International Journal of Innovative Research in Information Security (IJIRIS)
Issue 02, Volume 3 (February 2016)
ISSN: 2349-7017(O)
ISSN: 2349-7009(P)
www.ijiris.com

Frequency Domain Approach of Image Steganography

Himadri Bhattacharjee
M.Tech,Dept. of Computer Science & Engineering
University of Calcutta
Kolkata, India

Dr.Samir Kumar Bandyopadhyay
Prof., Dept. of Computer Science and Engineering
University of Calcutta
Kolkata, India

Abstract-- Image steganography is the art of hiding a message, image, or file within another message, image, or file. Likely, an old term in Ancient Greek, Steganography is derived from steganos meaning —"concealed" and graphein meaning —"writing", in other word we can say it refers to the science of "invisible" communication. Unlike cryptography, where the goal is to secure communications from an eavesdropper, steganography techniques strive to hide the very presence of the message itself froman observer. In this research paper we deal with hiding a digital message image inside a digital cover image leading us to the stego image. With the combination of Message Preparation using Spatial Domain image modification technique, discrete cosine transforms (DCT) and image scrambled using modified Arnold Transform, an algorithm based on the three technologies is proposed. The effectiveness of the proposed methods has been estimated by computing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR) and experimental result shows that the proposed algorithm is highly secured with good perceptual invisibility.

Keywords — Image Steganography, Discrete Cosine Transform, Arnold's Transform, Frequency domain, PSNR

1. INTRODUCTION

In the digital world, various schemes are adopted to hide information. Cryptography and Steganography are two major techniques used for this purpose. In this paper we mainly focus on digital image steganography which is all about using digital images to hide information. Steganography incorporates two major algorithms, firstly **embedding** algorithm and other one is **extracting** the Secret image. Technical names used for images are Host image (cover image) which is visible to everyone, Secret image which is to be hidden and Stego image containing visible host image and hidden Secret image. Extracted Secret image is the data retrieved from a Stego image. The main goal is to not raise suspicion and avoid introducing statistically detectable modifications into the cover image. We point out that the ability to detect the presence does not automatically imply the ability to read the hidden message. We further note that un-detect ability should not be mistaken for invisibility, a concept tied to human perception.

Steganography is divided into two main categories: Spatial Domain based and Frequency Domain based.

Spatial Domain includes Least Significant Bit (LSB) Substitution [1], DC Coefficient LSB and Frequency Domain includes Discrete Wavelet Transform (DWT)[1][2], Discrete Cosine Transform (DCT) etc. Discrete Cosine Transform (DCT) is being used to convert an image from spatial domain to frequency domain. Each category has its own advantages. LSB substitution has more embedding capacity while DCT has more robustness. Different parameters like Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) are used to measure the efficiency of the Stego image.

Our **embedding algorithm** contain two Phases ,In the first phase deals with modification on hidden Secret image such that Secret image change into a completely different meaningless image, it is a pre-processing phase during hiding information of the digital image. This phase includes Initial Preparation of hidden Secret image, followed by Digital image scrambling based on Arnold's Transform. The second phase deals with **embedding process**, at first cover image is decomposed into 8x8 pixel block and on each 8x8 pixel block two-dimensional discrete cosine transform(2D DCT) is applied which results a 8x8 matrix of DCT coefficients. Now on each 8x8 DCT matrix, we have hide one pixel of modified secret image by changing the value of DCT coefficients using blending technique. We can obtain the Stego image when all the pixels of secret image have been embedded into the cover image.

Just like our embedding algorithm, our **extracting algorithm** also contain two Phases, In the first phase is the reverse process of the second phase of embedding algorithm, where the Stego image is decomposed into 8x8 pixel block and on each 8x8 pixel block two-dimensional discrete cosine transform(2D DCT) is applied which results a 8x8 matrix of DCT coefficients. Now on each 8x8 DCT matrix, we can recover the hidden pixel of the secret image and reconstruct the secret image. In the second phase secret image is modified such that we can reconstruct its meaning, i.e the actual secret image that has been modified during the first phase of the embedding process .So this phase is nothing but inverse transformation of the first phase of the embedding process.

© 2014-16, IJIRIS- All Rights Reserved

International Journal of Innovative Research in Information Security (IJIRIS)
Issue 02, Volume 3 (February 2016)
ISSN: 2349-7017(O)
ISSN: 2349-7009(P)
www.ijiris.com

The organization of the rest of the paper is as follows, section 3 describes Literature Survey& Methodology while section 4consists of the proposed Algorithm and section 5consists of the simulation results. Conclusion is drawn in section 6.

2. LITERATURE SURVEY & METHODOLOGY

2.1 Related Theory of Discrete Cosine Transform (DCT)

Similar to discrete fourier transform (DFT), discrete cosine transform (DCT) is a function that maps the input signal or image from spatial domain to frequency domain. DCT transforms the input into a linear combination of weighted basis functions[1-2]. These basis functions are the frequency component of the input data. The two-dimensional DCT is just a one-dimensional DCT applied twice, once in the x direction, and again in the y direction. When you apply the DCT to an input image, it yieldsa matrix of weighted values corresponding to how much of each basis function is present in the original image. For most images, much of the signal energy lies at low frequencies; these appear in the upper-left corner of the DCT. The lower-right values represent higher frequencies, and are often small – small enough to be neglected with little visible distortion.

The definition of the two-dimensional DCT for an input M x N image A and output image B ishas been given in (1):

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{matrix} \qquad \ldots (1)$$

Where

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \sqrt{\frac{2}{M}}, & 1 \le p \le M-1 \end{cases} \qquad \alpha_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \sqrt{\frac{2}{N}}, & 1 \le q \le N-1 \end{cases}$$

M and N are the row and column size of A, respectively. If you apply the DCT to real data, the result is also real. The DCT tends to concentrate information, making it useful for image compression applications.

Inverse 2-D DCT is also available to reverse the application of 2D-DCT on any image. That has been defined in (2):

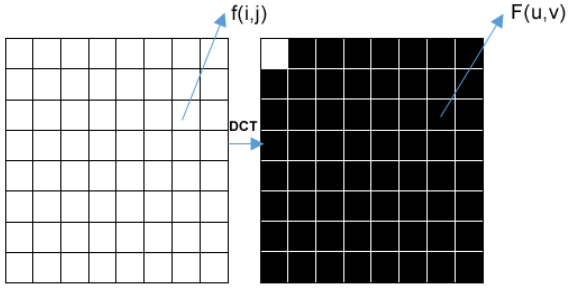
$$A_{mn} = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} \alpha_p \alpha_q B_{pq} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le m \le M-1 \\ 0 \le n \le N-1 \end{matrix} \qquad \ldots (2)$$

Where

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \sqrt{\frac{2}{M}}, & 1 \le p \le M-1 \end{cases} \qquad \alpha_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \sqrt{\frac{2}{N}}, & 1 \le q \le N-1 \end{cases}.$$

Human eyes, ears and brain are analog devices. Human are less sensitive to distortion around edges and less effective to perceive subtle differences in fine textures. Moreover, most of the pixels in an image are often similar to their neighbourhood. These factors opens an arena of data hiding which implies that even after removal of higher frequency elements from an analog signal, there is high probability that human brain might not perceive a difference. DCT actually concentrate major image information within few coefficients which provides opportunity to hide data in insignificant DCT coefficients[3-5].

In figure 1.(a) The pixel of 8x8 image block has been considered as f(i, j) and in the figure 1.(b) DCT coefficients of the image block consider as F(U, V), the coefficient of top left corner*(denoted as white color)* is called direct current term known as DC coefficient or DC basis function which is constant in nature. This DC coefficient defines the average grey level of the image block. The rest 63 coefficients out of 64 basis functions are called alternating current term known as AC coefficients which represents grey scale change in the image block. AC coefficients hold low frequency details of an image.



(a) (b)

Figure1: (a) 8x8 image block (b) DCT Coefficients

© 2014-16, IJIRIS- All Rights Reserved

ISSN: 2349-7017(O)
ISSN: 2349-7009(P)
www.ijiris.com

2.2 Traditional Arnold Transform And modified Arnold Transform

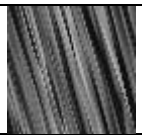
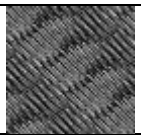
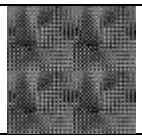
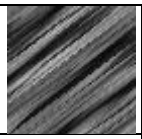
Arnold Transform: Arnold transform was advanced by Russia mathematician named Vladimir I. Arnold. For an N×N image, two-dimensional Arnold transform is defined as (3).

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \text{ where } x, y \in \{0,1,2,..,N-1\}. \ldots (3)$$

Here (x,y) is the pixel of original image and (x',y') is the pixel of transformed image. N is the order of image matrix, generally the cat map has worked on square matrix only.

The most important feature of cat map is that it randomizes the image by some iteration cycle. Randomizing makes the image imperceptible in a term scramble. This is actually a **periodic cycle** i.e. after repeated Arnold transformation scrambled image turns back to original image. Iteration number is used as the encryption key. When Arnold Transformation is applied, the image can do iteration, iteration number is used as a secret key for extracting the secret image[6-9].

TABLE 1: RESULT OF ARNOLD TRANSFORM ON IMAGES

PICTURE:						
ARNOLD ITERATION		1	4	24	95	96

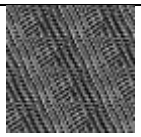
Modified Arnold Transform: It performs similar Operation to Arnold transform except its matrix coefficients are different from traditional Arnold transform. The transform algorithm for above proposed algorithm is given below:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \text{ Where } x, y \in \{0,1,2,3..,N-1\}. \ldots (4)$$

It has proved that for a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ when elements satisfying the criteria that ad-bc = 1.Demerits of above algorithm is that out of four matrix coefficients only two coefficient are unknown so we have a limited choice to choose different matrix coefficients i.e. or simply 2. Secondly its first matrix coefficients i.e. are still fixed to one or unity. So finally we get equation (5) as a modified Arnold transform.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ i & i+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \text{where } x,y \in \{0,1,2,3..,N-1\} \text{ and } i \in \{1,2,3...\}. \ldots (5)$$

TABLE 2: RESULT OF MODIFIED ARNOLD TRANSFORM ON IMAGES

PICTURE:						
ARNOLD ITERATION WITH MATRIX $\begin{pmatrix} 1 & 1 \\ 4 & 5 \end{pmatrix}$		1	4	24	96	128

Advantage of Modified Arnold transform over above variants of Arnold Transform:

i) In Modified Arnold transform, various sets of matrix coefficients can be used while conventional Arnold matrix uses fix set of matrix coefficients.
ii) For an NxN image Arnold Transform periodic cycle depend only on the value of the N. But in case of modified Arnold transform it depends on value of N and *i*. That mean for a same NxN image if we use different values of *i*, then we get different periodic cycle.
ii) Images scrambled with a particular transform matrix cannot be restored using a deferent transform matrix.

Arnold Transform is applicable only on square image , this can be extended to handle any 2D image if we divided image into square sub blocks and then Arnold transform is apply to each block and then scrambling the square sub block.

2.3 Message Preparation Using Spatial Domain Image Modification Technique

We know that the major advantage of the Arnold transform it's periodic in nature but this advantage become major disadvantage when security is concern.

© 2014-16, IJIRIS- All Rights Reserved

ISSN: 2349-7017(O)
ISSN: 2349-7009(P)
www.ijiris.com

To enhance the security aspect of the message (secret image) an encryption mechanism which can be called as a child function of a standard of cryptography DES is use. It includes logical XOR operation as a step function manner, which secures the message from brute force attack or direct use of multiple logical XOR operation with the key as a guess.

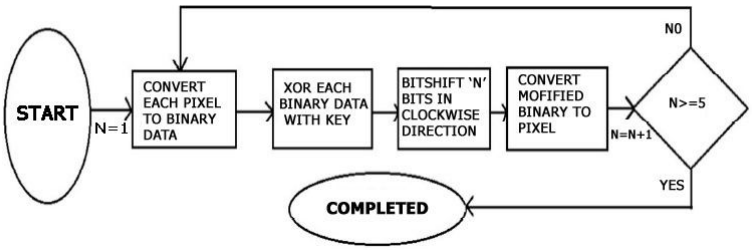


Figure 2: Flow Chart describing the Encoding Process of Message Preparation

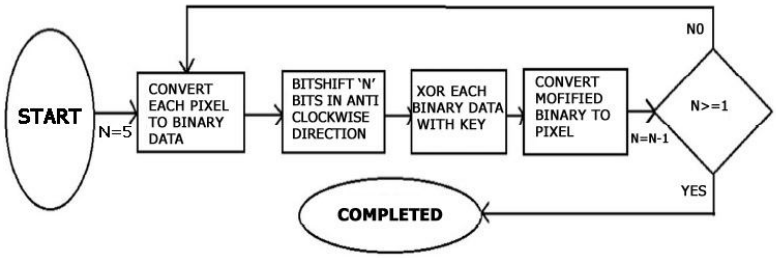
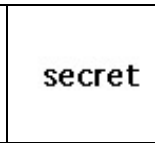
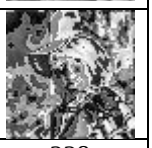


Figure 3: Flow Chart describing the Inverse Process of Message Preparation

The result of this process is shown in Table 3:

TABLE 3: RESULT OF MESSAGE PREPARATION ON VARIOUS IMAGES

PICTURE:			
MESSAGE PICTURE:			
XOR KEY USED:	84	212	228

2.4 Methodology

Any stenographic technique constitutes of an initial preparation followed by an embedding procedure. An extraction procedure is essential to extract the message from the stego image. Generalized framework of any stenographic technique is shown in Figure 4

.

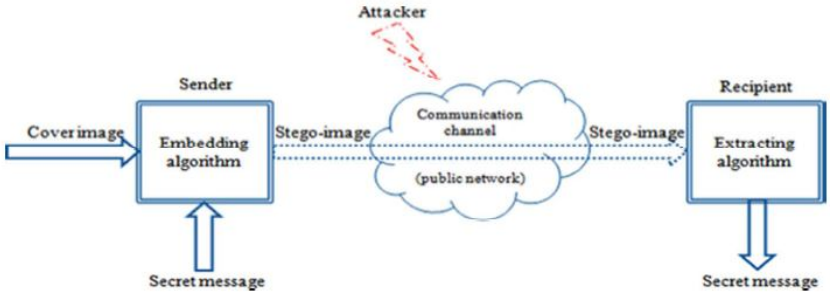


Figure 4: Structure and Working of a Steganography Algorithm

We have already state a little view of our propose method in the introduction part, now here we elaborate it. Our proposed embedding algorithm and extracting algorithm both have two phase. First phase of the embedding algorithm is convert secret image into a meaningless image using scrambled secret image followed by a special domain image transform based on XOR operation with a secret key, we call this step as **Message Preparation** which is already describe in the previous section .

© 2014-16, IJIRIS- All Rights Reserved

ISSN: 2349-7017(O)
ISSN: 2349-7009(P)
www.ijiris.com

The next phase of the embedding algorithm is to perform the DCT on cover/host image to hide the secret image obtain from first phase. Extracting algorithm is very similar to the embedding process, but here two phase of the embedding process are interchange with a little modification .First phase of the Extracting process is to obtain the meaningless secret image from the stego (i.e output of the embedding algorithm) using DCT operation. Then the **inverse transform** of Message **Preparation** is perform to obtain the actual secret image. Now we state how the DCT is perform on an image in figure.

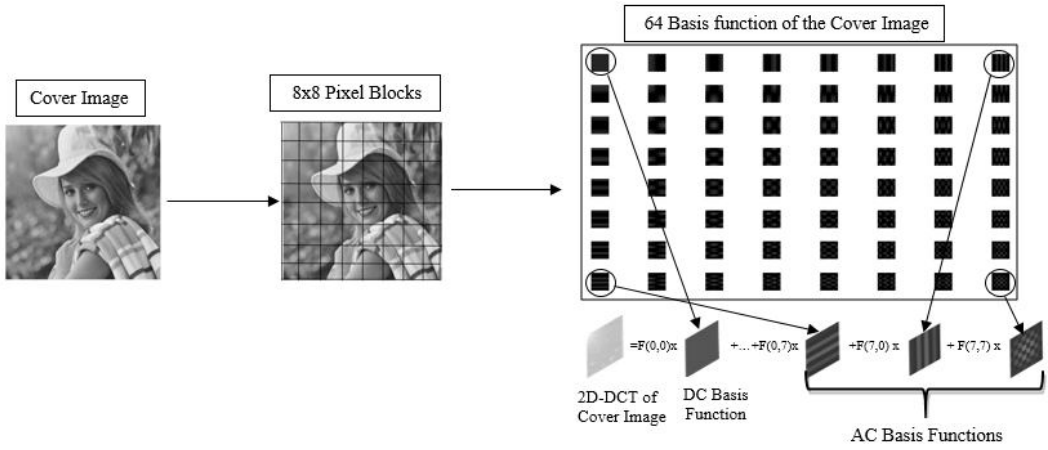


Figure 5: Performing 2D-DCT on input cover image.

Fig.5 show how 2D-DCT for given cover image has been computed. Here cover image is decomposed into 8x8 pixel block and on each pixel block two-dimensional discrete cosine transform is applied which results a 8x8 matrix of DCT coefficients of image block as F(x, y).

The 64 DCT coefficients have been scanned in zigzag manner which reveals that there are 6 low frequency coefficients (F_L), 22 mid-frequency coefficients (F_M – highlighted region in the fig.4) and rest 36 are high frequency coefficients (F_H). In the proposed method this F_M region has been chosen as area of secret data embedding to keep alteration in cover image minimum, because human eyes are very sensitive to low frequency – therefore F_L cannot be chosen. The high frequency region F_H has varied high coefficients therefore modification of coefficient may tamper the cover. F_M region coefficient values are quite similar and modification doesn't reveal existence of secret data. We select one of location from F_M region and replace it value with a hidden image pixel using a scaling factor. Alternatively LSB substation also can be used to hide data.

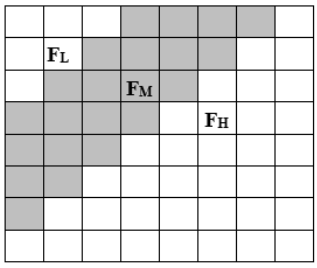


Figure 6: DCT domain of an image.

3. ALGORITHMS OF STEGANOGRAPHY

A. Embedding Algorithm

Here the algorithm to embed secret image into the Cover Image is described as below

Input: A M1xM2cover image and a NxN secret image. Two secret key K1 and K2, Arnold Transform matrix and a alpha value use to hide secret image pixel in 8x8 DCT block of cover image.

Output: A stego-image.

STEP-1: *Read the secret image (i.e secret message), if the image is not gray scale than convert it to gray scale image.*
STEP-2: *Read the cover image, if the image is not gray scale than convert it to gray scale image.*
STEP-3: *Determine the size of cover image, maximum message size based on cover image and block size, resize the cover image if number of 8x8 block of the cover image is less than total pixel of secret image (i.e message size).*
STEP-4: *Perform Arnold transform for iteration K1 times on secret image with transform matrix to get the scrambled secret image.*
STEP-5: *Perform Message Preparation on scrambled secret image using key k2 and obtain message image.*
STEP-6: *Reshape the message image to a vector.*
STEP-7: *Process the cover image in blocks (i.e sub divide the cover image into 8x8 block).*
STEP-8: *Check whether the message image is smaller for cover image, if then store the number of unused image block.*
STEP-9: *Transform cover image block one by one into frequency domain using 2D-DCT.*
STEP-10: *Remove the top most element of message vector and multiply with alpha value, then place the obtain value in DCT block at position (5,2) .*
STEP-12: *Transform block back into spatial domain using Inverse 2D-DCT, and repeat from Step9 until message vector is not empty.*
STEP-13: *Write the output stego image in a file.*

© 2014-16, IJIRIS- All Rights Reserved

ISSN: 2349-7017(O)
ISSN: 2349-7009(P)
www.ijiris.com

B. Extraction Algorithm

Here the algorithm to extract secret image from the stego Image is described as below:

Input: stego-image, two secret key K1 and K2, Arnold Transform matrix and a alpha value, dimension of the secret image.

Output: secret image.

STEP-1: *Set the size of the block in cover to be used for each bit in message,(i.e 8x8 block).*

STEP-2: *Read in the stego image and Determine size of stego image.*

STEP-3: *Determine maximum message size based on stego image size and block size.*

STEP-4: *Determine the number of block used to hide secret message image using the dimension of the secret image.*

STEP-5: *Process the image in blocks*

STEP-6: *Transform block using DCT*

STEP-7: *Read the DCT coefficient at location (5, 2) divide it with alpha to obtain pixel and store it message vector.*

STEP-8: *repeat from step6 until all the message pixels are recover.*

STEP-9: *Reshape the recovered message and obtain message image.*

STEP-10: *Perform inverse of Message Preparation on message image using key k2 and obtain scrambled secret image.*

STEP-11: *Perform Arnold Transform on scrambled secret image for iteration K1 times with Transform matrix to obtain Actual secret image.*

STEP-12: *Display restored secret image/Massage.*

4. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

The above mentioned algorithms have been simulated using MATLAB 7.7.0 version. The result has been analyzed by traditional **Mean Squared Error (**MSE),**Peak Signal To Noise Ratio (PSNR)** approach as well as more improved i.e. by **Structural SIMilarity (SSIM) index** .Peak Signal to Noise Ratio Measures the distortion between original cover image and stego image. Higher the value of PSNR low is the distortion and vice- versa. MSE corresponds to the difference between the cover image and stego image. For high efficiency of Steganography algorithm there should be minimum difference between stego image and cover image. Higher MSE value signifies more difference.

MEAN SQUARED ERROR (MSE): It is a factor to indicate difference in the error. 'I' is grey level image and 'K' is noisy approximation, both image dimensions is $m_x n$.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \ldots (6)$$

PEAK SIGNAL TO NOISE RATIO (PSNR): It states the fidelity of the system and gives the quality of reconstructed data. It is mathematically represented as:

$$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right) \ldots (7)$$

Where, MAX_f is maximum pixel value of cover image (noise free image).

STRUCTURAL SIMILARITY (SSIM) INDEX: It is a metric of similarity among two images where one image is being compared with the other image called reference image with perfect visual quality, it has been stated that images are highly structured and contains high precision structural information derived from spatial proximate. The SSIM index is a decimal value between -1 and 1, and value 1 is only available in the case of two identical sets of image.

Suppose that m and n are two images that are being compared. The SSIM index, defined in (8), measures three elements of the image: the similarity of luminance (brightness values), the similarity of contrasts and the similarity of structures.

$$SSIM(m,n) = \frac{(2\mu_m\mu_n+c_1)(2\sigma_{mn}+c_2)}{(\mu_m^2+\mu_n^2+c_1)(\sigma_m^2+\sigma_n^2+c_2)} \ldots (8)$$

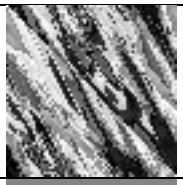
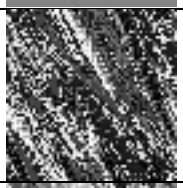
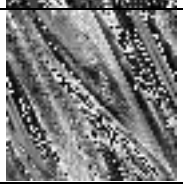
Where, $\mu_m$is the mean of image m and $\mu_n$is the mean of image n; σ_m is standard deviation of image m and σ_n is standard deviation of image n; σ_{mn} is cross correlation of m and n after removing their means.

Simulated Result: A set of 8-bit gray scale images of size 512 × 512 have been used as the cover object and a set object of size 64x64 have been used as message object. After the embedding procedure, the resultant object i.e. the stego object is quiet good in quality with respect to visibility. In extraction procedure it has been aimed to extract the original message intact which has been executed successfully by the above mentioned extraction algorithm. Results are shown in the Table 4.

© 2014-16, IJIRIS- All Rights Reserved

ISSN: 2349-7017(O)
ISSN: 2349-7009(P)
www.ijiris.com

TABLE 4: RESULT ANALYSIS ON VARIOUS IMAGES

S.NO.	COVER IMAGE	SECRET IMAGE	SCRAMBLED SECRET IMAGE	STEGO IMAGE	EXTRACTED SECRET IMAGE	IMAGE QUALITY METRICS
1						MSE : 0.0353 PSNR : 62.3436 SSIM: 0.9997
2						MSE: 0.0785 PSNR: 58.8351 SSIM: 0.9992
3						MSE: 1.7837 PSNR: 45.5835 SSIM: 0.9957
4						MSE: 1.0618 PSNR: 47.3800 SSIM: 0.9950

5. CONCLUSION

Image Steganography is the method of hiding secret message in a cover image. There are several popular algorithms available in Image Steganography. In this research paper a frequency domain approach of Image Steganography has been proposed. Here first the message image is pre-processed with XOR and shifting operation followed by Arnold Transform to scramble it then Discrete Cosine Transform is used to get frequency domain components and data has been embedded within the DCT matrix. This proposed algorithm has shown very good result in visual analysis as well as numerical analysis i.e. calculation of PSNR and SSIM.

The payload capacity can be increased if we use lossless compression technique before applying the proposed scheme. The present work can be extended in future by introducing new masks compressing the message image simultaneously with the embedding process leading to high payload as well as computational efficiency. The strength of proposed technique lies in secrecy of the parameters that are transmitted separately. Without knowledge of these parameters it is not possible to extract the hidden secret image from given stego image. Further the technique can be extended for different types of carrier media such as color image, audio, video etc.

6. REFERENCES

[1] Gauresh Vanjare, Saylee Gharge,"Performance Evaluation of LSB Substitution and DWT Method for Steganography",International Journal of Advanced Research in Computer Science and Software Engineering,Volume 5, Issue 3, March 2015,ISSN: 2277 128X. Page 699-705

[2] Barnali Gupta Banik,Prof. Samir K. Bandyopadhyay,"A DWT Method for Image Steganography",International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 6, June 2013 ISSN: 2277 128X

[3] Gurmeet Kaur, Aarti Kochhar,"A Steganography Implementation based on LSB & DCT",International Journal for Science and Emerging Technologies with Latest Trends,4(1): 35-41 (2012),ISSN No. (Online):2250-3641,

[4] Arunima Kurup P& Poornima D Sreenagesh,"A Novel Technique for Image Steganography Based On Block-DCT and Huffman Encoding",International Journal of Computer Science and Information Technology, 2010

[5] DES Encryption Standard (DES), National Bureau of Standard (U.S.). Federal Information Processing Standards Publication 46, National Technical Information Service, Springfield, VA, 1997.

© 2014-16, IJIRIS- All Rights Reserved

ISSN: 2349-7017(O)
ISSN: 2349-7009(P)
www.ijiris.com

[6] Minati Mishra, Ashanta Ranjan Routray, Sunit Kumar." High Security Image Steganography with Modified Arnold's Cat Map",International Journal of Computer Applications (0975 – 8887),Volume 37– No.9, January 2012

[7] YANG Jie," Algorithm of Image Information Hiding Based on New Anti-Arnold transform and Blending in DCT Domain",Communication Technology (ICCT), 2010 12th IEEE International Conference .

[8] Gyan Vardhan Artist, Dr. Mahesh Kumar Porwal,"Dual Layer Image Scrambling Method Using Improved Arnold Transform",American International Journal of Research in Science, Technology, Engineering & Mathematics,ISSN (Print): 2328-3491, ISSN (Online): 2328-3580, ISSN (CD-ROM): 2328-3629

[9] Chang, C.C., Chen, T.S. and Chung, L.Z., "*A steganographic method based upon JPEG and quantization table modification*", Information Sciences, 2002, 141(1-2), pp.123-38.

© 2014-16, IJIRIS- All Rights Reserved