Secure Data by Espionage Method using Substitution+Steganography

Grishma Trivedi[#1], Chirag Patel[*2], Kishor Bamniya[#3]

[#]*Electronics & communication Department, Gujarat Technical University*
KITRC, Gujarat, India
[1]grishma88trivedi@gmail.com
[3] bamniya.kishor@gmail.com
[*]*EC Department, LCIT*
Gujarat, India
[2] chiragkumar.patel.ec@lcit.org

Abstract— **The internet is a method of communication to distribute information to the masses. Digital image are excellent carriers for hidden information. steganography and cryptography are technologies that are used for secret and secure communications. The authenticity and copyright protection are two major problems in handling digital multimedia. The main purpose in cryptography is to make message concept unintelligible, while steganography aims to hide secret message existence. We propose a method of combining steganography and cryptography for secret data communication. In this we propose high performance steganography along with a substitution encryption methodology of AES algorithm. Embedding approach uses the DCT+DWT technique which used in the frequency domain for hiding data within image. It's very difficult to detect hidden message in frequency domain and for this reason we use steganography based on DCT+DWT. Result shows the algorithm provides high imperceptibility as well as high robustness The effectiveness of the method has been estimated by computing mean square error (MSE) and peak signal to noise ratio (PSNR). This technique for gray BMP image is performs the least loss in cover image.**

Keywords- **Steganography, Cryptography, Encryption, Substitution, DCT, DWT, Mean square error and Peak signal to noise ratio.**

I. Introduction

Hiding data is the process of embedding information in to digital content without causing perceptual degradation In data hiding three famous techniques can be used. They are watermarking, steganography and cryptography[1]. Steganography intent is to hide the existence of the message, while cryptography scrambles a message so it cannot be understood[2].So it's two layers of security in order to maintain data privacy. Data security is the practice of keeping data protected from corruption and unauthorized access. The focus behind data security is to ensure privacy while protecting personal or corporate data[3].Presently we have very secured method for both cryptography and steganography- AES algorithm is a very secure technique for cryptography and steganography methods,which use frequency domain are highly secured.

In steganography possible cover carriers are innocent looking carriers (Image, audio, video, text or some other digitally representative code) which will hold the hidden information. A message in the information hidden, may be plain text, cipher text image or anything that can be embedded in to bit stream. Together the cover carrier and the embedded message create a stego-carrier. Hiding information may requires a stego-key which is additional secret information such as a password required for embedding the information. When a secret message hidden within a cover image the resulting product is a stego-image [2].

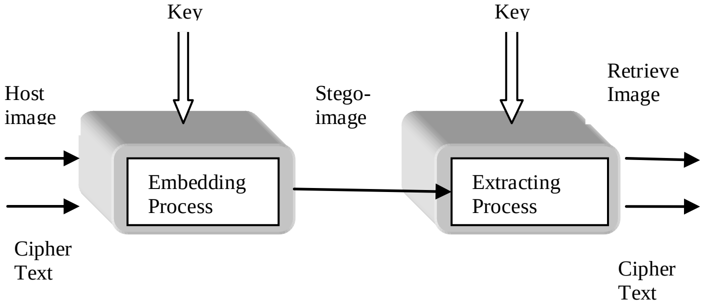


Figure 1.1 Graphical version of the steganographic system

The advantage of steganography is that it can be used to secretly discover. Often using encryption might identify that somebody with something to hide.

Research in steganography technique has been done back in ancient Greek where during that time the ancient Greek practice of tattooing a secret message on the shaved head of a messenger, and letting his hair grow back before sending him through enemy territory where the latency of this communications system was measured in months. The most famous method of traditional steganography technique around 440 B.C. is marking the document with invisible secret ink, like the juice of a lemon to hide information. Another method is to mark selected characters within a document by pinholes and to generate a pattern or signature[4,5]. However, the majority of the development and use of computerized steganography only occurred in year 2000. The main advantage of steganography algorithm is because of its simple security mechanism. Because the steganographic message is integrated invisibly and covered inside other harmless sources, it is very difficult to detect the message without knowing the existence and the appropriate encoding scheme. There are several steganography techniques used for hiding data such as batch steganography, permutation stehanography, least significant bits (LSB), bit-plane complexity segmentation (BPCS) and chaos based spread spectrum image steganography (CSSIS) [6].

A bitmap (bmp) image will be used to hide the data. Data will be embedded inside the image using the pixels. Then the pixels of stego image can then be accessed back in order to retrieve back the hidden data inside the image. Two stages are involved. The first stage is to come up with a new steganography algorithm in order to hide the data inside the image and the second stage is to come up with a decryption algorithm using data retrieving method in order to retrieve the hidden data that is hided within the stego image.

II. Encryption algorithm

Several cryptographic algorithm have been clubbed with steganography to make information hiding more efficient but most of them fail because of the either the weakness of the encryption algorithm used or the steganographic technique used[16].

AES is the next-generation of Encryption Standard. It is basically an improvement over the DES (Data Encryption Standard) as well 3DES. One of its prerequisite is a 128-bit block cipher to replace the current 64-bit ciphers [11].

A. Need for AES/a 128-bit block cipher

1. The key used in various prevalent 64-bit ciphers like DES is too short for acceptable commercial security requirements of today.
2. Recent advances in distributed key-search technique have made the earlier ciphers prone to cryptanalytic attacks.
3. Ciphers like Triple-DES, which despite being 64-bit offer greater number of rounds to meet the required security, are too slow.
4. Another disadvantage of 64-bit ciphers is that the 64-bit block length is open to attacks when large amount of data are encrypted under the same key.

The encryption algorithm that we used is the AES Rijndael algorithm. AES Rijndael is an iterated block cipher, meaning that the initial input block and cipher key undergo multiple transformation cycles before producing the output. The algorithm can operate over a variable-length block using variable-length keys; a 128-, 192-, or 256-bit key can be used to encrypt data blocks that are 128, 192, or 256 bits long, and all nine combinations of key and block lengths are possible. The algorithm is written so that block length and/or key length can easily be extended in multiples of 32 bits, and the system is specifically designed for efficient implementation in hardware or software on a range of processors [12].

AES Rijndael is a substitution-linear transformation network with 10, 12 or 14 rounds, depending on the key size. A data block to be encrypted by AES is split into an array of bytes, and each encryption operation is byte-oriented. AES's round function consists of four layers. In the first layer, an 8x8 S-box is applied to each byte. The second and third layers are linear mixing layers, in which the rows of the array are shifted, and the columns are mixed. In the fourth layer, sub key bytes are XORed into each byte of the array. In the last round, the column mixing is omitted [14].

B. AES substitution(s-box)method

This is a byte-by-byte substitution and the substitution byte for each input byte is found by using the same lookup table. Here sub bytes involve 16 independent byte to byte transformation.The Substitute bytes stage uses an S-box to perform a byte-by-byte substitution of the block. There is a single 8-bit wide S-box used on every byte. This S-box is a permutation of all 256 8-bit values, constructed using a transformation which treats the values as polynomials in GF(2^8) – however it is fixed, so really only need to know the table when implementing. Decryption requires the inverse of the table. These tables are given in Stallings The table was designed to be resistant to known cryptanalytic attacks [7].

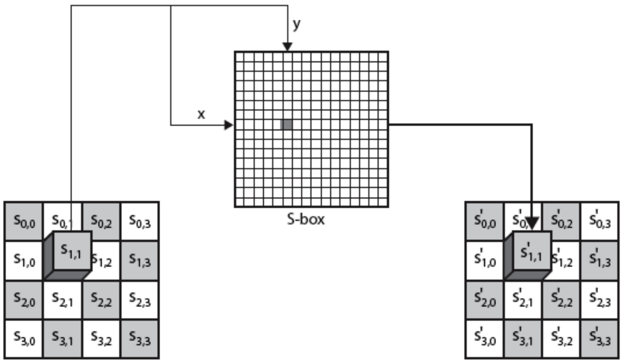

y
x
S-box
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,1}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

Figure 2.1 Basic phenomena of substitution method

1) Interpret the byte as two hexa decimal digits xy.
2) SW implementation use row (x) and column (y) as look up pointer.

Substitution set of s-box followed by pseudo-random permutation step in which bits are shuffled between groups is multiplied out in matrix fashion and result are added to sub key for the round. Here we experiments for the 24-character as secret text message. This used linear substitution with 10 rounds and 128 bit key size.

III. EMBEDDING ALGORITHM

The algorithm proposed is a combined DCT/DWT based process. In the proposed algorithm the benefits of DWT are taken into consideration in choosing the most proper subband for watermark embedding in order to provide both robustness and imperceptibility and hence the LL subband is chosen after performing one level DWT on the host image[14]. Compared to the different DCT/DWT based algorithms proposed in the literature the proposed algorithm exhibits higher robustness and imperceptibility and the computational complexity involved in the algorithm is less. The algorithm is very easy to implement and less time consuming.

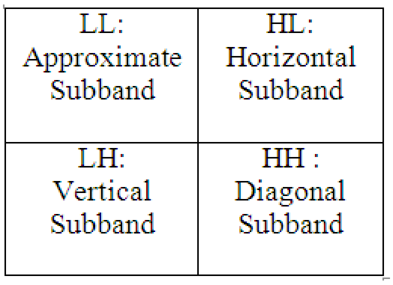
The wavelet transform has several advantages : The DWT is a multi-resolution description of an image: the decoding can be processed sequentially from low resolution to higher resolutions. The DWT is closer to human visual system than DCT [9]. Hence, the artifacts introduced by wavelet domain coding with high compression ratio are less annoying than those introduced at the same bit rate by DCT.

In the DWT-DCT method, the most proper sub-bands are selected to take these benefit of DWT in case of robustness and imperceptibility. Then, the block based DCT is applied on these selected band to embed watermark in middle frequencies of each block to improve further robustness of watermarked image. By combing the two common frequency domain methods, we could take the advantageous of both two algorithms to increase robustness and imperceptibility. Improvement in the performance in DWT-based digital image watermarking algorithms could be achieved by combing DWT with DCT. Two transforms are combined to make up for the disadvantages of each other, so as to increase the effectiveness of watermarking algorithm [8].

A. DWT(Discrete Wavelet Transform)

Discrete Wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image. It is useful for processing of non-stationary signals [10]. The transform is based on small waves, called wavelets, of varying frequency and limited duration. Wavelet transform provides both frequency and spatial description of an image. Unlike conventional Fourier transform, temporal information is retained in this transformation process. Wavelets are created by translations and dilations of a fixed function called mother wavelet. This section analyses suitability of DWT for image watermarking and gives advantages of using DWT as against other transforms [12].

The Cover image is a NxN gray image. The sub bands LL, HL, LH, and HH are referred as shown in the figure. LL-A, HL-H, LH-V and HH-D. A (Approximation sub band) H (Horizontal sub band),V(Vertical sub band) and D(Diagonal sub band)[8].



LL: Approximate Subband	HL: Horizontal Subband
LH: Vertical Subband	HH : Diagonal Subband

Due to its excellent spatiofrequency localization properties, the DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively. In general most of the image energy is concentrated at the lower frequency sub-bands LLx and therefore embedding watermarks in these sub-bands may degrade the image significantly.Embedding in the low frequency sub-bands, however, could increase robustness significantly. On the other hand, the high frequency sub-bands HHx include the edges and textures of the image and the human eye is not generally sensitive to changes in such sub-bands.

Here we used the LL sub band to hide the cipher text which we get after encryption process [12].

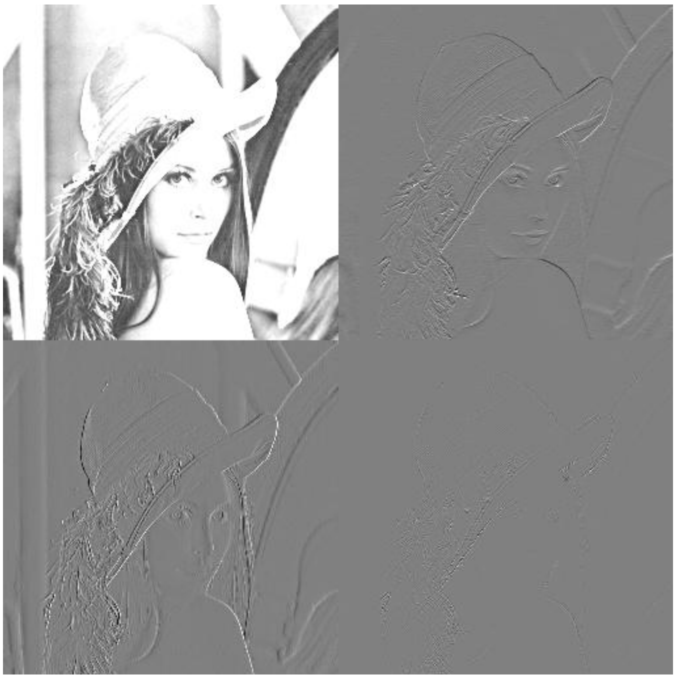


Figure 3.1 single level decomposition on lena image

Figure shows the four sub-bands on standard lena image, where LL sub band is more clearly visible. So we hide our cipher text in it by performing DCT transformation next.

The DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively [8,10]. In particular, this property allows the exploitation of the masking effect of the human visual system such that if a DWT coefficient is modified, only the region corresponding to that coefficient will be modified. In general most of the image energy is concentrated at the lower frequency coefficient sets LL and therefore embedding watermarks in these coefficient sets may degrade the image significantly. Embedding in the low frequency coefficient sets, however, could increase robustness significantly.

B. DCT(Discrete Cosine Transform)

A transformation function, which transform the representation of data from space domain to frequency domain. The twodimensional DCT of an M-by-N image A is defined as follows

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

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

The DCT Inverse transform is given by

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

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

This transform allow an image to be broken up in to various frequency bands and making it easier to embed watermarking information in to the middle frequency bands of an image[9]. The middle frequency bands are elected such a way they have diminished to avoid the largest visual important parts of the image without over exposing themselves to eliminate.

B1 Embedding Process

In the Embedding algorithm, when the message bit is a ‘1’ then it is checked whether (5,2) is less then (4,3) or not. Stipulation answer is not then the two blocks are swapped so as to formulate (5,2) < (4,3). Likewise, whilst the message bit is a ‘0’ then it is checked whether (5,2) is greater than (4,3) or not .Stipulation answer is not then the two blocks are swapped so as to make (5,2) > (4,3).The swapping of such coefficients should not alter the watermarked image extensively because generally assumed that DCT coefficients of middle frequencies have similar magnitudes. The robustness of the watermark can be enhanced by strength constant *k*, such that (5,3) – (4,3) > *k*. Condition of the coefficient does not meet the criteria, then modified while the use of random noise when satisfy the relation. Increasing *k* consequently reduces the chance of detection errors at the expense of further image degradation.

B2 Extraction Process

During extraction process whole color image is broken down up into 8x8 alike blocks and discrete cosine transform performed on it. Each block is checked that whether the block (5,3) is greater than block (4,2). When (5,3) > (4,3) then ‘0’ is detected otherwise ‘1’ is detected.

IV. PROPOSED ALGORITHM

A. Watermark Embedding

Step 1: Acquire the gray scale bitmap image.
Step 2: Detach gray frame of the cover image.
Step 3: Read the message image (cipher text in matrix form) and which is to be embed in the respective gray frame.
Step 4: Take block discrete cosine transform of gray frame in isolation.
Step 5: Take the first block of the transformed frame.
Step 6: Ensure the message bit, if it is ‘1’ then take values of (5,2) and (4,3) coefficients of a frame of a block , if values of (5,2) is greater than (4,3) then swap the values of blocks otherwise keep both values as it is. Now, analysed the difference (4,3) and (5,2). If difference is less than k, compute new values for the coefficients; otherwise keep values of the coefficients as it is.
New values of the coefficients are calculated as following.
(4,3) = (4,3) + k/2;
(5,2) = (5,2) - k/2;
If message bit is ‘0’ then, Take values of (5,2) and (4,3) coefficient of a frame of a block , if values of (5,2) is less than (4,3) then swap the values of blocks otherwise keep both values as it is. Now, analysed the difference (5,2) and (4,3). If difference is less than k, compute new values for the coefficients; otherwise keep values of the coefficients as it is.
New values of the coefficients are calculated as following.
(5,2) = (5,2) + k/2;
(4,3) = (4,3) - k/2;
Step 7: Perform inverse discrete cosine transform of secured image.

B. Watermark Extraction

Step 1: Acquire the secured image.
Step 2: Get the frame from the gray scale image
Step 3: Perform block discrete cosine transform for a frame
Step 4: Check the coefficients (5,2) and (4,3). If (5,2) is greater than (4,3) then save the message bit ‘0’ and otherwise save message bit as a ‘1’.

V. EXPERIMENTAL RESULTS

We are taking a variety of images and observe the results, which is show in this section. Our results show, the effectiveness and success of secured information in frequency domain [13].Check the image quality using peak signal to noise ratio and mean square error formula.

$$PSNR = 10 \lg\left(\frac{255^2}{E}\right) dB$$

Where, *255* is the maximum possible pixel value of the image. The mean square error (MSE) of an image with 3 * m * n pixels is defined as,

$$\mathrm{MSE} = \frac{1}{M * N} \sum_{i=1}^{M} \sum_{j=1}^{N} (X_{ij} - W_{ij})^2$$

we gets the below results for parameters like elapsed time of CPU , PSNR and MSE of watermarked images. Where elapsed time means cpu start time, how much time it’s took for the process which gives the output in sec.

Here stego-image content the text data of 24-chractres, Depends on the size of the cover image you can hide the data behind the pixels. Below figures shows the original and watermarked images of lena.bmp and baboon.bmp with their histograms.

Fig-5.1 lena Image

Fig-5.2 Stego lena Image

Below is the histogram of the Original image as well as stego-image (watermarked image).

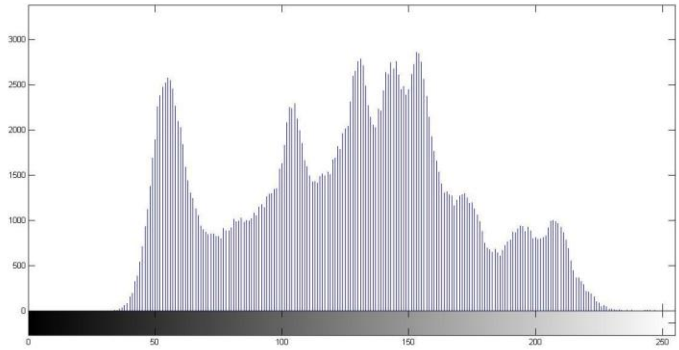


Fig-5.1.1 Histogram of Original lena image

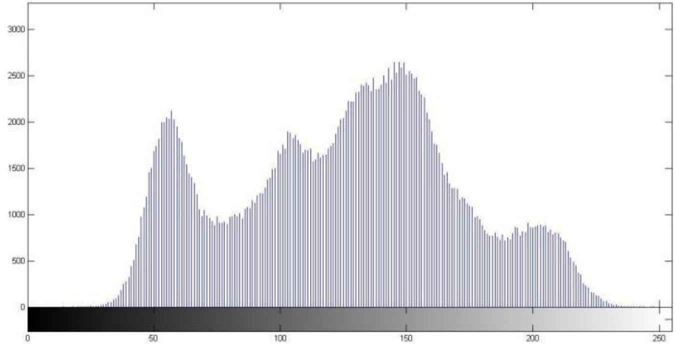


Fig-5.2.1 Histogram of Stego lena Image

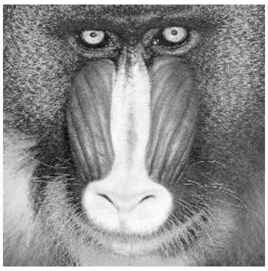


Fig-5.3 Baboon Image

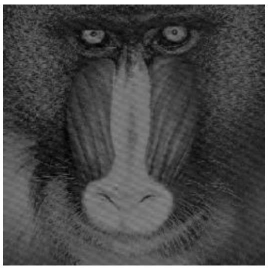


Fig-5.4 Stego Baboon image

Histogram of baboon original as well stego image respectively.

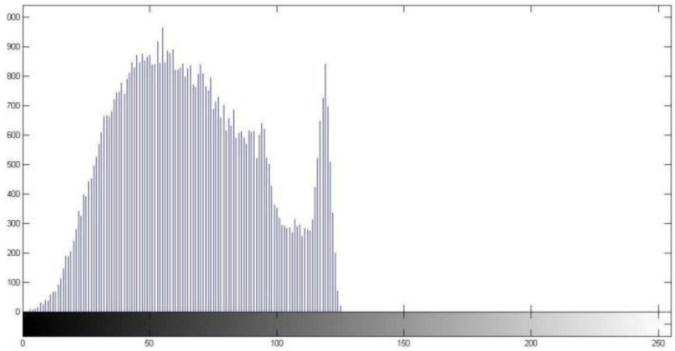


Fig-5.3.1 Histogram of Original Baboon Image

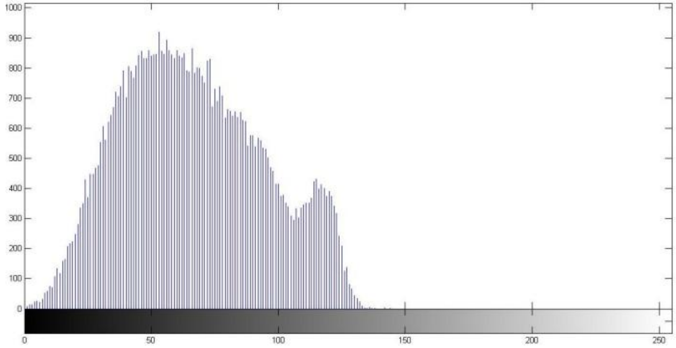


Fig-5.4.1 Histogram of Stego Baboon Image

On the basis of the histogram one can say the presence of any hidden data cause of the visible comparative difference of the histograms of images.

Below table shows the PSNR, MSE and elapsed time (compute time) of some watermarked images (stego-images).

Gray scale watermarked images (512*512) with block size 8

	Image	MSE(dB)	PSNR(dB)	Execution Time(sec)
1	lena	27.5662	33.7270	0.7956
2	baboon	7.5428	39.3555	0.4056
3	Photo1	30.5941	33.2749	1.3260
4	barbara	31.8236	33.1033	0.7332
5	peppers	30.4296	33.2978	1.0140
6	lion	26.5168	33.8956	0.9672
7	girl	25.5168	34.0610	0.7800
8	Home	33.9139	32.870	0.7332

VI. CONCLUSION

The benefit of the embedding message in gray scale image is that it makes image low profile. Due to double security of algorithm even if presence of message identified it’s become difficult for eavesdroppers to extract the original secret data without the encryption key. Gets the best result in baboon image with high PSNR and quite low MSE comparatively.And all results available in table are achieved at the zero bit error rate (No loss of secret information) so it can be consider as intact and most efficient method.

Acknowledgment

Author need to thank the KITRC (Kalol Institute of Technology) and L.C.Institute of Technology (Bhandu) for gives required resource's facilities and providing guidance. I wish to place on record my profound gratitude to Gujarat Technical University for the unique opportunity to indulge this paper.

REFERENCES

[1] Current Steganongraphy approach : A survey, IJARCSSE , Volume-1 issue-1 December- 2011.

[2] Steganography – A data hiding Technique , International Journal of computer application (0975-8887) Volume 9- No. 7,November – 2010.

[3] Steganography Image system (SIS) : Hiding secret message inside an image, Proceedings of the world congress on Engineering and computer science , Volume 1, October-2010.

[4] Digital Image Steganography: Survey and analysis of current Methods, Faculty of Computer and engineering, United kingdom, March 2010.

[5] An over view of Image steganography, ICSA, Research group department of computer science

[6]Steganography algorithm to hide secret message inside an image.Computer technology and application,February-2011

[7]Federal Information Processing Standards Publication 197 . November 26,2001.Announcing the Advanced Encryption Standards (AES).

[8] Robust watermarking scheme based on discrete wavelet transform and discrete cosine transform for copyright protection., IJCSNS, vol-11,aug-2011.

[9] Implementation of secret information hiding using frequency domain technique,IEEE,2011.

[10] A DWT Based Approach for Image Steganography , International Journal of Applied Science and Engineering2006. 4, 3: 275-290.

[11] COMBINING JPEG STEGANOGRAPHY AND SUBSTITUTION ENCRYPTION FOR SECURE DATA COMMUNICATION,David C. Wyld, et al. (Eds): CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 149–160, 2012.

[12] New comparative study between DES,3-DES and AES within nine factors, Journal Computing,volume 2,Issue 3,March-2010,ISSN 2151-9617

[13] Comparison of Digital Image watermarking Methods DWT & DWT-DCT on the basis of PSNR.IJIRSET,Volume-1,Issue-2,December-2012,ISSN 2319-8753.

[14] A combined DCT/DWT based watermarking algorithm.Deaprtment of Ec, Assam.

[15] Modification to AES algorithm for complex Encryption. IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.10,October 2011.