Data Hiding in RGB image Using DCT Compression and DWT

Arun Kumar Singh
PhD Scholar
SNU Ranchi, Jharkhand
Dr. Harsh Vikram Singh
Assistant Professor
KNIT, Sultanpur, UP

Abstract- Secure information transmission over the web is one of the critical parts of the information correspondence as the information is a critical resource for correspondence over the web. Accordingly, information security plays a standout amongst the most noteworthy parts for conveyance and transmission of data over unreliable organize. Information security includes insurance of information from different kinds of assaults like interruption or unapproved access of information which are done over the web. Distinctive procedures like cryptography, steganography, watermarking or fingerprinting are utilized to add security to the information exchanged over the web. While cryptography utilizes encryption of information for the reason of security, information concealing methods are utilized for steganography, watermarking and fingerprinting. Steganography makes utilization of information pressure and also cryptography to give a superior security to the information. It can be utilized for various sorts of information like content, picture, sound or video. Information pressure procedures like DCT and DWT are utilized as various changes for giving a higher security and protection of the data.

Keywords: Data hiding, Steganography, BER, DCT, DWT, PSNR.

1. Introduction

Steganography is a phenomenal and powerful technique for concealing information that has been utilized all through history. The improvement in innovation and systems administration has postured genuine dangers to get secured information correspondence. The word steganography is gotten from the Greek words "stegos" signifying "cover" and "grafia" signifying "composing" characterizing it as "secured written work". In picture steganography the data is shrouded solely in pictures. Cryptography alone isn't adequate for the protected transmission of information over the web. Steganography gives a higher level of security when utilized with cryptography. Steganography employments diverse kinds of techniques to shroud data behind a covering information. The covering information can be a literary information, a picture, a sound or a video. In view of the covering information, steganography can be delegated Text Steganography, Image Steganography, Sound Steganography and Video Steganography. A System/Protocol Steganography is likewise utilized where information is covered up into the conventions like TCP, UDP, IP, and so forth. Steganography is to a great extent utilized as a part of clandestine correspondence to conceal the information from the outsider with the end goal that the data is safely transmitted between the sender and the expected collector. This additionally helps in keeping up the privacy of the information.

2. Related works

Nishant Madhukar proposed three methods based DWT discrete wavelet transform and analyze each of them. These three methods are respectively Haar DWT, Diamond Encoding in DWT and Redundant DWT and QR Factorization The comparison of the all methods were based on various comparison parameters like peak signalto-noise ratio (PSNR), mean square error (MSE), structural similarity index matrix (SSIM), normalized cross correlation (NCC) and the payload size (capacity).. The higest PSNR achived in this method is 73.31. [1]

Mohammad Reza Dastjani Farahani [2] proposed a paper, Discrete Wavelet Transform (DWT) based immaculate secure and high limit picture steganography strategy is exhibited. This technique is utilized for steganography of the pictorial messages in a cover picture (bearer information). To start with, the message information and the cover picture information are changed utilizing Haar channels based DWT, and afterward, the message DWT coefficients are inserted to the cover picture DWT coefficients. In this manner, some DWT based diverse message information installing approaches are considered. The vigor and picture splendor are considered as the principle criteria. Subsequently, the PSNR is considered as a target criteria and the picture shine is considered as a subjective criterion for assessment. The recreations come about affirm that not just the proposed technique is a high limit picture steganography strategy, yet likewise utilizing this strategy, the cover picture information remains unaltered. Besides, if the message information size to be expanded, after the message information extraction, there will be existing high PSNR cover picture information. The PSNR value in this technique achieved was 35.4299.

The proposed technique chips away at the recurrence space to implant mystery bits in the higher recurrence parts of the cover picture by applying 2D-Haar DWT on cover picture. To authorize the security three ways method has been taken after. At initial, a decimal exhibit from the mystery bits is framed. Also, a dynamic square containing qualities from three extraordinary higher recurrence segments is built and ultimately bits are installed in some chose parts of the square. [3]

Steganography is the Art and Science of covering up the data and wonderful cover media. Along these lines, as not to stimulate on Eaviesdropper's doubt. In this paper, mystery picture is stowing away into two unique spaces like as Integer Wavelet Transform and Discrete Wavelet Transform. The cover picture and mystery picture co-proficient qualities are implanted by 512*512 utilizing combination process systems. We connected different blends of Integer Wavelet Transform and Discrete Wavelet Transform on the two pictures and gotten a decent quality stego pictures. The both space gives more secure with mystery key and certain strength of our calculation. This Dual Wavelet Change Used in Color Image Steganography Method model gives high limit and security. This proposed calculation is tried with picture quality parameters and contrasted with different calculations. The exploratory Results demonstrate that double based approach accomplished high limit and high security of our framework and furthermore enhances the execution of steganography framework. The proposed calculation accomplished high Peak Signal to Noise Ratio proportion and other parameter esteems accomplished the ideal arrangement and this strategy contrasted with other mix of change. PSNR value of this method was 48.5597dB. [4]

3. The proposed method

Data Hiding Algorithm

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 RGB cover image (Fig-2)
5. Select one color plane of RGB image and 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

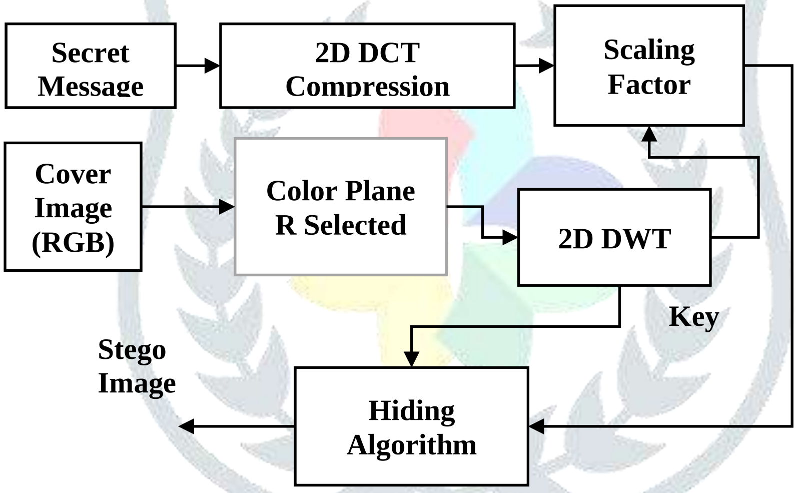

Fig1: Algorithm for Data Hiding

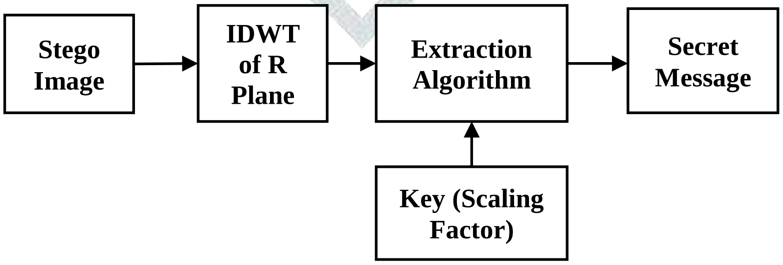

Fig. 2. Algorithm for Data Extraction

Data Extraction Steps

1. Take stego Image
2. Calculate 2-level IDWT of R plane 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 coefficients

Fig3: Original Cover Image Taken for Data Hiding

Fig4: Stego Image After Data Hiding

4. Noise Analysis and Experimental Result

Mean Square Error (MSE) and Peak Signal to Noise Ratio are two parameters for quality measure and their corresponding equations are also given below. [5]

Consider two images, x (a, b) and y (a, b) of M×N dimensions. The formula for mean square error is

$$\text{MSE}=\frac{1}{MN}\sum_a \sum_b [x(a,b)-y(a,b)]^2$$

$$\text{PSNR}=10\log\left(\frac{255}{\sqrt{MSE}}\right)$$

Bit Error Rate (BER)- Bit error rate (BER) can be calculated as the actual number of bit positions which are changed in the stego-image compared with cover image.

There are seven images image selected for this paper and result in given table shown below

S. No.	Cover Image	PSNR(dB) of Cover Image	BER of Cover Image
1	CoverImage1	114.7982	0.0821
2	CoverImage2	132.4954	0.0737
3	CoverImage3	165.5039	0.0726
4	CoverImage4	114.2245	0.0743
5	CoverImage5	145.8755	0.0830
6	CoverImage6	128.2460	0.0834
7	CoverImage7	134.1697	0.0736

Table 1. Experimental Result of Various Cover Images

5. Conclusions

The PSNR and BER calculated in all cases for the comparison. The experimental result showing very good result. For any method to be good based on various parameters the PSNR should be high and BER should be minimum.

We have examined and broke down some as of late proposed methods that make utilization of inborn advantages of DWT along with different calculations and changes. Every one of these systems give great outcomes regarding impalpability and their execution relies upon the payload estimate. Aside from the strategies specified in this paper, we can utilize different changes and calculations in DWT space for expanding the intangibility and limit of picture steganography and influencing it more to secure and hearty. This gives a further extent of research in the DWT area for computerized picture steganography.

References

[1] Nishant Madhukar, “A Comparative Study on Recent Image Steganography Techniques Based on DWT” IEEE WiSPNET 2017 conference.

[2] Mohammad Reza Dastjani Farahani, “A DWT Based Perfect Secure and High Capacity Image Steganography Method”, 2013 International Conference on Parallel and Distributed Computing, Applications and Technologies.

[3] Sabyasachi Kamila, “A DWT based Steganography Scheme with Image Block Partitioning”, 2015 2nd International Conference on Signal Processing and Integrated Networks (SPIN).

[4] Prabakaran G, “Dual Wavelet Transform in Color Image Steganography Method”, 2014 International Conference on Electronics and Communication System (ICECS -2014).

[5] Prajanto Wahyu Adi, “High Quality Image Steganography on Integer Haar Wavelet Transform using Modulus Function”,2015 International Conference on Science in Information Technology (ICSITech).