ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

TO CONCEAL AND SECURE DIGITAL DATA FOR INTELLECTUAL PROPERTY RIGHT IN MEDICAL IMAGES USING DCT AND DWT IN WATERMARKING TECHNIQUE

Raj Vikram Singh[1] Dr. Subodh Wariya[2] Dr. Javed Ahmad[3] & Balendu Bhushan Pandey[4]
[1]Assistant Professor (ECE deptt.) CEST Lucknow
[2]Professor (EC deptt.) IET Lucknow
[3]Professor (EN deptt.) CEST Lucknow
[4]Assistant Professor (ECE deptt CEST Lucknow

ABSTRACT

There are a lot of possibilities of reproduction and manipulation of digital data for example in digital image, hence a strong digital copyright mechanism must be produced in place. So the security of digital data content from unauthorized users and the problem of copyright management plays very vital role. The Digital watermarking is being used to protect and safe the data of researchers and to keep secret information inside a signal which cannot be easily detected by unauthorized person or users, so digital watermarking is a field of data hiding which hide the crucial information or data in the original data for protecting illegal duplication and to restrict disturbance of multimedia data. in this paper we represent a technique that are used to hide and secure data that is Discrete Cosine Transform and Discrete Wavelet Transform. This method will be used for concealing a mystery picture inside a cover picture utilizing one mystery keys to acquire a stego-picture. The close examination between this procedure and the other existing systems has demonstrated in this paper also.

Keywords: *DWT, DCT, Image Compression, Watermarking, Data Hiding*

I. INTRODUCTION

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The intention of Steganography mainly characterized is: Imperceptibility (or undetectibility), Security, embedding payload, and Robustness (required against common attacks).

In this Paper, we suggest a very simple method to achieve these characteristics in frequency domain based on DCT and DWT. Frequency domain can gives good Imperceptibility as compared to time domain approach. DCT are used for compression of secret message image and this approach of compression is to optimal minimized payload. In next step we use 2-level DWT of cover Image and select Vertical Detail matrix(LH) for data hiding.

Advantage of taking LH matrix is to improve the robustness.

II. PROPOSED METHOD

In spatial domain there are various scheme of data hiding in which most common and easiest method is LSB hiding the 5th bit insertion technique. In LSB hiding scheme, after data hiding if changes in cover image is negligible then distortions coused by the insertion process remain imperceptible. To minimize the changes due to insertion process, the DCT coefficients are divided by the scaling factor. Scaling factor for various images are given in the table 1.

S. No.	Cover Image	Average Value of DCT Coefficient of Secret Image (A)	Average Value of 2L DWT Coefficient of Cover Image (B)	Scaling Factor(A/B)
1	Image 1	24.6815	0.0124	1.9930e+03
2	Image 2	24.6815	0.0005	4.8934e+04
3	Image 3	24.6815	0.0206	1.1969e+03
4	Image 4	24.6815	0.0043	5.7714e+03
5	Image 5	24.6815	0.0025	1.0043e+04
6	Image 6	24.6815	0.0162	1.5221e+03
7	Image 7	24.6815	0.0012	2.0814e+04

The filter used in proposed technique for data compression having following

```
Filter Coefficient = [1 1 1 1 1 1 0 0;
                      1 1 1 1 1 0 0 0;

                      1 1 1 1 0 0 0 0;
                      1 1 1 0 0 0 0 0;
                      1 1 0 0 0 0 0 0;
                      1 0 0 0 0 0 0 0;
                      0 0 0 0 0 0 0 0;
                      0 0 0 0 0 0 0 0];
```

From above filter coefficients, it's clear that only 21 coefficients of 8*8 matrix taken. Rest 43 coefficients are zero.So in hiding algorithm only 21 elements of DCT coefficient will replace DWT of cover image in each 8*8 grid.

III. LITERATURE REVIEW

In LSB hiding method chose gray scale secret image. Each pixel of this image is first computed with XOR and the secret key. That will be again applied at the time of data extraction .In next step compute DWT of cover image and select any two band(i.e. HL/HH or LH/HH or HL/LH). After that break up given secret image pixel in to higher and lower nibble. Select higher and lower four bits of secret information and embed into the lower four bits of wavelet coefficients of one of the band selected. Main detriment of this procedure is low PSNR and data hiding in high frequency DWT coefficient. High frequency coefficient data compression methods affected robustness .

To get higher capacity and security we proposed to replacing mantissa part of cover image to payloads generated mantissa The Lifting Wavelet Transform (LWT) is applied on both payload of sizes and cover image a *a and 3a * 2a respectively. The mantissa values of Vertical band (CV), Horizontal band (CH) and Diagonal band (CD) of cover image are taken out to convert into real values. The approximation band of payload is considered and the odd column element values and even column element values are divided by 300 and 30000 respectively to generate only mantissa part of payload. The new converted odd and even column vector pairs are added element by element to form one resultant vector. The column vector elements of cover image and resultant column vector elements of payload are added to generate stego object. The inverse LWT is applied to generate stego image. PSNR value calculated in this procedure was 58.52dB. [5]

The singular value decomposition (SVD) of m×n real valued matrix A with m _ n, operated orthogonal row and column operations on A in such a way that the resulting matrix is diagonal and diagonal values (singular values) are arranged in decreasing value and coincide with the square root of the Eigen values of ATA [14]. The column of the m×m, U has mutually orthogonal unit vectors, as are the columns of the n×n, V matrix. U and V are orthogonal matrices i.e.[7] In this work, Haar discrete wavelet transform are proposed for new steganographic methods. The binary bits of the secret message are distributed among the coefficients of H, V, D bands and hidden in the integer part of the coefficients by two methods having a high imperceptibility. The key chooses a random selection of the pixels where data is embedded. The Mean Square Error and the Peak Signal to Noise Ratio are calculated to evaluate the quality of the hiding process.[8]

Mohammad Hadi at al proposed method based on Lattice Vector Quantization and Reed-Soloman Encoding. [9] SamanehShafee proposed a method based on compressive sensing(CS) with considering human visual system(HVS) features in data hiding area. HVS visible spectrum is not been able detect small changes in cover image which determines the security factor of image. This property of HVS is used in certain area of spatial domain region of image where secret messages can be embedded without being seen into a cover image. [10]

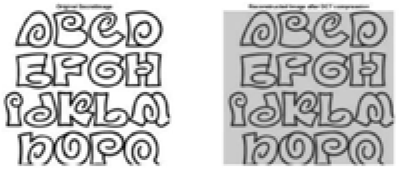

Fig1: Original Data Images & Image reconstructed after compression

Fig2: Original Cover Image Taken

IV. THE PROPOSED ALGORITHM

Data Hiding Steps

1. Take Secret Image as Data(Fig-1)
2. Compress above Data using DCT transform (up to 52dB) (Fig-1)
3. Take mean of DCT coefficients of step 2
4. Select cover image (Fig-2)
5. Calculate 2-level DWT of cover Image and select Vertical Detail matrix for data hiding
6. Take mean of Vertical Detail matrix in above step
7. Take ratio of quantities in step 6 and step 3(Scaling Factor)
8. Take DCT coefficient matrix in step 2 and divide this matrix with the ratio calculated in above step
9. Hide above found matrix directly in Vertical Detail matrix of step 5

Fig3: Stego Image After Data Hiding

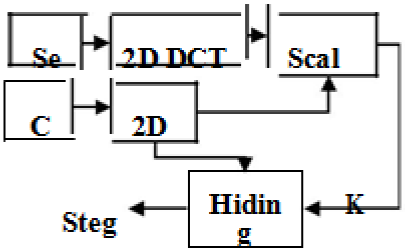

Fig4: Algorithm for Data Hiding

Data Extraction Steps

1. Take stego Image
2. Calculate 2-level DWT of the stego image
3. Extract DCT coefficient from Vertical Detail Matrix
4. Multiply above found coefficient with the ratio found in Data Hiding steps 7 (Scaling Factor)
5. Take IDCT of above extracted image

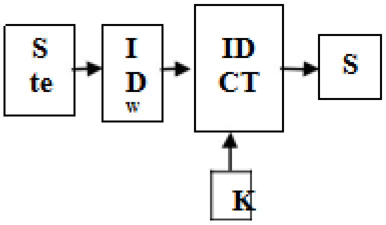

Fig5: Algorithm for Data Extraction

V. NOISE ANALYSIS AND EXPERIMENTAL RESULTS

There are many image quality measuring parameters. Mean Squared Error (MSE) is most important quantitative parameter. The basic definition of MSE is given below in form of equation Mean Square Error (MSE) – MSE is the general estimation parameter method used to check image distortion. It calculates the power of error signal generated in the proposed method. Consider two images, c (a, b) and s (a, b) of A×B dimensions. The formula for mean square error is MSE= $^{1}\sum\sum[(\,,\,)-(\,,\,)]^{2}$

Peak Signal to Noise Ratio - PSNR uses above calculated MSE to evaluate image quality. PSNR and MSE relation is given below. It is calculated as the ratio of original image power against stego image power and is measured in terms of dB. Maximum value of PSNR desirable. It is calculated as PSNR=10log($\sqrt{\ }$ ^{255})There are seven images image selected for this paper and result in given table shown below.

Table1: Experimental Result of Various Cover Images

S. No.	**Cover Image**	**PSNR(dB)**
1	CoverImage1	105.8065
2	CoverImage2	132.8678
3	CoverImage3	140.9324
4	CoverImage4	109.4143
5	CoverImage5	130.4868
6	CoverImage6	104.7068
7	CoverImage7	120.2325

REFERENCES

1. *Sushil Kumar at al,A COMPARATIVE STUDY OF IMAGE STEGANOGRAPHY IN WAVELET DOMAIN, IJCSMC, Vol. 2, Issue. 2, February 2013, pg.91 – 101*
2. *http://www.ee.ic.ac.uk/hp/staff/dmb/courses/DSPDF/00300_Transforms.pdf*
3. *Ajaya Shrestha,"Color Image Steganography Technique Using Daubechies Discrete Wavelet Transform"9th International Conference on Software,Knowledge, Information Management and Applications (SKIMA), 2015*
4. *N Sathisha at al, "Image Steganography Based on Mantissa Replacement using LWT" ,InternationalJournal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 2, February 2015*
5. *Ahmed A. Abdelwahab at al, "A DISCRETEWAVELET TRANSFORM BASED TECHNIQUE FOR IMAGE DATA HIDING"25th NATIONAL RADIO SCIENCE CONFERENCE (NRSC 2008) March 18-20, 2008, Faculty of Engineering, Tanta Univ., Egypt*
6. *AsnaFurqan,"Study and Analysis of Robust*
7. *DWT-SVD Domain Based Digital Image Watermarking Technique UsingMATLAB", 2015 IEEE International Conference on Computational Intelligence & Communication Technology*
8. *Y. Taouil at al, "High Imperceptibility Image Steganography Methods based on HAAR DWT" International Journal of Computer Applications (0975– 8887) Volume 138 – No.10, March 2016*
9. *Mohammad Hadi at al, "A Image Steganography Scheme Based On DWT Using Lattice Vector Quantization and Reed-Soloman Encoding",2015 2nd International Confrence on KBEI, Tehran Iran.*
10. *SamanehShafee, "A Secure Steganography Algorithm UsingCompressive Sensing based on HVS Feature", IEEE 2017 Seventh International Conference on Emerging Security Technologies (EST).*

11. *SofyaneLadghamChikouche, “An Improved Approach for LSB-Based Image Steganography using AES Algorithm”, IEEE 5th International Conference on Electrical Engineering –Boumerdes (ICEE-B) October 29-31, 2017, Boumerdes, Algeria.*