, 65–74. DOI: 10.2478/v10127-010-0006-9, 2010.
12. N. Provos and P. Honeyman, Hide and Seek: An Introduction to Steganography, Security & Privacy, IEEE, Vol. 1, Issue 3, pp. 32 – 44, ISSN: 1540-7993, June 2003.
13. B. Dunbar, A Detailed look at Steganographic Techniques and their use in an Open-Systems Environment, SANS Institute 2002.

14. N. F. Johnson and S. Jajodia, Exploring Steganography: Seeing the Unseen, IEEE Computer, Vol. 31, Issue 2, p. 26-34, ISSN: 0018-9162, Feb. 1998.

15. F. A. Jassim, Hiding Image in Image by Five Modulus Method for Image Steganography, Journal of computing, Vol. 5, issue 2, 2151-9617, April 2013.

