Design of High Secure and Maximum Data Hiding Technique Using Wavelet Transform

1Priyanka Agrawal, 2Prof. Mahendra Rai
SRIT, Jabalpur

Abstract: **Proposed work is a unique DWT based method for steganography. The Covering image is divided into four sub bands using transform technique DWT. Data is been hidden inside HH, HL and LH sub-bands with a new fix mode of data hiding process. Proposed work reduces the detectable distortion in a joint photographic experts group (JPEG) file during data hiding process, by introducing new region selection rule. The new region selection rule considers three factors, i.e., the horizontal difference (HD), vertical difference (VD) and region size (RS). The JPEG image will be split into number of blocks and each pixel in it will be examined to calculate the variations. Depends upon the variation, the amount of secret information will be hide in an image. This proposed method of information hiding will help to solve the security issues in computer networks.**

Keywords: Peak Signal to Noise Ratio (PSNR), Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Bit Error Rate (BER)

I-INTRODUCTION

Today there are various applications to information hiding. Knowledge to data hiding might be used either in ethical or unethical ways. However, data hiding algorithms cannot easily be categorized either in steganography or watermarking[2] categories as there is no transparent boundary between these two terms & mostly classification relies on application to algorithm. Therefore regardless classifying data hiding most common data hiding applications are fingerprinting, secret communication, secure storage, covert communication, & copyright protection.

Literature Work: Kamila s Roy et al [1], A DWT base stenography scheme with image block partition scheme, In this paper they propose a new steganography technique which embeds secret messages in frequency domain.

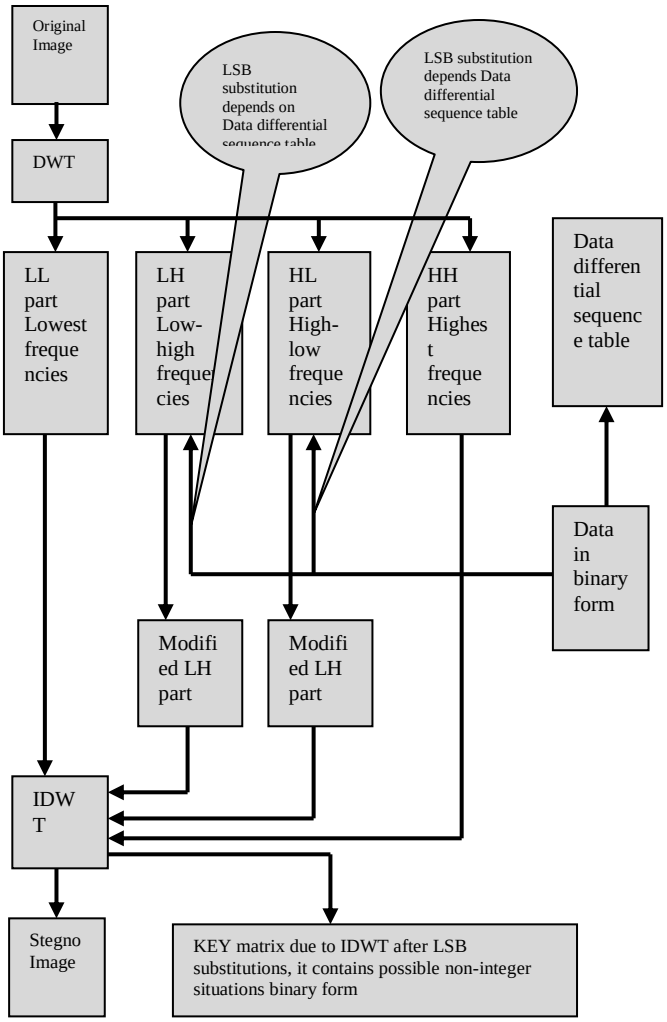

Figure 1 working modal for work by Kamila s Roy et al

Unlike space domain approaches, secret messages are embedded in high frequency coefficients resulted from Discrete Wavelet Transform. Coefficients in low frequency sub-band are preserved unaltered to improve image quality. few basic mathematical operations are performed on secret messages before embedding. These operations & a well-designed mapping Table keep messages away from stealing, destroying from unintended users on internet & hence provide satisfactory security, According to simulation results, PSNR is still a satisfactory value even highest capacity case is applied. This is due to various characteristics for DWT coefficients in various sub-bands. Since most essential portion (the low frequency part) is kept unchanged while secret messages

are embedded in high frequency sub-bands (corresponding to edges portion for original image), better PSNR is not a surprising result. In their future work they also discussed that to reduce extra data in stego-images, hence they have to compress size for 'Key matrix' as far as possible.

Kamila s Roy et al [1], size for key matrix was a extra burden on steganography procedure that they proposed due to this extra data they require to send key with various channel & that key matrix also need to be cipher or otherwise that particular may be find by intruders & if they will get key matrix steganography security will get scarifies.

Proposed work is design which hides key matrix along with stegno image & only a single numeric key need to be know by receiver hence no need to transmit key matrix that will save time & make proposed procedure better than available works.

II-PROPOSED DESIGN TECHNIQUE

In wavelet-based image coding choice to wavelet is crucial & determines coding performance. current compressions techniques involve time taking procedures to find out optimal basis Wavelet families are mainly distinguished into two categories: Orthogonal & Biorthogonal. Orthogonal wavelet families are, Daubechies, Coiflet & Symlet. performance to wavelet based coding depends on wavelet decomposition structure. it has been shown that symlet wavelet family gives better performance with increased compression ratio (CR) & energy retained (ER). work is applied to find out optimum filter order to Symlet wavelet family

The basic concept to DWT is to find out area where data may be hide efficiently, after taking DWT next objective is to IDWT to original image again & then transmit it.

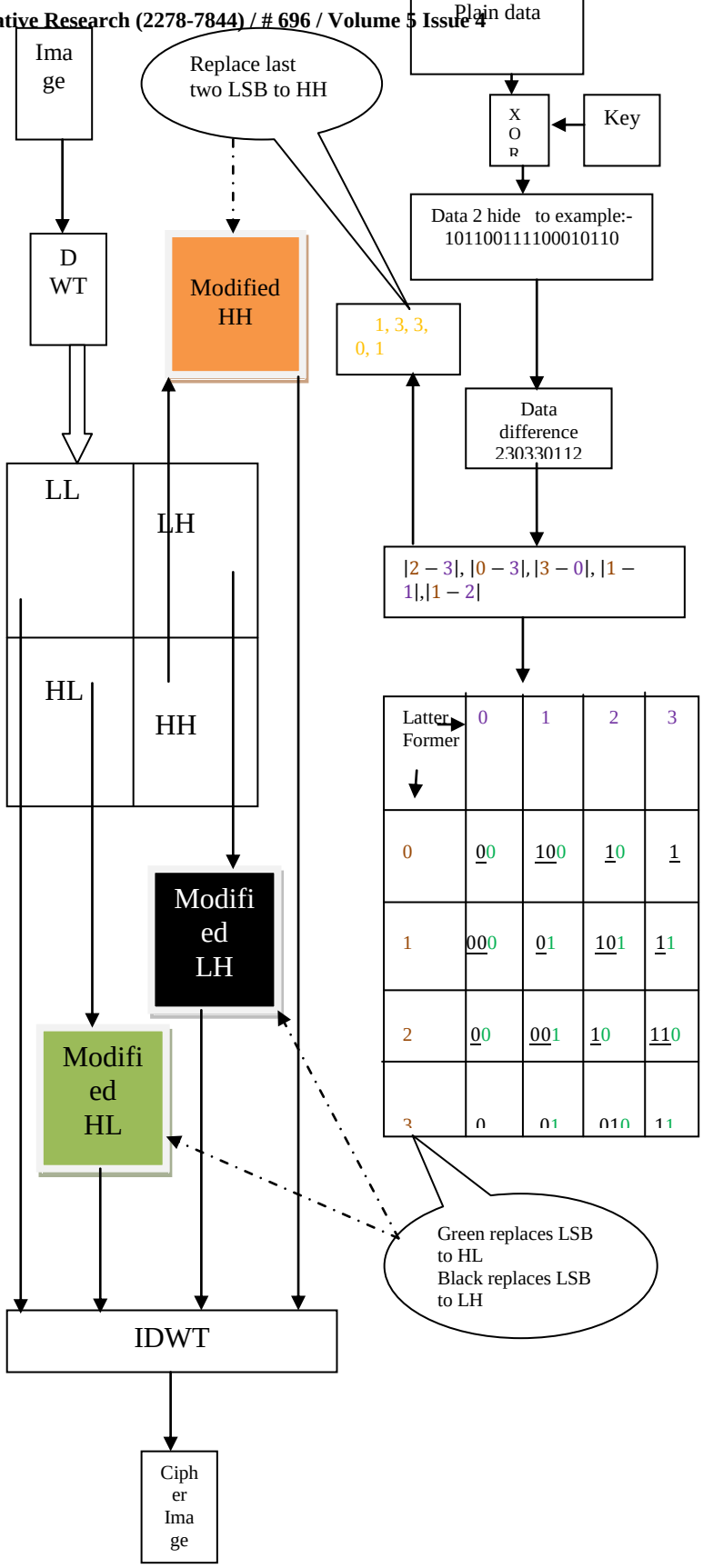

Figure 2: Proposed Encryption -block representation

Figure shown above is flow to proposed work may be describe by following steps:-

Step1: select image in which data to be hidden & then apply DWT on that image to & isolate its frequency components LL,LH, HH & HL.

Step 2: input data which is to be hide inside image & first convert that data into its ASCII standard than convert that into 8 bit binary number.

Step 3: perform logical XOR between binary sequence to original data & Key, hence XORed output gets hide not original & if someone tries to extract data he will get XORed data not original & he will nessesory Key to construct original from XRed data.

Step 4: let binaries to all XORed characters to text which is to hidden arranged in a single row is like
1011001111000010110

Step 5: arrange binary sequence above as in data difference form
230330112

Step 6: compute data difference mod like
$|2-3|, \quad |0-3|, |3-0|, |1-1|, |1-2| = 1, 3, 3, 0, 1$

Step 7: data difference mod two digit binary equivalent replace 2 LSB's to HH

1, 3, 3, 0, 1 = [01, 11, 11, 00, 01]

In above example five pixels to HH will substitute its last 2 LSB's

Step 8: table shown below shows how to replace LSB's to HL & LH. decision make as per data difference like in our example

$|2-3|$ Hence from table LH two LSB replace by '11' & HL one LSB replace by '0'

$|0-3|$ Hence from table LH one LSB replace by '1'

$|3-0|$ Hence from table LH one LSB replace by '0''

$|1-1|$ Hence from table LH one LSB replace by '0' & HL one LSB replace by '1'

$|1-2|$ Hence from table LH two LSB replace by '10' & HL one LSB replace by '1'

Latter → / Former ↓	0	1	2	3
0	00	100	10	1
1	000	01	101	11
2	00	001	10	110
3	0	01	010	11

Step 9: perform IDWT on modified HH, modified HL, Modified LH & unmodified LL.

Step 10: once all replacement made & IDWT in our example total five replacement done & so it is also nessesory to hide length to total replacement so in proposed procedure length is been also hidden along with data inside cipher image.

Figure 3 shows decryption procedure to as may be observed it exact reverse order than encryption procedure & our aim is to extract data not construct original image so we did procedure to have original data only.

In decryption side reconstruction to cover image is not required however 'symlet' DWT required so we may isolate HH,LH,HL & LL part & extract hidden data inside it-

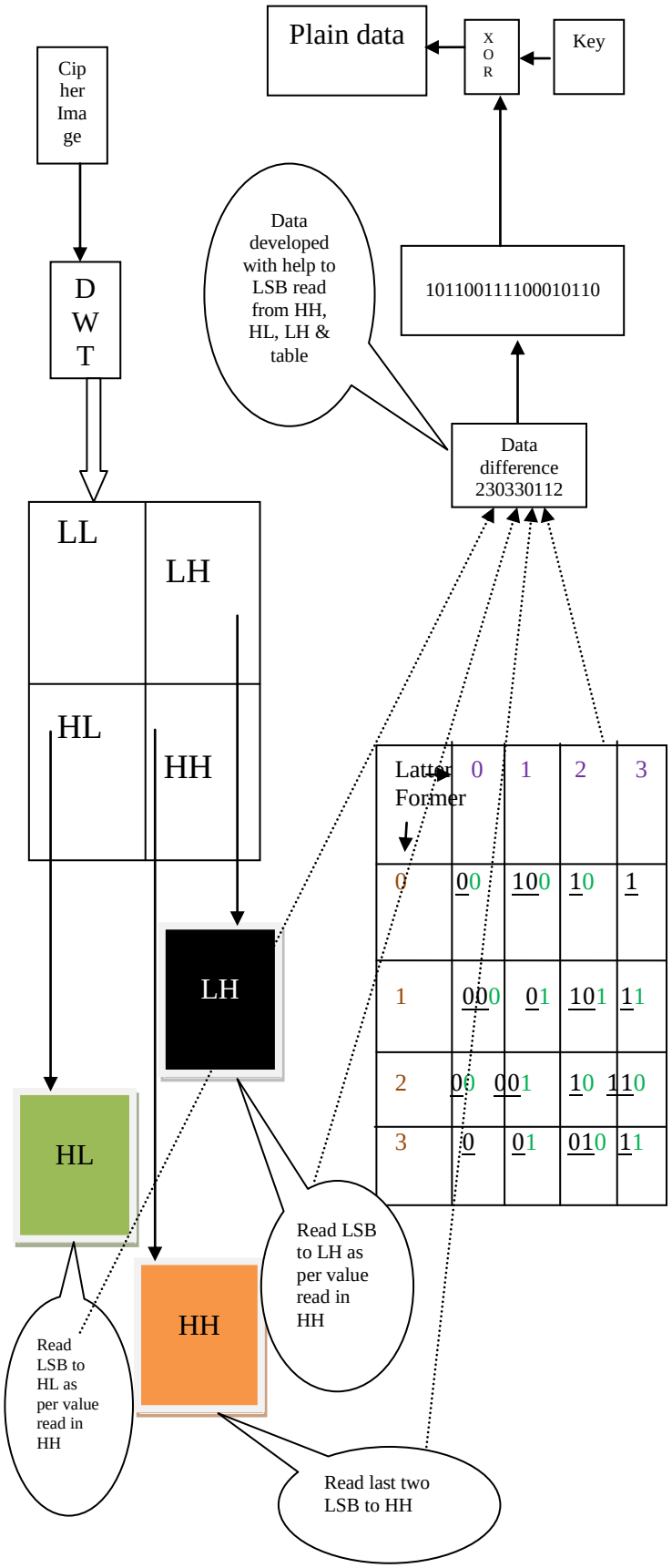

Figure 3 Proposed decryption block representation

Figure shown above is flow to proposed decryption work may be describe by following steps:-

Step1: select image in which data to be hidden & then apply DWT on that image to & isolate its frequency components LL,LH, HH & HL.

Step 2: extract 2 LSB's form he HH
Step 3: As per value to HH read LSB's from LH & HL
Step 4: from table & LSB value read finf out data difference
Step 5: convert data difference into its binary equivalent
Step 6: perform logical XOR with key & find plain data as output binary & convert that into text.

III-SIMULATION RESULTS

The simulation is been performed to various MATLAB standard test image like image to lena, image to boat, Girl, image to Cameraman, image to woman image to peppers & image to baboon. This images are Standard image which is been taken by researchers to work in field to image processing. to genuine compression standard image is been taken to proposed work. Figure 4, 5 & 6 shows simulation results observed to Standard image to Lena.

Figure 4 original MATLAB standard image to 'Lena' & its Gray forma

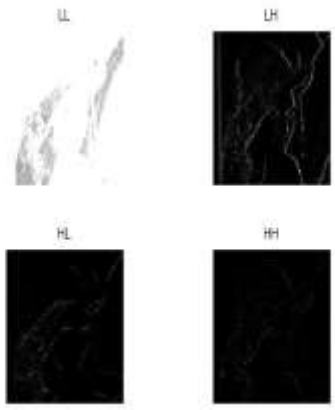

Figure 5 DWT on Cipher Image

Test Image	BER	PSNR	MSE
Lena	1.73E-04	60.9663	3.75E-04
Boat	9.38E-05	58.7387	7.51E-04
Girl	9.88E-05	58.5739	7.90E-04
Camera man	1.26E-04	57.7873	9.88E-05
Woman	1.16E-04	58.0556	9.28E-04
Peppers	2.99E-05	64.4447	1.27E-04
Baboon	1.28E-04	59.837	5.33E-04

Table 2 Results observed to various standard images

Table 2 shows observed results it terms to MSE, BER & PSNR results is been observed to various MATLAB standard image to genuine comparison with others available work & base work.

In Kamila s Roy [1], size for key matrix was a extra burden on steganography procedure that so proposed work is design which hides key matrix along with stegno image, kamila s roy [1] have tested their work to MATLAB standard image like 'lena', 'boat', 'girl', prepares & 'baboon' & obtain PSNR between plain image & stegno image, hence proposed work also did PSNR calculation to all test images that taken by kamila s roy[1].

Test Image	Proposed	Base[1]
Lena	60.9663	50.8021
Boat	58.7387	50.7499
Girl	58.5739	50.7746
Prepares	64.4447	50.7975
Baboon	59.837	50.7647

Table 3 comparative results

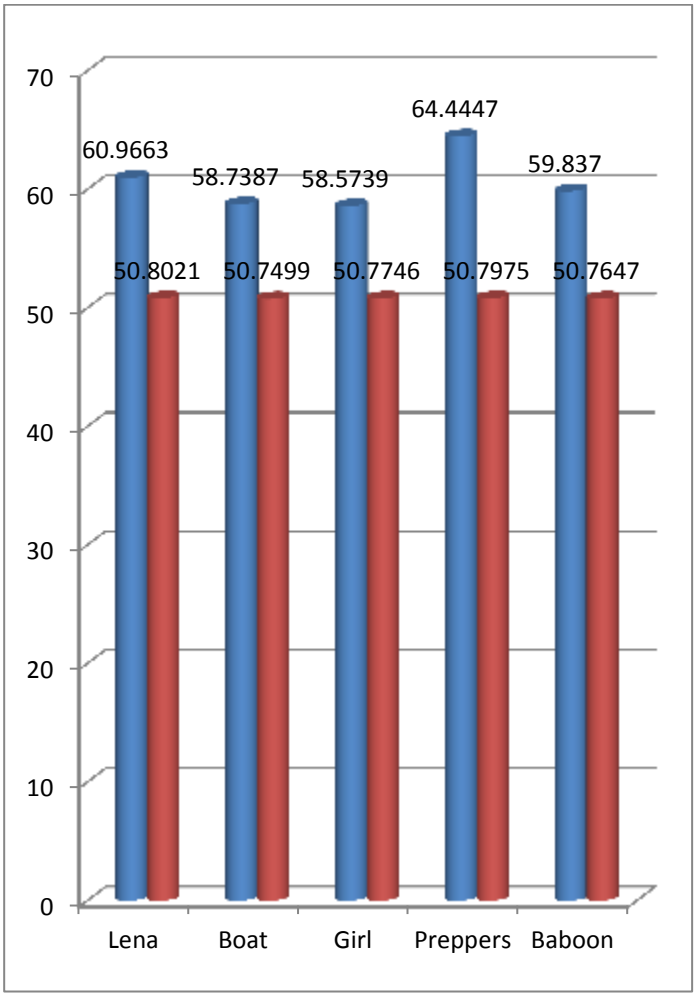

Figure 6 Comparative results observation

Figure 6 & table 3 shows a a comparative results with available work it may be observed that proposed work is better that base work in terms to SNR, BER & MSE.

IV- CONCLUSION

The original objective to thesis work was to develop an optimised technique to hiding image & data inside cover image also to reduce amount to data on channel while stenograph data transmission which is been achieved. Proposed approach hide data efficiently into any covering object (image in our case) & it should do that any intruder cannot interpret it by any means , as from proposed procedure that is been achieved & one may say that our generated stegno image cannot be interpreted easily by any intruder, also total SNR observed to any scenario

where data image & cover image has ration to 1:8 or less is between 58 to 64 to MATLAB standard images , & it is a good results to that ration better than previous work on area.

REFERENCES

[1] Kamila s Roy, S changder , A DWT base stenography scheme with image block partition scheme, Signal Processing & Integrated Networks, IEEE International Conference, pp 471-485 yr-2015

[2] Muhammad Bilal · Sana Imtiaz, Wadood Abdul, Sanaa Ghouzali, Shahzad Asif, Chaos based Zero-steganography algorithm, Multimed Tools Appl (2014) 72: 1073–1092, DOI 10.1007/s11042-013-1415-y, Springer Science+Business Media New York 2013

[3] Sandra Bazebo Matondo, Guoyuan Qi,,Two-Level Image Encryption Algorithm Based on Qi Hyper-Chaos, 2012 Fifth International Workshop on Chaos-fractals Theories & Applications, 978-0-7695-4835-7/12 $26.00 © 2012 IEEE, DOI 10.1109/IWCFTA.2012.47

[4] Belmeguenaï Aïssa, Derouiche Nadir, Redjimi Mohamed , Image Encryption Using Stream Cipher Algorithm with Nonlinear Filtering Function, 978-1-61284-383-4/11/2011 IEEE

[5] Krishna Rao Kakkirala & Srinivasa Rao Chalamala, Block Based Robust Blind Image stegnography Using Discrete Wavelet Transform, TCS Innovation Labs, TATA Consultancy Services, HiTec City, Madhapur, Hyderabad, India, 2014 IEEE 10th International Colloquium on Signal Processing & its Applications (CSPA2014), 7 - 9 Mac. 2014, Kuala Lumpur, Malaysia

[6] Tanmay Bhattacharya , Nilanjan Dey & S. R. Bhadra Chaudhuri, A Novel Session Based Dual Steganographic Technique Using DWT & Spread Spectrum, International Journal to Modern Engineering Research (IJMER), Vol.1, Issue1, pp-157-161 ISSN: 2249-6645

[7] Imran Sarwar Bajwa, A New Perfect Hashing based Approach to Secure Stegnography, 978-1-4577-1539-6/11/2011 IEEE

