ISSN:0975-9646

High Capacity Image Steganography Method Using LZW, IWT and Modified Pixel Indicator Technique

Swati Goel
M.Tech(CSE),CDAC Noida

Pramod Kumar
M.Tech(IT),CDAC Noida

Rekha Saraswat
Sr. Lecturer (SOIT) ,CDAC Noida

Abstract –This paper presents a novel lossless data hiding approach for hiding the text in color image. We use integer wavelet transform (IWT), LZW compression and Modified pixel indicator technique, to achieve high hiding capacity and good visual quality. Firstly Secret message is compressed using LZW compression algorithm and then compressed message is embed into the least significant bit (LSB) of high frequency integer wavelet coefficients using modified pixel indicator technique, if MSB of high frequency coefficients is 1 then embed 3 bit otherwise embed 1 bit and finally apply optimal pixel adjustment procedure (OPAP) after embedding the Secret message. We use the LZW compression for reducing the size of secret message .We utilize the frequency domain to improve the robustness of steganography and finally we implement OPAP to reduce the difference error between the cover and the stego-image.The proposed system shows the high hiding capacity with low distortions.

Keywords-Steganography, pixel indicator technique ,IWT,OPAP,LZW compression.

1. INTRODUCTION:

Steganography is the science and art of sending a secret message in such a way that no one apart from the intended receipents knows the existence of the secret message. Steganography is used to conceal the secret message so that no one can sense the information. The word Steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphic meaning "writing". The steganographic techniques are broadly classified as(i) Spatial domain embedding and (ii) Transform domain embedding. Spatial domain approach embeds messages in the intensity of image pixels directly. Where as in the transform domain the images are transformed into frequency domain and then message are embedded in transformed coefficients. The requirements of steganographic system are Transparency, more capacity and Security and Robustness.

Commonly used methods of embedding payload in cover image are:

(i)*Least Significant Bits (LSB) substitution*: The LSBs of cover image pixel are replaced without Modifying the complete cover object to hide the payload and more data can be hidden in edges. [15]

(ii)*Spread Spectrum Steganography*: The message is spread over wide range of frequencies using pseudorandom noise sequences. [15]

(iii) *Color Palette* is generated Using color quantization and message is hidden with the help of coding structure. Payload is embedded into the color palette as index of pixel positions around centroids.[15]

(iv) *Transform Domain Steganography:* The

Cover image and/or payload are converted into frequency domain and the payload is embedded into the coefficient of cover image to derive stego image. The various transform domain techniques are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Fast Fourier Transform (FFT) and Integer Wavelet Transform (IWT). [15]

The advantages of transform domain techniques over spatial domain techniques are their high ability to tolerate noises and some signal processing operations but on the other hand they are computationally complex and hence slower and have low embedding capacity [1].

The challenge in this work is to find a way to embed a secret message in an image without perceptible degrading the image quality and to provide better resistance against steganalysis process and to increase the capacity.

So to overcome the disadvantages of transform domain we propose an approach, in our approach we first compress the text(secret message) using LZW compression algorithm and compressed message is converted into binary form and stored in an one dimensional array, then we take the cover image and perform color plane separation on true color image and IWT is applied on individual red, green and blue plane, then we hide the data in high frequency coefficients by using modified pixel indicator technique, if the MSB of the pixel value is 1 then embed 3 bit otherwise embed 1 bit. we first embed data in blue plane then in green plane and then in red plane and finally apply OPAP algorithm to minimize the error difference.

I. LZW compression technique:

LZW is a general compression algorithm capable of working on almost any type of data.LZW compression creates a table of strings commonly occurring in the data being compressed, and replaces the actual data with references into the table. The table is formed during compression at the same time at which the data is encoded and during decompression at the same time as the data is decoded.

LZW uses fixed-length code words to represent variable-length strings of symbols/characters that commonly occur together, e.g., words in English text. The LZW encoder and

decoder build up the same dictionary dynamically while receiving the data. LZW places longer and longer repeated entries into a dictionary, and then emits the code for an element, rather than the string itself, if the element has already been placed in the dictionary. [5]

II. INTEGER WAVELET TRANSFORMATION:

Generally wavelet domain allows us to hide data in regions that the human visual system (HVS) is less sensitive to, such as the high resolution detail bands (HL, LH and HH), Hiding data in these regions allow us to increase the robustness while maintaining good visual quality. [1]

Integer wavelet transform maps an integer data set into another integer data set. In discrete wavelet transform, the used wavelet filters have floating point coefficients so that when we hide data in their coefficients any truncations of the floating point values of the pixels that should be integers may cause the loss of the hidden information which may lead to the failure of the data hiding system [12].

To avoid problems of floating point precision of the wavelet filters when the input data is integer as in digital images, the output data will no longer be integer which doesn't allow perfect reconstruction of the input image [13] and in this case there will be no loss of information through forward and inverse transform [12]. Due to the mentioned difference between integer wavelet transform (IWT) and discrete wavelet transform (DWT) the LL sub band 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 sub band is distorted as shown in figure 1. Lifting schemes is one of many techniques that can be used to perform integer wavelet transform it is also the scheme used in paper.[1]

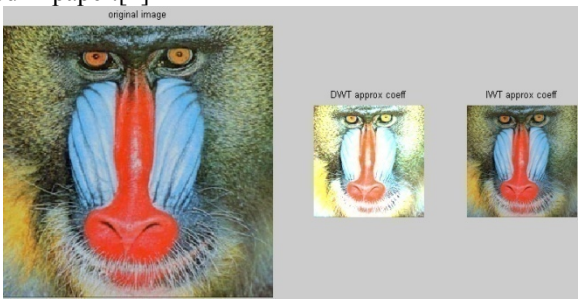


Figure 1: (a) Original image baboon. (b) Subband LL by 2D DWT(c) Subband LL by 2D IWT

If the original image (I) is X pixels high and Y pixels wide, the intensity of each of the pixel at (i,j) is denoted by I(i,j) . Lifting Scheme is one of the techniques on IWT. The decomposing filter in IWT can be calculated as:

$$A_{i,j} = \lfloor (I_{2i,2j} + I_{2i+1,2j})/2 \rfloor$$

$$V_{i,j} = I_{2i+1,2j} - I_{2i,2j}$$

$$H_{i,j} = I_{2i,2j+1} - I_{2i,2j}$$

$$D_{i,j} = I_{2i+1,2j+1} - I_{2i,2j}$$

The inverse transform is obtained by

$$I_{2i,2j+1} = A_{i,j} + \lfloor (H_{i,j}+1)/2 \rfloor$$

$$I_{2i,2j} = A_{i,j} - \lfloor H_{I,J}/2 \rfloor$$

$$I_{2i+1,2j} = I_{2i,2j+1} + V_{i,j} - H_{i,j}$$

$$I_{2i+1,2j+1} = I_{2i+1,2j} + D_{i,j} - V_{i,j}$$

Where, $1 \le i \le X/2$, $1 \le j \le Y/2$ and $\lfloor\ \rfloor$ denotes floor value.[6][13]

III. PIXEL INDICATOR TECHNIQUE:

The pixel indicator technique (PIT) is used for steganography utilizing RGB images as cover media. The technique uses least two significant bits of one of the channels Red, Green or Blue as an indicator of secret data existence in the other two channels. The indicator channel is chosen in sequence from R, G and B, i.e. RGB, RBG, GBR, GRB, BRG and BGR. The indicator relation with the hidden data and the other two channels is shown in Table 1**.**

Table: Indicator values Based action

Indicator Channel	Channel 1	Channel 2
00	No hidden data	No hidden data
01	No hidden data	2bits of hidden data
10	2bits of hidden data	No hidden data
11	2bits of hidden data	2bits of hidden data

They have selected the indicators in sequence, if the first indicator selection is the Red channel in the pixel, the Green is channel 1 and the Blue is the channel 2 i.e. the sequence is RGB. In the second pixel if we select, Green as the indicator, then Red is channel 1 and Blue is channel 2 i.e. the sequence is GRB. [3]

IV. MODIFIED PIXEL INDICATOR TECHNIQUE:

The main drawback of pixel indicator technique is that one of the channels cannot be used to store the actual message, Moreover, algorithm uses fixed number of bits 2 bits per channel to store data, So we use all the three channels for embedding the 3 bit in least significant bits by considering the channel most significant bit, if the MSB is 1 then embed 3 bit of message otherwise embed only 1 bit. Use all the three channels MSB as the indicator. Channel sequence for embedding is blue plane, green plane and red plane.

V. OPTIMAL PIXEL ADJUSTMENT PROCEDURE:

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 coefficients is 1000(decimal number 8) and the message vector for 3 bits is 111, then the pixel

number will change to 1111 (decimal number 15) and the embedding error will be 7, while after applying OPAP algorithm the fourth bit will be changed from 1 to 0, and the embedding error is reduced to 1 [9].

Let *Pi* be the pixel value of the high frequency coefficients of *i*th pixel in the cover image and *P′i* be the corresponding pixel value of the high frequency coefficients of the Stego - image obtained by the above defined substitution method. Then the embedding error between *Pi* and *P′i* can be calculated as $ei = P'i - Pi$.

Assume that k is the size of LSBs to be replaced, and therefore $-2^k < ei < 2^k$. Let $P''i$ be the corresponding stego-pixel value .

The OPAP algorithm can be described as follows:

Case 1: $(2^{k-1} < ei < 2^k)$

If $(P'i \geq 2^k)$

then $P''i = P'i - 2^k$

else $P''i = P'i$.

Case 2: $(-2^{(k-1)} \leq ei \leq 2^{(k-1)})$

$P''i = P'i$.

Case 3: $(-2^k < ei < -2^{(k-1)})$

If $(P'i < 256 - 2^k)$

then $P''i = P'i + 2^k$

else $P''i = P'i$.[9]

2. PROPOSED METHOD:

a. Embedding procedure:

Step1: Firstly**,** apply LZW compression algorithm on the secret text message.

Step 2: Convert the compressed message in binary form.

Step 3: Take the cover image, perform color plane separation on it.

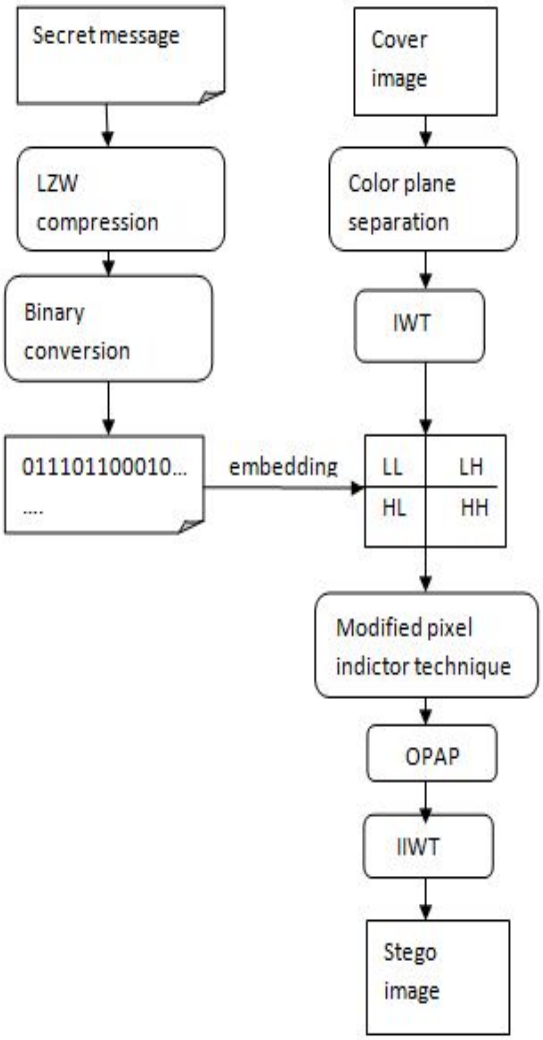
Step 4: Transform the individual plane from spatial domain to frequency domain using integer wavelet transform.

Step 5: Compressed message is embedded in the high integer wavelet coefficients using modified pixel indicator technique.

Step 6: Apply OPAP procedure on the cover image to minimize the error difference or improve the imperceptibility.

Step 7: Inverse integer wavelet transform is applied on the image for converting from frequency coefficients to spatial domain.

Step 8: Now the image is stego image and the image is ready for transporting through the network.



b. Extraction procedure:

Step 1: Take the Stego image, perform color plane separation on it.

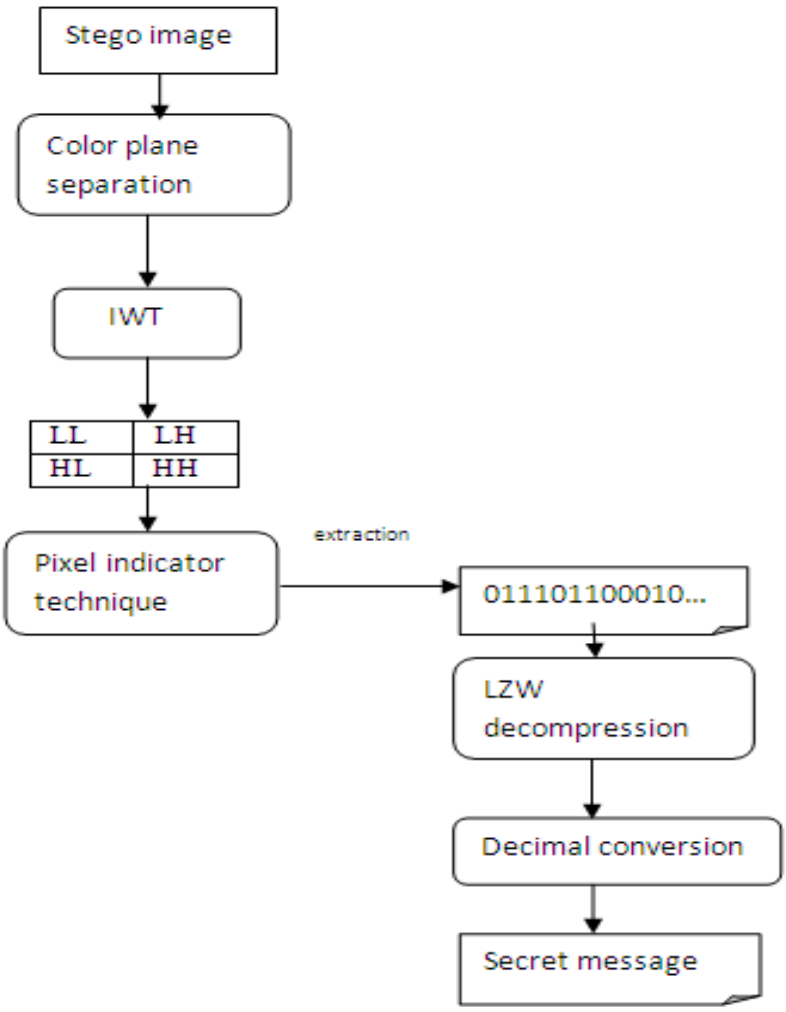
Step 2: Apply the Integer wavelet transformation on the stego image, image is converted from spatial domain to frequency domain coefficients.

Step 3: Extract the secret data from the high frequency coefficients by using the modified pixel indicator technique.

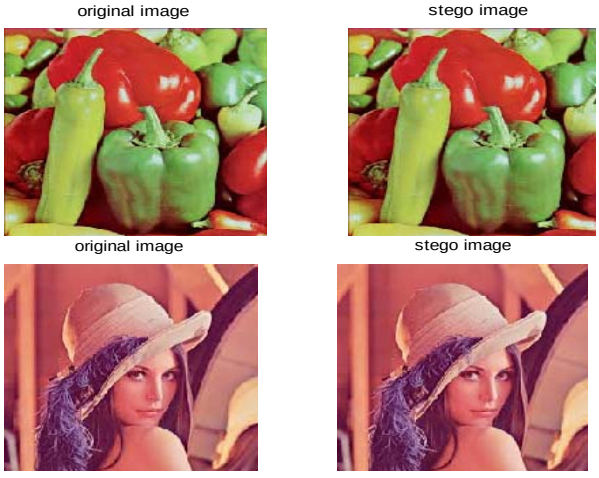
Step 4: Convert the binary data in a decimal format.

Step 5: Apply the LZW decompression algorithm for decoding the plain text.

Step 6: Finally the result from the all above steps is the Secret message.



3. EXPERIMENTAL RESULTS:



4. CONCLUSION:

This approach provide high hiding capacity and better imperceptibility (quality) of the image after embedding the text in an image.

Wavelet transforms that map integers to integers allow perfect reconstruction of the original image that is used to improve robustness.LZW compression is employed so that not only the capacity of payloads will increased indirectly, but also the quality and robustness enhanced.

Modified pixel indicator technique provide the randomness so improved undetectability. We also applied OPAP to improve the imperceptibility of the image. The results are compared with the results of similar techniques and it is found that the proposed technique is simple and gives better PSNR values than others.

REFERENCES:

1. S. Jayasudha," **Integer Wavelet Transform Based Steganographic Method Using Opa Algorithm**" ISSN: 2278-4721, Vol.2, Issue 4 (February 2013), Pp 31-35
2. D.K. Sarmah, N. Bajpai, **"A new horizon in data security by Cryptography & Steganography"**, IJCSIT, pp.212-220, Vol. 1 (4), 2010
3. Adnan Abdul -Aziz Gutub**" Pixel Indicator Technique for RGB Image Steganography"** Vol. 2, No. 1, February 2010
4. Amitava Nag, Sushanta Biswas, Debasree Sarkar & Partha Pratim Sarkar **"A Novel Technique for Image Steganography Based on DWT and Huffman Encoding"** (IJCSS), Volume (4): Issue (6)
5. Haroon Altarawneh**"Data Compression Techniques on Text Files: A Comparison Study"** Volume 26– No.5, July 2011
6. Hemalatha S1, U Dinesh Acharya2, Renuka A3, Priya R. Kamath4**" a secure color image steganography in transform domain"** (IJCIS), Vol.3, No.1, March 2013
7. Mohammad Tanvir, Parvez and Adnan Abdul-Aziz Gutub**" RGB Intensity Based Variable-Bits Image Steganography"** 978-0-7695-3473-2/08 $25.00 © 2008 IEEE DoI 10.1109/APSCC.2008.105
8. Morteza Bashardoost, Ghazali Bin Sulong and Parisa **Gerami " Enhanced LSB Image Steganography Method By Using Knight Tour Algorithm, Vigenere Encryption and LZW Compression"** IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 1, March 2013 ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784
9. Medisetty Nagendra Kumar, S. Srividya**" Genetic Algorithm based Color Image Steganography using Integer Wavelet Transform and Optimal Pixel Adjustment Process"** International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-3, Issue-5, October 2013
10. M. F. Tolba1, M. A. Ghonemy1, I. A. Taha2, and A. S. Khalifa1**" using integer wavelet transforms in colored image"** IJICIS Vol. 4 No. 2, July 2004
11. Yasir Ahmed Hamza **"Securing Image Steganogarphy Based on Visual Cryptography and IWT"** e-ISSN: 2278-0661, p- ISSN: 2278-8727 Volume 12, Issue 6 (Jul. - Aug. 2013), PP 60-65
12. S. Lee, C.D. Yoo and T. Kalker, **"Reversible image watermarking based on integer-to-integer wavelet transform"** IEEE Transactions on Information Forensics and Security, Vol. 2, No.3, Sep. 2007, pp. 321-330.
13. M. Ramani, Dr. E. V. Prasad and Dr. S. Varadarajan**,"Steganography Using BPCS the Integer Wavelet Transformed image",** UCSNS International Journal of Computer Science and Network Security, VOL. 7 No.7, July 2007.
14. P.Thiyagarajan, G.Aghila, V.Prasanna Venkatesan**" Dynamic Pattern Based Image Steganography"** journal of computing ,volume 2, issue 8, August 2010, ISSN 2151-9617
15. H S Manjunatha Reddy**" Wavelet based Non LSB Steganography"** Int. J. Advanced Networking and Applications 1203Volume: 03; Issue: 03; Pages:1203-1209 (2011)