International Journal of Advanced Technology in Engineering and Science
Vol. No.4, Special Issue No. 01, May 2016
www.ijates.com
ijates
ISSN 2348 - 7550

DESIGN OF IMAGE STEGANOGRAPHY USING HYBRID TECHNIQUES

Priyanjali N K[1], Y. Manjula[2], M.Z. Kurian[3]

[1]PG Student (Vlsi and ES), [2]Assistant Professor, [3]HOD,

Dept. of Electronics & Communication Engineering,

Sri Siddhartha Institute Of Technology, Tumakuru, Karnataka, (India)

ABSTRACT

Secure data communication is very important as the transmitted data can be hacked by some of the unauthorized users. To avoid the illegal accessing of the data two methods came into existence they are cryptography and steganography. Where cryptography just deals with encrypting the message, such that the plain text is converted into the cipher text form such it its converted into some other forms which cannot be readable by the unauthorized persons. Many researchers have been made to achieve the secureness of the data , the technique called steganography was proposed . Steganography is also called as invisible communication. The existence of communicated information is hided. This technique deals with the hiding of the data in digital media. To protect the transmitted data still more efficiently we can use cryptography along with steganography. In the image steganography most of the information is hided into the image. In the cryptography the contents of the messages are kept secret ,Whereas in the steganography the existence of the message is kept secret. Image is basically the 2-Dimensional,which consists of pixels. Usually the images are of two types gray scale images and normal images.

In steganography two types of images are going to be used they are payload image and the carrier image. The payload image is the one which is also called as the secret file, which has to be transmitted over the carrier image. The payload image along with the carrier image is called stego file. The secret data is hidden in the cover image such that its invisible to the illegal users. The reliability of the information sent from the transmitter to the receiver should be maintained. The method improves the bit error rate and the PSNR.

Keywords: Steganography, cryptography, encryption

I. INTRODUCTION

Steganography is the invisible communication between two parties. Many encryption and decryption algorithms are used to provide the secrecy of the data. There are many steganographic techniques and they are text, image, audio and protocol steganography

Images are encrypted to ensure the security of the data. The encryption has been used in wide application such as internet banking, internet communication, multimedia applications, medical imaging, telemedicine and military communication etc. The signature of the user can be forgered in the net-banking, where as password of the user can be hacked in the internet communication this can be avoided by securing the user data by efficient image steganography method in conjunction with cryptography.

The aim of this project is to cover the following objectives and they are: 1. To design a system an efficient secured algorithm for transmission of image. 2. To minimize loss during transmission and reception. 3. This is done by the use of certain techniques which helps with minimum efforts and high efficiency.

In real time data transmission for image video requires security to maintain secrecy .this requires to hide the identity of the person in banking transaction where cloud servers play the major role. The data or the information requires encryption for big data analytics. So this motivates the use of advanced secured encryptions and improve the error rate in steganography. In existing steganography algorithm the use of spatial domains and frequency domain individually yields in less accuracy and also the originating decrypted image is distorted. So there is a need for improvement.

The combination of spatial and frequency domain can be used to improve the error rate with better PSNR value. The scope of the lies with the using of different combinations of spatial and frequency domain and also modifying the fusion based embed algorithm to improve the performance of the algorithm.

II. LITERATUIRE SURVEY

Hsien – chu et al,[1] proposed the use of least significant bit (LSB) method and pixel value differencing (PVD)method. Secret data can be hided in to the cover image i.e in the smooth area where the color quality of the pixel is high by the LSB method. Whereas PVD method is used in edged area. In the PVD method the difference value of the two uninterrupted pixels are taken. If the difference value is small then it can be placed in smooth area and if difference value is large then its placed on the edge area.

Chikwong Chan et al, [2] proposed a simple LSB substitution method for data hiding. Along with the LSB the Optimal pixel adjustment process(OPAP) is also applied to LSB stego output to improve the image quality. In OPAP the refinement of the pixel values are made.

H.B.Kekre et al, [3] uses LSB method and compared to PVD. The grayscale cover image is considered and the secret key is XORed with the data to be embedded. The embedded data can be recovered by using the same XOR operation by the same key. Depending on the range the secret data is embedded in to the 8-bit cover image. By observing the MSB positions of cover image the secret data is embedded into the LSB positions.

Aarti dalvi et al, [4] proposed the RGB color phases of cover image DWT and SWT coefficients of cover images and the secret images are extended. Both the coefficient values are fused into the single image by wavelet based fusion technique. By obtaining the ISWT/IDWT of the fused image the stego image is obtained. For the embedding process the different combinations of DWT and SWT are used (DWT-DWT,DWT-SWT,SWT-SWT,SWT-SWT).In the extraction process the combination of transform used must be same.

Po-yueh chen et al, [5] proposed the embedding algorithm which is divided into two modes and, the varying mode and fixed mode. In varying mode prediction of the capacity range of embedding the secret data is made complex. The varying mode is considered in 3 cases and they are low embedding, median embedding and high embedding capacity requirements. In the fixed mode the specified range is defined for the capacity of the required data.

Jayasudha et al, [6] uses integer wavelet transform (IWT) and optimal pixel adjustment(OPA) for hiding the data into the cover image. Here the data is hidden randomly so that data cannot be detected easily. IWT is used to increase the hiding capacity and OPA is used to increase the quality of the stego image.

Reyadh Naoum et al, [7] proposed a method of embeding (RGB) secret image within the (RGB) cover image and this is done by resilient back propagation's. In the encryption process there are three stages. They are , selection of the best cover image and processing, selection of secret image and processing and best embedding threshold selection stage.

Kamal pradhan et al, [8] proposed system uses the LSB and AES methods. The LSB method is used to embed the text into the audio file. But the encryption of the text is done by using the Advanced Encryption Standard (AES). The system performance will mainly depend on the robustness, security, data hiding capacity.

G.S.Sravanthi et al, [9] proposed the use of the method plane bit substitution method(PBSM).In the pixel value of the image the message bits are embedded .Firstly to solve the binary operation in the original image is manipulated by the LSB method. Secondly encryption and decryption of the pixel is done under both the theoretical and experimental evolution.

Barnali gupta banik et al,[10] proposed the method of applying the DWT to the image and image is divided into frequency component. Lower frequency components are those which holds the original image and higher frequency components are called as detailed components, which holds the additional information about the image. The secret image is embedded into the detailed coefficients. In the embedding process the secret data is embedded into the cover image. In addition to the steganography object the pseudo-random numbers are also added. In the extraction process the secret data is extracted from the cover image along with this the correlation theory is also applied.

Dr. Mahesh kumar et al,[11] proposed the method of hiding the large amount of the data using DWT and IDWT transformations technique .The magnitude of the DWT coefficients of three sub-bands are altered i.e, HH, HL and LH of the cover image based on that the secret data is hided into the cover image.

Mamta et al, [12] proposed embedding algorithm to hide the encrypted message in the random pixels locations and the smooth area of images. Firstly the secret message is encrypted and later on edges present in the cover images all detected by using the edge detection filter . In the LSB the message bits are embedded randomly and across the smooth area of the image. The 1-3-4 LSB of red, green, blue components are selected. This method does not ensure that the message bits are hidden in the image and the length of the secret image cannot be determined correctly.

Namita et al, [13] proposed the spatial domain technique so as to compress the image size. The main objective here is to increase the capacity of the hidden data. MSB's of randomly selected pixel values used as indicator. Randomization technique is used to hide the secret data into the cover image.

Saleh Saraireh et al, [14] proposed filter bank cipher technique which is used to encrypt the secret message to provide the high security, scalability and speed. By modifying the wavelet coefficients of cover image the encrypted message is hided and this technique is called DWT. Performance is evaluated by the PSNR and histogram analysis.

III. PROPOSED METHOD

In the proposed scheme, the Gray scale secret image is transformed using DWT technique to reduce its dimensions. The reduced secret image is subjected to Visual Cryptographic method.. This avoids cheating attacks of the shares. Inverse DWT is applied to decompress the recovered image. Hence original image is

reconstructed Loading of database DWT decompress the recovered image. Hence original image reconstructed loading of database.

The proposed architecture for image stenography using 2D-DWT and LSB technique is shown in Fig.1.

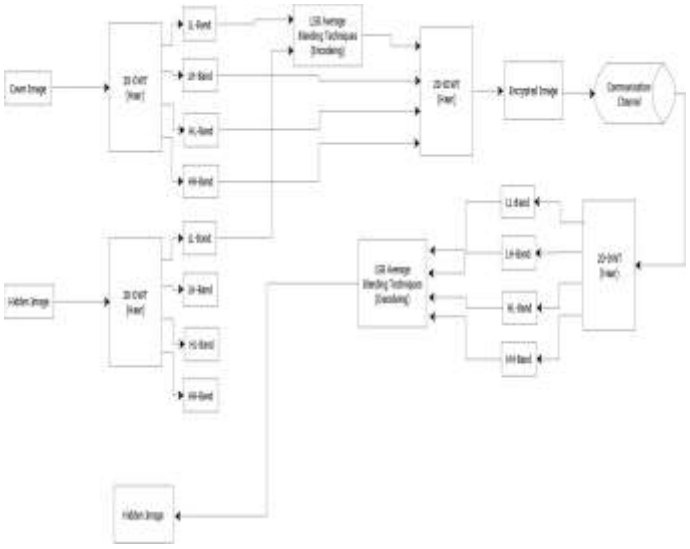

Fig.1: Block Diagram of Proposed Steganography

Firstly the secret and the cover images are taken of same or variable sizes and they are subjected to the preprocessing as shown in fig 1.

3.1 Pre-Processing

In this section different sizes of images are converted into uniform size (256x256). To reduce the design complexity color image is converted into gray image is converted into gray image. Also Gaussian filter is used in this section to remove noises present in input images. The Gaussian mask filter of 3x3 is derived from equation (1) to obtain mask given in equation (1).

3.2 Discrete Wavelet Transform

Discrete Wavelet Transform:

- To convert an image from time or spatial domain to frequency domain we use DWT technique.
- Discrete wavelet transform is a frequency domain technique where cover image is transformed to frequency domain.

After transforming into frequency domain obtain frequency coefficients of cover image. These frequency coefficients are modified according to the transformed coefficients of the Hidden image. After this step stego image is obtained. This stego image is robust i.e. it can withstand various types of attacks. Two separate one dimensional transform are performed to obtain two dimensional transform of an image.

In discrete wavelet transform the image will be filtered along both x-direction and y-direction. Initially we filter the image along x-direction by utilizing low pass and high pass analysis filter coefficients and decimate the

result by two.Store low pass filter coefficients on left part of matrix and high pass filter coefficients are stored on the right part of matrix.

The filtering of image along x-direction which uses high and low pass analysis filter coefficients is as shown in thefig2.As a result obtain two sub bands of the image namely low frequency band (L) and high frequency band (H).

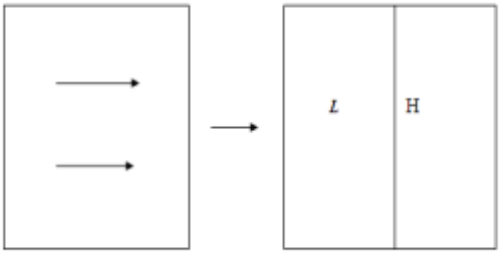

Fig 2 .Horizontal Transform-2 Sub-bands

Then filtering of the sub-image will be performed along y-dimensions and decimate the result by two. Perform decimation to maintain the total size of transformed image and original image equal. Image is decomposed in three spatial directions namely horizontal, vertical and diagonal we obtain four bands namely LL, LH, HL and HH as shown in the fig 3.

The lowest resolution level is represented by LL which consists of the approximation part of the cover image. The detailed information of the cover image will be present in the remaining three levels namely, LH, HL and HH. The magnitude of DWT coefficients will be larger in the lowest bands (LL) and will be smaller in other bands (HH, HL and LH) at every level of decomposition.

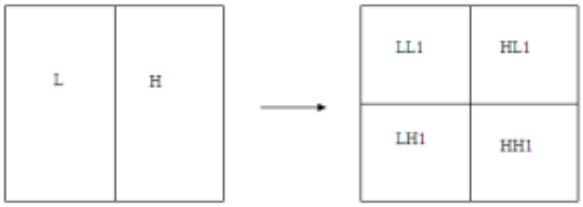

Fig 3. Vertical Transform-4 Sub-bands

The fig 4. below shows first and second level decomposition. In first level the image is decomposed into four components. In second level decomposition the lowest resolution band is further decomposed into four components. If we perform more levels of decomposition the stego image will be more robust.

Fig 4. First and Second Level Decomposition

3.2.1 Proposed Encoding Process

The encoding process in digital image steganography is shown in fig 3.1.Here; first we take the gray scale image as a cover image and Haar DWT (Discrete Wavelet Transform) is applied to the image. After applying Haar discrete wavelet transform, the cover image is decomposed into four components.

The four sub-bands of the decomposed image are as follows:

- Low frequency approximation (LL),
- Low frequency horizontal (LH),
- Low frequency vertical (HL) and
- High frequency diagonal (HH) components.

The magnitude of DWT coefficients will be larger in the lowest band (LL) at every level of decomposition and the magnitude of DWT coefficients will be smaller in other bands (LH, HL and HH). In the similar manner DWT is also applied to the hidden image which has to be embedded into the cover image. The hidden image is also decomposed into four components as shown in figure 3.1. Here cover image is used as a carrier image to carry the hidden data. The hidden image which has to be transmitted is inserted into the cover image through of the inserting technique. Once the hidden image is inserted into the cover image we will obtain stego image.

3.2.2 Haar DWT Scheme

2-dimensional Haar DWT consists of two operation and they are described as follows:

Operation 1

1. In the horizontal direction the pixels are scanned.
2. The addition and subtraction operations are performed on the neighbouring pixels.
3. On the left the sum is stored whereas on the right side the difference is stored.
4. This operation is continued until all the rows are processed.
5. Low frequency part is denoted by the pixel sum whereas the high frequency is denoted by pixel difference of the original image as shown in the fig5.

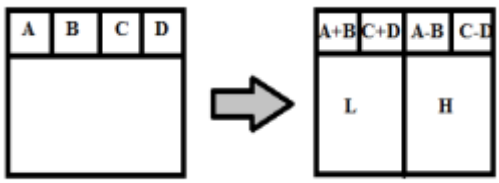

Fig. 5: Scanning of pixels from left to right

Operation 2

1. In the vertical direction the pixels are scanned from top to the bottom.
2. Addition and subtraction operations are performed on the neighbouring pixel
3. at the top sum is stored and at the bottom the difference is stored .
4. This operation is continued until all the column are processed.
5. Lastly we are obtained with the four sub-bands which are denoted as LL, HL, LH and HH.

6. The low frequency portion is the LL sub-band and is similar to that of the original image as shown in the fig 6.

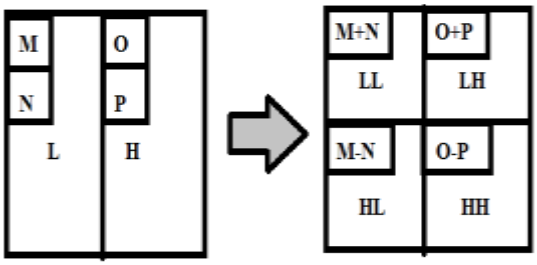

Fig. 6: Scanning of pixels from top to bottom

The LL sub-bands of both the cover image and the secret images are fused by using the average alpha blending technique.

3.2.3 2D-Haar discrete wavelet transform

The hardware structure for generating LL-band using2D Haar transform is shown in Fig. 7. The non-overlapping 2x2 matrix block of an image is considered to compute LL coefficients.

The *D flip-flops (D_ff's)* and *Shift Register* are connected in series to form shift register of 258 data samples for 256x256 image. The connections from four flip flops which form 2x2 matrices are connected to adder which performs addition of all four pixel values in turn right shifted using shifter block to obtain the required LL coefficients.

The clk_div block is used to achieve divide by 2 of *clk* which in turn connected to *D_ff* to obtain 2x2 non-overlapping matrix.

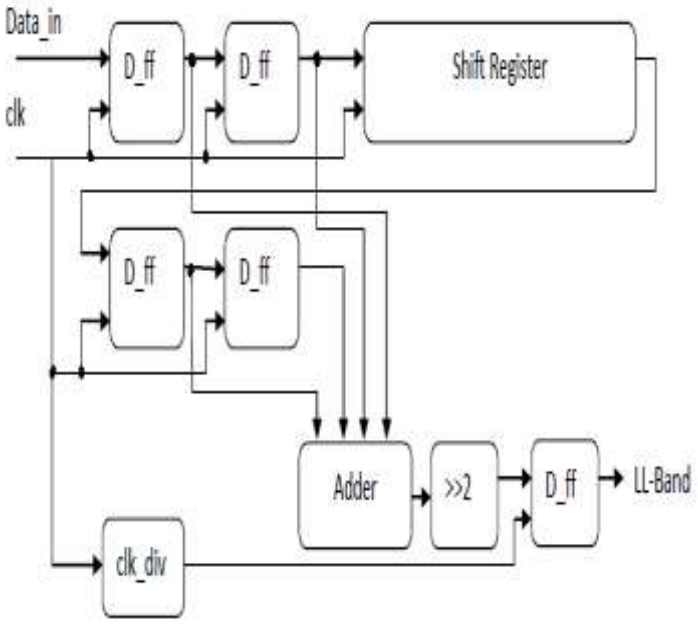

Fig. 7: Hardware Structure for LL band of 2D Haar Transform

IV. LSB AVERAGE ALPHA BLENDING TECHNIQUE

The technique utilized here for inserting the hidden image is alpha blending. In this technique the disintegrated components of the cover image and the hidden image which are obtained after applying Lift DWT to both the images, are multiplied by a scaling factor and are added.

- The alpha blending is achieved by blending each pixel values from the hidden image with the corresponding pixel values of the cover image.
- After blending each pixel values from the hidden image with corresponding pixel values of the cover image we get the stego image.

The alpha Blending technique is given by the following equation:

$$\text{Alpha Blending} = \quad) + (1- \quad) * \quad) \qquad (10)$$

Where = Scaling Factor.

= Lowest resolution band of cover image.

= Lowest resolution band of hidden image.

From the equation we can see that the decomposed components of original image and hidden image are multiplied by scaling factor and are added.

The main features of Alpha Blending Technique are as follows

- After alpha blending technique we will obtain the stego image which consists of both hidden image along with the cover image.
- The stego image which consists of secret data can therefore be transmitted to the receiver end securely.
- Since the stego is invisible the information cannot be extracted by any illegal persons.
- We can prevent security breaches and transaction frauds.

After subjecting both the LL-bands of the cover image and the secret image to the average alpha blending technique, the inverse discrete wavelet transform (Haar) is applied. The encrypted image is transmitted along the communication channel.

The encrypted image is again subjected to the 2D-DWT (Haar).Where the LL, LH, HL and HH sub-bands are obtained. Again the LSB average blending technique is used for the decoding of the image, to obtain hidden the secret image.

V. CONCLUSION

In the proposed technique the Haar DWT has been implemented, this scheme is used to obtain the four band coefficients and the steganography using LSB average blending technique in the appropriate manner to get better PSNR values. The block diagrams of proposed method is discussed which will be implemented further stages with better PSNR values.

REFERENCES

[1] Wu, H.-C.; Wu, N.-I.; Tsai, C.-S.; Hwang, M.-S ," Image steganographic scheme based on pixel-value differencing and LSB replacement methods," Vision, Image and Signal Processing, IEE Proceedings - Volume 152, Issue 5, 7 Oct. 2005.

[2] C.K Chan and L.M Cheng," Hiding data in images by simple LSB substitution", Pattern Recognition, pp. 469-474, Mar. 2004.

[3] Dr. H. B. Kekre, Ms. ArchanaAthawale, "Information Hiding using LSB Technique with Increased Capacity" International Journal of Cryptography and Security, Vol-I, No.2, Oct-2008

[4] Aarti Dalvi1, R. S. Kamathe,"Color image steganography by using dual wavelet transform" 2014

[5] Po-Yueh Chen* and Hung-Ju Lin," A DWT Based Approach for Image Steganography" March 2006

[6] S.Jayasudha ," Integer Wavelet Transform Based Steganographic Method Using Opa Algorithm"Feb 2013

[7] Rayed Naoum, Ahmed shihab, Sadeq AlHamouz,"Enhanced image steganography system based on discrete wavelet transformation and resilient back-propogation" Jan 2015

[8] Kamal Pradhan ,"Robust audio steganography technique using AES algorithm and MD5 hash" Nov 2014

[9] By Ms.G.S.Sravanthi, Mrs.B.Sunitha Devi, S.M.Riyazoddin & M.Janga Reddy," A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method"2012

[10] Barnali gupta banik,Prof Samir k,"A DWT method for image steganography" June 2013

[11] Dr.Mahesh kumar ,Munesh yadav ,"Image steganography using frequency domain" Sept 2014

[12] Mamta juneja and Parvinder S.Sandhu, 'An improved LSB based steganography technique for RGB color image', july 2013

[13] Namita Tiwari, 'Spatial domain image steganography based on security and randomization', 2014.

[14] Saleh saraireh , 'A secured data communication system using cryptography and steganography', may 2013.