NESTING OF FIVE MODULUS METHOD WITH IMPROVED LSB SUBTITUTION TO HIDE AN IMAGE IN IMAGE

Praneeta Dehare[1], Sheela Verma[2]

[1]*M.E (CTA) Scholar, Department of Computer Science & Engineering, SSGI, SSTC, Bhilai, Chhattisgarh, India*
[2]*Assistant Professor, Department of Computer Science & Engineering, SSGI, SSTC, Bhilai, Chhattisgarh, India*

Abstract

Steganography refers to the process of hiding secret message inside an appropriate multimedia carrier e.g. image, audio and video files. Today, by using of wireless communication more data are available electronically, which can leak from the medium where the data transmission takes place. The goal of steganography is to communicate very securely, which is completely undetectable from the medium. In this paper image steganography has used, where a secret image can transfer within an image called cover image. To hide a secret image in cover image, both the images embedded by using two techniques. The first algorithm called five modulus methods applied on the half of the both images (Secret and Cover Image) and rest of the parts of images embedded with improved LSB substitution technique. A private stego-key is also used on half parts of both images while applying FMM algorithms to make the detection of secret image from the cover image more difficult for any unauthorized recipients. The paper uses two algorithms for embedding the both secret and cover images, so for nesting of two algorithms make it difficult for any opponent (who has not involved in communication parties) to extract the hidden image from cover image.

Keywords: *Image Steganography, Cryptography, Five Modulus Method, Improved LSB Substitution, Security.*

----------***----------

1. INTRODUCTION

In today's electronic era, steganography is an art and science of hidden communication. The word steganography is of Greek origin and means "concealed writing" from the Greek words where *steganos* stands for covered or protected and *graphei* is for writing, which originated as far back as 440(B.C.). Steganography is an 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.

Through the development of electronic devices, the rapid growth of wireless communication has increased. Security and privacy in these wireless communications has desired when any secret or confidential information has shared between two parties. Many hackers try to attack on channels where the data transmission has processed. So the possibility of intrusion increased when the systems used internet extensively. Therefore sharing information via internet becomes a major issue for user and developers. To overcome on this problem steganography has used through various digital media like text, image, audio and video files. 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. Secret information can be hidden inside any cover information. To explain the procedure R. Doshi, P. Jain and L. Gupta [5] provides a generic description of the pieces of the steganographic process as:

cover_medium + hidden_data + stego_key = stego_medium.

The main aim of using the steganography is to prevent detection of secret information from the unauthorized parties.

2. RELATED WORK

The data hiding process for embedding the information into any digital content can be done by steganography techniques without causing perceptual. To hide data, the popular techniques used 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. The famous method used in around 400 B.C. is tradition steganography technique in which the document marked with invisible ink lie lemon juice.

There are various techniques proposed for image steganography. 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 [1]. Further an improved LSB substitution method used by V. K. Sharma and V. Shrivastava in [3], where MSB of secret image in to LSB of cover image get embedded. A. Sharma, A. Agrawal and V Kumar introduced a technique [4], 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. There are several another steganography techniques to hide data inside in image discussed by many researchers in [6-9]. El-Sayed M. El-Alfy and Azzat A. Al-Sadi [6] 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. Joyshree Nath and Asoke Nath [7] introduced a randomization method where the encryption and decryption takes place for generating the randomized key matrix. 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 [8] 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 [9] deal with the steganographic algorithm LSB (Least Significant Bits) in images (JPEG). It concentrates on minimizing of the number of modified DCT coefficients using Hamming codes. Also, good theoretical knowledge about steganography and steganalysis could be studied in [10-12].

3. BASICS OF EMBEDDING DATA

In steganographic technique embedding of information or message, which is form of any media files like plain text, cipher text, images, audio or video; is to be hidden into an another digital file. There are three different features in information hiding system: security, capacity and robustness. Capacity refers to the amount of information that could be hidden in the cover media, security to an unauthorized recipients's inability to detect hidden data, and robustness is on to the amount of modification on stego medium can withstand before an adversary can destroy hidden information [9].

This paper uses the image steganography for embedding the information. The image which holds the hidden information called cover image. The second file is the message which is to be hidden. This message could be any digital file.

Information hiding system relates with both watermarking and steganography, 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.

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 [12].

4. PROPOSED METHODOLOGY

This paper used two methods called Five Modulus Method and Improved LSB Substitution method, proposed by Firas A. Jassim [2] and V. K. Sharma - V. Shrivastava [3] respectively. 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 Improved LSB Substitution.

In proposed technique,

- The secret image gets partitioned into two parts. The first part of the image hides into cover image by applying Five Modulus Method. 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.

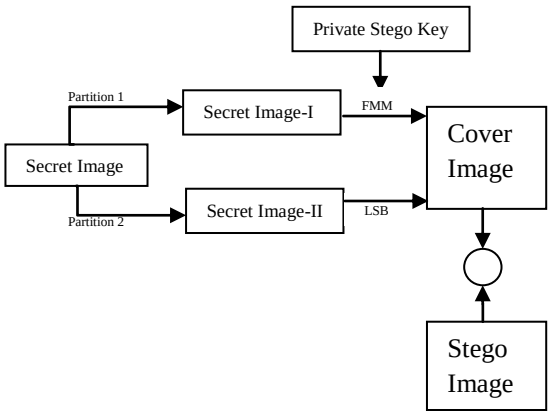

Fig -1: Embedding Secret Image in Cover Image (Sender Side)

- The Stego Image has sent over the channel to the recipients, where the secret image needs to be transferred.
- On the receiver side the stego image receives, and by applying the same private stego key, the secret image extracted from the cover image.

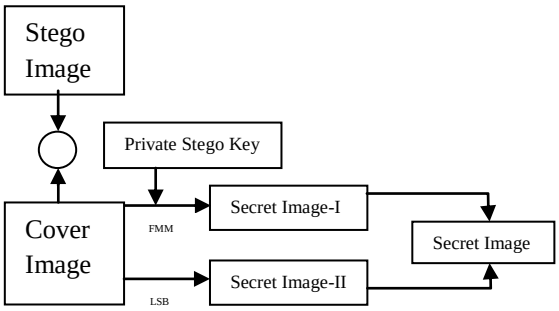

Fig -2: Extracting the Secret Image from Cover Image (Receiver Side)

4.1 Five Modulus Method

Idea behind FMM is to transform the whole image into multiples of five. Proposed 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 digital color image, 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. To find the pixels value and place we can partition the image in no of k x k windows. The FMM method will be applied for both the cover and the stego images.

4.2 Improved LSB Substitution Method

It is a steganographic algorithm for 8bit (grayscale) or 24 bit (colour image). Based on Logical operation algorithm embedded MSB of secret image in to LSB of cover image. This way, the cover image's n LSB, from a byte is replaced by secret image's n MSB. The image quality of the stego-image could be improved with low extra computational complexity. Better PSNR is achieved by this technique because results show that the stego-image is visually indistinguishable from the original cover-image when n<=4, where n= number of Significant Bits.

5. EXPECTED OUTCOME

This paper proposed the two methods which are nested to provide more security on image steganography. The Five Modulus Method reduces the original pixels range from 0...255 into 0...51. It provides a good image quality without any dissimilarity between the original stego image and constructed stego image. The LSB provides a low data computation complexity. A stego key also used with the cover image to make the way of extracting information 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]. R. Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques", Proceedings 2001 International Conference on Image, Vol. 3, pp. 1019-1022.
[2]. Firas A. Jassim, "Hiding Image in Image by Five Modulus Method for Image Steganography" Journal of computing, volume 5, issue 2, April 2013, 2151-9617.
[3]. Vijay Kumar Sharma and Vishal Shrivastava, "A steganography algorithm for hiding image in image by improved LSB substitution by minimizes detection", Journal of Theoretical and Applied Information Technology, volume 36, February 2012, ISSN: 1992-8645.
[4]. Adity Sharma, Anoo Agarwal and Vinay Kumar, "A simple technique for steganography", arXiv: 1307.8385v1 [cs.MM] 31 Jul 2013.
[5]. R. Doshi, P. Jain and L. Gupta, "Steganography and Its Applications in Security", International Journal of Modern Engineering Research (IJMER), Volume 2, Issue 6, pp. 4634-4638, ISSN: 2249-6645, Dec 2012.
[6]. 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.
[7]. Joyshree Nath and Asoke Nath, "Advanced Steganography Algorithm using Encrypted secret message", International Journal of Advanced Computer Science and Applications, (IJACSA, Volume. 2, No.3, March 2011.
[8]. Ajit Danti and Preethi 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.
[9]. Matus Jokay and Tomas Moravcik, "IMAGE-BASED JPEG STEGANOGRAPHY", Tatra Mt. Math. Publ. 45 (2010), 65–74. DOI: 10.2478/v10127-010-0006-9.
[10]. Niels Provos and Peter Honeyman, "Hide and Seek: An Introduction to Steganography", Security & Privacy, IEEE, Volume 1, Issue 3, p. 32 – 44, ISSN: 1540-7993, June 2003.
[11]. Bret Dunbar, "A Detailed look at Steganographic Techniques and their use in an Open-Systems Environment" SANS Institute 2002.
[12]. Neil F. Johnson and Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", Computer, Volume 31, Issue 2, p. 26-34, ISSN: 0018-9162, Feb. 1998.

BIOGRAPHIES

Praneeta Dehare is a final year student of ME (CTA) of SSGI, SSTC, Bhilai, Chhattisgarh. She holds a bachelor's degree (BE) in Computer Science & Engineering from Chhattisgarh Swami Vivekananda Technical University. Her area of interest in the field of research includes Cryptography & Steganography.

Sheela Verma is an Assistant Professor in Department of CSE in SSGI, SSTC, Bhilai, Chhattisgarh. She holds a Master's degree (ME) in Computer Technology & Application and Bachelor's degree (BE) in CSE. She has 4 years of experience with area of specialization in the Field of Cryptography and Steganography.