International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

A Hybrid Image Steganography Method

Ilyas Abbasi, Ranjana Roychoudhuri, H. Leishang Chanu, Sujit Rabha, Tapodhir Acharjee

Abstract*: This is age of fast communication and data revolution. Huge amount of data is transmitted and received in every second utilizing the current infrastructure. Providing the security and maintaining integrity of the data while it is being transferred through the public channels is a challenging task. Steganography can be used in this purpose by concealing the data inside text, image, audio or video file formats and send the files to the other end. This paper gives an overview of various image steganography methods. To hide secret information in images various steganographic methods are available which have their own pros and cons. In this paper we have discussed the types of image steganography. Here we propose two different image steganography methods using Modified Least Significant Bits (LSB) and Discrete Wavelet Transform (DWT) methods. Also, the results are analyzed using different parameters like Peak signal to noise ratio(PSNR), Mean Square Error(MSE) to find out the efficiency of the proposed methods.

Keywords* : Confidentiality, Integrity, Steganography, Discrete Wavelet Transform (DWT),Peak signal to noise ratio(PSNR),Mean Square Error(MSE).

I. INTRODUCTION

Steganography refers to the style of obscuring information in digital media in order to camouflage the existing data. It comes from the Greek word 'STEGAN-OGRAPHY' meaning "Protected Writing". Perhaps denied while proceeding at the time whichever data root inner face of the conveyor entity alike so the data cannot b recognized by the human visual system (HVS).[1] Requirements of steganography consists of bearer body, confidential file, implanting algorithm, and from time to time undisclosed key and encryption algorithm to upsurge the security.[2]

Manuscript published on 30 September 2019
* Correspondence Author
Ilyas Abbasi , Department of CSE, Assam University, Silchar, Assam , India. Email: ilyas.abbasi42@gmail.com
Ranjana Roychoudhuri , Department of CSE, Assam University, Silchar, Assam , India. Email: ranjanashontu@gmail.com
H. Leishang Chanu , Department of CSE, Assam University, Silchar, Assam , India. Email: leishangchan20@gmail.com
Sujit Rabha , Department of CSE, Assam University, Silchar, Assam , India. Email: **sujitrabha123@gmail.com**
Tapodhir Acharjee*, Department of CSE, Assam University, Silchar, Assam , India. Email: tapacharjee@gmail.com

The execution take count into the swapping of data between worldwide governments and defense administrations, medical imaging, online banking security, smart identity card security, online voting security, and firm reciprocity of data sensed by wireless sensor nodes in WSNs. In negative sense it can be used for sending viruses and Trojan horses and offers a greatest process to be used by extremists and criminals for their private communication[3,4].

The chief objective of steganography is to communicate securely in a totally imperceptible method and to skip dubious with regard to the imparting of confidential information where characteristics of these methods are to alteration in the structure and features so as not to be identifiable by human eye[5,6].

It has been seen that all digital file formats may be used as cover for steganography, but if the formats are having high intensity of redundancy, these are more useful as the confidential data can be swapped with redundant segments without being recognized. The redundant segments of an object are those segments that can thus be transformed without the transformation being spotted effortlessly. Image, Text, Audio, Video and Network Protocol often have redundant data present in their binary representation and comply with the requirement of steganography[7].

Image steganography has the capacity to hide the confidential data and it becomes hard to detect which strengthens of the confidentiality of the hidden data. There have been the use of image steganography for centuries, although with the advent of digital technology, have taken on a new form. Image steganography has a wide range of applications mainly in the security of the digital data. They are also getting attentions because of self -awareness to increase security system and also after the world-wide security attack.

Image steganography is all about exploiting the limited powers of the human visual system (HVS). In the case of steganography, the images have attained a huge popularity and have been proved as the most useful cover image. Digital images often have a huge amount of redundant data thus, making it possible conceal confidential messages inside the image files. In steganography, the images are the most common and prevalent carrier means. This numeric representation method forms a grid and the distinct points are referred to as pixels. These pixels, thus, result in the formation of images raster data. The limitation of the human visual system (HVS) is that it has a low sensitivity in pattern changes and luminance, thus enabling the data hiding in images taking advantage of it. The secret messages which are embedded in the images involve some slight alterations in the non-significant parts which are unseen to human perception system. Image steganography has two categories: Spatial Domain and Frequency Domain.

II. LITERATURE SURVEY

A. LSB Bit-Plane Substitution

The LSB based image steganography[9,10] is simple method. It assumes that average human vision is not able to distinguish between minor level precision in many image formats. In this method Firstly, RGB image is converted into gray image. The image obtained during this process is called as 'Stegano-embed image'. The message is embedded into the intensity values of image obtained during image to matrix conversion. Embedding process starts with conversion of Image to Matrix. After this conversion process the matrix is stored in a text file.

Extracting is performed by first converting Matrix to Image. Here, image is obtained from the intensity values and it is having the message embedded into it. Important thing is that the cover image and the obtained image here have to be indistinguishable by common human being. Thus, the goal of steganography is achieved.

The advantage is that LSB technique is used for encryption which is easier and simple to implement. Here, 8-bits of cover image is replaced by 8-bits of secret data. Disadvantage of this method is that the PSNR value obtained is 25.9 which is quite low. In this method, the stego image formed is a bit distorted and of low quality form.

B. Using LSB Technique and Pseudo Random Encoding[10]

Here in the embedding process, firstly, the pixel of the cover image is extracted and also the characters of the text file and the stego key are extracted. The element of the pixel is placed first after choosing first pixel and picking the characters of the stego key. A '0' is used here as a termination symbol. The first element of next pixels will be replaced by the characters of the text file. Likewise, after a number of iterations stego image is obtained when characters are exhausted.

In this method, pseudo-random technique is used in place of simple LSB technique for encryption which gives high imperceptibility and tamper resistance characteristics from the default one. The random key used in this method of pseudo-random technique for pseudo-random number generator needs to be initialized each time we permute the pixels of cover image

and reshape into a matrix.

C. Least Significant Bit Algorithm for Image Steganography[11]

Here the secret bits are written directly to the cover image pixel bytes. The least significant bits in pixel values are replaced by embedding secret message. In the encryption process, grayscale images are created after reading the secret and cover images and then make sure that the size of the secret image is less than the cover image. After getting the binary values of the secret image, it is divided into RGB parts and substitute MSB bits of secret image into LSB bits of cover image. Reverse process takes place for decryption at the receiving end. Advantage of this proposed work is that the intensity values of both the cover and the secret images are represented, so it becomes easier to embed or encrypt secret images to cover images by following up intensity values. In this algorithm, the size of secret image should be less than cover image, otherwise there is no embedding of MSB of secret image to LSB of cover image.

D. Color Image Hiding Using RGB Color Planes And DWT[12]

This method is wavelet based Steganographic technique using DWT for the color image. In the embedding process, the cover image and the secret image are taken which should be of equal size. Then they are decomposed into four sub-bands by separating into RGB individual plane. Here a method called alpha blending is used to hide the planes of the secret image with RGB planes of cover image. Also, the inverse DWT is applied. Then the stego image is generated by combining the alpha-blended inverse wavelet transforms. In the time of the extraction process, the first part is reversed. Here, inverse DWT is applied. At last, the true colour secret image is generated after combining all the alpha-blended inversed wavelet transformed planes. In this model, 3-level DWT is used for embedding secret image in the cover image which results in high security and excellent space-frequency localization properties. It also uses alpha-blending technique for mixing two images to form a final image. The PSNR value here in this model is relatively low.

E. LSB Substitution Based On Image Blocks And Maximum Entropy[13]

In this paper, the image taken is being devised into different blocks followed by the calculation of the entropy of each block. Then the watermark is being inserted into sub-images which have the maximum entropy and the value of PSNR is calculated. The image devised is recognized to have the original image. And lastly the watermark is retrieved with extraction method. The cover image here is broken to blocks and then the blocks are watermarked. After that the block with maximum entropy is embedded with message plus no distortion occurs in the watermarked image and we can embed our message into the highest entropy block which will give high PSNR value. As we have to calculate the entropy of each block, it requires time and efficiency which is reduced as it requires effort to calculate PSNR for each MSB bits substituted for LSB bits in each block that is watermarked.

F. Implementation Of Image Steganography Using 2-level DWT Technique[14]

Here, the embedding process involves 2-level DWT technique which uses the cover image and secret image as inputs and the output stego image is generated. In the time of extraction, secret image is extracted out of the stego image by a process involving the key information. The proposed model is a simple, secured and robust for hiding images. It provides good embedding capacity. The PSNR value is comparatively low which results in low quality of the stego image.

III. PROPOSED METHOD

Our proposed method works in two phases. Firstly. With modified LSB method and then by DWT based method. These two methods work for hiding image in image and text in image respectively.

A. Modified Least Substitution Bit(LSB) Method

In this model, we are using image as a secret image and another image as a cover image in which we will hide the secret

image into the cover image by applying LSB technique on the cover image and secret image.

Embedding Process

Step 1: Input the cover image.

Step 2: Input the secret image.

Step 3: Resize the cover image and secret image in same size.

Step 4: Convert the cover image into matrix form by using any image to matrix conversion method.

Step 5: Convert the secret image into matrix form by using any image to matrix conversion method.

Step 6: Every bit except the one at pixel bit position is 1 by using

mask = 0xff(1 << pixelbit)

Step7: Shift the LSB of the secret to the pixel bit position.

Step 8: Generate the cover plane by using AND operation between cover array and mask and adding secret bits in the result of the AND operation.

Step 9: Convert the cover plane into cover array.

Step 10: Convert the cover array into stego image by using matrix to image method.

Step 11: Write the stego image.

Extracting model

Step 1: Convert the stego image into matrix form by image to matrix format.

Step 2: Remove the cover plane from the stego array.

Step 3: Expose secret image from stego array by using matrix to image method.

Step 4: Write the exposed secret image and cover image.

Fig. 1.Cover Image and secret image

One example taken for image hiding in image can be given: Let us consider a secret image that has to be concealed in the cover image. Figure 1 shows the cover image and secret image and we can see that the two images (cover image and stego image) are exactly the same. We take a cover image and a secret image as inputs and then resized both the images into same size. We convert both the images into matrix form by using image to matrix method. Every bit except the one at pixel bit position is 1 by using masking function. The LSB of the secret image is shifted to pixel bit position and the cover plane is generated using the AND operation and converting it to cover array. Lastly we convert the cover array to stego image by using matrix to image method and thereby generating the stego image. During extraction, stego image is converted into matrix form by image to matrix method followed by removing the cover plane from the stego array. The secret image is exposed from stego array by using matrix to image method which results in writing the exposed secret image and the cover image.

B. Modified Discrete Wavelet Transform (DWT) Method

In this model, we are using text as a secret message and image as a cover image in which we will hide the secret message into the cover image by applying DWT technique on the cover image.

The embedding algorithm

Step 1: Input a text as secret message.

Step 2: Input an image as cover image.

Step 3: Apply the 1 level DWT on the cover image.

Step 4: Select the HH band to be modified as 'col'.

Step 5: Obtain the length of secret message as 'Len'.

Step 6: Apply iteration up to length of the secret message.

Step 7: Change the bits of the HH band with the bits of the secret message

Step 8: Apply the IDWT (Inverse DWT) Operation and the stego image is obtained.

Step 9**:** The key information is formed by the location that we have used for hiding secret message and the length of the message for extracting the secret message.

The extracting algorithm

Step 1: Input the stego image and length of the message.

Step 2: Apply the 1 level DWT transform on the stego image.

Step 3: Select the HH band.

Step 4: Apply the iteration up to the secret message length.

Step 5: Extract the secret message from the HH band.

Step 6: Display the secret message on the screen.

The hiding of a text in image can be explained through this example: Let us consider a secret message that has to be concealed in the cover image. Figure 2 shows the cover image and secret message and we can see that the two images (cover and stego images) are exactly the same.

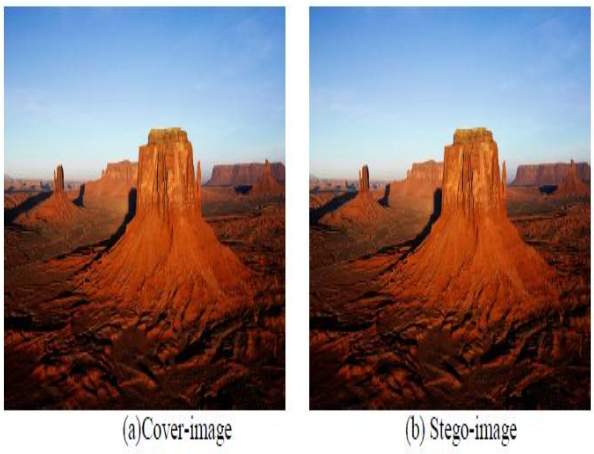

Fig. 2.Cover Image and stego image

Here, a text is taken as secret message and an image as cover image. We apply the 1-level DWT on the cover image resulting in formation of four bands i.e., LL, HL, LH and HH and the HH band is selected for hiding the secret message by changing the bits of HH band with the bits of the secret message.

We then apply IDWT (Inverse DWT) technique to retranslate the frequency domain information to the spatial domain. And hence we obtain the stego image. After applying the reverse process, we can extract the secret message from the stego image.

IV. RESULTS AND DISCUSSION

A. Quality Measurement Parameters

We have to measure the quality of the stego image and the extracted secret image by using some quality measurement metrics [6]. These metrics can be used to compare the original image and the modified image. We use the following metrics:

Peak Signal to Noise Ratio(PSNR): PSNR is used to measure the recreation of the compressed image. It can help to distinguish between the cover and stego image. The computation is also easy as given below:

$$PSNR = 10 \log_{10} (255^2/MSE)$$

A small value of PSNR indicates that the constructed image is not of acceptable quality.

Mean Square Error (MSE): MSE can be calculated by finding the average of the square of difference between the intensities of the stego image and the cover image. It is popularly used because of the mathematical tractability it offers. It is represented as:

$$MSE = 1/MN \sum_{i=1}^{M} \sum_{j=1}^{N} [f(i,j) - f'(i,j)]^2$$

where f(i,j) is the original image and f'(i,j) is the stego image. A large value for MSE means that the image is of poor quality.

B. Experimental Results

(a) Image 1 (b) Image 2 (c) Image 3

Fig. 3.Cover Image 1 to 3

The table given below shows the value of the PSNR and the MSE presenting the comparison between the original image and the stego image formed at the end of the embedding module for all the five cover images. In the table, PSNR value for the original cover image and stego image as computed by our working algorithm method was found to be 103.87.

Table- I: Comparison between cover image and stego image

Cover Image	PSNR	MSE
Image 1	103.87	2.6667e-06
Image 2	101.93	4.1667e-06
Image 3	100.35	6.0000e-06

The table given below shows the value of the PSNR and the MSE presenting the comparison between the original image and the stego image formed at the end of the embedding module for three cover images. In the table given below it is shown that the maximum PSNR value obtained is 31.94 for the three cover images that we have chosen is achieved by Modified LSB method. Also minimum MSE is attained by Modified LSB method with image 3.

Table- II: Comparison between cover image and stego image

Cover Image	Method	PSNR	MSE
Image 1	Modified LSB	29.38	219.60
Image 2	Modified LSB	31.94	212.72
Image 3	Modified LSB	27.93	195.32
Image 1	Modified DWT	29.12	217.12
Image 2	Modified DWT	30.74	211.23
Image 3	Modified DWT	26.12	198.12

V. CONCLUSION

In this paper we have tried to propose a model for image steganography which is simple, secure and robust. The stego image and cover image are almost similar to each other and the differences between them are hardly detectable. The high PSNR value suggests the high quality of constructed images. The stego image is found to be secured, but further analysis is remain to be performed.

REFERENCES

1. Muhammad, K., Ahmad, J., Rehman, N. U., Jan, Z., and Qureshi, R.J., (2015), 'A secure cyclic steganographic technique for color images using randomization', Technical Journal, University of Engineering and Technology, Taxila, vol. 19, pp.57- 64.
2. Muhammad, J. A. K.., Farman, H., Jan, Z., (2015), 'A new Image steganographic technique using pattern-based bits shuffling and magic LSB for grayscale images', Sindh University, Research Journal(Science Series),vol.47.
3. Holub V. and Fridrich J., (2013), 'Digital Image Steganography using universal distortion', in Proceedings of the First ACM workshop on information hiding and multimedia security, pp.5968.
4. Rezaei F., Ma, T., Hempel, M., Peng, D. and Sharif, H., (2013), 'An anti-steganographic approach for removing secret information in digital audio data hidden by spread spectrum method', IEEE International Conference on Communications(ICC), pp.2117-2122.
5. Chandramouli, R.; Kharrazi, M. and Memon, N., (2004), Image steganography and steganalysis: Concepts and practice. In Digital Watermarking (pp. 35-49). Springer Berlin Heidelberg.
6. Raphael, A. J. and Sundaram, V. (2011), 'Cryptography and Steganography A Survey', International Journal of Computer Technology and Applications, Vol. 2, No. 3, pp. 626-630.
7. Anderson, R. J. and Petitcolas, F. A., (1998), 'On the limits of steganography', IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, pp. 474-481.
8. Hamid, N.; Yahya, A.; Ahmad, R. B. and Al Qershi, O. M. (2012). 'Image Steganography Techniques: An Overview', International Journal of Computer Science and Security (IJCSS), Vol. 6, Issue 3, pp.168-187.
9. Roy, T. S. (2016), 'Image Steganography Using LSB Bit-plane Substitution', International Research Journal of Engineering and Technology (IRJET) ,Vol. 03,No.12.

10. K. Jenita Devi and Dr. Sanjay Kumar Jena, “A Secure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique”, B.Tech Thesis, National Institute of Technology-Rourkela Odisha ,2013.
11. B.S. Champakamala, K. Padmini. D. K Radhika, “Least Significant Bit algorithm for image steganography”, International Journal of Advanced Computer Technology (IJACT), Vol.3, No,4,2014
12. Nilanjan Dey, Anamitra Bardhan Roy, Sayantan Dey, "A Novel Approach of colour Image Hiding using RGB color planes and DWT", International Journal Computer Applications, Vol:36-No.5,, 2011.
13. Mohamed Radouane,, A Method of LSB substitution based on image blocks and maximum entropy, IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, 2013
14. Aayushi Verma, Rajshree Nolkha, Aishwarya Singh and Garima Jaiswal, "Implementation of Image Steganography Using 2-Level DWT Technique" , International Journal of Computer Science and
15. Business Informatics, ol:1,No:1, 2013.

AUTHORS PROFILE

Ilyas Abbasi received his B.Tech. degree in Computer Science and Engineering from Assam University, Silchar, India in 2017 and now working in OGS India Private Limited , Hyderabad, India.
.

Ranjana Roy Chowdhury received her B.Tech. degree in Computer Science and Engineering from Assam University, Silchar, India in 2017 and now pursuing M.Tech degree in Computer Science and Engineering from Indian Institute of Information Technology (IIIT) Guwahati, India. Her current research interests include machine learning, service computing ,cloud computing.

H. Leishang Chanu received her B.Tech. degree in Computer Science and Engineering from Assam University, Silchar, India in 2017 and Working as a Front-End Developer in a Start-up company .

Sujit Rabha received his B.Tech. degree in Computer Science and Engineering from Assam University, Silchar, India in 2017 and currently serving in Indian Railways.

Dr Tapodhir Acharjee is working as an Assistant Professor in the department of Computer Science and Engineering in Assam University, Silchar. His areas of interests are ad-hoc networks, cryptography and network security, machine learning etc.