Efficient Routing Strategy for Structured Peer to Peer System Using DWT Based Steganography

D. Pradeepa[1], S. Rani Lakshmi[2]

[1, 2]Assistant Professor, Department of Computer Technology
Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore-49, India

Abstract: ***In structured P2P systems, message deliverance can be done by identifying the peer IDs of the individual systems. The message passes from one hop to another correctly by identifying the IP address and finally reaches the destination. In this paper we propose an efficient routing strategy to control the routing path and to identify the malicious nodes. We also eliminate the drawbacks of encryption by introducing steganography in message deliverance. A lossless data hiding scheme is presented based on quantized coefficients of discrete wavelet transform (DWT) in the frequency domain to embed secret message. Using the quantized DWT based method; we embed secret data into the successive zero coefficients of the medium-high frequency components in each reconstructed block for 3-level 2-D DWT of cover image. The security of the proposed scheme can be further improved by employing compression and encryption techniques using AES. The experimental results show that the algorithm has a high capacity and a good invisibility. Moreover the quality of the messages/images are measured by the PSNR, Figure of Merits, MSSI (Mean Structural Similarity Index) of cover image with stego-image shows better results in comparison with other existing steganography approaches.***

Keywords: peer-to-peer system, DWT, 2D-DWT, PSNR, MSE

1. Introduction

Steganography is a secret communication technique, in which the event of communication taking place itself is concealed. [1]Cryptography and watermarking are the close related techniques to steganography. Fundamentally both cryptography and steganography are information securing technique but they differ in their implementation. Cryptography makes secret data unreadable bya third party, [8] whereas steganography hides secret data from a third party. Both of their notions remain the same. The cover medium suitable for a steganography can be any entity that can be digitally represented such as a text file, image, audio, video and un used portion of TCP/IP packet headers.

During the process of hiding the information three factors must be considered that are **capacity** it includes amount of information that can be hidden in the cover medium. **Security** implayes to detect hidden information and **Robustness** to the amount of modification the stego medium can withstand before an adversary can destroy hidden information [2].

There are two kinds of image teganographic techniques: spatial domain and frequency domain based methods. The schemes of the first kind directly embed the secret data within the pixels of the cover image such as Least Significant Bit (LSB) insertion. The schemes of the second kind embed the secret data within the cover image that has been transformed such as DWT (discrete *wavelet* transforms). The DWT coefficients of the transformed cover image will be quantized, and then modified according to the secret data [4].

The intensity values in the two dimensional matrix of an image are represented by n bits, which is called as bit depth of an image. Bit depth vary from 2 to 32 bits depends upon the support offered by the hardware and software. Among the redundancy, coding redundancy is the one which can be confidently used to attain error-free or lossless compression. Huffmanen coding is a variable length lossless compression technique, can be applied to any entity which can be digitally represented. Several coding techniques can be used in conjunction with Huffman encoding to compress the payload. Integrating all the above said entity under a single strand ends up with higher compression results in high embedding capacity of a steganography algorithm. This is discussed detail in background section. The objective of the proposed work is to embed a grayscale secret image on a 24 bit RGB cover image using various coding technique. The gray coded binary data of secret image is bit planed and run length encoded, prior it is submitted to Huffman encoding technique results in supporting higher embedding capacity and peak signal to noise ratio.

2. Least Significant BIT (LSB)

Least Significant Bit (LSB) Embedding Steganography application that hides data in image generally uses a variation of least significant bit (LSB) embedding. [5]In this technique the data is hidden in the least significant bit of each byte in the image, the size of each pixel depends on the format of the image and normally ranges from 1 byte to 3 bytes. An 8 bit pixel is capable of displaying 256 different colors. Given two identical images, if the least significant bits of pixels in one image are changed the two images still looks identical to the human eye [3]. 24-Bit Image To hide an image in the LSBs of each byte of a 24-bit image, we can store 3 bits in each pixel. A 1,024 * 768 image has the potential to hide a total of 2,359,296 bit (294,912) bytes of information.

E.g. the letter A can be hidde n in three pixels. The original raster data for 3 pixels (9 bytes) may be;

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

The binary value for A is 10000011. Inserting the binary value for A in the three pixels would result in;

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

On average, LSB requires that only half the bits in an image be changed.

3. The Wavelet Transform (DWT)

Wavelets are special functions which (in a form analogous to sins and cosines in Fourier analysis) are used as basal functions for representing signals. The discrete wavelet transform (DWT) we applied here is Haar-DWT, the simplest DWT. In Haar-DWT the low frequency wavelet coefficient are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. For 2-D images, applying DWT (Discrete Wavelet Transform) separates the image into a lower resolution approximation image or band (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components as shown in figure 2. And subsequent 2-D IDCT on the composite image (cover image + targetimage1 + targetimage2).

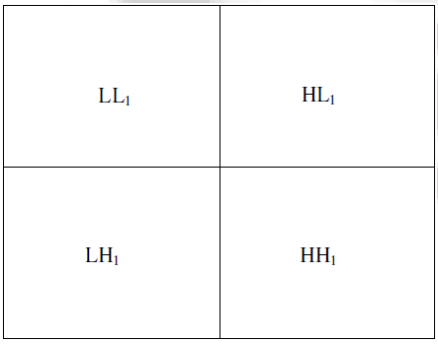


Figure 2: Components of 1-level 2-Dimensional Discrete Wavelet Transform

Lastly, the main advantage of this method is that two images can be hidden behind one image. Moreover during transmission, a complete new image (different from cover or target images) is transmitted over network thereby reducing the chance of suspicion of the network eavesdropper.

3.1 Huffman Encoding and Huffman Table

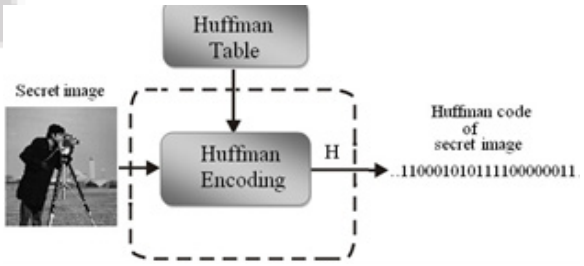
Huffman code has been widely **used** in data, image, and video compression [6]. Huffman encoding takes a sequence (stream) of symbols as input and gives a sequence of bits as output. The intent is to produce a short output for the given input. Each input yields a different output, so the process can be reversed, and the output can be decoded to give back the original input. In this software, a symbol is a non-negative integer. The symbol limit is one plus the highest allowed symbol. For example, a symbol limit of 4 means that the set of allowed symbols is {0, 1, 2, 3} before embedding the secret image into cover image, it is first encoded using Huffman coding. Huffman codes are optimal codes that map one symbol to one code word. For an image Huffman coding assigns a binary code to each intensity value of the image and a 2-D M2 × N2 image is converted to a 1-D bits stream with length LH < M2 × N2. Huffman table (HT) contains binary codes to each intensity value. Huffman table must be same for both the encoder and the decoder. Thus the Huffman table must be sent to the decoder along with the compressed image data.

We proposed the secret message/image embedding scheme comprises the following five steps:

Step 1: Decompose the cover image by using Haar wavelet transform.
Step 2: Huffman encoding. Perform Huffman encoding on the 2-D secret image S of size M2 × N2 to convert it into a 1-D bits stream H.
Step 3: 3-bit block (Bi) preparation Huffman code H is decomposed into 3-bits blocks and thus form a decimal value ranging from 0 to 7. For example, the binary sequence …. 110 001 010 111 100 000 011 will be changed to the decimal sequence (Bi) … 6 1 2 7 4 0 3.
Step 4: Bits replacement Select one sub-band for embedding the secret message. If we donate 'f' as coefficients matrix of the selected sub-band, then using the following equation, the 3 least significant bits of wavelet coefficients is replaced by the 3 bits of Huffman encoded bit stream in the form of 3 bit block Bi.

$$f'(x,y) = f(x,y) - f(x,y) \% 8 + Bi \quad \text{----------(1)}$$

Step 5: IDWT
[7]Apply the Haar inverse DWT (IDWT) on the DWT transformed image, including the modified subband to produce a new image f1 which contains secret image.



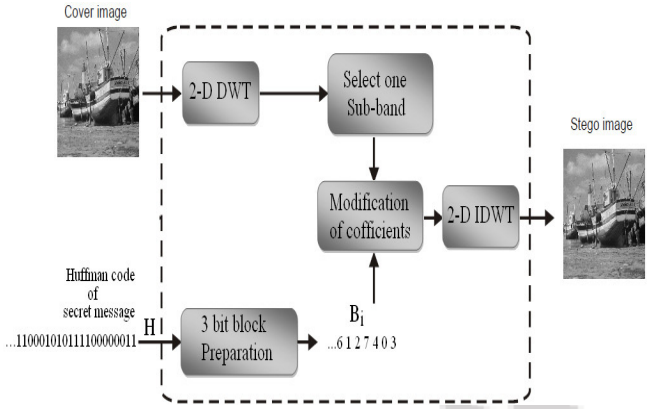
(a) Huffman encoding of secret image (or message)

3.2 Embedding Algorithm

Input: An M1×N1 carrier image and a secret message/image.

Output: A stego-image.

1. Obtain Huffman table of secret message/image.
2. Find the Huffman encoded binary bit stream of secret-image by applying Huffman encoding technique using Huffman table obtained in step 1.
3. Decompose the cover image by using Haar wavelet transform
4. Calculate the size of encoded bit stream in bits.
5. Repeat for each bit obtained in step 4 (a) Insert the 3 consecutive bits into 3 LSB position in each DWT coefficient of the selected subband.
6. Repeat for each bit obtained in step 2 (a) Insert the 3 consecutive bits into 3 LSB position in each DWT coefficient (excluding the first four coefficients in each sub-band) of the selected sub-band.
7. Repeat for each bit of the Huffman table
8. Insert the 3 consecutive bits into 3 LSB position in each DWT coefficient of the selected sub-band.
9. Apply inverse DWT.
10. End.



(b) Insertion of a Huffman code of secret image (or message) into a Cover image

3.3 Extraction of the Secret Message / Image

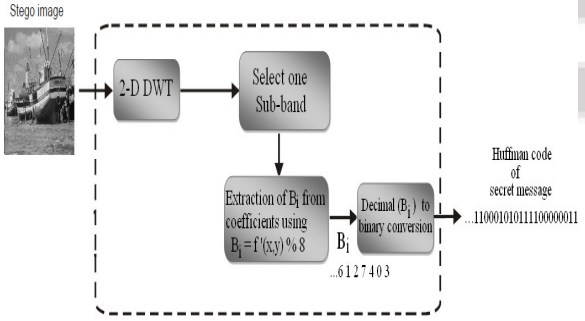
The stego-image is received in spatial domain. DWT is applied on the stego-image to transform the stego-image from spatial domain to frequency domain. The following formula is used to extract bit stream from wavelet coefficients in the form of blocks Bi. Bi =f˝(x,y) % 8 ---------- (2) The size of the encoded bit stream and the encoded bit stream of secret message/image are extracted long with the Huffman table of the secret message/image. The block diagram of the extracting process is given in figure (c) and (d) and the extracting algorithm as follow:

Extraction Algorithm

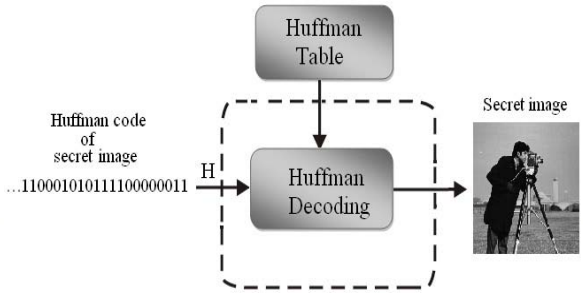
Input: An M1×N1 Stego-image.

Output: Secret image.
Apply DWT to the stego-image.

1. The size of the encoded bit stream is extracted from 1st four DWT coefficients in each subband by collecting the 3 least significant bits.
2. The 3 least significant bits of all of the DWT coefficients inside each sub-band (excluding the first four coefficients in each sub-band) are collected and added to a 1-D array.
3. Repeat step 3 until the size of the 1-D array becomes equal to the size extracted in step 2.
4. Construct the Huffman table by extracting 3 bits from the LSB of all of the DWT coefficients inside each sub-bands excluding the coefficients used in step 2 and step 3.
5. Decode the 1-D array obtained in step 3 using the Huffman table obtained in step 5.
6. End.



(c) Removal of Huffman code of secret Image (or message)



(d) Huffman decoding of secret image (or message)

4. Key Providing for Authentication Using AES

In AES Implementation, we are getting the cipher text in the hexadecimal form and the length of the cipher text is very large. In the newly proposed technique we partially hide the encrypted information in the image and with the help of the remaining part of the encrypted message we generate two keys. These two keys are secret keys and the receiver needs to know these two keys to retrieve the original encrypted message.

4.1 Hiding Text

- Generate the cipher text in hexadecimal form by AES algorithm [13] in the form of alphabets (A, B, C, D, E, F) and digits (0, 1, 2, 3, 4, 5, 6, 7, 8, 9).
- Separate the alphabets and digits with the help of Separator 1 and keep track of the original position of the alphabets and digits in the form of the first key (**Key 1**).
- Take the first 7 characters of the alphabets; this part will be hidden in the image.
- Take the rest of the alphabets and combine with the digits; this will form the second key (**Key 2**).
- Hide the characters in the Image.

4.2 Retrieving Text

- Retrieve the 7 characters from the image.
- Separate alphabets and digits from **Key 2** with the help of Separator 2.
- Add back the rest of the alphabets from **Key 2** to 7 characters retrieved from the image.
- Reorganize the alphabets and digits with the help of the **Key 1** to get back the original cipher text in hexadecimal form.
- Regenerate the original text message from the cipher text with the help of AES algorithm

5. Results and Discussion

Comparative analysis of LSB based and DWT based steganography has been done on basis of parameters like PSNR. Both grayscale and colored images have been used for experiments. Peak signal to noise ratio is used to compute how well the methods perform. PSNR computes the peak signal to noise ratio, in decibels, between two images. This ratio is used as a quality measurement between two images. If PSNR ratio is high then images are best of quality. The fig 3 and fig 4 shows the result for dwt and dwt with huffman encoding respectively. Ane psnr ration for dwt is 34; in dwt with huffman encoding is 44.0

$$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right)$$

Figure 1: Peak Signal-to-Noise Equation

where the **MSE** (*Mean Squared Error*) is:

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|^2$$

Figure 2: Mean Squared Error Equation

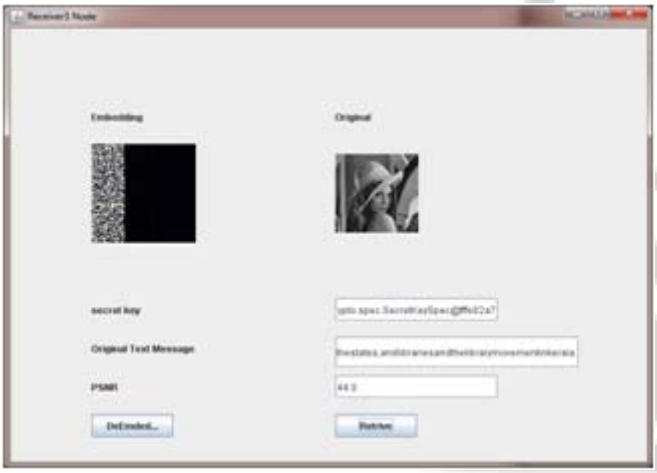


Figure 3: DWT Steganography

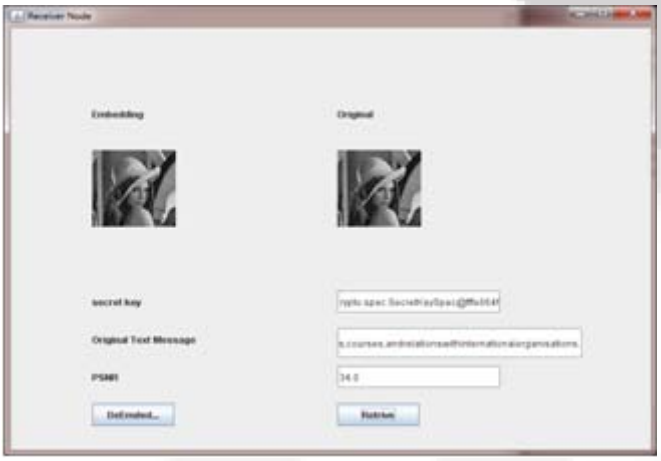


Figure 4: DWT Steganography combined with Huffman Encoding

6. Conclusion

In this paper, our objective is to provide directions for designing secure message routing with acknowledgement by using steganography. We consider three aspects: authorization, routing and safe message delivery using steganographic techniques. We have introduced a new steganographic encoding scheme which separates the color channels of the windows bitmap images and then randomly hide messages in the LSB of one component of the chosen pixel where the color coefficients of the other two are found to be equal to the keys selected. In addition to this we have introduced DWT based steganography which embeds the text message in LSB of DC coefficients. This paper implements LSB based steganography, 2D-DWT based steganography combined with Huffman Encoding and computes PSNR ratio. PSNR is the peak signal to noise ratio, in decibels, between two images. This ratio is used as a quality measurement between two images. If PSNR ratio is high then images are of better quality.Next have to implement Figure of Merits (FOM) steganography techniques in 3R-DWT for better performance

References

[1] W. Bender, D. Gruhl ,N. Morimoto, A. Lu"Techniques for dataHiding" IBM SYSTEMSJOURNAL, VOL 35, NOS 3&4, 1996

[2] Hniels Provos & Peter Honeyman,"Hide & Seek: An Introduction to Steganography" IEEE Computer Society Pub-2003.

[3] M. Castro, P. Duschel, A. Rowstron, and D. S. Wallach, "Secure routing for structured peer-to-peer overlay network". In Proceedings of the fifth Symposium on Operating System Design and Implementation, Dec 2002.

[4] G.Satyavathy, M.Punithavalli, "Steganography in Safe Message Routing and delivery for Structured Peer-to-Peer Systems". International Conference on Intelligent Information Systems and Management (IISM'2010), June10-12,2010

[5] Prof.S.V.Kamble1 ,Prof. B.G.Warvante2 A Review on Novel Image Steganography Techniques IOSR Journal of Computer Engineering (IOSR-JCE) ISSN: 2278-0661, ISBN: 2278-8727, PP: 01-04

[6] T.C. Bell, J.G. Cleary and I.H. Witten, Text Compression (Prentice Hall, Englewood Cliffs, NJ, 1990).

[7] Po-Yueh Chen* and Hung-Ju Lin "A Dwt Based Approach For Image Steganography" International Journal of Applied Science and Engineering 2006. 4, 3: 275-290

Author Profile

D. Pradeepa received the BCA and MCA degree in Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore in 2006 and 2009 respectively. One year worked as a assistant professor after that joined to do M.Phil in Sri Ramakrishna college of Arts and Science for Women. In that period she has presented two papers in international conference conducted by PSGR Krishnammal College for Women. In 2013 received M.Phil degree. At present working as a Assistant Professor in Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore with 3 years 7 months experience.