Steganographic Technique Using Integer Wavelet Transform Domain

Sangita Kumari Biswal, Alina Dash

Abstract**-**Now a days data transfer over internet is the main problem. Information security is one of the possible areas of research in present days, The data needs to be kept secure. So that it could be accessed by only authorized user. So that the data needs to be sent in a secure way which the receiver should be able to understand the message. In information hiding, cryptography and steganography are the most widely used areas that come to mind for sending sensitive and private information in a secured manner. The limitation of cryptography is that other person came to know that the probability of message being decoded by other person. Cryptography change the structure of the hidden message and steganography doesn't change the structure of the hidden message. To overcome this limitations we use a technique is called steganography. Steganography means secret writing. It means hiding secret information in specific carrier data. The steganography plays an important role to hide data in such media which is audio, video, text, image etc. This paper implements image steganography with an objective of improve security and allocating maximum amount of data to be hidden inside. To achieve this initially cover image is transformed from spatial domain to frequency domain using 2D wavelet transformed image allowing embedding inside high frequency region which maintains image quality . In this paper we applying 2D HAAR technique in cover image for decomposition and Huffman encoding technique for embedding the secret message and use a encryption key for better security. In existing paper there are used dwt technique but there are some problem. So in this paper we use IWT for hiding secret data using some algorithm and calculate the signal to noise ratio and mean square error.

Index Terms— *Spatial domain; Frequency domain ; HAAR Technique; Huffman encoding ;DWT; IWT; SNR ; MSE; Steganography.*

I.INTRODUCTION[1]

In the present world, the data transfers using Internet is rapidly growing because it is so easier as well as faster to transfer the data to destination. So, many individuals and business people use to transfer business documents, important information using internet. Security is an important issue while transferring the data using internet because any unauthorized individual can hack the data and make it useless or obtain information unintended to him. In information hiding, cryptography and steganography are the most widely used areas that come to mind for sending sensitive and private information in a secured manner. The limitation of cryptography was that other person .One of the very popular technique to protect the important information over the Internet is the cryptography method. In this method the data take a form in such a way that it becomes hard to recognize the original form except the intended recipient. But as the coded data are in unrecognized form, it encourages the opponent to attack. Another security method, i.e information hiding is also a widely used technique which dispirit the attacker by avoiding the suspicion of the information inside the carrier. The proposed approach provides higher security and can protect the message. Steganography is a method which means covered writing. It is a Greek word. Stegano means covered and graphy means writing. The Steganography is a technique which means writing a secret messages which a way no one can found that there is a hidden message. There are many different carriers that can be used to hide the information such as digital images, videos, sound files and other computer files but digital images are the most popular.

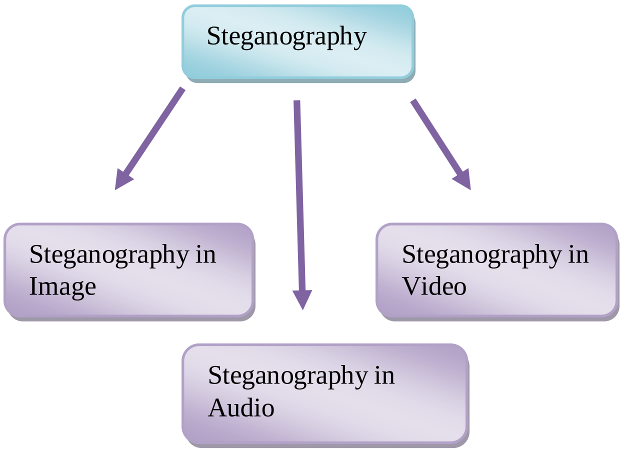


Fig.1

According to type of embedding domain Steganography in image is divided in spatial domain and transform domain. In spatial domain technique the real picture space is directly alter the position, It is a method in which information hiding is performed directly value of the pixel of the cover image. The effect of messages which is noticeable on the cover image. In transform domain, techniques are based on modifying the Fourier transform of an image the initial step is to transform the cover image into another domain. The transformed coefficients which is used for hide secret message. These changed coefficients are transformed back into spatial domain to get the stego image. The main problem is that it a lossless technique and the additive noise quantity which can be steals in the Transform domain methods are more benefit than spatial domain method if it used for hiding the information in the area of image which is a lesser quantity of expose in compressing, cropping and also image processing. Transform domain method which don't appear in the image and which is exceed lossless and lossy translations .Most of the stenographic systems recognized now a days which is essentially work on some method of transform domain. These technique is used to hide information which is important parts of the cover image. It make them extra strong to occurrences, One process is to use the Fourier and cosine transforms such as Discrete Fourier Transform (DFT) or Discrete Cosine Transform (DCT) to embed the information in the images. Another is the use of wavelet transforms such as Discrete Wavelet Transform (DWT) or Integer Wavelet Transform (IWT). We have used Integer Wavelet Transform in our proposed method. In this thesis, initially some steganography methods are analyzed. The main intention is to devise a steganography technique so that it can provide better security than some existing techniques.

In chapter 2 we discuss Background study, chapter 3 we discuss literature survey, chapter 4 we discuss about methodology and chapter 5 conclusion and future work

II. RELATED WORK

A. *DWT BASED*

The Discrete Wavelet Transform (DWT) is a comparatively test and organized method in computer science. Wavelet study is useful as it achieves local breakdown and multi-resolution study. Study of a signal in various frequency with altered resolutions is known as multi-resolution analysis (MRA). This technique transforms the purpose in wavelet area, processes the coefficient and then achieves inverse wavelet transform to represent the original format of the stego object.Discrete Wavelet Transform can recognise portions of cover image where secret data could be excellently hidden. DWT splitting data into high and low frequency components. High frequency part of signal cover specifics about the edge mechanisms, whereas the low frequency part comprises maximum of the signal info of the image which is once more divided into higher and lower frequency parts. For each level of decomposition in two dimensional applications, first DWT is implemented in the vertical direction monitored by horizontal direction.

B. *IWT BASED*

The planned algorithm works in the wavelet transform coefficients in which the message is embedded into the four sub bands of two dimensional wavelet transform. Those problems of floating point accuracy are ignored of the wavelet filters, we used the technique Integer Wavelet Transform . It gives better result as compare to dwt technique. IWT performs to become a nearer copy with compact scale of the original picture in LL sub band. When the LL sub band of DWT is inaccurate, the IWT procedure are achieves.

C. *ADVANTAGES OF IWT OVER DWT*

Usually wavelet domain allows us to hide the information. The human visual system (HVS) is less sensitive. High resolution detail band such as HL, LH and HH used to hide the data. In those region hiding data allows the robustness and the visual quality is also good. IWT maps an integer data set into another integer data set. In DWT the wavelet filters have floating point coefficients. When we hide data in their coefficients any truncation of floating point value of pixel which is integer and cause the loss of the hidden data which may lead to the failure of data hiding system. To avoid this problem of floating point of the wavelet filters when input data is integer as an digital images, the output data is no longer be integer which does not allow perfect reconstruction of the input image. IWT is a lossless data hiding method so it is more efficient approach to lossless compression .The wavelet transform maps integer to integer. In case of DWT if the input is integer then the resulting output is no longer consist of integers so the perfect reconstruction of the original image become difficult. In that reason we use IWT technique instead of DWT. In IWT technique it increases hiding capacity of the system as compare to DWT.In the proposed method we have used discrete wavelet transformation for converting image from its spatial domain to frequency domain.

In the proposed method we have used discrete wavelet transformation for converting image from its spatial domain to frequency domain. A wavelet which start in zero and return back to zero so it is called wave like oscillation.. Unlike the Fourier transform, which only construct a frequency demonstration of signal is constructed by Fourier transform the wavelet transform is able to construct a time-frequency representation of a signal simultaneously. The main purpose of converting an image into frequency domain during steganography is that when we insert our secret information into frequency domain it is very difficult to detect steganography. In discrete wavelet transformation for images we separate the high freq. and low freq. information. Low freq. info are encompasses information about the smoother places of the image and it is very sensitive information where slight modification affects the reconstructed (Stego image) image. On the other hand high freq data are contains the information of the edge, corner etc of a picture. Hence modification in this information results less noise in the reconstructed image. The data whose length is a integer and a power of two and the difference of the vector is also same length, there we works discrete wavelet transform .It is a implement which split up information into various frequency mechanisms, and then evaluating every element with determination exactly matched to its scale. DWT is calculated with a force of filters monitored by a factor 2 substitute Sampling. The DWT is also invertible and can be orthogonal . In this proposed method we have used Haar wavelet transformation. It was proposed by the mathematician Alfrd Haar in 1909. At every level the Haar wavelet transform divided and a discrete signal into two components with half of its length: an high sub band and low sub band. The low sub band is decomposed in first level. One of the most developed transforms that can be used to transform a signal from the spatial to the frequency domain and vice versa is the Wavelet transform. The Wavelet transform, and other related transforms, can be considered a second generation of transforms. Wavelets are defined as oscillations of short waves that decay rapidly over time .

Moreover, they have an enormous number of applications that can be implemented in various fields such as signal processing, data compressing, fingerprint verification, smoothing, image de-noising and speech recognition. It has been reported that the Wavelet transform can be applied to the steganography technique in order to increase the capacity as well as the robustness One of the Wavelet transform families known as “Haar” has been implemented in this work. It converts an image from spatial domain to frequency domain by applying horizontal and vertical operations, respectively.

D. 2D-HAAR-WAVELET TRANSFORM

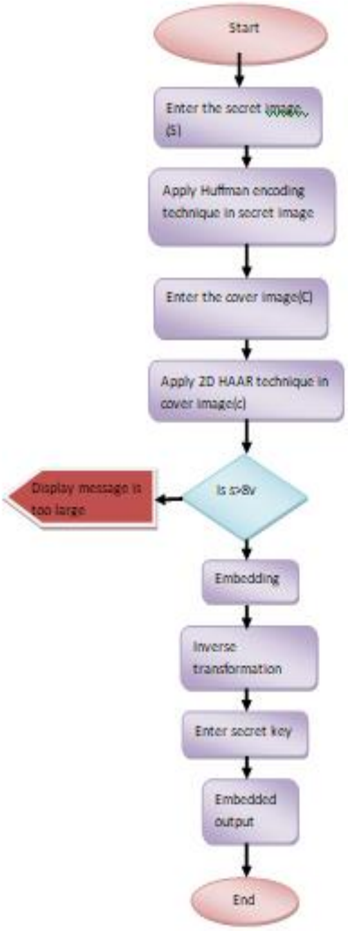
Wavelet transform has the capability to proposed many data on freq-time domain simultaneously. Time domain is delivered over high-pass and low- pass filters to remove high and low frequencies correspondingly in 2D HAAR wavelet transform. This technique is continual for a number of times and every time a subdivision of the signal is careworn out. Discrete wavelet transform analysis splits signal into 2 classes which is low sub-band and high sub band. Signal decomposition for different frequency bands and scales. DWT employs two function sets: scaling and wavelet which associate with low and high pass filters orderly. Decomposition follows the manner of dividing time separability. Meanly, only half of the samples in a signal are sufficient to represent the whole signal, doubling the frequency separability . Haar wavelet operates on data which is calculate by addition and subtract on of adjacent elements. The wavelet operated on 1st on adjacent horizontal components and then on the element of adjacent of vertical elements. One essential feature of the Haar wavelet transform is that the transform is similar to the inverse. Each transform computes the data energy in repositioned to the upper left hand corner.

E.HUFFMAN ENCODING TECHNIQUE

Huffman code is mostly used technique for data compression. Huffman algorithm applies greedy approach that considers the occurrence of each character and delivers an optimal string of binary letters. Huffman coding techniques is used for decreasing the amount of bits required to symbolize string of symbols. It is a variable length code that assigns short length codes to frequently used symbols, and long length codes to the symbols appearing less frequently .Huffman codes are optimal

codes that map one symbol to one code word. For image compression, Huffman coding assigms a binary code to every pixel intensity value and a two Dimensional (2D) pxq image is converted to a one dimensional(1D) bits stream with length less than pxq. Huffman Encoding is applied to secret object (image/text) and then each bit of Huffman code of secret object (image/text) is embedded inside the cover image.

Flow Chart


Start
Enter the secret image (S)
Apply Huffman encoding technique in secret image
Enter the cover image(C)
Apply 2D HAAR technique in cover image(c)
Is s>8v
Display message is too large
Embedding
Inverse transformation
Enter secret key
Embedded output
End

III.PROPOSED WORK

A distinctive feature of proposed system is that it allows user to select any image as cover image from the database of images formed which are a smaller amount of susceptible to steganalysis attacks. Here big size images are collected in the database in order to store as much data as possible inside the image. The block diagram of proposed steganographic system is given in figure 2 The proposed method contains the embedding phase.

A. EMBEDDING PHASE

Embedding is the process of hiding the secret image inside a cover image there by generating a stego image. It involves hiding secret image inside an image selected from the database of images by combining IWT, Huffman coding combined to form a stego-image The algorithm for the embedding data.

Embedding Algorithm

Inputs: Secret Data (D), Cover Image(C) Output: Stego image(S) with secret data embedded in it.

1. Apply Huffman encoding technique in the Secret Image.

2. Decomposed the cover image into 4 non over lapping sub bands. These are LL (Approximation coefficients). LH (Vertical details). HL (Horizontal details) and HH (Diagonal details).

3. The division of the planes is done by employing HAAR filters.

4. Information contains in the LL sub bands of secret images is separately embedded into different bands of cover image.

5.Apply logistic chaotic map in the embedded output

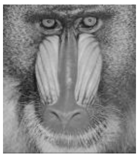
6. After embedding the secret image bit into the cover image inverse transformation is performed to retrieve them.. Then it is combined to generate the final stego image.

Fig.2 Flow Chart

IV.RESULT

This section provides the experimental results and analysis of the proposed scheme. This work is simulated using MATLAB2014a with the system specification-window 10 os, Intel i3 core processor and 64bit operating system. We take a 8 bit grey image. Then apply DWT method and find out the snr and mse of the decomposition image. Then apply the IWT method and compare the result. Fig:3 show the Cover Image & Secret image of DWT & IWT. Fig 4 show the embedded output of both technique And Fig 5 show the histogram result.

(Cover Image1)


(Cover Image2)

(Cover Image3)

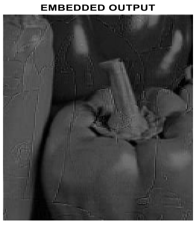
(Secret Image1)

(Secret Image2)

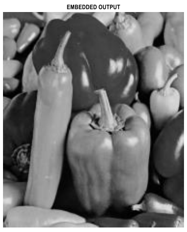
(Secret Image3)

Embedded output

For DWT

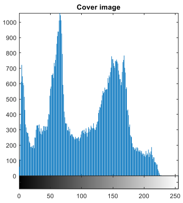


For IWT

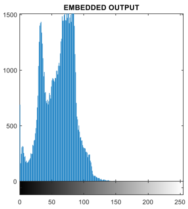


Histogram Result

For DWT

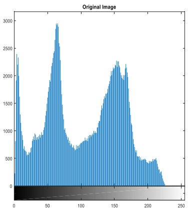


(Original Image)

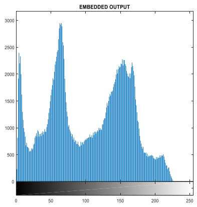


(Embedded Output)

For IWT



(Original Image)



(Embedded Output)

Figure shows that there are a very little changes between the structures of histograms of cover images and stego images. Hence the cover image and stego image accomplishes better noiselessness. Another factor to be considered is Signal to Noise Ratio (SNR). SNR is measure to image quality. Table 1 shows the SNR and MSE obtained from the proposed method. A steganographic system requires high SNR value which shows low difference between cover image and stego image. The measurement of the quality between the cover image and stego-image is defined by SNR as:

SNR= $10\log\frac{255}{MSE}$DB…………………..1

$$MSE = \frac{1}{X+Y}\sum_{j=1}^{M}\sum_{k=1}^{N}\left(X_{j,k} - X'_{j,k}\right)^2$$ ……..2

Comparison Table of SNR & MSE of DWT & IWT

		DWT		IWT	
	Secret Image	SNR	MSE	SNR	MSE
1	1	27.87	8.33	29.03	8.26
2	2	28.71	6.18	31.13	6
3	3	26.96	7.79	27.8	7.71

V . CONCLUSION & FUTURE SCOPE

Steganography is a technique which is used for secretly writing the messages in such a way that one can retrieve from the sender and receiver. In this paper analysis of DWT and IWT method is successfully implemented and result are delivered. Study on various steganographic methods We design of a steganographic techniques using Integer Wavelet Transform domain in order to increase the embedding capacity. Comparison of DWT technique in IWT technique. In near future we will implement IWT technique and generate a key for improving the hiding capacity for better result.

REFERENCES

[1]Gupta, Heena, and Palak Mahajan. "Improvisation of security in image steganography using DWT, Huffman encoding & RC4 based LSB embedding." In *Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on*, pp. 523-529. IEEE, 2016.

[2]Reddy, Ravinder Ch, and Roja A. Ramani. "The Process of Encoding and Decoding of Image Steganography using LSB Algorithm." *International Journal of Computer Science Engineering & Technology* 2, no. 11 (2012).

[3]Baby, Della, Jitha Thomas, Gisny Augustine, Elsa George, and Neenu Rosia Michael. "A novel DWT based image securing method using steganography." *Procedia Computer Science* 46 (2015): 612-618.

[4]Cheddad, Abbas, Joan Condell, Kevin Curran, and Paul Mc Kevitt. "Digital image steganography: Survey and analysis of current methods." *Signal processing* 90, no. 3 (2010): 727-752.

[5]Houssein, Essam H., Mona AS Ali, and Aboul Ella Hassanien. "An image steganography algorithm using Haar Discrete Wavelet Transform with Advanced Encryption System." In *Computer Science and Information Systems (FedCSIS), 2016 Federated Conference on*, pp. 641-644. IEEE, 2016.

[6]Abuadbba, Alsharif, and Ibrahim Khalil. "Wavelet based steganographic technique to protect household confidential information and seal the transmitted smart grid readings." *Information Systems* 53 (2015): 224-236.

[7]Salman, Afan Galih, and Bayu Kanigoro. "Application Hiding Messages in JPEG Images with the Method of Bit-Plane Complexity Segmentation on Android-Based Mobile Devices." *Procedia Engineering* 50 (2012): 314-324.

[8]Sharma, Vipul, and Sunny Kumar. "A new approach to hide text in images using steganography." *International Journal of Advanced Research in Computer Science and Software Engineering* 3, no. 4 (2013).

[9]Reddy, V. Lokeswara, A. Subramanyam, and P. Chenna Reddy. "Implementation of LSB steganography and its evaluation for various file formats." *Int. J. Advanced Networking and Applications* 2, no. 05 (2011): 868-872.

[10]Sharma, Neha, J. S. Bhatia, and Dr Neena Gupta. "An encrypto-stego technique based secure data transmission system." *PEC, Chandigarh* (2009)

[11]Joseph, A., and V. Sundaram. "Cryptography and Steganography–A survey." (2011).

[12]Siper, Alan, Roger Farley, and Craig Lombardo. "The rise of steganography." *Proceedings of Student/Faculty Research Day, CSIS, Pace University* (2005).

[13]Zaidan, B. B., A. A. Zaidan, A. K. Al-Frajat, and H. A. Jalab. "On the differences between hiding information and cryptography techniques: An overview." *Journal of Applied Sciences(Faisalabad)* 10, no. 15 (2010): 1650-1655.

[14]Bloisi, Domenico Daniele, and Luca Iocchi. "Image based steganography and cryptography." In *VISAPP (1)*, pp. 127-134. 2007

[15]Bloisi, Domenico Daniele, and Luca Iocchi. "Image based steganography and cryptography." In *VISAPP (1)*, pp. 127-134. 2007

[16]Bloisi, Domenico Daniele, and Luca Iocchi. "Image based steganography and cryptography." In *VISAPP (1)*, pp. 127-134. 2007

[17]Kawaguchi, Eiji, and Richard O. Eason. "Principles and applications of BPCS steganography." In *Multimedia Systems and Applications*, vol. 3528, pp. 464-474. International Society for Optics and Photonics, 1999.