Performance Analysis of Digital Image Steganographic Algorithm

N.D. Jambhekar
Department of Computer Science
S.S.S.K.R. Innani Mahavidyalaya
Karanja, Dist. Washim (M.S.), India
ndjambhekar@rediffmail.com

C.A. Dhawale
MCA Department
P.R. Pote College of Engineering & Management, Amravati (M.S.), India
cadhawale@rediffmail.com

R. Hegadi
Kruti Institute of Technology & Engineering (KITE)
Raipur (C.G.), India
rajendra.hegadi@gmail.com

ABSTRACT
Steganography is the technique with which the confidential data is hidden under the cover medium such as image, without reflecting any clue on the cover image. Many algorithms are designed to provide the security for the communication of data over the Internet. The good steganographic algorithm is identified by the performance of the algorithm measured with the help of the parameters such as PSNR, MSE, robustness and capacity to hide the information in the cover image. This paper analyzed the Digital Image Steganographic algorithms in spatial and frequency domain.

Keywords
Cover, stego, LSB, PVD, spread spectrum, DCT, DWT, DFT, IWT.

1. INTRODUCTION
Steganography is the technique that covers the confidential data under the cover medium such as image, without reflecting any clue on the cover image. Secrete Message transmission is possible by the technique steganography with the help of entities such as a secret message, message carrier and the embedding algorithm who embed the secret message in the cover message i.e. image. The Message is the secret data which is being hidden and carrier is the entity that covers the secret message. Using the image steganographic method, the secret message is covered by an image in such way that the secret message can be easily extracted as well as the cover image does not lose its visibility. The variations are done slightly, that do not reflect the visual changes in the image. The mathematical techniques, available in the cryptography have some limitations and can prone to crack mathematically.

The image steganography is more secure, but the processing and extraction of the secret message from the cover image need some more processing time. The good steganographic algorithms are able to hide the sensitive data under the cover medium such as image, without remaining any noticeable clue to the intruders. The strength of the steganographic algorithms is to keep the confidential information under an image such a way that, no any steganalysis method, or tool extracts the original message from the cover image without the proper stego key. In this paper, we analyzed the digital image steganography using the spatial and frequency domain. In the spatial domain, we have analyzed the spatial based methods carried out by the image pixel base using the techniques such as Lease Significant Bit (LSB) insertion, SVD and spread spectrum methods. In the frequency based methods, the Discrete Cosine Transformation (DCT), Discrete Wavelet Transformation (DWT), Discrete Fourier Transformation (DFT) and Integer Wavelet Transformation (IWT) steganographic transformation based methods are analyzed to hide secret image i.e. the payload to another cover image.

The efficiency of the above steganographic algorithms is analyzed with the help of comparing the cover image with the stego image. This comparison is carried out by calculating the parameters viz. Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE) with the help of programming the code in MATLAB. The following figure shows the digital image steganographic algorithms. The steganographic algorithms are classified using text, digital image, audio, video, internet protocols and 3d domain as shown in the figure 1. In this paper, we have selected the Digital Image Steganographic Algorithms for analysis and testing of performance using the available image (spatial) domain and transform (frequency) domain. The spatial or image domain consists of the LSB insertion, PVD and spread spectrum methods while the transform or frequency domain consists of DWT, DCT, DFT and IWT methods which are discussed below.

2. COVER SELECTION
The primary goal of image steganography is to embed the secret image in another image known as a cover image. The selection of the cover is completely dependent on the size of the secret image. The cover image is large enough to hold the secret image. To select the cover image, we analyze the distortion measure along with a threshold value. Before embedding an image, the quality of the cover image is tested against the measures such as MSE, PSNR results into the efficient distortion less embedding which tends to the stego image undetectable by any steganalyzer. The steganalyzer verify the stego image for the micro changes and distortion in the image to guess and extract the secret message or image from the stego image. The cover image selection is the issue of sender and receiver who engaged in the secret communication using the digital image steganographic algorithms. The secrecy of the secret communication depends on the key image, i.e. the cover image keeps secretly. This secret cover image must be transferred from sender to receiver secretly without giving any indication to the intruders.

ICTCS '14, November 14 - 16 2014, Udaipur, Rajasthan, India
Copyright 2014 ACM 978-1-4503-3216-3/14/11…$15.00
http://dx.doi.org/10.1145/2677855.2677937

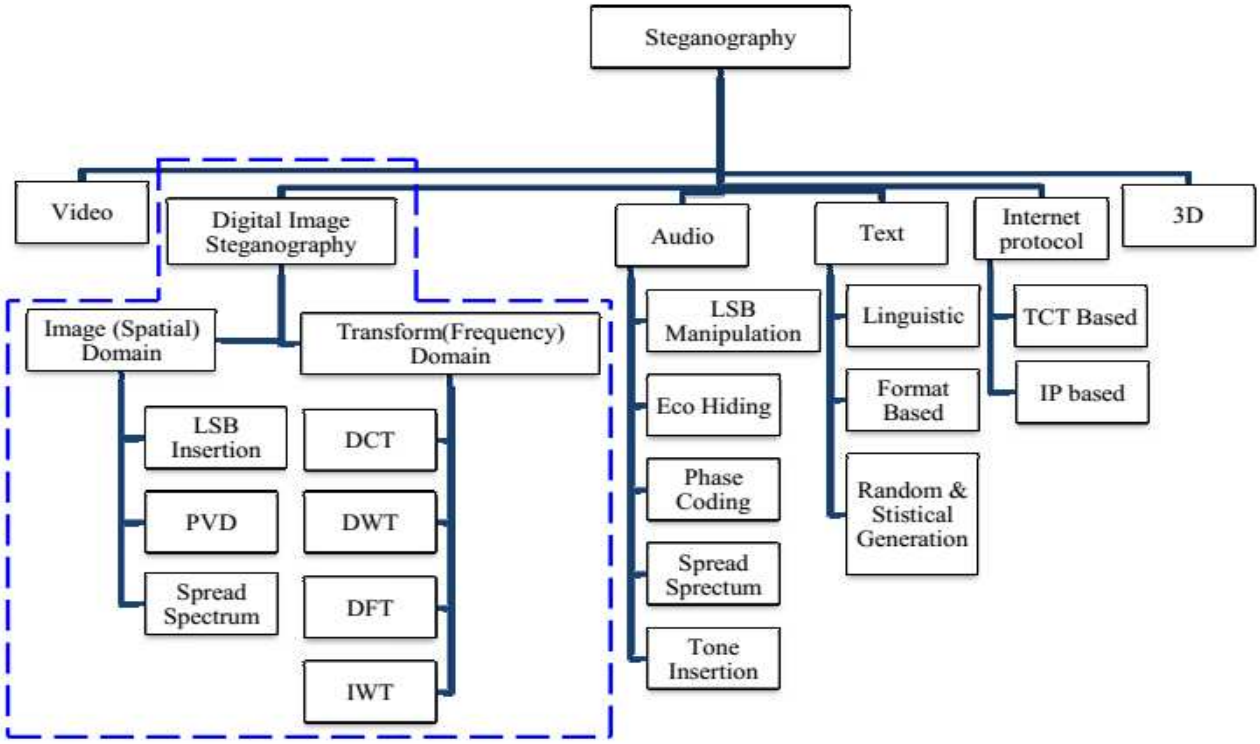

Figure 1. Steganographic Methods.

3. DIGITAL IMAGE STEGANOGRAPHIC ALGORITHMS

3.1 Image (Spatial) Domain

The image or spatial domain is the field through which the embedding of secret message can be performed by using working with the pixel of the image, by embedding the secret image in the pixels intensity. The techniques covered under the spatial domain are

3.1.1 Least Significant Bit Insertion Method

The LSB insertion method is a technique with which, the lease significant bits are cover image is replaced by the most significant bits of secret image [1], [15]. Due to this, the secret image is embedded in the cover image without any visible clue on the cover image. Digital images are commonly available in 8 bits, 16 bits and 24 bits. We can embed one, two and three bits for each image pixel for the 8 bits, 16 bits and 24 bits images respectively. The embedding positions are the LSB for each byte. Some or every byte of cover image can hide one bit of secret image information. The resulting product is the stego image. The secret message embedding is carried with the help of following procedure.

The secret and cover image bit position is calculated by Secret(i,j) and Cover(i,j).

Three possibilities are calculated as

if LSB(Cover(i,j)) = MSB(Secret(i,j)) then no change and continue to next position

if LSB(Cover(i,j)) >MSB(Secret(i,j))then LSB(Stego(i,j)) = LSB(Cover(i,j)) - 1

if LSB(Cover(i,j)) <MSB(Secret(i,j))then LSB(Stego(i,j)) = LSB(Cover(i,j)) + 1

Here the new image after embedding is the stego image similar with the cover image. The similarity is because of the change in the LSB of the cover image, which cannot affect the visual perception of the cover image. Here Stego(i,j) is the stego image.

The process of extracting secret image bits from stegoimage is straightforward.

if LSB(Stego(i,j)) = 0 then MSB(Secret(i,j)) = 0

if LSB(C(i,j)) = 1then MSB(S(i,j)) = 1

For this embedding process, the cover image large enough to hold the secret image's all bits.

3.1.2 Pixel-Value Differencing (PVD)

Secret date hiding in digital images with the help of the pixel-value differencing (PVD) [12] method gives higher embedding capacity without reflecting any clue on the cover image. The pixel-value differencing (PVD) method was originally developed for hiding the secret messages into 8 bits grayscale images. Even though the large amount of secret information is embedded, the PVD produces high definition stego image. PVD partitions the cover image into non overlapping blocks with two consecutive non overlapping pixels. The embedding of secret message get started using PVD with upper left corner of the cover image that reads the cover image in a zigzag fashion as shown in Fig. 2. Each two-pixel blocks are used to maintain the smoothness properties

of the cover image. There is a difference in the edge and the block pixels. If the difference is larger, more bits can be embedded in the cover image pixels pair. From each block the difference value d_i is calculated by subtracting p_i from p_i+1. The difference values are in between -255 to 255.

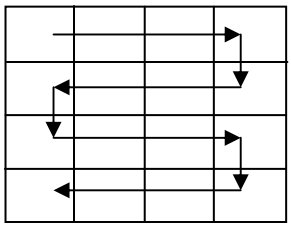

Figure 2. Blocks of images with zigzag scan.

3.1.3 Spread Spectrum

Using spread spectrum method, secret information is distributed around the cover image therefore it is difficult to locate the secrets [13]. Using spread spectrum method, the data from secret image is planted in noise and then mixed with the cover image to generate the stego image. Here the secret image data are embedded having lower signal than the cover image, the secret image is not noticeable by human as well as steganalyzer [14]. The Spread spectrum technique is statistically strong and proves the robustness practically, even if the secret data is scattered all over the cover image, without modifying the statistical properties.

3.2 Transform (Frequency) Domain

The transform or frequency domain methods hide a secret message in the significant parts of the cover image which makes the stego image more robust. In this, the image is transformed from pixel domain to frequency domain. The following methods are the frequency domain techniques used in the digital image steganography.

3.2.1 Discrete Cosine Transformation

Digital steganography for images is done with the help of two techniques- spatial domain and transform domain. The DCT is an orthogonal transformation for the digital and signal processing [16]. During 2-dimensional DCT, the image is divided into 8 x 8 blocks and then each block is transformed to the DCT domain. The different equal size band of the image is selected such as low, middle and high frequency bands.

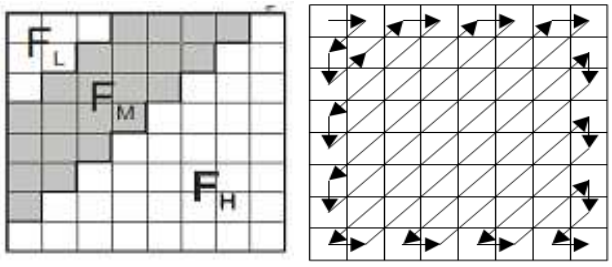

Figure 3. Bands of an image.

DCT coefficients are organized frequency wise by zigzag fashion so that the frequency positions 0 to 63 can be acquired.

Thereafter, it is easier to embed secret image to the selected frequency band(s) [17]. The visual part is kept under the low frequency. The low and high frequency bands are targeted for the compression and noise removal. Therefore, the middle frequency bands are more suitable for embedding because the secret image resides in without any loss and it cannot affect the visibility of the image. JPEG compression is accomplished with the help of DCT coefficients. I divide the cover image into portions. It translates cover image from the image domain to the frequency domain.

The following equation shows the 2-dimensional DCT

$$\boldsymbol{F}(\mathrm{u},\mathrm{v}) = \frac{c(u)c(v)}{4}\sum_{i=0}^{7}\sum_{j=0}^{7}\cos\left(\frac{(2i+1)u\pi}{16}\right)\cos\left(\frac{(2j+1)u\pi}{16}\right)\boldsymbol{f}(\mathrm{i},\mathrm{j}) \quad \textbf{(1)}$$

$$c(e) = \begin{cases}\frac{1}{\sqrt{2}} if\ e = 0\\ 1\ if\ e \neq 0\end{cases} \quad \textbf{(2)}$$

Here, f (u,v) and f (i,j) present a DCT coefficient at the (u,v) coordinate and a pixel value at the (i,j) coordinate, respectively. f(0,0) is the DC component, which corresponds to an average intensity value of each block in the spatial domain. f(u,v) is the AC component, in which u ≠0 and v ≠0.

Input: cover and secret image
Output: stego image embedded with secret image
while end of secret image file do
  read adjacent *f(i,j)* of cover image
  if *f(i,j)* = 0 and *f(i,j)*= 1 then
    get adjacent LSB of secret image
    replace DCT LSB with secret image bit
  end if
  insert *f(i,j)* into stego image
end while

3.2.2 Discrete Wavelet Transformation

The Discrete Wavelet transform (DWT) widely used in the signal processing, watermarking and image compression. The DWT decompose an image mathematically into a set of functions, known as wavelets. Wavelets are produced by converting and expanding of an existing original wavelet. The data are represented using high pass and low pass coefficients [2]. The DWT divides the signal into low and high frequency bands. The low frequency band contains coarse information of the signal while the edge components are represented by the high frequency band. The high frequency band is suitable for embedding because these regions are unnoticeable to the human eye on their edges. In two dimensional object, we perform DWT in vertical direction followed by horizontal direction. At the end of the first level decomposition, the four sub-bands: LL1, LH1, HL1, and HH1 are generated. The previous level decomposed LL band is used as input for the next successive decomposition. To carry DWT for second level, we perform DWT on LL1 & for third Level decomposition we applied DWT on LL2 & finally we get 4 sub band of third level that are LL3, LH3, HH3, HL3.

3.2.3 Discrete FourierTransformation

The embedding of a secret message into cover image is done by converting the cover image from the spatial domain to frequency domain. Then divide the image into equal blocks 2x2 pixels. Then the secrete message data get hidden in the LSB part of the real image using the DFT method. Thereafter the conversion is done from frequency domain to spatial domain to generate the stego

image. The frequency domain works in the analog nature of the image. The image is the collection of pixels, while the DFT converts image into the analog signals.

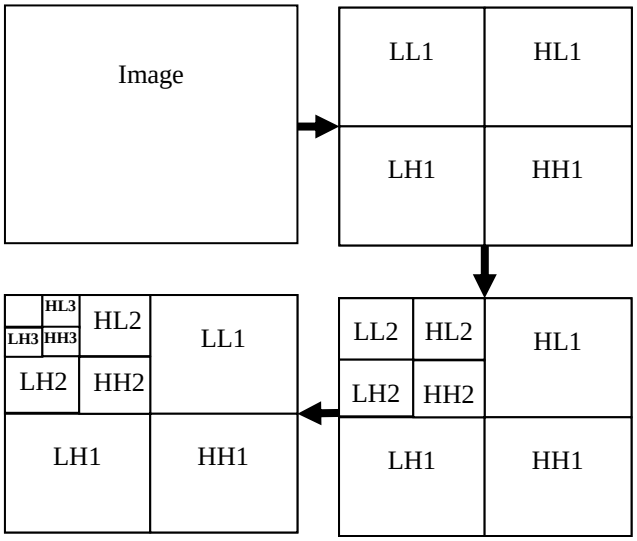

Figure 3. Three level Discrete Wavelet Decomposition.

3.2.4 Integer Wavelet Transformation

Integer Wavelet Transformation is a frequency domain method efficiently produces the lossless compression. It represents the image coefficient into an integer number [20]. The IWT uses a complete technique of DWT but maps integers to integers in the output. In discrete wavelet transform, the wavelet filter has the floating point coefficients [21]. When the secret information is stored, then data loss occurs because of the truncation of integer value due to floating point coefficient. This loss cannot persist in the Integer Wavelet Transformation, because it maps integer to integer in the output.

4. PERFORMANCE PARAMETERS

The performance of the algorithms used for the embedding of secret image on the cover, is measured by analyzing the cover image with the stego image [18]. The analysis is done by finding the parameters such as Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE), Normalized Cross-Correlation (NCC), Average Difference (AD), Structural Content (SC), Maximum Difference (MD) and Normalized Absolute Error (NAE). The following parameters are helpful to analyze the cover image with stego image and the difference will be calculated mathematically.

4.1 Peak Signal to Noise Ratio (PSNR)

The Peak Signal-to-noise ratio (PSNR) is the ratio between the peak signal and alteration noise signals that affects the accuracy of its presentation of stego image. PSNR is described using logarithmic decibel scale. The lower the PSNR rate indicates the low quality and compression, where higher the PSNR, the better the quality of the compressed or reconstructed image. The PSNR is calculated by following formula

$$PSNR = \log_{10}\left(\frac{\mathrm{MAX}_\mathrm{I}^2}{\mathrm{MSE}}\right) \quad \textbf{(3)}$$

The PSNR is calculated via Mean Squared Error (MSE). Here, $\mathrm{MAX}_\mathbf{I}$ is the highest existing pixel value. If pixels are defined by a 8 bit value, then it becomes 255.

4.2 Mean Squared Ratio (MSE)

The MSE is the successively incremented squared error between the stego and the cover image. The Mean Squared Error (MSE) is used to quantify the difference between values implied by an estimator and the true values of the quantity being estimated. It is calculated by following formula

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \quad \textbf{(4)}$$

Where $I(i,j)$ am the original image and $K(i,j)$ is the stego image. The m & n are the dimensions of the images. If MSE is low, then errors are less having high quality.

4.3 Normalized Cross-Correlation (NCC)

Normalized cross correlation is used to match template, i.e. it is a process used to find the relevancy of the structure or object in an image. Correlation is widely used as an effective similarity measure in matching tasks. This function returns the normalized cross correlation between the calling data series and the argument, the input data series. It is calculated by following formula

$$NCC = \frac{\sum_{j=1}^{M}\sum_{k=1}^{n}(I(x,y) - I'(x,y))^2}{\sum_{j=1}^{M}\sum_{k=1}^{n}(I(x,y)^2} \quad \textbf{(5)}$$

4.4 Average Difference (AD)

It is an average difference between the two selected pixel values of cover and stego image. If it is lower, both images match the correctness and without noise. It is calculated by following formula

$$AD = \frac{1}{M * N}\sum_{i=1}^{M}\sum_{j=1}^{n}(S(i,j) - C(i,j)) \quad \textbf{(6)}$$

4.5 Structural Content (SC)

The structural correlation or Content measures the similarity between the cover and stego image by analyzing the small areas having nearest low level structural information. The similarity is measured by counting the number of similar regions. If similar regions are large, then both images are more similar. The large value indicates the low quality and small value indicates the high quality. It is calculated by following formula

$$SC = \frac{\sum_{j=1}^{M}\sum_{k=1}^{n}I(x,y)^2}{\sum_{j=1}^{M}\sum_{k=1}^{n}(I'(x,y)^2} \quad \textbf{(7)}$$

4.6 Maximum Difference (MD)

It is used to measure the cover and stego images and the compressed quality of stego image. Large value indicates poor quality. It is calculated by following formula

$$MD = Max\left(\left|x_j, k - x_j, k\right|\right) \quad \textbf{(8)}$$

4.7 Normalized Absolute Error (NAE)

It is the statistical difference between the cover and stego image. The large value indicates the low quality and small value indicates the high quality. It is calculated by following formula

$$NAE = \frac{\sum_{j=1}^{M}\sum_{k=1}^{n}\left|x_j, k - x_j, k\right|}{\sum_{j=1}^{M}\sum_{k=1}^{n}\left|x_j, k\right|} \quad \textbf{(9)}$$

5. PERFORMANCE ANALYSIS

The embedding process of secret image in the cover image is analyzed in MATLAB and tested against the spatial and the transform domain method. The images selected for the process are the cover image and secret image producing the stego image.

Cover Image	Secret Image	Stego Image
		
lena.tif (257kb)	flower.jpg (13.2kb)	lena.jpg (41.5kb)

Figure 3. Images Tested against the selected algorithms.

The performance analysis of the spatial domain methods such as LSB insertion, PVD, Spread Spectrum and the transform, i.e. frequency domain methods such as DCT, DWT, DFT and IWT are analyzed by implementing the code for each algorithm in MATLAB. The cover and secret images are given to each algorithm and the output collected are the stego images.

A separate MATLAB code is designed, that analyze the performance of the spatial and frequency domain algorithms, by comparing the cover image with the stego image processed by each algorithm. The comparison is done by analyzing the parameters such as Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE), Normalized Cross-Correlation (NCC), Average Difference (AD), Structural Content (SC), Maximum Difference (MD), and Normalized Absolute Error (NAE). The detailed analysis is given in table 1.

These parameters are compared with same parameter of the other steganographic method. The performance parameters and results are varied by using the different sizes of cover and secret images as well as selecting the different type of images for operation such as JPEG, BMP, TIF, PNG. The results are also affected if the images selected are the 8, 16 or 24 bits and color or grayscale. The analysis performed on the selected cover and stego images, used by the embedding operation for each algorithm, is shown below by each performance parameter. The performance analysis of the LSB, DCT and DWT methods are discussed in the table 2.

When the parameters are compared with each other for the selected cover and stego image, the result appears as

5.1 Peak Signal to Noise Ratio (PSNR)

Lower PSNR indicates the larger difference between cover and stego image. Even if, the lower PSNR cannot reflect the perceptual quality. Here the DWT algorithm has lower PSNR and LSB insertion is very higher PSNR. It means that the spatial domain method produces high PSNR where the DWT has lower PSNR.

5.2 Mean Squared Ratio (MSE)

Lower MSE tends to lower error. The spatial domain methods have very low values.

5.3 Normalized Cross-Correlation (NCC)

The value NCC = 1 indicates the equal identity of both images. All algorithms produce the stego image identical to the cover image.

5.4 Average Difference (AD)

It is found from the comparison of respected three algorithms, the frequency domain embedding methods produces the lower noise with greatest pixel accuracy as compared with algorithms in the spatial domain. The steganalyzer finds the noise of the stego image and can calculate the secret message or image. The main objectives of the algorithms are embedding with less noise.

5.5 Structural Content (SC)

The SC lower value indicates the highest quality. The frequency domain algorithms have lower value compared with spatial domain algorithms. It means, they produced the stego image with high quality and similarity of structural content between cover and stego images.

5.6 Maximum Difference (MD)

The large value of MD indicates the poor quality compression. The spatial domain methods produce the stego images with very good quality and compression as compared with transformation domain.

5.7 Normalized Absolute Error (NAE)

The larger NAE indicates the large visual difference in image. The spatial domain methods NAE is very small indicates a very small difference in cover and stego image denotes the good quality. Also the frequency domain is near about the good quality having lower NAE.

Table 1. Practically Implemented and Collected Result of Performance Parameters

Algorithm	PSNR	MSE	NCC	AD	SC	MD	NAE
LSB Insertion	43.5678	2.8596	0.9999	0.0190	1.0001	23	0.0038
PVD	38.84	8.4798	0.9978	0.0213	1.0013	27	0.0101
Spread Spectrum	42.11	27.4350	1.0104	0.0295	1.0097	26	0.0245
DCT	31.8513	42.4570	0.9991	0.0028	0.9984	66	0.0516
DWT	30.4040	59.2495	1.0010	-0.0358	0.9934	30	0.0580
DFT	40.4234	45.4342	0.9989	0.0034	0.9964	70	0.0497
IWT	44.63	62.4345	1.0023	0.0023	0.9976	33	0.0510

Table 2. Performance Analysis

Features	LSB	PVD	Spread Spectrum	DCT	DWT	DFT	IWT
PSNR	High	Medium	Medium	Medium	Low	Medium	Low
MSE	Low	Medium	Medium	Medium	High	Medium	High
NCC	Nearest	Nearest	Medium	Nearest	Nearest	Nearest	Medium
AD (Noise)	High	High	High	Medium	Low	High	Medium
SC	High	High	High	Medium	Low	High	Low
MD	Low	Low	Low	High	Medium	Low	Medium
NAE	Low	Low	Low	Medium	High	Low	High
Invisibility	Low	Low	Medium	High	High	Medium	High
Payload Capacity	High	High	Medium	Medium	Low	Medium	Medium
Robustness of stego image	Low	Low	Low	Medium	High	Medium	High

6. CONCLUSION

The performance of spatial and frequency domain algorithms have investigated by implementing the code in MATLAB. The cover and secret images are supplied to the algorithms and the stego images are collected. The cover images and respected three stego images are then supplied to the performance analysis code, coded in MATLAB. It is found that the Average Difference i.e. noise is higher in using spatial domain methods as compared to the frequency domain methods such as medium in DCT and lower in the DWT. The steganalyzer detect and extract the secret message by analyzing the noise in the stego image. Here DWT produces very small noise, cannot tend to attack. But LSB and DCT are more vulnerable. The structural content measures the total weight content and the difference between the cover and stego image. The DWT and IWT have lower difference and ideal for steganography. In some terms, the LSB is more suitable than other but it is somewhat vulnerable. The DWT is more adequate having the requisite qualities and functions to meet robustness and safety. The lower invisibility of the secret image has investigated using the DWT method. DWT is robust due to the lower noise impression on the stego image. The histograms for each cover and stego image have generated for each method with help of MATLAB code. Still the spatial domain methods are simple and more suitable, but the DWT method is distortion less with less noise and greater image quality because of the Average Difference and Structural Content.

7. REFERENCES

[1] Chi-Kwong Chan, Cheng, L.M. 2004. Hiding data in images by simple LSB substitution. Pattern Recognition Society 37, pp. 469-474, Published by Elsevier Ltd.

[2] Barni, M., (2001) "Improved Wavelet-Based Watermarking Through Pixel-Wise Masking", IEEE Transactions on Image Processing, Vol. 10, No. 5, ISSN: 1057-7149, pp. 783-791.

[3] Fan-Hui Kong, (2009) "Image Retrieval using both Color and Texture Features", Proceedings of the Eighth International Conference on Machine Learning and Cybernetics, Baoding, IEEE, vol. 4, pp.12-15.

[4] Demirel, H., Jafari, G. A., (2011) "Image Resolution Enhancement by Using Discrete and Stationary Wavelet Decomposition", IEEE Transactions on Image Processing, Vol. 20, No.5, pp. 1458-1460.

[5] Fang, J. Liu, Gu, W., Tang, Y., (2011) "A method to improve the image enhancement result based on image

fusion", International Conference on Multimedia Technology (ICMT), Hangzhou, pp. 55-58.

[6] Provos, N. Honeyman, P., (2003) "Hide and seek: an introduction to steganography", Security & Privacy, IEEE Journals & Magazines, Vol. 1, no. 3, pp. 32-44.

[7] Bender, D. G., Morimoto, N., Lu, A., (2010) "Techniques for data hiding", IBM Systems Journal, Vol. 35, No. 3 & 4, pp. 313-336.

[8] Ker, A.D., (2005) "Steganalysis of LSB matching in grayscale images", Signal Processing Letters, IEEE, vol. 12, no.6, pp.441- 444.

[9] Cheddad, A. Condell, J. Curran, K. McKevitt, P., (2010) "Digital image steganography: Survey and analysis of current methods", Signal Processing 90, pp. 727-752.

[10] Yoo, J.-C., Ahn, C.W., (2012) "Image matching using peak signal-to-noise ratio-based occlusion detection", IEEE, Image Processing, IET, vol. 6, no. 5, pp. 483-495.

[11] Gonzalez, R.C., Woods, R.E., Eddins, S.L., (2010) "Digital Image Processing Using Matlab", Second Edition, Tata McGraw Hill Education Private Limited, New Delhi, ISBN-13: 978-0-07-070262-2.

[12] Wu, D.-C., Tsai, W.-H., (2003) "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters 24, Published by Elsevier, pp. 1613-1626.

[13] Wang, H., Wang, S., (2004) "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, vol. 47, no. 10

[14] Marvel, L.M., Boncelet Jr., C.G., Retter, C., (1999) "Spread Spectrum Steganography", IEEE Transactions on image processing, vol. 8, no. 8.

[15] Chan C. K., Cheng, L., (2004) "Hiding data in images by simple LSB substitution", Pattern Recognition Society, Published by Elsevier, vol. 37, no. 3, pp. 469-474.

[16] Hashad, A.I., Madani, A.S., Wahdan, A.E.M.A., (2005) "A robust steganography technique using discrete cosine transform insertion", Enabling Technologies for the New Knowledge Society: ITI 3rd International Conference on Information and Communications Technology, Cairo, pp. 255-264.

[17] Sakr, A.S., Ibrahem, H.M., Abdullkader, H.M. Amin, M., (2012) "A steganographic method based on DCT and new quantization technique", 22nd International Conference on Computer Theory and Applications (ICCTA), Alexandria, pp. 187-191.

[18] Kumar, V., Kumar, D., (2010) "Performance evaluation of DWT based image steganography", IEEE 2nd International Advance Computing Conference (IACC), Patiala, pp. 223-228.

[19] Shejul, A.A., Kulkarni, U.L., (2010) "A DWT Based Approach for Steganography using Biometrics", International Conference on Data Storage and Data Engineering (DSDE), Bangalore, pp. 39-43.

[20] Ghasemi, E. Shanbehzadeh J., ZahirAzami, B. (2011) "A steganographic method based on Integer Wavelet Transform and Genetic Algorithm", International Conference on Communications and Signal Processing (ICCSP), Calicut, pp. 42-45.

[21] Hemalatha, S., Acharya, U.D., Renuka, A., Kamath, P.R. (2012) "A secure image steganography technique using Integer Wavelet Transform", World Congress on Information and Communication Technologies (WICT), Trivandrum, pp.755-758.

[22] Sun, F. Liu. (2010) "Selecting Cover for Image Steganography by Correlation Coefficient", Second International Workshop on Education Technology and Computer Science (ETCS), Wuhan, vol.2, pp. 159-162.