Three Level Discrete Wavelet Transform Based Image Steganography

Emy V Yoyak
PG Scholar,
Jaya Engineering College, Thiruvallur ,India

***Abstract*-Steganographyis the art of inconspicuously hiding data within data. Steganography's goal in general is to hide data well enough that unintended recipients do not suspect the steganographic medium of containing hidden data. . The detection of steganographically encoded packages is called steganalysis. Proposed technique using three level wavelet decomposition taking a single plane of the cover image for embedding and processing the image as 4 × 4 blocks with swapping. Experiments show that Peak Signal Noise Ratio (PSNR) generated by the proposed method is better than those generated by the existing schemes. . In Discrete Wavelet Transform (DWT) based steganography approaches the wavelet coefficients of the cover image are modified to embedded the secret message. DWT based algorithm for image data hiding has been proposed in the recent past that embeddeds the secret message in CH band of cover image.**

Keywords – Steganography, Steganalysis, Peak Signal Noise Ratio, Discrete Wavelet Transform

I-INTRODUCTION

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used.

The detection of steganographically encoded packages is called steganalysis. The simplest method to detect modified files, however, is to compare them to the originals. To detect information being moved through the graphics on a website, for example, ananalyst can maintain known-clean copies of these materials and compare them against the current contents of the site. The differences, assuming, that the carrier is error free, will compose the payload.

In general, using an extremely high compression rate makes steganography difficult, but not impossible; while compression errors provide a good place to hide data, high compression reduces the amount of data available to hide the payload in, raising the encoding density and facilitating easier detection, in the extreme case, even by casual observation. The exchange of information is greater today than at any other time in history, and with the way technology is improving, this exchange will only become greater. The threat of a group or individual misusing standard channels of communication to send stolen information, or communicate a plan against a nation, is more likely now than ever.Due to the nature of these communications, the need for a means to hide them is ever present; this is where steganography comes into play. Through the use of steganography, information can be transmitted while being disguised within another piece of data. Significant amounts of data can be moved through common means of electronic communication, with little threat of detection. This data can be transmitted with the hidden information included, and travel across networks looking like normal traffic. Any third party that intercepts the data

will not expect it to contain such a secret. Implementation of steganography is not hard to achieve, and there are multiple variations of programs that will encode and decode information . Hiding data through steganographic means has become easier due to the availability of free programs online. In addition, the number of technologically adept individuals is increasing on a daily basis. The ability to deal with steganography will become a more crucial skill in future information flows.

Effort has been made to establish ways of detecting whether or not a piece of data contains a steganographic element. Unfortunately, not many steganographic messages can be detected . In addition to the difficulties related to detection, the message is still encoded, and extra time is needed to translate the message into an understandable format. The message can even be encrypted while hidden in the data via steganographic means, allowing the data to be sent without there appearing to be an encrypted file, but still having the benefits of being encrypted.This process of detection and analysis can be time consuming, meaning that the attack against steganography is not a real-time attack.

The interception and analysis of steganography is not always necessarily needed. What is important is preventing the intended party from receiving the data that is being sent. This could be accomplished by simply stopping data that is detected as steganographic, however, in the course of detection, there is still a significant amount of false positives, which would result in data being stopped that has no steganographic content. In addition, not all data that has steganographic content will be detected and stopped. A need for a better form of security against the transmission of steganography must be implemented, one which can be achieved in real time.

This end could be accomplished through alterations to the picture. These alterations can either be made within the cover image, or directly to the bits that store the hidden message. Both methods result in the destruction of the hidden data with little damage to the image it is embedded in, also known as the cover image. Destruction of steganography on a mass scale will serve as hidden communication.

II DISCRETE WAVELET TRANSFORM

To use the wavelet a means to protect information, and prevent transform for image processing we must implement a 2D version of the analysis and synthesis filter banks. In the 2D case, the 1D analysis filter bank is first applied to the columns of the image and then applied to the rows. If the image has N1 rows and N2 columns, then after applying the 1D analysis filter bank to each column we have two subband images, each having N1/2 rows and N2 columns; after applying the 1D analysis filter bank to each row of both of the two subband images, we have four subband images, each having N1/2 rows and N2/2 columns. This is illustrated in the diagram below. The 2D synthesis filter bank combines the four subband images to obtain the original image of size N1 by N2.

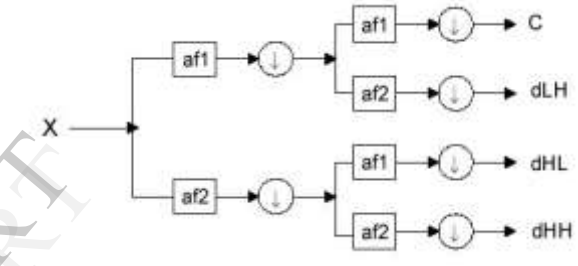

Fig.a. One stage in multi-resolution wavelet decomposition of an image

III IMPLEMENTATION OF THE PROPOSED METHOD

A. Procedure for Embedding using Three Level Wavelet Decomposition

l. Perform three level 2D-Haar DWT decomposition as follows:

a) Take the cover image (JPEG) (512 x512) and its green plane alone and perform first level 2D-DWT on the image to obtain approximation 1 coefficient (LL 1), horizontal 1 coefficient (HL 1), vertical 1 coefficient (LH 1), diagonal 1 coefficient (HH1) respectively.

b) Take the approximation 1 coefficient (LLl) and perform second level 2D-DWT on the image to obtain approximation 2 coefficient (LL2), horizontal 2 coefficient (HL2), vertical 2 coefficient (LH2), diagonal 2 coefficient (HH2) respectively.

c) Take the approximation 2 coefficient (LL2) and perform third level 2D-DWT on the image to obtain approximation 3 coefficient (LL3), horizontal 3

coefficient (HL3), vertical 3 coefficient (LH3), diagonal 3 coefficient (HH3) respectively.

2. Take the secret image and turn it into black and white.

3. Perform Embedding as follows:

a) Assume an embedding coefficient of value of0.05.

b) Process LL3 block by block (4x4).

c) Process the secret image block by block(4X4).

d) The following formula is used to obtain the secret image block (4x4) which is basically swapping,

Secret image block =(1-Embedding Coefficient) x LL3 intensity value) + (Embedding coefficient x secret image intensity value)

4. Perform three level 2D-Haar inverse DWT for reconstruction which is the inverse process of three level 2D-Haar DWT decomposition in order to obtain the stego image

5. Calculate the PSNR value in order to check for the visual quality of the stego image.

$$PSNR = 10\ I0g_{10}\frac{255^2}{MSE} \quad \_(7)$$

where MSE (Mean Square Error) stands for the mean-squared difference between the cover-image and the stegoimage. The mathematical definition for MSE is:

$$MSE = \left(\frac{1}{M\ x\ N}\right)\sum_{i=1}^{M}\sum_{j=1}^{N}(a_{ij} - b_{ij})^2 \quad \_\_ (8)$$

In Equation 8, aij means the pixel value at position (i,j) in the cover-image and bij means the pixel value at the same position in the corresponding stegoimage.

The calculated PSNR usually adopts dB value for quality judgment. The larger PSNR is, the higher the image quality is (which means there is only little difference between the cover-image and the stegoimage). On the contrary, a small dB value of PSNR means there is great distortion between the coverimage and the stego-image.

B. Procedure for Extracting using Three Level Wavelet Decomposition

1. Perform three level 2D-Haar DWT decomposition on the stego image as well the cover image as we did in the embedding procedure.

2. Calculate the PSNR for the decomposed stego image as well as the cover image for finding out in which sub-band the secret image has beenembedded. On examining we will find it out to be LL3.

3. Process LL3 of the stego image block by block (4x4).

4. Process LL3 of the cover image block by block (4x4).

5. Assume an embedding co efficient of 0.05

6. Use the formula which follows to get the image blocks of the secret image.

Secret image block = (LL3 intensity value of the stego image-((l-embedding coefficient) x LL3 intensity value of the cover image))/Embedding coefficient.

IV CONCLUSION

A new image data hiding technique based on discrete wavelet transform has been proposed. The stego-image is looking perfectly intact and has high peak signal to noise ratio value. Hence, an unintended observer will not be aware of the very existence of the secret-image. The extracted secret image is perceptually similar to the original secret image.

In this paper the technique using three level discrete wavelet transformfor hiding images has been proposed and implemented.

ACKNOWLEDGMENT

I take immense pleasure in thanking my dept internal guide **Mrs.C.Jayashree ,M.E.** , who motivated enthusiastically in all our efforts in completing this paper successfully. I am grateful to her precious guidance and suggestions.

I would also thank my Institution and Faculty members without whom this project would have been a distant reality. I also extend my heartfelt thanks to my Family andWell Wishers.

REFERENCES

[1] Kumar, V., Kumar, D,Performance evaluation of DWT based image steganography , Advance Computing Conference (IACC), 2010 IEEE 2nd International

[2] Po-Yueh Chen, Hung-Ju Lin, "A DWT Based Approach for Image Steganography", InternationalJournal of Applied Science and Engineering 2006. 4, 3: 275-290

[3] Wang, H, Wang, S, "Cyber warfare: steganography vs.Steganalysis", Communications of the ACM, 47:10, October 2004

[4] Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", SANS Institute, January 2002

[5] Artz, D., "Digital Steganography: Hiding Data within Data", IEEE InternetComputing Journal, June 2001

[6] Petitcolas, Fabien A.P., "Information Hiding: Techniques for steganography and Digital Watermarking.", 2000.

[7] Sellars, D., "An Introduction to Steganography",URL:www.cs.uct.ac.zalcourses/CS400 W INIS/papers991 dsellarslstego. Html

[8] Johnson, N. F., S. Jajodia, "Exploring Steganography: Seeing the Unseen," iEEE Computer, vol. 31, no. 2, 1998, pp. 26-34.