Integer Wavelet based Secret Data Hiding By Selecting Variable Bit Length

Sumanth Sakkara.
M.Tech
R.N.S. Institute of Technology,
ECE Department,
Bangalore, India

Akkamahadevi D.H.
Professor
ECE Department
Bangalore, India.

K. Somashekar.
Asst. professor
R.N.S. Institute of Technology,
ECE Department,
Bangalore, India.

Raghu k.
AIEMS.
ECE Department,
Bangalore, India.

ABSTRACT
Steganography is a process of hiding secret information's like image, video, audio, and text message in a carrier's like image, video, and audio. Proposed method uses the secret information as a text message which is embedded in a color image. The existing methods hide the information using constant bit length in integer wavelet coefficients. This paper uses variable bit length based on integer wavelet coefficients to hide the data in a particular positions using secret key by LSB substitution method. Hence this algorithm increases the embedding capacity of the text message and obtained stego image is imperceptible for human vision. This technique embeds binary bit stream of secret text message into the 8 bit color image. The embedded confidential information can be extracted from stego image without the knowledge of original image by considering the same secret key. On average of 2.50 bits can be embedded in each wavelet coefficient of the input color image. Hence this method gives better results in both embedding capacity and PSNR than the existing methods.

Keywords
Steganography, Integer Wavelet Transform (IWT), Variable Bit Length, Secret Key, PSNR (Peak-Signal-to-Noise-Ratio).

1. INTRODUCTION
Nowadays communication systems have become digitized conveniently to transmit data over the network. It is essential to maintain the secret information in the areas such as, confidential communication, secret data storing, protection of data alteration, access control system for digital content distribution and Media Database systems.

In the field of information security, several techniques are being developed to overcome unauthorized attacks and to protect the secret information during transmission. Steganography is one such technique [1,2,3], where the secret information is embedded in an appropriate multimedia carrier like image, audio and video files and this carrier is transmitted through the communication network. At the receiver, only the authenticated user can extract the secret information by sharing the secret key.

There are basically three types of steganographic techniques used [4]. They are: Pure Steganography, Secret Key Steganography and Public Key Steganography. Pure Steganography is defined as a steganographic system that does not require the exchange of a stego key. Secret Key Steganography is defined as a steganographic system that requires the exchange of a secret key prior to communication. Public Key Steganography is defined as a steganographic system that uses a public key and a private key to secure the communication between users. In this technique sender will use the public key during the encoding process and the private key is used to decipher the secret message which is mathematically derived from the public key.

Hiding techniques used in steganography are Spatial Domain Techniques and Transform Domain Techniques. Spatial domain technique includes the Least Significant Bit (LSB) substitution [5], Pixel value differencing etc. The transform domain technique includes DCT, DWT and IWT. In DCT [6] based steganographic technique, due to energy compaction all the pixel information is concentrated in just a few coefficient of DCT, whereas the rest of the coefficients are approximated to zero. Hence data hiding capacity and quality of the stego image is not efficient. In DWT [7] based technique, floating point coefficient pose a problem for high data hiding and hence lifting scheme is applied to obtain integer to integer wavelet transform (IWT) [1,2,8].

The hiding technique proposed in this paper uses wavelet transform, in which the cover image is splitted into RGB planes and each plane is divided into 8x8 blocks. The Haar IWT is applied to each block, resulting in integer wavelet coefficient and the data bits are embedded in these integer wavelet coefficients by using secret key. By applying inverse integer wavelet transform, the image is reconstructed back to spatial domain, which is a stego image. The high embedding data capacity and security with good visual quality of stego image is obtained by using variable bit length algorithm.

Hence embedding secret information in digital images widely used in digital word to maintain security. Thus it has an advantage of limited perception of human visual system, and it is very important part of the open systems such as internet to maintain security and privacy.

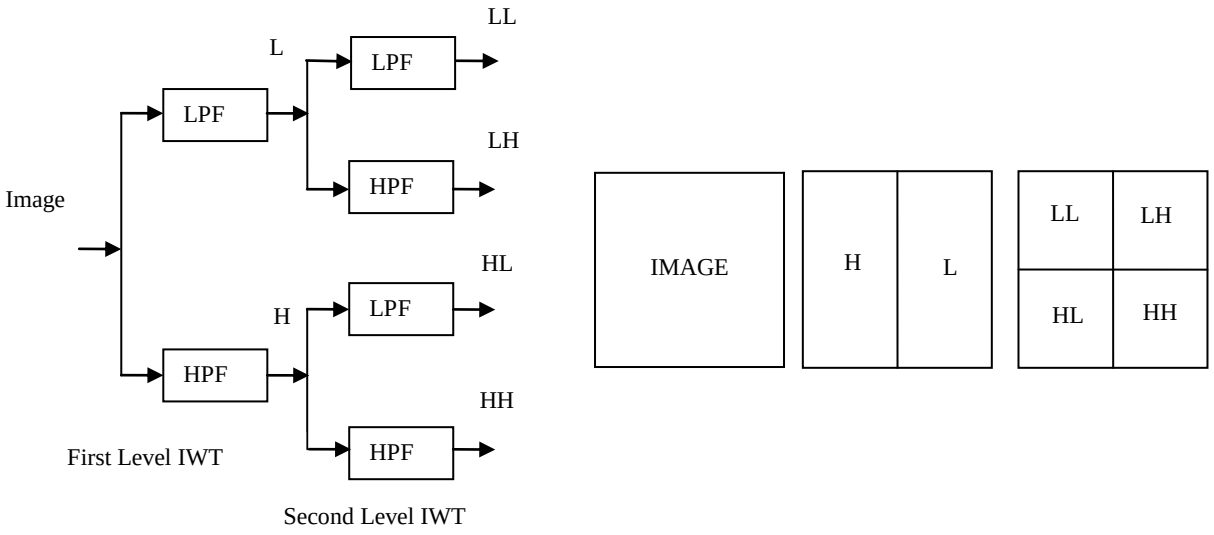

Fig1: IWT Filter Banks

2. INTEGER WAVELET TRANSFORM

In this proposed paper, Haar integer wavelet transform is applied to the cover image for embedding the secret data bits .The first level IWT will result the high(H) and low(L) frequency wavelet coefficients of the cover image. High frequency wavelet coefficients are obtained by taking the edge information between the adjacent pixel values and low frequency wavelet coefficients are obtained by suppressing the edge information in each pixel values [3].

First Level IWT:

$H = C_z - C_e$
$L = C_e - [H/2]$

Where C_o and C_e is the odd column and even column wise pixel values. The H and L bands of the first level IWT is passed through the second level of high pass and low pass filter banks to get the IWT coefficients as shown in the Fig1, which contains LL, LH, HL, HH bands, where LL band contains highly sensitive information of the cover image. The other 3 bands LH, HL and HH contain the detailed information of the cover image.

Second Level IWT:

$LH = L_{odd} - L_{even}$
$LL = L_{even} - [LH / 2]$
$HL = H_{odd} - H_{even}$
$HH = H_{even} - [HL / 2]$

Where, H_{odd} is odd row of H band, L_{odd} is odd row of L band, H_{even} is even row of H band and L_{even} is even row of L band. As IWT is reversible transformation, the image is reconstructed by applying inverse integer wavelet transform to the LL, LH, HL and HH bands.

3. PROPOSED METHOD

Fig 2: refers the proposed steganographic model. It contains two main processing units such as embedding and extracting the secret data. The RGB planes are decomposed into 8x8 blocks and integer wavelet transform is applied to the each block to get the wavelet coefficients. By using the secret key ecret data bits are embedded in the wavelet coefficients.

After embedding, the stego image is obtained by applying the inverse IWT to embedded wavelet coefficients. This stego image is then transmitted through the channel. At the receiver side the secret data bits are extracted from the stego image using the same secret key used at the transmitter side.

3.1 Embedding procedure:

1. The 2D 512x512 input cover image is splitted into RGB planes and the pixel intensity values are adjusted within 15 to 240 ranges to keep the pixel value range in between 0 to 255 after embedding. The modification of histogram can be achieved using equation (1).

$$I_m = \begin{cases} I_c - 2^n, I_c >= 255 - ((2^n) - 1) \\ I_c + 2^n, I_c <= (2^n - 1) \\ I_c, \text{Otherwise} \end{cases} \quad (1)$$

   Where 'n' is the number of bits used to represent the secret message, 'I_c' is the cover image and $I_{m\,is}$ the output image after histogram shifting.

2. Each RGB plane is decomposed into 8x8 blocks.
3. Each 8x8 pixel block is converted into frequency domain by using Haar integer wavelet transform.
4. The number of secret data bits to be embedded in each wavelet coefficient are determined using the Bit Length (BL) calculation algorithm as follows

   If ($wc >= 2^4$)
   BL = 4;
   Else if ($wc < 2^4$ && $wc >= 2^3$)
   BL = 3;
   Else
   BL = 2;

   Where wc is wavelet coefficient, BL is number of bits to be embedded in the respective wavelet coefficient. In this algorithm the bit length value depends upon the wavelet coefficient. Hence high capacity image is obtained by using variable bit length algorithm.

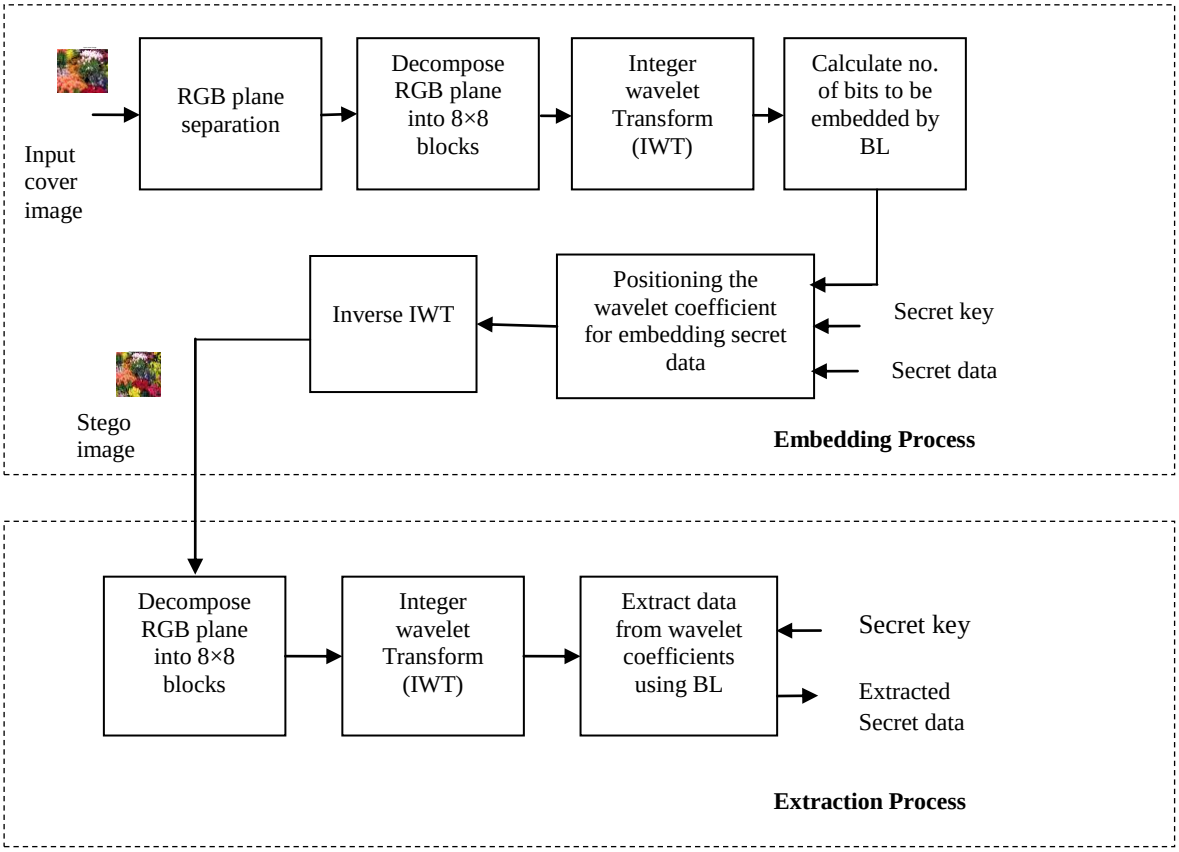

Fig 2: Block diagram of steganographic model

5. The obtained wavelet coefficients from the IWT are selected according to the secret key. This secret key is a 8x8 matrix of zeros and ones in which zeros represents no embedding of secret data bits and ones represents embedding of secret data bits in that particular wavelet coefficient. Here only LH, HL and HH bands are selected for embedding secret data bits.
6. The secret data bits are LSB substituted in each selected wavelet co-efficient by using this mathematical formula in equation (2)

$$wc_e = wc - \text{mod}(wc, 2^{BL}) + M_{BL} \quad (2)$$

Where wc_e is the embedded wavelet coefficient, M_{BL} is the decimal value of secret data bits.

7. This embedded wavelet coefficient is converted into stego image by using inverse IWT.
8. Peak signal to noise ratio (PSNR) and capacity are used to check the performance of the algorithm.

3.2 Extraction procedure:

1. In this step the obtained 2-Dimensional 512x512 stego image is read and it is splitted into RGB planes.
2. Each RGB plane is decomposed into 8x8 blocks.
3. Each 8x8 pixel block is converted into frequency domain by using haar integer wavelet transform as explained in section 2 to get the embedded wavelet coefficient wc_e.
4. By using the same predefined secret key and bit length calculation algorithm used at the transmitter side, the secret data bits are extracted in each selected wavelet coefficient as shown in equation (3).

$$M_{BL} = \text{mod}(wc_e, 2^{BL}) \quad (3)$$

5. The extracted secret data bits are converted into text data.

4. RESULTS AND DISCUSSION:

In this paper, Flowers and Earth 512x512x3 color digital images have been considered as input cover image. Fig 3: shows the resultant stego images for two different input cover images and their respective histograms using key-1 from Table 1. From the Fig 3 stego images the pixel intensity values are adjusted within 15 to 240 range Using the histogram modification algorithm.

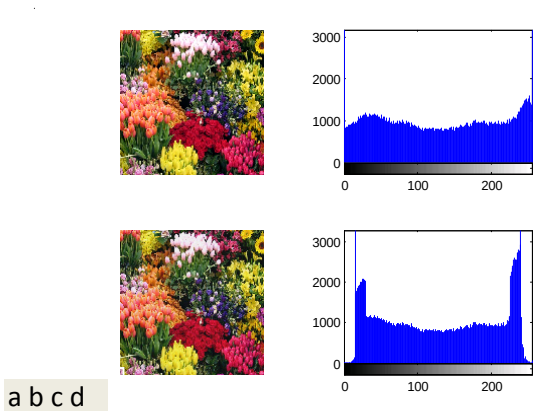

Table 1: Experimental results for various key

Various keys	No. of ones in 8x8 key matrix	Input cover image	Bits per wavelet co-efficient in average	PSNR	Maximum No. of bits to be embedded
Key-1	27	Flowers	2.3739	46.4971	884736
		Earth	2.1598	48.2042	675840
Key-2	32	Flowers	2.3941	46.3245	933888
		Earth	2.1358	48.1599	786432
Key-3	40	Flowers	2.3933	46.2648	1179648
		Earth	2.1258	48.0058	983040
Key-4	42	Flowers	2.4449	45.6877	233472
		Earth	2.1191	47.9487	1032192
Key-5	48	Flowers	2.3909	45.2174	1339392
		Earth	2.1138	47.6216	1179648

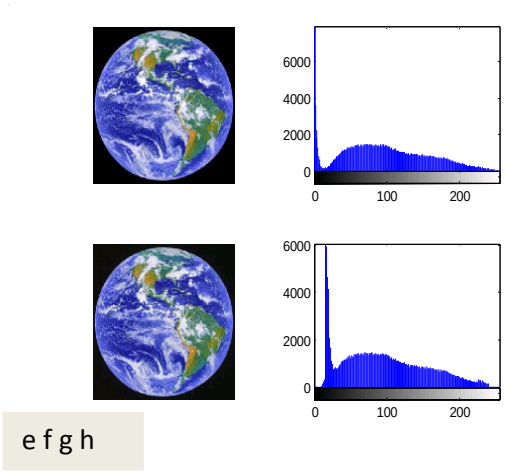

Fig 3: [(a) and (e)] input cover images, [(b) and (f)] histogram of [(a) and (e)], [(c) and (g)] stego images of [(a) and (e)], [(d) and (h)] histogram of [(c) and (g)]

Table 1: represents the PSNR and maximum number of bits to be embedded in two different flower and earth cover images using various secret keys, which depends on the size of the cover image and number of ones present in 8 x 8 key matrix. The PSNR obtained for an earth image is better than that of flower image because the histogram of earth image is not occupying the entire range of pixel intensities. The maximum number of bits to be embedded is more for these cover images when key-5 is used since it contains maximum number of ones.

5. CONCLUSION AND DISCUSSION:

This method introduces a wavelet employed image steganographic model with high embedding capacity based on the Variable-bit length LSB substitution algorithm. In the embedding process, corresponding to the secret key the positions of the wavelet coefficients of cover image is chosen for embedding secret data bits to ensure high security . In an average variable 2-4 bits are embedded in the wavelet coefficient, to maximize the capacity per pixel. Using this proposed method, approximately three message bits are embedded in each pixel while maintaining the imperceptibility. For the security requirement this technique has presented two different ways to deal with the issue. The major benefit of supporting these two ways is that the sender can use different secret keys in different sessions to increase difficultly of steganalysis on these stego images. Using only the secret keys, which is used to determine the position of wavelet co efficient in each 8x8 block of cover image and second a variable bit length to ensure the complexity of the data bits embedded finally the receiver can extract the embedded messages exactly. Experimental results verify that the proposed model is effective and efficient.

The main drawback of this paper is overflow of pixels may occur in integer wavelet domain after embedding. This may probably results bit error while recovering secret information.

Future scope of this paper is to avoid bit error rate by limiting wavelet coefficient range in each subband depending on applications and also to increase the capacity of secret information by selecting different variable bit length for different RGB planes.

6. REFERENCES

[1] Souvik Bhattacharyya et. al, 2010. A Novel Approach to Develop a Secure Image based Steganographic Model using Integer Wavelet Transform. International Conference on Recent Trends in Information, Telecommunication and Computing.

[2] Thanikaiselvan.V et al, 2011. Wave(Let) Decide Choosy Pixel Embedding for Stego. International Conference on Computer, Communication and Electrical Technology ICCCET.

[3] Saeed Sarreshtedari et al, 2010. High Capacity Image Steganography in Wavelet Domain. IEEE CCNC.

[4] Jammi Ashok et.al, 2010. Steganography: an overview International Journal of Engineering Science and Technology,.

[5] Dr. V. Vijayalakshmi et al, 2009. A Modulo Based LSB Steganography Method. International Conference On Control, Automation, Communication And Energy Conservation.

[6] KokSheik Wong et. al, 2006. Graphical Comparative Study on DCT-based Steganographic Methods. IEEE.

[7] Ahmed A. Abdelwahab et. al, 2008. A Discrete Wavelet Transform Based Technique For Image Data Hiding. 25th National Radio Science Conference (NRSC),

[8] Guorong Xuan et. al, 2002. Lossless Data Hiding Based on Integer Wavelet Transform. IEEE.

[9] Fabien A. et. al, 1999. Information Hiding-A Survey. IEEE.

[10] R.Amirtharajan et al. 2010. Tri-Layer Stego for Enhanced Security – A Keyless Random Approach. IEEE.

[11] Mehdi Hussain et al, 2010 "Pixel Intensity Based High Capacity Data Embedding Method", IEEE,.

[12] Bret Dunbar et. Al. 2002. A Detailed look at Steganographic Techniques and their use in an Open Systems Environment", SANS Institute Reading Room.

[13] Beenish Mehboob, 2008. A StegnographyImplementation.IEEE.

[14] Hanan Mahmoud et al, 2010. Novel Algorithmic Countermeasures for Diffirential power analysis attacks on smart cards. Sixth International conference on Information Assurance and Security.

[15] Ahmad Khalil Khan et. al, 2006. An Analytical Framework for Comparative Analysis of Various Watermarking and Steganographic Techniques. IEEE.