International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Comparative Analysis of Embedding Data in Image using DCT and DWT Techniques

Mamata J[1], Poornima G[2]

[1]M. Tech-Student (Digital Communication), Department of Electronics and Communication, BMSCE, Bangalore Karanataka-2014, India

[2]Associate Professor, Department of Electronics and Communication, BMSCE, Bangalore Karanataka-2014, India

Abstract: ***Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication. It is the science of embedding information into the cover image viz., text, video, and image (payload) without causing statistically significant modification to the cover image. This paper deals with hiding credit card numbers in an image file (bank logo) using, Discrete Cosine Transform (DCT) based Steganography and Discrete Wavelet Transform (DWT) based Steganography. It is a novel Lossless Secure data embedding algorithm in which the vital information can be embedded into the cover image while preserving the quality of cover image and maintaining the security of the data. The security of the data embedded and cover image quality are two main issues that need to be considered during the process of the data embedding. SDEM-DCT and SDEM-DWT (Scramble Data Embedding in Mid-frequency range of DCT and DWT) Algorithm consists of three major security levels that can be used to hide Credit Card Numbers of customers inside the bank LOGO. The performance and comparison of techniques is evaluated on the basis of the parameters MSE, PSNR, Capacity, Correlation, Processing time and Embedding capacity.***

Keywords: Steganography, Malakooti's Randomize key generator; DCT and DWT coefficients; Matlab; reversible Data hiding; watermarking; SDEM-DCT; M-K scramble descramble.

1. Introduction

The rapid growth of internet usage over high bandwidth and low cost computer hardware has propelled the explosive growth of Steganography. In the present year, secure and hide message in one to one communication is the leading requirement of the people. Therefore Steganography is capturing more attraction by people due to the security issues over internet. Steganography has evolved into a digital strategy of hiding a file in some form of text, cover image, an audio file or even a video file (1). The objective of Steganography is hiding the payload (embedded information) into the cover image such that the existence of payload in the cover image is imperceptible to the human beings (2). There are different techniques to implement Steganography namely least significant bit (LSB), discrete cosine transform (DCT) & discrete wavelet transform (DWT) technique. There are two groups of data embedding applications. The first group is Steganographic applications in which the message will be hidden inside the cover image (i.e. logo) without attracting the attention of third party.

The main goal of Steganography is to protect the message so that eavesdropper cannot detect the presence of message inside cover image. In steganographyic applications there are two methods of embedding: Spatial embedding in which messages are inserted into the LSBs of the image pixels, and Transform embedding in which a message are embedded in the cover image by modifying frequency coefficients. Transform embedding methods are more durable than the spatial embedding methods (3).

The second group of data embedding methods is digital watermarking. The messages will be hidden inside the cover image without attracting the attention of third party. The main aim of watermarking is to protect the message so that eavesdropper cannot remove or replace the message hidden in the cover image. The message gives some additional information about the image, such as author signature, image caption, supplementary data about the image origin, image authentication code, etc. There are, however, some applications for which any distortion introduced to the image is not acceptable. A good example is Bank transactions which need same data in both receiver and sender sides. Most of data embedding techniques, especially high data capacity embedding techniques, in which some amount of distortion into the original image and the distortion was permanent and not reversible. Least Significant Bit (LSB) embedding and quantization schemes are examples of irreversible methods (4).

2. Proposed Work

The model proposed for data embedding handles three security levels. In the first security level the customer credit card number (16 digits) is obtained from a data file and then scrambled with the M-K (Malakootikhederzadeh) randomize key generator Algorithm. In the second security layer the credit card numbers of scrambled will be XOR with the keys generated by Malakooti's Randomize key generator to encrypt the scrambled data and increase the security. In the third security level the cover image (Bank Logo) will be divided into blocks of size 8 x 8 and then the encrypted scrambled data regarding to each credit card will be hidden inside the mid-frequencies of the DCT. Thus one can insure that credit card numbers or any other bank vital information can obtained from a file and then be embedded inside the LOGO using the algorithm without losing much information and providing the security while transferring bank transaction over the internet or over many other communications facilities. The Logo of Bank is used with the size of 256 x 256 as our cover image and then divided the image into three matrices (Red, Green and Blue) of each 8 x 8. Then the image is used to divide by following steps:

- Read the bank logo cover image file and save the information of Red, Green, and Blue layers into three matrices.
- Dividing each matrix into segments of 8 x 8 blocks
- Calculate the DCT of all segments of Red, Green, and Blue matrices
- Read the Original Data, which is the Credit Card numbers of the Bank Customers.
- Read Scramble data from M-K randomize key generator
- Generate the secrete keys using the M-K Key Generator
- Scrambled element is xored with the secret keys by using MK generator to increase the security
- Inserting all the scrambled, encrypted, and weighted credit card number into the selected matrix of DCT i.e. Red, Green, or Blue matrices
- Repeat the step 1-7 to insert all credit card numbers inside the 8 x 8 DCT blocks of Red, Green, and Blue matrices
- Calculate the IDCT of the each blocks Red, Green, and Blue matrices
- Copy the modified, embedded data into 8 x 8 IDCT blocks which contains Red, Green, and Blue matrices to get more detailed information into matrices and then from the Stego Image.

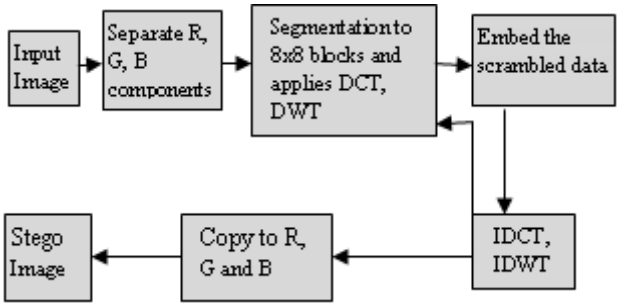

Figure 1: Process of embedding scrambles data

Figure 1 shows the process of embedding data as well Scramble algorithm can solve the problem of distortion exist in the spatial embedding in which the data are embedded inside the DCT of the cover image (fig2). It is also able to embed many credit card numbers inside the cover image with high degree of performance on both data hiding and retrieving. Distortion is less and the retrieved message is the same as the embedded message while the retrieved cover image is almost the same as cover image before the embedding process.

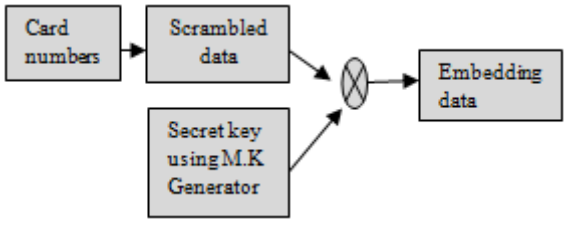

Figure 2: Block diagram for M-K method for data embedding

3. Implementataion

The algorithms used for data embedding in image are described in the implementation part and simulations are carried out in mat lab.

A. Scramble Data and Descramble Data Algorithm

The novelty of using Scramble Data Algorithm is to hide data inside the mid frequency range of DCT matrices. The output array of DCT coefficients contains integers; these can range from -1024 to 1023. In this algorithm received one value and scramble it to a new value based on the proposed scrambling algorithm. This algorithm has the ability to retrieve the original values from the scrambled one. In other words the value should Descramble to its original values. At the first Length Parameter is received which determine the size of original data array that is length of array is 16 data because each Credit card Number have 16 Digits. Assume N=16 in this array each data are between 0 to 9 According to Figure 2.1 and name this matrix as OData. The next step to enhance the Security issue in the below algorithm and do not start scrambling data from the first value but start from the position that is determined by User and Save the content on S parameter which it means Start Point (suppose S=4), so start Scrambling data from the OData (4) =0.

$$\text{Length} = \sqrt{N} \tag{1}$$

$$K = \sum_{I=0}^{\text{Length}-1} \sum_{J=0}^{\text{Length}-1} J + I * 4 \tag{2}$$

$$L = \sum_{I=0}^{\text{Length}-1} \sum_{J=0}^{\text{Length}-1} (S + J * 4 + I) \bmod 16 \tag{3}$$

$$\text{ScData}(K) = \text{OData}(L) \tag{4}$$

Where N=Length of the credit card numbers

The L and K in Equation (1) and (2) are just auxiliary index that can be used to control the scrambling and de-scrambling of 16 Digit Credit cards that would be scrambled and then embeds inside the DCT and DWT coefficient of the cover image.

The process of descrambling is reverse of scrambling data algorithm and the equations used for descrambling algorithm by

$$\text{Length} = \sqrt{N} \tag{5}$$

$$L = \sum_{I=0}^{\text{Length}-1} \sum_{J=0}^{\text{Length}-1} J + 4 * I \tag{6}$$

$$K = \sum_{I=0}^{\text{Length}-1} \sum_{J=0}^{\text{Length}-1} (S + I + J * 4) \bmod 16 \tag{7}$$

$$\text{DeSData}(K) = \text{OData}(L) \tag{8}$$

In the above equations DeSData is a Descramble Data array. After calculation we have DeSdata = OData.

B. M-K randomize Key Generator pseudo code

In the second layer of security robust M-K (Malakooti-khederzadeh) key generator algorithm which can create randomize keys in order to make an Exclusive OR of these keys with the Scramble Data.

Inputs = P, Q, M
Outputs = 16 keys in K array
Step 1) suppose P, Q and M are three prime numbers:
P=11, Q=13 and M=3
Step 2) A=P*Q, i=1
Step 3) K_i=A mod 10
3.1) P'=(K_i+1)*M
3.2) Q'=int (P/Q)+i
3.3) A=P' * Q', i=i+1
3.4) if i<=16 then go to step 3
Step 4) end

Where the inter P and Q and M just are three prime numbers and we have selected as prime to make the generated key more likely random.

C. Algorithm for data embedding and retrieving using DCT Based Steganography:

Step 1: Read the cover image of size 256 x 256.
Step 2: Read the credit card numbers and converting those message into binary.
Step 3: The cover image of size 256 x 256 is divided by the bitmap color matrices into 8×8 block for Red, Green and Blue matrices as shown in fig 1.

$$\text{sub\_r} = \sum_{rw=1}^{Dim/64} \sum_{cl=1}^{Dim/64} R(8rw - 7 : 8cl - 7 : 8cl) \qquad (9)$$

Step 4: DCT is applied to each block of image pixels. DCT separates the image into parts of differing importance. It transforms an image from the spatial domain to the frequency domain. DCT of an image is separated into high, mid and low frequency components.

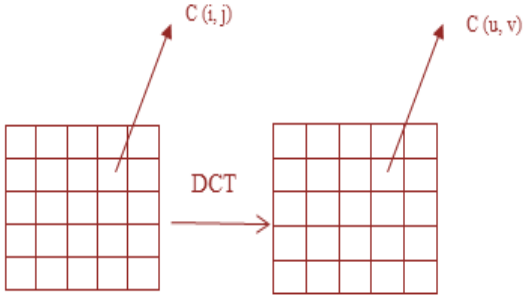

Figure 3: DCT of an image

Here, the input image is of size N x M. C (i, j) is the intensity of the pixel in row I and column j; C (u,v) is the DCT coefficient in row u and row v of the DCT matrix.

Step 5: Each 8x8 block is compressed through quantization table.

$$DCT_{sub_r} = T \times sub_r \times T' \qquad (10)$$

Calculate T by the following equation:

$$T_{ij} = \begin{cases} \frac{1}{\sqrt{N}} \text{ if } i = 0 \\ \sqrt{\frac{2}{N}} \cos\left[\frac{(2_i + 1)}{2} \frac{i\pi}{N}\right] \text{ if } i > 0 \end{cases} \qquad (11)$$

In the above algorithm N=8, i and j are started from 1 to 8. The columns of T from an orthogonal set, is called an orthogonal matrix.

Step 6: Read the credit card numbers and store them into OData(L) array based on scrambling equations we calculate ScData (K).
Step 7: execute the key generation algorithm and produce 16 random keys. Then create encrypted by the following equation

$$E(i) = ScData(i) \otimes K(i) \qquad (12)$$

Step 8: Write the stego image after that read the stego image, extracting keys K(i) again step 3, 4, and 6 is performed.
Step 9: Copy the 16 digits that are in mid frequency and create our original data, here we use descrambling algorithms and save the values int DeSData array.
Step 10: Apply IDCT on the 8×8 block and copy this block into original matrix image.
Step 11: Calculate the Peak signal to noise ratio (PSNR) and MSE, Processing time, Correlation, Capacity and Embedding capacity of the stego image.

D. Algorithm for data embedding and retrieving using DWT Based Steganography:
Step 1: Read the cover image of size 256x256 and credit card numbers which is to be hidden in the cover image.
Step 2: Convert the credit card numbers into binary and apply 2D-Haar transform on the cover image.
Step 3: Obtain the horizontal and vertical filtering coefficients of the cover image. Cover image which includes data information is added for DWT coefficients.
It decompose an image in basically three spatial directions i.e., horizontal, vertical and diagonal in some of results separating the image into four different components namely LL, LH, HL and HH.

- LL level is the lowest resolution level which consists of the approximation part of the cover image,
- Rest three levels i.e., LH, HL, HH give the detailed information of the cover image.

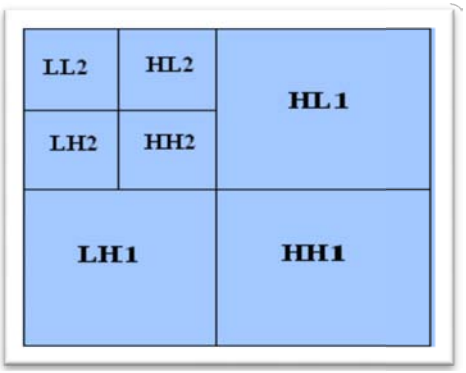

Fig4: DWT of an image

Step 4: Obtaining stego image after that read the stego image again step 2 and 3 is performed.
Step 3: Convert the data into message vector. Compare it with original message.
Step 5: Calculate the Peak signal to noise ratio (PSNR) and MSE, Processing time, Correlation, Capacity and Embedding capacity of the stego image.

4. Evaluation of Image Quality

For comparing stego image with cover results requires a measure of image quality, commonly used measures are Mean-Squared Error, Peak Signal-to-Noise Ratio and capacity.

D. Mean-Squared Error:
The mean-squared error (MSE) between two images I1(m, n) and I2(m, n) is:

$$\mathrm{MSE} = \frac{\sum_{m,n}[I_1(m,n) - I_2(m,n)]^2}{M * N} \qquad (13)$$

Where, MSE is mean square error,
M x N is the dimension of the images,
$I_1(m,n)$ is the original image,
$I_2(m,n)$ is the watermarked image.

E. Peak Signal-to-Noise Ratio:
Peak Signal-to-Noise Ratio (PSNR) avoids the problem by scaling the MSE according to the image range:

$$\mathrm{PSNR} = 10\log_{10}\left[\frac{R^2}{\mathrm{MSE}}\right] \qquad (14)$$

PSNR is measured in decibels (dB). PSNR is a good measure for comparing restoration result for the same image. Where R=255.

F. Correlation Coefficient:
Correlation coefficient is given by

$$C_r = \frac{\sum_m \sum_n (X_i - X')(Y_i - Y')}{\sqrt{(\sum_m \sum_n (X_i - X')^2)}\sqrt{(\sum_m \sum_n (Y_i - Y')^2)}} \qquad (15)$$

X' is the average value of the original image and
Y' is the average value of the modified image
The closeness between the original image and the modified one is measured by the correlation coefficient.

G. Processing time:
It is the time required to embed and encrypt the credit card numbers using DCT and DWT techniques into the cover image.

H. Capacity:
It is the size of the data in a cover image after applying DCT and DWT to 8× 8 blocks of image. The resulting matrices consist of non zero DCT coefficients which are less in number compare to the number of pixels in the image.

5. Result & Conclusion

Following examples have been performed based on the SDEM-DCT/DWT algorithm to prove the performance parameter between DCT and DWT. The security level, quality of original image and credit card numbers are three factors that should be taken care in embedding and retrieving process. Several images have been tested and the retrieve images have been displayed algorithms were developed using Mat lab programming language. Following images are the original image (logo images) which we need to embed the data inside the original image i.e cover images.

Figure 5.1: (a): Mellant Bank Fig5.1(b):American Bank

Figure 5.1: (c): Sederat Bank

Taking each bank logo image as shown in the above figures and converting those images into gray scale image.

Figure 5.1:(d,e):Selected cover image, Gray scale image

The above fig 5.1 (d) shows the selected cover image is a bank logo which is the selected image from the data file and that cover image is divided into three components RGB. This means that every color is represented as a combination of Red, Green and Blue. Then the (RGB) converts the true color image RGB to the grayscale intensity image by eliminating the hue and saturation information while retaining the luminance converted into gray scale image as shown in the fig 5.1(e).

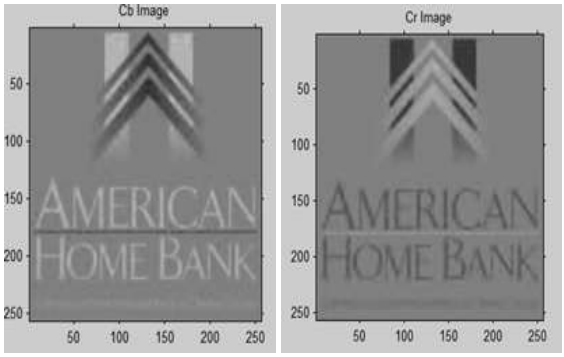

Figure 5.1: (f, g): Chrominance Cb and Cr image

The selected image is converted into the chrominance blue and red images as shown in the above figures 5.1 (f), 5.1 (g). The JPEG image compression technique is actually used in a number of different formats. YCbCr map converts the YCbCr values in the color map ycbcr map to the RGB color space. If ycbcr map is M-by-3 and contains the YCbCr luminance (Y) and chrominance (Cb and Cr) color values as columns, rgb map is returned as an M-by-3 matrix that contains the red, green, and blue values equivalent to those colors and gray scale image is selected to embed the credit card numbers.

Figure 5.2 & 5.3: DCT and DWT Watermarked image

Taking gray scale image as an input image and hiding a key encryption data in gray image by applying DCT and DWT. But here after embedding data the cover image and the watermarked DWT and DCT image is similar.

The below table shows the different values of PSNR, MSE, Correlation, Processing time, Capacity. Peak signal to noise ratio is more in case of the DWT technique for different images. Consider lesser the value of PSNR more will be the degradation in the quality of the original image. The values of the PSNR give the quality of the watermarked image and are good in case of DWT compared to DCT. Processing time in seconds is more in case of DCT as the time required to embed and encrypt (using DCT and DWT) the credit card numbers into the cover image.

Table 1: Comparison of DCT and DWT methods for various images (size256×256, M=8×8).

Image	American Bank		Mellant Bank		Sederat Bank	
Transform Type	DCT	DWT	DCT	DWT	DCT	DWT
PSNR(db)	38.12	40.39	38.44	45.20	38.52	46.79
MSE	9.80	5.93	9.30	1.96	9.14	1.35
Processing time(sec)	4.37	2.65	2.86	2.29	2.15	1.99
Correlation	0.99	0.99	1.00	0.99	1.00	0.99
Capacity	900	16384	900	16384	900	16384

Table 2: Comparison of DCT and DWT methods for various images (size512×512, M=8×8).

Image	American Bank		Mellant Bank		Sederat Bank	
Transform Type	DCT	DWT	DCT	DWT	DCT	DWT
PSNR(db)	38.56	40.13	38.57	46.51	38.53	53.58
MSE	9.047	2.50	9.01	1.44	9.10	0.284
Processing time(sec)	4.055	2.50	3.48	2.73	3.57	2.210
Correlation	1.000	0.99	1.00	0.99	1.00	1.00
Capacity	3844	65536	3844	65536	3844	65536

Table 3: Comparison of DCT and DWT methods for various images (size1024×1024 , $M = 8 \times 8$)

Image	American Bank		Mellant Bank		Sederat Bank	
Transform type	DCT	DWT	DCT	DWT	DCT	DWT
PSNR(db)	38.58	49.34	38.58	52.61	38.56	55.56
MSE	9.00	0.75	9.00	0.356	9.04	0.18
Processing time(sec)	9.00	2.73	8.83	2.404	8.951	3.65
Correlation	1.00	0.99	1.00	1.00	1.00	1.00
Capacity	15876	26214	15876	26214	15876	26214

The scheme has been evaluated on the different set of images. The watermarking method increases the robustness and also ensures the quality of the image. From the above tables shows of different image sizes and blocks it is observed that DWT is more robust then DCT by comparing PSNR. DWT performs better in comparison to DCT. PSNR for the Sederat bank image consider is to 55.56db for varying from 46.79 for 8×8 block, keeping the mse as low 0.180.

Capacity is calculated after applying DCT to 8×8 blocks of image. The resulting matrices consists of non zero DCT coefficients which are less in number compare to the number of pixels in the image. This compressed form of the image representation gives the capacity of the image i.e. Capacity is the multiplication of rows and columns of obtained DCT and DWT watermarked image.

Embedding Capacity: To calculate the embedding capacity of the cover image based on the size of cover image as well as the levels of DCT and DWT applied on this image. The embedding capacity helps the user to calculate the appropriate number of DCT and DWT levels applied on the cover image as well as obtaining the optimum size of the each sub blocks that prevent the image distortion. Image distortion depends on several factors DCT and DWT levels and number of DCT and DWT coefficients that it is used on each embedding process. Let DL be the DCT and DWT levels .To maintain the quality of transferable image we used just one level of DCT and two level of DWT for the above proposed algorithm (DL=1, DL=2) and checked the PSNR values for the embedding process of several Credit Card digits, i.e. ND=16, 8, 4 digits. It is assumed that cover image has a size of N x N and it has been divided into M x M blocks. Thus, the Embedding Capacity (EC), Total Digits that can be embedded into cover image, can be obtaining from the above Equation 10 as following:

$$EC=3\times DL \times \left(\frac{N}{M}\right)^2 \times ND \qquad (16)$$

Here one DCT level, DL=1, size of image
N=512 x 512, block size M =8 x 8, and ND = {16, 8, 4}. Thus
ND=16, EC=196608 Digits or 12288 Credit Card Number

ND= 8, EC= 98304 Digits or 6144 Credit Card Number
ND= 4, EC= 49152 Digits or 3072 Credit Card Number
Here one DWT level, DL=2, size of image
N=512 x 512, block size M =8 x 8, and ND = {16, 8, 4}. Thus
ND=16, EC= 393216 Digits or 24576 Credit Card Number
ND= 8, EC= 196608 Digits or 12288 Credit Card Number
ND= 4, EC= 98304 Digits or 6144 Credit Card Number

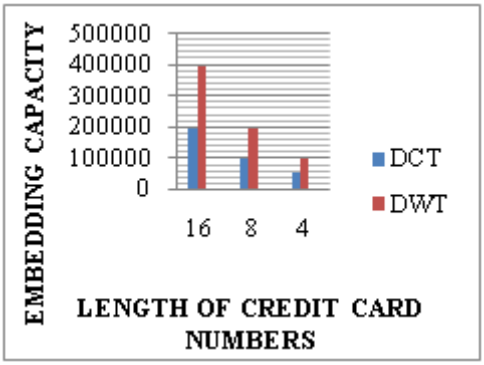

Figure 5.4: Graph of Embedding Capacity using 8 x 8 blocks and size 512 x 512

Size of image N=256 x 256, block size M =8 x 8, and ND = {16, 8, 4}. Thus
ND=16, EC=49152 Digits or 3072 Credit Card Number
ND= 8, EC= 24576 Digits or 1536 Credit Card Number
ND= 4, EC= 12288 Digits or 768 Credit Card Number
Here one DWT level, DL=2, size of image
N=256 x 256, block size M =8 x 8, and ND = {16, 8, 4}. Thus
ND=16, EC= 98304 Digits or 6144 Credit Card Number
ND= 8, EC= 49152 Digits or 3072 Credit Card Number
ND= 4, EC= 24576 Digits or 1536 Credit Card Number

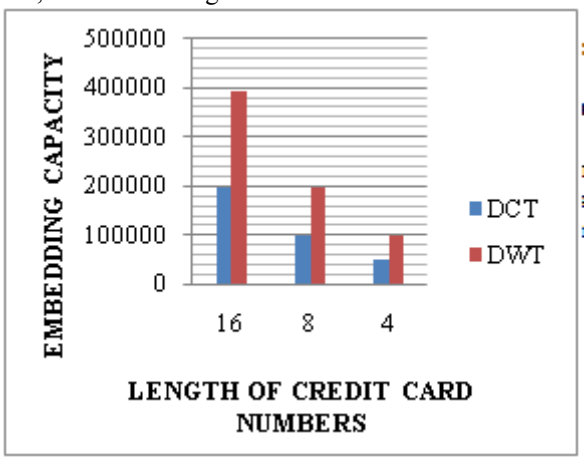

Figure 5.5: Graph of Embedding Capacity using 8 x 8 blocks and size 256 x 256

From the above graphs it can be concluded that size and embedding capacity of DWT is higher than the DCT.

6. Conclusion

In this paper a high capacity data hiding method is used to embed the Credit card numbers into the images but it cannot be done in a direct manner. To have a more Security levels for data embedding a robust Scramble and Descramble Data embedding algorithm is introduced which consist of MK randomize key Generator. In this method, three levels of security are used, first in Scrambling original data, second Exclusive OR the Scramble original data with Generated keys by M-K randomize key generator and third the place of DCT coefficients to embedding. In DWT Based Steganography, coefficients in the low frequency sub-band could be preserved unaltered for improving the image quality. This is because of different characteristics of DWT coefficients in different sub-bands. Since the most essential portion (the low frequency part) remain unchanged, when the secret messages are embedded in the high frequency sub-bands corresponding to the edges portion of the original image, PSNR will be being recommended. The performance and comparison of these DCT and DWT techniques is evaluated on the basis of performance PSNR, MSR, Correlation, Processing time, Capacity and Embedding estimation. The proposed Method is very practical for most transferable Banks transactions on the internet for example LOGO image files.

7. Future Scope

In future the same technique can be extended by applying different DCT levels (DL> 1) and embedding more and more credit number digits in one Block DCT (ND> 16) as well as same quality of cover image with high security levels. The comparison can be done using hash codes and DWT-SVD in place of DWT.

8. Acknowledgement

The authors would like to express their gratitude to Vision Group on Science and Technology, Govt of Karnataka for providing the infrastructure support to carry out this research work.

References

[1] Beenish Mehboob and Rashid Aziz Faruqui, "A Steganography Implementation", International Journal of Image, Graphics and Signal Processing, Vol 5, No 8, pp.23-34, 2010.

[2] K Suresh Babu, K B Raja, Kiran Kumar K, Manjula Devi T H, Venugopal K R, and L M Patnaik, "Authentication of Secret Information in Image Steganography" TENCON Conference, pp1-6, 2008 .

[3] Jessica Fridrich, Miroslav Goljan, Rui Du, "Lossless Data Embedding For All Image Formats", EURASIP Journal on Applied Signal Processing, Vol No 2, pp 185–196, 2002

[4] Hanizan Shanker Hussain, et.al., "A Novel Hybrid Fuzzy SVM Image Steganographic Model, International Symposium on Information Technology, pp 1-6, 2010

[5] Dr. Mohammad V. Malakooti , Mehrzad Khederzdeh "A Lossless Secure Data Embedding in Image Using DCT and Randomize Key Generator," IEEE International Conference paper on Digital information and communication technology and its application, pp 236-239, 2012.

[6] Stuti Goel, Arun Rana, Manpreet Kaur, "Comparison of Image Steganography Techniques" International

Journal of Computers and Distributed Systems, Vol. No.3, pp 20-30, 2013.
[7] Nidhi Bisla, Prachi Chaudhary, "Comparative Study of DWT and DWT-SVD Image Watermarking Techniques", International Journal of Advanced Research in Computer Science and Software Engineering. Vol N0.3, pp 821-825, 2013.
[8] K.B.Raja, C.R.Chowdary, Venugopal K R, L.M.Patnaik, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images", IEEE International Conference on Intelligent Sensing and Information Processing , pp 803-588, 2005.
[9] Chang, C.C., T.S. Chen and L.Z. Chung "A steganographic method based upon JPEG and Quantization Table Modification" IEEE International Conference in Information Sciences, Volume 6, No. 1, pp. 123-138, 2002.
[10] Ali Al-Ataby and Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform" International Arab Journal of Information Technology, Vol. 7, No. 4, pp 358-364, 2010.
[11] Kobayashi, H., Y. Noguchi and H. Kiya . A method of embedding binary data into JPEG bit streams. IEICE Trans. Information and Systems, Vol No 83, pp1582-1588,2000.
[12] K. B. Raja, Vikas, Venugopal K. R and L. M. Patnaik, "High Capacity Lossless Secure Image Steganography using Wavelets,"International Conference on Advances Computing and Communications, pp 230 – 235, 2006.
[13] Radovan Ridzon, Dushan Levisky and Tomas Kanocz, "Information Hiding within Still Images Based on the DCT Coefficients Flipping and Encryption," Fifty Second International Symposium ELMAR, pp 147 – 150, 2010.
[14] NedaRaftari and Amir Masoud Eftekhari Moghadam, "Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT", Fourth International Conference on Computational Intelligence, Communication Systems and Networks, pp 295-300,2012
[15] Navpreet Saroya, Prabhpreet Kaur, "Analysis of IMAGE COMPRESSION Algorithm Using DCT and DWT Transforms", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 4(2), pp 897-900, 2014
[16] Saraswathy, K., D. Vaithiyanathan, and R. Seshasayanan. "A DCT approximation with low complexity for image compression." International Conference on Communications and Signal Processing. pp 465-468, 2013.
[17] Kunal D Megha1, Nimesh P Vaidya2, Asst. Prof Ketan Patel. "Digital Watermarking: Data Hiding Techniques using DCT-DWT Algorithm". International Journal of Advanced Research in Computer and Communication Engineering. Vol. 2, Issue 6, pp 2397-2402, 2013.
[18] T. Narasimmalou, Allen Joseph .R, "Optimized Discrete Wavelet Transform based Steganography" , IEEE International Conference on Advanced Communication Control and Computing Technologies, PP 88-91,2012.

Author Profile

Poornima. G is an Associate Professor in the Department of Electronics and Communication, BMS College of Engg, Bangalore. She has received the BE degree in Electronics and Communication Engg from Bangalore University in the year 1996 and has obtained Master of Engineering in Digital Communication from Bangalore University. She is currently pursuing Ph.D. in Computer Science and Engineering at University of Visvesvariah College of Engineering, Bangalore University under the guidance of Dr. K Suresh Babu, Professor, Department of Electronics and Communication Engineering, University Visvesvaraya College of Engineering. Her research interests include signal processing and computer networks. She has 04 research publications in refereed International Conference Proceedings. She is a life member of Indian Society for Technical Education, New Delhi.

Mamata J is student of M. Tech in Digital Communication from BMS College of Engg, Bangalore. She has completed her degree in PDA College of Engg, Gulbarga in the year 2011.