A SURVEY OF IMAGE STEGANOGRAPHY

Vikranth.B.M[1], Muzammil Hasan Momin[2], Sayed Muneer Mohsin[3], Saurav Rimal[4], Saswat Raj Pandey[5]
*Department Of Computer Science and Engineering, BMSCE, Bengaluru

***Abstract*--Image Steganography is the art of hiding information within an image which is implied to act as a carrier image[14]. The secret message to be transmitted is then encrypted within this carrier image with a secret shared key. This process is achieved by changing the LSB of the pixels within the image to the bits of the data. Multiple algorithms have been suggested which offer different techniques to carry out the steganographic process. Some techniques that we have researched are the Enhanced LSB, F5, JSteg/JPHide and YASS. This paper outlines the proposed benefits and limitations of these techniques and suggests a suitable technique to carry out the steganographic process.**

Keywords: StegoFile, Encryption, Encryption, Cover Image, LSB

1. INTRODUCTION

Steganographic techniques have been used extensively throughout history. It involves hiding information in a cover document or file. This may be achieved using a selected algorithm to hide data. A cover file may be of any extension. Image steganography[10] hides data within a carrier image (.jpg or .png) creating a stego image wherein the LSB of the pixel is replaced with the bits of the message file. Watermarking is an important feature of image steganography that aids in verifying the authenticity of a file created by a certain user. The process of analysing an image to verify the existence of a secret message is called steganalysis. Image steganography may also be used by governments to transfer top secret documents.

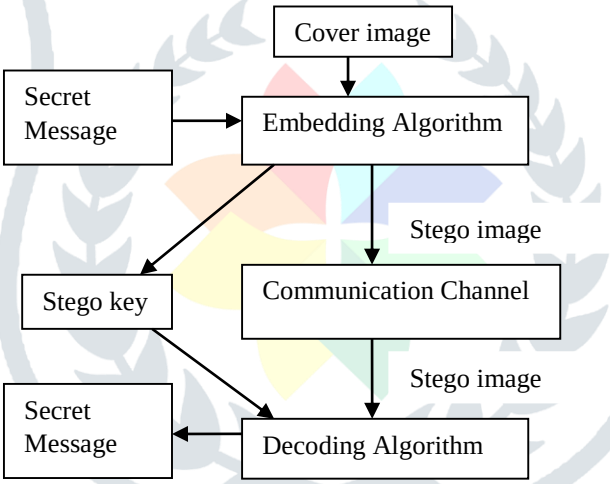

Figure 1.1: Block diagram of Image Steganography

2. LITERATURE SURVEY

EVALUATION METRICS: The metrics that are taken as the basis of evaluation for determining the efficiency of an algorithm with respect to image steganography are given below.

A relative embedding strength factor (ESF) is used for embedding the message in the cover-image Signal-to-noise ratio (SNR) is the ratio of signal power to noise power. Lesser value of this metric indicates less noise created in the image. Peak signal-to-noise ratio (PSNR) is another metric used to evaluate the quality of reconstruction of the image or the distortions created in the image during lossy compression of images in image steganography. A larger value of PSNR indicates less distortions created in the image. As ESF increases, PSNR value decreases. Mean Square Error(MSE) measures the mean square error of a cover image which can calculated and compared to other steganographic algorithms. A lesser value of MSE indicates less distortions in an image. As ESF increases, MSE value increases. Cross Correlation Code is a parameter that helps us to distinguish between the cover image and the stego image provided the mean value of the cover image and stego image is known. It decreases slowly up to a value for ESF and then rapidly starts decreasing. Entropy is a statistical measure that measures the randomness which later can be used to characterize the texture of the input image. This tends to increase with the ESF's increasing value.[1]

OVERVIEW OF EXISTING WORK

This paper gives an idea on the various algorithms present to carry out the Steganographic processes. Some acceptable guidelines for data hiding are:

*The cover image and output (stego image) should be identically similar.
*Capable to withstand any attack inflicted upon it by an attacker
*Able to carry a maximum amount of information payload based on the size of the image.
*Security may be implemented using a key for the encryption and decryption processes.

STUDY ON STEGANOGRAPHIC ALGORITHMS

The study of the steganographic algorithms can be done based on various criteria. DWT (Discrete Wavelet Transform): Decomposed into 4 parts: LL, HL, LH and HH. Any information encrypted within LL can survive an attack and/or compression.IWT (Integer Wavelet Transform): Used for a more efficient approach to lossless compression. In DWT where integers are removed from the input resulting in difficulty in recreating the original image, IWT output maps integers to integers.

Proposed method: The input is 128*128 where the cover image is 256*256.A key is generated to allow for a confidential transportation of image .This key is hidden within the cover image using IWT.

Key Generation and Embedding: Involves the use of DWT. Generated key is then encrypted using exclusive or operation and hidden within the cover image using IWT.[2]

The information contained within the paper provide an alternate method of encrypting data creating images with high PSNR values when compared to other methods.

The algorithm used, hides data within the middle bit planes which may be considered more secure. The encryption key is assumed to be sent to the recipient by some secure form of communication.

Blowfish and RC6 may be used to encrypt the key to vastly improve upon the security. The key is also assumed to be hidden with the cover image.

ALGORITHMS

The Hide & Seek approach replaces LSB of the pixel with the bits of the message to be hidden. The modified approach of this technique, Hide & Seek**:** Randomised Approach**,** scatters the bits of the message amongst the pixel of the image; thereby making it harder to detect using a single algorithm

JSteg/JPHide is another technique that replaces LSB of only non-zero quantized DCT coefficients with the bits of the data to be transferred. In F5 Algorithm, DCT coefficients are first reduced by the f5 algorithm which aids in the prevention of chi square attacks. This method also reduces the alterations needed in the cover image. The YASS (Yet Another Steganographic Scheme) is a technique where nput data is first split into blocks of a pre-selected size, Sub block is selected which is then encrypted into the DCT coefficients of the blocks. The combination of blocks is inversed and used as a JPEG image. The paper analyses the various possible solutions to create a steganographic image. Depending on the laws of a country governed by a specific government which under laws certain steganographic techniques, new methods are routinely created based on suitable research. [5]

3. CONCLUSION

From this project we hope to create a software capable of successfully encrypting files within a stego image with a key. The key may be transported securely to the receiver who may separate the stegan file into the constituent files.

This application may be used by users who wish to securely transfer files. History has shown that governments have been known to use image steganography to transfer documents securely between allied nations. An extended use of this application includes watermarking to verify the authenticity of the document to point to a user responsible for creating the file.

ACKNOWLEDGEMENT

The work reported in this paper is supported by the college through the TECHNICAL EDUCATION QUALITY IMPROVEMENT PROGRAMME [TEQIP-II] of the MHRD, Government of India.

REFERENCES

[1] Mazhar Tayel, Hamed Shawky, "A Proposed Assessment Metrics for Image Steganography", International Journal on Cryptography and Information Security (IJCIS), Vol. 4, No. 1, March 2014
[2] Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath, "A Secure Color Image Steganography In Transform Domain ", International Journal on Cryptography and Information Security (IJCIS), Vol.3, No.1, March 2013
[3] Niels Provos and Peter Honeyman, " Hide and Seek: An Introduction to Steganography, 2003", - Volume 3, Issue 7, July 2013 ISSN: 2277 128X
[4] Priya Thomas, "Literature Survey On Modern Image Steganographic Techniques ", Vol. 2 Issue 5, May-2013 ISSN: 2278-0181
[5] Chinchu Elza Andrews, Iwin Thanakumar Joseph ,"AN ANALYSIS OF VARIOUS STEGANOGRAPHIC ALGORITHMS" , International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 2, Issue 2, February 2013
[6] Wai Wai Zin, "Message Embedding In PNG File Using LSB Steganographic Technique" ,International Journal of Science and Research(IJSR) Volume 2 Issue 1, January 2013

[7] Shilpa Gupta1, Geeta Gujral, Neha Aggarwal, "Enhanced Least Significant Bit algorithm For Image Steganography ", IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2013 ISSN (Online): 2230-7893
[8] Gabriel Macharia Kamau Stephen Kimani Waweru Mwangi, "An enhanced Least Significant Bit Steganographic Method for Information Hiding ", Journal of Information Engineering and Applications ISSN 2224-5782 (print) ISSN 2225-0506 (online) Vol 2, No.9, 2012
[9] Shailendra Gupta, Ankur Goyal, Bharat Bhusan, " Information Hiding Using Least Significant Bit Steganography and Cryptography",I. J. Modern Education and Computer Science, Vol. 6, Pages No. 27-34, 2012.
[10] Arvind Kumar Km. Pooja , "Steganography- A Data Hiding Technique ", International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010
[11] Kathryn Hempstalk, "Hiding Behind Corners: Using Edges in Images for Better Steganography"
[12] Ross J. Anderson, Fabien A.P. Petitcolas, "On The Limits of Steganography", IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 1998. Special Issue on Copyright & Privacy Protection. ISSN 0733-8716.
[13] Anil Kumar, Rohini Sharma, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique "
[14] Behrouz A Forouzan, Debdeep Mukhopadhyay, "Cryptography and Network Security 2nd Edition", ISBN-10: 007070208X, ISBN-13: 9780070702080, 2011
[15] International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-5) Data Security with Image Clustering using Steganography Mitali Garg, Vikas Wasson Research scholar, Computer Science Department Chandigarh University, India
[16] International Journal on Cryptography and Information Security (IJCIS), Vol.3, No. 3, September 2013 DOI:10.5121/ijcis.2013.3302 11 A SECURE BLOCK PERMUTATION IMAGE STEGANOGRAPHY ALGORITHM Hussein Al-Bahadili Faculty of Information Technology, University of Petra, Amman, Jordan
[17] International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-5) Steganography Techniques –A Review Paper Jasleen Kour Deepankar Verma M-tech Student,Computer Science Assistant Professor, Computer Science R.B.I.E.B.T, India R.B.I.E.B.T, India
[18] 2014 IEEE Security and Privacy Workshops Steganography in Long Term Evolution Systems Iwona Grabska, Krzysztof Szczypiorski Institute of Telecommunications Warsaw University of Technology Warsaw, Poland
[19] Edge Adaptive Image Steganography Based on LSB Matching Revisited- Weiqi Luo ; Guangdong Key Lab. of Inf. Security Technol., Sun Yat-Sen Univ., Guangzhou, China ; Fangjun Huang ; Jiwu Huang
[20] Digital image steganography: Survey and analysis of current methods Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt School of Computing and Intelligent Systems, Faculty of Computing and Engineering, University of Ulster at Magee, Londonderry, BT48 7JL, Northern Ireland, UK
[21] A New Approach for LSB Based Image Steganography using Secret Key S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain Computer Science and Engineering Discipline Khulna University, Khulna 9208, Bangladesh.
[22] High Capacity Image Steganography in Wavelet Domain Saeed Sarreshtedari and Shahrokh Ghaemmaghami Sharif University of Technology, Tehran 14588-89694 Iran
[23] Review of Comparison Techniques of Image Steganography IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 6, Issue 1 (May. - Jun. 2013), PP 41-48 www.iosrjournals.org www.iosrjournals.org
[24] A SECURE DATA COMMUNICATION SYSTEM USING CRYPTOGRAPHY AND STEGANOGRAPHY International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013
[25] Visual Cryptographic Steganography in Images IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.4, April 2012 Manuscript received April 5, 2012