IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 5, Ver. III (Sep. – Oct. 2015), PP 53-59
www.iosrjournals.org

A New Approach to Compressed Image Steganography Using Wavelet Transform

Tapan Kumar Hazra[1], Anurag Anand [1], Antra Shyam [1] , Dr Ajoy Kumar Chakraborty[2]

[1]*Department of Information Technology, Institute of Engineering & Management, Salt Lake Electronics Complex, Kolkata-700091,West Bengal, India*
[2]*Department of Electronics and Communication Engineering , Institute of Engineering & Management, Salt Lake Electronics Complex, Kolkata-700091,West Bengal, India*

Abstract : *This paper proposes a novel steganographic technique that embeds compressed payload image within cover image. The pixel adjustment of the cover image is done optimally using Fourier Transform, so that visual characteristics change of the cover image is kept as minimum. The work presents the application of Discrete Wavelet Transform (DWT) for image compression, Discrete Fourier Transform (DFT) as the efficient selection of pixel locations in cover image and suggests as a new approach to compressed image steganography. We apply the Fourier Transform to our cover image and calculate the coefficients less than or higher than a particular threshold value. These coefficients coordinates are stored in an array. Wavelet transform is applied to the payload image and the approximate coefficients are calculated. These coefficients replace the Fourier coefficients of the original image. The distortion in the stego-image is less when the size of the coefficient matrix is smaller. For the extraction part, the intensity values at the above stored coordinates are extracted and the approximate coefficient matrix is obtained. Inverse Wavelet Transform is applied to obtain the hidden payload image.*

Keywords: Cover Image, Discrete Fourier Transformation, Discrete wavelet transformation, Payload Image, Steganography, Stego-image

I. Introduction

Steganography is the art and science to hide data in a cover, the data can be text, audio, video, image etc. Steganography derives from the Greek word, "Steganos", meaning covered or secret, and "graphy" means writing or drawing. On the simplest level, steganography is hidden writing, whether it consists of invisible ink on paper or copyright information hidden in an audio file. Today, steganography is most often associated with data hidden with other data in an electronic file. This is usually done by replacing that least important or most redundant bits of data in the original file. Where cryptography scrambles a message into a code to obscure its meaning, steganography hides the message entirely. Steganography is the process of hiding a secret message within a larger one in such a way that someone cannot know the presence or contents of the hidden message. The purpose of Steganography is to maintain secret communication between two parties.

Data hiding techniques are generally divided in two groups: spatial and frequency domain. The first group embeds message in the Least Significant Bit (LSB) of the image pixel. These methods are sensitive against slight modification such as compression and low pass filtering but, its implementation is simple and capacity is high [1]. Algorithms using LSB in grayscale images can be found in [2, 3].

The second group embeds the message in the frequency coefficients of the images. This method is more robust than LSB method. Least significant bits (LSB) insertion is a simple approach to embedding information in image file. The simplest Steganographic techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small.

Masking and filtering techniques, usually restricted to 24 bits and gray scale images, hide information by marking an image, in a manner similar to paper watermarks. The techniques performs analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the noise level.

Transform techniques embed the message by modulating coefficients in a transform domain, such as the Discrete Cosine Transform (DCT) used in JPEG compression, Discrete Fourier Transform, or Wavelet Transform are also used for this purpose. These methods hide messages in significant areas of the cover-image, which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image, or other variants. R. Chandramouli and N. Memon in 2001, considered some specific image based steganography techniques and shown that an observer can indeed distinguish between images carrying a hidden message and images which do not carry a message [4].

The paper is organized as follows: Section 2 introduces the proposed Steganographic method in detail. Section 3 discusses the achieved result and compares the five cases. Section 4 concludes the paper.

II. Proposed Steganographic Method

A. Discrete Wavelet Transformation:

A time-scale representation of a digital image is obtained using digital filtering technique. Signal is passed through a series of high pass filter to analyze the high frequency and low pass filter to analyze the low pass frequency. A half band low pass filter removes all the frequencies that are above half of the highest frequency in the signal. In discrete signals frequency are represented in radians.

B. How DWT is computed :

The DWT analyze the signal at different frequency bands with different resolutions by decomposing the signal into coarse approximation and detail information.

Dwt employs 2 sets of functions called scaling function and wavelet function. Scaling function is associated with low pass filter and wavelet function is associated with high pass filter. Decomposition of the signal into different frequency bands is simply obtained by successive high pass and low pass filtering of the time domain signal. The original signal x[n] is first passed through half band high pass filter g[n] and low pass filter h[n]. After filtering half of the samples can be eliminated according to Nyquist's rule. Since the signal now has a highest frequency of p/2 radians instead of p radians. The signal can be sub sampled by 2 simply by discarding every alternate sample. This constitutes one level of decomposition. The decomposition halves the time resolution since only half the number of samples now characterizes the entire signal. Frequency resolution doubles since the frequency band of the signal spans only half the previous frequency bands, effectively reducing the uncertainty in frequency by half. This procedure is called sub band coding.

Discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency and location information (location in time).

The discrete wavelet transform (DWT) is a linear transformation that operates on a data vector whose length is an integer power of two, transforming it into a numerically different vector of the same length. It is a tool that separates data into different frequency components, and then studies each component with resolution matched to its scale.

The main feature of DWT is multistage representation of function. By using the Wavelets, given function can be analyzed at various levels of resolution. The DWT is also invertible and can be orthogonal.

To use the wavelet 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 N_1 rows and N_2 columns, then after applying the 1D analysis filter bank to each column we have two sub band images, each having $N_1/2$ rows and N_2 columns; after applying the 1D analysis filter bank to each row of both of the two sub band images, we have four sub band images, each having $N_1/2$ rows and $N_2/2$ columns. The 2D synthesis filter bank combines the four sub band images to obtain the original image of size N_1 by N_2 [5].

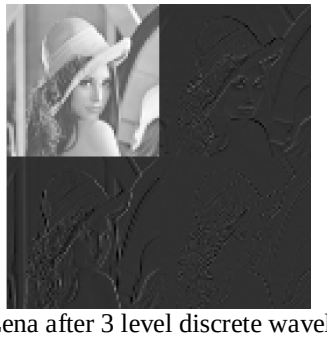

Figure 1: Image Lena after 3 level discrete wavelet transformation

The Fourier Transform is a tool that breaks a waveform (a function or signal) into an alternate representation, characterized by sine and cosines. The Fourier Transform shows that any waveform can be re-written as the sum of sinusoidal functions.

The proposed method applies Fourier transform on the cover image to calculate the coordinates where intensity values are less or higher than threshold value. Also, Wavelet transform is applied on the payload image to calculate the approximate wavelet coefficients of the payload image. These wavelet coefficients are

embedded at those pixel coordinates of the cover image where the intensity value was less than or higher than the threshold value. This paper presents the 5 different cases of the proposed steganography method.

Case 1.

A. Encoding Algorithm

Step1. Fourier transform is applied to the cover image and coordinates where intensity value is less than the threshold values are calculated.

Step2. 3-level discrete wavelet transform is applied on the payload image. Approximate coefficient matrix LL3 of size 32*32 is obtained.

Step3. The intensity values at the calculated coordinates are replaced by these 1024 wavelet coefficient values to obtain the Stego image.

B. Decoding Algorithm

Step1. Stego image is read and the intensity values are extracted from the already calculated coordinates.

Step2. These values are used to form the 32*32 approximate coefficient LL3 matrix.

Step3. 3- level inverse wavelet transform is applied to obtain the hidden payload image.

For chosen threshold value 256.43, results are given in Fig. 2 (a) – (d).

Case 2.

A. Encoding Algorithm

Step1. Fourier transform is applied on the cover image and coordinates where intensity value is less than the threshold values are calculated.

Step2. 2-level discrete wavelet transform is applied on the payload image. Approximate coefficient matrix of size 64*64 is obtained.

Step3. The intensity values at the calculated coordinates are replaced by these 4096 wavelet coefficient values to obtain the Stego image.

B. Decoding Algorithm

Step1. Stego image is read and the intensity values are extracted from the already calculated coordinates.

Step2. These values are used to form the 64*64 approximate coefficient matrix.

Step3. 2-level inverse wavelet transformation is applied to obtain the hidden payload image.

For chosen threshold value 128.5, results are given in Fig. 3 (a) – (d).

Case 3.

Image Steganography using LL3 wavelet coefficients to replace the high intensity Fourier coefficients, to generate the Stego image. Original image is lena of size 512*512. Cover Image is image.bmp of size 256*256. For threshold value 96637.4, the results are given in Fig. 4 (a) – (d).

A. Encoding Algorithm

Step1. Fourier transform is applied on the cover image and coordinates where intensity value is higher than the threshold values are calculated.

Step2. 3-level discrete wavelet transform is applied on the payload image. Approximate coefficient matrix of size 32*32 is obtained.

Step3. The intensity values at the calculated coordinates are replaced by these 1024 wavelet coefficient values to obtain the Stego image.

B. Decoding Algorithm

Step1. Stego image is read and the intensity values are extracted from the already calculated coordinates.

Step2. These values are used to form the 32*32 approximate coefficient matrix.

Step3. 3-level inverse wavelet transformations are applied to obtain the hidden payload image.

Case 4.

Image Steganography using LL3 wavelet coefficients to replace the high intensity Fourier coefficients, to generate the Stego image. Original image is image.bmp of size 256*256. Cover Image is lena.bmp of size 512*512. For threshold value 3631.5, the results are given in Fig. 5 (a) – (d).

A. Encoding Algorithm

Step1. The cover image and the payload image are interchanged (objective is to embed even higher payload image within smaller cover image).

Step2. Fourier transform is applied on the cover image and coordinates where intensity value is higher than the threshold values are calculated.

Step3. 2-level discrete wavelet transform is applied on the payload image. Approximate coefficient matrix of size 64*64 is obtained.

Step4. The intensity values at the calculated coordinates are replaced by these 4096 wavelet coefficient values to obtain the Stego image.

B. Decoding Algorithm

Step1. Stego image is read and the intensity values are extracted from the already calculated coordinates.

Step2. These values are used to form the 64*64 approximate coefficient matrix.

Step3. 3 level inverse wavelet transformations are applied to obtain the hidden payload image.

Case 5.

A. Encoding Algorithm

Step1. Fourier transform is applied on the cover image and coordinates where intensity value is less than the threshold values are calculated.

Step2. 3-level discrete wavelet transform is applied on the payload image. Approximate coefficient matrix of size 32*32 is obtained.

Step3. In order to obtain the Stego image, the intensity values at the calculated coordinates of the Fourier transformed image and the approximate wavelet coefficients are converted to 8 bit bit-stream.

Step4. 4 least significant bits of the Fourier coefficients are replaced by the 4 least significant bits of the wavelet coefficients.

Step5. The bit stream is reconverted to decimal values. In this way the payload image is hidden in the cover image. The Stego image obtained is lossless.

B. Decoding Algorithm

Step1. Stego image is read and the intensity values at the already calculated coordinates are extracted.

Step2. The magnitude of these values are calculated and converted to 8 bit bit-stream.

Step3. The 4 least significant bits are extracted and converted into decimal values.

Step4. These values are used to obtain the 32*32 wavelet approximate coefficient matrix.

Step5. 3 level inverse wavelet transformations are applied to obtain the hidden payload image.

For chosen threshold value 128.5, results are given in Fig. 6 (a) – (d).

III. Analysis and Comparison of RESULTS

Case 1

Figure 2. (a) (b) (c) (d)

(a) Shows cover image. (b) Shows the payload image. (c) Shows the stego image after embedding b into c. (d) Extracted payload image from c

Case 2

Figure 3. (a) (b) (c) (d)

(a) Shows cover image. (b) Shows the payload image. (c) Shows the stego image after embedding b into c. (d) Extracted payload image from c

Case 3

Figure 4. (a) (b) (c) (d)

(a) Shows cover image. (b) Shows the payload image. (c) Shows the stego image after embedding b into c. (d) Extracted payload image from c

Case 4

Figure 5. (a) (b) (c) (d)

(a) Shows cover image. (b) Shows the payload image. (c) Shows the stego image after embedding b into c. (d) Extracted payload image from c

Case 5

Figure 6. (a) (b) (c) (d)

(a) Shows cover image. (b) Shows the payload image. (c) Shows the stego image after embedding b into c. (d) Extracted payload image from c

The problem an ideal steganography scheme has to face is to preserve the details of the cover image when the secret message is being embedded in so that the differences between the stego-image and the cover image can be perfectly imperceptible to the human eye.

The higher the stego image quality, the more invisible the hidden message.

Therefore, the stego-image quality is a very important criterion to use when we evaluate the performance of a Steganographic technique. Whether the Stego-image quality is acceptable to the human eye

can be judged by using the Peak Signal-to-Noise Ratio (PSNR) and MSE, whose formula is given by (1) and (2) respectively:

$$PSNR = 10\ log_{10} \frac{255^2}{MSE} \quad (1)$$

$$MSE = \left(\frac{1}{M * N}\right) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (P(x,y) - P'(x,y))^2 \quad (2)$$

Here M and N represents the image dimension. In (2), P(x, y) stands for the pixel value of cover image, and P'(x, y) represents the pixel value at position (x, y) of the Stego image. A greater PSNR value means a lower degree of image distortion after the hiding of the secret data.

Table 1: Comparison between above 5 cases

Case	*MSE*	*PSNR (db)*
1	1.00	48.1817972
2	3.98	42.1611972
3	1.00	48.1817972
4	15.94	36.1405973
5	0.70	49.7336213

IV. Conclusion

In this paper we have applied Discrete Wavelet transform on the payload image and Fourier transform on the cover image for the purpose of steganography. DWT is used to reduce the size even larger payload image. The process of efficient selection of pixels from cover image for embedding secret payload image will reduce the visual characteristics difference error between the cover image and stego-image. In this way we can increase the hiding capacity with low distortions. The comparisons between the results are shown using five different cases in TABLE 1. Only in case 4, the role of cover and payload image is changed. The cover image is grayscale image of Lena of size 512*512. Among the five different mentioned cases, the mean square error is least in case 4, where the size of cover image is 256*256 and size of payload image is 512*512.

Case 5 gives the best result. Here the mean square error is less than 1.0. Hence the value of PSNR is maximum, and consequently the degree of distortion is least. The modifications done into the cover image, stego-image in order to embed the secret image is considerably good and invisible to the human eye since the value of PSNR in all the above cases is beyond 36db value [1].

References

[1] N.Wu and M.Hwang. "Data Hiding: Current Status and Key Issues," International Journal of Network Security, Vol.4, No.1, pp. 1-9, Jan.2007
[2] A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution Hengfu YANG, Xingming SUN,Guang SUN.
[3] C. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, pp. 469-474, Mar. 2004.
[4] R. Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques," International Conference on Image Processing, Thessaloniki, Greece, pp. 1019-1022, 2001.
[5] Image compression using Haar wavelet transform, Colm Mulcahy,Ph.D

Author Profile

Tapan Kumar Hazra completed his M.E degree from Jadavpur University, Kolkata, West Bengal, India. Since from 2003, he is working as Assistant Professor of Department of Information Technology at Institute of Engineering & Management, Salt Lake, Kolkata, West Bengal, India. His research interest includes Design and Analysis of Algorithms, Image Processing, Wavelet transforms and its various applications, Multimedia technology, Machine learning, Cryptography, Watermarking and Steganography for secure communication, Natural Language processing.

 **Anurag Anand**, pursuing B.TECH degree in Information Technology at Institute of Engineering & Management, West Bengal University of Technology, West Bengal, India and is in his Final year (Final Semester). His areas of interest for research include image Processing.

 **Antra Shyam**, pursuing B.TECH degree in Information Technology at Institute of Engineering & Management, West Bengal University of Technology, West Bengal, India and is in her Final year (Final Semester). Her areas of interest for research include image Processing.

 Dr. Ajoy Kumar Chakraborty graduated in science in 1961 and did his M. Tech in applied Physics in 1966 from calcutta University. He did his doctorate degree from University of Paris, France, in 1974. He served calcutta University, as a faculty in Department of Applied Physics and Department of Applied optics and Photonics, for about 38 years. At present he is worhing as Professor of Department of Electronics and Communication Engineering at Institute of Engineering & Management, Salt Lake, Kolkata, West Bengal, India. His current research interest includes polarization optics, birefringement networks, Image Processing, Wavelet transforms and its various applications, Cryptography, Watermarking and Steganography for secure communication, Digital holography.