DCT Based Steganography:

Algorithm to implant secret text message:-
Step 1: Study cover image.
Step 2: Study secret message and transform the message in binary form.
Step 3: The cover image is divide into 8x8 blocks of pixels.
Step 4: Operating from left to right and top to bottom for subtract 128 in each block of pixel.
Step 5: DCT is perform to each block of pixel.
Step 6: Each block is compressed by using quantization table.
Step 7: Compute LSB of each DC coefficient and swap with each bit of secret message.
Step 8: Create stego image.
Step 9: Evaluate the Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) of the stego image.

Algorithm to regain secret text message:-
Step 1: Study stego image.
Step 2: Stego image is divide into 8x8 blocks of pixels.
Step 3: Functioning from left to right, top to bottom subtract 128 in each block of pixels.
Step 4: DCT is perform to each block.
Step 5: Each block is compressed through quantization table.
Step 6: Analyse LSB of each DC coefficient.
Step 7: Get back and translate each 8 bit into character.[5]

4. Evaluation of Image Quality

For differentiate stego image with cover image we need some measures of image quality, usually Peak Signal to Noise Ratio, Mean-Squared Error and Capacity are use to evaluate the quality of an image.

Mean-Square Error: The mean-square error (MSE) between two Image I1(m,n) and I2(m, n) is denote as:

$$MSE = \sum_{M,N} [I1(m,n) - I2(M,N)]^2$$

Here M and N show the number of rows and columns in image matrix of input images, respectively.

Peal Signal to Noise Ratio: PSNR remove this problem by using the MSE according to the range of image:

$$PSNR = 10\log_{10} \frac{256^2}{MSE}$$

PSNR is calculated in decibels (db). PSNR is a fine measure for evaluating restoration results for the same image.

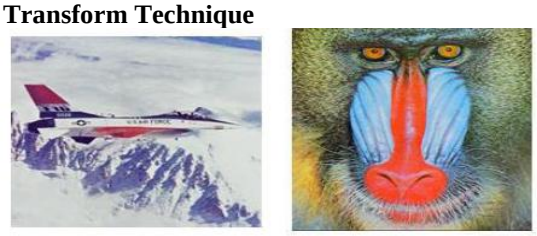
Capacity: Capacity is the size of data in a cover image which can be altered without degrade the quality of the cover image. The embedding operation of Steganography desires to protect the statistical properties of the cover image besides its perceptual quality. Thus capacity of an image lies on total number of bits per pixel and number of bits implanted in each pixel. Unit of capacity is bits per pixel (bpp) and in terms of percentage it calculated as Maximum Hiding Capacity (MHC).

Type of Domain (DOM): DOM can be two types either Transform (T) or Spatial(S). The technique that uses transform domain to hide data in considerable region of the cover images may be more difficult for attackers. [6]

5. Result & Conclusion

Comparative analysis of DWT based & DCT based Steganography has been perform on the basis of parameters like PSNR, MSE, Robustness and Capacity on two images and the results are analyzed. If PSNR ratio is high then quality of images are best. [7]

DCT Transform Technique



(a) Mig (b) Atelidae

Table 1: DCT Transform Technique

COVER IMAGE	PSNR(db)	MSE(db)
MIG	55.6473	.420896
ATELIDAE	58.3766	.30740

DWT Transform Technique

(a) Mig (b) Atelidae

Table 2: DWT Transform Technique

COVER IMAGE	PSNR(db)	MSE(db)
MIG	44.76	1.4741
ATELIDAE	44.96	1.4405

Table 3: Parameters Analysis of Steganography Methods

Features	DCT	DWT
Invisibility	High	High
Payload capacity	Medium	Low
Robustness against image manipulation	Medium	High
PSNR	High	Low
MSE	Low	High

6. Conclusion

Steganography is a technique of writing secret message such a way that no one can doubt for the existence of the message apart from the sender and considered recipient. In this paper, we compare two image Steganography techniques by using DCT & DWT through MSE and PSNR. We have presented background discussion of DCT & DWT, algorithm of Steganography and parameters for evaluation of image quality after embedding the data. From the results, we get the conclusion that PSNR of DCT is higher than DWT techniques. It shows that DCT gives best quality of image. If the embedded message can be retrieved properly from the cover image without being destroyed, then embedding algorithm is called robust. DWT is more robust method for

extracting the message without being destroyed. It gives maximum security.

References

[1] Po-Yueh Chen and Hang-Ju Lin, "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering, 4, 3:275-290, 2006.
[2] Jay Desai, Hemalatha S, Shishira Sr, "Comparison between DCT and DWT Steganography Algorithms", International Journal of Advanced Information Science and Technology (IJAIST), Vol.24, No.24, April, 2014.
[3] Snehal O. Mundhada, V.K. Shandilya, "Spatial and Transformation Domain Techniques for Image Enhancement", International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 1, Issue 2, November 2012.
[4] Navnidhi Chaturvedi, Dr. S. J. Basha, "Comparison of Digital Image Watermarking Methods DWT & DWT-DCT on the Basis of PSNR", International Journal of Innovative Research In Science, Engineering and Technology, Vol. 1, Issue 2, December 2012.
[5] Gurmeet Kaur and Aarti Kochhar, "Transform Domain Analysis of Image Steganography", International Journal for Science and Engineering Technologies with Latest Trends" 6(1): 29-37, 2013.
[6] Vanita T. Anjalin D Souza, Rashmi B. And Sweeta Dsouza, "Review on Steganography Latest Significant Bit Algorithm and Discrete Wavelet Transform Algorithm", International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 5, October 2014.
[7] Stuti Goel, Arun Rana, Manpreet Kaur, "A Review of Comparison Techniques of Image Steganography", IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE), Volume 6, Issue 1, Pp 41-48, May-Jun, 2013.