An Image Steganographic Technique Using More Cover Images to Embed the Source Image Data Randomly At 2-Lsb's of STEGO Images

DR. K. S. SADASIVA RAO[1], DR. R. SRIDEVI[2]
[1]*Professor in CSE, Dean R&D, Sri Indu College of Engineering and Technology*
[2]*Professor in CSE, JNTUH, College of Engineering, Hyderabad*

Abstract— In the recent digital era of business operations, it requires to give importance for the data in transmission. Information security is a branch of computer science and engineering which provides security for the data under transmission through various channels. Information security can be provided by using the techniques like either cryptography or steganography. Cryptography deals within formation security where the plain text converted into cipher text using encryption algorithm with the help of key. It alters the structure of the secret message. At receiver end again it convert the Cipher text back in to plain text, using the decryption algorithm along with the key. Steganography is a branch of information security, which is useful to embed the data in a cover file without altering the structure of the cover file.. This carrier/cover file may be of text, audio, video, image or any important information in any format. After embedding the secret information on cover file, that file was identified as stego file. If the information bits are embedded on any image file, that process is called as Image Steganography [1]. An Image is a combination of horizontal and vertical pixels. There are basically two types of images are used in image steganography called (1) Gray scale images (2) Color images. Most of the Cryptographic techniques were commonly known by all but the present strong algorithms are resistant to attack and very high computing power is required to crack the data. But at the other side efficient Steganalysis system are designed to crack the steganographic process. Hence, Steganographic techniques still need to improve for certain formats. The main advantage of Steganography over Cryptography is that, the Steganography prevents the discovery of the very existence of secret data in the communication [3]. In this proposed image steganographic technique, more cover image files were used to embed the data of source image. The sequence of bits that were embedded at 2-LSB positions of the cover images are selected by the user and they vary as per the sequence selection randomly by the user at sender side. At the receiver side, it is required to gather all the stego images, so as to recollect back the data bits of source image. At the receiver end, receiver side steganographic algorithm used along with the key (which recollects the sequence of bits embedded) to regenerate the cover image. It is also required to use the same sequence selection at the receiver end, which is made at sender side as randomly. In this novel Steganographic method source image bits are embedded in more stego images and the sequence of bits embedded are also random, which depends on the sender side user selection. Hence this technique is more secured and robust, as any powerful steganalysis technique cannot detect the cover image by using any or all stego images without a key. The key transferred from sender to receiver by using any powerful cryptographic technique or by using any secret media, so as to improve the security level of the proposed algorithm.

Index Terms- Cryptography, Steganography, Encryption, Decryption, Cover file, Stego file, Steganalysis.

I. INTRODUCTION

Information Security is a multidisciplinary area of study and professional activity which is concerned with the design, improvement and implementation of security methods of all existing types in order to keep information in all its locations and, consequently, information systems, where information is created, processed, stored, transmitted throughout the net and destroyed, should free from threats. Cryptography and Steganography are the two different techniques for providing security for information. In cryptography the existence of the data can be identified by the intruder while in steganography the existence of the data was hidden in stego file and with human eye it is not possible to identify the hidden data [3]. Hence, Steganography is more secured than cryptography. A powerful steganalysis technique is required to identify the steganographic process. Steganographic technique plays an important role in protecting the data like passwords, OTP, images, text, important letters / documents related to MOU's / defence information,

audio, video etc. Cryptography deals with all the data encryptions and decryptions, where the plain text is converted into cipher text at sender end by using cryptographic encryption algorithm on plain text along with key. The cipher text is not in understandable form. After converting plain text into cipher text, these bits will be transmitted on the channel from sender to receiver. At receiver end again the cipher text is converted back into plain text using cryptographic decryption algorithm along with key on cipher text.

Steganography is a process of sending secret information on a carrier or cover file. Steganography is a branch of network security, where instead of converting the plain text into cipher text like in cryptography, the original message bits are embedded on some carrier or cover file. This carrier file may be text, audio, video, image etc. After embedding the secret information on cover file, that file was identified as stego file. If the information bits are embedded on an image file, then that process is called as Image Steganography. An Image is a combination of pixels. There are basically two types of images are used in image steganography, they are gray scale and color images. While comparing the cover file with stego file, if the PSNR value is > 20 (for grey scale images) and PSNR > 40 (for color images) then with human eye it is not possible to measure the difference between the cover and stego images. This concept is the origin for implementing Image steganography. By using Hybrid Crypto-Steganographic techniques it is possible to combine the both cryptographic and steganographic features, through which information can be transmitted with high security.

II. STATE OF THE ART

Steganography is a process of hiding data in other media to transfer the secured information [1]. Most of the steganographic algorithms are working on gray scale images, but some unauthorized user may suspect that useful information is going in gray scale image, because now a day's nobody is interested in using gray scale images as general images [7]. Actually many steganographic techniques have been implemented either in gray scale or color images. But in color images all the three planes RGB have been used to stuff the bits. Hence in color image steganography, by using LSB method 3bits/pixel can be stuff / replaced with secret data.

In most of the proposed spatial domain or transform domain algorithms, the existing techniques will replace the cover image bits with the original message bits using least significant bit algorithm or some other variations on those algorithms. The Spatial Domain uses the LSB's of RGB planes to stuff the data bits. But in Transform Domain, the pixel values are converted into transformed coefficients and the transformed coefficients are used to modify the data. The below are the some of the articles identified to know about the work done in the area of Image steganography:-

1. Anil kumar et al. [8] proposed a work, in which the authors uses hash function to generate a pattern for hiding the data bits into LSB's of RGB pixel values of the cover image. This method makes confident that the information has been encrypted prior to embedding it into a cover image. In any case if the cipher text got exposed from the stego image, the intermediate person other than receiver can't access it, as it is in encrypted form, which requires suitable decrypting algorithm to get original data.

2. Mekha Jose et al. [9] proposed steganographic algorithm, which allows hiding an image with in a cover image. The proposed algorithm makes the use of LSB technique. The bits of the secret image are embedded in random pixels of the cover image and these random pixels are generated by RC4 algorithm. Through this method user can embed 3 bits at each pixel, hence the cover image should be at least 8 times bigger than the secret image, since each pixel requires 24 bits of memory.

3. Odai M. Al-Shatanawi et al. [10] presented a narrative approach, in which a new algorithm proposed to hide large amount of data in color image. This algorithm based on different size image segmentations (DSIS) and modified least significant bit (MLSB), where the DSIS algorithm applied to embed a secret image randomly at stego image. The number of bits replaced in each byte is non uniform. This proposed approach is efficient and satisfied high imperceptible with high payload reached to four bits per byte.

4. Xinyi Zhou et al. [11] Proposed a work, proposed a more secure steganography by implementing randomness of the LSB embedding positions and encrypt the message which control embedded

positions, so the hidden information should not be extracted lacking the matching private key.

5. Marghny H. Mohamed et al. [12] offered a steganographic process, where the image is divided into two parts, one to embed the secret message and applies change to the value of some bits that have the secret bits obtained by the simple LSB substitution technique. The other part is used to indicate which change is applied to each pixel exist in the first part.

6. Pratiksha Sethi et al. [13] offered a descriptive approach assured that Steganography hides the extension of data and Cryptography converts data into cipher text. In the proposed anticipated system, the file we want to protect is firstly compressed to shrink in size and then it was transformed into cipher text by using AES algorithm and then the encrypted data is hidden in the image. Genetic algorithm is used for pixel mixture of image.

7. Anil Kumar et al. [8] presented a steganographic method using RSA and Hash-LSB techniques, where the algorithm designed to provide more security to data and for data hiding method. The projected method uses hash function to produce a pattern for embedding data bits into LSB of RGB pixel values of cover image. This method makes sure that the message encrypted prior to hiding it into a cover image.

8. Hemalatha S et al. [14] proposed a work novel image steganographic method to hide both image as well as he key in color cover image by means of Discrete Wavelet Transform (DWT) and Integer Wavelet Transform (IWT). In this proposed work 256 x 256 size color image used as cover image and the secret information is a gray scale image of size 128 x 128. To transmit secret image, first a key is produced and encrypted. Only the resulting key hidden in the cover image by using IWT.

III. PROBLEM DEFINITION

Now a day's information security has become the most challenging task. There are many ways for securing the data but still we are facing security issues inspite of using well designed existing information security techniques, which needs improvement. Cryptography and Steganography are widely used techniques to secure the information. Cryptography is related with the procedure of altering ordinary plain text into making no sense text and vice-versa. It is a process of storing and transmitting data in a exacting form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration but can also be used for user authentication. Earlier cryptography was effectively synonymous with encryption but nowadays cryptography can be decrypted by the computer experts very easy and data is misused. And another drawback of the cryptography is anyone can easily identify that some information is present in the given file. Steganography moves the cryptography a stage farther by embedding an encrypted message, so that no one suspect its existence. Preferably, anyone by scanning data will be unsuccessful to recognize that it contains encrypted data. To make information more secure steganography techniques are performed in which data is embedded in a Cover file and it cannot be recognized by everyone. The Cover file after embedding the information is known as Stego file. Some more Novel and Intellectual steganographic techniques required to protect the information and modern crypto-steganographic techniques can improve the security.

Least Significant Bit method of Embedding (LSB) is a universal steganographic method that may be working to embed data into a diversity of digital media, but one of the largely studied applications is "using LSB embedding to hide one image inside another". LSB embeddings are remarkable for their simple design and alarming effectiveness. The simplest of LSB embeddings allow for large amount of data to be embedded without observable changes, which allows to embed the data without distortion in the quality of the cover image. The balance of ease of implementation and effectiveness make LSB embedding is an interesting area of study, which has less Mean Square Error.

Least Significant Bit (LSB) embedding is a easy scheme to put into practice steganography. Like all other steganographic methods, it embeds the data into the cover so that it cannot be detected by a informal observation. The technique works by replacing some of the information in a given pixel, with the information in the image. The LSB embedding is performed on the least significant bits, which will minimize the deviation in colors that the embedding process creates. For example, embedding into the single least significant bit changes the color value by

one. Embedding into the last two bits can change the color value maximum by 3. If embedding is performed on the least significant two pixels, the result is that a color in the cover can be any of four colors (i.e. 00, 01, 10, 11) after embedding. Steganography avoids introducing as much variation as possible, to minimize the likelihood of detection. In a LSB embedding, we always lose some information from the cover image. This is an effect of embedding directly into a pixel. To do this we must discard some of the cover's information and replace it with information from the data to hide. LSB algorithms have a choice about how they embed that data to hide.

IV. PROPOSED TECHNIQUE AT SENDERSIDE

Here in this proposed technique, we use 2 it LSB method. Initially, we select a source image and four cover images. Then, we embed the source image information into 4 cover images by dividing each pixel/plane of the source image replaced at orresponding pixel/planes of the 4 coverimages at 2 LSB positions. In color images, each pixel requires 24 bits (8 bits for Red, 8bits for Green and 8 bits for Blue). Out of 8 bits of each pixel of plane, 2 bits replaced at 1st cover file, next 2 bits at 2nd cover file, next 2 bits at 3rd cover file and last 2 bits at 4th cover file LSB positions. Such that, 2 LSB's of all the 4 stgo images were replaced with the source image corresponding pixel/plane data. If we use more than 2 least significant bits to embed the source file data, than the quality of the stego images are disturbed.

V. PROPOSED ALGORITHM AT SENDERSIDE

Algorithm at Sender Side: -

- Step 1: Start the program.
- Step 2: Read a Source Image and 4 Other Carrier Images.
- Step 3: Convert the Source Image and 4 Stego Image files into decimal matrixes which represents RGB planes of size 256 X 256.
- Step 4: Convert all images RGB planes decimal value into binary format.
- Step 5: INPUT the sequence of Source image 8 bits basing on which embedding process implemented in 4 stego images ('key generation').
- Step 6: For i in 1 to 256 do
- Step 7: For j in 1 to 256 do
- Step 8: Embed / Replace 2 LSB (4 images x 2 bits = 8 bits) of RGB pixel/planes of all 4 stego images with the 8 bits of every pixel/plane of source image.
- For eg: -

RED plane bits of source image only at RED planes of 4 images: -

% p1 & p2 bits of source image RESPECTIVE BITS at 2 LSB's of First image
% p3 & p4 bits of source image RESPECTIVE BITS at 2 LSB's of Second image
% p5 & p6 bits of source image RESPECTIVE BITS at 2 LSB's of Third image
% p7 & p8 bits of source image RESPECTIVE BITS at 2 LSB's of Fourth image
% The input sequence (p1 to p8) may alter according to user selection for bit Replacement

- Step 9: End for j
- Step 10: End for i
- Step 11: Regenerate all 4 images with 6 original bits and 2 replaced bits at LSB of RGB planes and send the regenerated/stego pictures through channel.
- Step 12: Transfer the generated 4 stego images and key to receiver.
- Step 13: Terminate the program.

VI. PROPOSED TECHNIQUE AT RECEIVERSIDE

Here in this proposed receiver side technique, we select the four stego images. Then, we construct matrix values of those images. Then the 2 LSB at RGB planes of all the 4 images were recollected (as each pixel requires each pixel requires 24 bits (8 bits for Red, 8bits for Green and 8 bits for Blue)) and the corresponding decimal values are reconstructed at matrix. Using the prepared matrix values again the Source image regenerated at receiver end.

VII. PROPOSED ALGORITHM AT RECEIVERSIDE

Algorithm at Receiver Side: -

- Step 1: Start the program.
- Step 2: Read 4 stego images.
- Step 3: Input the 'Secret Key' (sequence of bits need to recollect from stego images).
- Step 4: for i in 1 to 256 do
- Step 5: for j in 1 to 256 do

- Step 6: Recollect 2 LSB's from 4 STEGO IMAGES through RGB pixel / planes and convert the binary number into equal decimal value (using 'key' sequence).
- Step 7: Generate RGB matrixes with decimal values (from the collected 2 LSB of stego image).
- Step 8: End for j
- Step 9: End for i
- Step 10: Reconstruct the source image with the Generated Matrix values of RGB
- Step 11: Terminate the program

VIII. TEST RESULTS

Inputs at Sender Side: -

(A)Source Image and 4 Cover Images taken as Input: -

SOURCE IMAGE	COVER IMAGE 1
	

COVER IMAGE 2	COVER IMAGE 3	COVER IMAGE 4
		

(B) The generated 4 Stego images by stuffing 2 LSB's with Source image pixels: -

STEGO IMAGE 1	STEGO IMAGE 2
	

STEGO IMAGE 3	STEGO IMAGE 4
	

Outputs at Receiver End: -

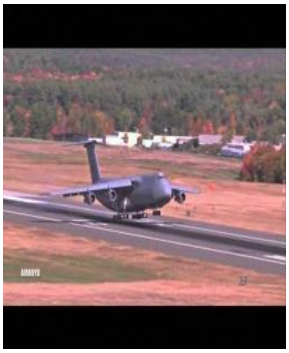
(a) The 4 stego images received from sender: -

STEGO IMAGE 1	STEGO IMAGE 2
	

STEGO IMAGE 3	STEGO IMAGE 4
	

(b) The Reconstructed Source Image from the 4 Stego Images: -

SOURCE IMAGE



TEST RESULT

IMAGE TITLE	SIZE	MSE (After embedding 2 LSB's)	PSNR (After embedding 2 LSB's)
STEGO-IMAGE (FLOWER 1)	256 X 256	2.7395	43.7540
STEGO-IMAGE (FLOWER 2)	256 X 256	2.5546	44.0575
STEGO-IMAGE (FLOWER 3)	256 X 256	2.7566	43.7271
STEGO-IMAGE (FLOWER 4)	256 X 256	2.1902	44.7260
SECRET IMAGE (FLIGHT)	256 X 256	0	INF

IX. RESULT ANALYSIS

The quality of the image at receiver end can be analysed by comparing with the source image at sender side. If there is a major distortion in the quality, then powerful steganalysis tools can predict the secret information embedded in the stego image. To evaluate the quality of the stego image MSE (Mean Square Error) is the statistical formula to access the difference between source image at sender side and the reconstructed image at receiver side. It evaluates the pixel-by-pixel value difference between original image at sender side and the reconstructed image at the receiver side to identify the quality in regenerating the image. It is also useful to find the difference between original cover image and stego-image to test the quality degradation due to steganographic process.

MSE (Mean Squared Error) calculation :-

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|^2$$

Mean Squared Error Equation

Peak signal to noise ratio (PSNR) and structural index similarity (SSIM) are two assessment tools that are extensively used in image quality evaluation. The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is used as a quality measurement between the original and stego-image. The higher the PSNR, the better the quality indication. If the PSNR value is grater than 40, then it implies that no human eye can identify the difference in the quality of image even if the image contains some modifications due to steganography.

PSNR is as follows: -

$$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right)$$

Peak Signal-to-Noise Equation

CONCLUSION

To test the quality distortion in the Stego image comparing with Cover image as well the quality of the source image at receiver side, all the pictures were resized with 256 x 256. As per the size of the image pixels, the appropriate matrix generated with RGB values. The above test results showing the least Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) is also > 40, which shows the less quality distortion in the stego image comparing with cover images. No human eye can identify the

distortion in the quality of Stego-image comparing with the Cover image. We can observe that there is no distortion in the quality of source image at receiver end, that was proved with the comparison of the source image at sender end with the reconstructed image at receiver end. The MSE = 0 and the PSNR = INF, indicates that there is no single bit of distortion in the secret image. Future work Image Steganography is a branch of Information security, which will provide high security by embedding information within a picture. To enhance the security at high level we can use Cryptographic techniques to convert the Plaintext into Ciphertext and then the Ciphertext can be embedded in image by using Image Steganogrphic techniques. Such type of Crypto-Stegonographic technique can enrich the power of maintaining secret data.

REFERENCES

[1] Niels Provos and Peter Honeyman, Hide and Seek: An Introduction to Steganography, IEEE Security & Privacy, 2003.

[2] Niel F Johnson, Sushil Jajodia, Exploring Steganography: Seeing The Unseen, IEEE, 1998.

[3] Tahir Ali, Amt Doegar, "A Novel Approach of LSB Based Steganography Using Parity Checker", IJARCSSE, Vol.5, Issue 1, January 2015, pp. 314-321.

[4] Wien Hong And Tung-Shou Chen, A Novel Data Embedding Method Using Adaptive Pixel Pair Matching, IEEE Transactions On Information Forensics And Security, Volume 7, No. 1, February 2012.

[5] T. Morkel, J.H.P. Eloff, M.S. Oliver, "An Overview of image steganography", Pretoria, South Africa, Information and Computer Security Architecture (ICSA) Research Group, pp 1-11, June 2005.

[6] Mehdi hussain and Mureed hussian, "A survey of image steganography technique", International Journalof Advanced science and technology, vol.54, May 2013, pp.113-123.

[7] Neha Gupta, Nidhi Sharma, "Hiding Image in Audio using DWT and LSB", IJCA, Vol. 81, No. 2, November 2013, pp.11-14.

[8] Anil kumar, Rohini Sharma, "A Secure Image Steganography Base on RSA Algorithm and Hash-LSB Technique", IJARCSSE, Vol. 3, Issue 7, July 2013, pp. 363-372.

[9] Mekha Jose, "Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality", IJSR, Vol. 3, Issue. 9, Sept. 2014, pp. 2281-2284.

[10] Odai M. Al-Shatanawi, Nameer N. El. Emam, "A NEW IMAGE STEGANOGRAPHY ALGORITHM BASED ON MLSB METHOD WITH RANDOM PIXELS SELECTION", IJNSA, Vol. 7, No. 2, Mar 2015, pp. 37 – 53.

[11] Xinyi Zhou, Wei Gong, Wenlong Fu, LianJing Jin, "An Improved Method for LSB Based Color Image Steganography Combined with Cryptography", IEEE, ICIS 2016, Japan, June 2016.

[12] Marghny H. Mohamed, Loay M. Mohamed, "High Capacity Image Steganography Technique based on LSB Substitution Method", An Internation journal of Applied Mathematics & Information Sciences, Vol. 10, No. 1, Jan 2016, pp. 259 – 266.

[13] Pratiksha Sethi, V. Kapoor, "A Proposed Novel Architecture for Information Hiding in Image Steganography by using Genetic Algorithm and Cryptography", ELSEVIER – ScienceDirect, Procedia Computer Science 87 (2016), pp. 61 - 66.

[14] Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath, " A SECURE COLOR IMAGE STEGANOGRAPHY IN TRANSFORM DOMAIN", IJCIS, Vol. 3, No. 1, Mar 2013, pp. 17 – 24.

[15] T. Morkel, J.H.P. Eloff, M.S. Olivier, An Overview of Image Steganography, Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.

[16] Domenico Bloisi and Luca Iocchi, Image based steganography and cryptography, International Journal of Computer Applications, 2010.

[17] V. Lokeswara Reddy, Dr. A. Subramanyam, Dr.P.Chenna Reddy, Implementation of LSB Steganography and its Evaluation for Various

File Formats, Int. J. Advanced Networking and Applications, Volume: 02, Issue: 05, Pages: 868-872 (2011).

[18] A. Joseph Raphael, Dr. V. Sundaram, Cryptography and Steganography – A Survey, Int. J. Comp. Tech. Appl., Vol 2 (3), 626- 630, ISSN:2229- 6093, 2010

[19] M. Kharrazi, H. Sencar and N. Menon, "Image Steganography: Concepts and Practice", Lecture Notes Series, Institute for Mathematical Sciences, National University of Singapore, 2004.

[20] Ing. Giacomo Cancelli, "New techniques or steganography and steganalysis in the pixel domain" Ph. D. Thesis, Ciclo XXI – May 13th, 2009, Available online at:http://www.arehna.di.uoa.gr /thesis/uploaded_ data/New_Techniques_for_ Steganography _and_Steganalysis_in_the_Pixel_ Domain_2009_thesis_1245340893.pdf

[21] T Morkel, JHP. Eloff , MS Olivier, "An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA 2005), Sandron, South Africa, June/July 2005(Published Electronically)

[22] Bret Dunbar, "A detailed look at Steganographic Techniques and their use in an OpenSystems Environment", SANS Institute InfoSec Reading Room,Available:at:http://www.sans.org/ reading_ room/whitepapers/covert/a_detailed_look_at_ steganographic_techniques_and_their_use_in_ an_ opensystems_environment_677.