A STEGANOGRAPHIC METHOD BASED ON INTEGER WAVELET TRANSFORM & GENATIC ALGORITHM

Nitesh Kumar Jangir
Assistant Professor
Department of CSE
Sobhasaria Group of Institution,Sikar, Rajasthan, India

Abstruct:- The proposed system presents a novel approach of building a secure data hiding technique of steganography using inverse wavelet transform along with Genetic algorithm. The prominent focus of the proposed work is to develop RS-analysis proof design with higest imperceptibility. Optimal Pixal Adjustment process is also adopted to minimize the difference error between the input cover image and the embedded-image and in order to maximize the hiding capacity with low distortions respectively. The analysis is done for mapping function, PSNR, image histogram, and parameter of RS analysis. The simulation results highlights that the proposed security measure basically gives better and optimal results in comparison to prior research work conducted using wavelets and genetic algorithm.

Keywords- Steganography, Genetic Algotithm, RS-Analysis, Optimal Pixel Adjustment process, PSNR

1. INTRODUCTION

Steganography is a method of hiding a secret message in any cover media. Cover media can be a text, or an image, an audio or video etc. It is an ancient art of hiding information in ways a message is hidden in an innocent looking cover media so that will not arouse an eavesdropper's suspicion[6]. A covert channel could be defined as a communications channel that transfers some kind of information using a method originally not intended to transfer this kind of information. Observers are unaware that a covert message is being communicated. Only the sender and recipient of the message notice it. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size.

The application of Genetic Algorithm in steganography can increase the capacity or imperceptibility [10-12]. Fard, Akbarzadeh and Varasteh [11] proposed a GA evolutionary process to make secure steganography encoding on the JPEG images. Rongrong et al [12] introduced an optimal block mapping LSB method based on Genetic Algorithm. This paper proposes a method to embed data in Integer Wavelet Transfonn coefficients using a mapping function based on Genetic Algorithm in 8x8 blocks on cover images and, it applies the Optimal Pixel Adjustment Process after embedding the message to maximize the PSNR.

2. IMAGE STEGANOGRAPHY TECHNIQUE

A block diagram of a generic image steganographic system is given in Fig. .

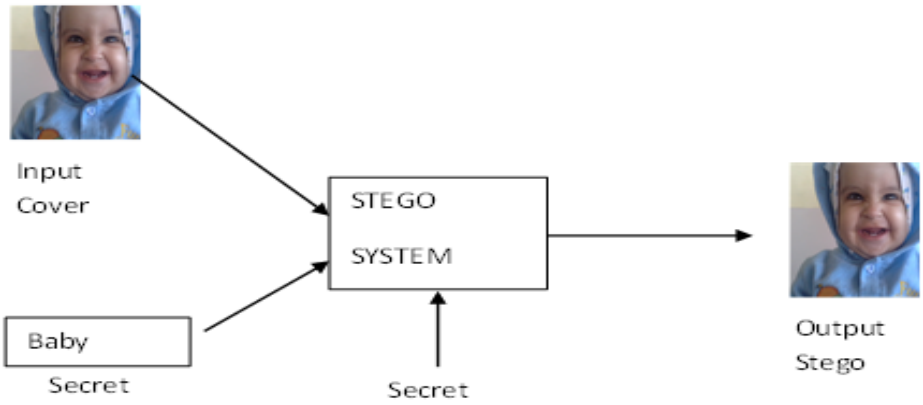


Fig.2.1 Generic form of Image Steganography

A message is embedded in a digital image (cover image) through an embedding algorithm, with the help of a secret key. The resulting stego image is transmitted over a channel to the receiver where it is processed by the extraction algorithm using the same key. During transmission the stego image, it can be monitored by unauthenticated viewers who will only notice the transmission of an image without discovering the existence of the hidden message.

A. Image Steganographic Techniques

The various image steganography techniques are: (i) Substitution technique in Spatial Domain: In this technique only the least significant bits of the cover object is replaced without modifying the complete cover object. It is a simplest method for data hiding but it is very weak in resisting even simple attacks such as compression, transforms, etc. (ii)Transform domain technique: The various transform domains techniques are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Fast Fourier Transform (FFT) are used to hide information in transform coefficients of the cover images that makes much more robust to attacks such as compression, filtering, etc. (iii) Spread spectrum technique: The message is spread over a wide frequency bandwidth than the minimum required bandwidth to send the information. The SNR in every frequency band is small. Hence without destroying the cover image it is very difficult to remove message completely. (iv)Statistical technique: The cover is divided into blocks and the message bits are hidden in each block. The information is encoded by changing various numerical properties of cover image. The cover blocks remain unchanged if message block is zero. (v) Distortion technique: Information is stored by signal distortion. The encoder adds sequence of changes to the cover and the decoder checks for the various differences between the original cover and the distorted cover to recover the secret message.

B. Steganalysis

Steganalysis is the science of detecting hidden information. The main objective of Steganalysis is to break steganography and the detection of stego image is the goal of steganalysis. Almost all steganalysis algorithms rely on the Stenographic algorithms introducing statistical differences between cover and stego image. Steganalysis deals with three important categories: (a) Visual attacks: In these types of attacks with a assistance of a computer or through inspection with a naked eye it reveal the presence of hidden information,

which helps to separate the image into bit planes for further more analysis. (b) Statistical attacks: These types of attacks are more powerful and successful, because they reveal the smallest alterations in an images statistical behaviour. Statistical attacks can be further divided into (i) Passive attack and (ii) Active attack. Passive attacks involves with identifying presence or absence of a covert message or embedding algorithm used etc. Meanwhile active attacks are used to investigate embedded message length or hidden message location or secret key used in embedding. (c) Structural attacks: The format of the data files changes as the data to be hidden is embedded; identifying this characteristic structure changes can help us to find the presence of image. In this work a specific image based steganography method for hiding information in the transform domain of the gray level image has proposed. The proposed approach works by converting the gray level image in transform domain using discrete integer wavelet technique through lifting scheme .In this method instead of directly embedding the secret message into the wavelet coefficients of cover image a mapping technique has been incorporated to generate the stego image. This method is capable of extracting the secret message without the presence of the cover image. This paper has been organized as following sections: Section II describes some related works, Section III deals with proposed method. Algorithms are discussed in Section IV and Experimental results are shown in Section V. Section VI contains the analysis of the results and Section VII draws the conclusion.

3. THE STEGANOGRAPHY METHOD

In the proposed method, the message is embedded on Integer Wavelet Transfonn coefficients based on Genetic Algorithm. Then, OPAP algorithm is applied on the obtained embedded image. This section describes this method, and the embedding and extracting algorithms in detail.

3.1 Haar Discrete Wavelet Transform

Wavelet transform has the capability to present data information in time and frequency simultaneously. This transform passes the time domain data through low pass and high-pass filters to extract low and high frequency information respectively. This process is repeated for several times and each time a section of the signal is drawn out.

DWT analysis divides the discrete signal into two segments (i.e. approximation and detail) by signal decomposition for various frequency bands and scales. DWT utilizes two function sets: scaling and wavelet which associate with low and high pass filters. Such a decomposition manner bisects time separability. In other words, only half of the samples in a signal are sufficient to represent the whole signal, doubling the frequency separability. Haar wavelet operates on data by calculating the sums and differences of adjacent elements. This wavelet operates first on adjacent horizontal elements and then on adjacent vertical elements. One nice feature of Haar wavelet transform is that the transform is equal to its inverse. Figure 3.1 shows image Lena after one Haar wavelet transform. After each transformation, the size of the square that contains the most important information is reduced by 4. For detail information on DWT.

Fig3.1:- The Image Leena after one half wavelet transform

3.2 Integer Wavelet Transform

The proposed algorithm employs the wavelet transform coefficients to embed messages into four subbands of two dimensional wavelet transform. To avoid problems with floating point precision of the wavelet filters, we used Integer Wavelet Transform. The LL subband in the case of IWT appears to be a close copy with smaller scale of the original image while in the case of DWT the resulting LL subband is distorted [9] as shown in "Fig.

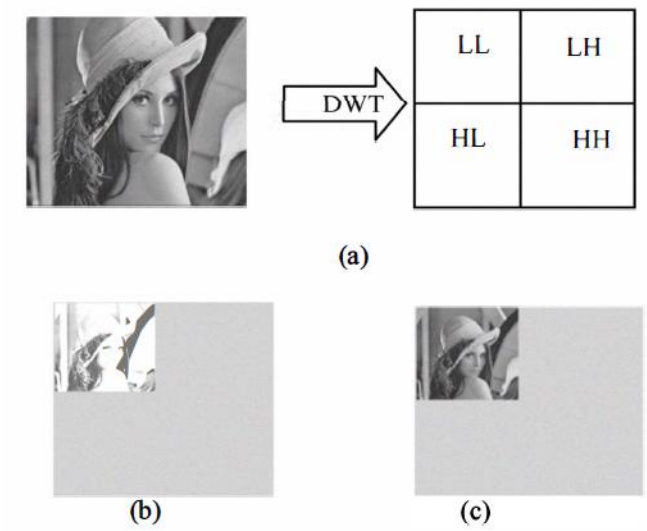


Fig 3.2:- a) Origional image Leena and how to analyis in domain
(b) One level 2DDWT in subband LL
c) One level 2DIWT in subband LL.

3.3 Genetic Algorithm

This paper embeds the message inside the cover with the least distortion therefore we have to use a mapping function to LSBs of the cover image according to the content of the message. We use Genetic Algorithm to fmd a mapping function for all the image blocks. Block based strategy can preserve local image property and reduce the algorithm complexity compared to single pixel substitution.

• Chromosome Design

In our GA method, a chromosome is encoded as an array of 64 genes containing permutations 1 to 64 that point to pixel numbers in each block. Each chromosome produces a mapping function as shown in "Fig. 2".

60	7	24	.....	52	3

Figure. A simple chromosome with 64 genes

• GA Operations

Mating and mutation functions are applied on each chromosome. The mutation process causes the inversion of some bits and produces some new chromosomes, then, we select elitism which means the best chromosome will survive and be passed to the next generation.

• Fitness function

Selecting the fitness function is one of the most important steps in designing a GA-based method. Whereas our GA aims to improve the image quality, Pick Signal to Noise Ratio (PSNR) can be an appropriate evaluation test. Thus the defmition of fitness function will be:

$$PSNR = 10\log_{10}\frac{M\times N\times 255^2}{\sum_{i,j}(y_{i,j}-x_{i,j})^2}$$

Where M and N are the image sizes and, x and y are the image intensity values before and after embedding.

3.4 OPAP algorithm

The main idea of applying OPAP is to minimize the error between the cover and the stego image. For example if the pixel number of the cover is 10000 (decimal number 16) and the message vector for 4 bits is 1111, then the pixel number will change to 11111 (decimal number 31) and the embedding error will be IS, while after applying OPAP algorithm the fifth bit will be changed from 1 to 0, and the embedding error is reduced to 1.

The OPAP algorithm can be described as follows:

Case 1 ($2k-1< \delta_i < 2k$): if pi $\geq$ 2k, then pi " = pi'- 2k otherwise pi" = pi';

Case 2 ($-2k-1 < \delta_i < 2k-1$): pi " = pi';

Case 3 ($-2k < \delta_i < -2k-1$): if pi' < 256 - 2k, then

pi "= pi' + 2k; otherwise pi "= pi';

Pi, pi' and pi" are the corresponding pixel values of the ith pixel in the three images; cover, stego and the obtained image by the simple LSB method, respectively.

3.5 Embedding Algorithm

The following steps explain the embedding process:

- Take the input standard cover image.
- Take the secret text message.
- Apply the secret key (in digits only).
- Perform the Integer Wavelet Transform of the input cover image using lifting scheme.
- Add primal ELS to the lifting scheme.
- Perform integer lifting wavelet transform on image.
- Divide the input cover image in 8*8 blocks.
- Select any of the wavelet coefficients (redundant coefficients) from the obtained high frequency coefficients.
- Generate 64 genes containing the pixels numbers of each 8x8 blocks as mapping function.
- Initialize empty matrix to store the wavelet values.
- Obtain 8 x 8 blocks for R G B.
- Concatenate all coefficients together.
- Store the coefficient in new image.
- Embed in K-LSBs IWT coefficients in each pixel according to mapping function.
- Select any one of the pixels from RGB.
- Now the selected coefficients are processed to make it fit for modification or insertion.
- Fitness evaluation is performed to select the best mapping function.
- The secret message plus the message length is embedded into the processed coefficients.
- This modified coefficient is now merged with the unmodified coefficients.
- Calculate embedded capacity.
- Apply Optimal Pixel Adjustment Process on the image.
- Convert image to binary.
- Finally, the inverse 2D-IWT on each 8x8 block is applied to obtain the Stego image.
- Stego image to be obtained.

3.6 Extraction Algorithm

The extraction algorithm consists of four steps as follows:

- Take the desired stego image.
- Apply the same secret key as given in embedding process.
- Divide the stego image into 8x8 blocks.
- Extract the transform domain coefficient by 2D IWT of each 8x8 blocks.
- Find the pixel sequences.
- Select the desired pixels for process.
- Extract K-LSBs in each pixel.
- Process the selected pixels coefficient to make it fit, for extraction.
- Now extract the message length and the secret message from these processed coefficients.
- Secret message to be obtained.

In the proposed technique, the blocks are labeled before the adjustment. Thus, the computational complexity is minimized.

4. EXPERIMENTAL RESULT ANALYSIS AND DISCUSSION

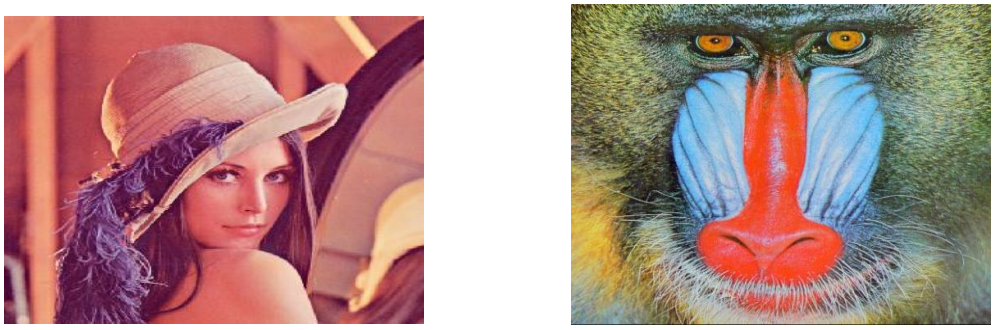
The proposed work is done on 2 set of data image as shown in previous section. Both cover images have utilization of 100% and their respective accomplished results of reversible statistical analysis are as follows.

TABLE 4.1

COMPARISON OF CAPACITY AND PSNR FOR 4-LSBS

Cover Image	Hiding Capacity (bits)	Data Size (KB)	PSNR (dB)
Lena	2137696 (4-LSBs)	260	64.83
Baboon	2137696 (4-LSBs)	260	65.65

Figure 4.1 shows the images after embedding with 4-LSBs. As we compare these embedded images with the input cover images (figure 6.1), we realize that there are no significant changes in images. The embedded images look like the same as cover images. So the attackers cannot realize in between the communication of two parties that secret message is embedded in these images.



(a) Lena image after embedding with 4-LSBs (b) Baboon image after embedding 4-LSBs

Fig.4.1 Images after embedding the secret data

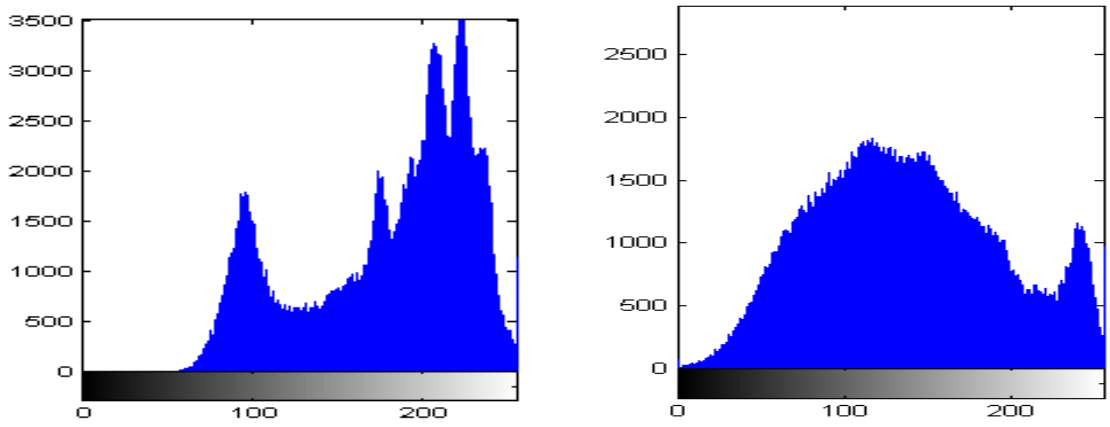
TABLE 4.2

MAXIMUM HIDING CAPACITY AND PSNR OBTAINED FROM PROPOSED METHOD AND ITS COMPARISON WITH THE EXISTING METHODS

Cover Image	Method	Max. H. C. (bits)	PSNR (dB)
Lena	Proposed method	2137696	64.83
	A steganographic method based on IWT and GA [9]	1048576	35.17
	An Adaptive steganography technique	986408	31.8

	based on IWT [5]		
Baboon	Proposed method	2137696	65.65
	A steganography method based on IWT and GA [9]	1048576	36.23
	An Adaptive steganography technique based on IWT [5]	1008593	30.89

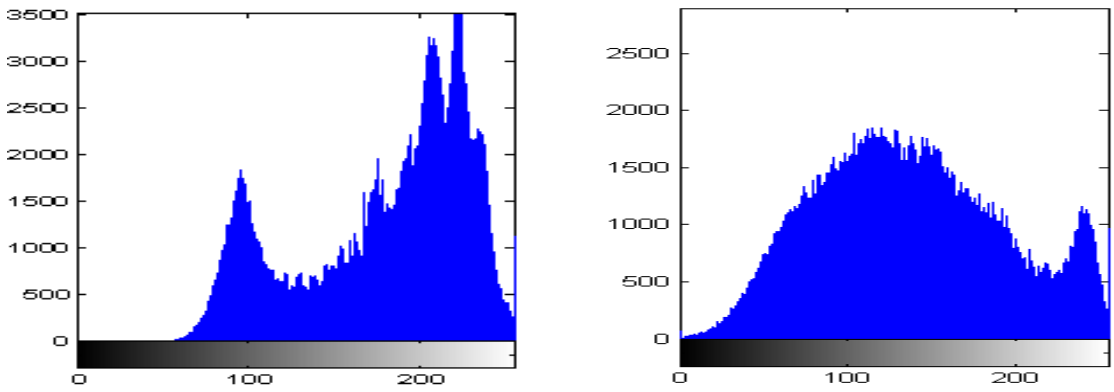
The above Table 6.4 clearly states that the proposed method is much more superior in terms of maximum hiding capacity and in terms of PSNR.



a) Histogram of Lena b) Histogram of Baboon

Fig.4.3. Input cover images histograms

Figure6.3 show the histogram of input cover images. The output stego image histogram after embedding the data is represented in Figure 6.4.



a) Lena Histogram b) Baboon Histogram

Fig.4.4. Output stego images histogram of k=4 after embedding data

REFERENCES

[I] A. Z. Tirket, R.G. Van Schyndel, C. F. Osborne, "A digital watermark," Proceedings ofiCIP, Austin Texas, Vol. II, 1994, pp. 86-90,1994

[2] W. Bender, N. Morimoto, "Techniques for data hiding," IBM Sys. J. 35(3/4) (1996) 313 336.

[3] K. L. Chung, C.H. Shen, L. C. Chang, "A novel SVD and VQ- based image hiding schem," Pattern Recognition Let. 22(9) 1051- 1058 July 2001.

[4] N. Wu and M. Hwang, "Data hiding: current status and key issues," International Journal of Network Security, vol4, No.1, pp. 1-9, Jan. 2007.

[5] W. Chen, "A comparative study of information hiding schemes using amplitude, frequency and phase embedding," PhD thesis, National Cheng Kung University, Taiwan, May 2003

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

[7] N. Provos, P. Honeyman, "Hide and Seek: an introduction to steganography," IEEE Computer Society, pp. 32-44, May-June 2003.

[8] N. Provos, "Defending against statistical steganalysis," In Proc. OfiOth Usenix Security Symp, Usenix Assoc, pp. 323-335,2001.

[9] El Safy, R.O, Zayed. H. H, EI Dessouki. A, "An adaptive steganography technique based on integer wavelet transform," ICNM International Conference on Networking and Media Convergence, pp 111-117,2009.

[10] K. B. Raja, Kiran Kumar. K, Satish Kumar. N, Lashmi. M. S, Preeti. H, Venugopal. K. R. and Lalit. M. Patnaik "Genetic algorithm based steganography using wavelets," International Conference on Information System Security Vol. 4812, pp, 51-63. 2007.

[II] A.M. Fard, M.R Akbarzadeh and A. F Varasteh. "A new genetic algorithm approach for secure JPEG steganography," International Conference on Engineering ofintelligence Systems, pp 1-6,2006.

[12] Ji. Rongrong, Yao. Hongxun, L. Shaohui and W. Liang, "Genetic algorithm based optimal block mapping method for LSB SUbstitution," International Conference on Information Hiding and Multimedia Signal Processing, pp, 215-218, Dec 2006.

[13] A. R. Calderbank, I. Daubechies, W. Sweldens and B. Yeo., "Wavelet transforms that map integers to integers," Applied and Computational Harmonic Analysis, vol. 5, no. 3, pp. 332-369, July 1998.

[14] G M. K. Ramani, E. V. Prasad, S. Varadarajan, "Steganography using BPCS to the integer wavelet transformed image " IJCSNS, Vol. 7, No. 7, pp. 293-302, July 2007.