Concealing Data for Secure Transmission and Storage

Abirami.P1, Shanmugam.M2
1Department of Civil Engineering, Institute of Remote Sensing, Anna University, Chennai, India
2Scientist, Institute of Remote Sensing, Anna University, Chennai, India

Abstract

Transfer of secret information over the internet and storage of it in Personal Computer has been traced by unauthorized user. In order to prevent this, the images which are secret are hidden inside another image. Here three algorithms are proposed for image hiding. The Least Significant Bit Technique hides the secret image Least Significant Bit into the Cover image Least Significant Bit by masking the lower bits of it. Thereby the message is hidden. Alpha Blending Technique is done by separating the individual plane of both images, which are decomposed into four sub bands (LL, LH, HL and HH) using Discrete Wavelet Transform. Using alpha blending embedding technique and Discrete Wavelet Transform message is hidden. The RSA-Discrete Wavelet Transform technique is done by RSA encryption of secret image and splitting cover image into four sub bands using Haar-Discrete Wavelet Transform. Message image is hidden by modifying one sub-band in the cover image. Analysis is done for checking the quality of secret image, which is extracted back from the cover and also to check the quality of stego image with cover image. With the analysis done, the best algorithm for concealing image is thus chosen.

Keywords - *Alpha Blending, Haar-Discrete Wavelet Transform. Least Significant Bit, RSA encryption, Steganography.*

I. INTRODUCTION

The use of internet in the world becomes the root cause of communication and subsequently digital crime becomes the major threat to the mankind. Therefore it is most essential to have a secured data communication. The commonly used information securities are Cryptography, Steganography, Coding, etc. Evolution of Cryptography technique is Steganography.It embeds the secrete data into cover object such as images, videos audio files, sounds etc.The main goal of steganography is mainly concerned with the protection of contents of the hidden information. Usually images are ideal for information hiding because of the large amount of redundant space is created in the storing of images. The strength of steganography can be improved by combining it with cryptography.Steganography used in a large amount of data formats in the digital world such as bmp, gif, jpeg, mp3, txt, wav etc. The redundant or noisy data can be removed from these formats easily and replaced with a hidden message.

II.RELATED WORK

The Steganography technique that deals with three main challenges capacity, imperceptibility, and security has been used in 'Genetic Optimal' scheme [4]. This is achieved by hybrid data hiding scheme incorporates LSB technique with a key-permutation method. Final experimental results show decrement in computation time when increasing number of keys.

A schema for embedding data within JPEG image in the spatial domain based on statistical analysis. "Improving Visual and Statistical Properties (IVSP)" method used [1] helps in precluding of revealing with the presence of statistical anomalies in the stego medium.Stego-image considers two components. Minimum Error Replacement (MER) that minimizes the embedding induced error and Improved Gray Scale Compensation (IGSC) that eliminates the false contours.

The new secret spatial information hiding technique for remote sensing image [7], is used. The wavelet information hiding algorithm adapting to features of a remote sensing image based on DWT embedding and HVS is implemented. The novel spatial information hiding technique and algorithm has no influence on applied value of a remote sensing image and doesn't need the remote sensing image while extracting the secret spatial information, namely it is a blind algorithm.

A novel technique for image steganography based on DWT, where DWT is used to transform original image (cover image) from spatial domain to frequency domain. Two D Discrete Wavelet Transform (2-D DWT) is performed [2] on a gray level cover image of size M × N and Huffman encoding is on the secret messages image before embedding.

III.METHODOLOGY

Three different algorithm is performed on image concealment and finally choosing the best among them.

A. The LSB Steganography Technique

1) Least Significant Bit Replacement: In Least Significant Bit Replacement steganography data hiding techniques try to alter least significant information in the cover image. Altering LSB doesn’t change the quality of image to human perception.

2) Embedding Steps: The Cover image is converted into 8-bit format so that the images used in concealing which may be in any n-bit format is converted to 8-bit for further steps is shown in Fig. 1.

11001010 10010011 11111111 ------>cover pixel

11110000 11110000 11110000------>binary form of 240

11000000 10010000 11110000 ------>modified cover

After modifying the cover, the next step is shifting 4 LSB of secret image to right in order making the modification in MSB of the secret image indirectly.

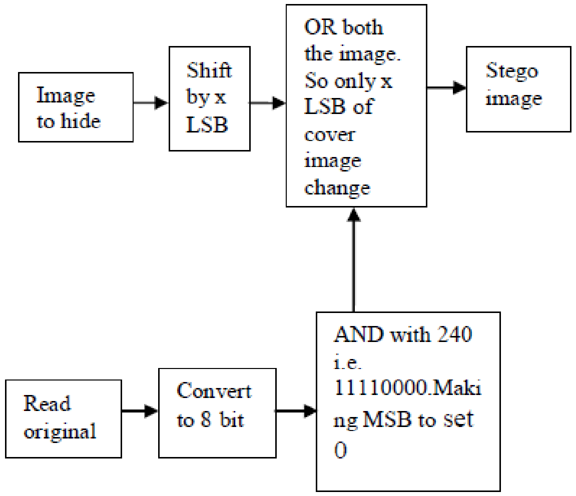


Image to hide
Shift by x LSB
OR both the image. So only x LSB of cover image change
Stego image
Read original
Convert to 8 bit
AND with 240 i.e. 11110000.Making MSB to set 0

Fig.1 Encoding Steps for LSB Steganography.

01101001 10101010 01010100------->secret pixel

00000110 00001010 00000101------->shift 4 bits to right

Now, with the modified cover and secret image, the stego-image is formed

11000000 10010000 11110000 -------->modified cover

OR

00000110 00001010 00000101--------->shifted 4 bits

11000110 10011010 11110101---------->stego image

To get back the original secret message AND with 255 is done is shown in Fig. 2.

B. Alpha Blending Technique

Discrete Wavelet Transform is performed to both Secret image and Cover image individually. After that, alpha blending is done to one of the band in the resultant images. Alpha blending is the way of mixing the two images together using different alpha value. Here in this paper, the alpha value remains same. Alpha Blending can be accomplished in computer graphics by blending each pixel from the first source image with the corresponding pixel in the second source image.

The equation for alpha blending is used as follow (1)

Final pixel = alpha * (First image's source pixel) + (1.0-alpha) * (Second image's source pixel) (1)

The blending factor or percentage of colours from the first source image used in the blended image is called the "alpha." The alpha used in algebra is in the range 0.0 to 1.0, instead of

0 to 100%.

Now, IDWT is applied to the blended image in order to bring back the image from one-suband to form the full complete stego image. The formation of stego image is shown in Fig. 3.

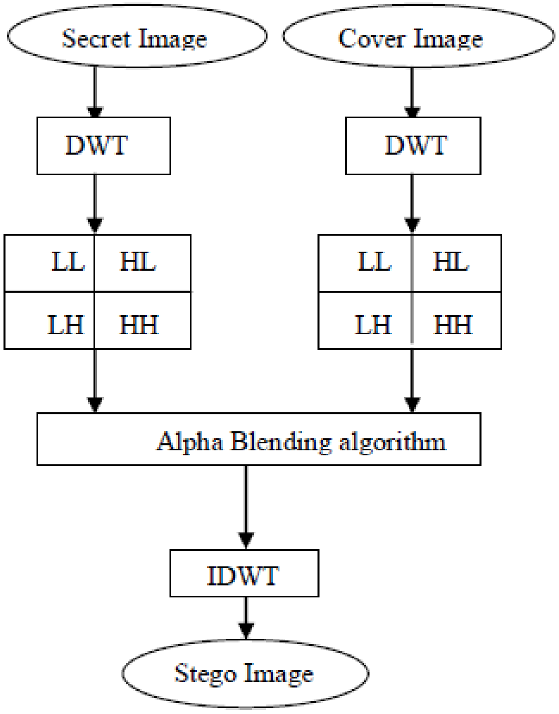


Fig 3 Steps for Alpha Blending Technique

C. RSA-DWT Technique

The Cover image is subjected to Haar-DWT.The LH of the resultant image is the place where the encrypted secret image is hidden.

1) *RSA encryption*: RSA is a Public key cryptography named after its inventors: Ronald Rivest, Adi Shamir

and Leonard Adelman. RSA can be used for encryption as well as for authentication.

2) *Haar-DWT*: Haar-DWT is the simplest DWT. A 2-dimensional Haar-DWT consists of two operations which are described as follows.

Step 1: Scan the pixels from left to right in horizontal direction and perform the addition and subtraction operations on neighbouring pixels. Store the sum on the left and the difference on the right. Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H)

Step 2: Scan the pixels from top to bottom in vertical direction and perform the addition and subtraction operations on neighbouring pixels. Then store the sum on the top and the difference on the bottom. Repeat this operation until all the columns are processed. Finally 4 sub-bands denoted as LL, HL, LH, and HH respectively are obtained. The LL sub-band is the low frequency portion and hence looks very similar to the original image. The first-order 2-D Haar-DWT applied on the Cover Image.

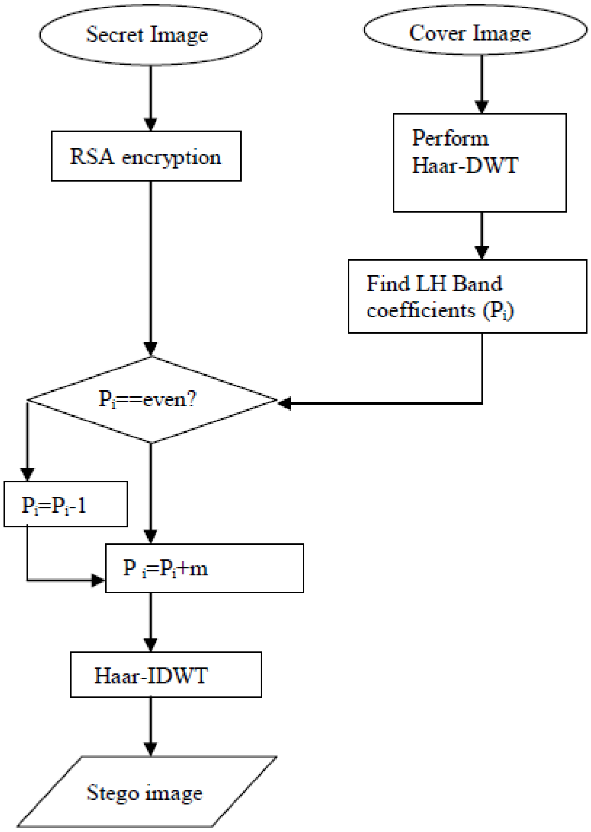


Fig 4 Steps for RSA-DWT Technique

IV.ALGORITHM

A.The LSB Steganography Technique

1) *Image Hiding (Steganography):*Steps of embedding algorithm are given as follow

1. Read the original image and the image which is to be hidden in the original image

2. Shift the image to hide in the cover image by X bits.

3. And the original image or cover image with 240 which is 11110000. So four LSB's set to 0.

4. The shifted hidden image and the result of step 3 are ORed. This makes changes only in the X LSB bits so that the image is hidden in the original image.

2) *Image Extracting (Steganalysis):*

1. The stego image shifted by 4 bits since it was shifted by 4 bits to insert it into the original image.

2. The image is the ANDed with 255 i.e., 11111111, which gives the original image. It is ANDed with 255 because initially all the LSB's were made 0. Now it is recovered back.

3. To get it to Unit8 format we, convert it back to unit8 which is the extracted image.

B. Alpha Blending Technique

1) *Image Embedding:*

Steps of embedding algorithm are given as follow

1. Cover Image and Secret Image of same size are separated into individual bands.

2. The individual planes are decomposed into four sub bands (LL, LH, HL and HH) using DWT.

3. The individual planes of the secret image are hidden within the individual planes of the cover image using alpha blending embedding technique and inverse DWT is applied individually.

4. All three alpha-blended inversed wavelet transformed planes are combined to generate the stego image.

2) *Image Extracting:*

Steps for extraction algorithm are given as follow

1. Cover image and Stego Image are separated into individual planes.

2. The individual planes are decomposed into four sub bands (LL, LH, HL and HH) using DWT.

3. The individual planes of the secret image is extracted from the individual planes of the stego image using alpha blending extraction technique and inverse DWT is applied individually.

4. All three alpha-blended inversed wavelet transformed planes are combined to generate the final extracted true colour secret image

C. RSA-DWT Technique

1) *RSA encryption algorithm:* Steps for encrypting image in RSA.

1. Select two prime numbers r, s.

2. Calculate n= r × s and φ (n) = (r-1) (s-1)

3. Select integer „e‟ such that e is relatively prime to φ (n).
Gcd (φ (n), e) =1; 1<e < φ (n)
4. Calculate d such that d × e=1mod (φ (n))
5. Now Public key (PU) for encryption is {e, n} and Private Key (PR) for decryption is {d,n}.
6. At sender side, message (M) is converted into cipher text (C) by C= M e mod n
7. At receiver side, cipher text is converted back to original message by M= C d mod n

2) *Image Hiding:* Steps of embedding algorithm are illustrated in the Fig 4.
1. Encrypt the secret image using RSA encryption key.
2. Perform Haar-DWT transform on cover image to decompose it into four sub bands (LL, LH, HL and HH).
3.Apply mod2 operation on coefficients (Pi) of selected sub band (LH) and modify it to hide data (mi) in following way
Qi = mod2 (Pi)
a) If Qi is 0 i.e. Pi is even then modified coefficients MPi = Pi+ mi or
b) If Qi is 1 i.e. Pi is odd then modified coefficients MPi = (Pi-1) +mi
4. Four sub bands including modified sub band are combined to generate stego image using Haar- IDWT transform.
5. Send the stego image to receiver.

3) *Image Extracting:* Steps for extraction algorithm are given as follows
1. Perform Haar-DWT transform on stego image to decompose it into four sub bands (LL, LH, HL and HH).
2. Apply mod2 operation on coefficients (Pi) of selected sub band (LH) to extract data (mi) in following way:
Qi = mod2 (Pi) Message bit mi = Qi
3. Concatenate the message bits to obtain cipher message.
4. Decrypt the cipher message using RSA decryption keys and display it on screen.

a)Cover image

b) Secret image

c) Extracted secret image

d) stego image

V.RESULTS AND DISCUSSION

Quality measures are performed to find the resistant of images against geometric distortion and signal processing attacks and to get best method for hiding

A.Mean-Squared Error (MSE)

The mean-squared error (MSE) between two images I1 (m, n) and I2(m ,n) is given (2)
MSE=(ΣM,N[I1(m,n)-I2(m,n)]2)/M*N (2)
M and *N* are the number of rows and columns in the input images, respectively. Mean-squared error depends strongly on the image intensity scaling. A mean-squared error of 100.0 for an 8-bit image looks dreadful; but a MSE of 100.0 for a10- bit image ([0, 1023]) is barely noticeable. Mean-squared error depends strongly on the image intensity scaling.

B.Peak Signal-to-Noise Ratio (PSNR)

Peak Signal-to-Noise Ratio (PSNR) avoids this problem by scaling the MSE according to the image range. The equation used is given (3)
PSNR=10 log 10(R2/MSE) (3)
PSNR is measured in decibels (dB). PSNR is a good measure for comparing restoration results for the same image.

.

C. Discussion of experiment 1

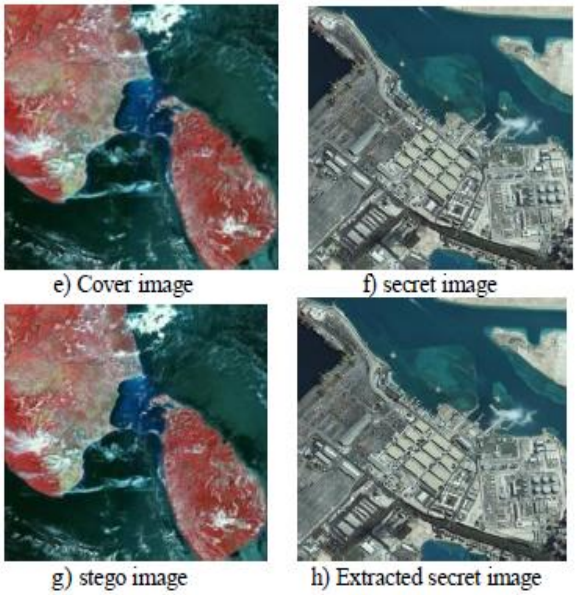
Considering two different images cover image and secret image, the LSB technique shows good for gif format cover image.259×194 with the capacity 8.98KB as cover image and 259×194 with the capacity of 12.4KB as secret image, the result of stego-image is performed. The Quality is experimented in Table 1

TABLE 1
COMPARATIVE ANALYSIS OF PSNR and MSE VALUES

	Stego image Vs Cover image	**Secret image Vs Extracted Secret image**
PSNR	29.826	42.41
MSE	69.826	67.21

D. Discussion of experiment 2

In Alpha Blending technique, by varying the alpha values we can achieve different PSNR values according to the application user.PSNR is good for low values of alpha as shown in Table 2.



e) Cover image f) secret image

g) stego image h) Extracted secret image

TABLE II

COMPARATIVE ANALYSIS OF PSNR and MSE VALUES

		Cover Vs Stego image	**Secret Vs Extracted Secret image**
Alpha=0.1	PSNR	29.0663	10.7082
	MSE	68.23	70.32
Alpha=0.5	PSNR	15.08	15.79
	MSE	69.35	69.04
Alpha=0.9	PSNR	9.93	29.7718
	MSE	71.92	68.00

E. Discussion of experiment 3

In RSA-DWT technique, high PSNR value is achieved is shown in Table 3. In addition to retrieve the better quality image, the high security is also obtained by using RSA Technique.

TABLE III

COMPARATIVE ANALYSIS OF PSNR and MSE VALUES

	Stego Vs Cover image	**Secret image Vs Extracted Secret image**
PSNR	46.1948	42.42
MSE	58.97	60.86

VI. CONCLUSION

Alpha blending technique and RSA-DWT technique can also be applied for audio steganography, because DWT is applicable for any digital signal. The use of LSB is less but when using the image of different file format, LSB provides best image quality. The Image quality depends also on application of where it is used.

REFERENCES

[1] Arafat Ali H. (2007), ‘Qualitative Spatial Image Data Hiding for Secure Data Transmission’ *GVIP Journal*, Vol.7, Issue 2.

[2] Amitava Nag, Sushanta Biswas and Partha Pratim Sarkar(2009), ‘A Novel Technique for Image Steganography Based on DWT and Huffman Encoding’, *International Journal of Computer Science and Security, (IJCSS)*, Vol.4: Issue 6.

[3] Bani Younes M. A., Jantan A.(2008),’A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion’, *International Journal of Computer Science and Network Security* (IJCSNS), vol. 8 No. 6.

[4] Fadwa Al-Afari, Marghny Mohamed and Mohamed Bamatraf (2011), ‘Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation’, International *Arab Journal of e-Technology*, Vol. 2, No. 1.

[5] Muhammad Usama, Muhammad Khurram Khan, Khaled Alghathbar, Changhoon Lee (2010), ‘Chaos-based secure satellite imagery cryptosystem’, Computers and Mathematics with Applications 326_337.

[6] Manjunatha Reddy H.S and Raja K.B (2012), ‘Wavelet based Secure Steganography with Scrambled Payload’, *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, ISSN: 2278-3075, Vol.1, Issue 2.

[7] WANG Xianmin, WANG Cheng, ZHOU Jianzhong, ZHANG Yongchuan(2007), ‘Secret spatial information hiding technique for remote sensing image’, International Symposium on Photo electronic Detection and Imaging : Image Processing, edited by Liwei Zhou,.

[8] Zaidan A. A., Zaidan B. B. and Alaa Taqa Y. (2010), ‘Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem’, *International Journal of the Physical Sciences* Vol. 5(11), pp. 1776-1786.